LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

IT-policyer i organisationer:

En fallstudie av anställdas informationsäkerhetsmedvetande

Kandidatuppsats 15 HP, INFK11, VT16

Författare: Henrik Greco, 861120-1412
Jesper Östling, 891028-4010

Handledare: Umberto Fiaccadori

Examinator: Markus Lahtinen
Anders Svensson

IT-policyer i organisationer:

En fallstudie av anställdas informationsäkerhetsmedvetande

Författare: Henrik Greco och Jesper Östling

Utgivare: Institutionen för informatik, Ekonomihögskolan, Lund Universitet

Dokumenttyp: Kandidatuppsats

Antal sidor: 67

Nyckelord: Informationssäkerhet, Informationssäkerhetspolicy, ISA, Efterlevnad och Medvetenhet, TPB och RCT.

Sammanfattning

Informationssäkerhet blir allt mer aktuellt inom företagsvärlden. Information anses vara en organisations största tillgång och organisationer utsätts ständigt för inre och yttre hot. Traditionellt har man sett detta som ett tekniskt problem med tekniska lösningar, men det största hotet är de anställda som genom illvilja, omedvetet slarv eller brist på kunskap inte beter sig säkert. Detta hanteras genom att ta fram och etablera policyer kring säkerhetsarbetet, men det är utbrett att organisationer brister i att etablera dessa bland anställda, vilket kan motverkas genom utbildning. Författarna har genom en kvalitativ enkätundersökning undersökt anställda inom fyra företag för att analysera deras medvetande och agerande kring säkerhetspolicyer och jämfört resultatet med tidigare forskning. Undersökningen kom fram till att medvetenheten var högre än väntat och att de anställda som ansåg sig känna till policyer följde dessa. Det framgick att människor kan ha grundläggande kunskaper om säkerhet i tekniska hjälpmedel även om de inte är utbildade av arbetsgivaren, men de applicerar detta i högre utsträckning i privatlivet än i organisationen. I resultatet syns en koppling mellan utbildning, medvetande och efterlevnad kring policyer och att de med högre utbildning tog konsekvenser för arbetsgivaren i beaktning i större utsträckning än de med lägre utbildning.

Innehåll

Förkortningar

ISA – Information Security Awareness

ISP – Information Security Policy

ISP Awareness – Information Security Policy Awareness

TPB – Theory of Planned Behavior

RCT – Rational Choice Theory

Figurer

Tabeller

1. Inledning

I detta kapitel beskrivs bakgrunden till uppsatsens ämne och en mer specifik beskrivning av problemområdet ges. Detta mynnar ut i uppsatsens frågeställning och vad syftet med att besvara denna är. Slutligen beskrivs de avgränsningar som gjorts runt frågeställningen.

1.1 Bakgrund

Informationssystem har länge använts av organisationer och utgör idag en väsentlig del av deras verksamhet. Enligt många kan information ses som en organisations största tillgång och till och med organisationens ryggrad (Häussinger, 2015). Med användning av informationssystem tillkommer risker kring hot som kan orsaka stora skador och dessa risker är idag en av de största utmaningarna en organisation står inför (Bulgurcu et al. 2010). Arbetsområdet med att minska dessa risker och skydda sig från utomstående hot kallas för informationssäkerhet.

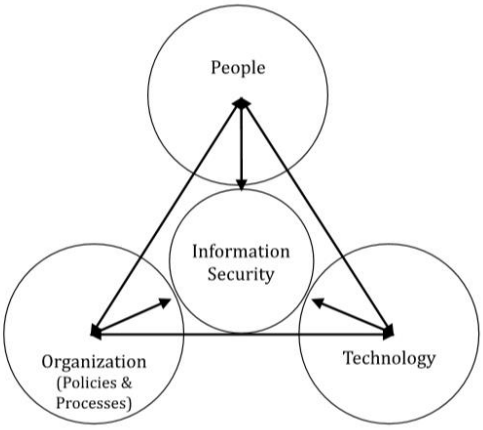
När internet blev allmängods uppstod stora säkerhetsluckor eftersom tekniken var skapad för slutna nätverk, vilket motarbetades med tekniska lösningar som antivirusprogram, brandväggar och kryptering (De Leeuw & Bergstra, 2007). På senare år har det uppmärksammats att det inte räcker med tekniska lösningar på säkerhetsproblem eftersom människor har visats utgör den största risken (Sherif, Furnell, & Clarke, 2015). Idag ligger stort fokus akademiskt på att komma till rätta med dessa problem, men företagsvärlden ligger fortfarande efter och fokuserar på tekniska aspekter av säkerhet. I de fall som policyer och strategier runt det mänskliga beteendet tagits fram är det sällan de förankras i organisationen, vilket leder till liten eller ingen förändring bland personalen (Safa, Von Solms, & Furnell, 2016; Chen, Wen, & Ramamurthy, 2012).

Organisationer ser fortfarande informationssäkerhet som ett tekniskt problem som ägs av en IT-avdelning, när det egentligen borde vara ett problem som genomsyrar hela organisationen i en mer holistisk anda (LeVeque, 2006). Detta hänger också ihop med det faktum att det är den mänskliga faktorn som utgör den största risken och att det därför är viktigt att inkludera alla anställda i säkerhetsarbetet (Sherif, Furnell, & Clarke, 2015). Organisationer kan åtgärda många yttre hot med antivirusprogram och brandväggar, men dessa löser inte problemet med naiva eller fientligt inställt anställda (Waly, 2013).

Det är alltså den mänskliga faktorn som anses vara den absolut viktigaste delen och den största svagheten i informationssäkerhet (Häussinger, 2015; Safa, Von Solms, & Furnell, 2016; Bulgurcu et al. 2010; Tariq, Brynielsson, & Artman, 2014). Det finns många olika åtgärder för att uppnå och upprätthålla ett effektivt arbete med informationssäkerhet; Allt från teknologiska lösningar till arbete med anställdas medvetenhet om befintliga risker tas upp, men den mest avgörande åtgärden som tas upp är arbetet med informationssäkerhetspolicy (Hädanefter ISP) (Höne & Eloff, 2002).

Trots detta känner de flesta anställa inte till sin organisations policyer och strategier kring informationssäkerhet och det dagliga arbetet kring dessa (Von Solms & Von

Solms, 2004). I figur 2 nedan ser man hur olika delar tillsammans utgör informationssäkerhet.



Figur 1, Informationssäkerhetenstriangeln, (Nayak & Rao, 2014, s. 43).

Som figuren visar handlar informationssäkerhet om teknik, organisation och den mänskliga faktorn, men fokus ligger alltså oproportionerligt mycket på tekniken.

Denna uppsats ämnar undersöka ämnet på typiska arbetsplatser och har fokuserat på företag inom Hospitality (hotell, vandrarhem) och detaljhandeln. Dessa båda branscher har som praxis att använda informationssystem. I båda branscherna finns arbetssätt som kan vara talande för många arbetssituationer inom fler branscher när det gäller informationshantering, som hanterande av kundinformation och statistik.

1.2 Problemområde

Informationssäkerhet är inte ett nytt ämne inom företagsvärlden, men det innebär ett kostsamt och tidskrävande arbete vilket leder till att många företag ändå ligger efter (Gollman, 2011). Det är också många företag som skapar policyer och strategier runt sitt arbete med informationssäkerhet, för att sedan lägga dessa åt sidan utan att införliva dem i organisationens arbete, eller se till att de som jobbar i organisationen har kännedom om dessa (Chen, Wen, & Ramamurthy, 2012). Det de inte inser är att hotbilden förändras med tiden och att det inte går att bara släcka bränder som startar utan att organisationer också måste vara pro-aktiva och jobba för att undgå hot redan innan de uppstår (Gollman, 2011).

Ett centralt hot mot informationssäkerhet är slarviga anställda som inte följer ISP (Siponen et al. 2014). Tidigare litteratur påvisar också att användares ovilja att följa informationssäkerhetspolicy ofta ses som ett av de mest centrala problemen inom informationssäkerhet för organisationer (Puhakainen & Siponen, 2010). Att anställda bryter mot informationssäkerhetspolicy kan ofta härledas till deras ignorans eller okunskap om dessa och uppskattningsvis sker mer än hälften av alla säkerhetsöverträdelser inom informationssystem på grund av att de anställda inte följer ISP (Siponen & Vance, 2010).

1.3 Frågeställning

I vilken omfattning efterlevs IT-policyer avseende anställdas informationssäkerhetmedvetande inom en organisation?

1.4 Syfte

Syftet med uppsatsen är att undersöka i vilken omfattning slutanvändare av IS-system är medvetna om och efterlever IT-policyer inom informationssäkerhet. Denna uppsats ämnar göra detta genom att genomföra en kvalitativ enkätundersökning med användare av informationssystem hos organisationer, för att sedan jämföra resultaten med den befintliga litteraturen på det aktuella området. I samband med denna jämförelse hoppas författarna se om teorierna kring mänskligt beteende och efterlevnad av IT-säkerhetspolicys är applicerbara på de undersökta företagen.

1.5 Avgränsningar

Uppsatsen undersöker enbart policyer gällande IT-säkerhet och inte IT i allmänhet. En ytterligare avgränsning är att den bara behandlar information i tekniska hjälpmedel och inte manuell informationshantering (Pärmar, Whiteboards etc.), eftersom ämnet för uppsatsen är informatik där informationssystem har en ledande roll och mer och mer ersätter manuellt hanterande av data. I de fall policyer gått att ta del av har detta gjorts, men enbart för att hjälpa till vid utformning av enkäten då studien inte undersöker själva policyerna i sig. De som tillfrågats är anställda "på golvet" som inte är i någon chefsposition, eftersom chefer bör vara väl insatta i arbetet kring it-policyer och det som undersöks är de anställdas attityder och om de efterföljer policyer. Av den anledningen har inte heller chefer ansetts kunna tillföra någonting till denna uppsats då det som undersöks inte är efterlevnad i relation till vad företaget ansett sig utföra för aktiviteter.

2. Teori

I detta kapitel presenteras befintlig litteratur som är relevant inom området för uppsatsens syfte och frågeställning. Det som beskrivs är det som oftast dykt upp under förstudierna till uppsatsen. De olika områdena är uppdelade i underkapitel för att läsaren lätt ska kunna bilda sig en uppfattning om varför de är relevanta. I slutet på kapitlet återfinns en sammanfattning och en sortering av författarna samt vilket område i teorin de tillhör.

2.1 Vad är informationssäkerhet?

Informationssäkerhet handlar om att skydda en organisations information, vilken kan ses som dess största tillgång och basen till dess verksamhet (Häussinger, 2015), från att missbrukas, delas med obehöriga eller bli stulen, vilket kallas för informationsläckor.

Informationssäkerhet kan ses som en triangel vars tre sidor består av människor, teknologi och organisation (Tariq, Brynielsson, & Artman, 2014). Det handlar om teknisk infrastruktur, organisation, anställda och andra komponenter som samlar och behandlar information (till exempel datorer), samt hur system har blivit inskränkta för att skydda informationen genom till exempel kryptering och behörighetskrav (De Leeuw & Bergstra, 2007). Det var det amerikanska försvarsdepartementet som först, i en rapport publicerad 1970, kom fram till att säkerhet i informationssystem var ett problem som rörde designen av själva informationssystemet, varpå de 1973 utvecklade de första informationssäkerhetspolicyerna. TCP/IP-tekniken skapades först för stängda nätverk så som militären, varför stora säkerhetsbrister i form av till exempel virus uppstod när internet delades med allmänheten. Som följd uppstod en rad tekniska kommersiella lösningar som brandväggar och antivirusprogram. Idag ligger stort fokus på de mänskliga aspekterna av informationssäkerhet, då det är allmänt känt, åtminstone i den akademiska världen, att det är människor som är den största risken (Sherif, Furnell, & Clarke, 2015).

2.2 Vad är informationssäkerhetspolicyer?

Policyer kan generaliseras som ett eller flera dokument i vilka, enligt ledningen, önskat eller förväntat beteende för de anställda inom organisationen är dokumenterat (LeVeque, 2006). Det är vanligt med policyer som till exempel beskriver regler kring hur lösenord skapas, hur de ska se ut och hur ofta de ska bytas. Hur dessa policyer sedan anammas av de anställda påverkas av deras attityd gentemot dem, positiv attityd innebär starkt lösenord och vise versa (Choong & Theofanos, 2015; Knapp & Ferrante, 2012). Vidare säger LeVeque (2006) att en bra policy ska beskriva vem som ska göra vad, samt vad anställda får och inte får göra. Likt LeVeques (2006) förklaring av en policy, förklarar Höne & Eloff (2002) att en informationssäkerhetspolicy är ett dokument i vilket riktlinjer ges för hantering av information, att det indikerar ledningens åtagande och support, samt vilken betydelse informationssäkerhet har för organisationens vision och mål. Informationssäkerhets-policyer ska också förklara behovet av informationssäkerhet och reflektera hur

ledningen på ett säkert och kontrollerat sätt vill styra organisationen (Höne & Eloff, 2002). Informationspolicyer ger instruktioner till de anställda om vad de ska göra i olika situationer när de interagerar med informationssystemet och informations-resurser inom organisationen (Bulgurcu et al. 2010).

Det är viktigt att se till att säkerhetshanteringen är konsekvent genom hela organisationen, vilket går att uppnå genom starkt ledarskap (LeVeque, 2006). Av samma anledning är det viktigt att säkerhetsansvariga känner till hur organisationens ledarskapskultur fungerar. Konsekvenserna av att information läcker från en organisation kan innefatta att kunder tappar tillit till organisationen, inkomstbortfall och lagbrott (Khan, Alghathbar & Khan, 2011).

2.3 Den mänskliga faktorn

Många studier visar att organisationer i sin problemlösning runt informationssäkerhet har fokuserat på tekniska perspektiv snarare än processerna kring säkerhetshantering och tidigare forskning bekräftar att många traditionellt har sett informationssäkerhet som just ett tekniskt problem med tekniska lösningar. Eftersom det är människor som jobbar med informationssäkerheten så går det inte att se det som ett rent tekniskt problem, utan organisationer måste inse att de anställdas beteenden och attityder kring organisationen kan skada företagets verksamhet. Detta eftersom de anställda direkt påverkar hanteringen av informationssäkerhet. Därför är det viktigt att se arbetet kring informationssäkerhet som ett problem för styrningen av en organisation och inte bara som en del av IT-avdelningens arbetsuppgifter. Det bör vara någonting holistiskt som genomsyrar hela organisationen. (LeVeque, 2006)

Många av svårigheterna med den mänskliga faktorn beror på att individer både har en personlig och en social identitet såväl som en som är kopplad till deras yrkesroll (Ashenden, 2008). Ashenden (2008) menar att organisationen måste arbeta med sin kultur och kommunikation mellan olika deltagare i organisationen. Vidare säger Ashenden (2008) att det ligger en stor utmaning i att hantera människors säkerhetsarbete i en organisation eftersom samma individ reagerar olika på liknande situationer och därför är oförutsägbar.

Den vanligaste anledningen till användarmisstag är brist på kunskap om informations-säkerhet, ignorans, oaktsamhet, apati, ont uppsåt och motstånd (Safa, Von Solms, & Furnell, 2016). Detta innebär att även personer med gott uppsåt kan vara en reell säkerhetsrisk, genom att till exempel dela med sig av inloggningsuppgifter till kollegor eller skriva upp dem på klisterlappar som sätts på datorn, öppna länkar i e-mail från osäkra avsändare, ladda ner program till jobbdatorn från tveksamma källor, fortsätta att vara inloggad i systemet när det lämnas för till exempel toalettbesök och så vidare (Safa, Von Solms, & Furnell, 2016).

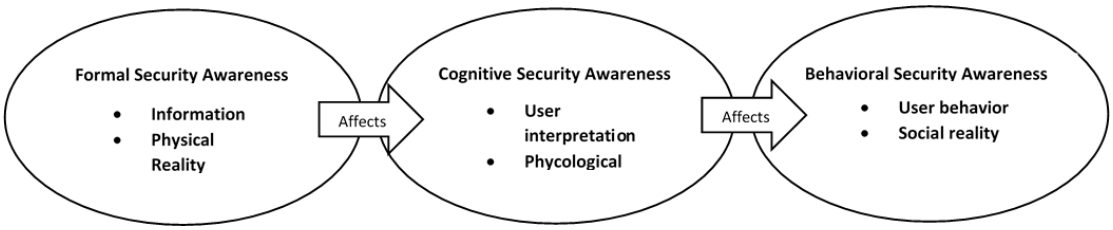
Även kunskapsbrist eller ovilja att använda tekniska säkerhetslösningar på ett korrekt sätt är en stor del av problematiken med den mänskliga faktorn i informationssäkerhet (Kauer et al. 2013).

Den kanske viktigaste aspekten i mänsklig informationssäkerhet är ”ISA” (information security awareness, eller informationssäkerhetsmedvetenhet) vilken kan uppnås genom bland annat informationsdelning (Safa, Von Solms, & Furnell, 2016; Tariq, Brynielsson, & Artman, 2014).

2.4 ISA (Information Security Awareness)

”Security Awareness” används i flertalet forskningsområden och handlar om hur medvetna vi är angående risker i vår närmiljö (Hellqvist et al. 2013; Siponen, 2000). ISA behandlar denna medvetenhet men ur perspektivet informationssäkerhet bland deltagarna i en organisation, där anställda följer regler som finns, förstår potentialen i dessa, samt förstår vikten av ansvarsområden och att de agerar i enlighet med detta (Ahlan, Lubis, & Lubis, 2015). Att det sker så många säkerhetsincidenter som beror på den mänskliga faktorn innebär att det måste läggas mer uppmärksamhet på hur individer, organisationer och miljö påverkar detta, för att kunna optimera arbetet med ISA.

ISA kan ses som att det vilar på tre grundvalar som ska finnas i paritet med varandra; formell, kognitiv och beteendemässig medvetenhet. Formell medvetenhet handlar om de policys och strategier som finns, kognitiv medvetenhet handlar om hur användarna förstår dessa kognitivt och beteendemässig medvetenhet om hur användarna agerar på denna medvetenhet (se figur 2). (Hellqvist et al. 2013)



Figur 2. ISA enligt Hellqvist et. al. (2013, s. 6)

Bulgurcu et al. (2010) definierar ISA som en anställds generella kunskap och förståelse kring informationssäkerhet och dennes medvetenhet om gällande informationssäkerhetspolicy inom organisationen (”ISP awareness”). En anställd kan ha vetskap om att lösenord är viktigt att använda men inte veta om att organisationens ISP kräver en viss utformning av lösenordet eller att det ska ändras regelbundet. Detta tyder på en generell kunskap om informationssäkerhet hos användaren men en bristande ”ISP awareness” (Bulgurcu et al. 2010). Utan tillräcklig ISA är risken stor att säkerhetsåtgärder missuppfattas eller används på fel sätt av användarna, vilket i sin tur kan orsaka att en säkerhetsåtgärd som egentligen fungerar blir otillräcklig (Siponen, 2000). Ett ökat ISA bör leda till att användarfelen minimeras samtidigt som säkerhetsprocedurer maximeras från ett användarperspektiv (Siponen, 2000).

När anställda har en hög nivå av medvetenhet förstår de risker bättre och anstränger sig mer för att se till så att organisationen är säker. Det betyder både att de skyddar organisationens intressen från utomstående hot och att risken för interna hot minskar i och med den anställdes vilja att hålla företaget säkert. På detta sätt är i hur framgångsrik en organisation är i sitt säkerhetsarbete. Trots detta har de flesta anställda i organisationer en låg nivå av ISA. (Häussinger, 2015)

Det finns dock en koppling till tekniken. Bland annat har det visat sig att användare tar större risker när de vet att det finns säkerhetsprogramvara installerad på datorn (Tariq, Brynielsson, & Artman, 2014). Alltså finns det en paradox i att ju mer

medveten en person är om vad företaget vidtagit för säkerhetsåtgärder, desto större risker tycker de sig kunna ta.

2.4.1 ISP Awareness (Information Security Policy Awareness)

ISP Awareness är en del av ISA men handlar specifikt om medvetenheten runt informationssäkerhetspolicyer (Hellqvist et al. 2013). Det har visat sig att när en organisation har kommunicerat sina policyer på ett adekvat sätt och på så sätt skapat en bra medvetenhet hos deltagarna i organisationen (med andra ord att formell och kognitiv medvetenhet är på en tillfredställande nivå) så har deltagarna ändå inte följt policyer. Detta tyder på att ovilja att följa befintliga policyer främst ligger i deltagarnas beteende och mer specifikt deras underliggande anledningar till att sätta sig emot att följa policyer. För att skapa en bra säkerhetskultur räcker det därför inte att skapa bra policyer och förmedla dem på ett tillräckligt sätt, utan det är nödvändigt att gå till botten med varför deltagare inte följer dem när så är fallet genom att studera deltagarnas beteenden och attityder, vilket bland annat Sang Hoon et al. har gjort (2014).

En anställds medvetenhet om befintliga informationssäkerhetshot ses som generell ISA medan om en anställd vet vad denne ska göra i olika situationer tyder på ISP awareness. För att uppnå efterlevnad av ISP hos de anställda, måste de förstå vad som motiverar dem till att följa ISP. Detta är ett beteendeproblem som informationssäkerhets-management står inför. (Bulgurcu et al. 2010)

2.5 Informationssäkerhetsträning

Olika former av träning har visats öka anställdas ISA och detta har i sin tur påverkat deras attityd mot informationssäkerhet och efterlevnad av ISP (Safa, Von Solms, & Furnell, 2016). Tidigare litteratur har undersökt olika tillvägagångsätt för att uppnå efterlevnad av ISP. Dessa inkluderar bland annat sanktionsbaserade metoder, som menar till att avskräcka anställda från att inte följa ISP genom olika påföljder och vanlig träning eller utbildning, vilket är ett av de vanligast föreslagna tillvägagångsätten. (Puhakainen & Siponen, 2010) Till skillnad från sanktionsbaserade metoder riktar sig träning av ISP till att övertyga anställda och aktivera dem att tänka själva inom området, för att på så sätt få dem att ta till sig och förstå vikten av att följa säkerhetspolicyer. Samtidigt som det har visat sig att sanktionsbaserade tillvägagångsätt har minskat säkerhetsöverträdelser och ökat efterlevnad hos de anställda, så visar mycket forskning att kognitiv träning och utbildning kan vara än mer effektivt för att uppnå detta. (Puhakainen & Siponen, 2010) Olika träningsmoment som kan användas är kurser, formella presentationer, workshops, hemsidor och nätbaserad utbildning (Safa, Von Solms, & Furnell, 2016).

Träning handlar inte bara om att skapa ett medvetande hos de anställda om rådande ISP och varför de måste följas, det innebär också att utbilda de anställda kring tekniken som behövs för att följa en viss policy och hur de ska göra för att följa den.

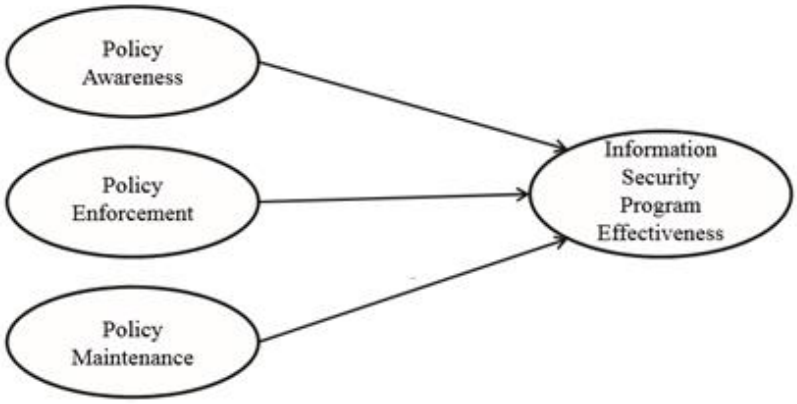
"Practitioners should strive to simplify the security procedures that employees are required to perform and provide adequate training to their employees so employees will not perceive the requirements and procedures specified by the ISP as burdensome." (Bulgurcu et al. 2010, s. 542)

Vidare säger Bulgurcu et al. (2010) att en anställds uppfattning om sin förmåga att genomföra en uppgift, i detta fall att följa ISP, positivt påverkar dennes avsikt att efterleva ISP och att det därför är mycket viktigt att en organisation tränar sina anställda så att de vet vad som måste göras för att följa de befintliga informationssäkerhetspolicyerna. Det är förekommande att anställda gör valet att kringgå säkerhetsåtgärder om det behövs för att kunna slutföra en viss uppgift (Ifinedo, 2012). Organisationer bör sträva efter att ha en säkerhetsmedveten kultur, vilket kan skapas genom awareness programs (se 2.5.1 awareness programs) som ska öka ISA hos de anställda och säkerställa deras förmåga att genomföra uppgifter för att följa ISP (Bulgurcu et al. 2010).

Träning för att uppnå högre efterlevnad av ISP bör involvera metoder som motiverar användarna till kognitiv bearbetning av informationen de tar till sig. Det är också viktigt att en kontinuerlig kommunikation kring ämnet etableras inom organisationen. (Puhakainen & Siponen, 2010)

2.5.1 Awareness programs

Det är viktigt för organisationer som hanterar känslig information att aktivt se till att det finns formella policyer som underhålls, uppdateras och etableras i arbetsstyrkan. Det gäller också att hålla en balans i sina policyer, eftersom en allt för sträng attityd kan påverka organisationens lönsamhet negativt och motarbeta organisationens mål, medan en allt för slapp attityd kan få allvarliga konsekvenser i och med information som äventyras (Knapp & Ferrante, 2012). Knapp & Ferrante (2012) visar med en modell, se figur 4 nedan, vad som påverkar effektiviteten av ett awareness program.



Figur 3. Effektivitet av ett awareness program (Knapp & Ferrante, 2012, s.70).

Studier har visat att många människor inte känner till sin organisations policyer och strategier, i de fall sådana finns (Von Solms & Von Solms, 2004). Istället har det visat sig att de anställda i en organisation ofta inte är särskilt motiverade att följa säkerhetspolicyer och att de snarare följer invanda beteendemönster och rutiner utan större intresse att ändra på dessa beteenden, samt att de hittar på ursäkter för att inte följa organisationens policyer (Chen, Wen, & Ramamurthy, 2012).

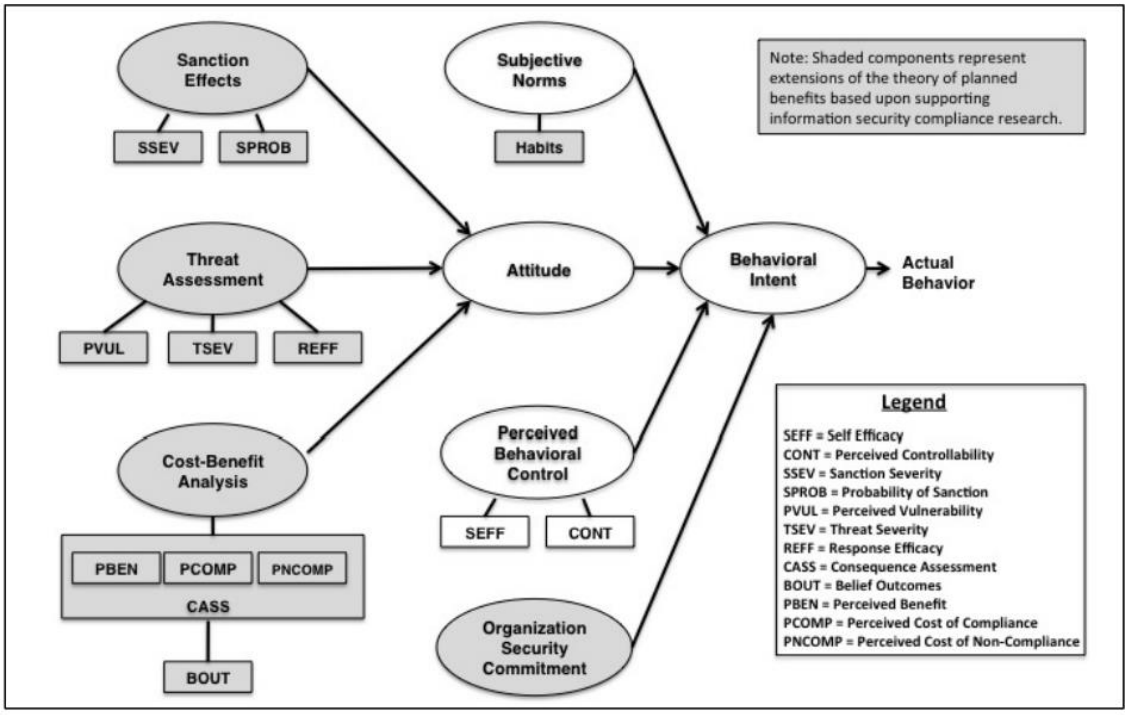
Awareness programs har därför blivit en stor del i att hantera den mänskliga faktorn i informationssäkerhet. Många gånger består dessa av olika standarder och riktlinjer som till exempel ENISA och NIST. Dessa hjälper organisationer att utveckla dokument eller andra material där anställda kan ta del av hur viktigt det är med

informationssäkerhet. Dessa standarder och riktlinjer brukar i första hand handla om processer och innehållet i programmet och vilket sorts beteende som önskas etableras i organisationen. De brukar däremot inte behandla huruvida den ökade kunskapen och medvetenheten faktiskt leder till ökad säkerhet. Det är också viktigt att försöka förmå de anställda att ändra sitt synsätt på upplevda risker och hur de fattar beslut kring dessa risker och att på så sätt ta i beaktande människors förmåga runt beslutsfattande (Tsohou, Karyda, & Kokolakis, 2015)

Det verkar dock som att det finns ganska få bevis inom litteraturen för att så kallade awareness programs faktiskt minskar säkerhetshot bland personalen (Waly, 2013; Puhakainen & Siponen, 2010; Siponen et al. 2014) och de verkar inte heller påverka till vilken grad personalen följer säkerhetspolicyer. Det räcker inte att bara utvärdera ett sådant programs effektivitet genom att låta de som deltagit i det utvärdera det, med andra ord hur deltagarna känt direkt efteråt. De borde istället baseras på hur anställda faktiskt använder de erhållna kunskaperna i det dagliga arbetet. (Waly, 2013) Som figur 4 visar räcker det inte med att bara göra anställda medvetna om policyer, utan det måste även finnas ett policyunderhåll för att programmet ska bli effektivt. Waly (2013) säger att allting ska utvärderas och inte bara själva implementeringen ske.

2.6 Beteendeteorier

Det finns flera teorier rörande beteende som passar bra när slutanvändares vilja att följa informationssäkerhetsstrategier och informationssäkerhetspolicyer undersöks. Två vanliga teorier som dyker upp i litteraturen är Theory of planned behavior (TPB) (Ifinedo, 2012; Safa et al. 2015; Siponen, 2000; Lebek et al. 2014; Bulgurcu et al. 2010) och the rational choice theory (RCT) (Bulgurcu et al. 2010; Sang Hoon, Kyung Hoon, & Sunyoung, 2014; Aurigemma & Panko, 2012), vilka även är teorier som passar bra i denna uppsats och därför kommer att användas i analys och diskussion. De har även använts tillsammans tidigare av till exempel Aruigemma & Panko (2012), Sang Hoon et al. (2014) och Bulcurcu et al. (2010). Bulgurcu et al. (2010) har även med teorier om ISA i sin studie. Figur 5 visat hur Aruigemma och Panko har sammansatt flera teorier för att skapa ett teoretiskt ramverk kring ISP-medvetenhet och efterlevnad, vars komponenter till stor del återfinns i de beteendeteorier som används för denna uppsats.



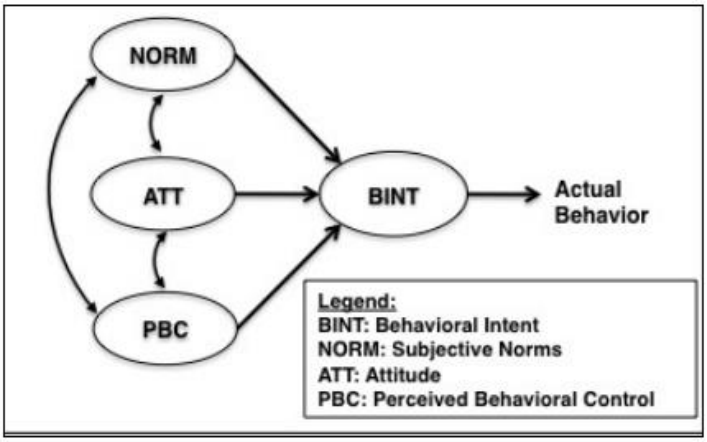
Figur 4. Sammanslagning av beteendeteorier (Aruigemma & Panko, 2012. s. 3249).

I modellen ovan kan man se hur olika beteendemetoder kan användas tillsammans för att analysera människors beteende kring risk, vilket många författare till artiklar gjort på olika sätt. Komponenterna i modellen återfinns i kommande två kapitel.

2.6.1 The theory of planned behavior (TPB)

Denna teori skapades först av en forskare vid namn Ajzen 1985 och har visat sig vara ett bra sätt att förklara hur människor beter sig kopplat till avsikt. Enligt denna teori går det att med hjälp av en persons attityd mot ett beteende eller en aktivitet, tillsammans med uppfattning om beteendet (socialt acceptabelt och subjektiva normer) och den uppfattning om den ansträngning som beteendet skulle medföra (upplevd beteendekontroll), förutsäga viljan att genomföra ett visst beteende. (Finke, Hickerson, & McLaughlin, 2015)

TPB har använts i stor utsträckning inom olika domäner och den är vanligt förekommande vid undersökningar av individers beslut om att acceptera och följa säkerhetsåtgärder, samt följa ISP (Ifinedo, 2012). Den har visat att en anställds anledning till att följa en organisations ISP starkt påverkas av attityd, subjektiva normer och upplevd beteendekontroll (Ifinedo, 2012; Safa et al. 2015). Attityd handlar om en persons negativa eller positiva inställning till ett visst beteende, subjektiva normer beskriver en persons uppfattning om vad betydande personer till dem tycker om ett visst beteende och upplevd beteendekontroll handlar om en persons enkelhet eller svårighet att bete sig på ett visst sätt (Ifinedo, 2012; Safa et al. 2015). Figur 6 visar den klassiska TPB modellen.



Figur 5. The theory of planned behavior (Aurigemma & Panko, 2012, s. 3248).

Personliga normer refererar till en anställds värderingar och syn på att efterleva en organisations ISP och tidigare litteratur har visat att detta påverkar en anställds attityd gentemot att ha ett felaktigt beteende kring informationssäkerhet (Safa, Von Solms, & Furnell, 2016). Subjektiva normer reflekterar inverkan på de anställda när det gäller närståendes åsikter angående deras beslut. Det kan till exempel, från en organisation, vara tryck på att följa ISP från ledning och arbetskollegor (Safa et al. 2015).

Med hänsyn till informationssäkerhet påverkas anställdas attityd av deras förväntningar kring konsekvenserna av att följa de satta säkerhetsriktlinjerna eller policyerna. Uppfattning om beteendet inom informationssäkerhet berörs av en organisations normer eller kultur, den anställdes roll i fråga och tillkommande ansvar, samt efterlevnad av säkerhetsriktlinjer. Den sista aspekten ser till en persons uppfattning om ansträngningen ett visst beteende skulle kräva eller innebär. Detta kan hanteras genom teknisk utbildning för att öka kunskapen hos de anställda (Siponen, 2000)

Bulgurcu et al. (2010) menar att en persons normativa tro, den upplevda egna effektiviteten och attityd mot efterlevnad spelar in på dennes vilja att följa ISP. Attityden hos en anställd påverkas av fördelen med att efterleva, kostnaden att efterleva och kostnaden av att inte efterleva, vilket kan förklaras med en anställds förväntning av de konsekvenser som följer av att göra något eller inte (Bulgurcu et al. 2010). En anställds attityd mot att följa ISP påverkas också av dennes åtaganden och normer (Safa, Von Solms, & Furnell, 2016; Lebek et al. 2014). Lebek et al. (2014) säger att en anställds avsikt att följa ISP beror på dennes synsätt och normativa tro till beteende gällande lydnad.

"Benefit of compliance is shaped by intrinsic benefit, safety of resources, and rewards, while cost of compliance is shaped by work impediment; and cost of noncompliance is shaped by intrinsic cost, vulnerability of resources, and sanctions." (Bulgurcu et al. 2010, s. 523)

Bulgurcu et al. (2010) kommer fram till att ISA har en stark inverkan på anställdas attityd mot efterlevnad av informationssäkerhetspolicy och att ISA spelar en stor roll för anställdas förväntningar på konsekvenserna av en handling.

2.6.2 The rational choice theory (RCT)

RCT handlar om att individer har preferenser som gör att de väljer den valmöjlighet som passar dem bäst. Det talas om ”rationella agenter” som när de fattar sina beslut väger in sådana aspekter som tillgänglig information, troligheten att någonting ska ske och potentiella kostnader och fördelar, vilket ISA och ISA-träning påverkar. Med andra ord är rationalitet en stor grund till människans beslutsfattande. (De Jonge, 2012) Något som påverkar detta är individens egen uppfattning (Sang Hoon, Kyung Hoon, & Sunyoung, 2014) och dennes tro på hur och till vilken grad deras efterlevande av policyer får konsekvenser (Aurigemma & Panko, 2012). Enligt denna teori överväger individer olika valmöjligheter och deras olika eventuella följder (med följd menas en konsekvens av en aktiv händelse) (Bulgurcu et al. 2010). På grund av individers olika preferenser kan de tolka eventuella följder som att deras kostnad eller fördel beror på hur tillfredsställande följden blir för individen. Detta styrker att individens egna attityder påverkar dennes riskbedömning, vilket även återfinns i TPB.

Trots att RCT har visat sig användbar för att förklara en individs beteende i ett visst sammanhang, är den inte utan brister. Viktigt att tänka på är att en persons syn på potentiella fördelar och kostnader påverkas av dennes egna perspektiv på saker. Det är inte allmängiltigt vad som uppfattas som en kostnad eller en fördel. Vissa individer lägger stor vikt vid materiella saker medan andra föredrar sociala, kulturella eller psykologiska intressen. En individs tillfälliga känslotillstånd kan också vara avgörande vid ett beslutstagande. (Bulgurcu et al. 2010)

2.7 Sammanfattning av teorin

Teorierna som tagits upp behandlar den mänskliga aspekten kring arbetet med informationssäkerhet genom att göra de anställda medvetna om säkerhet och säkerhetsrisker för att minska dessa hot.

Informationssäkerhet handlar om att genom tekniska hjälpmedel och mänskligt uppförande skydda en organisations information. Ett sätt att försöka göra så att anställda i en organisation beter sig ”rätt” ur ett säkerhetsperspektiv är att ha uttalade och dokumenterade IT-säkerhetspolicys som förankras hos de anställda. Exempel på vanliga policyer är de runt utformandet av lösenord. Med ett starkt ledarskap går det att se till så att policyerna används konsekvent genom hela organisationen.

Det är vida ansett att den största säkerhetsrisken för organisationer är den mänskliga faktorn, eller de anställda, men att organisationer trots detta traditionellt har sett och fortfarande ser informationssäkerhetsarbete som ett rent tekniskt problem. Utöver de tekniska hoten måste också de anställdas attityder och beteenden beaktas, eftersom även vänligt inställt anställda kan begå säkerhetsbrott på grund av faktorer som bristande kunskap, ignorans eller dålig attityd.

Information Security Awareness, ”ISA”, är ett utbrett begrepp som adresserar just den mänskliga faktorn inom informationssäkerhet. ISA innebär att anställda har en generell kunskap inom informationssäkerhet och en medvetenhet om rådande ISP, att dessa efterföljs och att de förstår nyttan med att de finns, eller förenklat att anställda känner till varför regler kring säkerhetsarbete finns och att de följer dem. När anställda har en hög nivå av medvetenhet förstår de risker bättre och anstränger sig mer för att se till så att organisationen är säker.

Inom ISA finns begreppet ISP awareness, som mer specifikt handlar om just medvetenheten kring policys. Det har nämligen visat sig att anställda tenderar att inte följa policys trots att de känner till dem. Därför måste de anställdas attityder och beteenden undersökas.

Genom träning går det att öka de anställdas ISA och på så sätt påverka deras attityd så att de efterlever policyer i en högre grad. Litteraturen menar att träning inom ISP riktar sig till att öka de anställdas medvetenhet kring informationssäkerhet och på så vis öka deras förståelse om varför policyer finns och nyttan med att följa dem.

Träningen kan vara en del av ett ”Awareness program”, som är en övergripande strategi för hur policys ska underhållas, uppdateras och etableras i arbetsstyrkan. Det finns standarder om ENISA och NIST som hjälper organisationer att utveckla dokument eller andra material som anställda kan ta del av för att förstå vikten av informationssäkerhetshantering. Dessa dokument är dock inte bra som underlag för uppföljning för att se om arbetet faktiskt fått effekt.

Kopplingar till anställdas beteende dyker upp på flera ställen i litteraturen inom områden kring ISP. Bland annat har det påvisats att anställda inte följer policyer trots att de finns och att ISA till viss del grundar sig i anställdas kognitiva medvetenhet kring säkerhetspolicyer, hur de tolkar och förstår dem och anställdas beteendemässiga medvetenhet, hur de utifrån sin förståelse av policyn väljer att agera. Vidare är det vanligt att litteraturen diskuterar de anställdas beteende när det kommer till att förstå varför de väljer att efterleva policyer eller inte. Två teorier som förekommer inom tidigare forskning och som är relevanta för uppsatsen är Theory of planned behavior (TPB) och Rational choice theory (RCT), vilka båda bottnar sig i att en persons attityd och uppfattning påverkar dennes beslut och att olika individer därför inte fattar samma beslut i samma situationer.

Teorierna går att kategorisera enligt tabellen nedan. Ur detta har frågor utvecklats och det går att se i tabellen var i teorin varje fråga har sin grund.

Teori	**Författare**	**Intervjufrågor**
ISA & ISP Informationssäkerhet Kunskap Medvetenhet Säkerhetstänk Policykunskap	Siponen (2000), Hellqvist et al. (2013), Ahlan et al. (2015), Bulgurcu et al. (2010), Häussinger (2015), Safa et al. (2004), Von Solms & Von Solms (2004)	1, 2, 4, 5, 6, 7, 10, 11, 15, 16, 17
Utbildning Awareness program Medvetande Träning Kommunikation och motivation	Bulgurcu et al. (2010), Tsohou et al. (2015) Waly (2014), Knapp & Ferrante (2012), Puhakainen & Siponen (2010), Safa et al. (2016)	4, 6, 7, 15, 16, 17
Beteende/(Mänsklig faktor) Subjektiva normer Attityd Beteendekontroll Subjektiv rationalitet	Sherif et al. (2015), Ashenden (2008), Safa et al. (2015), Safa et al. (2016) Kauer et al. (2013), Tariq et al. (2014), Chen et al. (2012), Sang Hoon et al. (2014), Finke et al. (2015), Ifenido (2012), Aurigemma & Panko (2012), De Jonge (2012), Siponen (2000), Bulgurcu et al. (2010), Lebek et al. (2014)	1, 2, 8, 9, 10, 11, 12, 13, 14, 17

Tabell 1: Teorisammanställning

Intervjufrågor med teorikoppling och motivering:

1. Tänker du mycket på hot när det gäller säkerhet kring tekniska hjälpmedel i ditt privatliv, och hur skyddar du dig mot dessa? (öppen fråga)
   Motivering: För att kontrollera säkerhetstänk och jämföra med detta privat och på jobbet, och se om arbetsgivaren påverkat säkerhetstänket eller om det redan fanns hos individen.

2. Tänker du mycket på hot när det gäller säkerhet kring tekniska hjälpmedel på din arbetsplats, och hur skyddar du dig mot dessa? (öppen fråga)
   Motivering: Inledande fråga för att testa nivå av ISA.

3. Borttagen på begäran av ett av företagen.

4. Känner du till begreppet IT-policy sedan tidigare? (Ja/Nej-fråga)
   Motivering: Inledande fråga för att testa nivå av ISP för att senare se om detta påverkar ISA.

5. Beskriv vad som för dig, kan tänkas vara en informationssäkerhetspolicy? (Öppen fråga)
   Motivering: Testa nivå av ISP awareness.

6. Känner du till om det finns några informationssäkerhetspolicys på din arbetsplats? (Ja/Nej-fråga)
   Motivering: För att testa nivå av ISA/ISP, och för att se om teorin om att det är vanligt att anställda inte känner till policyer stämmer på våra företag.

7. Om JA på fråga 6, nämn de informationspolicys som du känner till. Skriv max 5 stycken. (Öppen fråga)
   Motivering: För att testa nivå av ISA/ISP, och för att se om teorin om att det är vanligt att anställda inte känner till policyer stämmer på våra företag.

8. I vilken utsträckning följer du dessa policys, och varför? (Öppen fråga)
   Motivering: För att undersöka deltagarens attityd, och se om teorin om att även om anställda känner till policyer så följs de inte passar in.

9. Följer du vissa policys mer noggrant än andra? I så fall vilka? (Öppen fråga)
   Motivering: För att undersöka deltagarens attityd, och se om teorin om att även om anställda känner till policyer så följs de inte passar in.

10. Har du några egna regler som du följer när det gäller säkerhet? (Öppen fråga)
    Motivering: Testa attityder och ISA, och för att se om anställda utan kunskap om organisations policyer ändå har ett grundläggande säkerhetstänk.

11. Bland följande exempel på vanliga policys, finns det några som du följer i ditt arbete (även om det inte är på grund av din arbetsgivares uppmaningar)? (flervalsfråga)
    Motivering: Kontrollfråga för att se om även anställda som svarat att de inte känner till några policyer kanske faktiskt gör det ändå, för att det till exempel kallas något annat på just det företaget.

12. Varför följer du informationssäkerhetspolicys? (Öppen fråga)
    Motivering: Testa beteende och attityd.

13. Varför följer anställda inte informationssäkerhetspolicys? (Öppen fråga)
    Motivering: Testa beteende och attityd.

14. Vad skulle få dig att välja att inte följa en informationssäkerhetspolicy? (Öppen fråga)
    Motivering: Testa beteende och attityd.

15. Vad har din arbetsgivare gjort för att göra dig medveten om organisationens policys? (Exempel: delat ut häften, utbildningar, muntligt berättat) (Öppen fråga)
Motivering: Se om arbetsgivaren gjort något för att förankra policyerna, vilket teorin säger att de ofta inte gör. Se om de använt utbildning, awareness programs etc. Och om detta har påverkat ISA, ISP eller attityder.

16. Vad har din arbetsgivare gjort för att du ska följa organisationens policys? (Öppen fråga)
Motivering: Se om arbetsgivaren gjort något för att förankra policyerna, vilket teorin säger att de ofta inte gör. Se om de använt utbildning, awareness programs etc. Och om detta har påverkat ISA, ISP eller attityder.

17. Om du bryter mot en informationssäkerhetspolicy, vad kan det få för konsekvenser? (Öppen fråga)
Motivering: Testa beteende och attityder.

3. Metod

Detta kapitel beskriver hur man valt att utföra undersökningen, med besluten grundade i litteratur kring metoder om enkäter och intervjuer. Undersökningsformen motiveras, liksom valet av fallföretag och deltagare i underökningen. Även utformningen av själva undersökningen beskrivs och motiveras, precis som tillvägagångsättet i analysen längre fram i uppsatsen. Det finns också ett kapitel om undersökningens kvalitet för att försäkra läsaren om att undersökningen gått rätt till och att resultaten är välgrundade och trovärdiga.

3.1 Metodval

Inledningsvis gjordes en litteraturgenomgång för att identifiera artiklar inom ämnet informationssäkerhetspolicyer och anställdas medvetenhet och efterlevnad till dessa, för att skapa en bild om befintlig forskning. Detta gjordes med hjälp av artikeldatabasen Ebscohost och Google Scholar och utifrån sökningen lyftes de mest relevanta och framstående skrifterna fram.

Det finns två övergripande metodansatser att välja mellan för insamling av data vid en forskningsundersökning; kvalitativ eller kvantitativ (Jacobsen, 2002). För att på bästa sätt uppfylla uppsatsens syfte och besvara frågeställningen har en kvalitativ undersökning genomförts. Jacobsen säger att en kvalitativ metod passar bäst vid undersökningar av sociala fenomen, vilket lämpar sig för uppsatsen då den mänskliga faktorn inom arbete med informationssäkerhetspolicy är just ett socialt fenomen. Beslutet att genomföra en kvalitativ datainsamling gör det möjligt för uppsatsen att tolka och förstå empirin och på så sätt skapa större klarhet kring varför slutanvändare av informationssystem och andra tekniska hjälpmedel i organisationer, inom branscherna hospitality och detaljhandel, väljer att följa, alternativt inte följa IT-policyer för informationssäkerhet. Att beakta är att med en kvantitativ ansats hade ett större svarsunderlag förmodligen kunnat samlas in och en mer generell bild hade kunnat skapas kring ämnet. Dock hade inte en kvantitativ ansats gett samma djup i undersökningen och då uppsatsen ämnar skapa förståelse och tolka insamlade empirin valdes den kvalitativa metoden. En fallstudie har genomförts där fyra företag inom två olika branscher undersöktes. Fallstudien passar när ett visst beteende på en viss plats (Jacobsen, 2002) ska undersökas, i detta fall organisationer inom två olika branscher.

Enkät valdes som form för insamling av empirin. Enkäten utformades med öppna frågor som besvarades med deltagarens egna ord. Fördelarna med detta är att deltagaren inte styrs eller begränsas av bestämda svar och att svaret blir utförligt och nyanserat (Andersson, 1994), vilket passar den här uppsatsen bra då det är kunskap och attityder som undersöks. Liknande tar Bryman & Bell (2013) upp att öppna frågor inte leder in respondenternas tankar i någon specifik riktning, utan de får själva formulera sina svar och på så sätt visas deras kunskapsnivå vilket är väsentligt för uppsatsen.

Genom att använda enkäter eliminerades effekter som intervjuaren kan ha på den intervjuade. Då en intervjuare är närvarande kan det finnas en viss benägenhet hos den intervjuade att försöka ge en positiv bild av sig själv, framförallt när det gäller frågor som berör en social önskvärdhet, vilket i sin tur kan påverka den intervjuades

svar (Bryman & Bell, 2013). Vidare säger Bryman & Bell (2013) att det finns en tendens hos de intervjuade att inte beskriva sådant som kan verka ängslande. Då frågor kring de anställdas medvetenhet och efterlevnad gällande organisationens informations-säkerhetspolicy förekom, vilket kan vara ett känsligt ämne som berör social önskvärdhet, var enkäter ett bra val för denna uppsats. Eftersom antalet deltagare inte var jättehögt blev det ändå ett greppbart resultat som kunde användas till analys och diskussion. Genom att göra undersökningen i enkätform försvann dock möjligheten till att fördjupa sig med följdfrågor och vidareutvecklingar, men detta ansågs inte vara lika viktigt som att kunna garantera anonymitet.

Någon undantagsfråga hade alternativ för att dubbelkolla hur personens medvetande och beteende är sammankopplade (se fråga 11). Eftersom uppsatsen har för avsikt att undersöka anställdas medvetenhet om policys och hur de känner inför användandet av dessa så hade inte en kvantitativ undersökning med frågor och svar i siffror passat lika bra. Möjligheten att kunna dra paralleller och se samband mellan en specifik deltagares svar hade inte heller varit möjlig i samma utsträckning.

3.2 Val av fallföretag

Fyra företag i två branscher valdes ut. Den första branschens två företag var verksamma inom hospitality; Ett större vandrarhem med ca 45 rum och ett hotell med 221 rum. Båda företagen jobbar med informationssystem där vissa kunduppgifter behandlas och har även hantering av kreditkort. Den andra branschen är detaljhandeln, där en återförsäljare av möbler, accessoarer och annan inredning och en återförsäljare av nya och begagnade böcker valdes ut. Båda företagen behandlar personinformation. Att beakta är att ett företag i var bransch har en hög omsättning och många anställda medan ett i varje bransch är en betydligt mindre verksamhet än det större.

Företag	**Typ**	**Anställda (hela organisationen2014)**	**Ort (för undersökningen)**
Hospitality 1 (H1)	Hotell	Ca 3500	Malmö
Hospitality 2 (H2)	Vandrarhem	Ca 225	Malmö
Detaljhandel 1 (D1)	Inredning	Ca 250	Stockholm
Detaljhandel 2 (D2)	Begagnad studentlitteratur	> 10 (med timmanställda ca 60)	Lund

Tabell 2: Företag

3.3 Urval

Först valdes två företag ut eftersom författarna genom sina egna deltidsjobb hade lätt tillgång till dessa och att de hade tillräckligt många arbetare för att få ett bra svarsunderlag från enkäten. Dessa två företag råkade vara inom hospitality och detaljhandeln. Med det som första steg resonerades det att de fungerar bra därför att de är vanligt förekommande branscher och arbetssättet med kund och i informations-system återfinns på många arbetsplatser. För att få större bredd på undersökningen valdes ytterligare ett företag ut inom var bransch, även dessa genom författarnas egna deltidsjobb eller kontakter, som också mötte kriteriet att de hade tillräckligt många anställda som använde informationssystem. Då uppsatsen ämnar undersöka i vilken omfattning IT-policyer efterlevs avseende anställdas informationssäkerhetmedvetande inom en organisation är enkäterna riktade till de anställda inom företaget som använder informationssystemen, det mest lämpade för att få in relevant empiri.

3.4 Utformning av enkätfrågor

Efter att ha sammanställt teorin i en tabell mynnade vissa teorier ut i frågor. Med andra ord var frågorna förankrade i teorin. För att utforma enkätfrågorna utgick författarna främst ifrån Bengt-Erik Anderssons bok Som man frågar får man svar - en introduktion i intervju- och enkätteknik (1994). Nedan beskrivs den metodteori som använts vid utformandet av enkäten till uppsatsen.

Det är viktigt att i en enkät beskriva syftet med den och varför den vänder sig just till den deltagaren som läser det. I den inledande instruktionen är det också bra att beskriva vem som ligger bakom och vad informationen ska användas till.

Det bör också informeras om att enkäten är anonym om detta kan utlovas, men det bör inte utlovas skydd om detta inte kan hållas. Det är också viktigt att skriva tydligt hur frågorna ska besvaras.

Eftersom informationssäkerhetspolicy inte är en term som används i dagligt tal fanns det i början av enkäten en kort förklaring till vad det handlar om, för att undvika missförstånd eller bristfälliga svar på grund av att deltagarna inte känner till ämnet. Dock fick deltagarna inte veta vilket ämne det handlade om innan de tog del av undersökningen

Vidare skriver Andersson att instruktionerna inför varje fråga måste vara enkla och simpla att tyda, eftersom deltagaren annars kan tröttna eller missuppfatta på grund av ovana att läsa skriftliga instruktioner. Själva längden på enkäten styr också utrymmet för hur långa instruktionerna till varje fråga kan vara eftersom en för lång enkät kan verka avskräckande.

Genom att använda en tratt-teknik, skriver Andersson, kan man börja med generella frågor för att sedan gå närmare och närmare de frågor som egentligen är av intresse, något som även den här undersökningens frågor följer. På så sätt blir det en mjukare start och deltagaren i enkäten slängs inte in i att plötsligt besvara personliga frågor på en gång. Enligt tratt-tekniken ska inte heller ledande frågor ställas, som till exempel ”Har ditt företag varit dåliga på att förmedla policys?”. Det gäller även att inte vara ledande i instruktionerna.

En annan sak som Andersson tar upp är att inte ha frågor med negationer då dessa är svåra att svara på. I slutet av sin bok har Andersson en check-lista (Bilaga 1) som användes av författarna.

3.6 Analys av enkäter

Det finns två sätt att kategorisera på, dels att kategorisera medan materialet bearbetas och dels i förväg (Andersson, 1994). Att göra det under tiden passar bäst om det område som undersöks är nytt eller relativt outforskat, eller om det finns en risk att svaren har nyanser som inte fångas upp av förkategoriseringen. Annars passar det att i förväg göra kategorier baserade på teoretisk kunskap. Eftersom denna uppsats empiri bygger till största del på öppna svar om beteenden och attityder kan många olika svar på frågorna ges och det finns en risk att dessa är svåra att förkategorisera. Därför kategoriserades frågorna under tiden som materialet bearbetades.

Analys av kvalitativ data kan göras i tre steg, *beskrivning, systematisering och kategorisering,* samt *kombinatinon*. I det första steget ska en så detaljerad och noggrann beskrivning av det insamlade materialet göras. Under systematisering och kategorisering ska datan reduceras och förenklas, detta för att göra datan mer greppbar för andra som kommer att läsa uppsatsen. I det sista steget ska datan tolkas för att kunna generalisera eller skapa ordning kring den. (Jacobsen, 2002)

Beskrivning har skett genom transkribering av alla enkäter som samlats in, vilket har gjorts i tabeller för att underlätta att senare jämföra datan. Då de som besvarat enkäterna antingen gjort det för hand eller på en dator har svaren kunnat återges i sin exakta form.

Systematisering och kategorisering gjordes genom att skapa en struktur med olika kategorier, i vilken den insamlade datan skulle kunna placeras in. För att göra det enkelt och överskådligt valdes som huvudkategorier de framtagna teoriområdena från teorisammanställningen; ISA & ISP, Utbildning och Beteende.

Under *Kombinationssteget* sammanfattades den insamlade datan som var relevant för de olika kategorierna och specifika svar valdes ut som var representativa för mängden. Detta för att göra det möjligt att på ett tydligt sätt dra paralleller och hitta skillnader och likheter mellan datan.

3.5 Undersökningskvalitet

3.5.1 Validitet

Validitet innebär bedömning av slutsatser av en undersökning och om de hänger ihop eller inte (Bryman & Bell, 2013). Det finns bland annat intern validitet och extern validitet, där intern validitet handlar om kausalitet och om en slutsats som har ett kausalt förhållande mellan variabler är hållbar eller inte. Enligt Jacobsen (2002) handlar intern validitet om deltagarnas uppfattning om ett visst fenomen och att frågor måste utformas så att olika personer har samma bild av en viss beskrivning. Enkätfrågorna är utformade på ett sådant sätt att det tydligt framgår vad frågorna

handlar om, med beskrivningar innan varje fråga som ser till att tolkningsutrymmet för begrepp och termer är minimerat.

Extern validitet handlar om ifall undersökningsresultat kan generaliseras utöver just den undersökningens kontext (Bryman & Bell, 2013). Ur det perspektivet är själva valet av undersökningsplats och undersökningsdeltagare väldigt viktigt. Rapportens undersökningsplatser är vanliga miljöer för arbetare i Sverige, där de anställda jobbar på ”golvet” med direkt kontakt med kunder, eller i kontorsmiljö. Tre av företagens IT-miljöer är köpta färdiga lösningar vilket innebär att de återfinns på många andra arbetsplatser i Sverige. Det fjärde företaget har själva tagit fram sin backoffice-miljö. Utifrån denna undersökning kan det dock vara svårt att generalisera resultaten eftersom den omfattar ett mindre antal deltagare, men den visar intressanta paralleller och kopplingar, samt likheter som är värda att uppmärksamma.

3.5.2 Reliabilitet

Med reliabilitet menas huruvida undersökningsresultaten skulle bli desamma om undersökningen genomfördes igen. Det handlar också om ifall svar kan påverkas av slumpmässiga eller tillfälliga betingelser (Bryman & Bell, 2013). Med andra ord ska det finnas en stabilitet. Om undersökningen också görs om kort efter den första gången ska resultaten inte skilja sig nämnvärt. Det finns också en risk med enkäter med öppna svar, att när det är flera som bedömer och kategoriserar svaren (som i denna uppsats fall med två författare) kan de tolka svaren olika. För att motverka detta har författarna kategoriserat och tolkat alla svaren tillsammans. Deltagarna har typiska arbetsuppgifter för sin bransch som kan tänkas återfinnas på många arbetsplatser och problemet med att organisationer inte förankrar policyer i sin arbetskraft är utbrett, så om testet upprepades på en annan liknande plats så finns det skäl att tro att resultaten skulle kunna bli liknande.

3.5.3 Etik

Deltagarnas överordnade erbjöds möjligheten att först ta del av enkätfrågorna, vilket vissa ville och detta resulterade i att en fråga togs bort. Det var också de överordnade som godkände att enkäten ägde rum på just deras arbetsplats och de blev uppmanade att inte berätta för de anställda om ämnet i förväg. Detta för att inte de anställda skulle tänka extra mycket på det, ta reda på vad det innebär, ta del av organisationens policyer etc. vilket hade gett ett resultat som inte speglade verkligheten. Både företagen och deltagarna utlovades anonymitet och det har inte under arbetets gång gått att identifiera vem som svarat på vad.

3.6 Metodreflektion

Om undersökningen hade varit kvantitativ hade fler personer kunnat delta i den och underlaget för analys och diskussion hade blivit större. Genom att ta en kvalitativ ansats kunde dock attityder och beteende undersökas mer ingående och paralleller dras.

Att använda enkäter i en kvalitativ undersökning har fördelen att den negativa effekt en fysiskt närvarande människa kan ha på den intervjuade, speciellt eftersom vissa av deltagarna i den här undersökningen har en professionell relation till författarna, kunde undvikas. Anonymitet kunde helt enkelt i annat fall inte utlovas. Det som är

negativt med valet av en anonym enkätundersökning med öppna svar är att det inte funnits möjlighet till uppföljning eller kompletterande frågor, men eftersom ämnet är relativt känsligt så var anonymitet högre prioriterat för att kunna försäkra sig om att få så uppriktiga svar som möjligt.

4. Empiri

I denna del kommer en sammanfattning av enkätresultaten att presenteras under de tre kategorier som frågorna tillhör, ISA & ISP, Utbildning och Beteende. Resultaten kommer att presenteras med tabeller, svarsexempel, samt sammanfattningar för att återge ett jämförbart material. Typiska exempel på representativa svar från undersökningen presenteras för att läsaren ska få en bild av hur vanliga svar såg ut. Deltagarna är kodade efter hospitalityföretag 1 och 2 (H1 och H2) och detaljhandelsföretag 1 och 2 (D1 och D2). Siffran efter beskriver vilken av deltagarna det handlar om. Till exempel innebär alltså D1:1 deltagare nummer 1 på detaljhandelsföretag 1. I bilaga 3 finns lättöverskådliga sammanställningar över alla deltagare.

4.1 ISA & ISP

Deltagarna som svarat på enkäten har delats in i hög eller låg ISA (se tabell 3). Denna indelning har gjorts utifrån frågorna 2-8 och 10-11, där relevanta svar som berör ämnet gällande ISA och ISP har identifierats. Detta har gjorts för att på ett tydligare och enklare sätt kunna dra paralleller till de andra teoridelarna, dels i detta kapitel men också i förlängningen i diskussionen. För att skilja på om de anställda hade kännedom om ifall arbetsgivaren har ISP eller inte, har en egen tabell gjorts där det resultatet redovisats (se tabell 4).

ISA

	Deltagare	**Antal**	**Procent**
Hög*	D1:1, D1:3, D1:5, D2:4, H1:1, H1:3, H1:4, H1:5, H2:2, H2:3, H2:4 H2:5, H2:6	13	59 %
Låg	D1:2, D1:4, D2:1, D2:2, D2:3, D2:5, D2:6, H1:2, H2:1,	9	41 %
Total:		22	100 %

**Uträknat genom antal svar där deltagarna visat medvetenhet jämfört med där de inte visat medvetenhet. Om antalet svar där de visat medvetenhet var högre än antalet där de inte visat det blev bedömningen att ISA var hög och vise versa. På fråga 11 krävdes det 4 eller fler ikryssade alternativ för att bedömas som att medvetenhet visats.*

Tabell 3: Uppdelning av svarande mellan hög och låg ISA.

ISP (Känner du till om det finns policyer på din arbetsplats?)

	Antal	Procent
Ja	9	41 %
Nej	13	59 %
Total:	22	100 %

Tabell 4: kännedom om informationssäkerhetspolicyer existerade på arbetsplatsen.

Sett till resultaten kring hög alternativ låg ISA och om anställda visste om det fanns informationssäkerhetspolicyer på deras arbetsplats eller inte, visade det sig att nio av de med hög ISA visste om att det fanns policyer, medan ingen av dem med låg ISA visste om det fanns.

4.1.1 Hög ISA

Nedan följer en sammanfattning av den data som är representativ för mängden som har hög ISA.

Svaren från ovan nämnda frågor behandlar områden kring de anställdas inställning, kunskap och medvetenhet, både privat och på arbetsplatsen, om informationssäkerhet och IT-policyer inom det området. Av deltagarna som placerats under hög ISA har 6 av 13 påvisat att de inte lägger någon större vikt vid hot gällande tekniska hjälpmedel och hur de bör skydda sig mot dessa på sin arbetsplats. Vad som framkommit är att de förlitar sig på företaget och dess tekniska utrustning och att de därför inte behöver tänka på det i någon större utsträckning. Detta på grund av antaganden om att de tekniska lösningar och hjälpmedel som finns på arbetsplatsen, samt IT-avdelning, hanterar all säkerhet kring information.

"Nej, inte på ho(t) som intrång då jag förutsätter att vår IT-avdelning är så pass kompetent att jag i viss mån kan luta mig tillbaka." (D1:3, fråga 2)

"Inte jättemycket, här tänker jag att vår IT avdelning har bra skalskydd. Tänker dock på eventuella spam email som kan skada datorn." (H2:2, fråga 2)

"Inte lika mycket som hemma. Jag tänker att det finns mer skydd kring tekniskutrustning på min arbetsplats eftersom det är väldigt viktigt att skydda känsliga uppgifter internt och för kunders räkning." (H2:5, fråga 2)

"Nej men det beror till största del på att jag inte bryr mig om informationen på mitt jobb. Det beror nog helt på vad det är man gör! Litar helt på de brandväggar + säkerhet som jobbet satt upp." (D1:1, fråga 2)

De resterande sju anställda som visade sig tänka mer kring ämnet informationssäkerhet på sin arbetsplats lade vikt vid säkerhetsaktiviteter så som att inte öppna okända mail, att använda lösenord och att inte surfa på osäkra hemsidor.

Vidare visade resultatet av enkäterna att nio av dem som visat på hög ISA kände till begreppet IT-policy sedan tidigare. Inom gruppen med hög ISA gav alla exempel på vad som för dem kunde tänkas vara en IT-policy. Vanligt förekommande var hantering av lösenord och att inte ladda ner eller öppna okända länkar på hemsidor eller mail. Det nämndes även att inte använda okända USB på arbetsdatorn.

"Byta lösenord med jämna mellanrum och använda vissa tecken i detta, typ stora och små bokstäver." (H2:2, fråga 5)

"svåra lösenord, ej ladda ner filer från okända aktörer, Inte ge ut lösenord, Sätt ej in okända usb i datorn" (H1:1, fråga 5)

"Att inte göra privata ärenden på företagets datorer. Att inte använda USB. Att byta lösenord relativt ofta. Att inte tala om sitt lösenord för andra. Att inte öppna bifogade filer om man är osäker på avsändaren." (H1:4, fråga 5)

"Att inte öppna en specifik länk. Att inte ge ut sina inloggningsuppgifter. Att inte dela med sig av information som kan beröra eller skada företaget." (D1:3, fråga)

Alla tillfrågade som kände till att företaget hade policyer angav minst en befintlig policy under fråga 7. Av dem angav alla förutom en, som inte svarade på frågan, att de följer dessa policyer i så stor utsträckning som möjligt. Det som uppmärksammats bland svaren var hantering av lösenord och att inte utlämna skadlig information om organisationen eller kunder.

"'Du har inte rätt att offentliggöra eller delge information som på något sätt kan skada organisationen' isch…" (D1:3, fråga 7)

"Vi byter lösenord var tredje månad. Vi får inte ge ut information om en gäst." (H2:6, fråga 7)

Tolv av de tretton som visade på högt ISA hade, förutom angivna policyer som de visste fanns på deras arbetsplats, egna policyer eller allmänna normer inom informationssäkerhet som de valde att följa på sin arbetsplats.

Öppna inte konstiga mail, undvik öppna nätverk, håll efter datorn med spyware/skit (D1:1, fråga 10)

Inte ladda ner program som är osäkra (D2:4, fråga 10)

Så svåra lösenord som möjligt, byta lösenord ofta och inte klicka på några konstliga länkar som kan leda till virus (H2:4, fråga 10)

4.1.2 Låg ISA

Nedan följer en sammanfattning av den data som är representativ för mängden som har låg ISA.

Alla de som placerats under låg ISA har visat på att de inte tänker särskilt mycket på hot gällande tekniska hjälpmedel och hur de bör skydda sig mot dessa på sin arbetsplats. Vissa har angett att de inte alls tänker på det, medan andra har angett att de tänker mindre på det på arbetet än hemma och de som ändå tänker på det i viss mån anger att de inte gör något speciellt åt det och att de litar på att det finns skydd på arbetsplatsen, samt att arbetsgivaren ser över det.

"Nej aldrig." (D1:2, fråga 2)

"Inte funderat över detta." (D2:1, fråga 2)

"Till en viss del, men det är inte något jag går runt och tänker på. Jag skyddar mig inte alls mot dessa." (D2:5, fråga 2)

"Inte lika mkt som privat och jag litar på att arbetsplatsen har skyddet som krävs." (D1:4, fråga 2)

"Ja, jag tänker på det men gör inte så mycket åt det. Tänker mindre på det på jobbet än privat då jag känner att det finns någon på arbetsplatsen som ser över detta, tex IT-avdelning." (H2:1, fråga 2)

Fyra av de nio med låg ISA kände sedan tidigare till begreppet informationssäkerhets-policy och av dessa gav två deltagare exempel på vad en informationssäkerhetspolicy kunde vara, medan två valde att inte svara på den frågan. Av de fem som inte kände till begreppet sedan innan, kunde fyra ge exempel på vad en informationssäkerhetspolicy kunde vara. Av alla de som angav någon form av policy inom informationssäkerhet var det vanligast förekommande området lösenordshantering.

"Lämna aldrig ut lösenord/koder till andra" (D1:2, fråga 4)

"Man ska inte ha för allmän information, eller information som många känner till i sitt lösenord." (D2:2, fråga 4)

"Skydda informationen vi har med starka lösenord, inte ge ut dessa till någon." (D2:3, fråga 4)

Trots att ingen av de med låg ISA hade kännedom om det fanns informations-säkerhetspolicyer eller inte på deras arbetsplats, har alla kryssat i minst en policy i fråga 11 som de följer på sin arbetsplats. Även här var det vanligast förekommande med policyer som handlar om hantering av lösenord och inloggningsuppgifter. Att inte öppna länkar från okända mail och att inte ladda ner programvara till arbetsdatorn var också förekommande.

4.2 Utbildning

Fråga 15 och 16 i enkäten behandlar utbildning eller andra aktiviteter som organisationen gjort för att de anställda ska känna till och följa policyer och normer som finns.

På frågan om arbetsgivaren gjort något för att de anställda ska *vara medvetna* om policyer svarar deltagarna enligt nedanstående tabell.

	Antal	**Procent**
Gjort någonting	13	59 %
Inte gjort någonting	9	41 %
Total:	22	100 %

Tabell 5: om företaget gjort något för de anställdas medvetenhet om policyer.

Med "Gjort någonting" avses att deltagaren gett ett svar som beskriver en eller flera aktiviteter som deras arbetsgivare utfört för att informera om policyer. Vanligast var muntlig informationsdelning.

"Muntligt berättat (...)" (D1:3, fråga 15)

"Muntligt berättat det vid möten." (H1:3, fråga 15)

"Muntligt berättat om några få när situationer har inträffat då det har varit nödvändigt att den delges." (H2:3, fråga 15)

På frågan om organisationen gjort något för att de anställda ska *följa* policyer, svarar deltagarna så här:

	Antal	**Procent**
Gjort någonting	7	32 %
Inte gjort någonting	15	68 %
Total:	22	100 %

Tabell 6: Om företaget gjort något för de anställda ska följa policyer.

Bland svaren finns ingen tydlig tendens åt någon specifik aktivitet. Aktiviteter som tas upp är bland annat muntligt, att skriva kontrakt, e-mail etc. Många är lite diffusa och siffran på 68 % kan också ses som något låg jämfört med verkligheten.

En majoritet av de tillfrågade ansåg alltså att företaget gjort åtminstone någonting för att de skulle känna till policyer kring säkerhet på jobbet. Däremot svarade en ännu större majoritet att arbetsgivaren inte gjort någonting för att de anställda ska följa dessa policyer.

Fråga 13 blir också relevant i detta kapitel då en majoritet av deltagarna (12 stycken) svarar att de anser att anledningen till att anställda inte följer policyer är på grund av för dålig utbildning/information.

"Pga dålig information om vilka policys som gäller från arbetsgivare" (D1:2, fråga 13)

"För att de inte är informerade om informationssäkerhetspolicyn." (D2:5, fråga 13)

"För att de inte känner till riskerna." (H1:2, fråga 13)

I ett av företagen inom hospitality (H2) har 5 av 6 deltagare högt ISA (se tabell 3, kap 4.1) vilket också speglas i att samtliga av företagets deltagare anger någonting som organisationen har gjort för att göra dem medvetna om organisationens säkerhetspolicyer. Samtidigt är det dessa personer vars organisation har gjort aktiviteter för att göra dem medvetna som på ett eller annat sätt svarar att anledningen till att de följer policys är för att skydda organisationen (eller dess kunder) vilket utgör en parallell till kategorin beteende.

4.3 Beteende

De frågor i enkäten som rör beteende och attityd är fråga 1, 2, 9, 12 och 17. Även 13 och 14 gör det i viss mån men de är mer generella och inte lätta att kategorisera.

Tabellen nedan redovisar hur många procent av de svarande som tänker på hot när det gäller säkerhet kring tekniska hjälpmedel i deras privatliv respektive på deras arbetsplats.

	Antal procent av alla svarande*
Privatlivet	68 %
Arbetsplats	32 %

**Det är en tillfällighet summan är 100%*

Tabell 7: Svarande som tänker på hot kring tekniska hjälpmedel i privatlivet, respektive arbetsplatsen.

Det går att se att fler tänker på hot i sitt privatliv än på arbetsplatsen. Sju av deltagarna uppger att en anledningen till detta är att de litar på att arbetsplatsen tar hand om säkerhetsarbetet;

"Nej, inte på ho(t) som intrång då jag förutsätter att vår IT-avdelning är så pass kompetent att jag i viss mån kan luta mig tillbaka" (D1:3, fråga 2)

"Tänker mindre på det på jobbet än privat då jag känner att det finns någon på arbetsplatsen som ser över detta, tex IT-avdelning" (H2:1, fråga 2)

Utöver denna anledning (att lita på arbetsplatsens säkerhetsarbete) syns inga tydliga tendenser till andra anledningar, utan svaren är spridda. Endast en person uppger att denne tänker mer på det på jobbet än hemma:

"I större utsträckning än privat. Jag försöker vara observant på bluffmail men är generellt inte ute på nya hemsidor utan arbetar surfar mest inne i våra (...) program." (D1:5; fråga 2)

I frågekategorin om beteende (frågorna 9, 12, 17) som handlar om beteendet kring att följa policyer, är det väldigt jämnt mellan personliga anledningar och anledningar som innebär att skydda företaget. Båda typerna av anledning nämns drygt 20 gånger, lite beroende på hur vissa svar tolkas. Det var alltså ungefär lika vanligt att se om sig själv som att se om organisationen och svaren lät ofta så här:

"För att hjälpa företaget att inte få problem med utomstående som inte ska få ta del av vår information. Dessutom för att skydda all vår information som vi anvä(n)der i vårt dagliga arbete" (H2:5, fråga 12)

"För min och företagets trygghet." (D1:3, fråga 12)

På frågan varför deltagarna följer policyers angav 15 av dem konsekvenser för företaget som anledning. De som svarade med personliga anledningar hade också oftast med konsekvenser för organisationen som anledning.

"För att jag respekterar företagets utrustning och vill inte förstöra för mig eller mina kollegor" (D1:1, fråga 12)

"För att företaget som jag är lojal mot ska vara säkert mot intrång som även i längden kan göra det svårare för mig att sköta mitt jobb" (H2:2, fråga 12)

På frågan vad det kan få för konsekvenser att inte följa policyers var tendensen att se om sig själv högre och (12 stycken) angav personliga själ till detta medan 11 angav företaget som anledning (1 person angav båda).

"Varning/tillsägelse (antagande)" (D1:2, fråga 17)

"Jag antar att min arbetsgivare skulle bli missnöjd med mitt agerande." (D2:6, fråga 17)

"En utskällning. Datorn kan krascha" (H1:1, fråga 17)

"Antar att grova överträdelser kan leda till avsked." (H2:2, fråga 17)

Tio deltagare anser att anledningen till att anställda inte följer policyer är lågt intresse, ovilja etc. Denna fråga är ställd generellt och tar inte reda på deltagarens individuella anledning till att inte följa policyer, men talar ändå om deltagarens tankar kring ämnet och på så sätt deras attityd.

När det istället gäller varför deltagarna själva skulle välja att inte följa en policy svarade deltagarna med dessa typer av anledningar:

Anledning	**%***
Ser ingen nytta/korkad	39 %
Står i vägen för bra utfört arbete	22 %
Inget/Följer alltid	22 %
Privata anledningar**	17 %
Totalt	100 %

**Av faktiska svar på frågan. "Vet ej" etc. ej inräknade.*
*** Slarvar medvetet, kränkande etc.*

Tabell 8: Varför anställda väljer att inte följa en policy.

Det går att se att den största anledningen till att deltagarna inte skulle följa policyer är att de inte ser nyttan med dem, eller att de anser att de står i vägen för deltagarens arbete. Typexempel på svar är:

"Om policyn var i vägen (eg. ofrånkomlig, omtolkat av författarna) för att jag skulle kunna utföra mitt arbete på b(ä)sta sätt." (D1:3, fråga 14)

"Om jag inte såg syftet med att göra det och om det innebar för mycket jobb" (D2:2, fråga 14)

"Om jag inte ser anledningen bakom policyn eller förstår meningen med den" (H1:5, fråga 14)

"Om den kändes kontraproduktiv" (H2:2, fråga 14)

I företag H2 har alla deltagare angett att deras organisation gjort någon aktivitet för att de ska bli medvetna om befintliga säkerhetspolicyer och de utmärker sig i undersökningen genom att de har flest antal deltagare som känner till organisationens policyer. Samtidigt svarar samtliga ändå att de inte tänker särskilt mycket på informationssäkerhet på arbetsplatsen eftersom de förlitar sig på att arbetsgivaren tar ansvar för detta.

5. Diskussion

I denna del kommer resultatet av den empiriska data som samlats in att analyseras och diskuteras, samt knytas samman med teorierna som presenterats tidigare i uppsatsen.

5.1 ISA & ISP

Av de som deltog visade sig en majoritet ha ett relativt högt grundläggande säkerhetsmedvetande, baserat på om de kände till policyer och om de följde dessa, tillsammans med allmänt tänkande kring informationssäkerhet oberoende av arbetsgivarens insatser. Dessutom kände nästan hälften av de tillfrågade till organisationens informationssäkerhetspolicyer, vilket är mer än väntat (grundat i teorin). Enligt litteraturen är det utbrett att anställda inte känner till informationssäkerhetspolicyer alls.

Enligt teorin bör ett högt ISA leda till att anställda anstränger sig mer för att organisationen ska vara säker, men vi såg att flera med hög generell ISA inte kände till företagets informationssäkerhetspolicyer. Dock kan det påpekas att samtliga deltagare som ansågs ha låg ISA inte heller kände till organisationens säkerhetspolicy, vilket är i linje med vad som kunde förväntas eftersom ISA skapas av en anställds kunskap kring befintliga ISP och dennes generella informationssäkerhetskunskap.

Det visade sig alltså att även anställda som inte kände till organisationens policyer kunde bedömas ha hög nivå av ISA, baserat på deras generella kunskaper kring IT-säkerhet.

Det visade sig även att knappt hälften av dem som hade hög ISA-nivå och samtidigt kände till organisationens policyer inte lade särskilt stor vikt vid säkerhetstänk på arbetsplatsen eftersom de förväntade sig att företaget, inte sällan IT-avdelningen, tar ansvar för detta. Detta beskrivs i litteraturen som en känd paradox: ju mer man vet om organisationens säkerhetsarbete desto mindre lägger man ansvaret på sig själv (Tariq, Brynielsson, & Artman, 2014). Många gånger litade de på tekniska lösningar som organisationen står bakom. Även bland de med låg ISA återfanns attityden att förlita sig på organisationen, med stort fokus på tekniska lösningar, gällande IT-säkerhet. Detta pekar mot det mest grundläggande problemet i arbetet kring informationssäkerhet; nämligen att man ser problemet som rent tekniskt och inte lägger större vikt vid attityd, beteende och andra mänskliga faktorer. Därför är det bra om en organisation förankrar hos sina anställda att det tekniska i sig inte räcker, utan att det är de anställdas agerande som gör den största skillnaden.

All deltagare, oavsett nivå på ISA, angav minst en policy som de följer på arbetsplatsen när de presenterades med alternativ att välja och flera av dem med låg ISA gav konkreta, konventionella exempel på säkert beteende (fråga 5 och 10), vilket tyder på att vissa av dessa åtgärder (till exempel öppna inte länkar från okända mail) har blivit allmänt sunt förnuft och att en grundläggande kunskap kan tänkas finnas hos de flesta människor. Detta betyder att de svarande inom området ISA har visat på en högre grad av allmän kunskap kring informationssäkerhet än kunskap om befintliga policyer på arbetsplatsen.

Häussinger (2015) skriver att de flesta anställda i organisationer har låg ISA, men i denna undersökning har majoriteten bedömts ha hög ISA, (men de båda undersökningarna har förstås inte samma kriterier). Trots detta är det en minoritet som känner till sin organisations policyer, vilket tyder på att en person kan ha ett högt säkerhetstänk trots att de inte känner till organisations policyer. Organisationen verkar därför inte ta till vara på de anställdas kunskaper genom att nära dessa och ge tillräcklig input för att vidareutveckla dem till en bra säkerhetskultur. Ingenstans i svaren framgår det att företagen har någon form av awareness programs eller liknande och förekomsten av utbildning upplevs också som låg.

5.2 Utbildning

Vad som tydligt framkommit är att de anställda upplever att deras arbetsgivare antingen inte gjort någonting alls för att informera om befintliga policyer eller att det skett vid något enstaka tillfälle. För det mesta har det i de fall det skett gjorts muntligt eller genom att häften delats ut. Vidare anger majoriteten av de tillfrågade att arbetsgivarna inte gjort någonting för att de ska följa policyer. Enligt Puhakainen & Siponen (2010) ökar olika former av träning de anställdas ISA och med det deras attityd till att efterleva ISP. Det är också av vikt att inte bara förmedla policyer utan att också göra de anställda medvetna om varför de måste följas och hur. Den brist på vidare träning eller utbildning som de anställda visar i sina svar kan anses vara en orsak till att majoriteten av de tillfrågade inte har kännedom om rådande ISP och att flera av de som ändå har kännedom om ISP inte lägger någon större vikt vid säkerhetstänk på arbetsplatsen. Trots detta syns det i resultaten att de som är medvetna om befintliga policyer i stor utsträckning upplever sig följa dessa, vilket de enligt Chen et. Al. (2012) inte borde göra på grund av den bristande utbildningen. Detta skulle kunna förklaras av aspekter som inte undersökningen tar upp, till exempel företagskultur, eller en felaktig självbild där deltagarna överdriver sitt beteende och vinklar det positivt.

I företag H2 angav alla deltagare utom en att arbetsgivaren hade informerat dem om organisationens säkerhetspolicyer. En deltagare angav till och med en utbildning på intranätet. Detta är intressant då ingen annan angett detta. Alla utom en angav också att de kände till att organisationen har policyer. De svarade också att de följer policyer och att anledningen är att skydda företaget i hög utsträckning. Teorin beskriver att utbildning leder till högre medvetande kring säkerhet och ökad efterlevnad av policyer (Bulgurcu et al. 2010; Puhakainen & Siponen, 2010). I enlighet med detta har undersökningen visat att det företag vars anställda upplevde att de fått utbildning i högst grad, även var det företag där flest anställda kände till att det fanns policyer och att det fanns en tillräckligt stor nytta, sett till företaget, för att faktiskt följa dem.

I H1 däremot svarade enbart två personer att de kände till företagets policy. Båda dessa angav att skydda sig själv som anledning till att inte följa dem (för att inte chefen ska bli arg, på grund av det dagliga arbetet). Den ena nämnde att undvika virus, vilket visserligen kan tolkas som en inställning om att skydda företaget, men i liten utsträckning. Det kan lika gärna handla om att det skulle bli omständigt för personen själv. De övriga anställda svarade på (den i deras fall hypotetiska) frågan om varför de följer IT-policys på liknande sätt, med svar att antingen skydda sig från arga personer i organisationen, eller för att följa lagen, kunder etc. med undantag för en

anställd som skrev att om de följde policyer skulle göra det för att skydda företaget. Lojalitet mot organisationen syntes inte på samma sätt som i H2, vilket ytterligare belyser vikten av utbildning, eftersom de anställda i H2 på ett eller annat sätt ansåg sig informerade om företagets policyer.

Tendensen att se om sig själv märktes också tydligt i företag D2 där deltagarna inte kände till policyer i företaget, men däremot angav de flesta både privata skäl och organisationen som anledning till att följa policyer. Här fanns alltså en tendens att tänka även på företagets bästa. Dock var detta hypotetiskt eftersom de inte kände till några policyer inom organisationen och därför är det svårt att säga hur de hade resonerat om så var fallet.

I organisationer där utbildningen var mer bristfällig kunde man alltså tydligt se att deltagarna angav att de skulle följa policyer för att skydda sig själva, men i ett företag angavs även företaget som anledning. Vad som däremot syntes tydligt var att i den organisation där anställda uppfattade sig själva som informerade om säkerhetspolicyer förstod de också genomgående att företaget skyddades av att säkerhetspolicyer följdes, vilket de anställda också uppgav att de gjorde. Sett till personliga och subjektiva normer som Safa et al. (2016) menar ligger till grunden för en anställds värdering och syn på att följa en policy, går det i ovan nämnda fall att se att de personer som har fått utbildning ser värdet för organisationen med att följa policyer som finns, medan i det andra fallet där utbildning varit bristfällig sågs främst personliga skäl till grund för ifall policyer följs eller inte. Detta visar att ett företag skulle kunna tänkas påverka de anställdas personliga och subjektiva normer, vilket i sin tur påverkar attityden hos de anställda angående att efterleva ISP.

5.3 Beteende

En majoritet av deltagarna uppger att de tänker mer på säkerhet kring tekniska hjälpmedel privat än på jobbet, eftersom de räknar med att arbetsgivaren tar ansvar för detta. Enligt RCT väljer individen den valmöjlighet som passar den bäst baserat på bland annat tillgänglig information och troligheten att något ska inträffa. Med tanke på att svaren från deltagarna visade att samtliga företag inte hade någon vidare utbildning i ISA, även i de organisationer där deltagare uppgav att de blivit utbildade så var organisationernas aktiviteter i enklaste laget och informationen som ligger till grund för deltagarens beslut angående hur mycket de ska arbeta runt säkerhet var bristfälliga. Därför blir det lätt att inte inse allvaret i området och "outsourca" arbetet till arbetsgivaren och inte sällan IT-avdelningen. Med bättre utbildning hade deltagarna kanske känt till hur viktig deras roll i arbetet med säkerhet är. Det går att föreställa sig att om de haft bättre informationsunderlag hade de fattat andra beslut och tagit en mer aktiv roll i arbetet. Detta kan sättas i relation till Häussinger (2015) som menar att högre medvetenhet (vilket kan uppnås genom informationsdelning) leder till att anställda tenderar att jobba mer för att hålla informationen säker. Om man inte är särskilt informerad i risker och dessutom vet att organisationen har en IT-avdelning som man förutsätter tar hand om informationssäkerheten, så framstår det som rationellt att luta sig tillbaka och låta IT-personalen ta ansvaret och just rationalitet är enligt De Jonge (2012) en stor grund till beslutsfattande inom RCT.

Rationaliteten återfinns även i svaren på varför deltagarna skulle välja att inte följa en policy. Störst andel svar fick kategorin "Ser ingen nytta/korkad", följd av "Står i

vägen för utfört arbete". Båda är grundade i rationellt tänkande och utgör cirka två tredjedelar av svaren. Resterande svar utgjordes till stor del av "Inget, jag gör alla" och innebär alltså inget alternativ till de rationella svaren. Endast ett fåtal svarade med mer subjektivt känslosamma anledningar, som att de inte skulle följa en policy som var kränkande för deras person.

Siponen (2000) nämner att en anställds attityd mot efterlevnad av ISP påverkas av den anställdes uppfattning om ansträngningen det skulle medföra att följa den. Precis som nämnt i stycket ovan om svaren på varför de tillfrågade inte skulle välja att följa en policy, kan en koppling göras till att de anställda inte vill utföra onödigt arbete som de inte ser nyttan med och som skulle innebära mer jobb för att utföra den egentliga uppgiften. Dock visar resultaten att det handlar om policyer som de själva inte ser nyttan med och detta tyder på vikten av att skapa en medvetenhet, hög ISA, hos de anställda om varför policyerna existerar och hur de ska utföras, så att de inte ser dem som onödiga och jobbiga.

Inom TPB behandlas också personliga och subjektiva normer som en faktor till en anställds attityd mot att följa ISP. Resultaten har visat att de flesta tillfrågade tänker mer på hot inom IT-säkerhet i sitt privatliv än de gör på sin arbetsplats och alla har angivit minst en allmän ISP som de följer på sin arbetsplats, även om de inte känt till om det fanns policyer på deras arbetsplats. Detta kan tyda på att de anställda följer personliga eller subjektiva normer som de har anammat inom informationssäkerhet. Resultaten visar också att företaget som förmedlat mest information om ISP till sina anställda hade högst antal anställda som kände till att policyer fanns, angav att de efterlevde dem och hade högt ISA, samt visade på inställningen att de ville följa dem för organisationens bästa. Detta samtidigt som de angav att de inte tänker på informationssäkerhet i någon större utsträckning på arbetsplatsen. Svaren tydde på att tillförlit gavs till företagets tekniska lösningar och IT-avdelningen. Även i situationen där arbetsgivaren gjort mest för att förmedla information om ISP syns alltså en brist på engagemang kring säkerhetstänket hos de anställda på arbetsplatsen.

Människor överväger följder i sitt beslutsfattande och hur följder ses på bestäms på individnivå. Därför är det svårt att förutsätta vilken typ av beslut individer fattar. I denna undersökning framgår detta genom ett väldigt spritt resultat när det gäller varför individer följer policyer. Dels ser vi att alla som kände till att företaget hade policyer och som svarade på frågan om de följer dessa, svarade att de gör det. De angav även kända eller potentiella följder som skulle kunna uppstå om de inte skulle följa policyerna. De överväger alltså följder vilket de enligt RCT har som grund till sitt beslut att följa policyerna, men på grund av individers olika synsätt, referenser, moral etc. är följderna som ligger till grund spridda mellan personliga följder och följder för arbetsgivaren. Detta är även i enlighet med TPB som visar att anställds attityd till att efterleva policyer påverkas av förväntningar kring konsekvenserna av att följa eller inte följa policyer (Siponen, 2000; Bulgurcu, 2010).

6. Slutsats och förslag på vidare forskning

I detta kapitel sammanfattas de slutsatser som diskussionen tar upp och förslag på fortsatt forskning inom ämnet presenteras.

6.1 Slutsats

Forskningsfrågan som ställdes i inledningen av uppsatsen var:

- *I vilken omfattning efterlevs IT-policyer avseende anställdas informationssäkerhetmedvetande inom en organisation?*

Det syntes i undersökningen att människor kan ha hög grundläggande ISA personligen, även om detta inte appliceras i större grad på jobbet. Många kände till typiska policyer även om de inte kände till eller följde företagets, vilket tyder på att det finns en utbredd grundläggande kunskap i samhället kring säkerhet när det gäller tekniska hjälpmedel. Något annat som visade sig var att fler än vad man kunde ha väntat sig (nästan hälften) angav att de kände till företagets policyer. Tydligt var att de som bedömdes ha hög ISA och ansåg sig känna till organisationens säkerhetspolicyer angav att de följer dessa, vilket det enligt teorin är vanligare att anställda inte gör. Slutsatsen kan dras att i ett företag som H2 där personalen uppfattat att de fått lära sig om organisationens policyer och dessutom anser sig känna till dem, finns en större tendens att följa dem för att de förstår att detta skyddar företaget. Inom de företag där anställda ansåg att inte särskilt mycket eller inget gjorts för att informera om eller utbilda inom informationssäkerhetspolicyer var det tydligare att personliga skäl låg bakom varför de anställda valt att följa policyer.

Det var utbrett bland deltagarna att förlita sig på att arbetsgivaren genom IT-avdelningen tog hand om säkerheten, vilket också syntes i att det var vanligare att tänka på säkerhet i privatlivet än på jobbet. Detta kan tänkas motverkas med utbildning, vilket majoriteten av de anställda ansåg att företagen i undersökningen inte hade genomfört i någon större utsträckning, vare sig för att skapa kännedom eller för att få anställda att följa policyerna. Vad som kan utläsas ur uppsatsens resultat är att användning av ISP ökar de anställdas medvetenhet kring IT-säkerhet och deras vilja att följa dem, förutsatt att de känner till att policyerna finns.

Som grund för sitt beteende och sina attityder angav deltagarna rationella anledningar vilket enligt de beteendeteorier som tagits upp i teorin ligger som grund till beslutsfattande. Dock blev utfallet av det rationella tänkandet olika hos olika deltagare och som anledning till att följa policyer var det nästan lika vanligt för deltagarna att ange företagets bästa som privata anledningar. Detta beror troligen på att individers subjektiva referenser och synsätt påverkar detta tänkande och ibland ledde det till att se om sig själv och ibland till att se om organisationen i första hand. Med utbildning skulle man teoretiskt sätt kunna påverka denna subjektivitet till att rikta sig mer mot att se om organisationen än den egna personen.

De huvudsakliga slutsatserna blir följande fyra:

- Trots att ett högt säkerhetstänk existerade privat hos deltagarna så visade det sig var bristfälligt på arbetsplatsen.
- Medvetenhet om policyer främjar en attityd hos deltagarna om att följa dessa.
- Rationella anledningar låg till grund för varför deltagarna valde att följa eller inte följa policyer.
- Utbildning har visat sig bidra till högre medvetenhet hos de anställda gällande ISP och en attityd till att efterleva dem.

6.2 Förslag på vidare forskning

Mycket av existerande litteratur utgår ifrån säkerhetstänk på arbetsplatsen. I denna undersökning kunde man se att många deltagare hade ett grundläggande säkerhetstänk kring informationssäkerhet och tekniska hjälpmedel i privatlivet, men lade detta på hyllan när de kom till jobbet. Av intresse kan vara att gå djupare in på denna relation och undersöka hur en organisation kan införliva de anställdas grundläggande kunskap i organisationen.

Denna uppsats har enbart undersökt företag i Sverige, men nästan all litteratur som använts är baserad på undersökningar gjorda i andra länder. Författarna har inte kommit över någon litteratur som tar upp hur skillnader länder och kulturer emellan kan påverka säkerhetstänk och ISA. En del av undersökningens resultat stämmer inte väl överens med litteraturen, kan detta vara en av anledningarna?

Vissa av resultaten i uppsatsen skulle kunna härledas till företagskultur vilket inte tas upp i litteraturen i större utsträckning än om just specifik säkerhetskultur. Det skulle vara intressant att se om till exempel företag som lyckats skapa hög generell lojalitet bland sina anställda även har en högre grad av anställda som efterlever policyer.

Referenser

Ahlan, A., Lubis, M., & Lubis, A. (2015). Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures. *Procedia Computer Science, 72*, 361–373.

Andersson, B.-E. (1994). *SOM MAN FRÅGAR FÅR MAN SVAR.* Kristianstad: Rabén Prisma.

Ashenden, D. (2008). Information Security Management: A Human Challenge? *Information Security Technical Report*, 195–201.

Aurigemma, S., & Panko, R. (2012). A Composite Framework for Behavioral Compliance with Information Security Policies. *Hawaii International Conference on System Sciences*, (ss. 3248-3257). Hawaii.

Bryman, A., & Bell, E. (2013). *Företagsekonomiska forkningsmetoder.* Stockholm: Liber.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *Journal MIS Quarterly, 34*(3), 523-548.

Chen, Y., Wen, K.-W., & Ramamurthy, V. K. (2012). Organizations' Information Security Policy Compliance: Stick or Carrot Approach? *Journal of Management Information Systems, 29*(3), 157-188.

Choong, Y.-Y., & Theofanos, M. (2015). What 4,500+ People Can Tell You – Employees' Attitudes Toward Organizational Password Policy Do Matter. *Human Aspects of Information Security, Privacy, and Trust:* (ss. 299-310). Switzerland: Springer international publishing.

De Jonge, J. (2012). *Rethinking Rational Choice Theory A Companion on Rational and Moral Action.* Hampshire: Palgrave Macmillan.

De Leeuw, K., & Bergstra, J. (2007). *History of Information Security: A Comprehensive Handbook.* Amsterdam: Elsevier B.V.

Finke, E. H., Hickerson, B., & McLaughlin, E. (2015). Parental Intention to Support Video Game Play by Children With Autism Spectrum Disorder: An Application of the Theory of Planned Behavior. *Language, Speech & Hearing Services in Schools, 46*(2), 154-165.

Gollman, D. (2011). *Computer Security.* John Wiley.

Hellqvist, F., Ibrahim, S., Jatko, R., Andersson, A., & Hedström, K. (2013). Getting their Hands Stuck in the Cookie Jar - Students' Security Awareness in 1:1 Laptop Schools. *International Journal of Public Information Systems, 9*, 1-18.

Häussinger, F. (2015). *Studies on Employees' Information Security Awareness.* PhD, Göttingens universitet.

Höne, K., & Eloff, J. (2002). Information security policy – what do international information security standards say? *Computers & SecurityComputers & Security, 21*(5), 402-209.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*, 83-95.

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

Kauer, M., Günther, S., Storck, D., & Volkamer, M. (2013). A Comparison of American and German Folk Models of Home Computer Security. *Human Aspects of Information Security, Privacy, and Trust* (ss. 100-109). Switzerland: Springer International Publishing.

Khan, B., Alghathbar, K. S., & Khan, M. (2011). Information Security Awareness Campaign: An Alternate Approach. *Information Security and Assurance: International Conference, ISA 2011* (ss. 1-10). Brno: Springer.

Knapp, K. J., & Ferrante, C. J. (2012). Policy Awareness, Enforcement and Maintenance: Critical to Information Security Effectiveness in Organizations. *Journal of Management Policy & Practice, 13*(5), 66-80.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). Information security awareness and behavior: a theory-based literature review. *Management Research Review, 37*(12), 1049-1092.

LeVeque, V. (2006). *Information Security – A Strategic Approach.* Hoboken, N.J.: Wiley-IEEE Computer Society Press.

Mishra, D., Akman, I., & Mishra, A. (2014). Theory of Reasoned Action application for Green Information Technology acceptance. *Computers in Human Behavior, 36*, 29–40.

Nayak, U., & Rao, U. H. (2014). *The InfoSec Handbook: An Introduction to Information Security.* Apress.

Puhakainen, P., & Siponen, M. (2010). IMPROVING EMPLOYEES' COMPLIANCE THROUGH INFORMATION SYSTEMS SECURITY TRAINING: AN ACTION RESEARCH STUDY. *MIS Quarterly, 34*(4), 757-778.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security, 53*, 65-78.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56*, 70-82.

Sang Hoon, K., Kyung Hoon, Y., & Sunyoung, P. (2014). An integrative behavioral model of information security policy compliance. *The Scientific World Journal*, 12.

Sherif, E., Furnell, S., & Clarke, N. (2015). An Identification of Variables Influencing the Establishment of Information Security Culture. *Human Aspects of Information Security, Privacy, and Trust, HAS 2015* (ss. 436-448). Switzerland: Springer International Publishing.

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *T., 8*(1), 31 - 41.

Siponen, M., & Vance, A. (2010). NEUTRALIZATION: NEW INSIGHTS INTO THE PROBLEM OF EMPLOYEE INFORMATION SYSTEMS SECURITY POLICY VIOLATIONS. *MIS Quarterly, 34*(3), 487-502.

Siponen, M., Mahmood, A. M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study . *Information & Management , 51*, 217–224 .

Tariq, M., Brynielsson, J., & Artman, H. (2014). The Security Awareness Paradox: A Case Study. *Advances in Social Networks Analysis and Mining (ASONAM)* (ss. 704-711). Stockholm: IEEE conference proceedings.

Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers & Security, 52*, 128-141.

Waly, N. S. (2013). *Organisational information security management: The impact of training and awareness.* PhD, School of Computing, Informatics and Media University of Bradford, Department of Computing, Bradford.

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security, 23*(5), 371–376.

Yin, R. K. (2007). *Fallstudier : design och genomförande.* Malmö: Liber.

Bilaga 1 - Enkätformulär

Enkätformulär

Var vänlig och läs igenom instruktionerna noga!

Den här undersökningen handlar om policys inom informationssäkerhet, vilket innebär säkerheten kring ert arbete med IT-lösningar på er arbetsplats. Man kan också kalla det för säkerhetsregler kring ditt datoranvändande på arbetsplatsen. En policy är en uttalad ”regel” för hur du ska göra, som din arbetsgivare har bestämt. Dessa policys brukar finnas dokumenterade, men inte alltid. Ett exempel på en IT-säkerhetspolicy skulle kunna vara; ”Ge inte ut ditt lösenord till kunder”. Det är inte säkert att det kallas för policy på just din arbetsplats.

Dina svar kommer att användas som grund i en kandidatuppsats inom systemvetenskap på Lunds Universitet. Det vi vill undersöka är om de som jobbar i en organisation känner till organisationens IT-säkerhetspolicys. Dina svar är anonyma. Din arbetsgivare kan komma att få ta del av uppsatsen, men undersökningen sker på flera arbetsplatser och det framgår inte i uppsatsen vilka svar som kommer ifrån vilken arbetsplats.

Undersökningen är inte ett kunskapstest där du behöver prestera genom att svara så rätt eller bra som möjligt, utan svara så ärligt som du kan på frågorna. Det går självklart bra att utelämna svar på frågor om du inte kan svara på dem, men försök gärna att skriva åtminstone någonting.

Du kan skriva så mycket som du vill på varje fråga, dokumentet anpassar sig.

Det är viktigt att du svarar helt själv och inte diskuterar svaren med någon annan under tiden.

Läs frågornas instruktioner noga.

Vi skulle uppskatta om du kunde skicka in den till oss senast på måndag klockan 12:00.

Maila till (...) om ni inte fått andra instruktioner.

Tack på förhand för ditt deltagande, det betyder allt för vår uppsats!

Fråga 1 (Svara med egna ord)

Tänker du mycket på hot när det gäller säkerhet kring tekniska hjälpmedel i ditt privatliv och hur skyddar du dig mot dessa?

Svar:

Fråga 2 (Svara med egna ord)

Tänker du mycket på hot när det gäller säkerhet kring tekniska hjälpmedel på din arbetsplats, och hur skyddar du dig mot dessa?

Svar:

Fråga 3: Denna fråga är borttagen

Fråga 4 (Skriv ”Ja” eller ”Nej”)

Känner du till begreppet IT-policy sedan tidigare? Svar:

Fråga 5 (Svara med egna ord)

Beskriv, vad som för dig, kan tänkas vara en informationssäkerhetspolicy? (Exempel: Man ska inte ha sitt eget namn som lösenord)

Svar:

Fråga 6 (Skriv ”Ja” eller ”nej”)

Känner du till om det finns några informationssäkerhetspolicys på din arbetsplats? Svar:

Fråga 7 (Svara med egna ord)

Om JA på fråga 6, nämn de informationspolicys som du känner till. Skriv högst 5 stycken. (Om svaret på fråga 6 var ”Nej”, gå direkt vidare till fråga 10)

Svar:

Fråga 8 (Svara med egna ord)
I vilken utsträckning följer du dessa policys och varför?

Svar:

Fråga 9 (Svara med egna ord)

Följer du vissa policys mer noggrant än andra? I så fall vilka och varför?

Svar:

Fråga 10 (Svara med egna ord)

Har du några egna regler som du följer när det gäller säkerhet?

Svar:

Fråga 11 (Kryssa i flera alternativ med ett ”X” inom parentesen)

Bland följande exempel på vanliga policys, finns det några som du följer i ditt arbete (även om det inte är på grund av din arbetsgivares uppmaningar)?

Lösenord ska bytas med jämna mellanrum	( )
Lösenord ska innehålla bokstäver, siffror och minst en stor bokstav	( )
Man får inte koppla in egna USB i datorerna	( )
Öppna inte länkar från okända avsändare i e-mail	( )
Dela inte med dig av användarnamn och lösenord till kollegor	( )
Ladda inte ner programvara till arbetsdatorn	( )
Surfa inte privat på arbetsdatorn	( )
Skriv inte ner inloggningsuppgifter på kom ihåg-lappar	( )
Rapportera alla misstänkta virus etc. till IT-avdelningen	( )

Fråga 12 (Svara med egna ord)
Varför följer du informationssäkerhetspolicys?

Svar:

Fråga 13 (Svara med egna ord)
Varför följer anställda inte informationssäkerhetspolicys?

Svar:

Fråga 14 (Svara med egna ord)

Vad skulle få dig att välja att inte följa en informationssäkerhetspolicy?

Svar:

Fråga 15 (Svara med egna ord)

Vad har din arbetsgivare gjort för att göra dig medveten om organisationens policys? (Exempel: delat ut häften, utbildningar, muntligt berättat)

Svar:

Fråga 16 (Svara med egna ord)

Vad har din arbetsgivare gjort för att du ska följa organisationens policys?

Svar:

Fråga 17 (Svara med egna ord)

Om du bryter mot en informationssäkerhetspolicy, vad kan det få för konsekvenser?
(Om du inte vet, gör ett antagande)

Svar:

Tack för din medverkan!

Bilaga 2 – Checklista enkätfrågor

Bengt-Erik Anderssons (1994) check-lista:

1: Är orden och frågan och instruktion enkla och direkta och välkända för alla tillfrågade? Undvik teknisk terminologi – inte minst samhälls- och beteendevetenskaplig. Undvik också en jargong som kanske är välbekant för vissa men främmande för andra. Samma gäller slanguttryck eller uttryck som ger intryck av att man talar ner till den tillfrågade.

2: Är frågan så klar och specifik som möjligt? Använder man obestämda uttryck av typen ofta, många, några så får man svar där varje svarande själv definierat en egen innebörd.

3: Rymmer frågan mer än en aspekt? Man begår ofta det felet att en fråga rymmer flera aspekter, som inte behöver gå samman. Det blir då omöjligt att tolka svaret, eftersom man inte vet vilken del av frågan som besvarats. Exempel:

Föredrar du bilar som är stora och har stor motorstyrka eller som är små och ekonomiska?
Är hon lydig och tillbakadragen?

4: Är frågan ledande eller vilseledd?

5: Är frågan tillämplig på alla som får den? Kan alla besvara den?

6: Kan svaret påverkas av speciell svarsstil? Är t.ex. frågor i påståendeform som man skall instämma i eller ta avstånd ifrån formulerade så av instämmanden alltid innebär exempelvis en positiv inställning till ett visst begrepp och avståndstagande en negativ inställning. Man riskerar då att personer som har en tendens att alltid hålla med eller säga emot blir registrerade för en positiv alternativt negativ attityd utan att egentligen ha tagit ställning till innehållet. Man bör därför variera innehållet i frågorna så att man ibland instämmer i en negativ attityd och ibland i en positiv. På samma sätt bör frågor med svarsalternativen uppställda vågrätt variera i innebörden så att man undviker att positiva svar alltid ligger till höger eller vänster och vice versa.

7: Kan frågan göras kortare utan att innebörden går förlorad.

8: Ligger frågan bra i munnen? Går den lätt att läsa för intervjuaren eller för den som skall besvara enkäten.

Bilaga 3 – Transkribering av enkäter

Fråga 1 *(Svara med egna ord)*
Tänker du mycket på hot när det gäller säkerhet kring tekniska hjälpmedel i ditt privatliv, och hur skyddar du dig mot dessa?

Detaljhandel:

D1:1	D1:2	D1:3	D1:4	D1:5	D1:6
Självklart känner man en viss oro vid köp över internet och detta med bank-id i mobil känns tyvärr alldeles för bräckligt till skillnad från en dator, även om jag vet att det inte är någon skillnad. Jag har ett bra antivirusprogram och håller efter min dator, betalar oftast lite mer för saker men hos större aktörer (känns säkrare, varför vet jag inte)	Ibland. Lösenord som innehåller både siffror och bokstäver	Ja, jag försöker vara mer eftertänksam med vilka platser jag besöker.	Det händer då och då. Försöker uppdatera när det erbjuds.	Ja men skulle påstå att jag är relativt oförsiktig trots detta. Jag undersöker inte hur jag kan skydda mig mot ”hot” genom virusprogram osv utan lever i tron om att virus drabbar PC och inte Mac.	
D2:1	D2:2	D2:3	D2:4	D2:5	D2:6
Jag tänker en del på detta. Hade täppt igen kameralinsen på min dator ett tag. Skyddar mig genom att inte använda sociala medier i stor utsträckning.	Tänker på att använda säkra lösenord och lösenord som är personliga för mig	Ibland, försöker att ha olika lösenord, inte gå in eller ladda ner skumma saker på nätet. Har något virusprogram för att skydda. Annars ser jag till att inte ha allt för viktiga saker på mina tekniska enheter.	Ja, jag tänker ganska mycket på eventuella hot. jag skyddar mig genom att uppdatera alla senaste uppdateringar (har en mac och iphone) som finns tillgängliga. Detta gör jag via både dator och telefon. Jag har alltid brandväggar och övriga skydd aktiverade. + jag trycker aldrig på länkar, pop-up fönster och håller mig ifrån konstiga tävlingar/sidor på facebook.	Tänker inte så mycker kring det, har något säkerhetsskydd (dock något jag inte har en aning om vad det). Det är tack vare mina vänner samt föräldrar som hjälpt mig med detta.	Nej det gör jag inte. Dock är jag alltid noggrann med vilka personliga uppgifter jag lämnar ut och framförallt till vem jag lämna ut dem.

Hospitality:

H1:1	H1:2	H1:3	H1:4	H1:5	H1:6
Man är alltid rädd att någon ska hacka in i ens telefon eller dator. Särskilt rädd är jag att de ska Ta sig in i min internet bank. Skyddar mig själv genom att använda svårare lösenord, antivirus program.	Nej, bara kollar att brandväggen är på. Om det är någon som verkligen vill ta sig in i ens dator och är duktig på det, så är det inte mycket man kan göra.	Jag har lösenord på både dator och telefon. Har även virusprogram på min laptop.	Jag är noga med att inte öppna bifogade filer som jag inte vet vem som skickat. Vid ändring av lösenord, t. ex. från bank, ringer jag och kollar att det stämmer att de skickat ut. T. ex mobilt bankid. Jag gör inga bankärenden via WIFI eller via min telefon.	Eftersom jag spelar mycket datorspel och laddar ner mycket film och program osv så tänker jag mycket på att ha virusskydd och sökskydd i min webbläsare. Försöker också att inte ladda ner saker från sidor som verkar osäkra. Att söka igenom och rensa datorn manuellt med jämna mellanrum är också något jag försöker tänka på. Och att inte öppna skumma mail!	
H2:1	H2:2	H2:3	H2:4	H2:5	H2:6
ja, jag tänker på det men gör inte så mycket åt det.	Ja, jag försöker endast att använda mig utav säkra nätverk och är vaksam mot eventuella misstänksamheter på websidor som jag besöker.	Med hot i detta fall, tolkar jag det som intrång i mina tekniska hjälpmedel. I det fallet är det något jag är medveten om i min vardag. Jag är noga med att skydda dator och mobiltelefon med hjälp av antivirusskydd och antimalwareprogram och genomför regelbundna genomsökningar. Jag tycker även om att använda sunt förnuft för att skydda mig från "dumma" mail.	Nej, faktiskt inte.	Ja, framförallt när det kommer till virus på min dator. Jag anser att det är viktigt med bra virusskydd på datorn. Därför väljer jag att köpa virusskydd och inte ha någon gratis variant	Jag tänker en del på det. Jag stänger ofta av platstjänster i mobilen om jag inte måste använda det och är rätt restriktiv med vad jag lägger upp på internet.

Fråga 2 *(Svara med egna ord)*

Tänker du mycket på hot när det gäller säkerhet kring tekniska hjälpmedel på din arbetsplats, och hur skyddar du dig mot dessa?

Detaljhandel:

D1:1	D1:2	D1:3	D1:4	D1:5	D1:6
Nej men det beror till största del på att jag inte bryr mig om informationen på mitt jobb. Det beror nog helt på vad det är man gör! Litar helt på de brandväggar + säkerhet som jobbet satt upp.	Nej aldrig.	Nej, inte på hos som intrång då jag förutsätter att vår IT-avdelning är så pass kompetent att jag i viss mån kan luta mig tillbaka.	Inte lika mkt som privat och jag litar på att arbetsplatsen har skyddet som krävs.	I större utsträckning än privat. Jag försöker vara observant på bluffmail men är generellt inte ute på nya hemsidor utan arbetar surfar mest inne i våra Saas-program.	
D2:1	D2:2	D2:3	D2:4	D2:5	D2:6
Inte funderat över detta.	Nej	På jobbet tänker jag faktiskt inte på det i lika stor utsträckning. Så länge vi håller oss till det system eller de program som vi blivit informerade om att använda känns det tryggt.	Ja, men säkerheten är väldigt bristfällig på vår arbetsplats. Datorerna är daterade och gamla, ALLA borde uppdateras och bytas ut.	Till en viss del, men det är inte något jag går runt och tänker på. Jag skyddar mig inte alls mot dessa.	Samma svar som ovan. När det kommer till att lämna ut uppgifter i någon annans namn, t.ex. min arbetsgivare är jag kanske extra försiktig.

Hospitality:

H1:1	H1:2	H1:3	H1:4	H1:5	H1:6
Ibland om är t.ex när man är inne på en streaming sida på jobb är man rädd ibland att det kan komma någon pop up som kan vara skadlig. Vi använder anti virus skydd. Lösenord till olika sidor.	Nej, men öppnar inga konstiga mail elelr liknande.	Nej.	Jag använder inte USB i företagets datorer. Jag öppnar inte bifogade filer som inte har ett sammanhang med en bokning eller ett utskick från (arbetsgivare).	Tänker mindre på det på min arbetsplats då vi inte laddar ner saker eller besöker mer ”osäkra” webbplatser. Men vårt e-mailkonto är nog det som gör oss mest utsatta mot hot och bedrägerier som kommer från folk som vill lura oss att ge ut inloggningsuppgifter till bokningskanaler och liknande. Där tänker jag nog till lite extra innan jag klickar in på vissa mail som ser ut som spam eller verkar osäkra.	
H2:1	H2:2	H2:3	H2:4	H2:5	H2:6
Ja, jag tänker på det men gör inte så mycket åt det. Tänker mindre på det på jobbet än privat då jag känner att det finns någon på arbetsplatsen som ser över detta, tex IT-avdelning.	Inte jättemycket, här tänker jag att vår IT avdelning har bra skalskydd. Tänker dock på eventuella spam email som kan skada datorn.	Nej. Återigen använder jag mig av mitt sund förnuft vid mailhantering. Jag skulle vilja säga att mailen annars är det största hotet på min arbetsplats.	Lite mer då det är mycket kontaktuppgifter till gäster osv.	Inte lika mycket som hemma. Jag tänker att det finns mer skydd kring tekniskutrustning på min arbetsplats eftersom det är väldigt viktigt att skydda känsliga uppgifter internt och för kunders räkning.	Jag är noggrann med att hålla mina lösenord hemliga och tänker på att skydda gästernas information men jag känner inte samma hot som när det gäller mig som privatperson.

Fråga 4 *(Skriv ”Ja” eller ”Nej”)*

Känner du till begreppet IT-policy sedan tidigare?

Detaljhandel:

D1:1	D1:2	D1:3	D1:4	D1:5	D1:6
Ja	Ja	Ja!	Ja	Ja, från skolgången	
D2:1	D2:2	D2:3	D2:4	D2:5	D2:6
Nej	Nej	Nej	Nej	Nej	JA

Hospitality:

H1:1	H1:2	H1:3	H1:4	H1:5	H1:6
nej	Nej	Ja	Ja	Ja	
H2:1	H2:2	H2:3	H2:4	H2:5	H2:6
ja	ja	ja	nej	ja	ja

Fråga 5 *(Svara med egna ord)*

Beskriv, vad som för dig, kan tänkas vara en informationssäkerhetspolicy?
(Exempel: Man ska inte ha sitt eget namn som lösenord)

Detaljhandel:

D1:1	D1:2	D1:3	D1:4	D1:5	D1:6
Öppna inga mail du inte känner igen, kryptera viktig info via mail, jobba inte med känsliga saker på öppna nätverk. Ha inte lösenord som lösenord.	Lämna aldrig ut lösenord/koder till andra	Att inte öppna en specifik länk. Att inte ge ut sina inloggningsuppgifter. Att inte dela med sig av information som kan beröra eller skada företaget.	Inget svar	Att inte ha samma lösenord till olika tjänster. Om man använder samma till allt så finns det säkerligen lätta sidor att hacka för att få åtkomst till mitt lösenord och då har de alla mina lösenord.	
D2:1	D2:2	D2:3	D2:4	D2:5	D2:6
Inte ha sitt personnummer som lösenord eller sina namn.	Man ska inte ha för allmän inforamtion, eller information som många känner till i sitt lösenord.	Skydda informationen vi har med starka lösenord, inte ge ut dessa till någon. Även att vi ser till att skydda informationen vi har om våra kunder, så att infon inte ligger synlig för vem som helst att se.	Ehhhm, svårt att säga tyvärr. Att man inte ska ladda ner program utan vetskap eller klarhet kring vad det är och vem/vilka utgivarna är? Att man har klara riktlinjer kring it-säkerhet och hur man ska bete sig på internet.	Inget svar	Att någon annan inte skall kunna förändra information eller fakta. T.ex. mina egna uppgifter.

Hospitality:

H1:1	H1:2	H1:3	H1:4	H1:5	H1:6
svåra lösenord, ej ladda ner filer från okända aktörer, Inte ge ut lösenord, Sätt ej in okända usb i datorn	Att inte ladda ner filer från nätet. Att inte koppla in privata usb-stickor.	Inte använda en okänd USB i, inte surfa privat på arbetsdatorn, inte spara okända program/filer	Att inte göra privata ärenden på företagets datorer. Att inte använda USB. Att byta lösenord relativt ofta. Att inte tala om sitt lösenord för andra. Att inte öppna bifogade filer om man är osäker på avsändaren.	Att lösenord tex ska innehålla en kombination av gemener, versaler och siffror. Att ha bestämda tider för virusgenomsökning via virusprogrammet.	
H2:1	H2:2	H2:3	H2:4	H2:5	H2:6
Inget svar	Byta lösenord med jämna mellanrum och använda vissa tecken i detta, typ stora och små bokstäver.	Man ska inte ha samma lösenord till flera konton och helst blanda versaler, gemener, siffror och specialtecken för att få ett starkt lösenord.	Man ska inte klicka på konstiga länkar som skickats via mail.	Att man är försiktig med kunders kortuppgifter, man har egen inloggning till datorer. Att alltid låsa dator för att skydda känsliga uppgifter.	Hur man ska hantera de olika parternas information och tillgången till denna informationen så att den inte kan missbrukas eller användas till något som parten inte har godkänt.

Fråga 6 *(Skriv ”Ja” eller ”nej”)*

Känner du till om det finns några informationssäkerhetspolicys på din arbetsplats?

Detaljhandel:

D1:1	D1:2	D1:3	D1:4	D1:5	D1:6
Nej	Nej	Ja	Nej	Ja	
D2:1	D2:2	D2:3	D2:4	D2:5	D2:6
Nej	Nej	Nej inte på rak arm direkt, det skulle i så fall gälla. Våra egna lösenord att de är personliga samt att informationen om kunderna förblir skyddad. Då vi har hand om personnummer och sådan info.	JA, Det finns det INTE.	Nej	Nej

Hospitality:

H1:1	H1:2	H1:3	H1:4	H1:5	H1:6
nej	nej	ja	Ja	nej	
H2:1	H2:2	H2:3	H2:4	H2:5	H2:6
nej	ja	ja	nej	ja	ja

Fråga 7 *(Svara med egna ord)*

Om JA på fråga 6, nämn de informationspolicys som du känner till. Skriv högst 5 stycken.
(Om svaret på fråga 6 var ”Nej”, gå direkt vidare till fråga 10)

Detaljhandeln:

D1:1	D1:2	D1:3	D1:4	D1:5	D1:6
Inget svar	Inget svar	”Du har inte rätt att offentliggöra eller delge information som på något sätt kan skada organisationen” isch…	Inget svar	Att gäster inte tillåts vara inne på arbetsplatsens närverk utan att vi har byggt ett eget för gäster.	
D2:1	D2:2	D2:3	D2:4	D2:5	D2:6
Inget svar	Inget svar	Inget svar	Jag känner till att vi inte har några/någon policy.	Inget svar	Inget svar

Hospitality:

H1:1	H1:2	H1:3	H1:4	H1:5	H1:6
Inget svar	Inget svar	Inte använda en okänd USB i, inte surfa privat på arbetsdatorn, inte spara okända program/filer	Se svaret på fråga 5		
H2:1	H2:2	H2:3	H2:4	H2:5	H2:6
Inget svar	Lösenord byts 1 gång per ett visst antal dagar. Lösenord måste innehålla stora och små bokstäver samt siffror. Ingen får lov att arbeta på någon annan persons inlogg	Byt lösenord varje kvartal. Detta lösenord ska blanda versaler, gemener och siffor. Anslut inte usb-enheter i våra datorer - dessa får endast ansutas i specifika gästdatorer.	Inget svar	inte mer än att man får berätta för vem som helst vem som ska ha möte/bo hos oss. Samt att vi har egna inloggningar	Vi byter lösenord var tredje månad. Vi får inte ge ut information om en gäst.

Fråga 8 *(Svara med egna ord)*

I vilken utsträckning följer du dessa policys och varför?

Detaljhandel:

D1:1	D1:2	D1:3	D1:4	D1:5	D1:6
Inget svar	Inget svar	Till 100% för att visa företaget respekt och mitt fulla förtroende.	Inget svar	Inget svar	
D2:1	D2:2	D2:3	D2:4	D2:5	D2:6
Inget svar	Inget svar	Inget svar	Skulle följa dem om de fanns	Inget svar	Inget svar

Hospitality:

H1:1	H1:2	H1:3	H1:4	H1:5	H1:6
Inget svar	Inget svar	Jag följer de flesta men surfar privat.	Jag kopplar aldrig in ett USB. Jag talar inte om mina lösenord för utomstående. Jag öppnar inte bifogade filer som jag inte vet vem de kommer ifrån	Inget svar	
H2:1	H2:2	H2:3	H2:4	H2:5	H2:6
Inget svar	Helt, går inte riktigt att undvika då systemen låser sig om man inte följer det.	Helt. Det finns ingen anledning att inte följa dessa. De är logiska och det går inte att gå runt dem.	Inget svar	Jag följer alltid de regler som gäller. Dels för kunders skull men också för att inte vi ska få problem för vi varit oförsiktiga	Jag tycker att det är i allas intresse och att det är viktigt för allas säkerhet att man behandlar människors och företagets information förtroligt.

Fråga 9 *(Svara med egna ord)*

Följer du vissa policys mer noggrant än andra? I så fall vilka och varför?

Detaljhandel:

D1:1	D1:2	D1:3	D1:4	D1:5	D1:6
Inget svar	Inget svar	Jag försöker följa de policys jag vet om till punkt och pricka.	Inget svar	Inget svar	
D2:1	D2:2	D2:3	D2:4	D2:5	D2:6
Inget svar	Nej	Inget svar	Inget svar	Inget svar	Inget svar

Hospitality:

H1:1	H1:2	H1:3	H1:4	H1:5	H1:6
Inget svar	Inget svar	Ja, surfar privat. Brist på fritid.	Nej, jag är försiktig i största allmänhet.	Inget svar	
H2:1	H2:2	H2:3	H2:4	H2:5	H2:6
Inget svar	Nej, inte direkt.	Nej, jag följer alla till samma grad.	Inget svar	Hur man har hand om kortuppgifter samt låsa dator. På min tidigare arbetsplats var man tvungen att följa alla policys de hade som att inte ha mobil vid arbetsplatsen m.m. annars kunde man bli avskedad	De som handlar om personers integritet.

Fråga 10 *(Svara med egna ord)*

Har du några egna regler som du följer när det gäller säkerhet?

Detaljhandel:

D1:1	D1:2	D1:3	D1:4	D1:5	D1:6
Öppna inte konstiga mail, undvik öppna nätverk, håll efter datorn med spyware/skit	Lämna inte ut lösenord till kunder	Jag försöker logga ut mig från de webplatser jag besökt. Stänga av min dator när den inte används frekvent byta mina lösenord.	Nej inga direkta.	-Att inte öppna mail från okända avsändare -Att inte klicka på oseriösa reklambanners, popup fönster och liknandne	
D2:1	D2:2	D2:3	D2:4	D2:5	D2:6
Nej.	Nej	Nej	se fråga 1. - ladda ner nya uppdateringar , både via dator och mobil - inte ladda ner program som är osäkra - att ha brandvägg + virusskydd - inte trycka på pop-up, länkar mm (typ på Facebook)	- Att inte ha ett lösenord som är lättillgängligt (ex. ens namn, födelsedag, adress). En dålig vana är att man har samma lösenord till olika saker på internet.	Nej, förutom att jag noggrann med vem som min information blir tillgänglig för.

Hospitality:

H1:1	H1:2	H1:3	H1:4	H1:5	H1:6
Ger inte ut lösenord, försöker inte att surfa på farliga sidor, Laddar ej ner tillägg på jobb dator.	Jag laddar inte ner något som jag inte litar på. Har olika lösenord på olika platser.	Nej	Se svaret på fråga 5.	Inte klicka på ads Inte ladda ner från ”suspekta” hemsidor Virusskanna Rensa datorn med jämna mellanrum Inte ha samma lösenord till alla konton Försöker komma på lösenord som inte är enkla att gissa såsom namn och födelsedatum osv. Är de jag kan komma på.	
H2:1	H2:2	H2:3	H2:4	H2:5	H2:6
Nej, använder nästan alltid samma lösenordskombinationer på allt jag har inlogg till. Rädd jag ska glömma lösenorden annars då jag har så många olika inlogg.	Ingenting som jag kan komma på	Jag tycker om att använda sunt förnuft och lita på min magkänsla.	Så svåra lösenord som möjligt, byta lösenord ofta och inte klicka på några konstliga länkar som kan leda till virus.	Försöker alltid skydda våra kunder, dels för att företaget inte ska få problem om att vi hanterat saker fel. Berättar heller inte om våra interna lösenord och liknande för utomstående	Inget svar

Fråga 11 *(Kryssa i flera alternativ med ett ”X” inom parentesen)*

Bland följande exempel på vanliga policys, finns det några som du följer i ditt arbete (även om det inte är på grund av din arbetsgivares uppmaningar)?

Detaljhandel:

D1:1	D1:2	D1:3	D1:4	D1:5	D1:6
Lösenord ska bytas med jämna mellanrum; Lösenord ska innehålla bokstäver, siffror och minst en stor bokstav; Öppna inte länkar från okända avsändare i e-mail; Dela inte med dig av användarnamn och lösenord till kollegor; Ladda inte ner programvara till arbetsdatorn; Rapportera alla misstänkta virus etc. till IT-avdelningen.	Öppna inte länkar från okända avsändare i e-mail; Ladda inte ner programvara till arbetsdatorn; Surfa inte privat på arbetsdatorn	Lösenord ska bytas med jämna mellanrum; Lösenord ska innehålla bokstäver, siffror och minst en stor bokstav; Öppna inte länkar från okända avsändare i e-mail; Skriv inte ner inloggningsuppgifter på kom ihåg-lappar; Rapportera alla misstänkta virus etc. till IT-avdelningen	Öppna inte länkar från okända avsändare i e-mail; Dela inte med dig av användarnamn och lösenord till kollegor; Ladda inte ner programvara till arbetsdatorn; Surfa inte privat på arbetsdatorn.	Lösenord ska innehålla bokstäver, siffror och minst en stor bokstav; Öppna inte länkar från okända avsändare i e-mail; Dela inte med dig av användarnamn och lösenord till kollegor; Skriv inte ner inloggningsuppgifter på kom ihåg-lappar; Rapportera alla misstänkta virus etc. till IT-avdelningen	
D2:1	D2:2	D2:3	D2:4	D2:5	D2:6
Skriv inte ner inloggningsuppgifter på kom ihåg-lappar.	Lösenord ska innehålla bokstäver, siffror och minst en stor bokstav.	Lösenord ska innehålla bokstäver, siffror och minst en stor bokstav; Lösenord ska innehålla bokstäver, siffror och minst en stor bokstav; Man får inte koppla in egna USB i datorerna; Öppna inte länkar från okända avsändare i e-mail; Dela inte med dig av användarnamn och lösenord till kollegor; Ladda inte ner programvara till arbetsdatorn; Surfa inte privat på arbetsdatorn; Skriv inte ner inloggningsuppgifter på kom ihåg-lappar; Rapportera alla misstänkta virus etc. till IT-avdelningen.	Ladda inte ner programvara till arbetsdatorn.	Rapportera alla misstänkta virus etc. till IT-avdelningen.	Öppna inte länkar från okända avsändare i e-mail; Dela inte med dig av användarnamn och lösenord till kollegor; Ladda inte ner programvara till arbetsdatorn; Skriv inte ner inloggningsuppgifter på kom ihåg-lappar.

Hospitality:

H1:1	H1:2	H1:3	H1:4	H1:5	H1:6
Lösenord ska bytas med jämna mellanrum; Lösenord ska innehålla bokstäver, siffror och minst en stor bokstav;Man får inte koppla in egna USB i datorerna;Ladda inte ner programvara till arbetsdatorn	Man får inte koppla in egna USB i datorerna; Öppna inte länkar från okända avsändare i e-mail; Ladda inte ner programvara till arbetsdatorn	Lösenord ska bytas med jämna mellanrum; Lösenord ska innehålla bokstäver, siffror och minst en stor bokstav; Man får inte koppla in egna USB i datorerna; Öppna inte länkar från okända avsändare i e-mail	Lösenord ska bytas med jämna mellanrum; Lösenord ska innehålla bokstäver, siffror och minst en stor bokstav; Man får inte koppla in egna USB i datorerna; Öppna inte länkar från okända avsändare i e-mail; Skriv inte ner inloggningsuppgifter på kom ihåg-lappar; Rapportera alla misstänkta virus etc. till IT-avdelningen	Lösenord ska bytas med jämna mellanrum; Lösenord ska innehålla bokstäver, siffror och minst en stor bokstav; Öppna inte länkar från okända avsändare i e-mail; Ladda inte ner programvara till arbetsdatorn	
H2:1	H2:2	H2:3	H2:4	H2:5	H2:6
Lösenord ska bytas med jämna mellanrum; Lösenord ska innehålla bokstäver, siffror och minst en stor bokstav; Öppna inte länkar från okända avsändare i e-mail; Dela inte med dig av användarnamn och lösenord till kollegor; Ladda inte ner programvara till arbetsdatorn; Skriv inte ner inloggningsuppgifter på kom ihåg-lappar; Rapportera alla misstänkta virus etc. till IT-avdelningen	Lösenord ska bytas med jämna mellanrum; Lösenord ska innehålla bokstäver, siffror och minst en stor bokstav; Man får inte koppla in egna USB i datorerna; Öppna inte länkar från okända avsändare i e-mail; Dela inte med dig av användarnamn och lösenord till kollegor, Ladda inte ner programvara till arbetsdatorn; Skriv inte ner inloggningsuppgifter på kom ihåg-lappar; Rapportera alla misstänkta virus etc. till IT-avdelningen.	Ladda inte ner programvara till arbetsdatorn; Surfa inte privat på arbetsdatorn; Skriv inte ner inloggningsuppgifter på kom ihåg-lappar; Rapportera alla misstänkta virus etc. till IT-avdelningen	Lösenord ska bytas med jämna mellanrum; Lösenord ska innehålla bokstäver, siffror och minst en stor bokstav; Man får inte koppla in egna USB i datorerna; Öppna inte länkar från okända avsändare i e-mail; Ladda inte ner programvara till arbetsdatorn; Surfa inte privat på arbetsdatorn; Skriv inte ner inloggningsuppgifter på kom ihåg-lappar; Rapportera alla misstänkta virus etc. till IT-avdelningen	Lösenord ska bytas med jämna mellanrum; Lösenord ska innehålla bokstäver, siffror och minst en stor bokstav; Öppna inte länkar från okända avsändare i e-mail; Dela inte med dig av användarnamn och lösenord till kollegor; Ladda inte ner programvara till arbetsdatorn; Surfa inte privat på arbetsdatorn; Skriv inte ner inloggningsuppgifter på kom ihåg-lappar; Rapportera alla misstänkta virus etc. till IT-avdelningen	Lösenord ska bytas med jämna mellanrum; Öppna inte länkar från okända avsändare i e-mail; Dela inte med dig av användarnamn och lösenord till kollegor; Ladda inte ner programvara till arbetsdatorn; Surfa inte privat på arbetsdatorn

Fråga 12 *(Svara med egna ord)*

Varför följer du informationssäkerhetspolicys?

Detaljhandel:

D1:1	D1:2	D1:3	D1:4	D1:5	D1:6
För att jag respekterar företagets utrustning och vill inte förstöra för mig eller mina kollegor	sunt förnuft	För min och företagets trygghet.	Respektera arbetsgivaren regler.	- För att vara en god medarbetare - För att inte lämna ut information till okända	
D2:1	D2:2	D2:3	D2:4	D2:5	D2:6
Inget svar	För att skydda privat och företagets inforamtion	För att man vill se till så att informationen vi har bevaras tryggt och säkert. Börjar vi slarva med sådant, kan det eventuellt även drabba våra kunder och därefter vårt rykte och vår image.	Man ska ju följa den för företagets och kundernas säkerhet (vi skriver ju upp personnummer osv) men tyvärr finns det inga sådana policys i företaget i dagsläget.	Eftersom det ger mig trygghet att mitt privata hålls privat och att ingen annan har tillgång till min privata information.	För att jag inte har den kunskap som krävs för att stoppa eventuell informationsspridning som skulle kunna skada mig eller min arbetsgivare. Varken tekniskt eller juridiskt.

Hospitality:

H1:1	H1:2	H1:3	H1:4	H1:5	H1:6
Pga it säger det	Vi har ingen väldefinierad sådan vad jag vet, men om det fanns så skulle jag följa den för att undvika problem för företaget.	Annars har vi en uppretad IT tekniker + chef.	Det underlättar det dagliga arbetet att inte få virus mm.	Vi har ingen informationssäkerhetspolicy som jag vet om. Ingen som är nerskriven någonstans. Att lösenord ska bytas med jämna mellanrum blir vi informerade om via de olika bokningskanalerna och hemsidorna som vi har konto hos. Att vi inte får spara gästers kreditkortnummer någonstans är kanske lite av en policy och att vi såklart inte får ge ut någon information om våra gäster till andra människor. De två ”reglerna” följer jag av respekt till våra gäster och lagen.	
H2:1	H2:2	H2:3	H2:4	H2:5	H2:6
För att jag blir tillsagd att göra det och att jag inte vill att obehöriga ska ta sig in och granska information som de inte har att göra med.	För att företaget som jag är lojal mot ska vara säkert mot intrång som även i längden kan göra det svårare för mig att sköta mitt jobb	Oftast är de logiska och det finns en logisk bakgrund till varför de finns. Om du kopplar in en okänd usb-enhet och hela systemet kraschar, har du orsakat så mycket onödigt merarbete, som exempel.	För att inte riskera att gästers kontaktuppgifter läcker ut och för att jobbdatorn inte skall få virus.	För att hjälpa företaget att inte få problem med utomstående som inte ska få ta del av vår information. Dessutom för att skydda all vår information som vi använder i vårt dagliga arbete	För jag skulle inte själv vilja att information om mig skulle hamna i fel händer och för företagets säkerhet. Jag skulle inte vilja riskera ett dataintrång i vårt system .

Fråga 13 *(Svara med egna ord)*

Varför följer anställda inte informationssäkerhetspolicys?

Detaljhandel:

D1:1	D1:2	D1:3	D1:4	D1:5	D1:6
Naiva, tekniskt ointresserade (”vad kan hända?”)	Pga dålig information om vilka policys som gäller från arbetsgivare	För att företaget, arbetsgivare, eller den ansvarige inte delger informationen till de anställda i de flesta fall.	Inget svar	- Okunskap	
D2:1	D2:2	D2:3	D2:4	D2:5	D2:6
För att det kanske inte känner till att det existerar policys?	För att de inte har tillräckligt med information om den	Antagligen är de inte medvetna om att policys existerar, eller så reflekterar de inte över konsekvenserna utav att inte följa dessa. Man har en slapp attityd till det hela. Eller så har man inte informerat om vikten av att följa dessa policys.	För att den inte finns,men annars; pga ovetskap kring konsekvenserna som kan uppstå.	För att de inte är informerade om informationssäkerhetspolicyn. Om man även inte är insatt eller intresserad av det i sitt vardagliga liv så är det någonting man följer eller tänker på om man inte blir informerad och undervisad i det.	Brist på uppmaningar från arbetsgivare

Hospitality:

H1:1	H1:2	H1:3	H1:4	H1:5	H1:6
Man vill inte. Vill gärna även kolla privata saker.	För att de inte känner till riskerna.	Vi är rebeller.	Kan hända att man måste göra ett ärende på arbetstid och bara har arbetets datorer.	Kanske om de inte anser de vara nödvändiga av någon anledning. Eller om de har behov av att använda arbetsdatorn till privata ändamål eller inte tar seriöst på informationssäkerhet. Kan också vara att de inte tar det seriöst för att de inte blivit informerade av sin arbetsgivare.	
H2:1	H2:2	H2:3	H2:4	H2:5	H2:6
Tror inte folk alltid tar det på så stort allvar, tror inte att det drabbar dem och att det alltid finns någon på arbetsplatsen som har koll till en.	För att det lätt kan bli omständigt att till exempel hela tiden byta lösenord.	Jag skulle vilja säga av ouppmärksamhet och okunskap om policys samt i vissa fall nonchalans om dess existens. Med detta menar jag framför allt när arbetsgivaren inte har spärrat vissa sidor och en anställd surfar privat.	Jag tror faktiskt många följer dom. Kan vara isåfall att man surfar privat på arbetsdatorn eller lämnar ut sitt användarnamn/lösenord	Osäker, kan vara att de inte ser det som något att oroa sig över.	För att de kan vara omständigt.

Fråga 14 *(Svara med egna ord)*

Vad skulle få dig att välja att inte följa en informationssäkerhetspolicy?

Detaljhandel:

D1:1	D1:2	D1:3	D1:4	D1:5	D1:6
Inget	Hade följt den om jag hade information om den.	Om policyn var ofrånkomplig för att jag skulle kunna utföra mitt arbete på bösta sätt.	Inget svar	Inget svar	
D2:1	D2:2	D2:3	D2:4	D2:5	D2:6
Om policyn var korkad. Kan inte komma på ett bra exempel tyvärr.	Om jag inte såg syftet med att göra det och om det innebar för mycket jobb	Vet inte, om det skulle vara en policy som jag ansåg kränkande. Men annars skulle jag nog följa dem.	Vet ej.. Möjlgtvis om den som gjorde/bestämmde policyn inte vet vad de gör?	Om den är alldelles för komplicerad. Lättast skulle vara om det finns en enkel och pedagogisk manual samt även påminna de anställda att följa informationssäkerhetspolicyn.	Kan inte komma på något.

Hospitality:

H1:1	H1:2	H1:3	H1:4	H1:5	H1:6
Privata önskemål.	Om den verkade orelevant och jag visste säkert att ingen skada sker.	Inget svar	Se svaret fråga 13.	Om jag inte ser anledningen bakom policyn eller förstår meningen med den.	
H2:1	H2:2	H2:3	H2:4	H2:5	H2:6
Vet ej	Om den kändes kontraproduktiv.	Om den är idiotisk och inte har någon egentlig mening. Alla policys som är angivna i fråga 11 har exempelvis en förklaring till sig, därför blir det så självklart att dessa ska följas.	På våran avdelning är det absolut att man i stundens hetta behöver låna varandras användarnamn och lösen.	Om jag tycker att den inte skyddar företaget. Annars följer jag allt mer eller mindre	Om jag inte kunde förstå logiken bakom den eller om den försvårade mitt arbete nämnvärt.

Fråga 15 *(Svara med egna ord)*

Vad har din arbetsgivare gjort för att göra dig medveten om organisationens policys?
(Exempel: delat ut häften, utbildningar, muntligt berättat)

Detaljhandel:

D1:1	D1:2	D1:3	D1:4	D1:5	D1:6
Inget att nämna, det mesta är blockerat, jobbar i fasta system	Ingen info alls	Muntligt berättat samt skickar IT-avdelningen en del mail med varningar om bluffmail, buggar eller liknande.	Muntligt, blockerat olämpliga web platser.	Delar ut ett häfte som jag fått kvitera	
D2:1	D2:2	D2:3	D2:4	D2:5	D2:6
Inget.	Inget	Inget speciellt, kanske nämnt något muntligt vid upplärning.	Inget	Fått tilldelat en handbok via inloggningskontot. Inga utbildningar har getts eller genomgångar.	Inget

Hospitality:

H1:1	H1:2	H1:3	H1:4	H1:5	H1:6
mailat	det fanns nån gång en lapp vid datorn om att inte koppla in privata usb-stickor.	Muntligt berättat det vid möten.	Mejl från IT avdelningen att inte öppna bifogade filer som vi inte vet vem de kommer ifrån.	Hen har inte informerat mig om några policys.	
H2:1	H2:2	H2:3	H2:4	H2:5	H2:6
Muntligt berättat.	Utbildning på intranät om it säkerhet och kreditkortsäkerhet.	Muntligt berättat om några få när situationer har inträffat då det har varit nödvändigt att den delges.	Berättat muntligt.	gjort elektronisk lärande om policys som handlar om kunder.	Berättat och gett ut ett häfte.

Fråga 16 *(Svara med egna ord)*

Vad har din arbetsgivare gjort för att du ska följa organisationens policys?

Detaljhandel:

D1:1	D1:2	D1:3	D1:4	D1:5	D1:6
Kontrakt	ingenting	Ingenting	Varnat för olämpliga sidor, virus risker, information generellt.	Inga andra aktiviteter	
D2:1	D2:2	D2:3	D2:4	D2:5	D2:6
Inget	Inget, möjligtvis uppmanat om information på hemsidan	Inget speciellt.	Inget	Han har bett mig läsa och förstå handboken, sedan även ha öppen kommunikation med honom om det finns oklarheter.	Inget

Hospitality:

H1:1	H1:2	H1:3	H1:4	H1:5	H1:6
inget, kan skälla om de kommer på en men händer väldigt sällan.	se förra	Muntligt berättat vid möten och face to face	Information via email från IT avdelningen. Förbjudit oss att använda egna USB minnen samt att koppla något externt in i våra hårddiskar.	Samma som ovan.	
H2:1	H2:2	H2:3	H2:4	H2:5	H2:6
Vet ej.	Påminner på mail med jämna mellanrum	Spärrat många hemsidor som kan användas för privat surfande - exempelvis olika sociala medier. Gjort så att datorn inte detekterar usb-enheter. Ett nytt lösenord kan inte skapas utan rätt kriterier. IT-avdelningen skickar ut mail när många spam-mail cirkulerar.	Inte så mycket mer än trott att vi gör det självmant.	Utbildat mig i det de anser vara viktigast som gäller för hela koncernen	Gett ut information och påmint oss om rutiner.

Fråga 17 *(Svara med egna ord)*

Om du bryter mot en informationssäkerhetspolicy, vad kan det få för konsekvenser?
(Om du inte vet, gör ett antagande)

Detaljahandel:

D1:1	D1:2	D1:3	D1:4	D1:5	D1:6
Arkebusering	Varning/tillsägelse (antagande)	Jag vet inte men jag förutsätter att konsekvensen skulle leda till att inte skulle ha tillgång till den informaitonen jag har inte min inloggning idag.	Kan väl gå så långt som uppsägning.	Att bryta mot IT-policyn skulle resultera i olika konsekventeser beroende på av vilken grad förtelsen är av. Om scenariot är av ringa karaktär kan det säkerligen resultera i en varning men i allvarligare i avsked och polisanmälan.	
D2:1	D2:2	D2:3	D2:4	D2:5	D2:6
Att personnummer sprids och kommer i obehörigas händer.	Att lösenord kommer i orätta händer	Riskerar att göra det möjligt för någon att ta del av känslig information eller tillgång till annat som endast är till för oss i personalen.	- Medarbetarsamtal där man berättar om riskerna och varför man införskaffat den. Konsekvenser kan såklart bli intrång, virus , läckt information och förstörda dokument i datorn.	Att obehöriga får tillgång till information som inte är ämnade för dem, vilket kan påverka företaget negativt.	Jag antar att min arbetsgivare skulle bli missnöjd med mitt agerande.

Hospitality:

H1:1	H1:2	H1:3	H1:4	H1:5	H1:6
En utskällning. Datorn kan krascha .	Det kan göra företaget utsatt för intrång.	i kan få virus på datorn, någon kan få tillgång till våra uppgifter osv.	Virus, trojaner och andra fulingar som man inte vill ska störa det dagliga arbetet. Det kan bli en dyr affär för (arbetsgivaren) att rensa. Under en period var vi svartlistade hos vissa företag då vi hade spridit virus.	Att okända människor utifrån kan ta sig in i datorn. Att de får tillgång till lösenord och kan ta sig in på våra bokningskanaler och hämta kreditkortsnummer och information om våra gäster och om företaget.	
H2:1	H2:2	H2:3	H2:4	H2:5	H2:6
Vet ej, bli avstängd, få en reprimand, få mindre tillgång till saker och ting.	Antar att grova överträdelser kan leda till avsked.	Som jag svarade tidigare kan det leda till så mycket onödigt extraarbete och merkostnader när något går fel och kraschar.	Virus på datorn, läckt kontaktinformation till gäster.	på nuvarande är jag osäker men min tidigare arbetsplats kunde man få varningar och slutligen bli avskedad om man fortsatte att missköta sig.	Man kan hållas ansvarig