LUNDS UNIVERSITET
Ekonomihögskolan
Institutionen för informatik

Vägen till säkerhet

En studie kring balansen mellan restriktioner och motivation i arbetet med informationssäkerhet

Kandidatuppsats 15 hp, kurs SYSK16 i Informatik

Författare: Augusta Manninger
Johanna Wickberg

Handledare: Markus Lahtinen

Rättande lärare: Björn Johansson
Björn Svensson

Vägen till säkerhet: En studie kring balansen mellan restriktioner och motivation i arbetet med informationssäkerhet

ENGELSK TITEL: The road to security: A study regarding the balance between restrictions and motivation in the work with information security

FÖRFATTARE: Augusta Manninger och Johanna Wickberg

UTGIVARE: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

EXAMINATOR: Odd Steen, Docent, Fil Dr

FRAMLAGD: juni, 2019

DOKUMENTTYP: Kandidatuppsats

ANTAL SIDOR: 79

NYCKELORD: Informationssäkerhet, compliance, motivation, medvetenhet, mänskliga faktorn

SAMMANFATTNING (MAX. 200 ORD):
I takt med digitaliseringen blir informationssäkerhet ett växande hot. De flesta organisationer arbetar fram säkerhetspolicys för att reglera arbetet. Ett av problemen som organisationer ofta stöter på är att de anställda inte följer de uppsatta riktlinjerna. Vi har genom att utföra en intervjustudie svarat på huruvida företag bör se över hur de arbetar med säkerhet. Vi har även undersökt hur balansen mellan restriktioner och tillit ser ut och hur det påverkar compliance. Vi har kommit fram till att företag generellt bör se över hur de arbetar med informationssäkerhet. Vår studie visade även att man bör arbeta med motivation för att få de anställda att till högre grad följa policys. Motiverade anställda kan tillochmed vara en tillgång till organisationen istället för en instans av den mänskliga faktorn.

Innehåll

Figurer

Tabeller

1 Introduktion

I följande kapitel kommer grunden för rapporten att presenteras samt val av forskningsfråga. Slutligen kommer syftet till undersökningen samt arbetets avgränsningar att presenteras.

1.1 Bakgrund

Informationssäkerhet handlar om att hindra information från att läcka, förvanskas eller förstöras (Dataskyddsinspektionen, 2019). Informationssäkerhet kretsar kring de tre principerna konfidentialitet, riktighet och tillgänglighet, dessa innebär att information endast är tillgänglig för rätt personer, är korrekt och tillgänglig för behöriga (Gollmann, 2011).

I takt med att mer information lagras digitalt har informationssäkerhet blivit ett omfattande problem för organisationer runt om i världen (Whitman & Mattord 2008). Ett flertal stora företag såsom Trafikverket, Equifax och Yahoo har senaste tiden råkat ut för informationsläckage med förödande konsekvenser (Bergel, 2017; Stempel, 2018). Trafikverkets information läckte på grund av en IT-upphandling som outsourcade känslig information vilket gick emot de lagar som gäller i Sverige (Riksdagen, 2018). Equifax data läckte på grund av dåliga rutiner vilket resulterade att ett certifikat var ogiltigt och icke fungerande (Bergel, 2017). När Yahoo blev utsatta för intrång fick miljontals användare fick sina konton hackade (Trautman & Ormerod 2016). Företag behöver därför investera i goda säkerhetsåtgärder och rutiner för att inte riskera att förlora både kunder och kapital (Stempel, 2018).

Det finns olika hot mot en organisations interna informationssäkerhet, dessa inkluderar bristfälliga brandväggar, ineffektiva virusskydd, utgångna certifieringar samt den mänskliga faktorn (Bowen, Devarajan & Stolfo, 2011).

1.2 Problemformulering

Idag benämns ofta den mänskliga faktorn som det största hotet mot en organisations informationssäkerhet (Aldawood & Skinner, 2018). Att utnyttja denna är ett av de vanligaste sätten att få tillgång till hemlig information inom organisationer (Ghafir et al 2016). De risker som de anställda utgör är inte alltid självklara eller lätta att kontrollera, det kan vara allt från att svara på mejl, till att klicka på länkar eller koppla in USB-minnen som inte kommer från organisationen (Hadnagy, 2011; Madnick & Nourian, 2018). Mänskliga faktorers påverkan på tekniska lösningar eller problem är ett ständigt återkommande ämne (Bowen, Devarajan & Stolfo, 2011). Att respektera dess inverkan på hur väl IT-lösningar fungerar kan vara avgörande för att det ska lyckas (Bowen, Devarajan & Stolfo, 2011).

För att minska risken som den mänskliga faktorn utgör har många organisationer skapat säkerhetsprogram (Whitman & Mattord, 2008). Dessa inkluderar oftast policys som de anställda ska förhålla sig till men ibland även olika utbildningar för att de anställda ska känna igen hot och inte råka dela med sig av information (Whitman & Mattord, 2008).

De senaste 20 åren har många av säkerhetslösningarna fokuserat på att kontrollera de anställda och ge dessa riktlinjer att följa, detta inkluderar ISO certifieringar, strukturella riktlinjer och policys (Puhakainen & Siponen, 2010). Att det finns policys för de anställda att följa betyder däremot inte alltid att de efterföljs, att få anställda att följa riktlinjer är ofta ett stort problem för organisationer (Whitman & Mattord, 2008). Undersökningar visar att den information de anställda får angående rutiner, policys och risker kombinerat med den motivation de har för att göra ett bra jobb är vad som bestämmer hur väl fungerande deras arbetet med informationssäkerhet är (Herath & Rao, 2009). Det är därför viktigt att arbeta med att motivera sina anställda på olika sätt för att nå bra säkerhetsbeteenden (Herath & Rao, 2009).

Det finns flera olika sätt att motivera anställda till att arbeta säkert, utbildning, tillit och ansvarskänsla är alla olika sätt att hålla anställda motiverade (Chen, Chen & Wu, 2018). Arbetsplatser kan även arbeta med olika former av belöningar och positiv betingning för att de anställda ska följa riktlinjerna och därmed nå en hög nivå av compliance (Herath & Rao, 2009). Det finns dock även sätt att få de anställda mindre motiverade till att följa riktlinjer och policies (Adams & Sasse, 1999). För mycket restriktioner i form av policys kan ha en negativ effekt på motivationen och få de anställda att inte vilja följa dessa (Adams & Sasse, 1999). Det är därför en svår balansgång mellan policies, utbildning och tillit till de anställda för att motivera och främja ett bra arbete med informationssäkerhet.

1.3 Forskningsfråga

Vår forskningsfråga kommer belysa hur organisationer upplever att anställda förhåller sig till informationssäkerhet samt vilket stöd de anställda får av organisationen för att kunna arbeta optimalt med säkerhet. Vi studerar hur motivation och eget ansvar påverkar hur väl de anställda följer riktlinjer avsedda för att främja säkerheten. Vi har därför valt följande forskningsfrågor:

-Bör organisationer se över vilket typ av stöd som erbjuds för att anställda ska kunna arbeta säkert?
-Hur ser avvägningen mellan restriktioner och tillit ut i arbetet med informationssäkerhet och hur påverkar det compliance till organisationens policys?

1.4 Syfte

Vi avser belysa hur företag kan ge stöd åt anställda för att tackla problem gällande informationssäkerhet. Studien kommer analysera huruvida compliance till organisationers policys går att uppnås med hjälp av restriktioner eller om tilliten till individens förmåga är en bättre väg. Vi har utgått från teorier inom ämnet och tidigare forskning samt resultatet av vår studie och därefter har vi utfört en analys rörande beteende och rutiner inom informationssäkerhet. Rapporten avser utreda vilka rutiner organisationer har gällande

informationssäkerhet samt om dessa är bristfälliga baserat på den litteratur och det resultat vi erhållit.

1.5 Avgränsningar

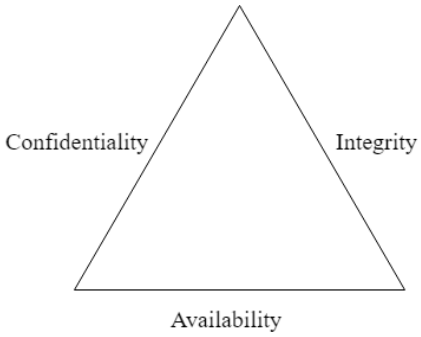
Informationssäkerhet är ett omfattande område vilket är anledningen till att vi har valt att avgränsa oss. Vi har granskat till vilket stöd som finns i form av tekniska lösningar, utbildningar och motivationsarbete samt vad som behövs för att skapa en bra kultur av säkerhetsarbete. Vi har valt att inte behandla hur privatpersoner hanterar sin privata internetsäkerhet utan vi har avgränsat oss till att arbeta med hur internetsäkerhet fungerar i ett professionellt forum. Rapporten diskuterar till vilken utsträckning restriktioner och eget ansvar värdesätts av organisationer vilket innebär att frågor gällande detta är vad intervjuerna har behandlat.

2 Teori

Nedan presenteras litteratur kopplat till ämnet vi valt att undersöka. Den kommer att fungera som grund till vår diskussion samt ge perspektiv till vår empiri för läsaren.

2.1 Informationssäkerhet

Målet med informationssäkerhet kan återfinnas i CIA-triaden som innehåller faktorerna konfidentialitet, integritet och tillgänglighet (Whitman & Mattord, 2008). Förutom att agera som målbild kan CIA-triaden även användas för att undersöka hur informationssäkerhet kan äventyras och på så sätt riskera att tillgångar blir utsatta (Gollmann, 2011). Konfidentialitet innebär att information ska enbart finnas tillgänglig för de som har behörighet att komma åt den (Karolinska institutet, 2019). Integritet inom säkerhet syftar till att information är korrekt och att all data är presenterad som den ska (Gollman, 2011). Den tredje och sista aspekten i CIA triaden fokuserar till skillnad från de föregående inte på att förhindra otillåtna händelser (Gollman, 2011). Availability syftar till att främja att de användare som ska ha tillgång till information faktiskt har det (Karolinska institutet, 2019)



Figur 2.1: CIA triad (Rousse, 2014**)**

2.1.1 Den mänskliga faktorn

En av de stora riskerna inom informationssäkerhet är den mänskliga faktor, en av de vanligaste metoderna för att komma åt information är att utnyttja mänskliga svagheter och på så sätt få tillgång till information (Aldawood & Skinner, 2018). Social Engineering är en teknik för att genom människans naivitet komma åt information (Ghafir et al, 2016). Detta kan ske via manipulation, influens eller övertalningsförmåga (Ghafir et al, 2016). Ett vanligt sätt att attackera med hjälp av social engineering är så kallad “phishing” (Hadnagy, 2011, s. 50). Det innebär att man försöker få personer att öppna elakartade filer, gå till elakartade sidor eller dela med sig av information med hjälp av väl valda email (Hadnagy, 2011).

Den mänskliga faktorn i säkerhetsåtgärder och rutiner är svår att automatisera vilket resulterar i dess avgörande roll i hur effektiv en organisations säkerhet fungerar (Aldawood & Skinner, 2018). Även information som kan verka betydelselös kan ha stor betydelse för någon som utövar social engineering och små misstag från personalen kan leda till oönskade

konsekvenser (Hadnagy, 2011). Utnyttjande av den mänskliga faktorn är en av de vanligaste metoderna för att komma åt information och en av anledningarna till att människor anses vara den svagaste länken gällande informationssäkerhet (Ghafir et al, 2016).

2.1.2 Policys och riktlinjer

Policys är grundprinciper kring hur en organisation ska agera som har accepterats av en grupp individer (NE, 2019; Cambridge Dictionary, 2019). För informationssäkerhet är en bra policy grundläggande och styr hur hela organisationen arbetar (Whitman & Mattord, 2008). En lyckad informationssäkerhetspolicy fungerar integrerat i organisationen och är en naturlig del i de anställdas vardag (Whitman & Mattord, 2008). En informationssäkerhetspolicy är inte bara ett dokument utan styr hur hela säkerhetsprogrammet ska fungera (LeVeque, 2006). Det är viktigt att policys utformas efter gällande lagar och att dessa inkluderar konsekvenser för felaktiga handlingar då policyn annars blir menlös (Whitman & Mattord, 2008). En välgjord policy hjälper organisationen att till högre grad kunna kräva compliance av sina anställda, samt hålla de anställda ansvariga i en eventuell laglig tvist (Whitman & Mattord, 2008).

2.1.3 Compliance

Compliance är akten att följa en order, regel eller önskan (Cambridge Dictionary, 2019). Inom informationssäkerhet är det viktigt att de anställda följer policys för att företaget ska kunna arbeta med information på ett säkert sätt (Whitman & Mattord, 2008). Pahnila, Siponen & Mahmood (2010) beskriver socialt tryck som en av huvudprinciperna för att nå compliance. Det är viktigt att både kollegor och överordnade lägger tryck på vikten av att följa policys för att anställda ska följa dessa (Pahnila, Siponen & Mahmood, 2010). Förutom socialt tryck nämns utbildning och olika awareness-program som ett sätt att få anställda att följa regler och policys (Whitman & Mattord, 2008).

2.2 Utbildning

För att säkerställa att anställda följer policys är utbildning en avgörande faktor (Bulgurcu, Cavusoglu & Benbasat, 2010). Utbildning av anställda spelar en direkt roll för om anställda följer policys eller inte (Kajtazi & Bulgurcu, 2013). Utbildning av de anställda är en faktor för att öka medvetande om hotbilden kring informationssäkerhet (Chen, Chen & Wu, 2018). Det är också viktigt att utbilda de anställda för att de ska förstå vad som förväntas av dem i förhållande till policys (Bulgurcu, Cavusoglu & Benbasat, 2010). Detta kan exempelvis handla om att en anställd är medveten om att det finns krav på lösenord men inte är medveten om att dessa ska ändras emellanåt (Bulgurcu, Cavusoglu & Benbasat, 2010). Whitman & Mattord (2008) menar på att utbildning av anställda bör ske direkt vid anställning för att de inte ska kunna fatta sig en egen uppfattning av regelverk innan de har blivit introducerade till den officiella policyn. I vissa fall kan utbildning även visa sig vara mer effektivt än policys för att styra säkerhetsbeteenden, exempel på detta är felaktig datoranvändning (Lee, Lee & Yoo, 2004).

Stewart & Lacey (2012) menar att utbildning inte alltid är nyckeln, redan etablerade mentala modeller och uppfattningar om säkerhet gör att traditionell informationssäkerhetsutbildning

inte alltid når ut till de anställda. Däremot skriver Whitman & Mattord (2008) att ett effektivt utbildningsprogram gör att organisationen kan förvänta sig mer av de anställda och hålla dessa ansvariga ifall de inte följer policys.

Information security awareness, härefter kallat ISA, är ett sätt att utbilda anställda inom informationssäkerhet (LeVeque, 2006). ISA-program fungerar på liknande sätt som marknadsföringskampanjer och bygger på att med väl valda budskap öka vetskapen om utvalda problem och försöka inkorporera detta i olika normer hos de anställda (LeVeque, 2006). Det är viktigt att viktigt att man i ett ISA-program, förutom information om informationssäkerhet, lär ut beteenden och rutiner för att säkerställa att de anställda har goda säkerhetsbeteenden både medvetet och undermedvetet (Thomson & von Solms, 1998). ISA kampanjer mäter även positiva förändringar hos de som man hade som målgrupp i kampanjen (LeVeque, 2006).

2.2.1 Medvetenhet

Medvetenhet i relation till informationssäkerhet refererar till ett tillstånd där användare eller anställda inom en organisation är medvetna om vad deras säkerhetsuppdrag innebär (Siponen 2000). De definierade uppdragen är ofta uttryckt i säkerhetsriktlinjer eller policys (Siponen, 2000). Medvetenhet inom informationssäkerhet är essentiellt för att motverka att säkerhetsprocedurer inte riskeras bli missbrukade, missförstådda eller oanvända av dem som de riktar sig till (Siponen, 2000). Om dessa procedurer inte följs, förloras syftet för dess existens (Siponen, 2000).

I samband med utformning av utbildningar för IS compliance, med syfte att förbättra både medvetenhet och motivation till att följa säkerhetspolicies, argumentar Puhakainen & Siponen (2010) för att metoder för systematisk behandling av information främjas. För att förbättra anställdas medvetenhet och motivation gällande informationssäkerhet bör ***Elaboration likelihood model*** (ELM) kopplas in för att bistå med konkret vägledning gällande val av utbildningsmetoder (Puhakainen & Siponen, 2010). ELM beskriver hur människan anstränger sig mer eller mindre inför beslut och vilka villkoren är för detta (Petty & Cacioppo, 1981). Den ena valmöjligheten är den *perifera vägen,* vilket innebär när personer ytligt iakttagit budskapet och sedan kommit fram till beslut baserat på saker som budbärarens klädstil eller andra irrelevanta aspekter som inte påverkar argumentet som förts fram (Petty & Cacioppo, 1981). Den *centrala vägen* å andra sidan är när människor systematisk kommer fram till beslut med stöd i ens erfarenheter, kunskaper och värderingar (Petty & Cacioppo, 1981). En individ som har känner hög grad av motivation är mer sannolik att välja den centrala vägen och alltså använda kognitivt tänkande för beslut, en person som inte är motiverad kommer ta den perifera vägen (Puhakainen & Siponen, 2010). Därför är det viktigt att användare inser varför det är viktigt och värdefullt att arbeta säkert (Jenkins, Durcikova & Burns, 2011). Väljer anställda den *perifera vägen* blir deras beteenden gällande säkerhet svåra att förutse och bedöma (Jenkins, Durcikova & Burns, 2011).

2.2.2 Kontinuitet

För att de anställda i högre grad ska ha förståelse för policys och följa dessa krävs det att man kontinuerligt följer upp med utbildning (Eminağaoğlu, Uçar & Eren 2009). Att kontinuerligt påminna de anställda om säkerhet med olika typer av kampanjer stimulerar de anställda att

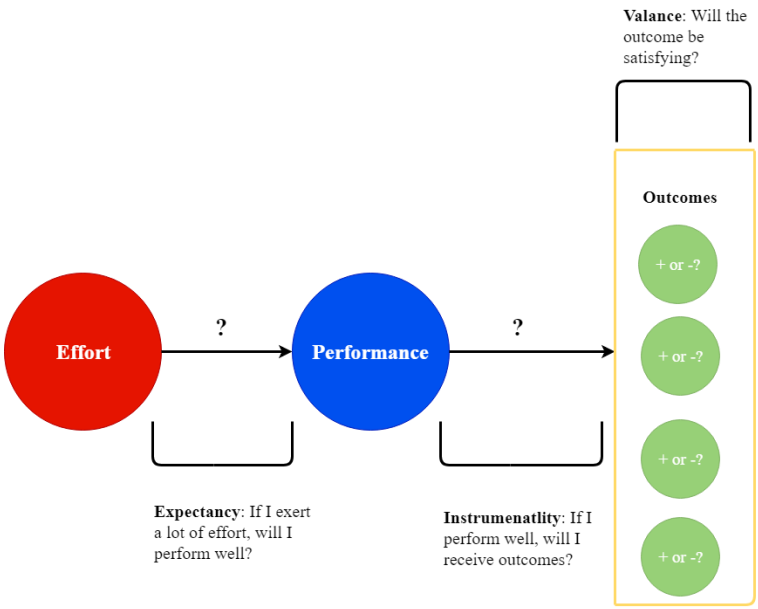
bry sig om det samt håller det aktivt i sinnet (Whitman & Mattord, 2008). Det är viktigt att organisationer håller arbetet med informationssäkerhet synligt för de anställda (Pahnila, Siponen & Mahmood, 2010). Detta håller de anställda medvetna om den hotbilden som finns samt bibehåller medvetenhet om konsekvenser vid avvikelser från policyn för att de anställda ska följa rådande policys (Pahnila, Siponen & Mahmood, 2010).

2.3 Motivation

De anställdas motivation att göra ett bra jobb på arbetsplatsen påverkar hur väl de anställda följer policys (Chen, Chen & Wu, 2018). Både positiv och negativ betingning påverkar hur motiverade de anställda känner sig och därmed hur bra arbete de gör (Herath & Rao, 2009). Negativ betingning har inverkan på huruvida den anställde känner sig motiverad på arbetsplatsen, dock kopplas ofta negativ betingning till negativa effekter på hur väl anställda följer policys (Herath & Rao, 2009). Positiv betingning är till större del kopplat till positiva resultat (Herath & Rao, 2009). Anställda som upplever medvetenhet angående arbetet med informationssäkerhet har även en tendens att känna sig mer motiverade på arbetsplatsen och således följa de uppsatta policys och riktlinjer som finns (Chen, Chen & Wu, 2018).

2.3.1 Expectancy theory

Expectancy theory förklarar varför människor motiveras på sin arbetsplats och bygger på de tre variablerna expectancy, instrumentality och valence (Colquitt, Lepine & Wessen, 2011). Expectancy berör den förväntan anställda har på sitt resultat baserat på vilket engagemang de lägger ner på uppgiften, instrumentality handlar om en förväntan på en belöning av bra resultat och valence behandlar vilket värde den anställda sätter på påföljden av ett resultat (Lee, 2019) Genom att multiplicera dessa variabler får man ett resultat som kan mäta motivationen på en arbetsplats (Colquitt, Lepine & Wessen, 2011).



Figur 2.2: Expectancy theory (Colquitt, Lepine & Wessen, 2011, s 182)

2.3.2 Herzbergs tvåfaktorsteori

Herzbergs tvåfaktorsteori är en teori för att förklara hur anställda motiveras på arbetsplatser (Farr, 1977). Herzberg argumenterar för att det finns två olika sorters faktorer; motivationsfaktorer som gör de anställda motiverade och hygienfaktorer som gör de anställda missnöjda ifall de inte finns på plats (Hur, 2018). De faktorer som enligt Herzberg motiverar anställda är prestation, erkännande, ansvar, tillväxt, möjlighet till befordran och själva jobbet, de faktorer som istället räknas som hygienfaktorer är lön, status, arbetskollegor, policies, arbetsförhållanden och administration (Habib, Awan & Sahibzada, 2017).

2.3.3 The human contribution

En artikel av Tsui et al. (1997) beskriver hur individer bidrar till sina arbetsplatser. De har genom en studie med anställda från tio olika företag kunnat dra slutsatsen att personer som känner stöd från sin arbetsplats utför bättre arbete och värnar om sin arbetsplats. En situation där den anställde känner att denna och företaget är lika investerade i sin relation eller att företaget är mer investerade än den anställde är dem miljöer som den anställde gör bäst ifrån sig (Tsui et al., 1997).

2.4 Tekniska stöd

2.4.1 Systemstöd

Enligt Stewart & Lacey (2012) bör människans svaghet gällande säkerhet tas större hänsyn till, författarna kritiserar ISA-program och argumenterar för att alternativ bör tas fram för att hjälpa människor att uppnå medvetenhet. ISA fokuserar på teknisk kompetens och förlitar sig på att tekniska experter ska förmedla hur de anställda ska tänka och vad de bör veta, utan ta hänsyn till att de möjligtvis redan gör det (Stewart & Lacey, 2012). Det finns risker för att anställda känner sig tvingade till ändrat beteende vilket i sin tur kan resultera i minskad motivation till att arbeta säkert (Adams & Sasse, 1999). Istället för att instruera anställda om vad de ska göra, bör alternativt fokuset ligga på varför beteendena uppstår (Stewart & Lacey, 2012).

Adams & Sasse (1999) diskuterar även den kognitiva börda som uppstår när företag begär att anställda använder flera samt komplexa lösenord. Frekvent byte av lösenord i kombination med antalet lösenord som den anställda krävs komma ihåg leder enligt studien till att säkerhetsgraden i sig minskar på lösenorden (Adams & Sasse 1999). En annan säkerhetsrisk som är knuten till komplexa lösenord är anställdas tendens att skriva upp dem (Haga & Zviran, 1991).

2.5 Litteratursamanfattning

Nedan presenteras en sammanfattning av den litteratur som använts som grund för studien, sammanställt i en tabell. Tabellen har delats in de olika teman som studien har haft som genomgående röd tråd.

Tabell 2.4.1.1: Litteratursamanfattning

Tema	Faktor	Litteratur
Informationssäkerhet	-Policys och riktlinjer -Compliance	*Aldawood & Skinner (2018)* *Ghafir et al (2016)* *Gollmann (2011)* *Hadnagy (2011)* *Karolinska institutet (2019)* *Pahnila, Siponen & Mahmood (2010)* *NE (2019)* *Rousse (2014)* *Whitman & Mattord (2008)*
Utbildning	-Utbildningar och säkerhetskampanjer -Anställdas medvetenhet -Kontinuitet -Introduktion till informationssäkerhet	*Bulgurcu, Cavusoglu & Benbasat (2010)* *Chen, Chen & Wu (2018)* *Eminağaoğlu, Uçar & Eren (2009)* *Jenkins, Durcikova & Burns (2011)* *Kajtazi & Bulgurcu (2013)* *Lee, Lee & Yoo (2004)* *Leveque (2006)* *Pahnila, Siponen & Mahmood (2010)* *Petty & Cacioppo (1981)* *Puhakainen & Siponen (2010)* *Siponen (2000)* *Thomson & von Solms (1998)* *Whitman & Mattord (2008)*
Motivation	-Motivation för bättre prestation -Möjlighet att påverka	*Chen, Chen & Wu (2018)* *Colquitt*, Lepine & Wessen *(2011)* Habib, Awan & Sahibzada (2017) *Herath & Rao (2009)* *Hur (2018)* *Farr (1977)* *Lee (2019)* *Tsui et al. (1997)*
Tekniska hjälpmedel	-Systemstöd	*Adams & Sasse (1999)* *Haga & Zviran (1991)*

		Stewart & Lacey (2012)

3 Metod

I detta kapitel kommer tillvägagångssätt för rapporten samt motiveringen till varför arbetet har utförts på följande sätt. Kapitlet avslutas med en presentation av den etik som har genomsyrat hela studien.

3.1 Procedur

Nedan kommer en redogörelse för den metod vi har använt för att nå fram till vårt resultat. Vår studie är influerad av en kvalitativ studie då det resultat som en kvalitativ studie medför är att föredra för att besvara en frågeställning av vår art så utförligt och korrekt som möjligt.

Vi har valt att använda oss av en intervjustudie då vi vill ha omfattande och detaljerade svar på våra frågor (Oates, 2006). De frågor vi vill ha svar på är ofta komplexa frågor som behöver längre svar och ibland möjligheten att ställa följdfrågor till vår intervjuperson (Oates, 2006). Våra frågor kan även uppfattas av en känsligare natur som intervjupersoner inte är villiga att svara på i enkätformulär (Oates, 2006). Våra intervjuer har skett semistrukturerat vilket grundar sig i Jacobsens (2002) rekommendation gällande hur en kvalitativ studie kan utföras.

3.2 Litteraturstudie

Vi har valt litteratur genom våra nyckelord samt genom den avgränsade forskning som har gjorts inom ämnet. Vi har valt att använda litteratur som avgränsar vår frågeställning och ger oss relevanta insikter i ämnet. Vi har valt att använda oss av tryckta böcker samt artiklar publicerade online. Vi har valt att till stor del använda oss av material tryckt i välkända akademiska journaler för att säkerställa innehållets äkthet (Oates, 2006).

Vår insamling av litteratur har till stor del skett genom sökmotorn LUBsearch och AISeLibrary då informationen som publiceras här blir granskad innan den publiceras. Vi har även valt att enbart använda oss av litteratur som finns på universitets olika bibliotek.

3.3 Datainsamling

3.3.1 Urval

Vi har genomfört intervjuer med olika personer ansvariga för informationssäkerhet på olika organisationer för att få information angående hur de ställer sig till informationssäkerhet och hur de stödjer sina anställda med att arbeta med säkerhet. Vi har även valt att intervjua en forskare i ämnet. Vi har valt att intervjua personer som arbetar på stora till medelstora företag eller företag som är en del av en större koncern. Mellanstora företag är företag med 51–249 anställda och stora företag har fler än 250 anställda (Upphandlingsmyndigheten, 2019). Detta för att få så representerbara svar som möjligt för vår studie. Vi har inte valt att avgränsa oss till en specifik sektor då problemområdet gäller i alla olika sektorer.

3.3.2 Intervjuer

Vi har valt att använda en semistrukturerad intervjustruktur då vi vill ha så djupgående svar som möjligt. En semistrukturerad intervju tillåter intervjupersonen att svara på frågan i större djup och får möjligheten att tillföra egna tankar och funderingar (Oates, 2006). Intervjufrågorna var bestämda på förhand men strukturen gav rum till att ställa följdfrågor ifall mer djupgående svar önskades. (Jacobsen, 2002). Vi hade även möjlighet att kunna byta ordning på frågorna baserat på tidigare svar och intervjuns stämning (Oates, 2006). Intervjuerna följer Oates (2006) rekommendation och är alla ca. 30 minuter. Det är en bra tid som inte gör intervjupersonen trött men samtidigt ger möjlighet till djupare svar.

Av de fem intervjuer som utfördes skedde fyra på intervjuobjektets kontor eller arbetsplats. Detta grundade sig i Oates (2006) rekommendation att intervjuer bör genomföras i en miljö där intervjupersonen känner sig trygg och bekväm. Den femte intervju skedde över videokonferens, detta fungerade bra och den fysiska distansen var inte ett hinder. Intervjuobjektet visade även genom delad skärm upp vad denne pratade om när han förklarade olika procedurer och systemlösningar vilket bidrog till att vi fick en sann bild av vad denne pratade om.

Tabell 3.3.2.1: Intervjuer

Respondent	Organisation	Organisations-typ	Position	Plats	Omfattning
R1	Organisation röd	Stort företag	CIO	Respondentens kontor	36 min
R2	Organisation gul	Litet företag, del i större koncern	Administrativ chef	Respondentens kontor	28 min
R3	Organisation grön	Stort företag, del i större koncern	CTO	Respondentens kontor	29 min
R4	Organisation blå	Stort företag	CIO	Videokonferens	37 min
R5	Forskare lila	Universitet	Forskare inom informations-säkerhet	Respondentens kontor	28 min

3.3.3 Intervjuguide

Vi har valt att dela upp våra intervjuer i två olika delar för att förenkla analysarbetet. Del 1 är inledande frågor som agerar som en presentation till intervjupersonen och till företaget. Del 2 innehåller frågor rörande informationssäkerhet, attityd och motivation. Det är dessa frågor som vi främst har valt att basera vår analys på. Vi har kommit fram till våra intervjufrågor efter den litteratur som vi har valt att använda oss av. Nedan presenteras frågorna som

återfinns i del två tillsammans med den litteratur samt identifierad faktor och område som den baseras på.

FP benämner våra primära intervjuer vilket är de vi har haft med säkerhetsansvariga på olika företag. FS benämner våra sekundära intervjuer vilket är de vi har haft med forskare inom ämnet.

Tabell 3.3.3.1: Intervjuguide

Fråga	Frågeformulering	Faktor	Område	Litteratur
FP1	Hur ser era säkerhetsåtgärder ut?	-Policys och riktlinjer -Utbildning och säkerhets-kampanjer	-Informations-säkerhet -Utbildning -Motivation	*LeVeque (2006)* *Pahnila, Siponen & Mahmood (2010)* *Whitman & Mattord (2008)*
FP2	Arbetar ni kontinuerligt med informationssäkerhet?	-Kontinuitet	-Utbildning	*Eminağaoğlu, Uçar & Eren (2009)* *Pahnila, Siponen & Mahmood (2010)* *Whitman & Mattord (2008*
FP3	Vilken typ av tekniska stöd används för att underlätta säkerhetsarbetet?	-Systemstöd	-Tekniska hjälpmedel	*Adams & Sasse(1999)*
FP4	På vilket sätt introduceras anställda till rutiner och regler kring informationssäkerhet?	-Introduktion till informations-säkerhet	-Utbildning	*Whitman & Mattord (2008)*
FP5	Hur medvetna om arbetet med informationssäkerhet tror ni att era anställda är?	-Medvetenhet -Compliance	-Utbildning -Informations-säkerhet	*Chen, Chen & Wu (2018)* *Siponen (2000)*
FP6	På vilket sätt kan anställda uppleva era säkerhetspolicies som begränsande?	-Motivation	-Motivation på arbetsplatsen	*Farr (1977)* *Habib, Awan & Sahibzada (2017)* *Hur (2018)*
FP7	Hur motiverar ni era anställda till goda säkerhetsbeteenden?	-Motivation	-Motivation på arbetsplatsen	*Chen, Chen & Wu (2018)* *Farr (1977)* *Habib, Awan & Sahibzada (2017)* *Herath & Rao, (2009)*

				Hur (2018)
FP8	Finns det något sätt för de anställda att bidra i arbetet med säkerhet?	-Möjlighet att påverka	-Motivation på arbetsplatsen	*Farr (1977)* *Habib, Awan & Sahibzada (2017)* *Hur (2018)* *Tsui, et al. (1997)*
FS1	In what way is the human factor a threat to information security?	- Policys och riktlinjer -Compliance	- Informations-säkerhet	*Aldawood & Skinner (2018)* *Ghafir et al (2016)* *Hadnagy (2011)*
FS2	What is your opinion regarding the agency vs. structure dilemma in organizations?	- Policys och riktlinjer - Utbildning -Motivation	- Motivation	*Farr (1977)* *Habib, Awan & Sahibzada (2017)* *Hur (2018)*
FS3	Is there a downside to policies and restrictions regarding security?	- Policys och riktlinjer - Motivation	- Motivation	*Farr (1977)* *Habib, Awan & Sahibzada (2017)* *Hur (2018)*
FS4	Should companies place a greater trust in their employees?	-Motivation	- Motivation	*Farr (1977)* *Habib, Awan & Sahibzada (2017)* *Hur (2018)*
FS5	How can companies create support for employees regarding conducting their work in a secure way	- Systemstöd	- Tekniska stöd - Utbildning	*Adams & Sasse (1999)*

3.4 Transkribering och dataanalys

För att skapa en avslappnad stämning under intervjun valde vi att inte anteckna intervjuobjektens svar utan istället spela in samtalet. Enligt Jacobsen (2002) kan antecknande påverka samtalets kvalitet då den som håller intervjun blir tvungen att ofta tittat ner och bryta ögonkontakt med sitt intervjuobjekt. Jacobsen (2002) uttrycker även att inspelningar kan leda till hinder då tekniska problem kan hända med inspelningsanordningen. För att minimera riskerna för att detta skulle hända valde vi att spela in samtliga intervjuer på båda våra telefoner. Vi var båda med och utförde samtliga intervjuer och vi båda utförde transkribering. Vi valde att dela upp alla inspelningar i hälften för att vi båda skulle få ta del av samma intervju och på så sätt bilda liknande uppfattningar. Alla transkriberingar skedde inom tre dagar efter att intervjuerna hade genomförts då det fortfarande var färskt i minnet vid det laget.

Enligt Jacobsen (2002) är det viktigt att transkribering av intervjuer ska ge en bild av datan i sin helhet. Detta innebär att ändringar ska undvikas då det kan leda till manipulation av resultatet (Jacobsens, 2002). Vi har valt att ta bort ord som "eh" och "hm" från transkriberingen då detta var utfyllnad som inte tillförde något av värde till studien. Vi valde dock att behålla "mm" då detta uttryckets istället för "ja" av en del intervjuobjekt.

Vår metod för dataanalys grundar sig i de punkter som finns i Researching Information Systems and Computing (Oates, 2006). Vi började med att sortera vår data utifrån tre punkter; data som inte behövs till vår undersökning, data som beskriver kontext till undersökningen och till sist data som är relevant för vår forskningsfråga. Den data som vi anser är relevant för studien har vi fortsatt analysera. Vi har sedan delat upp svaren från respondenterna efter fråga och analyserat de svar som vi fått genom att jämföra dem med varandra och koppla dem med de teorier som vi har valt att använda till vår studie. Vi har använt en matris (Appendix 1) för att enklare kunna se. (Oates, B.J. 2006).

3.5 Validitet och reliabilitet

En studies validitet eller giltighet är enligt Jacobsen (2002) uppdelat i två kategorier: intern och extern. En studie med kvalitativ ansats har ofta en hög intern giltighet vilket innebär att resultatet är riktigt och inte missvisande (Jacobsen, 2002). Detta kan ske genom att låta intervjuobjekten se över transkriberingen och komma med invändningar om de inte känner igen sig i svaren (Jacobsen, 2002). Vi gav därför respondenterna denna möjlighet, det var dock ingen av dem som valde att läsa igenom transkriberingarna.

Extern giltighet handlar om hur väl det går att generalisera resultatet från studien (Jacobsen, 2002). Då studier som utförts efter en kvalitativ metod, som vi har gjort, är flexibla och öppna blir det svårt att generalisera dem (Jacobsen, 2002). Dock är syftet med en kvalitativ studie inte att komma fram till ett generellt sammanhang utan att utifrån ett mindre urval av intervjuobjekt kunna skapa en generell teori (Jacobsen, 2002).

Studiens reliabilitet eller pålitlighet är knutet till huruvida något under studiens gång har påverkat dess resultat (Jacobsen, 2002). Vi valde att inte skicka ut frågorna i förväg utan istället endast informera intervjuobjekten om uppsatsens syfte i stora drag. Orsaken till detta var att vi ville ha spontana och ärliga svar vilket speglar verkligheten. Forskaren som intervjuades var dock ett undantag och bad om att få frågorna upplästa innan vi började spela in. Vi ansåg dock inte att detta var tillräckligt med tid innan intervjun började för att påverka svaren i tillräckligt stor utsträckning för att ge negativ effekt på svarens pålitlighet.

3.6 Etik

Enligt Jacobsen (2002) är det essentiellt att under en studies gång ta med den etiska aspekten samt respektera dess inverkan på arbetet. För att arbetet ska utföras korrekt är det av yttersta vikt att säkerställa att de intervjuade har fått den information som krävs för att de ska kunna besluta om de vill delta i undersökningen eller inte. Det är även av högsta vikt att intervjuobjekten endast är med i studien om det har skett av fri vilja (Jacobsen, 2002). Enligt Jacobsen (2002) är det viktigt att informerat samtycke sker under insamlingen av datan. För att säkerställa att detta skedde utformade vi ett mejl som skickades till samtliga respondenter med

information med syfte att hjälpa objekten att besluta vare sig de väljer att delta eller inte. Innan varje intervju återberättade vi lite om vad vi undersökte och informerade intervjuobjekten om att de hade rätt att ta tillbaka samtycke eller avbryta intervjun när som helst.

Vi valde även att anonymisera respondenterna och deras företag för att skydda dessa. Denna avvägning gjordes då informationen inte var väsentlig eller påverkade studiens resultat. Därför har vi döpt om intervjuobjekten till R, följt av siffran 1–5. Företagen har fått fiktiva namn efter färger. Dock har vi intervjuat respondenter från ett universitet, vi har valt att anonymisera vilket universitet det handlar men inte att det är ett universitet. Orsaken bakom detta är att en sådan anonymisering hade lett till att stora delar av transkriberingen hade behövts ändrats vilket Jacobsen (2002) menar kan korrumpera svaren. Enligt Jacobsen (2002) är det viktigt med riktig presentation av datan vilket innebär att den inte ska ändras eller förfalskas. Vilket är varför vi har valt att ta med och presentera vår transkribering i rapportens bilagor. Vi valde även att ge våra intervjuobjekt möjligheten att se över de transkriberade intervjuerna för att försäkra oss om att samtycket fortfarande gällde.

4 Empiri

Under den här sektionen avser vi att presentera resultatet av våra intervjuer.

4.1 Informationssäkerhet

4.1.1 Policys, regelverk och riktlinjer

R2 berättar om hur deras arbete med säkerhet är upplagt av ett omfattande regelverk som till stor del kommer från koncernen. Deras arbete styrs av policys som till stor del reglerar hela deras arbete. Intervjupersonen känner inte att regelverket är relevant men använder det på arbetsplatsen då det är påbjudet. R3 beskriver även att dem använder sig av regelverk som likt organisation gul är delvis styrt av koncernen. R1 beskriver att universitetet påbjuder relativt lite struktur utan försöker istället ge de anställda utrymme för att kunna sätta egna riktlinjer. Även R4 berättar att de använder sig av säkerhetspolicys för att reglera hur de arbetar med säkerheten.

R5 berättar att det finns baksidor med för mycket policys i ett företag. De kan uppfattas som väldigt begränsande och därmed svåra att motivera för de anställda och därmed få dem att följa dessa. För många eller för avancerade policys kan även vara svårt för de anställda att hålla koll på.

4.1.2 Compliance

R1 berättar att de anställda på universitetet inte följer uppsatta riktlinjer i deras arbete med informationssäkerhet. Han berättar även att på universitetet är arbetet med IT och informationssäkerhet decentraliserat och mycket av ansvaret ligger på de olika fakulteterna. Universitetet använder sig även av riktlinjer istället för policys.

"vi använder begreppet "riktlinjer för" för att de är inte tvingande regler..." R1(2019)

Likaså berättar R2 att deras anställda inte alltid följer de policys som de har satt upp. R3 berättar att de anser att de anställda följer alla riktlinjer efter bästa förmåga. De kan uppfatta att allt inte följs ordagrant då det ibland stör arbetet i för hög grad men att de anställda i sådana fall gör en egen riskbedömning som de anser är tillräcklig.

Båda intervjupersonerna nämner att de anställda kan känna sig begränsade av riktlinjerna och policys som en av anledningarna till detta.

"Alltså, man, missförstå mig rätt, fuskar därför att det är lite lättsammare än att göra rätt vissa gånger..." R2 (2019)

Ingen av det intervjuade arbetsplatserna har aktivt några konsekvenser för beteende som inte följer riktlinjer. R3 berättar att de anställda följer enligt hans förståelse de uppsatta reglerna enligt bästa förmåga. R4 berättar även han om att de anställda följer de uppsatta policys.

4.2 Utbildning

4.2.1 Utbildning på arbetsplatsen

Från våra intervjuer har vi märkt att flertalet av de intervjuade organisationerna försöker anordna någon form av utbildning för sina anställda. Däremot har vi märkt att det är skiftande hur stor vikt man låter utbildningen ta av de anställdas tid. R4 berättade om hur de lägger stor vikt vid att utbilda sina anställda för att höja säkerhetsmedvetenheten. Som nyanställd behöver du genomgå ett antal e-learning utbildningar, du kommer även behöva genomgå flera andra utbildningar under din anställnings gång samt utsätts de anställda för phishing-tester cirka en gång i månaden.

"...basically we do around 6 e-learning modules a year for all employees. So all employees are required to take that, and if you are a new employee you are also required to take an, I think it is four specific modules when you start with [företagsnamn], whether you are just starting as an consultant or starting as an employee." R4 (2019)

Ingen av de andra tillfrågade organisationerna arbetade lika strukturerat med arbete för att kontinuerligt stärka säkerhetsmedvetenheten. R3 berättade om hur man som anställd måste genomgå vissa utbildningar om man ska få en högre behörighetsgrad i deras system. De arbetar även med att höja säkerhetsmedvetenheten via en, liknande ISA, satsning där de ca. en gång i kvartalet påminde de anställda om specifika delar i deras säkerhetspolicy för att på så sätt öka medvetenheten om varför det är viktigt att följa dessa.

"...får ett mejl i kvartalet i alla fall om att just nu gör vi en liten rejd att, okej men, dubbelkolla att verkligen alla hårddiskar är krypterade liksom, eller dubbelkolla, eller att man påminner om hur bra lösenordet måste göras eller att…" R3 (2019)

R1 berättar att det finns ett antal utbildningar på universitets utbildningsportal som de anställda har möjlighet att genomgå. Dessa är däremot inte obligatoriska utan är frivilliga för personalen att genomgå. R2 berättade att de inte arbetar med någon internutbildning av sin personal alls.

4.2.2 Anställdas medvetenhet

Gällande anställdas medvetenhet inom informationssäkerhet fick vi olika svar angående graden av medvetenhet. R1 uttryckte att medvetenhetsnivån bland forskare har gått från icke-existerande till en prioritering.

"Men det var inte utifrån ett informationssäkerhetsperspektiv utan ett rent praktiskt. Jag måste kunna fortsätta forska. Så man hade inte det fokuset men GDPR och alla skriverierna runt det där har triggat väldigt mycket" (R1, 2019)

R3 upplevde att anställda hade en god medvetenhet angående säkerhet och arbetet med säkerhet. Han menar på att de anställda har koll på policyn men att han samtidigt inte förväntar sig att den genomsnittliga anställda ska ha järnkoll på den.

R2 och andra sidan upplevde att anställdas medvetenhet var låg och att intresset för att ändra på detta var lika lågt. Denne tillade även att den själv även ser på en det som en "hygienfaktor".

4.2.3 Kontinuitet

R3 berättade att de arbetade kontinuerligt med informationssäkerhet då du var tvungen att genomgå vissa utbildningar för att få högre behörighet. De arbetade också till viss del med att då och då påminna de anställda om specifika delar av policyn. R4 berättade att på organisation blå arbetade även de kontinuerligt. De hade ett rullande schema för alla anställda som innehåller både utbildningar och olika test, exempelvis gör det regelbundet så kallade phising-test.

"This is why we do regular awareness activities. Cause we want you know to keep people thinking about the security issues that are there because they are there whether it is in your personal life or at work you are facing, you know cyberthreats all the time" R4 (2019)

Både R1 och R2 berättade att de inte jobbar kontinuerligt med informationssäkerhet för de anställda. R2 berättade att de gärna ville hålla det aktuellt men gjorde inget direkt för att genomföra detta mer än att ibland nämna det på större möten. R1 berättade att de som var anställda för att arbeta med säkerhet hade kontinuerliga möten men det fanns inget för de anställda.

4.2.4 Introduktion till informationssäkerhet

De olika tillfrågade företagen hade liknande sätt att introducera informationssäkerhet till de anställda. Alla de tillfrågade företagen utom företag röd lät sina anställda skriva på ett avtal vid anställning där de avtalar att följa de rådande policys som finns.

"...är det inget som man skriver någonting överhuvudtaget, utan personalavdelningen fattar ett beslut om att man är anställd och så får man det hem i brevlådan…" R1(2019)

Företag grön valde att även använda den anställdes första dag som ett tillfälle att tillsammans med närmast överordnad gå igenom rådande policys så att den anställde har full förståelse till vad denne ska förhålla sig till. Företag blå tog introduktionen steget längre och hade förutom avtal obligatoriska utbildningar för sina anställda. Företag gul hade ingen ytterligare introduktion förutom att skriva på sekretessavtal.

R5 anser också att nyanställda bör skriva under avtal i början av anställningen för att organisationen ska känna sig skyddade redan från början.

4.3 Motivation på arbetsplatsen

4.3.1 Motivation

R1 anser att beroende på vilken nivå av känslighet som deras information innehåller bör de anställda få tillstånd att göra saker som höjer motivationen. De arbetar inte aktivt med att motivera de anställda till bra beteenden men tillåter och ger de anställda plats att själva kunna ta till åtgärder för att öka sin egen motivation. R2 berättar att de inte heller arbetar med motivation för att få de anställda att ha bättre beteenden.

R3 berättar att de försöker göra det enkelt att göra rätt som ett sätt att motivera de anställda. De arbetar även med att få en stark företagskultur och därmed få de anställda att känna sig motiverade. Förutom detta försöker de göra de anställda medvetna om att det går att göra fel och skrämmer upp de anställda när saker går fel. R4 berättar att de arbetar med motivation genom att försöka få de anställda medvetna om de fördelar som kommer av att arbeta säkert både privat och professionellt.

R5 berättar att motivation spelar en stor roll för att en organisation ska hålla sig levande. R5 berättar även att för mycket restriktioner kan få de anställda att känna sig mindre motiverade.

4.3.2 Möjlighet till att påverka

Alla intervjupersoner nämnde till viss mån att deras anställda hade möjlighet att komma med förslag på förändringar för att bidra till arbetet med informationssäkerhet. R3 berättade att denne ofta fick in förslag på förbättringar av sina anställda. Dessa mottogs gärna men man fick sålla bland dem då vissa var till viss del överdrivna.

> *"...vi jobbar ju med utvecklare och ingenjörer liksom. Många gånger kan de har väldigt svartvita, svartvitt sätt att se på saker. Så även om de rent tekniskt, eller man kan ju få in ett förslag som rent tekniskt skulle höja säkerheten jättemycket men du skulle också vara helt omöjligt att få det att fungera i verkligheten."* (R3, 2019)

R1 berättade att de anställda hade stor frihet att göra egna system och använda vilket många också gjorde. Universitetet jobbade även med möten där de ansvariga på de olika institutionerna fick träffas och diskutera sätt att höja säkerhetsnivån på universitetet. R2 berättade att de anställda kunde påverka de regler som inte kommer från koncernen, dock hade det hitintills inte hänt att en anställd hade haft en önskan att påverka.

> *"...kommer då någon och har en idé eller vill bidra på något sätt i en sån här fråga så kommer det att fångas och tas emot positivt och så kommer man utifrån det på något sätt förädla det. Det har inte hänt än så länge."* (R2, 2019)

R4 nämner att det finns möjlighet att påverka genom SANS-programmet och därmed öka nivån av medvetenhet angående säkerhet. R5 rekommenderar att anställda bidrar till informationssäkerhet genom att hålla sig uppdaterade och arbeta på bästa möjliga sätt med informationssäkerhet.

4.4 Tekniska hjälpmedel

4.4.1 Systemstöd

R2 berättar att de inte använder någon form av systemstöd. De delar som inte regleras av koncernen försöker de hålla så enkelt som möjligt för att minska den kognitiv belastningen på de anställda och motverka dåligt säkerhetsbeteende. R3 berättar att de i nuläget använder sig av en mjukvara för att kunna lagra lösenord åt sina anställda. Detta för att underlätta den kognitiva belastningen samt göra det enklare för de anställda att följa policys. R1 berättar att de har stöd främst för vissa av fakulteterna.

"Ja, vi har olika former av tekniska lösningar som gör att du kan skydda data olika mycket beroende va de är för data du har." R1 (2019).

De använder sig av olika lagrings- och bearbetningslösningar som skyddar den information som samlas där. Ett problem de stöter på är däremot att de olika forskningsgrupperna inte är medvetna om att mjukvaran finns så de skapar den på nytt när de hittar ett problem. Likt R2 berättar R4 att de inte använder sig av någon form av systemstöd.

R5 påpekar att det finns mycket programvara som kan hjälpa de anställda att göra ett bättre jobb, ett av dem är stöd i lösenordshantering. Det ligger på organisationen hur mycket stöd de vill ge sina anställda.

5 Diskussion

I detta kapitel ställer vi våra empiriska resultat mot vår litteratur.

5.1 Informationssäkerhet

I arbetet med säkerhet använde sig samtliga respondenternas arbetsplatser policys och riktlinjer i en viss utsträckning. Syftet med detta var att minska hotet som den mänskliga faktorn utgör för organisationernas informationssäkerhet. När det kom till uppföljning vid handlingar som bröt mot organisationens policys skiftade respondenternas metoder. Enligt både R1 och R2 hade bådas arbetsplats låg grad av uppföljning i samband med om anställda gick emot policys eller riktlinjer. Det var även dessa två intervjuobjekt som upplevde minst compliance från de anställda. R3 uttryckte högre compliance från anställda och att olika former av utvecklingssamtal eller påminnelser utfördes när anställda avvek från policys. R4 berättade under sin intervju hur även om anställda kontaktades om de upptäcktes bryta på policys var det inget som betydde egentliga konsekvenser.

"I would say in general [företagsnamn] has a very, let's say forgiving culture." (R4, 2019)

Vårt resultat angående policys och compliance stämde väl överens med Pahnila, Siponen & Mahmood (2010 som argumenterar för att otydliga eller icke existerande konsekvenser för non-compliance leder till att de anställda inte följer riktlinjer i den mån som är önskvärt.

R2 berättade att de hade väldigt mycket regler kring hur de anställda skulle agera, detta ledde delvis till att de anställda inte följde reglerna men kulturen kring informationssäkerhet ledde till ett stort ointresse där det varken fanns vilja eller ett enkelt sätt att påverka hur man arbetade. Detta stämmer även in i den åsikt som R5 delade med sig kring informationssäkerhet där denne argumenterar att för mycket restriktioner skapar ointresse och ett non-compliance beteende. Även ledningen på organisation gul visade ett visst missnöje över vilka regler som fanns vilket även kan spegla hur de anställda uppfattar reglerna, detta kan kopplas till Herzbergs tvåfaktorsteori där anställda inte känner att deras prestation kommer bli uppskattad av ledningen och därmed känner sig omotiverade (A Habib, Awan & Sahibzada (2017).

5.2 Utbildning

Likt Kajtazi & Bulgurcu (2013) ser vi en koppling mellan hur de anställda utbildas i informationssäkerhet och hur väl medvetna dem är kring hotbilden som finns. De organisationer som i högre grad utbildade och välkomnade en dialog med sina anställda rörande informationssäkerhet ansåg sig även ha anställda med en högre grad av medvetenhet kring informationssäkerhet.

R3 och R4 berättar båda att de arbetade till viss del kontinuerligt med att informera och utbilda sina anställda inom informationssäkerhet. Detta följer de riktlinjer som Whitman & Mattord (2008) skriver om. R3 berättade att de cirka en gång i kvartalet skickade ut mejl om en utvald del av policyn. Genom detta håller de anställda medvetna om policyn. R3 berättade även att de

hade individuella samtal med sina anställda ifall man visste att de var sämre till exempel på att genomföra en del av policyn eller ta till sig information. Även R4 berättade att de arbetade med ett väl strukturerat program för att öka medvetenhet, detta innehöll olika e-utbildningar samt regelbundna phising-tester. Detta arbetssätt stämmer överens med Pahnila, Siponen & Mahmood (2010) diskussion att man bör hålla de anställda medvetna om policyn, konsekvenser och hotbild. R3 ansåg även att de anställda i hög grad var medvetna om policyn och följde denna.

R2 berättade att de anställda skriver på ett avtal om att förhålla sig till reglerna men att de senare inte pratar mycket om innehållet eller betydelsen av det. R1 berättade att de inte heller har någon utbildning eller uppföljning kring kunskapsläget kring informationssäkerhet. Båda respondenterna ansåg att medvetenheten kring informationssäkerhet var förhållandevis låg på deras arbetsplatser.

"Vi bryr oss inte om den, vi funderar inte på den utan det är därför att jag tvingar dem att skriva på ett sekretessavtal" R2 (2019)

R1-R4 svarade att de introducerade policys till sina anställda i början av anställningen. Detta följer Whitman & Mattord (2010) som argumenterar att det borde ske tidigt för att de anställda inte ska kunna forma egna uppfattningar om vilka regler som gäller då detta är svåra beteenden att bryta. R1 berättade att de tillhandahöll viss utbildning till sina anställda som var fullt frivillig att delta i.

5.3 Motivation

Ingen av R1-R4 arbetade aktivt med att försöka motivera sina anställda till att göra ett bra arbete. Detta kan enligt Chen, Chen & Wu (2018) vara en av anledningarna till varför både R1, R2 och R4 inte ansåg att de anställda följde utsatta riktlinjer.

Enligt expectancy theory så baseras anställdas prestation utifrån deras förväntningar i form av eget resultat, belöning och värdet på den tilltänkta belöningen (Colquitt 2011). Därför kan en företagskultur som visar uppskattning vid bra beteende och som uppskattar påverkan främja dessa beteenden. Även detta kan vara en orsak till att vissa av respondenterna inte ansåg att de anställda följde policys. Önskan att göra bra ifrån sig och att få någon form av belöning för sitt arbete kan återfinnas i de anställdas möjlighet att påverka. De anställda som har möjlighet att påverka sin arbetsplats (R3/R1) kan hantera allmänna säkerhetsproblem bättre men även förbättra nuvarande säkerhetsläge.

Även Tsui et al (1997) argumenterar för att anställda som känner sig motiverade av sin arbetsplats och arbetsmiljö bidrar i högre grad till sin arbetsplats. Detta kan vara allt från att följa policys till att komma med ideer och förändringar. Baserat på detta anser vi att arbetsplatser i högre grad ska arbeta med att motivera sina anställda. Vi tror att förhoppningen om en mindre belöning får anställda att både känna sig motiverade att följa policyn men också påverka arbetet. Detta stöds även av Hearth & Rao (2009) som argumenterar för att organisationer ska använda sig av positiv betingning för att främja bra säkerhetsbeteenden.

Herzbergs tvåfaktorsteori beskriver även ansvar, prestation och belöning som faktorer som gör anställda motiverade (Awan, S et al 2017). Vi tror därför att det kan gynna organisationer att ge sina anställda en viss tillit baserat på att de har blivit utbildade och även uppmuntra

innovation. Vi tror att bristen på tillit från koncernen kan vara en av anledningarna till att R2 inte ansåg att de anställda var motiverade eller intresserade av informationssäkerhet och därmed inte var medvetna om det eller följde policys.

"Man piskas in i ett hörn och där ställer man sig. Men man är egentligen helt ointresserad om man frågar." R2 (2019)

Chen et al (2018) argumenterar även för att medvetenhet kring informationssäkerhet gör att de anställda följer riktlinjer till en högre grad. Detta kan förklara varför R3 och R4 som ansåg sig ha medvetna anställda också var de som ansåg sig ha anställda som bäst följer policys.

R3 berättade att ett av sätten de motiverar sina anställda är med hjälp av laganda och känslan att vara en del av företaget. Detta följer Tsui et al (1997) som vill att de anställda ska känna att organisationen är investerad i dem för att känna sig motiverade och tillochmed bidra till arbetsplatsen. Även Puhakainen & Siponen (2010) argumenterar för vikten av motivation. Motiverade anställda väljer oftare den centrala vägen och är då lättare att kontrollera än anställda som väljer den perifera vägen (Puhakainen & Siponen, 2010). Detta då de som följer den centrala baserar sina beslut på kognitivt tänkande och därmed i högre grad följer policys (Puhakainen & Siponen, 2010).

5.4 Tekniska hjälpmedel

Systemstöd som alternativ för att främja säkert arbete från de anställda var en faktor som gav väldigt olika resultat från de olika respondenterna. Företag blå var den organisation som i störst utsträckning använde sig av tekniska lösningar för att minska ansvaret för de anställda i form av att "ständigt" behöva vara sin vakt. De använde sig av en mjukvara som minskar hotet från mänskliga faktorn och specifikt social eingineering och phising. R3 berättade även att de använde sig av tekniska hjälpmedel, de använder sig av ett program för lösenordshantering som stöds av både (Adams & Sasse 1999) & (Haga & Zviran, 1991).

R1 berättade att de hade tekniska hjälpmedel för att säkra att forskning var säker från åtkomst och förstörelse. Detta stämmer överens med CIA-triadens första två punkter (sekretess och integritet) (Gollmann, 2011). Vi ifrågasätter dock om denna typ av säkerhet är anpassad till att vara nyttig i praktiken. Punkten om tillgänglighet fylls inte upp då om något låsts in är det fast och kan varken ändras eller nås (Appendix 1) (Gollmann, 2011).

Vi ser gärna att systemstöd tas fram för att hjälpa anställda att arbeta på ett säkert sätt och hjälpa organisationer skydda sina tillgångar. I samband med detta ställer vi oss frågande till om de finns en risk att teknologi blir ett hinder istället för en framgångsfaktor. Whitman & Mattord (2009) argumenterar för hur säkerhetspolicys måste integreras med arbetet inom organisationen för att ge någon faktiskt nytta. Vi argumenterar för att detta tankesätt bör appliceras på systemstöd för att främja ett bra arbete med informationssäkerhet. Det stöd som finns för de anställda i form av systemstöd bör vara väl förankrade i policys för att integreras i verksamheten. Även R5 håller med att det är och kommer förbli en svårighet för organisationer att få sina anställda att arbeta säkert. R5 tror att framtiden kommer gå mot mer teknisk övervakning,

Att kontrollera att anställda arbetar säkert kommer enligt R5 att vara en svårighet. Hennes prediktion angående hur informationssäkerhet kommer tacklas av organisationer är kopplat till övervakning av anställda i en högre grad än idag. Hon poängterade även svårigheten med att övervaka anställda då det inkräktar på deras privata sfär.

6 Slutsats

I detta kapitel avser vi svara på våra forskningsfrågor.

Vår grundläggande forskningsfråga "*Bör organisationer se över vilket typ av stöd som erbjuds för att anställda ska kunna arbeta säkert?"* besvaras genom vår studie. Vi anser att generellt bör företag se över hur de arbetar med informationssäkerhet för att nå optimalt resultat. Våra respondenter arbetar på olika sätt med informationssäkerhet utefter hur deras organisation ser ut, dock finns det delar som hade kunnat förbättras hos de alla.

Vi avser även att svara på frågan "*Hur ser samspelet mellan restriktioner och tillit ut i arbetet med informationssäkerhet och hur påverkar det compliance mot organisationens policys?".* De organisationer som arbetade med mycket regler för att säkerställa att de arbetar på ett säkert sätt upplevde att deras regelverk inte efterföljdes i den mån som det borde. Däremot var de nöjda över hur väl de anställda efterföljde policys. De organisationer som istället arbetade med mindre struktur kände även dem att deras riktlinjer efterföljdes till viss mån. De tillfrågade som arbetade med att utbilda sina anställda upplevde att deras anställdas medvetenhet rörande säkerhetsfrågan var högre än de som inte utbildar sin personal. De som inte utbildar sin personal upplevde att de anställda till högre grad följde policys utan att ha förståelse för dem. Att inte utbilda sin personal kan leda till att de väljer den perifera vägen och därmed blir okontrollerbara. Att utbilda leder istället till att de anställda väljer den centrala vägen.

Vår studie har visat att för mycket restriktioner bidrar till ett ointresse att följa dessa. Det tillsammans med en bristande företagskultur kring informationssäkerhet bidrar till att de anställda inte följer policys och riktlinjer i den grad som är eftersträvansvärt. En annan faktor som bidrar till om anställda följer policys är den uppföljning som sker, bristande uppföljning ger de anställda bristande incitament till att följa policys.

Vi anser att vår studie har visat att det är viktigt att utbilda sin personal mot medvetenhet kring informationssäkerhet för att kunna ge förståelse för arbetet och därmed lägga grunden för en bra säkerhetskultur på arbetsplatsen. Vi ser det som en nyckeldel för att kunna ge de anställda den tillit som krävs för att de ska kunna bidra till arbetsplatsens säkerhetsarbete. För att kunna arbeta optimalt med informationssäkerhet krävs det en strukturell grund som de anställda kan utgå ifrån för att få förståelse och därmed motivation att arbeta på ett säkert sätt.

Vår studie visar även vikten av motivation på arbetsplatsen för att anställda ska följa policys och arbeta säkert. Motivation går att nå på flera olika sätt, vår studie har visat effekten av utbildning, tillit, lagkänsla och ansvar. Ifall de anställda känner sig tillräckligt motiverade av sin arbetsplats kan de istället för att vara en svaghet bli till en tillgång. Studien har visat att de organisationer som arbetade mer aktivt med motivation och därtill med att ge sina anställda eget ansvar hade anställda som tillför ideér och förslag till sin organisation. Vi anser att detta är eftersträvansvärt för organisationer och borde vara den målbild man vill se i sitt arbete med informationssäkerhet.

Appendix

Appendix 1 – Sammanfattning av transkribering

Fråga	R1 (Organisation röd)	R2 (Organisation gul)	R3 (Organisation grön)	R4 (Organisation blå)
FP1. Hur ser era säkerhetsåtgärder ut?	En tunn policy och utbildning i medarbetarportal.	Policydokument till stor del från koncernen.	Policys på koncernnivå, policys på företagsnivå, grundutbildning och mer omfattande utbildning för behörighet.	Utbildning, policys och olika tester exempelvis phishing.
FP2. Arbetar ni kontinuerligt med informations-säkerhet?	Lite från och till, mycket beroende på fakultet.	Tar upp det på möten emellanåt.	Ja. Arbetar ständigt med att förbättra. Gör "raider" för att förbättra compliance kring utvalda delar av policyn.	Ja, arbetar ständigt med att förbättra. De anställda gör regelbundet utbildningar och tester.
3.Vilken typ av tekniska stöd används för att underlätta säkerhetsarbetet?	Beroende på behov finns det en tjänst där man kan låsa in data.	Inga.	OnePassword.	En programvara som gör att man kan se en länks sanna ursprung.
FP4. På vilket sätt introduceras anställda till rutiner och regler kring informationssäkerhet?	Introduceras till medarbetarwebben vid anställning.	Skriver på sekretessavtal vid anställning.	På anställningsdagen går man igenom policy med närmaste chef. Skriver på sekretessavtal.	Vid anställning skriver man på avtal och gör 4 olika moduler utbildning.

FP5. Hur medvetna om arbetet med informationssäkerhet tror ni att era anställda är?	Har gått från helt ointresserade till visst intresse.	Fullständigt ointresserade.	Genomsnittlig anställd är medveten.	På en skala 1–5 ligger de på 3–4.
FP6. På vilket sätt kan anställda uppleva era säkerhetspolicys som begränsande?	Begränsar att komma fram på det vis som man vill.	De är väldigt begränsande, till exempel får man inte föra personregister	De begränsar exempelvis vilken mjukvara som man får använda. Även delar som begränsas i lag.	Ja, arbeta säkert innebär alltid extra arbete.
FP7. Hur motiverar ni era anställda till goda säkerhetsbeteenden?	Görs inte, försöker göra det enkelt att göra rätt.	Görs inte.	Göra det enkelt att göra rätt, ibland positiv betingning men inget strukturerat. Skrämmer upp när något går fel. Jobbar med företagskultur.	Säljer in fördelar både privat och professionellt med att arbeta säkert.
FP8. Finns det något sätt för de anställda att bidra i arbetet med säkerhet?	Genom sitt arbete och genom möten med ansvariga för informationssäkerhet.	Om någon har en idé tas den varmt emot, det har dock inte hänt än.	Hålla i föreläsningar, hitta felaktigheter, bättra på policyn.	Delta i SANS-program och delta i övningar.

Fråga	Forskare lila
In what way is the human factor a threat to information security?	Teknologi är inte alltid lösningen och därmed inte alltid felet. Ca. 40% av alla intrång sker oavsiktligt på grund av den mänskliga faktorn.
What is your opinion regarding the agency vs. structure dilemma in organizations?	De flesta väldigt strukturella företag försöker närma sig agency och bli plattare organisationer.
Is there a downside to policies and restrictions regarding security?	Anställda kan känna sig begränsade. Och för många är svårt att komma ihåg.
Should companies place a greater trust in their employees?	Absolut men det beror också på vilken bransch man verkar inom.
How can companies create support for employees regarding conducting their work in a secure way	Borde ha en säkerhetsavdelning och en avdelning riktad mot compliance.

What do you think the future of information security in the workplace will look like?	Mer digitaliserat och eventuellt mer övervakning. Hotbilden kommer öka i takt med digitaliseringen.

Appendix 2 – Intervjuguide

Del 1: Inledande frågor: Företag

- Vad heter du och vad har du för roll på företaget?
- Vad har du för erfarenhet med att arbeta med säkerhetsfrågor?

Del 2: Frågor rörande informationssäkerhet

- Hur ser era säkerhetsåtgärder ut?
- Arbetar ni kontinuerligt med informationssäkerhet?
- Vilken typ av tekniska stöd används för att underlätta säkerhetsarbetet?
- På vilket sätt introduceras anställda till rutiner och regler kring informationssäkerhet?

Del 3: Frågor rörande anställdas roll och motivation

- Hur medvetna om arbetet med informationssäkerhet tror ni att era anställda är?
- På vilket sätt kan anställda uppleva era säkerhetspolicys som begränsande?
- Hur motiverar ni era anställda till goda säkerhetsbeteenden?
- Finns det något sätt för de anställda att bidra i arbetet med säkerhet?

Del 1: Inledande frågor: Forskare

- Would it alright if we record this interview?
- What's your name and job title?
- Why did you choose this field of studies?

Frågor rörande informationssäkerhet

- In what way is the human factor a threat to information security?
- What is your opinion regarding the agency vs. structure dilemma in organizations?
- Is there a downside to policies and restrictions regarding security?
- Should companies place a greater trust in their employees?
- How can companies create support for employees regarding conducting their work in a secure way?
- What do you think the future of information security in the workplace will look like?

Appendix 3-Transkribering organisation röd

Augusta: Då får vi fråga, vill du presentera lite och berätta lite om vad du jobbar med?

R1: - Ja! Jag heter [namn] och är IT-direktör här på universitetet. Jag har arbetat i många år utifrån en roll nere på rektors stab med att hålla ihop IT-frågorna för [universitet] och sedan för ungefär 2 år tillbaka så fick jag också ansvaret för den operativa avdelningen [universitetet]. De är huset som ni är i nu. Universitetets stora gemensamma IT-avdelning, det finns ju IT-avdelningar på ett antal fakulteter också. Några fakulteter väljer att köpa sina tjänster, här så. Sen i höstas är jag också ansvarig för informationssäkerhetsarbetet på universitetet. Vi har det nu uppdelat så att dataskyddsfrågorna ligger på chefsjuristen och informationssäkerhetsfrågorna ligger på mig. Vårt dataskyddsombud snedstreck informationssäkerhetssamordnare som vi anställde förra året inför GDPR sa upp sig så att därför har vi lite vakanser och sånt, så därför är jag lite halv insatt i de här frågorna nu också eftersom jag ansvarar för dem från och med oktober-november någon gång.

Augusta: Ja, vad har du för erfarenheter med att jobba med säkerhetsfrågor?

R1: Ja det är jag som har varit ansvarig för att skriva dom befintliga informationssäkerhetsriktlinjerna som en del utav det tidigare stabsjobbet. Jag har jobbat med de frågorna länge, mest utifrån IT-säkerhetsfrågorna, jag har ansvaret för de centrala beställningarna alltså rektorsuppdrag nu till [arbetsplats] under 10-15 års tid. Nu har jag båda delarna, nu beställer jag de här sakerna av mig själv. Det gör det lättare att komma överens.

Augusta: Ja!

Johanna: Kan tänka mig det.

R1: Utom budget. Det är ändå inte lätt.

Johanna: Ja, hur jobbar ni med säkerhet, vi tänker liksom; är det policies, utbildningar och på vilket sätt?

R1: Vilken säkerhet?

Johanna: Ja asså på vilket sätt… anställda.

R1: Ja asså säkerheten är, universitetets säkerhet är uppdelat i sex stycken områden som universitetsstyrelsen har lagt fast en säkerhetspolicy för universitetet och den är egentligen ganska tunn, mer en kappa. Och sen finns det inom de här respektive områdena riktlinjer för. Och vi använder begreppet "riktlinjer för" för att de är inte tvingande regler.

Augusta: Okej.

R1: Därför är det den definitionen. Skillnaden mellan föreskrift eller riktlinjer är att föreskrifter får du aldrig bryta. En riktlinje får du bryta emot om du kan motivera det av något rimligt skäl, inte bara att du vill inte. Mmm, brukar exemplifieras med att vi har en miljöpolicy som säger att du ska helst inte åka taxi, men måste du åka taxi så ska det vara en miljötaxi. Den är en riktlinje. Kommer man till stationen efter tjänsteresa klockan 22 en fredag och det hällregnar och står en taxi. Är det en föreskrift och den taxin inte är en miljötaxi, då får du gå hem i regnet.

Men är det en riktlinje så får du ta den taxin eftersom det inte finns en miljötaxi. Finns det både en miljötaxi och en annan taxi, ja då ska du ta miljötaxin. Det är det så vi har valt att skilja tydligheten, hårdhetsgraden inom beslutspapprena. Så vi har då i alla fall riktlinjer för sex olika säkerhetsområden. IT-säkerhet är ett och informationssäkerhet är ett, och sedan är det massa andra säkerhetsområden: fysisk säkerhet, brand, kemikalieskydd, alltså lås-och-larm delen av den. Lås-och-larmdelarna av de här hanteras utav vår byggnadsenhet eller byggnad som sköter fastighetsdelarna av det men IT och informationssäkerheten ligger här. Vi har styrdokument för det här och sen finns det utbildningar för anställda inom vår kompetensportal där man kan gå in och anmäla sig till olika typer av de, och det är framförallt på informationssäkerhetssidan. Vi har en egen version av det som myndigheten för samhällsskydd-och beredskap har tagit fram, den som heter "DISA". Så har vi en version som heter ["namn"] som man kan ta, den ska göras om men den finns.

Augusta: Har institutionerna och sådär lite egna, vad heter det, policies, du pratade om riktlinjer och sådär och sa att de var rätt så tunt?

R1: Mm. Det är ju tillämpningsföreskrifterna sen för hur väljer vi att göra på just vår arbetsplats? Det finns ju på en del institutioner, jag skulle säga att det är långt ifrån alla, det här är ju inte ett område som vi har tryckt speciellt hårt på utan det var GDPR och konsekvenserna utav dataskyddsförordningen som ju har drivit uppmärksamheten. Framförallt i forskningen. På utbildningssidan har man haft lite koll på det här därför man tyckt de bara varit logiskt o hålla koll på det här, asså att inte provpapper trasslar omkring i skrivare och papperskorgar hur som helst och sånt. Betygsgrundande information och färdigrättade tentor och sånt, det har man ju, det har inte varit där för att det funnits några papper kring det utan den stora grejen nu är hanteringen av personuppgifter och hur den har tuffats upp så mycket, dom bitarna, asså vi har ju haft PUL-lagstiftningarna tidigare som ingen har brytt sig om så Lunds universitets totala satsning på att följa upp PUL, har varit en utav vår jurister som har haft det som 5 % av sin tjänst.

Augusta: oj.

R1: Inte så jättemycket för en sån här stor verksamhet. Nu när det gäller dataskyddsfrågorna så ser det väldigt annorlunda ut, men vi ligger väldigt långt efter på många områden.

Augusta: När det handlar om att skydda era egen information och se till att anställda liksom inte gör ologiska grejer, och vad ska man säga? Råkar leda till att viktiga uppgifter kommer ut? Har ni något eller hur ser utbildningen och stödet ut där? Eller policies?

R1: Till att börja med så har vi väldigt lite information som är sekretessklassad i vår verksamhet överhuvudtaget, vi har inte den typen av verksamhet. Det finns vissa personer, och de är ganska nytt. Fram tills för några år sedan hade vi inga anställda med skyddade personuppgifter ens en gång, inte en enda. Vilket gör att de här frågorna inte har varit speciellt aktuella, eftersom vi sket i PUL behövde så vi inte bry oss om att skydda personuppgifterna utan de var ju mer att se till att grejerna inte försvinner, för vi har haft såna varianter där en forskargrupp fick all sin data stulen. Allting låg på en laptop som låg i en ryggsäck på parkeringen utanför triangeln i Malmö, någon knackade rutan och tog ryggsäcken.Allting fanns på en backup-hårddisk som låg i samma ryggsäck. Alltså man hade skyddat sig från att datan skulle bli korrupt och gå sönder, inte att man skulle få det stulet. O det var en forskargrupp som, ja de fick ju lägga ner sin verksamhet. Och det var 14 års forskning som försvann där. Det går ju inte att gå till finansiären och säga "hej, ni vet den här forskningen som ni har betalat för, vill ni göra det igen, tack?"

Därför så finns det ju en grund i, när det gäller på IT-säkerhetssidan som spinner över på informationssäkerhet här och ser till att grejerna inte försvinner. Så de jobbar vi ganska mycket med från olika håll tillsammans med de olika IT-organisationerna på universitetet och med [arbetsplats] så för att kunna erbjuda rätt lösningar till forskarna men vi har en arbets- och delegationsordning på universitetet som är extremt decentraliserad utan det är upp till, delegationerna går egentligen till dekanen och sedan till prefekten och kunna få bestämma vad är det för något som de tycker är bäst för att hantera sin verksamhet. Vad gynnar dem mest? Och det kanske inte har varit informationssäkerhetskraven som har legat högst, utan de har varit att få igenom utbildningen och få resultat och produktion i forskningen, det har ju varit högre. Nu med GDPR så har folk fått upp ögonen för att, vänta nu här de finns andra värden också som vi måste hantera, men det här är ändå ganska nytt på universitetet, det pågår oerhört mycket just nu, men framt till för några år sedan var det rätt kas.

Johanna: Du nämnde innan att där fanns utbildningar i en lärandeportal, är det något man måste göra eller är det…

R1: Mm, det finns ett beslut från rektor att alla anställda ska gå igenom den här [namn], informationssäkerhets informationen och det är universitetsstyrelsen jagar på och får halvårsvis rapportering kring läget på informationssäkerhet just eftersom man uppfattar att det inte var så bra och en av de sakerna som dom ju följer upp då är hur många som har gått den här utbildningen. Det är inte jättemånga.

Augusta: Så har vi en till fråga, när det kommer till informationssäkerhet, arbetar ni kontinuerligt med det med anställda eller är det med som sagt en introduktion och sen så…

R1: Jaa, det är en svår fråga. Det finns ingen rak linje, de här är olika på olika fakulteter och institutioner lite beroende på vad de är man gör. [Namn] fakulteten har inrättat ett informationssäkerhetsråd som består utav alla institutionerna, alltså prefekterna och de stora forksargruppsledarna från de stora forskargrupperna. De är inte nödvändigtvis stora forskagruppsledare. Där man tittar hur ska man kunna arbeta på medicinska fakulteten som ju har väldigt skyddsvärd information. Hur ska man kunna göra det här på ett enhetligt sätt? Var någonstans finns begränsningen till. Vi har kontinuerliga dialoger med säkerhetspolisen bland annat eftersom vi har en del personer, både anställda och doktorander eller anställda doktorander som kommer ifrån som har olika former av embargon. Hur hanterar man då informationssäkerhetsbitarna där? Det finns en klassisk skröna som för några år sedan från kemicentrum där säkerhetspolisen hade samlat ett antal forskargruppsledare och talat om att, som hade kinesiska doktorander, och då hade de så, vi vet om att all er forskning, alla era resultat, all er grunddata till er forskning skickas över till Kina, så att de skulle ha koll på det. Och varpå forskarna började asgarva och det vet vi väl. Vi är inte korkade, vi har redan bokat in ett besök i Kina om 7 år och se vad de har gjort med de här, tänkte vi stjäla tillbaka det så fortsätter vi. Det är så forskningen fungerar. Från att ha jättetight till att inte ha så tight alls.

Johanna: Används någon form av tekniska stöd för att kunna underlätta arbetet med informationssäkerhet?

R1: Ja, vi har olika former av tekniska lösningar som gör att du kan skydda data olika mycket beroende va de är för data du har. En som är framtagen eller egentligen båda två är från grunden framtagna för den medicinska forskningen som är stenhårt inlåst data. Du måste lägga in din grunddata i ett stängt utrymme, sen kan du bara arbeta med den där, du kan inte exportera den, du kan inte copy-pastea ut den, du kan inte printa den, du kan inte någonting. Och det finns två

sådana lösningar, egentligen en som är windowsbaserad för vissa typer utav användare och en som är linuxbaserad för dom som ska använda de stora beräkningsklustren för att räkna på det här. Så det finns det, så finns det olika nivåer för lagringslösningar och bearbetningslösningar, beroende på informationssäkerhetklassificeringen. Och de där är vi, vi håller på att reda ut vad som är [matris] av det här, därför det här har man ju gjort på egentligen utifrån forskarguppernas behov på de olika fakulteterna, men att de har varit svårt att veta att de finns något för den där forskargruppen där borta och den forskargruppen behöver samma sak men de vet inte om att den finns. Så då tar de fram det igen. Så det här har legat väldigt mycket på forskargrupperna att hantera och dom har varit bra på de här.

Augusta: Jag tänkte också på, under vår undersökning har vi tittat på de här, om man kan minska den kognitiva belastningen, istället för att vi ska komma ihåg massa jobbiga lösenord, om man kan lösa det på något annat sätt eller så, har ni någon typ utav såna lösningar här?

R1: Vi jobbar på att få en multifaktorautentiseringsvariant istället, så vi har, den finns tillgänglig, du kan använda typ de här google-authenticator, microsoft-authenticator-varianter för dem lösningar som har högre säkerhetsklassning eller vissa funktioner mot katalogssystemet om du ska tilldela behörigheter och sånt där så måste du ha multifaktorn, men det finns en massa praktiska problem med sånt här. Alltså av universitetets anställda är det ungefär, av 8000 anställda så är det ungefär 2000 som har mobiltelefoner från jobbet. Och nästan alla såna här lösningar bygger på att man har den här typen av utrustning men universitetet tillhandahåller inte det här, och 8000 mobiltelefoner som byts ut vartannat år som hygliga smartphones à 10 000 styck, de är en jävla massa pengar man ska ha fram för något som är tveksam i en nyttoberäkning, att man gör en roi-kalkyl på de här. Sen har ju alla mobiltelefoner ändå och de är ju det de litegrann bygger på men samtidigt är det svårt som arbetsgivare att ställa det kravet att som anställd på [universitet] ska du tillhandahålla din egen smartphone, utan att du får någon ersättning för det. Asså, de blir sån här politisk facklig fråga av det. Så att det är inte utrullat i stor skala men det finns ju för de mer känsliga tjänsterna och vi vill rulla ut det brett.

Augusta: Vi tänkte också på de här, med era policys och rutiner, på vilket sätt introduceras anställda till rutiner och regler kring informationssäkerhet?

R1: Man pekar på det här. Där är medarbetarwebben, där står alla regler. Läs dom.

Augusta: Okej.

R1: Och det gäller alla regler om allting. Det är helt värdelöst.

Johanna: Är det direkt när man blir anställd, så är det?

R1: Typ. Där kan du läsa om allting som står och den informationen som står där är dålig.

Johanna: Skriver man på något papper eller någonting?

R1: Nej!

Johanna: Nej.

R1: Det är jättespännande när man har en statlig anställning får man ett beslut hem som talar om att du är anställd. Man får inte som när du blir anställd i ett företag, har man

anställningskontrakt o man skriver på att, “okej, jag lovar att göra vissa saker och sköta mig på ett visst sätt med en motprestation lovar arbetsgivaren tillhandahålla bra arbetsmiljöer och inte ge mig sparken i onödan och sånt”. Men när det gäller staten så är det, så är det inget som man skriver någonting överhuvudtaget, utan personalavdelningen fattar ett beslut om att man är anställd och så får man det hem i brevlådan, vilket är lite “amen, okej...”

Augusta: Så du har inte, när du börjar här så har du inte gett aktivt samtycke liksom till att “ni gör det här, och jag gör det här och så skriver vi”...

R1: Nej.

Augusta: Under på det?

R1: Nej. Det finns ingenting sånt i den här regleringen. Sen så finns det då för vissa typer utav befattningshavare som får skriva på sekretessavtal och sånt när man väl börjar. Vi har ju de här, processen när de kommer nyanställda här så är det ju en massa saker, de är ju utbildningar de måste gå igenom, de är vissa avtal som de måste skriva på. Dom har ju, asså är du systemadministratör så kan du med automatik komma åt allting i ett system. Det är så, antingen litar man på systemadministratören eller så byter du ut den. Det finns inget alternativ. Men då är det ju att då skriver du på att du bara gör saker och ting som du behöver för tjänsten och att du har yttrandeförbud mot allt du eventuellt kan se och sånt där. Sen kan man ju diskutera om de stämmer överens med meddelarfriheten i grundlagen och sånt men det är en annan fråga.

Johanna: Intressant

Augusta: Så det är lite olika?

R1: Och det är ju, det är ju en rutin som är framtagen här. Det är inte generell för universitetet.

Augusta: Nej, det finns ingen gemensam liksom…

R1: Nej, det finns inget sånt nej. Utan det ligger som en del i det delegerade ansvaret att du måste på varje arbetsställe fatta beslut om dem sakerna som de .... Du har ett gemensamt regelverk att förhålla dig till men är det någonting universitetet är bra på är det att undvika regelverk. En utav de stora, mesta frågorna som kommer in till vårt dataskyddsombud just nu kring GDPR är “vi är ju ett universitet så de här reglerna kan väl inte gälla oss?”.

Augusta: Oj

R1: Asså det är ju så det ser ut och det har ju aldrig funnits några konsekvenser.

Augusta: Ah, för det är ändå känsliga uppgifter, speciellt när det kommer till studenter asså så här personnummer och sånt. Det är ändå en ganska känslig uppgift.

R1: Ah den är ju, det är ju inte klassat som en känslig uppgift men den är, det är ju en uppgift du inte ska strössla med i onödan.

Augusta: Nej precis, det är mer så jag menar.

R1: Och där är det ju så att för dem som är systemägare för studieadministrativa system till exempel så finns det ju krav på hur man ska hantera det där. Och att man måste tänka igenom vad är det för information som du faktiskt måste ha och vad är det du inte måste ha.

Augusta: Mmm okej

R1: Och när det gäller just utbildningssidan så har vi ju extremt mycket undantag ifrån GDPR i den svenska lagstiftningen som ger oss rätt att göra och behandla egentligen personuppgifter hur vi vill. Eftersom det räknas som samhällsnyttig verksamhet. Så det gör att vi lyder inte under GDPR på det sättet där.

Augusta: Ahh

R1: Det gäller samma för anställda för övrigt.

Augusta: Ja

Johanna: Hur medvetna om arbetet med informationssäkerhet tror ni att dem anställda på universitetet är?

R1: Har nog gått upp ganska dramatiskt dem senaste åren. Jag skulle säga att från extremt låg till iallafall visst intresse. Det är ganska många på forskarsidan så finns det ett stort intresse för man inser att man, att det här är någonting man faktiskt jobbar med. Jag skulle påstå att åtminstone en 80% av forskarna är intresserade av de här frågorna nu vilket de inte har varit tidigare. Asså det var 0% för några år sen, då var man intresserad av att inte bli av med sin forskning. Men det var inte utifrån ett informationssäkerhetsperspektiv utan ett rent praktiskt. Jag måste kunna fortsätta forska. Så man hade inte det fokuset men GDPR och alla skriverierna runt det där har triggat väldigt mycket. Så det kommer mycket frågeställningar kring det, hur ska vi hantera det, vad är det som gäller.

Johanna: Uppfattar ni att dem anställda följer riktlinjer?

R1: Nej. I vissa fall därför att det är svårt, därför att det går inte. Det är en sån enorm förändring som gör att vi inte är riggade för det här riktigt. Vi har en modell, vår informationssäkerhets riktlinjer, modellen där innehåller ju en klassificeringsmodell. Men den är det väldigt få som börjat jobba med eftersom vi tappade vår informationssäkerhetssamordnare tre månader efter att han blev anställd och har haft ett vakuum nu så har vi, de inte arbetats så mycket med att implementera den. Men där har vi nu nytt folk på väg in, informationssäkerhetssamordnare som börjar i maj och ett nytt dataskyddsombud som börjar i augusti. Så det kommer att bli deras stora puck att få ordning på de här frågorna på säkerhetssidan.

Augusta: Tror du att dem policys som finns nu, att man kan se en nytta i dem eller att det kan påverka lite varför ni tror att folk inte följer eller är det mest de här orsakerna med inga samordnare och sånt?

R1: Ja, jag tror att man inte ser någon nytta.

Augusta: Nej

R1: Med dem här, man ser dem som ett hinder för det man vill göra. De har blivit lärare och forskare av ett skäl, och att följa reglerna är liksom inte, det blir ju ett nödvändigt ont. Så är det ju inte. Och vi har ju den akademiska friheten, det begreppet, den akademiska friheten, som ju egentligen handlar om rätten att själv välja forskningsfråga. Skilt ifrån om du jobbar på Astra som säger att nu ska du forska kring huvudvärksmedicin, punkt. Så att jobbar du på universitet så får du välja själv vad det är för något du vill forska kring, vad din forskningsfråga är. Sen har det tolkats över till en generell frihet i att skita i regler.

Augusta: Så tror du att det kan vara så då att anställda upplever att policys är begränsande? Att om ni har policys…

R1: Ja. Det är dem ju.

Augusta: Ja.

R1: Det är ju det dem just är. Det är deras syfte, att begränsa till vad, att rita ut vad inom vilken ruta är det okej att springa och var någonstans är det inte okej. Och det gäller ju för alla policys som vi har.

Augusta: Men liksom begränsande för att kunna faktiskt komma fram till dit man vill? För det har vara en begränsning

R1: Det är dem ju nästan aldrig men de är begränsande för att komma dit jag vill på det sätt som jag vill.

Augusta: Ja.

R1: Och då finns det två varianter, antingen måste jag fundera ut ett nytt sätt för att komma dit jag vill eller så skiter jag i policyn och gör som jag ville. Alltså och där har det varit väldigt vanligt att man har skitit i dem här. Jag hade ju, [namn] var ju rektor här på mitten på 90-talet och hon sa att innan jag blev rektor så förstod jag inte att ett rektorsbeslut bara tolkas som ett inlägg i debatten. Och det har varit lite så, men lite mer tillskärpt idag. Men i grunden är det ändå samma.

Augusta: Men, tror du att det här har med liksom med motivation mycket att göra och så eller?

R1: Tradition.

Augusta: Tradition. Okej.

R1: Snarare tradition.

Augusta: På vilket sätt?

R1: Man har den där frihetstraditionen, alltså arbetar du i ett universitet så jobbar, de flesta som jobbar här som jobbar som lärare eller forskare dem jobbar dygnet runt, det är deras passion. Det är inte ett jobb, det är ett kall. Alltså du blir, satsar på att bli världsauktoritet på vänstergängade fjärilar. Alltså det är, du dedikerar ditt liv. Alla vakna timmar på dygnet, det finns ingen arbetstid. Skit i det, det är det här ditt fokusområde är. Det är såhär smalt. Och då, det som är störningsmoment för att liksom komma på alla de här bra sakerna kring det här,

uppfattas ju som negativt. Och vi har en styrstruktur som rent generellt universitetet och alla chefer väljs. Inte såna som jag då i stödverksamheten utan på institutionerna. Hela vägen uppifrån prefekterna till dekanerna till rektorn väljs ut av kollegorna. För att sitta under en, en prefekt sitter vanligtvis under en 3 år. Och blir chef över sina kollegor. Och efter dem tre åren så är det någon annan som blir chef så att nu är jag chef över dig i tre år och bestämmer över om du ska få forskningspengar, ska du få anställa en doktorand till, ska du hålla de här kurserna, ska du hålla det sen om tre år så är det du som ska tala om för mig samma sak. Sannolikheten att jag är taskig mot dig under dem här tre åren är ju rätt liten eftersom då vet jag att du får ju hämnd möjligheter om tre år. Och det gör ju att mina möjligheter som prefekt att driva igenom regelbaserade efterlevnader är ju ganska liten. Och tittar man på universitetet som organisation och jämför man med ett företag, säg att du har ett företag som har 300 anställda som omsätter 300 miljoner. Den som är VD för det har ju ofta någon form av utbildning för detta. Alltså chef för [universitetet], 8000 anställda omsättning på 8 och en halv miljard, han är expert på rävars migrations mönster. Det är en helt annan struktur runt allting som bygger ett universitet.

Augusta: Men tror du att det kan vara en negativ grej i det här att ledning inte har speciellt bra koll på informationsdelen. Tror du att det kan genomsyra hela organisationen?

R1: Ja. Dels så kan det genomsyra hela organisationen men samtidigt så har vi det läget att vi är rankade topp 100 i världen. Vårt stora problem med forskningen är att vi klarar inte av att göra av med alla pengar som vi får in. Och vi har haft ett högt söktryck på våra utbildningar. Det känns ju inte som vi har en dålig modell. För det vi egentligen är här för, det vill säga att utbilda och forska, ja vi saknar rätt mycket byråkratisk excellens. Vi är inte bra byråkrater, vi är inte bra på att följa regelverk. Men vi är uppenbarligen tillräckligt bra på att utbilda och forska.

Augusta: Så de här non-functional requirements är liksom inte så, de är inte så viktiga?

R1: Det är inte dem som värderas i din akademiska karriär. Alltså om du ska bli, från det att du doktorerar till din postdoktor till du får ditt lektorat och sen ska bli professor, det värderas och meriteras inte på något sätt om du är bra på att följa regler. Utan det meriteras att du publicerar. Och det gör att det finns liksom inga incitament eftersom det innan GDPR inte har funnit några konsekvenser av att skita i reglerna. Så har man inte brytt sig om dem. Det är motsvarande ett upphandlingsregelverk som vi har. Vi lyder ju under lagen om offentlig upphandling och det har man ju också glatt skitit i rätt mycket. Ända tills konkurrensverket kommer och gör en granskning, gör ett nedslag och ger oss böter för att vi inte följer lagen. Whoops helt plötsligt så ska man då börja följa lagen. Så det krävs såna saker, GDPR hotet om böter för GDPR som gör att det här faktiskt kan få konsekvenser för jag vill ju inte att man ska ta mina forskningspengar för att betala böter. Då är det bättre att göra rätt så slipper jag det så behöver jag inte bekymra mig om det så kan jag forska för pengarna istället. Så att det har aldrig funnits några incitament strukturer för att följa regelverken.

Augusta: Men det har aldrig känts, det har aldrig varit ett upplevt hot om intrång och liksom att information ska bli stulen eller försvinna framförallt kanske då? Det borde kanske…

R1: Det har funnits några, alltså det exemplet som jag sa om den stulna laptopen.

Augusta och Johanna: Precis.

R1: Det har ju triggat ledningen att göra saker och ting. Vi tillhandahåller ju såna här lösningar men det finns fortfarande ändrar inte styrelsen på på arbets och delegations ordningarna. Utan det är fortfarande upp till den enskilda forskaren. Det är den enskilda, alltså, tittar man på det för, när man gör riskvärderingen för universitetet och om en forskargrupp får all sin data stulen och får läggas ner så är det, det är inte skitsamma för universitetet men nästan. Det får ju ingen konsekvens för universitetet rankningar eller värderingar och trovärdigheten gentemot finansiärer eller samarbetspartner. Det är en katastrof fullständigt för den forskargruppen, det är ju riktigt tråkigt för instutionen, det är halvjobbigt för fakulteten och det är i princip skitsamma för universitetet. För då har vi 699 istället för 700 forskargrupper.

Augusta: Förstår.

Johanna: Det är väldigt intressant för det är ju en helt egen liten världsordning.

R1: Ja, det är det. Alltså ett universitet är en helt egen organism. Och dem som kommer in, vi märker det när vi anställer folk utifrån, de tror inte det är sant. Så här kan det inte vara, såhär kan man inte göra. Det måste ju finnas styrning och regler och uppföljning och sånt där. Nej, det går rätt bra ändå.

Johanna: Tror du att det är på något vis att det är den här lite fria strukturen, att det kan motivera dem anställda?

R1: Ja, det tror jag. Alltså det är därför folk väljer att vara här och forska istället för att vara på Astra och forska. För att Astra betalar 3ggr så mycket. Så det är ju friheten att kunna jaga sina egna drömmar här på ett annat sätt. Att faktistkt bränna fast i nån fix ide.

Johanna: Tror du att det här, att det är lite fritt kan bidra till att de individuella forskningsgrupperna till exempel utvecklar egna överlägsna sätt att hantera sin information?

R1: Ja, det kan vara. Både och det finns ju dem forskargrupperna som har säkert fullständigt överlägsen säkerhet på sina saker och folk som inte har någon alls. Och det är ju lite grann utmaningen att försöka liksom lyfta dem till någon gemensam lägsta nivå. Utan att pressa ned dem som har någonting högre. Alltså den klassiska varianten är att köra bulldozer och säga att det här är good enough och sen så trycker man ner det som är över och fyller i hålen sen har man en jämn metod. Och vi vill ju inte det, vi vill ju plocka det som är högt. Utan att försöka lyfta det som är, det som är lågt. Och det är, från vad ledningen kan göra är att försöka tillhandahålla då de här lösningarna, gärna finansierade så att de inte kostar någonting. För det är ju kronor och ören, det är ju typiskt att vi har ju jättemånga som när det åker på konferenser gör de inte reseräkningar för då kostar det ju traktamente och det har de inte råd med. Då är det bättre att liksom inte följa dem regelverken för då får de mer pengar över till forskningen och då kan de hålla på lite längre.

Augusta: Men hur, har ni något sånt här sätt, hur motiverar ni anställda? Om ni har något typ sätt att motivera anställda till att jobba säkert? Eller är det lite

R1: Finns inget särskilt sånt sätt utan det vi försöker göra är att ta fram lösningar som gör det enklare att göra rätt. Än att göra, antingen kan de använda de gemensamma lösningarna och då är de per definition tillräckligt säkra upp till en viss nivå. Eller så får de ta fram och göra sina egna lösningar och då kan de göra dem hur säkra eller osäkra som helst och då får de också ta kostnaderna själv. Det finns ju viss form av ekonomiska incitament och det har inte funnits så

mycket som säger att det är påväg fram så det är en av de grejerna som jag håller på med nu i den här rollen är ju att göra om de ekonomiska styrmodellerna. Så att vi ska kunna ha det, tillhandahålla det som är ledningens lägsta nivå. Det tillhandahålls. Vill du ha något annat, ja det står dig fritt att köpa det själv. Är det bättre eller sämre? Det har jag inga synpunkter på. Om du tar ansvaret själv för det, det du tycker är tillräckligt bra för dig. Men vi är inte där än riktigt, de håller på med såna växlingar hela tiden.

Johanna: Nu när vi har forskat lite på detta så har vi läst till oss bland annat att bring your own device till exempel är väldigt populärt ju för att det motiverar dem anställda till att göra ett bättre jobb. Men såna grejer, hur ställer ni er till det?

R1: Vi är helt öppna till det. Vi, vi jobbar ju, asså devices ska inte spela någon roll utan det som du är mest produktiv på med, det ska du använda. Det vi ska göra är att se till att tillhandahålla lagringslösningar som är säkra som gör att du kan, du kan med vilken device du vill ansluta till den här datan. Upp till en viss nivå där du inte får ansluta med någonting annat än en särskilt certifierad burk därför att det är liksom kravet på det. Det är ju alltid, all data ska ju delas upp egentligen efter tre ben. Egentligen från kapacitet, prestanda och informationsäkerhetsklassning. Det blir en kub med en massa fält i där vi måste tillhandahålla alla dem här olika lösningarna. Det gör vi inte idag . Vi tillhandahåller en del men vi håller på och bygger tillsammans, enda tills vi ska börja med det här eller att vi köper det någonstans ifrån. Nationella, internationella samarbeten. Då får man ju GDPR problem och privacy .. och amerikanska moln.. och sånt pyssel att dra i. Men det är..

Augusta: Men, ja då har vi väl en sista liten fråga här och det är egentligen, finns det något sätt för de anställda att, vad ska man säga, att bidra till arbetet mot, alltså, för säkerhet?

R1: Ja, alltså alla gör ju det hela tiden med sitt agerande men vi arbetar. En av de sakerna som ju är spridd är ju IT. Alltså It är decentraliserad och det enda som finns i vår arbetsordning med IT är att fakulteterna bestämmer själv. Det är det enda som står. Besluta själv över organisering och genomförande av IT är formella beskrivningen. Det gör ju att vi jobbar tillsammans med IT-frågorna ute. Vi hade ett möte i höstas där vi bjöd in alla som var intresserade av IT-säkerhet gällde det då. Kom med förslag på vad är det som kan höja, höja säkerheten på universitetet och då diskuterades ett antal punkter och sen har säkerhetsavdelningen suttit och skrivit papperna, beslutspapperna på det. Nu ska vi ha en ny avstämning av det sen så har vi ett, två gånger om året så har vi ett stort möte där alla IT-medarbetare på universitetet bjuds in där kommer det att vara en av punkterna, det här diskuteras, sen blir det grupparbete och prioriteringar och sen så får dem rapportera in från sina respektive institutioner, vad gör dem för att höja säkerheten. Så kan vi sammanställa det till en säkerhetsrapport till ledningen då. Jag är nämligen förespråkare för, jag är ganska ensam i, tillhör en minoritet i stödverksamheten som gillar den här arbete och delegationsordningen. Som inte tycker att vi ska införa så att säga bolagsstyrning, public management och där man bestämmer på toppen så ska man genomföra utåt utan jag tycker den här modellen faktiskt gynnar universitetet. Då gäller det också att dra nytta ut av dem sakerna som vi har. Och det är att vi har mycket folk ute som har kompetens och som sitter nära sina forskargrupper, sitter nära sina utbildningar som kan liksom se, vad är det för något som skulle gynna oss. Och så kan vi samla ihop dem oc hitta gemensamma initiativ och sen så rullar man på det och det är ju liksom successivt hela universitetet asså. De som är sämst höjs lite och de som är bäst höjs lite. Man kan liksom flytta hela universitetet upp på skalan lite och upp tullen viss punkt där det blir för mycket. Och det gäller ju att hitta den också. Det finns ju dem som är jätteambistösa och har för hög säkerhet och lägger pengar där som de

hade kunnat lägga på något annat, tillexempel utbildning eller forskning… Får inte ha ett eget syfte. .

Augusta: Ja, nej precis. Jag förstår.

Johanna: Ja, jag vet inte, har vi något mer?

Augusta: Nej, egentligen inte.

Johanna: Det var nog allt.

Augusta: Tack så jättemycket

Johanna: Ja, vi tackar!

Appendix 4 – Transkribering organisation gul

Augusta: Ja, och du är medveten nu att du får avbryta intervjun när du vill?

R2: Yes.

Augusta: Ja, jag heter Augusta och Johanna och vi skriver en C-uppsats om informationssäkerhet och interna, på det interna planet på företag om attityder och medvetenhet och stöd från ledning och sånt. Vill du berätta vad du heter och berätta lite om företaget som du jobbar på?

R2: Okej. Jag heter [namn] och vi sitter idag hos [företagsnamn]. Vi är ett ackrediterat kontroll och certifieringsorgan. Vår huvuduppgift är besiktning av kärnkraftverk och så utöver det besiktar vi massa annat och så certifierar vi en del ledningssystem huvudsakligen på en massa olika sätt. VI, iochmed att vi är ett ackrediterat organ så styrs vi väldigt hårt av en massa regler kring det hela och vi har därmed fått ett liksom, en ackreditering från myndigheten swedac som har gått igenom våra system och har liksom accepterat detta motsvarande dem regler som ställs. Det ställs också en massa regler, bland annat ifrån våra kärnkraftskunder som bland annat då reviderar oss och krediterar oss med avseende på informationssäkerhet bland annat. Såatte det är inte ett helt okänt begrepp och vi borde ha nån slags rimlig kontroll på läget kan jag, hoppas jag. Eh, personligen så fungerar jag som administrativ chef för bolaget och det betyder att jag gör allt det ingen annan kan eller vill.

Augusta: Ja. Då börjar vi med lite frågor kring informationssäkerhet. Eh hur ser era säkerhetsåtgärder ut? Exempelvis policys och liknande här på [företagsnamn]?

R2: Ehm, Informationssäkerhet. Allt det vi gör är väldigt strikt styrt av policydokument, i en rangordning som börjar med en management manual som beskriver då hur bolaget ska rattas då i relation till ägarens krav och så vidare. Nästa steg är då en kvalitetsmanual som beskriver allting hur vi hanterar saker och ting ur det verksamhetsperspektiv. Och så bryter vi ned det ytterligare då i en personalprocess, en uppdragsprocess sen en IT-process och så vidare där vi beskriver allt detta. I hela det här komplexet där, bakom hela detta komplexet så finns också en massa regler från Tüv-Nord. Ifrån koncernen, en tysk ägare, en tysk koncern som då implementerar sina regler i alla sina utlandsbolag. Tyskar är hysteriskt rädda vad det gäller

informationssäkerhet, när det gäller personsäkerhet eller personuppgifter. Asså GDPR och personuppgifter, dem är hysteriska va. Dem är så styrda av den här, av historien med stasi och allting annat gör att dem verkligen går på tårna och är jättenogranna med detta. Dessa regler får ju vi på oss också. Och då betyder det i sin tur att informationssäkerhet i någon mening börjar med att vi är jättetydliga på att det vi hanterar är vår kunds egendom. Det har vi inte rätt att läcka ut till någon annan eller till någon annan kund. Och en del i det att alla skriver ett sekretessavtal. Där vi liksom tydliggör detta och alla skriver under på att håll truten. En annan del är att, att det, all information hanteras ju digitalt och i våra datorer på diverse olika … och sådär. Där är det jättetydligt att alla såna här minnen dem förstörs, eller töms och förstörs när vi är färdiga med dem. En dator kastas inte på soptippen utan den rensar man hårddisken eller förstör den innan man kastar bort den. Var det ungefär vad du förväntade dig?

Augusta: ja, jag tycker det.

R2: Yes!

Augusta: Jag tänkte dock fråga om, har ni någon typ av utbildningar eller så för anställda, asså i form av information security awareness och liknande?

R2: Ja. Det är en, en integrerad del av introduktionen av en nyanställd. Varje nyanställd kommer alltid på en liksom introduktionsdag eller introduktionsutbildning. Och då finns det ett, en obligatoriskt part av den är att arbeta i ett ackrediterat organ. Och där går vi igenom de här reglerna och bland annat gör det här tydligt att den här sekretessen gäller, det här sättet hanterar vi information som vi fått. Vår kunds information.

Augusta: Är det, det är obligatoriskt för alla?

R2: Yes, yes.

Johanna: Det här arbetet med informationssäkerhet är det något som ni kontinuerligt arbetar på eller är det mer att det liksom finns de här policyn och sen så rör man inte det?

R2: Det är någonting som är, i någon mening väldigt självklart för oss och det är på något sätt så har vi stampat till och sagt att såhär är det och därmed så ifrågasätter vi det inte och omvärderar det inte förrän det finns skäl att ifrågasätta eller omvärdera det. Men det har varit väldigt klart och tydligt under ganska lång tid och det har liksom egentligen inte förändrats på ganska lång tid. Det, det blev ju en, ett omtag med detta när GDPR kom. Men egentligen inga förändringar utan bara några förtydliganden.

Johanna: Yes.

Augusta: Ja, vi tänkte också fråga, vad för typ utav tekniska stöd har ni för att, används då för att underlätta säkerhetsarbetet för, amen anställda och så? Förstår du hur jag menar? Systemstöd och så.

R2: Vi har inga system, systemstöd så för att underlätta i det här avseendet för våra medarbetare utan vi är, de system som vi använder är ju huvudsakligen våra vanliga sketna datorer. Vi använder ju då en, en databas för att hantera våra uppdrag och hantera det här, den här portalen som ni har tittat på en del va. Och då har vi i det sammanhanget haft någon slags genomlysning av den i avseende på GDPR. Med GDPR i ryggen men jag vill inte påstå att det på något sätt

är ett stöd i det här avseendet utan det här är nog mer en, ett medvetande och en, något slags, en. Jag hittar inte orden men ett sätt att agera från oss själva mer än ett systemstöd. Det största systemstödet vi kanske har i det här avseendet är papperstuggen vi har där ute. Som går ut på att väldigt mycket information vi får från våra kunder kommer i form av papper, i form av ritningar och sånt här underlag. När vi har jobbat med det och är färdig med det då kör vi det genom tuggen. Så blir det bara smulor av det sen så släpper vi det bekrymmret så att säga.

Augusta: För vi, vi pratade, när vi gjort våran förundersökning tittade vi lite på det här med kognitiv belastning på anställda och att komma ihåg mycket och sånt. Att det kan göra så att man kanske inte jobbar så säkert och så där. Ni har inga liksom, att, att systemet kanske hjälper en att slippa de här typerna av grejer som kan göra att man jobbar osäkert.
Sven: Nej

Augusta: Nej. Men det är ärligt och vi gillar ärligheten, det är jättebra!

R2: Det borde vi nog ha, men nej det har vi inte.

Augusta: Nej, okej. Super.

Johanna: Vi har redan varit inne lite på det men dem anställda, hur introducerar man dem till rutiner och regler kring just informationssäkerhet?

R2: Det är introduktion av nyanställd. Som sagt i den introduktionen så finns det en den här, en obligatorisk del. Som just heter att jobba i ett ackrediterat organ och där ingår just den biten.

Johanna: Är det någonting ni fortsätter jobba med alltså under anställningstiden eller är det mer bara en del av introduktionen?

R2: Det, vi ser till att vi håller det på ytan på ett sånt sätt att vi är ständigt medveten om detta. Det är inget alltså aktivt arbetande med frågan, däremot så förekommer det i våra möten, i erfarenhetsåterföring i flera olika sammanhang alltså att vi helt enkelt lyfter upp det och håller det på ytan igen så att alla ständigt är medvetna om det kravet på sekretess. Och egentligen jag exemplifierade detta med krav på sekretess och det är klart att krav på sekretess är bara en del i det hela men vi använder det begreppet i, och använder det i en betydligt vidare mening där vi då menar också då att säkerställa att vi behåller då kundens information också. Eller vår egen information på ett säkert sätt. Inte bara inte läcker utan även hanterar den på ett vettigt sätt alltså.

Augusta: En lite annan fråga, det har inget att göra med det här men du sa ju det här med tyskland och det. När man pratar informationssäkerhet så brukar man ju gå att desto mer man går åt säkrare säkrare desto mindre privacy får vi. Hur hur tror du att tanken där ligger ungefär på ert företag? Med det här med tyskland som du pratade om och stasi. Hur liksom, tror du att det påverkar lite hur ni arbetar det här med privat?

R2: Ja, alltså tyskarnas rädsla för detta påverkar oss så tillvida att reglerna, interna regler finns och vi måste förhålla oss till de. Och där vi då tycker att tyskarna överdriver och och är onödigt petiga i detta. Men det är ju liksom bara ett personligt tyckande från mig att det är så, jag har, är ju fortfarande, jag har ju bara att acceptera och gilla läget och följa detta. Och det är inget bekymmer för mig utan det är liksom bara att jag smårler lite och tycker att de är dumma ungefär sen går jag vidare och bara kan leva med det för det är inget problem för mig. Det är på samma

sätt som det här med GDPR är inte heller ett problem för att vi hanterar inte den typen av uppgifter utan vi hanterar vår kunds tekniska dokumentation, tekniska uppgifter sen rycker vi på axlarna, något annat är inte intressant. Vem vår kund är som person eller vilka åsikter eller religiös inriktning man har det är liksom icke fråga. Vi funderar inte ens på saken va. Samma med våra egna anställda. Vad man har för läggning på det ena eller andra sättet liksom det är bara en axelryckning. Vi har inte ens en fundering på det utan.

Augusta: Nej

Johanna: Ja, hur medvetna om arbetet med informationssäkerhet tror du att de anställda här är?

R2: Jättedåliga. Jättedåliga alltså. Det är på något sätt en icke-fråga. Vi bryr oss inte om den, vi funderar inte på den utan det är därför att jag tvingar dem att skriva på ett sekretessavtal, jag tvingar dem att aktualisera det hela på något sätt va, som gör att man liksom. Man piskas in i ett hörn och där ställer man sig. Men man är egentligen helt ointresserad om man frågar.

Augusta: Vad tror du det beror på?

R2: Okunskap och ointresse. Man vill fokusera på någonting annat.

Johanna: Uppfattar du att dem anställda följer de här riktlinjerna?

R2: Grovt uttryckt, ja. Grovt uttryckt men sen sker det massor av misstag och mer eller mindre omedvetna avvikelser från det hela.

Augusta: Tror du att det är mest omedvetet att man inte följer eller att det är att man ibland medvetet inte följer riktlinjer eller så?

R2: En kombination därav. Men jag tror att i grund och botten är summan av kombinationen lättja. Alltså man gör det här därför att det är lite enklare. Alltså, man, missförstå mig rätt, fuskar därför att det är lite lättsammare än att göra rätt vissa gånger och då kan det bli fel bara av det skälet. Ingen illvilja, ingen medveten vilja att göra på annat sätt utan bara att snedda hörn isåfall.

Johanna: Tror du att anställda kan känna att era policys är begränsade? Eller begränsande?

R2: Ja, absolut. Absolut. Överdrivna och besvärliga och jättetråkiga. Ja absolut.

Augusta: Tycker du att de är det också och inte bara kanske upplevs som det?

R2: Det kan nog hända. Ja, det kan nog vara. Såtillvida eller exempel på det är att vi för inga som helst personregister överhuvudtaget. Jag tänkte säga i datormiljö men egentligen i ingen miljö. Vi för inga personregister. Och det säger jag till alla medarbetare att ni får inte föra personregister, är det så att ni trots allt gör det så måste ni hålla mig medveten om detta eftersom det är jag som står som ansvarig för företaget i det avseendet. Och då säger alla, vi för inga personregister. Och så finns det ju någon som har en lista på sina kunder iallafall för att göra utskick om en ny tjänst eller någonting. Det är ju ett personregister och det är klart att då är ju det begränsande om jag säger att ni får inte och det är ju en överträdelse i nån mening om man trots allt gör detta. Men livet blir ju lite besvärligt om man inte ens kan ha en excel lista med namnen på sina kunder.

Augusta: Tror du att den här typen av begränsningar påverkar motivationen till att utföra sitt arbete till någon grad? Man känner sig begränsad i att få göra det man faktiskt vill?

R2: Jag tror man skiter i de här, mig och min reglerna i det här läget så genomför man sitt arbete i alla fall.

Augusta: okej.

R2: Så att, de kan hända att man upplever en viss begränsning men man rycker på axlarna åt det och så kör man på i alla fall.

Augusta: Okej… Förstår.

R2: Hahaha

Augusta: Ja, de är ju intressant att höra, haha.

Johanna: Alla sätt är bra…

R2: Jag vet inte.

Augusta: Det lär vi väl se. Men när vi ändå är inne på motivation, hur arbetar ni med motivation för att få anställda att ha goda säkerhetsbeteenden? Eller finns det något arbete med motivation?

R2: Ja asså väldigt lite. Det är återigen den här introduktionen av nyanställda då gör vi alla medvetna om vilka förutsättningar som gäller, varför de gäller och de är så och försöker ge motivation till, genom medvetenhet och kunskap, och sen försöker vi hålla det här på ytan genom att föra det på tal, genom att diskutera saken i olika möten av olika slag. Allt för ofta så blir det en gång per år vid våra årliga erfarenhetsåterföringsmöten. Då har vi ett pass där vi bland annat lyfter in den här typen av frågor och då gör vi då gör vi det som, där vi återigen tydliggör att det här är en förutsättning, ett villkor för vår existens, ett villkor för den tjänst vi erbjuder och den ackreditering vi har, asså de här är ett måste både i ifrån vår kund och i från myndigheten som ger oss de här körtillståndet, va. Och så motiverar också varför det ska vara så, vad det betyder för våra kunder, varför det är viktigt och så vidare, asså försöker att skapa en motivation genom kunskap och engagemang. Och jag tror att den här asså medvetenheten och kunskapen är de enda som ger motiv nog att jobba efter detta och försöka följa det. I de här diskussionerna är alla fullständigt överens, alla är helt med på att jajamensan, det här är rätt och så här ska vi göra, det finns ingen protest mot de,de är ingen som vill något annat men sen ta ibland lättjan över lite grann.

Augusta: Kan man, tror du att det finns något annat sätt att, för att kanske uppnå det här? De hrä goda beteendena, kanske via positiva liksom betingning?

R2: Nu, tror ju jag mer på piskan.

Augusta: Ja

R2: Mm, haha.

Augusta: haha, ja de funkar olika på olika arbetsplatser.

R2: Jag vet inte, det är en så i någon mening liten fråga, i någon mening så som är underordnad så vi har inte, som så tid och ork att spilla alltför på det här va? För det är närmast en hygienfaktor.

Augusta: Okej.

R2: Och de kan vara så att det är jag som inte har fattat bättre men för mig är det bara en hygienfaktor och därmed så är det liksom bara att tala om att så här gör vi och så alla nickar och ser glada ut och därmed så är jag nöjd. Om jag kunde göra på ett annat sätt eller borde göra på ett annat sätt, de vet jag inte helt enkelt. Jag har inte tänkt tillräckligt mycket på det.

Johanna: Finns det någon typ utav konsekvens om man inte följer de här riktlinjerna eller policies?

R2: Ja….

Johanna: Är det något som händer?

R2: Nej. nej, asså ja det finns en konsekvens ytterst, de finns djupt allvarliga konsekvenser ytterst i detta också. Det förekommer inte, det är otroligt sällan. Det är väldigt många år sedan nu men jag helt enkelt tog. Varje medarbetare hos oss eller allt det vi gör styrs det här kvaliets, det här management system, det här ledningssystemet som vi jobbar efter va. Och som att bland annat säger att varje medarbetare gör det han gör med den befogenhet att göra det här och utan den här befogenheten får han inte göra det han då är satt att göra. För bra många år sedan så tog jag befogenheterna ifrån medarbetare bland annat för överträdelser i det här avseendet va. Asså sätter gubben på lådan och säger han får inte gå ut till kunden och göra jobb och det är ju klart att det är en riktig käftsmäll för en vuxen människa så att säga.

(telefon ringer)
R2: Ursäkta mig, den ska bara bli tyst också.

Augusta: De är ingen fara.

R2: Så att det är klart att, det är ju en yttersta konsekvens som skulle kunna inträffa. Det händer inte, det har inte hänt, det kommer inte att hända för att det är en, vi sköter oss bättre än så.

Augusta: Men de här små grejerna som till exempel de här med de här listorna som du pratar om som egentligen inte ska hända. Det är ju egentligen inte om man säger så ett gott beteende som man inte riktigt följer. Hur ni när en sån sak händer, att du märker att folk har de här listorna även fast de inte ska ha listor, hur löser ni sånt?

R2: Pratar med dem. I mitt fall bara pratar med dem och sen bara återigen bara tydliggör, förklara vad och varför bara ber om att få information om detta, hanterar den listan på ett företagsgemensamt sätt, lägger den på en företagsgemensam plats på kraftverk och hantera den som företagsangelägenhet istället för din angelägenhet så att säga.

Augusta: Bättrar sig den personen då?

R2: Ja absolut, en stund.

Augusta: En stund?

R2: Hahaha. Ja men de är så va på något sätt och sen får man ge sig på det igen och så, men de är, asså, samtal, medvetandegör, skapa någon slags acceptans med samtal.

Augusta: Ja, förstår.

Johanna: Ja då sista…

Augusta: Ja då blir det sista frågan. Finns det något sätt för de anställda att bidra med säkerheten och att bli en tillgång?

R2: Hmm… Ja,, ja absolut. Hur ska jag säga. Vi är en väldigt liten organisation, vi är en väldigt platt och prestigelös organisation där samtalet flödar hela tiden och där varje god idé premieras på något sätt. Så att kommer då någon och har en idé eller vill bidra på något sätt i en sån här fråga så kommer det att fångas och tas emot positivt och så kommer man utifrån det på något sätt förädla det. Det har inte hänt än så länge, för att jag tror i huvudsak att de är en icke-fråga eller man har så många andra frågor man sätter först och så kommer det här långt därefter. Det här blir bara återigen bara en hygienfaktor och som man på något sätt bara hanterar det. Men att de medarbetare, eller våra medarbetare skulle kunna gör stor nytta, stor förändring i detta. Ingen tvekan om det. Jag har inte fantasi nog för att sätta det i, sätta fart på det så att säga.

Augusta: Vi pratade lite om det här, om det skulle komma in någon ny anställd som har en viss kompetens inom informationssäkerhet kanske inte är utbildad men kanske säger att "vänta de här ju egentligen konstigt, hur kommer det sig att vi jobbar på det här sättet?" Hur ställer ni er till det i så fall?

R2: Det skulle bara vara positivt. Det skulle, vi skulle bli jätteglada. Jag skulle sitta och vara bekymrad en liten stund och klia mig i huvudet och försöka förstå vad du säger men när du väl har baxat in mig på banan där kommer det bara vara positivt.

Augusta: Okej.

R2: Jag försöker se exempel, men jag kommer inte på något bra exempel just nu men det där förekommer nu och då. Kanske inte inom det här området så ofta men inom olika områden så kommer då någon med influenser från något annat håll och på det sättet förädlar våra processer.

Johanna: Jag tänker att det måste vara svårt att påverka de riktlinjerna som kommer från den stora koncernen?

R2: Det har vi ingen chans utan det är bara att tugga i sig och gilla men det går alltid att förstå dem rätt eller missförstå lite grann och skruva på dem lite grann. Vissa delar är hugget i sten och det är bara att tugga i sig men annat kan man nyansera och då kommer då erfarenheter från annat håll eller ett annat tankesätt än vad jag besitter och kan leda till att skruva det på rätt håll då.

Augusta: Mm, jag tänkte fråga en sak också som inte har med det här att göra men med säkerhet. Hur ser det ut med autentisering har många väldigt många lösenord eller vad har ni för typ utav

krav där på? Är det mycket att man ska ha många lösenord och svåra lösenord eller har ni lite facial recognition eller någonting? Hur fungerar det där?

R2: Förlåt, för att komma åt vad?
Augusta: Om du ska logga in på din dator, intranätet, hur…

R2: Nej, vi är jätteenkla, vi har, vi gör det busenkelt. Vi har vanliga standarddatorer, vi har vanliga standardtelefoner. Vi loggar in på våra telefoner som alla andra med tumavtryck eller fyra siffror eller något sånt där va. Vi loggar in på våra datorer med vanliga lösenord, inga större konstigheter. Koncernen ställer krav på att det här lösenordet måste ha visst antal tecken, visst variation i teckenarterna men det är inga, inget rocket science utan det är ganska enkelt.

Augusta: Är det en policy eller en riktlinje när det gäller det? Kan man som du sa, tolka det lite eller är det hugget i sten?

R2: Det är delvis, både och. Det är, vissa saker får vi via koncernen till exempel då mitt Tuv nord-konto inklusive e-postfunktion och då i e-posten så ingår det att koncernen ställer krav på att lösenordet ska vara så här långt och se ut på ett visst sätt och att det byts dessutom fyra gånger per år eller sex gånger per år, vad det nu är. Det påverkar ju både min dator, eller användandet av min dator och de påverkar också användandet av min telefon. Så till vida att att du kan, även om du kan öppna min telefon möjliggöra så kommer du inte åt min e-post därför att jag måste ställa om lösenordet dom här gångerna.Eller det är nog så till och med att om du skulle kunna öppna min telefon med lite skicklighet eller lite tur så kan du använda min e-post också under ganska lång tid och sen så småningom så tappar du den här möjligheten. Den här databashanteringen som ni tittade på här, det är en vanlig web-applikation, det är vanligt lösenord, det är inga konstigheter, inga definitioner att det måste vara si och så långt utan det är bara ett lösenord där vi just inför en sån tvåfasautensiering, heter det så?

Johanna, Augusta: Mm.

R2: Där jag precis just nu håller på att initiera att du en gång i månaden, en gång per halvår tror jag att vi har sagt tror jag måste identifiera dig själv med en sån här sifferkod, google-någonting.

Johanna: Ja vi har läst om det här fantastiska fenomenet att man blir tvingad att ha väldigt långa och väldigt många lösenord men de anställda skriver upp dem på lappar på datorn istället.

R2: Ja!

Johanna: Vilket ju är väldigt intressant för det är ju så motstridigt.

R2: Börja med att titta under skrivbordsunderlägget, där brukar de ligga.

Johanna: Ja.

R2: Nej, asså jättebasalt. Jättesvenssonaktigt.

Johanna: Jag tror nog att de är allt vi har.

Augusta: Har du någon fråga till oss eller sådär?

R2: Nej.

Augusta: Nämen dåså. Då avslutar vi med att tacka.

Johanna: Ja tack.

Appendix 5 – Transkribering organisation grön

Augusta: Eh då ska vi se här. Och du är medveten om att du får avbryta intervjun när du vill?

R3: Ja

Augusta: Så bra. Jag heter Augusta

Johanna: Jag heter Johanna

Augusta: Vi kommer från lunds universitet och håller på och skriver kandidatuppsats om informationssäkerhet. Främst om motivation och medvetenhet och lite balansen mellan strukturer och tillit.

Johanna: Ja, vill du berätta lite om företaget?

R3: Ehm ja. Vi är ju då på [företagsnamn] och vi är på [företagsnamn]. Vi är ju en koncern med ca 1700 anställda. Och som består av helägda dotterbolag då. Så [företagsnamn] där vi befinner oss nu är ett delägt dotterbolag till [företagsnamn] som är börsnoterat. Här i skåne är vi ca. 140 anställda, 130-140 någonstans. Och jobbar i princip i alla branscher vi, historiskt har vi haft ett ganska stort branch allokering mot telefon, alltså SONY, sony ericsson och ericsson och den typen av saker. Telekom är, numera har vi väl ingen bransch som står för mer än 17% tror jag är största branschen. Så vi är betydligt mer spridda och jobbar i princip med all form av mjukvaruutveckling och underhåll av mjukvaror. Och jag är, sitter jag här i skåne då så jag ansvar för all form av teknisk leverans vi gör. Vilket i praktiken innebär mest införsäljning av konsulter och men annars projekt med införsäljning och estimering, skapa lösningsförslag, och gå iland, hjälpa dem från att någon beställer någonting till att det är levererat helt enkelt. Bakgrund som utvecklare då.

Augusta: Ah, ja du började lite på det men vad har du för erfarenhet med arbete med informationssäkerhet?

R3: Är utvecklare i grund och botten och har jobbat framförallt med web, där är det ju väldigt höga krav på säkerhet hos många av kunderna vi jobbar med iallafall. Annars har jag, min bakgrund åh andra sidan, det beror ju på om man kopplar det till informationssäkerhet eller inte men jag har jobbat väldigt mycket med GDPR, jag har utbildat både internt och väldigt många kunder runt om i Europa på, med GDPR. Har även hållit i och ansvarat för vidareutbildningsprogram internt för just att höja säkerhetsmedvetenheten kring eller hos våra utvecklare för att säkerhet uppdateras väldigt det är så om man , i takt med att allt fler saker blir uppkopplade på ett allt mer sofistikerat sätt så finns det ju betydligt större och mer avancerade angreppsytor som man kanske inte tänkte på för 10år sedan men som nu är ett reellt problem.

Johanna: Hur ser era säkerhetsåtgärder ut?

R3: Det beror ju på hur man, om man tänker på hur vi skyddar och själva eller hur vi skyddar våra kunders information. Det är klart att det så klart det går hand i hand lite grann men jag tänker vad är det ni…

Johanna: Vi tänker hur ni skyddar er själva, om ni har policys, om ni har utbildningar, lite hur..

R3: Ja, alltså vi har ju på koncernnivå, på koncernnivå har vi ju ett antal strategier och policys som har med informationssäkerhet att göra på olika sätt. Informationssäkerheten kan man väl egentligen dela upp, i det perspektivet så delar vi upp det ganska mycket i buisiness cont… att vi ska kunna fortsätta driva verksamheten här om det händer någonting. Det är ju en del av informationssäkerheten att ha back-uper vi kan återställa, att ha alternativa drivsplatser för vår IT och såna saker. Den typen av policys som liksom, väldigt mycket från hur koncernens perspektiv trycks ned på oss. Det vill säga koncernen berättar inte hur vi ska göra det utan vi får ta fram egna såna planer att förhålla oss till att vi, kravet på oss är att vi ska ha en sån plan eller såna planer. Sen så finns det ju såklart skyddet mot medvetna angrepp. Där det handlar om både fysisk säkerhet, vem har tillgång till våra lokaler och på vilket sätt, fysisk nätverkssäkerhet, vem får tillgång till vilka resurser på nätverket beroende på vilket WiFi du är uppkopplad på osv osv. Och sen så är det såklart våra faktiska driftsmiljöer, vem har tillgång till vilken information, det kan ju gälla alltså filservrar men vem får tillgång till vilka dokument, och men det kan också gälla kunders information. Vi har ju väldigt mycket kunder som har väldigt höga säkerhetskrav där bara vissa personer hos oss som är godkända, man kan ju behöva vara godkänd genom länsstyrelsen eller SÄPO osv för att kunna komma åt vissa saker så då blir det väldigt styrt hur det administreras och vem som får lov att se vad där. Allting finns ju i skrivna policys i flera olika nivåer då. Det från koncernen är abstrakt, det jag har skrivit är … är lite mer kort och konkret och i vissa fall finns det specifika för ett enskilt projekt.

Augusta: Men hur ser det ut, ni har policys och riktlinjer och sådär men har ni någon typ ut av utbildning?

R3: Asså generellt sätt så, en grundläggande utbildning får man, en del av onboarden består av att man måste läsa personalhandbok, man måste läsa en allmän informationssäkerhetspolicy så alla får en grundnivå i utbildning av de policys som vi har, men de är ju ganska omfattande så ofta handlar det ju om att när du får access till någonting där det här börjar spela roll så att säga då måste du gå en ytterligare utbildning. Till exempel för att få tillgång till driftsmiljön för kunderna måste du gå en specialutbildning och beroende på vilken behörighet du har i den nivån så får du gå olika långa utbildningar mer eller mindre liksom. I princip kan du radera allting och dessutom sopa igen spåren efter dig så måste du verkligen veta vad du gör.

Augusta: Är det obligatoriskt då och att det är liksom…

R3: Ja, det är det ju. Det var inte det, vi hade en incident för, i höstas eller fram till i höstas var vi väl kanske, det var väl egentligen obligatoriskt då också men vi var väl, framförallt för våra interna miljöer lite slarviga ibland men så hade vi en kille som trodde att han skulle radera, att han raderade i sin egen utvecklingsmiljö men det visade sig att han raderade utvecklingsmiljön för hela [företagsnamn] men det gick att återställa. Och det var ett typiskt sånt fall av att han, han borde ha fått den utbildningen men han fick vissa behörigheter för att han behövde lösa någonting snabbt osv osv. Så lesson learned av det blev ju att vi gör inga quick fixes längre utan ska du få den typen av behörighet så ska du gå den utbildningen. Sen den är inte enormt

omfattande, den tar kanske 1 timme liksom och i princip består av att läsa ett väldigt utförligt dokument som består utav att så här ska du göra, om någonting mot förmodan skulle skita sig så har du, mycket handlar om att veta vad du ska göra om någonting går fel. Så att vi kan ha en chans att återställa efter en incident. För incidenter kommer alltid att inträffa på ett eller annat sätt.

Augusta: Men är det, testas man på det sen eller är det bara du ska läsa det här?

R3: Nej, det gör man inte. Sen så är det ju, vi väljer ju lite grann vem som får den behörigheten. Det är ju någonstans så. Det är ju jag som bestämmer vem som ska få vilka behörigheter på de här typen av sätt och jag skulle ju inte ge en sån behörighet till en person som jag inte litar på har sunt förnuft. Policyna finns ju där mest för att täcka in saker du kanske inte tänker på naturligt. Dessutom om det är något de själva skulle göra. Det testas inte riktigt, det finns liksom inte någon certifiering, det finns inte något quiz i slutet eller någonting. Det är så pass få personer, det är så pass sällan vi ger den typen av behörighet att det behövs.

Augusta: Men de som inte ska ha någon special behörighet eller sådär, behöver dem gå igenom nån, någon typ utav utbildning eller hur ser det ut där?

R3: Det är ju asså den grundläggande i början av en anställningn där man måste läsa igenom, jag tror personalhandboken, den täcker ju allt möjligt men en liten bit informationssäkerhet också. Säg att där är en del om informationssäkerhet sen finns det också en specifik informationsäkerhetspolicy som kanske, vad kan den va, på mellan 5 och 10 sidor kanske. Mycket handlar om, det är ju mycket stort och brett detta. Allting ifrån att du måste ha lösenord på din dator och din dator måste vara krypterad osv osv. Sen har vi ju, det finns väldigt få mekanismer för oss att kontrollera det här. Ibland har vi gjort det eller rättare sagt, en gång har vi gjort så att vi har skickat ut ett quiz för att undersöka, okej hur bra koll har faktiskt folk på det som står. Men det har ju mest varit ur ett, vi vill veta hur illa eller bra det är snarare än att man vill sätta dit någon.

Johanna: Arbetar ni alltså kontinuerligt med informationssäkerhet eller är det mer?

R3: Alltså kontinuerligt det är ju ett intressant ord. Men asså det är inte så att vi gör det en gång om året när vi har revision utan det är ju någonting man måste arbeta med. Sen , jag menar det faller ju, väldigt mycket av det ansvaret faller ju på mig och jag har ju väldigt många andra ansvarsområden så det är inte så att jag jobbar med det hela tiden men vi försöker hela tiden att bli bättre, vi försöker hela tiden att dokumentera och strukturera saker så att det ska bli, ja så att det ska finnas policys och att folk ska veta om dem policys som finns och är berörd av dem. Och det blir mer och mer.

Johanna: Använder ni någon typ av tekniska stöd för att underlätta arbetet för de anställda att liksom arbeta säkert?

R3: Mmm, asså vi har ju. Men tillexempel har vi en, vi använder en mjukvara som heter onepassword för som, där det ingår i policyn då att all typ av känslig information som man har får bara lov att sparas i OnePassword. Det är ju i grund och botten en mjukvara för att spara lösenord och inloggningar till platser. Vi har ju, en typisk utvecklare har ju fruktansvärt många användarnamn och lösenord till sina tjänster. Vissa som är ens privata och vissa som är HiQs och sen vissa som är hos kunderna. Och eftersom man dessutom byter uppdrag relativt ofta så kommer man ju tillslut ha, amen jag tror att innan jag började sån här mjukvara så många hundra

iallafall inloggningar. Väldigt svårt att hålla dem i huvudet, väldigt lätt att man börjar använda samma lösenord på flera platser och så vidare. Så därför, både för att underlätta och för att höja säkerheten tvingar vi alla anställda att spara den typen av information i mjukvaran. Och där finns även funktioner för att dela då liksom om det finns, vissa känsliga uppgifter kan ju vara gemensamma för alla som jobbar med en kund. Så att man kan dela det i team osv där då. Och man kan även dela med sig till kunden om kunden vill ha insikt i vilken information har vi sparad om känsliga saker och miljöer.

Augusta: Ni har inget sånt här, hur ser det ut med liksom era informationssystem och sådär? Hur, finns det något där ur ett tekniskt perspektiv som kan kanske hjälper dem anställda att arbeta säkert? Förutom det här då som du tog upp.

R3: Alltså…. Tja, alltså inga som jag kan komma på sådär jätte tydligt. Det är klart att en sak som hjälper folk att arbeta säkert är att de inte har behörighet att göra allting. Men om man kan kalla det ett mjukvarustöd.. Det är kanske att ta i. Nja inte som jag kan tänka på sådär. Nej.

Augusta: Det är helt okej. Bara en tanke. Då ska jag fråga också, på vilket sätt, du nämnde lite men hur introduceras nyanställda till informationssäkerhet?

R3: Första dagen man är anställd inleds alltid med att man träffar sin närmsta chef och bland väldigt mycket annat så går man då igenom personalhandboken steg för steg. Och man går igenom informationssäkerhetspolicyn. Så man läser den och man läser den tillsammans med sin chef som kan svara på frågor. Man får väldigt gott om tid att faktiskt läsa den ordentligt. Så introduktionen av nyanställda är ju i princip det. Och sen så sker ju ytterligare introduktion sker ju i princip stegvis i takt med att man får behörighet till vissa system. Så det blir ju mer vid behov. Men den grundläggande får man liksom de, den första förmiddagen går mycket åt det.

Augusta: Skriver man på någon typ av, när du skriver på ditt anställningsavtal och sådär är det någon typ av sekretess där eller kommer det sen?

R3: Dels så finns ju att man måste, man förbinder sig att följa vid vad tids gällande regler, policies, eller någon sån typ av form av formulering finns i själva anställningskontraktet sen till anställningskontrakten finns ju även en förbindelse om sekretess, lojalitet och så vidare. Väldigt mycket av det som står där är ju egentligen reglerat i lag men det är ju också många företag har ju typen av sekretessförbindelser och det är ju mycket för att påminna den anställda om vilka långtgående skyldigheter du har att, ja men hålla saker hemligt som du har fått veta som borde vara hemliga även om de egentligen från början är olagligt. Men det är, jag tror det är en sida med tänk på att inte sprida den här typen information och så vidare.

Johanna: Ni gjorde ju en undersökning men hur, hur medvetna om arbetet med informationssäkerhet tror ni att anställda är?

R3: Jag skulle säga att den genomsnittliga anställda här är medvetna om det, dom får ändå, nu brukar vi försöka göra lite punktinsatser eller som att vi försöker om man säger att de kanske får ett mejl i kvartalet i alla fall om att just nu gör vi en liten “ride” att, okej men, dubbelkolla att verkligen alla hårddiskar är krypterade liksom, eller dubbelkolla, eller att man påminner om hur bra lösenordet måste göras eller att, eller något i den typen saker kanske kommer en gång i kvartalet, så att på så sätt tror jag att man är ganska medveten om att vi gör ett arbete, man är nog ganska medveten om att det finns en policy sen tror jag inte att den genomsnittliga anställda har järnkoll på exakt varje detalj i den policyn. För som sagt man läser den en gång, man kanske

fräschar upp minnet någon gång då och då liksom,men det är ju inte så att man, jag förväntar mig inte att folk sitter och läser den på kvällarna hemma liksom.

Augusta: Men du sa det är med att ni skickar ut påminnelser, följs det upp på något sätt eller?

R3: Em, inte strukturerat, det beror på vad vi gör för typ av punktinsats. Vi har gjort någon gång så här men typ lite mer så här quiz liksom, och man kan ju ibland, kan man göra det i utvecklingssamtal. Vi vet ju med oss att vissa är väldigt bra på att göra, läsa sina mejl och göra det som står i mejlen vi vet också att vissa kanske inte ens läser sina mejl så himla bra, så det vet ju den närmaste av chefen ganska bra om så att ofta har man ju den typen av samtal in person då istället att man vet att den här personen är dålig på att läsa sina mejl och vet att den är dålig på att låt oss säga kryptera sin hårddisk för att den inte är så teknisk så vet ju jag också jag bara kan prata med den här personen och få det att hända istället. Men det är inget strukturerat uppföljningsområde.

Augusta: Vad händer då om man skulle som anställd göra de här grejerna? Vad blir biverkningarna då?

R3: Det beror på vilka intentioner man har med att inte göra det. Jag skulle säga att det aldrig har hänt oss att någon medvetet har inte följt det, utan det handlar ju om okunskap och så länge man ..., nu är det ju en hypotetisk diskussion men till syvende och sist är det du gör ju inte ditt jobb om du inte följer policyn, du är en risk en oacceptabel risk för företaget, för våra kunder, du hade ju fått en formell varning, du hade till slut blivit avskedad för alltså antingen det är beroende. Du hade blivit av med ditt jobb på ett eller annat sätt.

Johanna: Uppfattar ni att de anställda följer alla policies och riktlinjer och så?

R3: Ja, till deras bästa förmåga. Sen så om man skulle som göra en hård kontroll, om vi tar exemplet vem har krypterat sin hårddisk så tror ju jag kanske att en faktisk kontroll skulle kanske visa att någonstans mellan 80-90 procent gör det eller har gjort det och dom som inte har gjort det för att de har bytt dator och och glömt eller om-installerat sin dator och glömt aktivera det eller någonting så att och där är just därför om man bara påminner så tror jag alltså det är ingen som gör det av illvilja.

Augusta: Tänkte det med det här med policies och sånt. På vilket sätt kan anställda uppleva era säkerhetspolicies som begränsande?

R3: Alltså en del av vår policy är ju att du får inte använda applikationer som inte är förgodkända av mig, i princip. Och det är något som inte rimmar jätteväl med att vara mjukvaruutvecklare, mjukvaruutvecklare vill ju använda du stöter, du måste köra något program för att göra en viss specifik, fu måste alltså, det är väldigt många såna saker. Så de är ju en balans, där tror jag att man kan känna sig begränsad dom som verkligen följer den policyn ordagrant, sen så tror jag ju inte alla följer den ordagrant utan istället så handlar det om man gör en riskbedömning själv vilket i grund och botten är helt okej för att det handlar om att du får inte köra känsliga uppgifter du får inte hantera känsliga uppgifter i något som inte är godkänt, du får inte köra google docs istället för office 365 bara för att du känner för det liksom men... förlåt vad var frågan?

Augusta: Om, em, på vilket sätt kan anställda uppleva era säkerhetspolicies som begränsande?

R3 A, ja, just det, men den tror jag man kan känna sig begränsad av och jag tror att man kan känna sig begränsad genom mycket som kommer till oss genom lagkrav alltså, många saker som har med GDPR att göra kan ju kännas väldigt begränsande för då framförallt som, folk som jobbar med sälj till exempel är det ett stort frustrationsmoment för de är inte vana att arbeta på det sättet, så jag tror ju absolut att det främst är ett frustrationsmoment. Det är ju också ett nödvändigt ont. Om det att det inte varit ett frustrationsmoment hade folk inte behövt anpassa sig och hade folk inte behövt anpassa sig hade vi inte behövt ha informationssäkerhetspolicies, det handlar ju om att ha en balansgång mellan vad som är rimligt och vad som är orim, asså.

Johanna: Tror du att det på någotvis kan göra att folk inte följer policies eller är det mer att folk inser att det är ett nödvändigt ont men är lite irriterade?

R3: Det beror väl på hur osmidigt det är för dom i varje enskild situation. Jag tror att med tanke på hur många det är som kommer till mig och frågar om såna saker så skulle jag bedöma att de flestas lösning är att följa policyn genom att fråga mig kan vi godkänna den här applikationen, om vi tar det exemplet men jag tror de allra flesta följer den men muttrar lite över den.

Augusta: Mmm. Hur motiverar ni era anställda till goda säkerhetsbeteenden?

R3: Men så långt som möjligt är det ju att göra det enkelt att göra rätt. Sen så handlar det också om att skrämma upp folk med när du har saker som går fel eller när någon har andra saker som kan gå fel med hur illa det kan gå. Föreläsningen, eller undervisningen jag hade nu här timmen innan handlade om, handlade till viss del om informationssäkerhet och hur, hur det inte går att lita på DMS-post riktigt, man, att ha den typen av undervisning som visar på hur stora säkerhetsbristerna kan vara är väldigt många systemen vi använder daglig.. om man inte vet om dom om man inte motverkar dom. Så att någon forma av att göra det enkelt att göra det rätt och skrämma folk om hur illa det kan gå om det går fel, det är väl egentligen ja.

Augusta: Använder ni någon typ utav positiv, eller någon typ utav belöning om man utför detta på ett rätt sätt eller ett korrekt sätt?

R3: Vi har gjort vid enskilda tillfällen men inte strukturerat.

Augusta: Nej.

R3: Den gången vi gjorde ett quiz i höstas så var det till exempel att om man gör, om man hade mer än ex rätt eller om man svarade, nu minns jag inte exakt hur det var så där. Så var det att man fick en [företagsnamn] t-shirt liksom. Lite kulturbyggande, men, nej, inget eller, sen det är ju klart att vi har ju haft ibland att om man har lämnat in vissa grejer i tid, just såna här interna grejer så har man fått ta en extra öl när vi har haft en AW, liksom den typen av grej men inget strukturerat.

Augusta: Jag tänker lite, hur gör ni för att anställda att känna att, de är en del och det här är viktigt för mig?

Rickard: Nä men asså nä, vi gör, vi jobbar ju jättemycket med att man ska känna sig som en [företagsnamn] och att man ska vara del av den kulturen och att det är den kulturen och att i den kulturen ingår massa saker som man gör liksom men inte specifikt kopplat till informationssäkerhet.

Augusta: Det kan inte gå ihop lite om man känner en viss tillhörighet?

R3: Jo absolut.

Johanna: Ja då har vi sista frågan…

Augusta: Jaaa, vill du ta den?

Johanna: Jaa, finns det något Finns det något sätt för de anställda att bidra i arbetet med säkerhet?

R3: Ja jo men de är klart, jag har ju ingen, nu råkade de ju vara jag som höll en undervisning innan idag men det är inte så att jag kan allt och vet allt om informationssäkerhet. Vi har haft många lunch-and-learns, vi har mycket av internutbildningen består, eller på HiQ Skåne i alla fall av lunch-and-learns och det är ju upp till vem som helst att håll vilket vi försöker uppmuntra genom kulturen då att så där har varit flera tillfällen där vi haft vem som helst så att säga i organisationen som har hållt om någonting som helt och hållet handlar om säkerhet eller som åtminstone berör säkerhet som en del av ämnet. Så absolut att anställda kan vara tillgångar. Sen handlar det också om att anställda vara tillgångar kan vara tillgångar på så sätt att upptäcka saker som är fel, det, ja menar, upptäcka att vi inte följer policyn själva någonstans eller upptäcka att någonting saknas i policyn. Det är inte så att vi kan sitta på ett kontor och filosofera någon forma av ultimat dokument som kommer lösa allting.

Johanna: Men om man upptäcker något som är fel, är det dig man går till då?

R3: Det är en bra ide att gå till mig, det finns, det är nog väldigt olika från person till person, vem de känner tillit till. Visa går till sin chef, vissa går till vd:n, vissa går till mig, vissa går till sin projektledare. Det beror nog väldigt mycket på. Men vi får in en del tips, eller folk som tycker att vi borde fixa någonting, höja säkerheten någonstans och så vidare, så att det funkar i alla fall.

Johanna: Om vi tar liksom det, om ni gör något med det oftast?

R3: Asså ibland, det beror ju på, asså vi jobbar ju med utvecklare och ingenjörer liksom många gånger kan de har väldigt svartvita, svartvitt sätt att se på saker. Så även om de rent tekniskt, eller man kan ju få in ett förslag som rent tekniskt skulle höja säkerheten jättemycket men du skulle också vara helt omöjligt att få det att fungera i verkligheten. Det är klart att vi måste även om det är i grund och botten välmenat och bra förslag som sådan, så kanske inte all är genomförbart.

Johanna: Det är ju förståeligt.

Augusta: Mmm, man pratar ju mycket om det här med den mänskliga faktorn är så himla stor i säkerhet men man kan ju fråga sig hur människan kan vara en tillgång och så.

R3: Jo absolut, men ofta, det är ju nästan alltid, även om människan kan vara en tillgång så är de ju alltid det största hotet liksom att det är ju den som beter sig oberäkneligt och det är den som inte vet om saker, de är ju, den största faran är någon som tror sig veta hur någonting fungerar men som verkligheten inte har järnkoll på allting. Det är mycket bättre om man antingen har koll på det eller att man inser att man inte har koll på det, så att man går och frågar.

Augusta: Jaaa, vi har nog så mycket mer o fråga.

R3: Jaha.

Augusta: Då hinner du äta lunch.

R3: Ja visst!

Augusta: Tack så mycket.

Johanna: Ja tack så jättemycket för att du ställde upp.

R3: Absolut.

Augusta: Jättesjyst.

Appendix 6 – Transkribering organisation blå

Augusta: So, lets begin. So you are aware now that you can terminate the interview at any time?

R4: Ah, okay.

Augusta: Great. Yeah, so me and Johanna are from lunds university and we are studying the bachelors program in systems science and at the moment we are conducting our bachelor's thesis with the subject information security. Mainly discussing attitudes and motivation regarding such. So would you be able to tell us a bit about your organization?

R4: Sure, absolutely. So if we start at the top, i am not sure if you are aware but [företagsnamn] is a part of the larger [företagsnamn] group of companies. So you have [företagsnamn] as a holding company, then you have dayLeval … and Tetra Pak as the three that we call industrial groups. We have at a [företagsnamn] level, or an overall level, an audit group that handles audit and a small amount of policy and procedure. At the group level, and we then have within each industrial group different organizational structure and set-up. So, let's say, what I can show you for Tetra Pak is not necessarily applied for the IGs. But let me see here, I will share if i can. One let me get your video off that screen so I don't share it back to you, cause webex to freak out. Okay so hopefully you can see what I'm sharing.

Augusta: No, I´m sorry .

R4: Not yet?

Augusta: No. But I used to do an internship at [företagsnamn] and [name] your colleague has shown me this before. As a part of our job.

R4: Okay.

Augusta: Oh now it is happening something. Oh yeah that one.

Johanna: Yeah no we see it.

Robert: There we go. Yeah, so basically what we have for information security inside of [företagsnamn] is myself as the director of information security. Then I have a few different functions or staff reporting to me covering different areas. First we have what we call the information security incident response team. This is both a team and a process within the company and specific to handling significant events that might occur. Whether that is a potential breach of confidentiality or we had some information lost, stolen, that kind of thing could be also hardware, something of that nature as well it could be a major incident when we talk about, you know, [företagsnamn] website getting defaced or even lets say major rents and malware attack of some sort. So they would basically handle those kinds of events coming in and that's for the ISIR team. Data privacy, im sure you have heard about data privacy these days, with the general data protection rules initiated by the EU and now also being copied in minigeografies around the world. We have, what we terms as data privacy manager. Tetrapak does not store and or process a large amount of lets say consumers personal data. We really only have personal data for our internal staff. So we are not like google or facebook or someone of that size with millions and millions of people's personal information. So we didn't deem it necessary to have a data privacy officer per say, just a datamanager who basically manages the overall activities to, let's say, locate, understand the processing and secure the sensitive personal information that we do have on our internal staff and potentially consultants. Then we have [namn] on education and awareness so for education and awareness we have an overall plan for information security awareness. I can actually show it to you. But basically we do around 6 e-learning modules a year for all employees. So all employees are required to take that, and if you are a new employee you are also required to take an, I think it is four specific modules when you start with [företagsnamn], whether you are just starting as an consultant or starting as an employee. In theory you should have taken it as an intern but i don´t know of you did.

Augusta: I had to sign a confidentiality agreement.

R4: Confidentiality agreement.

Augusta: And SOA i think it was, something with security. That's about it.

R4: Yes. They may not have applied it to the interns yet but for all new employees and consultants they do have to take around four e-learning, you'd probably remembered if you had to take it.

Augusta: Yeah, we were there with school so I think they weren't as strict on us.

R4: Not as strict, probably not. Then as well the other thing we do under education and awareness, we also fish everyone at the company. So we go out and proactively attempt to fool people into clicking on the you know on the wrong thing simply to further their awareness and education so we impersonate internal systems, we impersonate external companies or systems as for example last month was DHL and a lot of staff apparently expecting a DHL package cause we had about 20% of the people clicking on the link. Which is, it is a fairly high number but we are working to improve that. I would say that industry best practice and, lets say, the leaders of this perspective those companies they have people failing fishing tests only about 5% of the time. So we have a little work to do there. And then policy and compliance of course, we have various policies and procedures within the company we have to update/maintain those …

questions on them as well as auditing to their compliance so Richard does that. Then the next three positions you see are what we call solution and service architects, so they are more technical staff that work primarily within projects but also within the security area under my self on various projects and solutions. Basically they help guide a project to design secure solutions basically. Then what we have, each one of the three, so [namn], [namn] and [namn] all focus on different areas of security. Nora is more privacy and general security, [namn] is specifically identity and privilege management so this is about segregation and duties and government of access. And then [namn] is more focusing on development security. So how to code securely. And then lastly [namn] is the service delivery manager for our security operation. So he basically has a team of analysts that sit at the secure operations center, and they are basically located all over the world. Primarily in India but also in Singapore and the US and Sweden. They operate the what we call SIM solution so security invent and management solution as well as work with the external parties, we have an external contractor that also is monitoring security events from our system. So we work as an interface to them and they find something then the software internally basically escalates it to the appropriate service team for the systems affected and works to ensure that things get addressed. Then lastly if you look at sort of the right hand side of that [namn], [namn] and [namn] are lets say technical specialists in networking clients and server. So they are basically what we call threat hunters. So they actually proactively look through the systems, look in the logs and look for indications of compromise in those systems. And then develop for the sock, lets say, what's called knowledge based articles for use cases for the SIM to look for different types of events. So right now there has been several recent issues with, lets see what is it called here, “immotet” is a specific threat, this has been out and I can share it real fast here you can see in our spread tracker we’re having various impressions of it and Leo is sharing with the team the specific hashes for the executables so that we can put those into our system and search for any potential executions of those programs to be sure we don’t have any compromises. So that is a real quick what we have for security at our back. Questions?

Augusta: Yeah, we have a few. Would you like to start, it is a bit

Johanna: Yeah, we will start with what is your experience working with security issues?

R4: So basically, I have been at Tetra-Pak for almost, i think this is 24th 25th year at Tetra-Pak. So I’ve, I started basically crawling under desks and supporting everyone with their PCs and we were macintosh bac in those days but then with the network architect I was the network manager for americas region, network architect for the company then I’ve, for quite a few years I was responsible for both our unified networking and unified communications for example the websystem we were using were one of the things that i brought in and then during that time I was responsible for networking I was also responsible for network security in the sock at that time. And then we decided about twenty fourteen twenty thirteen to move the sock to a dedicated security team. And then I moved from just networking security to general security. So networking security, you can say I’ve been dealing with that since about 98,99 and then general security since the twenty thirteenish time.

Augusta: You mentioned how you sort of worked with information security with employees so is it sort of a continuous work with security or is it something that just happens at the beginning?

R4: Yes, it is an, I mean you know it is basically a continuous process to educate and for keep people aware, cause I think even if you, let’s say we used to give people training basically when they joined and then it really wasn’t top or something you think about after the fact and over

time of course you know just like anything else sport or what not If you don't practise If you don't think about it then likely your not so good. So you know it is very much to keep in everyone's mind and to keep them thinking about these things. This is why we do regular awareness activities. Cause we want you know to keep people thinking about the security issues that are there because they are there whether it is in your personal life or at work you are facing, you know cyber threats all the time. Someone wants to you know hack your account, your money etc it doesn't matter. And you know at work, the same thing that is the primary threat we face as people attempt to steal money from us.

Augusta: Have you seen a change in people's awareness and motivation to work in secure ways since you implemented this tactic?

R4: I think the awareness i defiantly increasing and I think quite a few understand and you know, they get the idea and they understand that they need to be secure and they need to think about what they are doing at the same time of course everyone has their own objectives and their own initiatives so it is always a challenge because normally to do things securely you have to make it a little less easy. And that is always the challenge to balance being secure with being easy. Because rarely are they both. There are a lot of developers these days that look to improve that but it is still, it is always going to be a little bit of a trade off i'm afraid. It remains a challenge.

Johanna: How aware do you think the employees are in the work regarding information security?

R4: If we were to go back 5 years ago I would say not very, you know basically the you know, we've seen people posting passwords on post-it notes and stick it on their monitor, put it under their keyboard they even in our production facilities you know you see passwords post-it noted to operational consoles for some of our production factories and what not. So you know five years ago I would say it was not great. With you know the dedicated activities we've been doing the past two to three years I think the awareness is improving quite a bit so we actually check on a regular basis and I think we are do to do it later this year. Kind of a general assessment of where we stand and but the last time we did it let's say we were probably. I would say was, if we say on out of five, five being everyone is perfectly aware and one being aware of nothing I would say we are somewhere in the 3-4 range at this point as far as awareness goes.

Johanna: Do you think that the employees follow rules and guidelines?

R4: Absolutely not. Absolutely not. Unfortunately, you know, people don't intend necessarily to do things wrong or to break policy or procedure sometimes it is awareness and simply not being aware, sometimes some, you know for achieving their objectives or trying to get things done they will bend the rules if you will. I would say in general Tetra Pak has a very, let's say forgiving culture. So it is not like we, you know, er lets say, I've seen companies in the US that have things like you know 3 strikes and you are out basically. If you fail three fishes you are fired. They are that extreme, normally that kind of situation pf fishing exists where the risks are very high. So this would be military or you know something like, some of the nuclear power plant operators and these kind of things where the risks are extreme. For tetrapak the risks are not so extreme so we are not quite as severe concerning adherence to policy and procedure. But they do exist for a reason and it is there to protect everyone so again quite often it is more lack of awareness before anything else. But of course as you can imagine you know from our perspective lack of awareness, this is not necessarily a good excuse you know, Im sure if the

police catch you speeding, the fact that you didn't know the speed limit, they don't really care right?

Johanna: No.

R4: Hahaha. Unfortunately.

Augusta: You were talking a bit about people want to work against their objectives, do you there is anyway for employees to perceive company policies as limiting or restrictive?

R4: Restrictive. Limiting or restring them?

Augusat: Yes.

R4: Again, you know given that being secure often mean more work and less easy, certainly when it comes to implementing new systems, coding new applications. Quite often it is, it can be perceived as extra work and why do I have to do this extra work? So quite often you do have to do a bot of selling ,a bit of explaining, and normally once people understand the rationale for why, you know, we have a specific then there is usually not so much resistance. There might still be some grumbling but usually once people understand the why, then they, they are less difficult to adhere to it. So again, it's you know, it's about education and awareness so even for you know internal IT staff or developers you know, putting the policies and and procedures and enabling them to one understand it and then two as best as possible and as easy as possible adhere to it then things go much smoother.

Augusta: Emm, do you want to take the next question?

Johnna: Yeah, do, how do you motivate employees to good behaviours regarding information security?

R4: Hmmm, how do we motivate employees to have good behaviours. Yeah, like I said, we're not much of the, look at stick versus carrot we're not much on the stick, we're more agan on the carrot. So we, we try to you know, for example when we did the education awareness activities for the general employee population, what we tried to do is you know sell and explain how this is good for you personally and your private life as well as for us, the company. So you know there it's about trying to get peoples by end that you know participating in those trainings or really learning from those trainings and picking up the good behaviors are of benefit to you personally as well as to the company. I really think it's about you know selling the benefits you know and giving people personally bought in on you know why we as a company or you as a person you know should be paying attention to these things.

Augusta: We also wanted to ask about the human factor in information security, but is there any way for employees to become an asset or sort of work towards being a contribution for information security?

R4: Yeah, absolutely, there is it's funny cause there is the, I don't know if you are aware of SANS?

Augusta, Johanna: No

R4 So the SANS is a large education and training vendors, so actually have a classed called securing the human and again basically when you look att let's take tetra pak as an example where only as secure as our weakest link and the likely weakest link is one of the 26 000 employees because the you know the real easy way in these days, again I gave you the percentage of people that fail the DHL-phishing test so you know if you want to potentially penetrate any company not just [företagsnamn] phishing s the, is the, you know almost sure fired way they go. With a 20 percent success rate if you attack a 100 people likely you're gonna have 20 successes, so you know, that, that is what we face every day. And so you know by securing every individual we are essentially elimination those weak links in the chain because every last one of us has some part of the process of the business and the ones that are really you know heavily involved in finance, legal,etc. they are under regular attack if you will. People impersonate customers, people impersonate suppliers and both from you know we have systems to try and help mitigate some of these risks but in one of the most successful preventions is actually processed, actually the process we have in the business for example on how we can modify supplier information because the key thing that someone will try get you to do in a phishing attack is convince you that their banking details have changed so that you pay them instead of your supplier or customer and we have a very strict process around how those details can be changed and that can not in fact be changed by an email so you know making sure that every person involved in this part. Management and finance process around that is really the key to ensuring we're protected. It's not so much all of the systems we have to detect compromise you know, to protect all our systems etc those are other significant risks as well but our biggest risk that we see on the daily basis is really someone trying to steal money and it really comes down to convincing someone that you know are the customer and you need, you need to change the bank payment detail info so that, cause there is some problem with your existing bank account or something of that nature, we see it all the time.

Augusta: I can imagine.

R4: But thankfully we haven't had to many impacts ourselves but we have absolutely had customers and suppliers lose tens and hundreds of thousands of euro.

Augusta: We have one last question, so, with security there can be quite a cognitive load on employees do have any kinds of technical supports that are provide employees so that they can work in a secure way?

R4: Mmm, so we have lots of you know technical systems behind the scenes to help with things so basically one of the, there are quite a few things, of course you've got your standard anti-virus type things but we also have is another solution called "Crowd strike" that is basically watching for odd behavior on our servers and our end points so that software basically looks for anomalous behaviour that shouldn't exist as well as specific threats that the company has picked up we also have data loss prevention solution so we have another technical solution that basically is watching for, this is more watching for unfortunate malicious behaviour but it can also be a simple mistake by someone that might take sensitive information and place it where it shouldn't be. So we have some systems to watch for that as well we're right in the middle of changing it so we also have a system for helping with the phising, so I'm not sure. Let's see if I have been abided so let's see here… We have one for email, we're in the middle of changing it but let me show you so when we get link's through emails, if I hoover it will actually say original URL is that, however if I copy that hyperlink and go over here and, give me a new slide, and paste that in you can see that it's actually a different URL, basically we have from microsoft it's a basically link protection. When you click on something you're actually going

to go to this microsoft site first and that site basically checks the URL, checks the content that's being downloaded and protects you from basic malware, phishing attacks kind of things. So, we have deployed different technical solutions and we've tried to make them as , yeah invisible as possible and to keep people's lives easy but I can tell you the more technical solutions and tools you apply to the people's laptops the slower and slower they get. So have to find the balance between the technical controls and the educational ones.

Augusta: I was thinking about authentifications, when employees log in to their computers or such, do you mainly use passwords there or do you have other forms of authentifications?

R4: We are moving to, for the most part when you talk about logging on to your pc these days we have authentication via active directory from microsoft and we are moving to some of their new solutions in … cloud. We're basically, we do what is called two factor multi factor authentication, so when you're on, we can detect when you're on the internal network and when you're on the internal network we don't require additional authentication beyond the password and or a certificate so with windows you can tie your login credentials to a certificate on our badges so for all employees they have a badge that, that's a smart badge. It has a secured chip in it and you can set that card up to authenticate your machine so if you use your badge then you can use a shorter pin to get onto your machine instead of our very long 15 character password. Yes, there is a technical reason why it is 15 characters, it has to do with breaking legacy password support in windows. Cause if you don't, basically if you don't go to 25 characters your password is only 7 characters strong because when those, breaks them in to 7 character hashes. So that's why we have 15 but we are implementing, we have implemented this methodology with the certificate where you can then use the pin with the certificate. We also have in progress, deploy a new solution from microsoft called windows hello which uses facial recognition so it again ties a certificate or a virtual certificate in the TPM chips that the laptop to facial recognition software in the operating system that will also let you either by pin or your face authenticate and like you know face id does on your iphone. Now when you're outside the company so when you're not connected to corporate network then we have two things happening. One s multi factor and another one that is just getting implemented is conditional access so with the multifactor, if you're trying to access lets say office 365 from outside the company then you are required to authenticate via the authenticator app from microsoft, so that's an additional step beyond your username and password and with conditional access we are now adding as well that it has to be a, or we can lock it down to only a tetra pak issued machine can access our office 365 account. So basically it uses a combination of membership and our assure active directory along with that multi factor authentication with the microsoft app to control access to office 365. Which helps but I can actually tell you that even with that it is still possible to compromise an account because we have had someones account compromised even with multi factor access.

Augusta: Do you think that employees in someway can feel like their privacy being compromised under these kind of steps?

R4: I cannot recall a specific complaint on, when it comes to the authentication steps. Again it's more you know oh I have to go through extra steps to get onto my machine, or in on 365. Now where we have had privacy concerns, so one, again I didn't talk about this earlier. One of the technical solutions we have in place to compromise or to prevent ex… of sensitive information is from the inside you have to to access the internet, it all goes through a proxy server. You know what proxies are?

Augusta, Johanna: Yes

R4: Well they're to eliminate the threat factor of encryption and the fact that a SSL session can hide malicious software etc. we actually intercept and decrypt the SSL session so if you are browsing from the inside, certain types of encrypted sessions are basically let's say opened up and reviews for malicious threats. So there was some, some concerns issued and lots of discussion around it but the solution basically of course, because privacy is important you know it does not open up, basically known banks, health care, related topics so there's a large number of things that we don't open up and look at, but things that cannot be clearly identified or things that are uncertain, then we do open up those encrypted sessions and review what is coming through them. Because it is very easy factor to potentially deploy something malware wise and of course the hackers know that if they put it inside an encrypted SSL session that it will get by some companies radars.

Augusta: I think we have asked about everything basically.

R4: Alright!

Augusta: Thank you for lending us your time.

Johanna: Thank you so much.

Appendix 7 – Transkribering forskare lila

Augusta: So we are going to start with some introduction questions and would it be alright it we record this interview?

R5: Yes, definitely.

Augusta: Eh so, I'm Augusta and this is Johanna and we are writing a paper about information security and structure

Johanna: And yeah like views upon information security mostly. Yes, so will you tell us your name your job title?

R5: Yes, right. My name is [namn] and I work as an assistant professor [fakultet] at [universitet]. I mainly work in the information system security area as that is my expertise and my background in the education. That's it.

Johanna: Why did you choose this field of studies?

R5: Yes so in the very beginning when I started to research I was very much involved in trying to understand the effects of information literacy and logistics also in an organizational context. When I was trying to understand information literacy I was more or less focusing on how libraries actually used information literacy as a way to understand how to manage their resources which is books, information really. Physical but also digital infrastructures such as digital libraries. Then I moved on to information logistics which is a more broader area of trying

to understand more of how we deal with information. Really, how do we management of information. And that has always led to the question of security and privacy as well but overall security. That is because whenever you try to manage information you are gonna come across obstacles or challenges that will deal with security matters, and this narrows my scope even further and that is when I focused on information security in particular.

Johanna: Yeah, we will now go on to the questions regarding information security

R5: Right.

Johanna: Eh in what way is the human factor a threat to information security?

R5: Eh, At the time when digital infrastructures where pretty much in place, so after the world wide web, eh the expantion of technology
Started to become one of the leading forces of our modern life. So you started to think about security matters, cybersecurity was in place and most would think we would put the fault on to the technology per say, that there is a hole in the system itself that leads to an insecure management of your, of your platform of your software or of your information that you're storing or even your data. If we go to an even smaller scale. Then came the time when most organizations would switch a lot of their tasks into managing their daily tasks through technology. Often technology was either the sullotion or the fault when something wrong was happening such as someone would breach in and you would put the fault on technology itself. Then another side evolved pretty fast saying well we can't always blame the technology because technology is not always the sulotion. That is because we have to look at the human side which probably causes a lot of problem in terms of why do we come to the situation when security becomes a problem for the resources of an organization for instance. And this really makes me think a lot because a lot of statistics coming out from different ports intel … for instance. Talking that maybe even 40% of all the attacks that happen in the cybersphere might be unintentional done by the human factor from an organization point of view. So this is a short background I would say.

Augusta: Yes

Johanna: Do you think there is any way to eliminate the factor?

R5: From what I have read and followed along the trends it is almost impossible to eliminate the human threat. Technology can evolve and be sophisticated to a level that it can handle a lot of issues that come when it comes to information security. But the human factor is, especially from the unintentional side, can always be there. It is a very very important to think about.

Augusta: What is your opinion regarding agency versus structure in organizations?

R5: Ehm not really. Very structured organizations tend to have a more bureaucratic form of how they handle things and often when it comes to lower level operations sometimes security for an instance is .. on the side rather than drivers on the top management. That it lead to the collapse of the whole system .. Easily attacked or more vulnerable to outsiders and this is because to much structure tend to overlook into certain things, for example security. This thing that has happened along the years for many organizations, a lot of them have innovated with how the actually do security in organizations. Which they bring it up on top management nowadays. Making security as one of the key drivers of an organizations innovations. So I think

a lot of the traditional organizations are really moving towards becoming more flat. And that makes a lot of impact in how we deal with security nowadays. And how much work secure re towards organizations when they .. themselves.

Augusta: Do you think there is a way to achieve sort of like a balance between agency and structure in an organization?

R5; Very traditional organizations definatly are striving for that. They are going after that which is very important Eh the newly established start-ups, they, I think, already learned a lot about what is going on in the world and have seen or have good background not to fall into the same faults of becoming very very structured or very traditional in a way that makes it almost impossible to handle some of these side issues. So they become more flexible and more fluid in a way.

Johanna: Do you think there is a way for staff to become an asset for a company's information security?

R5: ehhh definitely there is a way, that is making sure that staff is always kept up to date with the security matters within an organizational context and that is how organizations develop security policys and also programs where they evolve particularly awareness programs so that they keep their staff up to date with how the organization handles and must handle information and delicate data in general. So yes, it is one of the greatest resources I would say. That staff should be there and up to date with how to keep up with all the trends and how …

Augusta: Is there any way for staff to sort of contribute, sort of like, I don't know. A suggestion box, something. Is there a way?

R5: Eh studies actually have been done to how, how can really employees in an organization be involved in to improve the overall atmosphere of how security is handled. So , what they, some studies have tried to do is see how they can incentivise employees to go towards better, towards better handling of security matters of an organization context. And it, the incentives will be by maybe giving rewards such as either higher salary in the next pay or for instance a praise where everybody will know how good you have reacted in a certain month. And some studied claim that if pick up some of these employees that are handling security matters much better you can take them as examples to others and maybe influence the others so one colleague sitting next the the other maybe will be influencing how important that action actually was. Because this employee handled the information very well or over daily tasks related to security … Well.

Augusta: Yes, so is there a downside to policys and restrictions regarding security?

R5: Definetly there is. That is why overall security has been seen as an isolated part of an organization and so on. Or a place where many people och many persons tradionally deal with. That is because an organization operates on the basis of moving on fast, and towards what the customer wants and what the world trends are so that we can follow up. On the other side there is security policys and restrictions that often might feel that it is restricting a certain process to be handled at a faster pace than you want. So yes it is definately seen as a barrier.

Augusta: Could It sort of affect motivation with employees?

R5: It does actually. There is … in an organization context that many employees but some are like bring your own device. This might mean that employees really apprichiate that but other companies is saying no device whatsoever can come out of our facilities inside. Now this can be an demotivator because a lot of employees often would like to work on the move and if they are very restricted on what kind of devices they can use at a certain time especially if they work with cloud services then they might feel that they are demotivated or just are very restricted in how they should operate. But of course employees should understand that there is organizations that handle very delicate processes and some of those just have to forbid some of this stuff. It has to be understandable or acceptable as opposed to an organization that is more flexible or where their priority is not to work with information per say but with their facilities and their operations. And those I think they should be a bit more flexible. If they are the opposite of that then.

Johanna: How important would you say motivation is in order to keep up a good security awareness?

R5: Ehm When I do information security and I go beyond the area itself, so I go for instance to study organizational science, management science and marketing science, you can definately see that motivation is one of the crucial aspects of keeping an organization alive. And how do you motivate employees can be from many different ends. But flexibility and fluidity of an organization that they can easily adapt to new situations but let the employees adapt to the environment easily and in an friendly way is always the way to go. If you do not keep motivation levels high, then of course you will not perform as well because you depend on those employees so.

Augusta: We were, when we did our research we were looking into how cognitive, like, what do you, like when you have to have a lot of things in your head like remembering lots of passwords. That might lead to having very simple passwords or whatever. So we were talking about, do you think there is a way for organizations to decrease the cognitive load on people in a way to sort of increase the motivation, increase the will to act more securely?

R5: Definitely, I mean there is so many solutions out there which would allow you to handle passwords. The latest technology which is quite applicable to Sweden is that you have services that you go through your, to that service through face ID for instance. So, or fingerprint like I can log in to my computer through fingerprint and I can also log in to some of my services such as even banking services through face ID. So, or fingerprint like I can log in to my computer through fingerprint and I can also log into some of my services such as even banking services through face-id and then there is solutions out there such as password managers that can handle all of your passwords, whatever they may be with a master password. So there is ways to easy us the only thing is how do organisations help employees to find these easy solutions so that they don't have to be cognitively overloaded with to many passwords that would lead them to actually go to even simpler passwords because they just can't handle it. So there really is this advanced ways on how you can handle technology today, face-id, fingerprint, password managers, so yeah it really depends on the organisation to try to help their employees with these solutions and this is how they can keep themselves more secure in fact.

Johanna: Do you think in any way that to many policies and restrictions can be a threat?

R5: Not necessarily a threat but if it is to many that can be easily overlooked than, that can turn into a threat because employees have to be aware of concise and short statements regarding

what it is required of the them to act securely and if that's a long list of 100 pages of things or just stretched out to the the point that they lose interest then they might miss out something very important that might happen as an action within 3 months after they have gone through a security policy reading or awareness training or so on so that is why awareness campaigns have come to the point to very short and concise in terms of flyers or very short clips so that the message goes through rather than long black and white papers, right. Black text and white paper just go and read and find yourself through the mass so no, this is no longer really applicable if you want to keep yourself secure.

Augusta: We were also thinking, with our upcoming interviews we are going to more companies and we were thinking. When you, as an employee start at new company almost the first thing that happens, that you have to sign a confidentiality agreement, do you think that it's wise to start with that right away when you start at a job or is that something that should happen after a while? Do you think that affects motivation?

R5: I am for signing that immediately as soon as you are in the facility of an organisation and you are a new employee. The organisation has to know that they can be protected from whatever can happen with that new employee so I don't think that would demotivate, what that might do to a new employee is rather stress them out a little bit if they would go through misconduct or something perhaps accidentally because normally you see those people as unintentionally doing something wrong from the beginning, intentions to do something wrong I think would come much later in the face of when your employed rather than in the beginning, as some of the trends show but still I am definitely for signing confidentiality agreements from the beginning that comes with the contract that you would make when you start working.

Johanna: Do you think companies should place a greater trust in their employees?

R5: Definitely, I think a lot of organisations try to do so which is not look an employee from the beginning as a threat. They serve one to open up but then they also, it matters a lot on what kind organisation we are talking about. If we are a security specialist handling a nuclear power plant, you would have to scan that employee 3 to 5 gates until until they enter a certain plant. That employee should not be seen as I don't trust you, is the general rules that apply within the policies that have been described within that context. As opposed to a more not so risky type of business, let's say the university, two differences where you don't really have to be scanned on a daily basis but where you will put something in or outside the facilities, right? So depending on where you work I think you have to kind of agree to some of these rules that might seem as you have not placed enough trust in your employees.

Augusta: Do you think that, because sometimes in different organizations and workplaces there is sort of these restrictions that are meant to help the employees to work in a secure way but are they sometimes, like affecting the motivation. Could that be seen from the employees point of view as non trusting from the employer, do you know what I mean?

R5: Hmm, this is not very easy to answer because again it depends on the context. What is the actual situation that the employee is brought to when such a behaviour happens like you feel like, I'm not trusted, and then you have to have reason for that because it depends on that context which definitely, it feels like it's normal to have happen but it has to be avoided and if the organisation is repetitive in those situations or in those contexts, the employee feels mistrusted. Then they have to do something about this because they themselves will lose credibility later

but if it happens or the context is very specific I think it should be taken as something that, yeah it could happen and I can be in that situation but you can go for it, you can overcome it.

Johanna: How do you think companies can create support for their employees regarding conducting their work in a secure way?

R5: There is always a need for a security department , an IT department but also a compliance department that's my view on how organisations should structure this area previously it used to be It and security all of the things together, compliance might or might not be there but I actually feel that these three different departments are crucial importance to most of the organisations that deal with sensitive information and that whatever the employee does an a daily basis can be not only traced but also helped through the day with certain processes if they find themselves in a difficult situation support must be there and for security is 24/7 basically.

Augusta: Is there anyway to have the different systems that you work with being a support to working in a secure way such as some kind of system support, like the ERP or such, what you work with as an employee so that they can…

R5: Definitely, so the larger the software solution or the application is or eve the platform is that a company uses where their employees do their most tasks, there must be specific specialized support for that. Because those solutions can often be very complex, can drive employees to do things to do things that maybe they shouldn't. How do you reverse an action, how do you actually make an action possible, there, the support must be there, yeah.

Augusta: Do you think that, in you opinion, do you think that it is there for most companies, or it isn't?

R5: I think it depends a lot on the type of the organisation and the type of the software that we are talking about. The ones that are the, so the daily operations depend on those software, I think that the companies definitely have the support. They at least outsource if not more if it is not in the house, but it is there to my understanding. Of course I'm talking in the sense or in the terms of organisations that are already shown success with how they reach out to their customers and how important it has become to the industry and the organisations that you don't really hear much, maybe the have internal problems that could have dealt with using it's specific solution that was not supported at all times perhaps one of the indicators of why the organisation have fallen sort of backwards but the success story it is there. You definitely see that whatever solution that drive operations in organisations is there, there is also support.

Augusta: We have our last question now. What do you think the future of information security in the workplace will look like?

R5: Hmm, I think more and more digitalised and to the point that you what to avoid every possible misconduct, intentional or unintentional but still as I said earlier to avoid everything is almost impossible because as digitalised as it can be there is a chance for you to just move away from the device that is maybe tracing you and do something harmful, harmful without being close to it, so this is the impossible mission sort of, of security trying to protect everything. But then again while we are talking about the future of security we see a lot of it coming at the expense of privacy so you're surveilled 24/7, you go to a train station, you're surveilled there 24/7. You go to your workplace, you might also surveilled 24/7 not just from the cameras, from every action you take while you're doing something in your computer, similarly it goes from,

for the mobile phone usage for instance. You might be surveilled just as well there and too everywhere, so what happens then? This is maybe how you can see that we can lower non-wanted activities in terms of security. But can we really forbid everything or clear of everything that comes to insecurity? We'll probably not be able to do so and as more digital we go this were the cyber world will develop as well, or cyber crime will increase too. So then you have to protect more from the outsiders, so you have to develop new technologies and not just focus on how to handle the insiders, and of curse organisations do tackle both, sometimes they forget about the insiders because they are more obsessed with the outsiders but in the end I think insiders or outsiders they'll all be a threat even with the future of security, because these, at least the outsider-threat evolves even faster than the actual security that we want. The insiders, yeah, I think we can develop more technology to benefit the organisations so they can reduce the number of unintentional threats but that will not go to zero as I understand it from this point in time.

Johanna: Yes.

Augusta: Do we have anything else?

Johanna: No… We really want to thank you.

R5: Great!

Augusta: Thank you so much!

R5: That's half an hour.

Referenser

Adams, A. and Sasse, M. A. (1999) 'Users Are Not the Enemy', *Communications of the ACM*, 42(12), pp. 40–46. doi: 10.1145/322796.322806. Tillgänglig online: http://eds.b.ebscohost.com/eds/detail/detail?vid=2&sid=d6aadd72-382a-449c-a6d5-422a24fdd060%40pdc-v-sessmgr05&bdata=JnNpdGU9ZWRzLWxpmUmc2NvcGU9c2l0ZQ%3d%3d#db=bth&AN=11872117 [Hämtad 2019-04-05]

Aldawood, H., Skinner, G. (2018). Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review' (2018) *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE), Teaching, Assessment, and Learning for Engineering (TALE), 2018 IEEE International Conference on*, p. 62. doi: 10.1109/TALE.2018.8615162. Tillgänglig online: https://ieeexplore.ieee.org/document/8615162?arnumber=8615162&SID=EBSCO:edseee [Hämtad 2019-03-25]

Alotaibi, M., Furnell, S., Clarke, N (2016) Information security policies: A review of challenges and influencing factors' 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), Internet Technology and Secured Transactions (ICITST), 2016 11th International Conference for, p. 352. doi: 10.1109/ICITST.2016.7856729. Available online: http://eds.b.ebscohost.com.ludwig.lub.lu.se/eds/detail/detail?vid=3&sid=13a03b10-5ae1-45df-a0fc-d1ede77796f5%40sdc-v-sessmgr06&bdata=JnNpdGU9ZWRzLWxpdmUmc2NvcGU9c2l0ZQ%3d%3d#AN=edseee.7856729&db=edseee [Hämtad 2019-03-25]

Tsui, A., Pearce, J.L., Porter, L.W., Tripoli, A.M. (1997) 'Alternative Approaches to the Employee-Organization Relationship: Does Investment in Employees Pay off?', *The Academy of Management Journal*, 40(5), p. 1089. Available at: http://ludwig.lub.lu.se/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsjsr&AN=edsjsr.256928&site=eds-live&scope=site [Hämtad: 2019-04-04].

Bergel, H (2017) Equifax and the Latest Round of Identity Theft Roulette' *Computer*, (12), p. 72. doi: 10.1109/MC.2017.4451227. Tillgänglig online: https://ieeexplore.ieee.org/abstract/document/8220474 [Hämtad 2019-03-25]

Benyon, D. (2014). Designing interactive systems. 3rd ed. Pearson Education limited.

Bowen, B.M., Devarajan, R., Stolfo, S. (2011) Measuring the human factor of cyber security, 2011 IEEE International Conference on Technologies for Homeland Security (HST), Technologies for Homeland Security (HST), 2011 IEEE International Conference on, p. 230. doi: 10.1109/THS.2011.6107876. Tillgänglig online: http://ludwig.lub.lu.se/login?url=http://search.ebscohost.com.ludwig.lub.lu.se/login.aspx?direct=true&db=edseee&AN=edseee.6107876&site=eds-live&scope=site [Hämtad 2019-03-25]

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010) 'Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness', *MIS Quarterly*, 34(3), pp. 523-A7. doi: 10.2307/25750690. Tillgänglig online: http://eds.b.ebscohost.com/eds/detail/detail?vid=12&sid=c52c75f2-e72b-4b53-9c93-

3193462dd769%40sessionmgr120&bdata=JnNpdGU9ZWRzLWxpdmUmc2NvcGU9c2l0ZQ%3d%3d#AN=52546353&db=bth Hämtad [2019-05-09]
Cambridge Dictionary (2019) Compliance. Tillgänglig online: https://dictionary.cambridge.org/dictionary/english/compliance [Hämtad: 2019-05-21]
Cambridge Dictionary (2019) Policy. Tillgänglig online: https://dictionary.cambridge.org/dictionary/english/policy [Hämtad: 2019-05-21]
Chen, X., Chen, L., Wu, D. (2018) 'Factors That Influence Employees' Security Policy Compliance: An Awareness-Motivation-Capability Perspective', *Journal of Computer Information Systems*, 58(4), pp. 312–324. doi: 10.1080/08874417.2016.1258679 Available online http://eds.b.ebscohost.com/eds/detail/detail?vid=2&sid=c52c75f2-e72b-4b53-9c93-3193462dd769%40sessionmgr120&bdata=JnNpdGU9ZWRzLWxpdmUmc2NvcGU9c2l0ZQ%3d%3d#AN=edselc.2-52.0-85041557196&db=edselc [Hämtad 2019-05-09]
Colquitt, J.A., Lepine, J.A., Wessen, M.J. (2011). Organizational Behavior: Improving Performance and Commitment in the Workplace. 2nd ed. McGraw-Hill/Irwin.
Dataskyddsinspektionen (2019). Informationssäkerhet. Tillgänglig online: https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/informationssakerhet/ [Hämtad 2019-05-21]
Eminağaoğlu, M., Uçar, E. and Eren, Ş. (2009) 'The positive outcomes of information security awareness training in companies – A case study', *Information Security Technical Report*, 14(4), pp. 223–229. doi: 10.1016/j.istr.2010.05.002. Tillgänglig online: http://ludwig.lub.lu.se/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=53573518&site=eds-live&scope=site [Hämtad 2019-05-12]
Farr, R. M. (1977) 'On the nature of attributional artifacts in qualitative research: Herzberg's two-factor theory of work motivation', *Journal of Occupational Psychology*, 50(1), pp. 3–14. doi: 10.1111/j.2044-8325.1977.tb00353.x. Tillgänglig online: http://ludwig.lub.lu.se/login?url=http://search.ebscohost.com.ludwig.lub.lu.se/login.aspx?direct=true&db=edselc&AN=edselc.2-52.0-84945795858&site=eds-live&scope=site [Hämtad 2019-05-17]
Ghafir, I., Alhejailan, A., Hammoudeh, M,. Prenosil, V. (2016) Social Engineering Attack Strategies and Defence Approaches' 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Future Internet of Things and Cloud (FiCloud), 2016 IEEE 4th International Conference on, ficloud, p. 145. doi: 10.1109/FiCloud.2016.28. Tillgänglig online: http://ludwig.lub.lu.se/login?url=http://search.ebscohost.com.ludwig.lub.lu.se/login.aspx?direct=true&db=edseee&AN=edseee.7575856&site=eds-live&scope=site [Hämtad 2019-05-12]
Gollmann, D. (2011). Computer security. 3rd ed. West Sussex: John Wiley & Sons.
Habib, N., Awan, S. H. and Sahibzada, S. A. (2017) 'Is Herzberg's Two Factor Theory Valid in the Context of Performance Management System? A Study of Private Banks of Pakistan', *Journal of Managerial Sciences*, 11, pp. 183–198. Tillgänglig online:: http://search.ebscohost.com.ludwig.lub.lu.se/login.aspx?direct=true&db=bth&AN=130384028&site=eds-live&scope=site [Hämtad: 2019-05-17].
Hadnagy, C. (2011). Social Engineering: The Art of Human Hacking. Wiley Publishing, Inc
Haga, W. J., & Zviran, M. (1991). Question-and-answer passwords: An empirical evaluation. *Information Systems*, 16(3), 335–343. Tillgänglig online: https://doi-org.ludwig.lub.lu.se/10.1016/0306-4379(91)90005-T [Hämtad 2019-05-17]
Herath, T. and Rao, H. R. (2009) 'Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness', *Decision*

Support Systems, 47, pp. 154–165. doi: 10.1016/j.dss.2009.02.005. Tillgänglig online: https://www.sciencedirect.com/science/article/pii/S0167923609000530?via%3Dihub [Hämtad 2019-04-04]

Hur, Y. (2018) 'Testing Herzberg's Two-Factor Theory of Motivation in the Public Sector: Is it Applicable to Public Managers?', *Public Organization Review*, 18(3), pp. 329–343. doi: 10.1007/s11115-017-0379-1. Tillgänglig online: http://eds.b.ebscohost.com.ludwig.lub.lu.se/eds/detail/detail?vid=0&sid=ffe7832f-45f1-4c93-89a1-37dff35385fb%40pdc-v-sessmgr01&bdata=JnNpdGU9ZWRzLWxpdmUmc2NvcGU9c2l0ZQ%3d%3d#AN=130897273&db=bth [Hämtad 2019-05-17]

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

Jenkins, J., Durcikova, A., Burns, M. (2011). Get a Cue on IS Security Training: Explaining the Difference between how Security Cues and Security Arguments Improve Secure Behavior. *ICIS 2011 Proceedings*. 8. Tillgänglig online: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1084&context=icis2011 [Hämtad 2019-04-05]

Kajtazi, M. Bulgurcu, B. (2013) 'Escalation of commitment as an antecedent to noncompliance with information security policy', *Information and Computer Security*, 26(2), pp. 171–193. doi: DOI: 10.1108/ICS-09-2017-0066. Tillgänglig online: https://pdfs.semanticscholar.org/ae44/4a1eaa6fbd30d19372c3036c8da1547265c6.pdf [Hämtad: 2019-04-05]

Karolinska Institutet (2019). Informationssäkerhet. Available online: *https://ki.se/medarbetare/informationssakerhet* [Hämtad 2019-05-21]

Lee SM, Lee S, Yoo S. An integrative model of computer abuse based on social control and general deterrence theories. *Inf Manage*. 2004;41(6):707–718. Tillgänglig online: https://www.sciencedirect.com/science/article/pii/S0378720603001204 [Hämtad 2019-05-09]

Lee, H.-W. (2019) 'Moderators of the Motivational Effects of Performance Management: A Comprehensive Exploration Based on Expectancy Theory', *Public Personnel Management*, 48(1), pp. 27–55. doi: 10.1177/0091026018783003. Tillgänglig online:http://eds.b.ebscohost.com/eds/detail/detail?vid=0&sid=78652083-8b16-4946-9420-59e596d5485b%40sessionmgr103&bdata=JnNpdGU9ZWRzLWxpdmUmc2NvcGU9c2l0ZQ%3d%3d#AN=134629612&db=ccm [Hämtad 2019-05-09]

LeVeque, V. (2006). Information Security – A Strategic Approach. Hoboken, N.J: John Wiley & Sons.

Madnick, S., Nourian, A. (2018). 'A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet' *IEEE Transactions on Dependable and Secure Computing, Dependable and Secure Computing, IEEE Transactions on, IEEE Trans. Dependable and Secure Comput*, (1), p. 2. doi: 10.1109/TDSC.2015.2509994. Tillgänglig online: https://ieeexplore.ieee.org/abstract/document/7360168 [Hämtad 2019-03-25]

Nationalencyklopedin (2019) Policy. Tillgänglig online: https://www.ne.se/uppslagsverk/ordbok/svensk/policy [Hämtad 2019-05-21]

Oates, B.J. (2006). Researching Information Systems and Computing. SAGE publications Ltd

Pahnila, S., Siponen, M and Mahmood, M. A. (2010) 'Compliance with Information Security Policies: An Empirical Investigation', *COMPUTER*, 43(2), pp. 64–71. Tillgänglig online:

http://search.ebscohost.com/login.aspx?direct=true&db=edswsc&AN=000274858800013&site=eds-live&scope=site [Hämtad: 2019-05-13].

Puhakainen, P. and Siponen, M (2010) 'Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study', *MIS Quarterly*, 34(4), p. 757. Tillgänglig online: http://search.ebscohost.com/login.aspx?direct=true&db=edsjsr&AN=edsjsr.25750704&site=eds-live&scope=site [Hämtad 2019-04-05]

Petty, R.E. & Cacioppo, J.T. 1981. Attitudes and Persuasion: Classic and Contemporary Approaches. Dubuque, IA: Westview Press.

Riksdagen (2019). Granskning av Transportstyrelsens upphandling av it-drift. Tillgänglig online:: https://data.riksdagen.se/fil/FB3C8AF9-BE36-4E7F-A09B-80D12887C189 [Hämtad 2019-05-21].

Rouse, M. (2014). Tillgänglig online:: https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA [Hämtad 2019-04-01]

Siponen, M. (2000) "A conceptual foundation for organizational information security awareness", *Information Management & Computer Security*, Vol. 8 Issue: 1, s.31-41. [Hämtad: 2019-05-13]

Stempel, J (2018). *Victims of Yahoo data breach can sue in the United States*. CIO. Available online: https://www.cio.com.au/article/634590/victims-yahoo-data-breach-can-sue-united-states/ [Hämtad 2019-03-25]

Stewart, G. and Lacey, D. (2012). Death by a thousand facts: Criticising the technocratic approach to information security awareness, *Information Management & Computer Security*, 20(1), pp. 29–38. doi: .DOI: 10.1108/09685221211219182. Tillgänglig online:https://www.emeraldinsight.com/doi/pdfplus/10.1108/09685221211219182 [Hämtad 2019-04-05]

Thomson, M.E., von Solms, R. (1998) 'Information security awareness: educating your users effectively', *Information Management & Computer Security*, (4), p. 167. doi: 10.1108/09685229810227649. Tillgänglig online: https://www.emeraldinsight.com/doi/full/10.1108/09685229810227649 [Hämtad 2019-04-04]

Tsui, A., Pearce, J., Porter, L., & Tripoli, A. (1997). Alternative Approaches to the Employee-Organization Relationship: Does Investment in Employees Pay off? *The Academy of Management Journal*, *40*(5), 1089-1121. Tillgänglig online: http://www.jstor.org/stable/256928 [Hämtad 2019-05-21]

Trautman, L. J. and Ormerod, P. C. (2016) 'Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach', *American University Law Review*, (Issue 5), p. 1231. Tillgänglig online:: http://search.ebscohost.com.ludwig.lub.lu.se/login.aspx?direct=true&db=edshol&AN=edshol.hein.journals.aulr66.38&site=eds-live&scope=site [Hämtad: 2019-04-22].

Upphandlingsmyndigheten (2019) Små och medelstora företag. Tillgänglig online:: https://www.upphandlingsmyndigheten.se/leverantor/SME/ [Hämtad: 2019-05-22]

Whitman, M,. Mattord, H. (2008) Principles of information security. CENGAGE Learning Custom Publishing.