Örebro Universitet
Handelshögskolan
Informatik C – Uppsatsarbete 15HP
Handledare: Andreas Ask
Examinator: Annika Andersson
HT16 – 2017-01-04

Säkerhet & Människan

Hur olika faktorer påverkar säkerhet och medvetenhet inom verksamheter

Andreas Andersson 900417
Erik Håkansson 880719
Martin Ström 910101

Sammanfattning

Många verksamheter som jobbar med sekretessbelagd information använder IT som ett stöd i någon utsträckning. Därför finns det ett behov av IT- och informationssäkerhet. Den här rapporten ämnar se över vilka faktorer inom verksamheter som inverkar på hur väl IT- och informationssäkerhet mottas och efterlevs av de anställda. Huvudfrågan för studien lyder *Vilka faktorer påverkar informations- och IT-säkerhet inom verksamheter?* För att besvara denna fråga har vi undersökt litteratur kring ämnet IT- och informationssäkerhetsefterlevnad inom verksamheter samt utfört intervjuer på olika företag för att höra hur de säkerhetsansvariga jobbar, och hur medvetenheten bland de anställda såg ut. Intervjuerna har baserats på faktorer som litteraturen tagit upp. Det vi har kommit fram till med studien är att säkerhetsefterlevnad inte är något som kan existera utan ett mångsidigt säkerhetsarbete, där flertalet faktorer beaktas.

Nyckelord:

”The human factor”, communication, compliance, human error, security practices, information security, IT Security

Innehållsförteckning

Förord

Vi är tre studenter från Örebro Universitet som skrivit våran C-uppsats inom det systemvetenskapliga programmet. Vi vill tacka de respondenter som ställt upp för våra intervjuer samt våran handledare Andreas Ask. Slutligen vill vi tacka Ella Kolkowska, vars inblick i forskningsområdet gav oss en bra utgångspunkt när vi inledde detta arbete.

Undertecknat av Andreas Andersson, Erik Håkansson och Martin Ström, 5/1 - 2016

1. Inledning

1.1 Centrala begrepp

Informationssäkerhet – De åtgärder som vidtas för att hindra att information läcker ut, förvanskas eller förstörs och för att informationen ska vara tillgänglig när den behövs. För en organisation kan det handla om att skydda information mot en uppsättning hot för att säkerställa verksamhetens kontinuitet ~ Wikipedia, informationssäkerhet

IT-säkerhet – Ansvarar för att skydda en organisations (företags, myndighets, etc.) värdefulla tillgångar som information, hårdvara och mjukvara. IT-säkerhet ingår som en beståndsdel i det totala säkerhetsramverket och liksom det totala ramverket skall hantera skydd mot allehanda hot och faror mot organisationen och dess verksamhet. ~ Wikipedia, IT-säkerhet

Kommunikation – De metoder och kanaler som verksamheten nyttjar för att förmedla information, exempelvis mailkontakt, verbala samtal, intranät, etc.

Säkerhetsansvarig – De anställda inom verksamheten vars primära arbetsområde är att designa säkerhetspolicys och förebygga informationssäkerheten inom verksamheten.

Säkerhetskultur – Nivån av säkerhetsmedvetenhet inom en verksamhet/på en arbetsplats. Säkerhetskultur kan sammanfattas som att säkerhet är en faktor som genomsyrar och beaktas i samtliga processer (beslut, riktlinjer, etc.) inom verksamheten.

Social engineering – Social manipulation (social engineering) är inom IT-säkerhet metoder för att manipulera personer till att utföra handlingar eller avslöja konfidentiell information, snarare än att göra inbrott eller använda sig av tekniska Crackningstekniker. ~ Wikipedia, Social manipulation

Vanlig arbetare/anställd – Person som jobbar inom verksamheten men inte med säkerhetsfrågor, men i någon utsträckning hanterar sekretesskyddad information i sitt arbete.

1.2 Bakgrund

Flertalet aspekter utav mänsklig interaktion med ett system eller en verksamhet är potentiella säkerhetsrisker (Tripwire, 2013); det kan vara strikt tekniska aspekter såsom svaga lösenord eller dålig hantering utav dem eller bristande följsamhet till rådande (om existerande) säkerhetspolicys, till mer mänskliga aspekter såsom social engineering eller att datorer/fickminnen med känsliga data tappas bort eller lämnas framme. Enligt rapporten *The Human Factor 2016* (Proofpoint, 2016) så fanns det under 2015 en tydlig trend som tydde på att attacker riktade mot IT främst utnyttjade den mänskliga svagheten. Detta rörde sig om allt från omfattande mailutskick innehållande skadlig mjukvara till så kallad ”social engineering”. En rapport utförd av CompTIA (2015) går vidare in på detta, och går in på säkerhetsproblematiken kring ”the internet of things”. Kortfattat säger de att flertalet enheter designas för att kopplas upp till IT-system, men saknar säkerhetsdesignen som ett IT-system ofta utgör. Rapporten innefattar en studie som visar att ca hälften av de intervjuade företagen anser att denna utökade sammanlänkning mellan enheter (i form av bl. a. molntjänster och diverse mobila appar) skapar ett IT-landskap med allt mer svårhanterliga säkerhetsaspekter.

Computer weeklys artikel *The human factor is key to good security* (2007) bekräftar mycket av vad som sägs angående den mänskliga faktorn, och belyser också problematiken ytterligare, då de säger att det traditionellt faller på informationsteknikerna att behandla de frågor som rör informationssäkerhet, men att problem då uppstår eftersom de sällan har den mänskliga faktorn i åtanke i sitt arbete. Ej heller kan de kontrollera den. Samtidigt hävdas det i artikeln att IT-säkerheten är förbisedd utav de som jobbar med de mänskliga faktorerna, just på grund utav att det är en ”IT-fråga”. Computer Weekly argumenterar för att en förståelse utav de mänskliga faktorerna måste ingå i ett proaktivt säkerhetsarbete. Detta stärks av bland annat av Inside Sources (2015) och Matthews (2015). *The Human Factor Report 2016* (Proofpoint, 2016) berör olika tekniska aspekter en verksamhet/organisation kan tillse för att öka sin säkerhet (email-filter, patcha bort säkerhetssvagheter i system som används, etc.), men också sociala aspekter som att hålla utkik efter bedragarkonton på Facebook-konton affilierade till organisationen eller verksamheten. Många verkar överens om att det rör sig om ett glapp mellan medvetenhet och handling; att veta vad som är säkert och inte är inte en garanti på att sund säkerhetssed kommer att efterlevas. Detta stärks av bland annat Vance (2010) och Karjlalainen (2011), som båda hävdar att dålig efterlevnad av säkerhetsbestämmelser är ett stort problem. Vi tänker således undersöka hur verksamheter i praktiken jobbar med att främja medvetenheten, vilka faktorer som inverkar samt hur de jobbar för att säkerställa sund efterlevnad.

1.3 Syfte

Under den preliminära undersökningen utav ämnesområdet så sökte vi primärt efter litteratur relevant för vad vi tänkt undersöka. Som ett komplement till detta så talade vi med Ella Kolkowska (forskare inom sociala och organisatoriska aspekter inom informationssäkerhet på Örebro Universitet) för att få en inblick i vilka eventuella kunskapsluckor som finns inom området. Genom dessa samtal i kombination med våran förberedande litteratursökning så kunde vi fastställa att en förbisedd aspekt är just relationen mellan de som formar säkerheten inom verksamheten samt de som ska jobba i enlighet med den. Därför vill vi undersöka vilka faktorer som påverkar hur informationssäkerhet tillämpas praktiskt.

Som fastställt i tidigare avsnitt är det ganska tydligt att den mänskliga aspekten är en relevant del i ett proaktivt säkerhetsarbete. Mycket utav den tidigare forskningen har dock nyttjat ett kvantitativt angreppssätt och fokuserat på faktorer kring efterlevnad av säkerhetsregler. Skillnaden i hur de anställda, i vardagligt arbete, ser på efterlevande av säkerhetsregler och policys jämfört med de som jobbar med att skapa och upprätthålla dessa har dock inte studerats i samma utsträckning. Studien ska bland annat undersöka om det finns ett samband mellan hur policys kring informationssäkerhet kommuniceras med de anställda och hur väl de efterlevs. Studiens syfte är således att skapa en djupare förståelse för relationen mellan IT-ansvariga och anställda och dess implikationer på säkerhetsarbete, och genom detta skapa kunskap om hur verksamheter kan agera för att gynna informationssäkerhetstillämpning.

1.4 Frågeställning

Huvudfrågan för studien lyder:

Vilka faktorer påverkar informations- och IT-säkerhet inom verksamheter?

1.5 Problematisering utav frågeställning

Intresset i studien är att undersöka säkerhetspolicys tänkta effekt kontra deras mottagande i praktiken, samt resonemangen kring deras praktiska roll. Medvetenheten kring dessa är också utav relevans, då det rimligtvis inte går att följa regler/policys en inte är medveten om. Tanken är att skapa en förståelse för problematiken kring hur säkerhetspolicys formas och appliceras jämfört med hur de mottas och efterlevs. Studien skall också undersöka om kommunikationen mellan dessa två arbetsgrupper påverkar medvetenheten och tendenser till god säkerhetssed. Detta för att fastställa om detta kan vara en bidragande faktor till efterlevande utav säkerhetspolicys.

1.6 Avgränsning

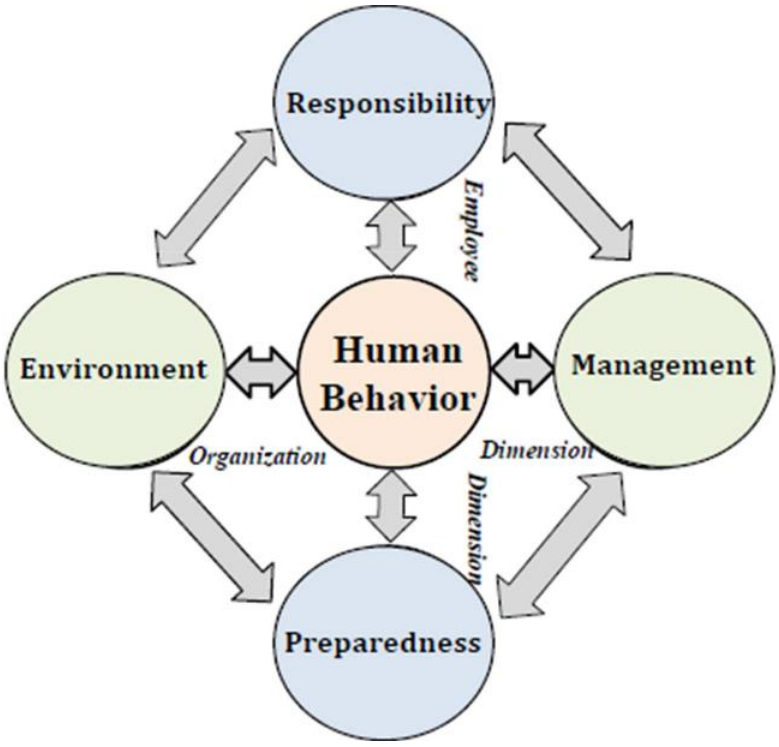
Vi har avgränsat oss till verksamheter som arbetar med sekretessbelagd information och har ett aktivt säkerhetsarbete. Detta på grund utav att vi vill kunna undersöka detta säkerhetsarbete och dess representation och mottagande inom verksamheten i vardagligt arbete.

1.7 Intressenter

Studien kan bidra till kunskapsutveckling inom undervisningen utav informationssäkerhet samt skapa en tydligare insyn i den praktiska problematik som ämnet berör. Företag/verksamheter såväl som privatpersoner kan gynnas av studieresultatet. Studien kan bidra till en ökad förståelse för svårigheterna och riskerna med säkerhetstillämpning och således hjälpa till att förebygga problematiken som kan uppstå. Vi har valt att göra en kvalitativ studie på grund utav att den mesta litteraturen och de flesta studier jobbat kvantitativt via enkäter, men få har utforskat relationen mellan säkerhetsansvarigas uppfattning av säkerhet och anställdas praktiska tillämpning via kvalitativ studie.

2. Teoretiskt ramverk

Vi ska här presentera den forskning och de ramverk som tagits fram i studier om ämnet IT/informationssäkerhet som visat sig relevanta för våran frågeställning. För att kunna basera våran undersökning i tidigare forskning samt få en inblick i vad som kan vara intressant att efterforska. Vi har genom våran litteraturstudie hittat ett omfattande ramverk, skapat utav Alhogail, Mirza, Bakry (2015). Detta ramverk behandlar olika aspekter utav den mänskliga faktorn inom informations- och IT-säkerhet. Dessa aspekter är *responsibility, management, environment, preparedness* och *human behavior* (se modell nedan). Dessa delas följaktligen in i två dimensioner, ”the organisation dimension” (verksamheten) och ”the employee dimension” (de anställda). Vi skall här redogöra för vårat användande av detta ramverk; vilka delar vi finner relevanta samt hur vi tolkar dessa aspekter för att skapa ett eget perspektiv att basera våran studie på. Då den är väldigt bred för att kunna appliceras på olika delar utav problematiken kring ämnet, har vi valt att smalna av den till de faktorer som vi bedömt ingå i våran forskningsfråga. Ramverket har kompletterats med övrig forskning inom ämnet för att ge en bredare kunskapsgrund. Våran intervju är konstruerad efter tanken att kunna inhämta data som kan ge oss en möjlighet att analysera dessa faktorer och således besvara våran frågeställning.



The Human Factor Diamond (HFD) - Alhogail, Mirza, Bakry (2015)

2.1 The Organisation Dimension / Verksamheten

2.1.1 The Environment Domain

2.1.1.1 Kultur / Arbetsmiljö

Forskning påvisar att verksamhetens så kallade ”kultur” har en markant inverkan på efterlevnad gällande informationssäkerhet. Detta skrivs om utav Beautement et al (2008) och Lim (2009), och är också en utav de centrala delarna i HFD-ramverket. Kultur i detta avseende kan sammanfattas som respektive verksamhets arbetssätt påverkar arbetsmiljön. Genom studien kommer vi hänvisa till denna aspekt som just *arbetsmiljö* för att tydliggöra begreppets innebörd enligt våran tolkning. Metalidou et al (2014), skriver att verksamheter bör jobba för att främja och bibehålla en kultur som uppmuntrar bra säkerhetsbeteende. Beautement et al (2008) bekräftar detta och tillägger att ju mer säkerhetsmedveten en verksamhet är, desto mindre sannolikhet är det att någon skulle riskera att ”stöta sig” med sina kollegor, då viljan att passa in i verksamhetskulturen motverkar detta.

”Real security culture lies in the security related beliefs, values, which manifest in employee's actions and behaviours towards information security problems” ~ Lim (2009)

2.1.2 The Management Domain

2.1.2.1 Kommunikation

Alhogail, Mirza, Bakry (2015) anser att kommunikation inom säkerhetsfrågor i en verksamhet är av stor vikt. Vidare anser de också att de ansvariga (”management”) måste jobba för att inkludera de anställda för att någon ändring i deras beteende överhuvudtaget skall kunna ske. Inkluderingen och stärkandet av de anställdas roll i frågor om informationssäkerhet kommer enligt dem bidra till en minskad riskfaktor. Detta stärks till viss del av Beautement och Wonham (2008), som säger att främja de anställdas medvetenhet kring säkerhetsfrågor skapar en tydligare bild av fördelarna med god säkerhetssed. Båda påvisar således att kommunikation är en viktig aspekt i ett proaktivt säkerhetsarbete.

”To change the behaviors and attitudes of employees, managers must clearly communicate with the employees in order to make them feel that they are part of the change and that change will affect them.” ~ Alhogail, Mirza, Bakry (2015)

Den kommunikativa aspekten av informationssäkerhet står i relation till de ansvarigas attityd kring säkerhetsfrågor. Alhogail, Mirza, Bakry (2015) skriver att det finns ett samband mellan hur de ansvariga bemöter frågor gällande ämnet, då det kommer påverka de som jobbar under dem. För att skapa en bättre säkerhetsefterlevnad är det viktigt att verksamhetens ledning tydligt visar att informationssäkerhet är en prioritet. De tar upp ett exempel som visar på att i en organisation där säkerhetspolicyn varit undermålig och dåligt kommunicerad, hade det resulterat i att 93% av säkerhetsincidenterna var mänskligt orsakade, medan i en organisation där de var välförstådda var samma siffra bara 47%. De säger dock följaktligen att en policy som inte implementeras och underhålls ordentligt är likvärdigt med att inte ha någon policy överhuvudtaget. Detta är tydliga exempel på hur de ansvariga/ledningen spelar en stor roll i detta.

2.2 The Employee Dimension / De anställda

2.2.1 The Preparedness Domain

2.2.1.1 Medvetenhet & Träning

Det genomgående temat vi identifierat i de studier vi undersökt är vikten av medvetenhet. Ett proaktivt säkerhetsarbete kan inte ske om medvetenheten kring riskfaktorer och säkerhetsrisker inte kommuniceras. Så vitt vi ser det kan denna kommunikation kan ske på flertalet sätt; det kan vara allt från utbildningar till föreskrifter, men även muntligt via kollegor, ansvariga samt via kulturen inom verksamheten. Lacey (2009) hävdar att i säkerhetsarbete så är *samtliga* inblandade i verksamheten relevanta, allt ifrån kunder till högste chefen. Stanton et al. (2006) anser att en liten insats för att främja medvetenhet kan medföra omfattande positiv verkan både för individ och (följaktligen) verksamhet. Utifrån detta kan vi sammanfatta att medvetenhet är en central del inom forskningsområdet och således en faktor värd att belysa.

Kontinuerliga träningsinsatser hjälper anställda att förstå och upprätthålla säkerhetsmedvetenhet. (Alhogail, Mirza, Bakry 2015). Träningsprogram bör innehålla både tekniska lösningar och mer praktiska inslag som kunskap kring säker datoranvändning.

2.2.2 The Responsibility Domain

2.2.2.1 Ansvar

Alhogail, Mirza, Bakry (2015) skriver att en individs förmåga till ansvarstagande påverkas av flertalet faktorer, bland annat kunskap om säkerhet, praktiska svårigheter att efterleva säkerhetsbestämmelser, individuella uppfattningar och värderingar. För att ha en god efterlevnad är det enligt dem också viktigt att främja känslan av personligt ansvar inom säkerhetsfrågor. Beautement et al (2008) säger angående detta att en individ bara kommer applicera säkerhetstänk till en viss utsträckning. Detta kan hämmas baserat på individens individuella uppfattning om nyttan i applicerande av säkerhetstänk, men också utav praktiska svårigheter. Detta bekräftar således mycket av det som Alhogail, Mirza, Bakry (2015) skriver.

3. Metod

3.1 Bakgrund till metodval och planerat utförande

Studien kommer använda sig utav en kvalitativ metod via semistrukturerade intervjuer. Tanken med detta är att genom samtal med säkerhetsansvariga samt vanliga arbetare få insyn i deras arbete och säkerhetsmedvetenhet genom de frågor vi ställer i intervjun. Frågorna har formats för att ge underlag till de faktorer som vår litteraturstudie tagit upp angående vad som påverkar informationssäkerheten. (Se bilaga) Anledningen till att en kvalitativ studie i form utav intervjuer valts är dels för att det ger en inblick i den faktiska verksamheten, men också för att det ger potential till att låta respondenten vidareutveckla sina svar. Detta öppnar upp för aspekter som inte tidigare tänkts på samt ger oss en bredare kunskapsgrund att stå på. Enligt Oates (2006) är en fördel med semistrukturerade intervjuer att respondenten kan gå in i mer detalj på frågor hen dömer som relevanta för intervjuns tema, samt att en kan tillägga ytterligare frågor angående vad som sägs i intervjun. Under intervjuerna har vi utgått från våran mall men formuleringen på frågorna har under intervjuernas gång i viss mån ändrats för att passa det individuella samtalet.

Kombinationen utav litteraturstudie och kvalitativ studie resulterar i att vi skapar en bas för vad god säkerhetssed är som kan användas som referens och kunskapsgrund samt försäkra att intervjun går att relatera till det teoretiska ramverket. Ett alternativt angreppssätt vore en enkätundersökning men vi anser inte att detta skulle skapa den djupare insyn vi är ute efter, då våran forskningsfråga söker efter att besvara frågan ur ett mer personligt perspektiv. Det valda intervjuformatet möjliggör också undersökning utav känslomässiga eller anekdotartade aspekter, något som hade missats i exempelvis en enkät. (Oates, 2006) Det hade heller inte gett oss möjligheten att få svar på ”de frågor som inte ställs”, det vill säga svar som innefattar områden som inte specifikt tas upp i intervjun.

3.2 Tillvägagångssätt för tidigare forskning

För att hitta tidigare forskning inom området har vi primärt brukat oss utav databasen Summon, som är en sammanställning utav flertalet akademiska databaser. Tjänsten tillhandahålls via Örebro Universitets biblioteks hemsida. Detta gav oss ett väldigt brett informationsomfång, och sökningen har också kompletterats med Google, som lett oss till forskningsartiklar i deras databas Google Scholar. För att hitta dessa artiklar har vi brukat oss utav våra nyckelord. Sökningen resulterade i väldigt många resultat men via att läsa rubriker och abstracts kunde vi bedöma vilka artiklar/studier som var relevanta för det vi vill undersöka.

Vi har utöver detta också besökt en informatikforskare på Örebro Universitet med insyn i området och genom detta kommit över viss forskning som visat sig vara relevant för våran studie. I denna forskning har vi hittat referenser till annan forskning som också berör området.

Det primära temat vi sökte efter var artiklar som berörde den mänskliga faktorn i frågor om informations- och IT-säkerhet. Begreppen vi tittat efter har varit våra nyckelord, i synnerhet ”human factor” och ”compliance”. Snöbollseffekten har nyttjats på de artiklar som samlats in utefter samma princip, det vill säga temat och nyckelorden. Artiklarna har sedan lästs och jämförts med varandra för att hitta gemensamma faktorer och begreppsanvändning. De har sedan använts för att komplettera teorin bakom ramverket.

Sökord: ”Security awareness”, ”compliance”, ”information security”, ”human factor”, ”IT security”

3.3 Semistrukturerade intervjuer

Insamlingen utav empiri skedde via semistrukturerade intervjuer, vilket skapar möjligheten för respondenten att själv få reflektera över och utveckla sitt svar. Det ger också möjligheten för oss att ställa följdfrågor, och för respondenten att ta upp sådant de bedömer relevant för intervjun. (Oates, 2006) Detta bedömdes som relevant för studien då det skapar en möjlighet att få en bred insyn i ämnet men samtidigt säkerställa att vi får svar på de frågor vi i förhand visste att vi ville ha svar på.

3.4 Val utav verksamheter för intervju

Vi har valt att besöka företag som arbetar inom olika branscher. Detta för att koppla till forskningen som talar om att företagets arbetsmiljö kan påverka människors beteende i säkerhetsfrågor. Genom

att välja olika typer utav verksamheter kan vi då se huruvida detta stämmer överens med våran frågeställning. Redan tidigt i planerandet av studien resonerade vi kring alternativ till verksamheter vi skulle kunna tänka oss intervjua. Målet var att intervjua två respondenter (en säkerhetsansvarig och en vanlig anställd) per verksamhet från ca fyra-fem olika verksamheter.

3.5 Genomförandet utav intervjuerna

När kontakt med de berörda verksamheterna hade etablerats så bokades intervjuer in så tidigt som möjligt. På tre veckor genomfördes åtta intervjuer på sammanlagt fyra verksamheter, det vill säga två individer per verksamhet.

3.6 Bearbetning av intervjudata

Insamlingen av våran intervjudata skedde via inspelning. När intervjuerna avslutats transkriberades dem och korrigerades sedan så de följde ett konsekvent format (Oates, 2006). Vi följde intervjuerna efter bästa förmåga, men otydliga ord och fraser föll i viss utsträckning bort (på grund utav mummel eller otydlig ljudupptagning). Det som bedömdes oväsentligt såsom ”euhm”, ”öh”, stamningar eller skratt valdes också bort på grund utav att vi inte ansåg att det bidrog till innehållet i intervjun.

3.7 Redogörelse för resultat

Presentationen utav våran data från intervjuerna sker under ett resultatstycke, separat från analys. Resultaten har grupperats under andra rubriker än de som presenterats under ramverket, för att ge en mer överskådlig bild av vad respektive respondent svarat inom de olika relevanta områdena. Då ramverket kommer användas i analysen finner vi ingen vidare relevans i att använda dess rubriker under resultatdelen, utan har istället valt att gruppera det på ett mer sammanfattat och lättläst sätt. Resultatdelen består utav sammanfattningar av vad som sagts utav respondenterna kring respektive ämne under intervjuerna. Fullständig intervjumall bifogas som bilaga.

3.8 Analysmetod

Resultatdelen analyseras mot det teoretiska ramverket HFD, presenterat i tidigare kapitel. Sammanfattningarna utav intervjuerna kommer ställas emot de komponenter som ramverket utgör för att sedan jämföra lik- och skiljaktigheter mellan verksamheterna. Analysen kommer bestå utav en jämförelse utav vad ramverket beskriver som säkerhetsfrämjande enligt de olika komponenterna, jämfört med hur resultaten visar. Vi vill genom detta skapa en tydlig koppling mellan vad teorin säger angående ramverkets komponenter (exempelvis kommunikation) och dess inverkan på säkerhetsarbetet i praktiken.

3.9 Etik

Enligt Oates (2006) ska för respondenternas skull intervjuerna hållas på en plats som känns bekväm. Således lät vi våra respondenter välja plats för deras egen bekvämlighets skull, samtliga valde sina respektive arbetsplatser. Då intervjuerna efter medgivande spelades in, markerade vi tydligt när inspelningarna startade och avslutades så att det inte skulle kännas obekvämt. Respondenternas anonymitet (både som individ och verksamheten) har stärkts i största möjliga mån. Detta inte bara för att skydda deras identitet men också för att respondenter då också kan enklare medge brister inom sitt arbetssätt eller verksamhet (Oates, 2006). Respondenterna gavs också möjligheten att få den transkriberade intervjun skickad till sig för korrekturläsning, så de kunde kontrollera att vad de sagt representerades korrekt. Enbart två respondenter valde detta.

3.10 Metodkritik

Genom semistrukturerade intervjuer blir det lättare att få de svar vi är ute efter, men samtidigt finns risken att intervjun missar faktorer som kanske uppdagats i en öppen intervju. (Oates, 2006) Det finns också en risk att respondenterna påverkats av det faktum att intervjuerna spelades in. En faktor vi diskuterade var den att våra resultat onekligen är färgade av respondenternas individuella uppfattning av och förkunskaper kring ämnet. I de anställdas fall finns det inget som säkerställer att respondenten är representativ för sin arbetsgrupp, men intervjun är utformad så att det i bästa möjliga mån ska motverka detta genom att ställa frågor som berör denna aspekt. Dock så frångår ju detta inte respondentens individuella tolkning av frågorna.

Analysen utav våran data kommer också påverkas utav våran tolkning av resultaten, samt hur vi tolkat ramverket i användning. Vi har försökt vara så tydliga som möjligt med hur vi dragit slutsatser ur våran data.

4. Resultat

4.1 Verksamhet A

Om verksamheten

Verksamhet A är ett IT-företag som arbetar med bland annat IT-konsultering, systemutveckling och backup. Vi träffade den säkerhetsansvarige för Örebro-kontoret och en servertekniker från samma arbetsplats, i samma byggnad. Respektive intervju tog plats på deras kontor och varade ca 20 minuter.

Kommunikation

Ansvarig

Verksamhetens kommunikation sker primärt via interna styrdokument och ett ansvar läggs på respektive avdelnings chefer att se till att deras respektive anställda följer dem. Verksamheten har också en ”code of conduct”. Vid en incident sker kommunikationen med de säkerhetsansvariga via en service desk. Respondenten uppger att deras service desk-personal är kompetent och vet hur en rad olika problem skall hanteras, och snabbt kan ge tydliga instruktioner till de drabbade samt hänvisa problemet till rätt avdelning eller grupp. Säkerhetsansvarige uppger att de anställda ”vet vilka dom ska vända sig till” angående frågan om direkt kommunikation mellan de anställda och de säkerhetsansvarige sker. Respondenten säger dock att kommunikationen sker ”lite för dåligt”.

Anställd

Den anställde beskriver kommunikationen som aktiv och öppen. Det som nämns är styrdokumenten men också mailkontakt med ansvarige samt att det förekommer möten med cheferna för att diskutera säkerhetsfrågor. Tillvägagångssättet att rapportera eventuella incidenter till service desk framstår som tydligt och väl kommunicerat. Respondenten verkar i stort vara nöjd med hur kommunikationen inom verksamheten sker: *”jag tror att det är nog ganska bra att dom kanalerna som vi har finns, dom duger nog ganska bra”*.

Förebyggande åtgärder & sanktioner

Ansvarig

Verksamheten innefattar flertalet förebyggandeåtgärder. Bland annat nämns kontinuerliga medvetenhetsutbildningar, introduktionsutbildningar för nyanställda, säkerhetsutbildningar för kunder och det som kallas ”nanoutbildningar”, små (ca två minuters läsning) utbildningar som kan komma till att skickas ut under någon vecka. Respondenten uppger att detta förebygger tidsbristen som föreligger säkerhetsarbetet, då dessa utbildningar kan tas del av från nästan var som helst, till exempel på väg till jobbet, vid fikapausen eller annat ledigt tillfälle. De är inte heller speciellt tidskrävande. Under EU:s säkerhetsmånad (Oktober 2016) hade verksamheten olika kurser angående säkerhetsrelaterade risker, såsom exempelvis phishingmail (en typ av ”spam”/massutskick som syftar till att samla in information från mottagaren. Denna information kan vara att lösenord, användarnamn etc.).Verksamheten skickar ut frågeformulär för att mäta om medvetenheten inom verksamheten ökar, och respondenten uppger vissa tvivel kring pålitligheten i dessa mätningar, men att de ändå verkar tyda på att medvetenheten förbättras.

Sanktioner i form utav sänkt behörighetsnivå förekommer i fall av säkerhetsmissar, det nämns också att anställda kan plockas bort från att jobba mot vissa kunder om det upplevs att den anställde ofta gör fel i ärenden gällande den kunden. Anställda informeras också om att i vissa fall kan de bli straffskyldiga under lagen. Så kallade ”audits” (granskningar) sker kontinuerligt, för att se över konton, lösenordspolicys och dylikt.

Anställd

Respondenten uppvisar god medvetenhet kring samtliga förebyggande insatser som nämnts tidigare av den säkerhetsansvarige. Respondenten uppger att säkerhetsmedvetenhet kommuniceras bra genom de olika förebyggande metoder som verksamheten applicerar, och uppger: *”Jag kan inte riktigt se hur det skulle vara annorlunda egentligen.”.* En sak som respondenten nämner som positivt i denna aspekt är att spårbarheten i deras arbete är väldigt hög; det är lätt att veta vem som har varit var och gjort vad: *”det är lätt att följa i många led”.* Respondenten nämner också att hen upplever att de risker som de anställda kan komma till att identifiera tas på allvar och ”brukar åtgärdas ganska snabbt”.

Hot mot säkerheten

Ansvarig

Respondenten svarar snabbt att användarna egentligen är det största hotet. Deras beteenden och (eventuellt) bristande kunskap om IT-hot uppges vara en risk. Tekniska hot såsom phishing-mail, falska CIO-mail (CIO står för Chief Information Officer, eller Informations/IT-chef på svenska), malware, ransomware (ransomware krypterar filerna på en dator, och gör så att filen helt enkelt inte går att läsa utan den rätta avkrypteringsnyckeln. En lösensumma begärs för avkrypteringsnyckeln), etc. nämns också som vanligt förekommande. Det nämns också att ett hot är att dessa phishingmail blir svårare och svårare att motverka, då de ser mer och mer autentiska ut. Respondenten uppger också att *”dom system vi kör idag inte är säkra överhuvudtaget”* och att det rent praktiskt försöks ”glömmas bort”. Det finns också vissa aspekter som glöms bort i policyn, bland annat det att det förekommer bristfällig lösenordshantering. Det är ”lätt att glömma” att lösenord kan lagras i datorn, eller att någon tillfälligt anger ett svagt lösenord för att underlätta sitt arbete under dagen. Respondenten nämner att policys och regler ibland kan frångås, då *”det är enkelt att göra fel, det ska gå fort och det är bråttom”.*

Anställd

Även här nämns användaren som det primära hotet. *”Det är generellt användare som brukar göra misstagen”.* Det uttrycks ett förtroende för de etablerade processer, och nämns att det är när processerna frångås som risker kan bli en faktor. Respondenten nämner att regler sällan frångås, men att det ibland sker ”i nödfall”, likt vad den säkerhetsansvarige sade.

Personligt ansvar

Ansvarig

Respondenten säger att verksamheten litar på det personliga ansvaret i ”ganska hög utsträckning”. Det nämns att revisioner sker, men *”annars litar vi ganska hårt på att teknikerna vet vad de gör. Det är ju dom som kan miljön”.* Privata lagringsmedier är förbjudet inom verksamheten. Privatsurfing förekommer men är reglerat via policys, och sker under eget ansvar. Webbfilter förekommer för att spärra åtkomsten av vissa sidor. I övrigt verkar det personliga ansvaret mest handla om att de anställda ska följa etablerade policys gällande verksamheten.

Anställd

Respondenten uppger sitt personliga ansvar som stort, då arbetsrollen i fråga innefattar ganska bred tillgång till verksamhetens olika system. Den viktigaste aspekten (enligt respondenten) av det personliga ansvaret ligger i att se till att de arbetsuppgifter som utförs faktiskt sker på beställning och inte på något eget initiativ. Det ska finnas direktiv för arbetet som utförs. Angående den generella säkerhetsmedvetenheten säger respondenten att *”den är ganska bra faktiskt”.* Angående privat surfing och dylikt uppger respondenten att det, likt vad den ansvarige sade, sker på eget ansvar och under sunt förnuft; *”man kanske inte sitter tankar torrents liksom”*. Respondenten uppvisar full medvetenhet kring förbudet mot privata lagringsmedier. *”Vi får inte använda något externt egentligen, egna USB-minnen, dropbox, etc. Inga öppna, eller vad man ska säga, tredjeparts ”cloud”-baserade lagringsmedier”.*

Hinder och begränsningar

Ansvarig

Det centrala här verkar röra sig om tid. Respondenten säger att *”det skulle vara lite mer seminarieforum, men det är svårt att hinna med.”* samt *”man har inte tid att sitta en halv dag och lyssna på nån säkerhetsgubbe”.* Värt att nämna är dock att som sagt så förebyggs ju denna tidsbrist med de så kallade ”nanoutbildningarna”. När vi nämner att andra verksamheter nämnt att säkerheten blivit mer i fokus de senaste åren, håller respondenten med: ”*Ja, precis, dom senaste tre åren, skulle jag vilja säga, att det har exploderat, även om kanske inte pengarna kommer, men medvetenheten kommer, faktiskt.”.*

Anställd

Ett ”problem” som nämns är att respondenten upplever (Speciellt under sin första tid inom verksamheten) att behovet av diverse access-konton skadade hans produktivitet. Däremot benämns detta som ”ett nödvändigt ont” ur en säkerhetsaspekt, och är således inte riktigt ett hinder eller en begränsning. Trots att respondenten uppger säkerhetsmedvetenheten som generellt hög, nämner hen också att *”det finns väl en o annan gammal räv som inte riktigt hängt med i utvecklingen”*, men det framgår aldrig tydligt om detta heller upplevs som ett hinder eller en begränsning. I stort verkar respondenten nöjd med hur säkerhetsarbetet på arbetsplatsen sköts, och identifierar inte så många hinder eller begränsningar.

4.2 Verksamhet B

Om verksamheten

Verksamhet B är en statlig förvaltningsmyndighet. Vi besökte deras kontor för intervju och talade med deras IT-avdelnings säkerhetsansvarige, samt en anställd som jobbar som utredare. Respondenterna befann sig på samma arbetsplats, inom samma byggnad. Intervjun med den säkerhetsansvarige varade ca 30 minuter, intervjun med den anställde varade ca 20 minuter.

Kommunikation

Ansvarig

Verksamheten kommunicerar sina säkerhetsbestämmelser primärt via styrdokument som ligger på deras intranät. Det är enligt respondenten chefens ansvar att medvetengöra de anställda om de relevanta styrdokumenten. Respondenten medger vissa brister i denna kommunikation, då hen anser att vikten i att kommunicera detta kanske inte alltid är uppenbar för chefen i fråga, och uppger *”det där kanske inte riktigt cheferna vet hur mycket dom måste jobba med”*. Vid eventuella incidenter sker kommunikationen via verksamhetens service desk. Respondenten ser gärna att hens (och andra inom säkerhetsområdets) möjlighet att komma ut mer i verksamheten förbättras, det vill säga deras möjlighet att komma ut och prata säkerhet med olika målgrupper.

Anställd

Respondenten uppger stor medvetenhet kring de dokument som finns tillgängliga angående säkerheten på verksamhetens intranät. Respondenten nämner att *”det finns ju riktlinjer för allting”.* Hen nämner också att det förekommer ”riktad” säkerhetsinformation, det vill säga information som berör enbart eras specifika avdelning. Ändringar utav rutiner kommuniceras via E-post, som skall läsas dagligen. Respondenten uppger att hen gör det minst en gång i veckan.

Förebyggande åtgärder & sanktioner

Ansvarig

I stort sammanfattar respondenten det förebyggande arbetet som *”det är ju då att medvetengöra, utbilda, att man ska förstå vilken information man hanterar”*. I dagsläget får nyanställda och konsulter inom verksamheten en grundläggande säkerhetsgenomgång. Det framgick i intervjun att organisationen var uppe i en omvandling, som primärt verkar för att främja kommunikationen, som vi upplevde att respondenten fann något bristande. Denna kommunikation skulle innefatta mer

omfattande introduktionsutbildningar, med ett fokus på mer målgruppsanpassade insatser, för att ”skräddarsy” ditt säkerhetstänk utifrån din arbetsroll. Respondenten nämner också att hen finner ett behov av att flika in med säkerheten vid ”rätt tillfällen” i verksamhetens olika utvecklingsprocesser, så att säkerheten hamnar i åtanke redan från början. Respondenten nämner också att *”utvecklarna ska kunna säker systemutveckling”*, och att behovet av säkerhets arkitekter bör minskas. Verksamheten har också vad de kallar en ”ledningsgenomgång” som sker minst en gång per år och innefattar mätningar av informationssäkerheten och medvetenheten inom verksamheten. Respondenten säger att detta bidrar till deras åtgärdsplan för säkerhetsarbetet. När frågan om hur den mänskliga faktorn förebyggs uppger respondenten att medvetengöra, utbilda och behörighetshantera är de centrala delarna i deras arbete. Tydliga sanktioner för de anställda vid säkerhetsrelaterade incidenter, menar respondenten, utan det regleras snarare utav arbetsgivaren eller ansvarig chef. Respondenten menar att incidenter av allvarlig natur kan dras inför personalansvarsnämnd som hanterar frågan, i vissa fall kan det bli polisiär åtgärd. Primärt verkar sanktionsarbetet dock vara att ”ta hand om” berörd individ och försäkra att dennes arbetsförmåga kan fortgå obehindrat, om den till exempel öppnat ett mejl med skadlig kod eller på annat sätt skadat IT-systemen. Personen i fråga kan enligt respondenten känna en väldig skuld och då anses det viktigare att se till att denne kan fortsätta sitt arbete.

Anställd

Påminnelser till de anställda angående efterlevnad av säkerhetsrutiner förekommer. Vid intervjuns tillfälle hade en sådan skett bara veckan innan. Respondenten nämner introduktionsutbildningen som den ansvarige talade om, men nämner att den inte specifikt fokuserar på IT-aspekten av informationssäkerhet. Ett gemensamt sekretessavtal för samtliga anställda förekommer, så information du eventuellt avläser från kollegas skärm skyddas under den. Vid frågan om kontinuerlig utbildning inom säkerhetsfrågor förekommer blir svaret nej, utan att det mer sker vid de tillfällen de känner att ett behov finns.

Hot mot säkerheten

Ansvarig

Respondenten menar att IT-säkerheten har varit, generellt sett, ganska låg, och stundvis förbisedd. Hen nämner också att det ofta har varit det första som kompromissats med i utvecklingsprojekt de gånger de jobbat mot en snäv deadline. Det nämns att *”säkerhet det är ju någonting man kan göra sen, eller det kan man lägga på i efterhand”*. Hen anser också att säkerheten är en förbisedd aspekt i

den pågående ”digitaliseringen”, det vill säga digitalisering av ”analogt” pappersarbete och hanteringen av sekretessbelagd information. I övrigt pratar hen om de ”klassiska hoten”, såsom phishingmail och andra webbangrepp. Ett annat hot som nämns är vad som i intervjun kommer till att kallas ”balansgången” mellan vad folk behöver veta kontra vad de inte får veta. Detta gäller både ledningen och de övriga anställda. Olika personal har olika informationsbehov, och att identifiera dessa kan stundvis bli problematiskt. När respondenten ställdes inför frågan om den mänskliga faktorn i säkerhetsarbetet, uppgav hen att det också kan ses som ett av de större problemen, och att det bör beaktas och förebyggas i form utav utbildningar.

Anställd

Det hot som respondenten upplever är av en annan natur än vad den ansvarige respondenten beskrev. Det rör sig här mer om ett mer fysiskt hot, att en individ faktiskt skulle komma in i byggnaden och få ”verklig” tillgång till en arbetsdator och informationen däri. Vid frågan om den mänskliga faktorn uppger respondenten att det primärt, i deras fall, handlar om att hålla obehöriga människor utanför lokalerna, och inte något vidare fokus på hur man hand håller systemen. Däremot uppger respondenten att *”jag vet inte riktigt rent tekniskt vilka möjligheter dom* (eventuella angripare) *har”.*

Personligt ansvar

Ansvarig

Svaren vi fick angående det personliga ansvaret var relativt kortfattade. Respondenten berättar dock att ”*ytterst är det ju alltid myndighetschef som är ansvarig”*, då de bär ansvaret för sina ”resurser” (anställda och konsulter under dem). Det personliga ansvaret verkar ligga i att följa etablerade bestämmelser, men respondenten verkar anse att denna syn på ansvar är något bristfällig, och att kommunikationen kring den individuella rollen är något otydlig och kanske otillräcklig.
Surfande i personliga ärenden är tillåtet under eget ansvar, men begränsas utav webbfilter. Privata USB-minnen och dylika lagringsmedier är i dagsläget också tillåtet. Respondenten verkar ha ett stort förtroende för de som handhar systemens personliga ansvar. De jobbar också för att uppmuntra attityden om att en kan och bör kontakta IT vid eventuell problematik.

Anställd

Det personliga ansvaret respondenten nämner är för det första det säkra undanröjandet av sekretessbelagda dokument, det vill säga köra dem i dokumentförstörare när en är färdig med dem, för det andra nämns vikten av att låsa arbetsdatorn när en lämnar arbetsstationen. Respondenten upplever att detta ansvar efterlevs väl, både personligen och för kollegor. Respondenten svarar positivt på frågan angående om hen upplever att säkerhetspolicys följs ordentligt överlag. Att anmäla problem och oro till verksamhetens service desk är vanligt förekommande, och sker kontinuerligt och vid ens minsta misstanke om skada på verksamhetens IT-system. Privat surfing förekommer under eget ansvar, men respondenten anger att privata lagringsmedier är förbjudet i arbetet.

Hinder och begränsningar

Ansvarig

Även här pratar respondenten om den så kallade *balansgången*. Respondenten nämner att en ”akilleshäl” kan vara just hemliggörandet utav säkerhetsrelaterade områden, och att det kan finnas ett värde i att medvetengöra i en större utsträckning än vad organisationen uppmuntrar eller tillåter. Den planerade omvandlingen som respondenten nämner, som skall ta fart under 2017, är ett resultat av att medvetengörande kring säkerhetsfrågor inte längre prioriteras bort, som tidigare verkar ha varit en stor begränsning som även idag bär ansvaret för vissa av de identifierade säkerhetsproblemen. Verksamheten i fråga är en sammanslagning av flera enheter. Att främja ett enhetligt arbetssätt mellan dessa nu sammanslagna enheter kan enligt respondenten innefatta svårigheter., då det finns ”rester” av gamla arbetssätt som tillhört de forna enheterna, som kan bli svåra att bryta.

Anställd

Under intervjuns gång så får vi inga specifika svar angående hur respondenten upplever några specifika hinder eller begränsningar i sin förmåga att efterleva säkerhetsbestämmelserna i dagligt arbete. Respondenten har en klar uppfattning om kommunikationsvägarna till service desk och följaktligen IT-ansvarige, och uppvisar också en adekvat förståelse för hur en ska tillgå verksamhetens säkerhetsrelaterade styrdokument.

4.3 Verksamhet C

Om verksamheten

Verksamhet C är ett statligt lärosäte. Intervjuerna skedde vid separata tillfällen, men båda respondenter intervjuades på sina respektive kontor. Respondenten som intervjuades angående säkerhetsarbetet är säkerhetsansvarig inom verksamheten, den andre respondenten är lektor. Respondenterna befinner sig på samma arbetsplats, men i olika byggnader. Respektive intervju tog ca 15-20 min.

Kommunikation

Ansvarig

Respondenten uppger att den primära kommunikationen kring säkerhetspolicys sker genom diverse användarpolicys och styrdokument, tillgängliga på verksamhetens intranät. Följaktligen uppger respondenten att *”vi är för dåliga på att nå ut till användarna”*. Respondenten uttrycker också att det finns svårigheter med att få tid och möjlighet till att informera nyanställda om informationssäkerhet. När en incident skett sker kommunikationen från de anställda via en service desk.

Anställd

Respondenten visar på medvetenhet kring de bestämmelser som finns tillgängliga på intranätet, men uppger att kollen på vad som ingår i säkerhetspolicyn inte är hundraprocentig. Det nämns också att det kan komma mail angående specifika händelser, som till exempel kan uppmana till att byta lösenord. Under intervjun framgår det att den mesta kommunikationen kring säkerhetsfrågor sker mellan respondenten och dennes kollegor. Respondenten uppger att ”det är möjligt” att någon inbjudan till seminarium angående säkerhet mejlats ut, men att det kan ha sållats bort i och med mängden mail som mottas. Respondenten är medveten om att kommunikationen med service desk är din första åtgärd vid en eventuell säkerhetsincident, exempelvis att öppna en skadlig länk.

Förebyggande åtgärder & sanktioner

Ansvarig

Respondenten uppger att om en användare beter sig på ett felaktigt sätt och/eller gör medvetna fel så existerar det disciplinära åtgärder. Tekniska lösningar som fångar upp misstänksam e-

postaktivitet finns på plats, men de är inte 100% effektiva, då ett hackat konto fortfarande kan förbli ”osynligt”. Respondenten nämner att oktober 2016 var ”europeiska säkerhetsmånaden” och att de i samband med det gick ut med information, men nämner också tvivel kring om denna information faktiskt mottas av användarna. Respondenten uppger: *”det kräver ju återigen att användarna läser det som står på intranätet och sådana här saker och det är ju inte det folk gör primärt”.*
Någon informationssäkerhetsutbildning vid nyanställning sker i dagsläget inte, men respondenten uppger att de önskar att se en förändring på det.

Anställd

En förebyggande åtgärd som nämns är att respondenten mottagit och följt en uppmaning att byta lösenord angående en säkerhetsincident. Användandet utav en av verksamheten tillhandahållen molnlagringstjänst är också en tilltagen förebyggande åtgärd. Förebyggande åtgärder såsom information vid anställning finns som sagt inte. Detta bekräftas utav respondenten.

Hot mot säkerheten

Ansvarig

Användarna identifieras direkt av respondenten som det största hotet. En aspekt utav detta hot är att respondenten anser att *”användare är alldeles för dåliga på eller lämnar ut sina uppgifter lite för lättvindigt”*. Detta kan vara en risk i och med exempelvis phishing-mail. Respondenter uppger också att olika användare är olika stora hot, beroende på sin respektive kunskap av IT-system och säkerhet, samt i hur de använder sig utav verksamhetens nätverk.

Anställd

Respondenten bekräftar här vad den ansvarige nämner som ett stort hot, nämligen phishing-mail, som enligt hen förekommer ”drösvis per vecka, om inte per dag”. Trots att respondenten själv verkar uppfatta sig själv som säker i detta avseende, nämns ändå detta som en risk för andra, kanske mindre medvetna, användare. Respondenten uttrycker också en viss oro över sin efterlevnad kring bestämmelserna angående lösenordssäkerhet. Hen antyder att både hen och kollegor är medvetna om risker kring bristfällig lösenordstillämpning, man att det rent praktiskt ändå inte tillämpas i den utsträckning det kanske borde.

Personligt ansvar

Ansvarig

Respondenten ger ett koncist svar angående personligt ansvar: *”När man är anställd så är man skyldig att följa de riktlinjer och policys som finns. Då är man personligt ansvarig för att man gör, där lägger vi ansvar på användarna.”* Det nämns också att det finns avdelningar inom verksamheten som stundvis jobbar med känslig information, och då är det upp till dem att hantera den varsamt, men att de också har hårdare regler och är mer medvetna. Webbfilter eller förbud av privata lagringsmedier finns inte på plats. Respondenten uppger: *”Om man nu surfar privat så ser vi inte något IT säkerhets relaterat problem med det. Det blir ju ett personalproblem om någon lägger mer tid på att surfa privat än att arbeta”*

Anställd

Respondenten reflekterar tydligt angående sitt personliga ansvar i flera aspekter genom intervjun. Respondenten uppger på frågan ”hur upplever du ditt personliga ansvar när det kommer att efterleva säkerhet?” att *”det är ju stort, alltså, det är ju enormt, jag har ju, som anställd på, en myndighet har man ju ett väldigt stort ansvar”.* Respondenten sitter utöver sin roll som lektor på andra positioner där hanterandet utav känslig information är utav relevans, så förståelsen för det personliga ansvaret är således genomgående. Det innefattar också inte bara IT-relaterade områden i strikt mening, utan också detaljer som att låsa datorn samt kontoret när en lämnar den/det. Angående privat surfing (på arbetstid) är respondenten införstådd i vad den ansvarige säger om att det sker på eget ansvar, och uppger *”i grund och botten handlar det om att, vi får, det jobb vi ska göra gjort”.* Angående privata lagringsmedier är respondenten restriktiv med hur hen lånar ut dem till kollegor och dylikt, samt påvisar medvetenhet kring vilken information som de kanske innehåller och hur en skall hantera den för att se till att den inte hamnar i fel händer/tappas bort.

Hinder och begränsningar

Ansvarig

Att möjligheten till att komma ut och informera vid exempelvis nyanställningar ses utav respondenten som en begränsning. Respondenten identifierar olika organisatoriska problem:

1. *”Det som kan vara svårt är att få tid och möjlighet att bli inbjudna vid exempelvis vid nya anställningar för att ge information och prata om informationssäkerhet. Dom kanske inte tycker att detta är tillräcklig viktigt så där kan det finnas ett organisatoriskt problem.”*

2. *”IT-säkerhet ses ofta som bromsklossar som bara är jobbiga och ställer krav ju högre upp i hierarkin man kommer.”*

Respondenten uppger dessutom att hen upplever att vissa avdelningar saknar intresse för säkerhet.

Anställd

Respondenten identifierar flertalet begränsningar; Bland annat nämns tidsbrist när det kommer till att läsa policys, samt nackdelarna med att detta är den primära kommunikationsformen, då den både är tidskrävande och svåra att ta till sig och omsätta praktiskt. Respondenten säger: *”för att få upp någon medvetenhet, man måste diskutera den, för att ta till sig någonting, och, få, en, vad ska man säga, skapa ett eget synsätt på, varför gör jag det här, och varför är det viktigt för att faktiskt, kunna göra mitt jobb på ett bra sätt, att det inte bara blir någonting annat då, en till policy som ligger på nätet, som man inte hinner gå in och läsa, i detalj, för att, hur ska jag få tid med det.”.*

Respondenten uppger att de ”*närmaste kollegorna tror jag har en relativt god syn på informationssäkerhet i och med att det är många som forskar inom det, och vi diskuterar det aktivt och vi ändå har hyfsad koll, hoppas jag på det här med IT här på avdelningen. Pratar man bredare på universitetet tror jag att det är väldigt varierande.”* Detta är i enlighet med vad den ansvarige säger om olika avdelningars varierade kompetens.

4.4 Verksamhet D

Om verksamheten

Verksamhet D är en kommunal verksamhet. Intervjuerna skedde vi separata tillfällen på respektive respondents kontor. Respondenten som intervjuades angående säkerhetsarbetet inom verksamheten är informationssäkerhetsansvarig över flera verksamheter, bland annat den vi besökte. Den andra respondenten är boendepedagog inom socialpsykiatrin. Respondenterna befinner sig således inte på samma arbetsplats. Respektive intervju tog ungefär 20-30 minuter.

Kommunikation

Ansvarig

Respondenten uppger att de primära kommunikationsvägarna är via policys och riktlinjer som finns tillgängliga på verksamhetens intranät. På frågan ”hur kommunicerar ni säkerhet med era anställda?” svarar respondenten att ”*Ja, det har ju varit brister på det och är brister som det är nu*”. Respondenten uppger följaktligen att hen är medveten om att kommunikationen har brister, men detta är något de håller på att åtgärda. Respondenten uppger att viss kommunikation sker även via deras IT-support.

Anställd

Respondenten ger en bild av att kommunikationen är bristfällig i dagsläget och kan inte ge exempel på varken rutiner eller riktlinjer när det kommer till säkerhet inom verksamheten. På frågan ”Hur kommuniceras säkerhet inom verksamheten?” säger respondenten ” *Ja, inte så värst mycket, men det kan ju komma ett mejl ibland kanske som dom skickar ut någon gång så. Jag vet inte ens om vi har några rutiner eller riktlinjer så för det*.”. Dock så uppger hen att det finns riktlinjer för sekretessbelagd information som enligt hen följs av alla inom verksamheten. Respondenten uppger att vid eventuella IT-säkerheters relaterade problem eller frågor kan hen vända sig till IT-supporten.

Förebyggande åtgärder & sanktioner

Ansvarig

Respondenten uppger att i dagsläget så finns inga centrala säkerhetsutbildningar som varje anställd måste genomgå. Dock inom vissa verksamheter med särskilda krav så sker lokala utbildningar. Respondenten påtalar att verksamheten just nu befinner sig i ett slags mellan läge där man ser över hela säkerhetsarbetet. På frågan ”vilka insatser gör ni för att öka medvetenheten om säkerhet?” så

svarar respondenten att ”*jag har tagit fram ny policy och nya riktlinjer som inte är beslutade än men när dom är beslutade, då kommer vi ju liksom kommunicera ut dom och även köra utbildningsinsatser då, och det kommer vara generellt för alla i verksamheten att man lägger upp det på intranätet att alla ska gå igenom det här, men sen kan det ju behövas speciell, specifik utbildning i en viss verksamhet, till exempel inom skolan eller inom vården eller någonting annat, då kan det ju vara kopplat till vissa system som man använder, men en generell utbildning kommer det bli för alla, som blir obligatorisk då.”.* Respondenten uppger att det finns idag inga sanktioner mot dåligt säkerhetsbeteende utöver tillsägelser från närmaste chef så länge det inte handlar om lagbrott.

Anställd

Respondenten uppger att hen inte fått någon utbildning kring IT-säkerhet inom verksamheten och svarar följaktligen på frågan ” Du fick inga utbildningar eller motsvarande när du tog anställning?” att ”*Nej, sen har ju jag jobbat inom statlig institution tidigare så man har ju det med sig sen tidigare.”.* Respondenten kan inte ge några exempel på förebyggande åtgärder som genomförts utöver enstaka E-mail under den tid hen varit anställd.

Hot mot säkerheten

Ansvarig

Respondenten uppger att verksamheten idag är mycket beroende utav att systemen fungerar och uppger ”*Det finns ju ett antal allvarliga hot, som om man ska titta på dom mest allvarliga, det kanske inte är samma som dom mest sannolika men, det är ju att kritiska, alltså att infrastrukturen inte fungerar, att internet inte fungerar. För det är väldigt mycket som är beroende av det, kritiska system. Det blir mer och så i och med digitaliseringen, det är beroende av att det fungerar, det kan vara många olika saker, det kan ju vara, ja, tekniska haverier och så vidare, men det kan ju även vara sabotage, terrorism eller något sånt där.*”. På frågan om hur den ”mänskliga faktorn” påverkar säkerheten uppger respondenten att hen är medveten om den och nämner ”ä*ven om vi skulle köpa in ny brandvägg eller annan teknisk utrustning så måste det alltid omgärdas med regelverk hur det ska användas, hur det ska konfigureras, hur det ska underhållas, och då måste vi ha utbildning också för dom som ska handha det, konfigurera, installera, men även underhåll och sköta det och så, och har man inte alla dom delarna så spelar det ingen roll hur bra dom här prylarna man har köpt är, både hårdvara och mjukvara.”.* Respondenten uppger att de även har problem med ”ransomware” och hen uppger att de hela tiden blir utsatt för nya typer av skadlig kod som

potentiellt kan skada verksamheten kraftigt.

Anställd

Respondenten uppger att hen ser hotet mer fysiskt än tekniskt och uppger bland annat ”*Nån oro kan man ju känna när papper och så ligger framme som vem som helst kan se*”. Respondenten är medveten om risken associerad med den mänskliga faktorn inom IT-säkerhet och svarar ”*Det är klart att man kan glömma att stänga av datorn eller ha den på och det kommer in fel folk och ser, eller om någon kommer in på min login eller att man glömmer att logga ut. Det är sånt jag kan tänka på ibland.”.* Respondenten uttrycker också en oro kring om det system som används dagligen skulle sluta fungera och uppger att *”Vi måste ju skriva ut ganska mycket sekretessbelagd information, exempelvis planering och handlingsplaner”.*

Personligt ansvar

Ansvarig

Respondenten ger ett tydligt svar när det kommer till vilket personligt ansvar varje medarbetare har, ”*Man har ju, dels har man ju ansvar att efterleva dom reglerna som är och i dom här nya riktlinjerna så kommer det att lite olika kapitel, men ett kapitel riktar sig till alla medarbetare, som alla ska få det, och då är man ju skyldig att följa dom, det är 8 områden då, och man är dessutom skyldig att rapportera misstanke om incidenter som inträffar om man ser saker*”. Utöver detta så ställs inte ytterligare krav på det personliga ansvaret så länge som lagar, policys och riktlinjer följs inom de olika verksamheterna.

Anställd

Respondenten uttrycker att hen känner ett stort personligt ansvar och svarar på frågan ” Hur upplever du ditt personliga ansvar när det kommer till frågor om informationssäkerhet?” att *”Det är ju klart att jag har ett personligt ansvar jag måste ju se till så att jag gör det jag kan för att skydda det som ska.”*. Hen säger också att övriga medarbetare inom verksamheten tar ett stort personligt ansvar och följer de sekretessregler som finns bland annat. Respondenten säger ” *Man aktar sig för att lägga utskrifter och sånt där, Vi har ju gemensamma datorer och man måste logga ut efter sig. Det är sånt som vi kan prata om att ibland att saker ligger på platser de inte ska och när det är andra folk i lokalen som inte ska vara här att vi plockar undan de saker som är sekretessbelagda osv*.”.

Hinder och begränsningar

Ansvarig

Respondenten säger att en begränsande faktor är resurser både personal och ekonomi. På frågan ”Finns det några begränsningar rent organisatoriskt, för eran förmåga att kommunicera, informationssäkerhet?” så svarar respondenten att ”*Ja, det gör det ju liksom rent resursmässigt, att dom här verksamhetsutvecklingarna jag nämnde, dom har ju precis börjat tillsättas, förvaltningsledare finns det ju ett fåtal av, bara fast vi har jättemånga system, men det är bara ett par system som har, egentligen ordentlig förvaltningsledning, och så men dom personerna som finns där, dom är ju bra, att man utbildar dom, pratar om informationssäkerhet ute i skolan, och socialen och så vidare, men det behövs fler, som har den, i en så här stor verksamhet, så det behövs mer resurser, helst skulle jag vilja ha, såna som bara, It, informationssäkerhetsexperter, ute, ett gäng, men det kommer jag nog aldrig få, men en, man kan ju utbilda en verksamhetsutvecklare, t. ex som är duktig på It, och informationssäkerhet och verksamheten också då, genom dom här frågorna, så att den hjälper verksamheterna och, även kommer till mig eller It och säger att, äh men nu måste vi förbättra det här, där finns det ett stort behov.”.* Respondenten ser idag också en brist när det gäller kontinuitetshantering, det vill säga hur en verksamhet fungerar i händelse av en, störning t. ex att elen försvinner, att IT-stödet försvinner. Detta tror respondenten beror på en naivitet bland högre chefer. Respondenten menar också på att säkerhet kan komma till att prioriteras bort i vissa avseenden. Hen uppger att detta kan bero på att de är under politiskt styre och således prioriteras andra saker för att tillgodose exempelvis vallöften.

Anställd

Respondenten säger att hen tror att säkerheten inte är prioriterad och att det finns naivitet kring säkerhetsfrågor. Respondenten säger att ” *Det är nog inte prioriterat. Jag är inte så insatt i det där med folk som kan ”hacka” sig in på nått sätt som man har hört talas om, det känns främmande och jag tror att det är så för många här. Man tror nog att det är säkrare än vad det är. Kanske är naiva.*”. Bristen utav utbildningar ser respondenten också som ett hinder för att kunna efterleva ett sunt säkerhetstänk och säger ”*Det är ju så att det lätt skapas egna rutiner och att man blir hemmablind på något sätt. Så det är ju bra om man kan bli uppdaterad säkerhet. Det skulle nog vara bra, jag tror man gör saker man inte tänker på.*”. Respondenten säger att hen tillsammans med alla på arbetsplatsen tycker att säkerheten är viktig men tror att den kan komma i andra hand.

5. Analys

I detta avsnitt kommer vi analysera resultatet enligt ramverket HFD, presenterat i tidigare avsnitt.

5.1 Kultur / Arbetsmiljö

Inom verksamhet A, B och C befinner sig den säkerhetsansvarige på samma arbetsplats som de anställda och är direkt tillgänglig för personalen, medan verksamhet D är unik i det avseendet att den informationssäkerhetsansvarige befinner sig på annan plats. Verksamhet D är också den verksamhet som påvisat minst medvetenhet kring säkerhetsbestämmelser. Verksamhet A är den verksamhet som haft säkerhetsansvariga närmast inpå den faktiska arbetsmiljön, och är också den verksamhet som påvisat den mest överensstämmande bilden kring informationssäkerhet som beskrivet utav verksamhetens säkerhetsansvarige. Verksamhet A också är den enda verksamheten där respondenten konkret jobbat med just IT, och kanske just därför påvisar medvetenhet i högre utsträckning. Den anställde ifrån verksamhet D uppger att ”*det är ju så att det lätt skapas egna rutiner och att man blir hemmablind på något sätt”* samt att *”det* (säkerhetsmedvetenhet) *är inget vi pratar om”.* Det är den enda verksamheten som uppvisat den typen utav problematik.

Både Metalidou et al (2014) samt Alhogail, Mirza, Bakry (2015) pratar om vikten av att bibehålla en arbetsmiljö som upprätthåller och uppmuntrar en medvetenhet kring säkerhetsfrågor. Metalidou et al (2014) skriver att *”organizations need to cultivate and maintain a culture where positive security behaviors are valued”.*

Arbetsmiljön/kulturen påverkas i det stora hela mycket av faktorer såsom medvetenhet, träning och kommunikation. Problematiken vi ser i verksamhet D kan härledas till att arbetsmiljön inte främjar säkerhetsmedvetenheten och bekräftar således det Metalidou et al (2014) antyder angående att en god säkerhetsmedvetenhet bör stärkas inom arbetsmiljön för att främja efterlevnad. I de övriga verksamheterna, i synnerhet verksamhet A, finns en väldigt påtaglig säkerhetskultur som också ger en synlig inverkan på hur de anställda ser på säkerheten inom sina respektive verksamheter.

5.2 Kommunikation

Flertalet verksamheter uppger att det finns tidsrelaterade hinder/begränsningar när det kommer till att kommunicera informationssäkerhet. Den säkerhetsansvarige för verksamhet A säger att *”man har inte tid att sitta en halv dag och lyssna på nån säkerhetsgubbe som mässar om någonting”* och den säkerhetsansvarige för verksamhet C uppger organisatoriska problem så som *”IT-säkerhet ses ofta som bromsklossar som bara är jobbiga och ställer krav ju högre upp i hierarkin man kommer”*.

Hur kompenseras då för tidsbristen? Verksamhet A är unik i det avseende att de är de enda som uppgett att de förebygger tidsaspekten via sina s.k. ”nanoutbildningar”. Denna insats är ”påminnelser” om rådande säkerhetsbestämmelser som de anställda ska kunna läsa och ta till sig på ett snabbt och enkelt sätt. Då de bara är ca en till två minuter långa så kan de genomföras även om arbetsbelastningen är hög. Verksamhet A är också unika i det avseende att de är den enda verksamhet som också gör mätningar för att kontrollera sin säkerhetsmedvetenhet.

Den primära kommunikationen kring säkerhetsbestämmelser inom samtliga verksamheter sker främst via policy/styrdokument, men de har olika tillvägagångssätt för hur de sprider den informationen. Verksamhet B får uppdateringar på sitt intranät när något som respondenten beskriver som ”stort” händer. Riktad säkerhetsinformation per avdelning förekommer också. Respondenten uppger att de ska uppdatera sig dagligen, men att i hens fall sker veckovis. Verksamhet C och D har ett liknande tillvägagångssätt, men medvetenheten kring dessa är hos den anställde inte lika omfattande. Hen uppger *”det kan ju komma ett mejl ibland kanske som dom skickar ut någon gång så. Jag vet inte ens om vi har några rutiner eller riktlinjer så för det.”*. Samtidigt har samtliga anställda uppvisat att de är nöjda med den rådande kommunikationen, medan samtliga säkerhetsansvariga har antytt att de anser att kommunikationen kring säkerhetsbestämmelserna kan eller bör förbättras.

Alhogail, Mirza, Bakry (2015) pratar mycket om vikten kring kommunikation av säkerhet, samt vikten av att inkludera alla inom organisationen i säkerhetsarbetet, för att minska riskfaktorer. Verksamheten måste också påvisa att säkerhet är en prioritet för att försäkra efterlevnad. En dåligt kommunicerad policy kan enligt dem likställas med avsaknad av policy, då den ändå inte kommer efterlevas. Nanoutbildningarna och mätningarna på plats inom verksamhet A stärker bilden av säkerhet som något som prioriteras, men den är som sagt också den enda som använder denna typ utav lösning. Verksamhet B, C och D har som nämnt ovan väldigt liknande kommunikation kring säkerhetsbestämmelser. Dock så påvisar verksamhet D en betydligt sämre nivå av efterlevnad och

kunskap – Vad beror då detta på? Den anställda inom verksamhet D påvisar inget som tyder på att hen på något vis blivit inkluderad i säkerhetsarbetet och har heller inte någon koll på säkerhetsbestämmelserna som gäller. Säkerheten framstår som något främmande och inte riktigt en prioritet i det vardagliga arbetet. I verksamhet B och C påvisas en bättre förståelse och medvetenhet kring dom bestämmelser som finns på plats, medan verksamhet D inte ens vet om det finns några. Detta tolkar vi som att de ansvariga inom verksamhet B och C påvisar en högre prioritet angående säkerhet för de anställda men det kan också beror på arbetsmiljömässiga aspekter, men kan också bero på att de faktiskt blir mer inkluderade i säkerhetsarbetet. De anställda inom verksamheterna B och C uppger också att de tagit till sig utav information angående säkerhet som kommunicerats till dem via mail. Verksamhet D:s respondent nämner inget om något sådant.

5.3 Medvetenhet & Träning

Medvetenhet

Verksamhet A är som sagt den verksamhet som påvisat mest överensstämmande syn på säkerheten mellan anställda och ansvariga, medan i de övriga verksamheterna har anställda och ansvariga mer skilda perspektiv på var hoten mot säkerheten ligger. Angående den mänskliga faktorn uppger både verksamhet B och D mest oro kring faktiska fysiska hot, såsom att få datorn stulen eller utsatt för otillåten tillgång (om en exempelvis glömmer att låsa), eller att sekretessbelagda papper råkar ligga framme och således hamnar i fel händer. De anställda ifrån verksamhet A och C uppvisar en större medvetenhet kring tekniska hot med bas i den mänskliga faktorn, såsom phishing, än vad de anställda i verksamhet B och D gör. Den anställda ifrån verksamhet B uppger *”jag vet inte riktigt rent tekniskt vilka möjligheter dom har”* angående otillåten tillgång till avdelningens IT-resurser. Den anställda ifrån verksamhet D uppger *”jag tror inte att man tänker så mycket på det”* som svar på frågan angående varför hen tror att verksamheten inte utfört några säkerhetsfrämjande insatser.

Samtliga ansvariga har uppgett själva, eller åtminstone hållit med om, att användare är det största (eller åtminstone ett av de största) hoten mot säkerheten inom respektive verksamhet. Den anställda ifrån verksamhet A är den enda som också uppgett detta. Den anställde ifrån verksamhet C visar viss medvetenhet kring detta, men nämner det mest som en riskfaktor, och inte som ett utav de större hoten. Respondent C uppger också *”jag tror att alla är ganska avtrubbade med det där”* angående phishingmail.

Träning

Trots att samtliga ansvariga identifierat hotet kring den mänskliga faktorn (användarna) så är det enbart verksamhet A och B som har kontinuerliga åtgärder som motverkar denna faktor, såsom introduktionsutbildningar, riktad säkerhetsinfo och i verksamhet A:s fall, nanoutbildningar. Samtliga säkerhetsansvariga (och vissa anställda) uppger att de gärna skulle se fler tillfällen och/eller möjligheter för träningsinsatser (exempelvis introduktionsutbildningar eller seminarier) men att det ofta finns hinder såsom organisatoriskt ointresse eller tidsbrist.

Enligt Alhogail, Mirza och Bakry (2015) så är kontinuerliga träningsinsatser ett hjälpmedel för anställda att förstå och efterleva säkerhetsmedvetenheten. Både verksamhet A och B visar på detta i och med att de båda brukar sig utav riktade säkerhetspåminnelser till sina anställda. Verksamhet A har som sagt också kontinuerliga utbildningar, de som de kallar för nanoutbildningar, för att försäkra sina anställdas medvetenhet. Lacey (2009) uppger att samtliga användare inom verksamheten är relevanta, och detta påvisar således ett behov av medvetenhet hos samtliga anställda. Stanton et al. (2006) pratar om att även små insatser för att främja säkerheten kan ge stor inverkan.

Verksamhet A och B är de verksamheter som jobbar mest med säkerhetsfrämjande insatser, såsom introduktionsutbildningar och kontinuerliga insatser, vilket är en förutsättning för god efterlevnad enligt ramverket. En kan tydligt se att detta påverkat deras arbetssätt och således deras medvetenhet, då de uppvisat en stor förståelse för säkerhetsarbetet, trots att den anställde inom verksamhet B kanske inte identifierat samma hot som den ansvarige. Verksamhet B uppger också att de är under direktiv om att uppdatera sig på säkerhetsuppdateringar, och att det sker åtminstone veckovis. Verksamhet C och D är under liknande direktiv, men påvisar betydligt sämre efterlevnad kring det. Verksamhet C har förhållandevis bristande säkerhetsinsatser ur ett träningsperspektiv, men den anställde uppvisar ändå stor förståelse för säkerhetsrisker. Verksamhet D, som har ett liknande arbetssätt, påvisar betydligt mindre medvetenhet, och uppger också att informationssäkerhet inte är något som de direkt diskuterar inom sin verksamhet. Vi tror att detta kan härledas till att den anställde inom verksamhet C jobbar inom ett område som är nära besläktat med IT, och det faktum att respondenten själv uppger att flertalet av de saker vi genom intervjun tagit upp, också är saker som diskuteras mellan henom och hens kollegor.

Den tidigare forskning vi baserat vårat ramverk på, påvisar ett tydligt samband mellan träning och medvetenhet. Detta är något vi också kan se speglat i verkligheten.

5.4 Ansvar

Samtliga anställda uppger att de känner ett stort ansvar att skydda den informationen de tillhandahåller. Hotbilden ser dock annorlunda ut mellan verksamheterna, då samtliga har en annorlunda bild utav vad hoten innefattar. Verksamhet A:s anställda uppger att hen känner primärt ett tekniskt ansvar, då hen innehar tillgång till flertalet system som är grundläggande för verksamheten, medan övriga pratar mer övergripande om sekretess, låsa datorn, förvara sekretessbelagda dokument säkert, etc. Respondenten ifrån verksamhet C pratar om informationssäkerhetshot som att råka sprida olika typer utav information som hen i sitt yrke har förtroende för, och att hen måste aktivt reflektera över vilka som ska och inte ska ha tillgång till denna information. Hen uttrycker sig angående sitt ansvar; *”det är ju stort, alltså, det är ju enormt, jag har ju, som anställd på, en myndighet har man ju ett väldigt stort ansvar”.* Denna attityd är genomgående hos de anställda. Således kan vi se att det personliga ansvaret är en faktor som tas på allvar. Samtliga säkerhetsansvariga säger att det primära ansvaret hos de anställda helt enkelt ligger i att följa rådande bestämmelser.

Alhogail, Mirza och Bakry (2015) säger att en faktor i det personliga ansvaret är den personliga kunskapen om säkerhet. Enligt dem är det viktigt att främja känslan av det personliga ansvaret och dess nytta. Beautement et al (2008) anser att en individs ansvar bara kommer sträcka sig så långt som den kan se nyttan i det.

Det personliga ansvaret kan enligt ses som en konsekvens av de övriga faktorerna (kommunikation, kultur/arbetsmiljö medvetenhet och träning) då de i slutändan är vad som kommer avgöra i vilken utsträckning som individen förstår sitt ansvar och de efterföljande konsekvenserna. Det vi kan se i våra resultat är att det personliga ansvaret är en faktor som i stor utsträckning existerar hos de anställda. Däremot så varierar kunskapsnivån om säkerhetshot och bestämmelser vilket följaktligen begränsar effekten som deras personliga ansvar innefattar. Detta kommer i sin tur innebära att det personliga ansvaret inom vissa verksamheter kanske inte betyder fullt så mycket, då de uppvisar bristande medvetenhet kring säkerhetsrelaterade aspekter. De kan således inte ta det ansvar som kanske är nödvändigt för en adekvat säkerhetskultur. Det personliga ansvaret blir ju egentligen bara relevant i den utsträckning som det kan appliceras praktiskt.

6. Diskussion

Det övergripande vi kommit fram till via våra resultat och våran analys är den att medvetenheten är det som avgör huruvida säkerheten efterlevs.

Detta i sin tur är en direkt konsekvens av hur väl kommunicerade säkerhetshoten inom verksamheten är. Verksamheter som tillämpar mångsidiga kommunikationslösningar (som exempelvis utbildningar, utskick och seminarier) har i regel en större medvetenhet och efterlevnad än de som inte gör det. Den här typen utav kommunikation påverkar också vilken typ utav ansvarstagande du som individ kommer åta dig. Det färgar också säkerhetskulturen inom arbetsmiljön.

Så hur påverkas verksamheterna rent praktiskt utav kommunikationen? Som tidigare forskning antyder så är det bara möjligt att ta ett personligt ansvar i den utsträckning som medvetenheten tillåter, och detta är ju en direkt konsekvens av hur kommunikationen inom verksamheten förs. Detta är något vi också upplever, då vi kan se en direkt relation mellan medvetenhet och kommunikation. Exempelvis så har verksamhet B har kommunikativt främjande insatser såsom introduktionsutbildningar och riktad säkerhetsinformation, medan dessa insatser inte kan återfinnas i verksamhet D, som också påvisar en bristfällig medvetenhet. Det vi kan se är således att hur kommunikationen sker (eller att den sker) har en avgörande påverkan på hur medvetenheten inom verksamheten kan se ut, men att medvetenhet också kan påverkas genom exempelvis säkerhetskulturen, som i verksamhet C:s fall.

Resultaten utav studien visar att det finns en klar relation mellan kommunikation och efterlevnad utav IT-/informationssäkerhetsbestämmelser, men att det finns fler faktorer än kommunikation som kan gynna en god säkerhetstillämpning, såsom god säkerhetskultur. Det vi kan se är trots att verksamhet B, C och D har liknande sätt att kommunicera och tillämpa säkerhetspolicys, så har de en väldigt varierad nivå utav efterlevnad, vilket vi tror kan härledas till faktorer som säkerhetskultur och personligt ansvar (härlett från egen kunskap om ämnet). En annan faktor som kan vara relevant är verksamhetens intresse i säkerhetsfrågor, då det vi också sett är att samtliga ansvariga beskriver vad som i princip är dagliga hot. De uppmärksammar också ett visst organisatoriskt ointresse i olika utsträckning. Detta är en trend som delvis är på väg att vända, vilket omorganisationerna inom verksamhet B och D tyder på, där säkerhet börjar få en högre prioritet.

Litteraturen som vi baserat ramverket för våran studie på går in mycket på dessa faktorer, i synnerhet den kommunikativa aspekten mellan verksamheternas ledning och de ansvariga för säkerhetsfrågor. Alhogail, Mirza och Bakry (2015) pratar om detta och hävdar att effektiv kommunikation påvisat stor inverkan på säkerheten inom verksamheter, och att ledningens intresse i dessa frågor är av stor vikt. Det vi kan se är att i de verksamheter där ledningen beaktar säkerheten (med exempelvis introduktionsutbildningar eller andra utbildningar) så finns det också en högre säkerhetsmedvetenhet återspeglat i de anställda.

Vi tror att en större urvalsgrupp, samt ett större fokus på verksamheter där IT inte är det primära intresseområdet skulle ge oss en bredare bild av problematiken kring de kommunikativa aspekterna. Resultaten vi har nu är samlat från fyra verksamheter, varav två har en tydlig koppling till IT-området, om än i olika utsträckning. I och med idén med studien var att undersöka just kommunikationens inverkan på medvetenheten, så undermineras denna idé lite av att respondenterna uppvisat egen införskaffad kunskap, oberoende av verksamhetens kommunikation. Vi tror att resultaten hade blivit annorlunda om fokus primärt legat på verksamheter utanför IT-området.

Alhogail, Mirza och Bakrys (2015) ramverk (med våra tolkningar och kompletteringar) skapade en överskådlig bild av problemområdet, och har dessutom påvisat att samtliga element som vi använde ur ramverket, faktiskt också har en reell påverkan på verksamheternas säkerhetstillämpning. Ramverket skapade en bra grund för oss att mäta och jämföra våra resultat.

Sammanfattningsvis kan vi se att informations- och IT-säkerheten inom en verksamhet påverkas av medvetenheten. Medvetenheten i sin tur har en stark relation till kommunikationen, men påverkas också utav faktorer såsom säkerhetskultur. Detta är ju dock bara gynnsamt i de fall som en positiv säkerhetskultur är ett faktum.

7. Slutsats & bidrag

Huvudfrågan vi tänkt besvara med studien var: *Vilka faktorer påverkar informations- och IT-säkerhet inom verksamheter?* Det vi kommit fram till är att kommunikationen är en vital del av tillämpning och efterlevnad utav säkerhetsbestämmelser, men bara en av många faktorer i vad som bör vara ett omfattande arbete. Vi kan se att samtliga faktorer som tas upp i vårat ramverk är viktiga och har en inverkan på hur säkerhet tillämpas i praktiken.

Fokus med studien har således legat på ett flertal aspekter, slutsatsen vi däremot kan dra är den att i de verksamheter där IT- och informationssäkerhetsmedvetenheten kanske inte är tillräcklig (och kanske inte driven av eget intresse), så är kommunikationen den mest vitala delen för att bibehålla positiv säkerhetskultur. Detta på grund utav att den främjar både medvetenhet och kunskap, och genom detta också inverkan av det personliga ansvaret.

Våran rapport har bidragit till att stärka teorin och bakgrunden kring ramverket HFD, då vi observerat dess områdens inverkan och samverkan i praktiken.

Vidare forskning bör fokusera på en större och annorlunda urvalsgrupp än vad vi valt, med ett fokus på verksamheter vars huvudsakliga intresseområde inte är IT. Vi anser det sannolikt (och med stöd i våran studie) att i verksamheter utanför IT-området, så existerar en sämre medvetenhet anammat av det personliga intresset. Den kommunikativa aspekten i dessa verksamheter blir desto viktigare, och dess inverkan kan vidare undersökas.

8. Referenslista

8.1 Böcker

Lacey, David (2009), Managing the Human Factor in Information Security. John Wiley & Sons, Incorporated. Hämtad från: http://site-ebrary-com.db.ub.oru.se/lib/universitetsbiblioteket/reader.action?docID=10300879

Oates, B.J. (2006). Researching information systems and computing. London: SAGE.

8.2 Avhandlingar

Karjlalainen, Mari (2011),

Improving employees' Information Systems (IS) Security Behavior

Hämtad från: http://jultika.oulu.fi/files/isbn9789514295676.pdf

Vance, Anthony (2010),

Why do employees violate IS security policies?.

Hämtad från http://jultika.oulu.fi/files/isbn9789514262876.pdf

8.3 Vetenskapliga artiklar

Alhogail, Mirza, Bakry (2015),

A comprehensive human factor framework for Information Security in organizations.

Journal of Theoretic and Applied Information Technology, (Volym 78, No. 2), 201-211

http://www.jatit.org/volumes/Vol78No2/6Vol78No2.pdf

Beautement A, Sasse MA & Wonham, M (2008),

The Compliance Budget: Managing Security Behaviour in Organisations

New Security Paradigms Workshop, (NSPW '08), 47-58

http://www.nspw.org/papers/2008/nspw2008-beautement.pdf

Lim, Joo Soo (2009),

Exploring the Relationship between Organizational Culture and Information Security Culture

7th Australian Information Security Management Conference, 87-97
http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1011&context=ism

Metalidou E, Marinagi C, Trivellas P, Eberhagen N, Skourlas C, Giannakopoulos G (2014),

The Human Factor of Information Security: Unintentional Damage Perspective.

3rd International Conference on Integrated Information (Volym 147), 424-428

http://ac.els-cdn.com/S1877042814040440/1-s2.0-S1877042814040440-main.pdf?_tid=bbafa64c-b55e-11e6-8c47-00000aacb360&acdnat=1480333096_3992042a2f1083a38fe8f4bfb34d776c

Stanton, Jeffrey M. (2005),

Analysis of end user security behaviors.

Computers & Security (Vol 24, issue 2), 124-133

http://www.sciencedirect.com/science/article/pii/S0167404804001841

8.4 Webb

CompTIA, (2015),

Technology: Not Your Biggest Security Problem. Hämtad 2016-11-17, från:
http://www.iatpr.com/technology-not-your-biggest-security-problem/

Computer Weekly (2007),

The human factor is key to good security. Hämtad 2016-11-17, från:
http://www.computerweekly.com/opinion/The-human-factor-is-key-to-good-security

Inside Sources (2015),

Opinion: The ‘Human’ Factor is Key in Cybersecurity. Hämtad 2016-11-17, från:
www.insidesources.com/opinion-the-human-factor-is-key-in-cybersecurity

Matthews, Earl (2015),

The Importance of Human Factors in Cybersecurity. Hämtad 2016-11-17, från: https://www.linkedin.com/pulse/importance-human-factors-cybersecurity-matthews-maj-gen-usaf-ret-

Proofpoint. (2016),

The Human Factor Report 2016. Hämtad 2016-11-17, från: https://www.proofpoint.com/sites/default/files/human-factor-report-2016.pdf

Tripwire. (2013),

Human Factors in Information Security Management Systems
Hämtad 2016-11-19, från: https://www.tripwire.com/state-of-security/security-data-protection/human-factors-effective-information-security-management-systems/

9. Bilagor

Detta är frågemallen vi baserat våra intervjuer på. Resonemangen bakom vad vi ville få ut av frågorna skrivs ut med röd text.

Säkerhetsansvariga	Anställda
Vad ser ni som det största hotet mot IT-säkerheten? (Om människan; Kommuniceras detta till era anställda?) Med denna fråga vill vi öppna för ett avslappnat samtal där vi låter respondenten resonera fritt kring ämnet	Vad ser ni som det största hotet mot IT-säkerheten?
Mycket forskning tyder på att ett stort hot mot IT-säkerhet är den mänskliga faktorn (t. ex. social engineering eller bristfällig säkerhetstillämpning). Vad anser ni om detta? Hur förebygger ni det? Denna fråga avser att undersöka medvetenheten kring just den mänskliga faktorn då det är en central del i studien	Mycket forskning tyder på att ett stort hot mot IT-säkerhet är den mänskliga faktorn. Känner du dig medveten om detta?
Hur kommunicerar ni säkerhet med era anställda? (direkt eller via nån person eller via dokument?) Denna fråga är relevant för att kunna jämföra skillnader i kommunikationen mellan olika verksamheter	Hur kommunicerar ni säkerhet med era ansvariga? (direkt eller via nån person eller via dokument?)
Vilka insatser görs för att öka medvetenheten kring god säkerhetssed? (Om inga; Varför?)	Vilka insatser görs för att öka medvetenheten kring god säkerhetssed? (Om inga; Varför?) Anser ni att medvetenhet kring god säkerhetssed

Denna fråga undersöker direkt hur medvetenhet främjas inom verksamheten	kommuniceras väl genom detta?
Hur har dessa insatser påverkat verksamheten? (Om nej eller vet ej; Varför?) Denna fråga ger en potentiell grund för analys utav relationen mellan medvetenhet och tillämpning	Hur har dessa (eventuella) insatser påverkat ditt arbetssätt?
Vilket personligt ansvar lägger ni på era anställda?	Hur upplever du ditt personliga ansvar gällande säkerhet?
Hur upplever ni säkerhetsmedvetenheten i er verksamhet? Följs eventuella policies? Underlag för analys kring om god kommunikation främjar säkerhetsmedvetenhet	Hur upplever ni säkerhetsmedvetenheten i er verksamhet? Följs eventuella policies? Om nej: Varför följs dem ej? Personligt ansvar obefintligt? Opraktiskt/omständigt?
Hur påverkas er möjlighet att kommunicera informationssäkerhet? Finns det begränsningar i form av ekonomiska/produktiva/organisatoriska aspekter? Relevant fråga för att undersöka faktorer som kan hämma medvetenheten	Hur påverkas er möjlighet att kommunicera angående/efterleva informationssäkerhet? Hur (om nåt) skulle du vilja ändra i kommunikationen?
Vad har ni för policies angående privat surfning på arbetstid? Följs dessa? Denna fråga undersöker relationen mellan kommunikation och efterlevnad	Vad har ni för policies angående privat surfning? Följer du dessa?
Vad finns det för åtgärder vid eventuella säkerhetsincidenter? Skadekontroll? ”Uppfostring”/Sanktioner? (Om ingen specifik finns; Hur rationaliseras det?)	1. Vad finns det för åtgärder vid eventuella säkerhetsincidenter? (om ogrundat svar;)

Undersöker huruvida respektive verksamhets åtgärdsplaner är välkommunicerade, samt ”monitoring/sanctions”	2. Vad gör du vid en eventuell säkerhetsincident?
Tillåts privata lagringsmedier? (t ex USB-minnen, externa hårddiskar) Denna fråga undersöker relationen mellan medvetenhet och efterlevnad	Använder du privata lagringsmedier i arbetet?
Hur hanterar ni säkerhetsfrågor mellan olika personalgrupper? Denna fråga ämnar att skapa inblick i hur de säkerhetsansvariga ser på de anställdas kunskap.	Anser du att din säkerhetsmedveten skiljer sig från andra personalgrupper?
Finns det problem ni identifierat som ofta (enligt er) förbises? Underlag för diskussion	Finns det problem ni identifierat som ofta (enligt er) förbises?