Examensarbete

HÖGSKOLAN I SKÖVDE

SÄKERHETSFÖRETAGS ARBETE FÖR ÖKAD SÄKERHETSMEDVETENHET

Examensarbete inom huvudområdet
Informationsteknologi
Grundnivå nivå 30 Högskolepoäng
Vårtermin År 2019

Christoffer Schmid

Handledare: Hanife Rexhepi
Examinator: Eva Söderström

Sammanfattning
Historiskt har mycket fokus lagt på tekniska åtgärder för att hålla information säkert. Idag finns mycket forskning som tyder på att det är människan som är den svagaste länken i säkerhetskedjan och anställdas säkerhetsmedvetenhet därför är av stor vikt för att hålla organisationers information säker.

Studien undersöker frågeställningen: ”Hur arbetar säkerhetsföretag med att höja sina medarbetares säkerhetsmedvetenhet?”

En kvalitativ metod har använts med semistrukturerade intervjuer som grund för datainsamling. Sammanlagt har tre företag och fem respondenter intervjuats som tillsammans med litteraturen har bidragit med den data som använts för att besvara frågeställningen.

Resultaten visar att företagen som deltagit i studien har gjort mycket som går i linje med det som litteraturen påpekat som viktigt, samtidigt som vissa saker inte är riktigt lika vanligt förekommande. Resultaten visar även att företagen jobbar med vissa tekniker som inte nämns omfattande i litteraturen. Detta innebär att det även finns en viss skillnad mellan det som litteraturen antytt som viktigt och hur företagen faktiskt i praktiken har jobbat med medvetenheten.

INNEHÅLLSFÖRTECKNING

Figurförteckning

Tabellförteckning

1 Inledning

Informationssäkerhet är idag en mycket viktig och vital del för dagens organisationer. Information är av största vikt för att den dagliga verksamheten ska kunna fungera och därav också viktig att hålla säker. Historiskt har mycket fokus lagts på tekniska lösningar för att hålla informationen säker (Crossler *m.fl.*, 2013). Människan är dock ansedd som en utav de viktigaste delarna när det gäller säkerheten och människan kommer alltid att stå i centrum. Att hålla människorna inom organisationerna medvetna om informationssäkerheten blir därför en mycket viktig del i arbetet att skydda sin information. Om människorna som jobbar med informationen inte är medvetna om vad som kan ske, eller deras roll gällande informationssäkerheten, kommer också riskerna för att incidenter sker att vara högre. Bland annat har tidigare studier visat att upp mot hela 75% av alla säkerhetsincidenter sker av egen personal (D'Arcy, Hovav och Galletta, 2009). Samtidigt börjar och slutar alla attacker med just människan, snarare än mot teknologin (Nohlberg, 2009). Om människorna har en högre säkerhetsmedvetenhet kommer därför också riskerna att kunna minimeras.

Ett sätt att formellt och organiserat arbeta med en organisations säkerhetsmedvetenhet är bland annat via medvetenhetsprogram. Medvetenhetsprogrammen som finns idag är dock inte alltid tillräckligt bra och tar oftast inte upp relevanta hot och uppdateras heller inte baserat på den effekt det har (Ernst & Young, 2009). Det leder till att medvetenheten gällande informationssäkerheten hos anställda inte är på den nivå den bör vara och organisationer är med det sagt också generellt relativt dåliga på att jobba med den del av säkerheten som berör människorna själva.

Denna studie syftar därför till att få en ökad kunskap i hur företag som befinner sig inom informationssäkerhetsbranschen arbetar för att öka den egna interna medvetenheten. Förhoppningen är att få fram de aktiviteter företag inom informationssäkerhetsområdet arbetar med för att öka sin medvetenhet. Detta kan sedan bli inspiration och grundstenar i arbetet för andra företag som inte kommit lika långt i processen för att öka säkerhetsmedvetenhet inom sin egen verksamhet. Frågeställningen som behandlats i denna studie är: "Hur arbetar säkerhetsföretag med att höja sina medarbetares säkerhetsmedvetenhet".

För att undersöka den här frågeställningen har en kvalitativ undersökning med semistrukturerade intervjuer som grund för datainsamling använts. Fem respondenter i tre olika företag har intervjuats för att samla in den data som krävs för att kunna besvara frågeställningen. En innehållsanalys har utförts och kategorier har identifierats vilket har blivit grund för det resultat som tagits fram. Resultatet är dessa identifierade kategorier tillsammans med en sammanställning av vad dessa företag gör och vad de tycker är viktigt inom respektive kategori. Resultaten visar att företagen som deltagit i studien har gjort mycket som går i linje med det som litteraturen påpekat som viktigt, samtidigt som vissa saker inte är riktigt lika vanligt förekommande. Resultaten visar även att företagen jobbar med vissa tekniker som inte nämns omfattande i litteraturen. Detta innebär att det även finns en viss skillnad mellan det som litteraturen antytt som viktigt och hur företagen faktiskt i praktiken har jobbat med medvetenheten.

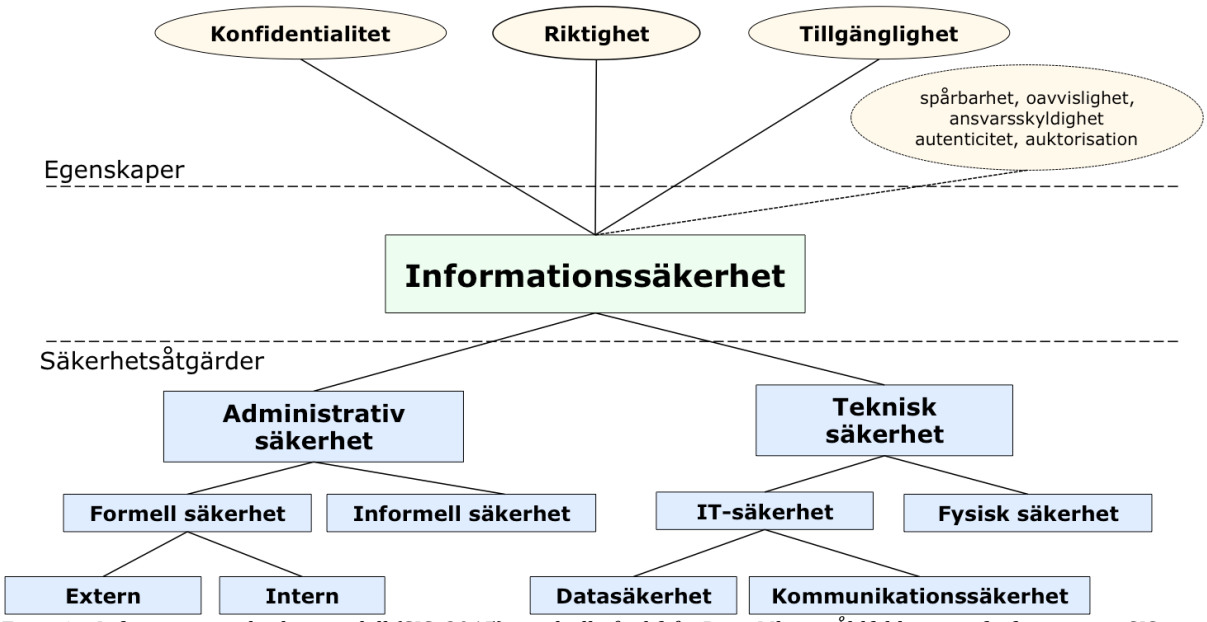
2 Bakgrundskapitel

I detta kapitel tas en bakgrund upp gällande området informationssäkerhet, vilket ger en grundläggande förklaring till huvudområdet studien befinner sig i. Begreppen organisationskultur och säkerhetskultur beskrivs, som är en bidragande faktor i hur väl informationssäkerheten faktiskt fungerar i organisationer. Begreppet säkerhetsmedvetenhet förklaras, vilket är det området studien syftar till att undersöka. Vidare tas olika sätt att öka säkerhetsmedvetenheten upp, vilket har blivit en grund till de intervjuer som har genomförts.

2.1 Informationssäkerhet

Information är en väsentlig del för att organisationer ska kunna fungera och därmed något som organisationer också är högst beroende av (Khan *m.fl.*, 2011). Vad är då information, vilken information är det som ska skyddas? Information finns i många olika former och det gäller att också skydda det som är de så kallade behållarna av information såsom exempelvis datorer. Det som är i behov av skydd kan delas in i tre olika kategorier om hårdvara, mjukvara och data. Hårdvara är exempelvis datorer, mjukvara är exempelvis applikationer eller operativsystem och data innebär själva informationen såsom dokument, foton eller email (Pfleeger, Pfleeger och Margulies, 2015). Hårdvara och mjukvara är relativt enkelt att ersätta medan data är unikt och därav också svårare att ersätta och kräver därför också en större eftertanke vid val av säkerhet.

Med tanke på den vikt som information utgör för organisationer idag är det också logiskt att hålla den informationen säker. SIS Tekniska rapport, Terminologi för informationssäkerhet (2015), beskriver att informationssäkerhet handlar om att skydda informationen genom bevarandet av tre olika egenskaper som är riktighet, konfidentialitet och tillgänglighet. Riktighet innebär att informationen är korrekt, konfidentialitet innebär att endast de som är behöriga till informationen ska ha tillgång till den och tillgänglighet handlar om att informationen faktiskt ska finnas när den behövs. För att goda nivåer ska uppnås gäller det att använda sig utav olika säkerhetsåtgärder för att förändra riskerna. Informationssäkerhet som helhet illustreras i informationssäkerhetsmodellen nedan.



Figur 1 – Informationssäkerhetsmodell (SIS, 2015)*, med tillstånd från Rose-Mharie Åhlfeldt, en av författarna av SIS (2015) Tekniska rapport, "Terminologi för informationssäkerhet".*

Informationssäkerhet kan generellt delas upp i två olika delar, nämligen administrativ och teknisk säkerhet. Detta tydliggörs även i informationssäkerhetsmodellen ovan.

Teknisk säkerhet delas in i IT-säkerhet och fysisk säkerhet där fysisk säkerhet relaterar till säkerhetsåtgärder såsom brandskydd eller larmsystem. IT-säkerhet kan sedan i sin tur bli uppdelad i datasäkerhet och kommunikationssäkerhet där säkerhetsåtgärder för datasäkerhet är exempelvis kryptering och relaterar mer mot säkerhet av hårdvara och dess innehåll. Kommunikationssäkerhet handlar om kommunikation mellan nätverk och datorer och således är brandväggar ett exempel på en säkerhetsåtgärd (Åhlfeldt, Spagnoletti och Sindre, 2007).

Administrativ säkerhet definieras som "säkerhetsåtgärder relaterade till hur verksamheten styr informationssäkerhetsarbetet i en organisation, formellt såväl som informellt" (SIS, 2015). Precis som modellen visar delas också administrativ säkerhet upp i en formell och en informell sektion. Den formella säkerheten omfattar exempelvis standarder, policys och rutiner. Den informella säkerheten handlar däremot om det som inte på samma sätt är synligt utåt på samma sätt som den formella säkerheten. Den informella säkerheten omfattar individers egna attityder och värderingar gällande informationssäkerheten (Åhlfeldt, Spagnoletti och Sindre, 2007).

När det talas om informationssäkerhet talas det ofta om att hålla informationen säker mot interna och externa hot. Ett externt hot beskrivs av Doherty och Fulford (2009) som hot som uppkommer från källor utanför organisationen som exempelvis hackers eller virus. Ett internt hot beskrivs som ett hot som uppkommer inom organisationen och ett vanligt internt hot är misstag av anställda. De vanligaste hoten är enligt forskning de interna hoten (D'Arcy, Hovav och Galletta, 2009).

Enligt Martins och Eloff (2002) bör informationssäkerhet ses som en holistisk fråga och där organisationskulturen är en viktig del när det gäller implementeringen av informationssäkerhet i en organisation. I övrigt menar Chang och Lin (2007) att det krävs att informationssäkerhet är en nyckelkomponent i företagets planering och

ledning för att lyckas säkerställa konfidentialitet, riktighet och tillgänglighet av informationen. Informationssäkerhet bör enligt Martins och Eloff (2002) vara en del av organisationskulturen och inkludera frågor som människorna, träning, processer och kommunikation.

2.2 Organisationskulturens vikt på informationssäkerheten

Kulturen i en organisation är en viktig faktor och stor del i hur organisationen i praktiken faktiskt fungerar och skapar värde. Idag är organisationskulturen i många fall ansedd som en central del i styrningen av en organisation (Hallberg *m.fl.*, 2017). Det finns ett stort antal olika definitioner på vad organisationskultur faktiskt innebär. En sammanfattning av dessa olika definitioner har gjorts och fått fram definitionen "gemensamma värden och grundläggande antaganden som förklarar varför organisationer gör vad de gör och fokuserar på det de gör; den existerar på en fundamental, kanske undermedveten, nivå, är grundad i historia och tradition och är en källa till kollektiv identitet och engagemang" (Schneider *m.fl.*, 2017). Med andra ord handlar det bland annat om organisationen och dess anställdas värderingar som i sin tur också kommer att påverka agerandet hos personalen. Organisationskultur handlar bland annat om de informella normer och beteenden som finns.

Informationssäkerhetskultur är en del av organisationskulturen och kan sägas vara den del av organisationskulturen som berör säkerheten, men på en mer detaljerad och lägre nivå (Guldenmund, 2000). Organisationskultur påverkar således även säkerheten. En definition av informationssäkerhetskultur är enligt Hallberg *m.fl.* (2017) "de gemensamma tanke-, beteende- och värderingsmönster som uppstår och utvecklas i ett socialt kollektiv genom kommunikativa processer, baserade på inre och yttre krav, som traderas till nya medlemmar och som har implikationer för informationssäkerhet" (Hallberg *m.fl.*, 2017). Informationssäkerhetskultur är alltså något som ursprungligen kommer från organisationskulturen men i ett säkerhetsperspektiv. Mycket av detta handlar om vad människor tycker och tänker om informationssäkerhet och hur de faktiskt beter sig, snarare än hur de officiellt borde bete sig.

Informationssäkerhetskultur är enligt Martins och Eloff (2002) en svår uppgift och kan ta flera år. Det är viktigt att organisationen värderar och eftersträvar att uppnå bland annat riktighet och tillgänglighet för att ha en informationssäkerhetskultur. Samtidigt handlar det om vad som är eller inte är accepterat inom organisationen i relation till informationssäkerhet, och uppkommer bland annat från att uppmuntra acceptabelt säkerhetsbeteende. Andra viktiga faktorer för att uppnå en informationssäkerhetskultur är att organisationen tar upp frågor om exempelvis informationssäkerhetspolicyn samt anställdas medvetenhet för att hålla organisationens informationstillgångar säker. Kulturen har med att göra hur saker i organisationen genomförs och därför är anställdas beteende gällande informationssäkerhet en faktor i att uppnå en informationssäkerhetskultur (Martins och Eloff, 2002).

Martins och Eloffs (2002) studie har visat att det är viktigt att, för att förbättra informationssäkerhetskulturen, granska informationssäkerhetspolicyn och bli en del av det vardagliga arbetet. Ledningen måste ha informationssäkerhet som prioritet och visa sitt engagemang i att implementera informationssäkerhet i organisationen, samtidigt som det bör finnas en dedikerad grupp eller person som ansvarar för att saker och ting

görs korrekt i förhållande till informationssäkerhet. På individnivå behöver anställda vägledning i vad som är accepterat beteende och vad som inte är accepterat.

2.3 Säkerhetsmedvetenhet

Det har gjorts väldigt mycket inom säkerhetsområdet när det gäller tekniska lösningar för att öka säkerheten såsom exempelvis flerfaktorslösningar, skalskydd och krypteringar. För att uppnå en god nivå av säkerhet krävs dock fler komponenter än enbart teknologi för att lyckas skydda sina tillgångar. Teknologi är en av tre komponenter där de resterande två är människorna och processerna som krävs för att kunna erhålla informationssäkerhet (Herath och Rao, 2009).

Utav dessa komponenter är det människan som ses som den svagaste länken när det gäller informationssäkerhet. Trots detta är människan inom informationssäkerhetsområdet något som organisationer tenderar att ignorera (Bashorun, Worwui och Parker, 2013). För att människan ska vara en tillgång i informationssäkerhetsarbetet snarare än en belastning krävs att människorna inom organisationen ökar sin medvetenhet gällande informationssäkerhet.

Ordet medvetenhet definieras enligt nationalencyklopedin som “uppnådd djupare insikt” (Nationalencyklopedin, 2019). Det handlar med andra ord om en förståelse och när det gäller säkerhetsmedvetenhet har en studie definierat säkerhetsmedvetenhet som den kunskap och attityd anställda i en organisation har gentemot säkerheten (Bashorun, Worwui och Parker, 2013). Med dessa definitioner som grund kommer den här studien att definiera begreppet säkerhetsmedvetenhet som “den förståelse, kunskap och attityd anställda besitter gentemot området informationssäkerhet”.

ISO standarden 27001 (2017) tar upp de krav som finns för ett ledningssystem för informationssäkerhet där medvetenhet är ett utav de krav som finns. Enligt denna standard är kraven gällande medvetenhet att personer som arbetar inom eller åt organisationen ska vara medvetna om:

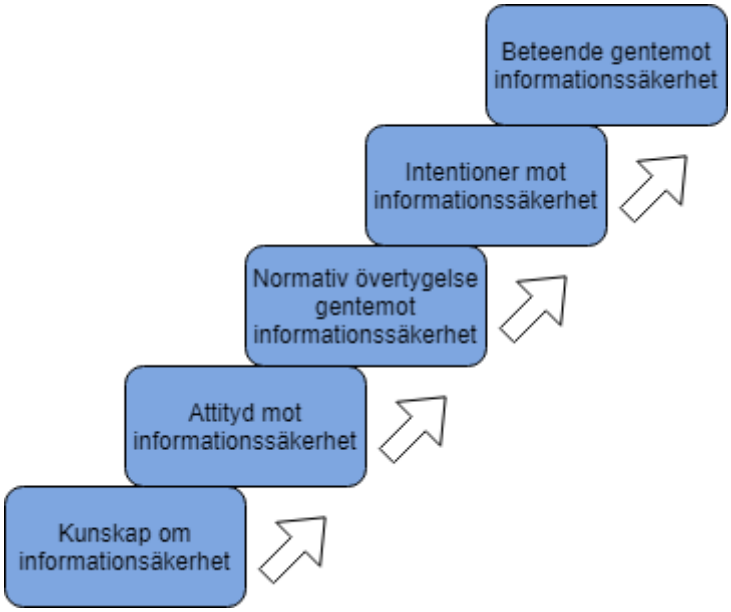
- Informationssäkerhetspolicyn
- Sina bidrag till ett väl fungerande ledningssystem för informationssäkerhet, inklusive fördelarna med att informationssäkerhetsprestanda förbättras
- Konsekvenserna av att inte uppfylla kraven i ledningssystemet för informationssäkerhet

Ghazvini och Shukur (2018) har gjort en studie inom sjukvården gällande säkerhetsmedvetenhet och menar på att informationssäkerhet är ett människoproblem och inte ett tekniskt problem. Teknologi är helt enkelt ansett som verktyg som kan bli missbrukade av användaren. Forskarna menar också på att ledning som enbart löser säkerheten med tekniska åtgärder har förbisett de mänskliga och organisatoriska faktorerna och är därför inte tillräckligt skyddade. Ghazvini och Shukur (2018) menar därför att anställdas medvetenhet är ett effektivt sätt för att minska de incidenter som sker och påpekar att det är viktigt att anställda är medvetna om potentiella hot och konsekvenserna av deras handlingar.

2.4 Öka säkerhetsmedvetenhet

Det finns många olika sätt och aktiviteter som kan göras för att öka medvetenheten inom en organisation när det kommer till informationssäkerheten. Processen att arbeta med säkerhetsmedvetenhet är enligt Tsohou *m.fl.* (2015) en process för att ändra individers uppfattningar, värderingar, attityder, beteenden, normer, arbetsvanor samt organisationskulturen- och strukturen.

Khan *m.fl.* (2011) gjorde en studie och testade olika tekniker som används av organisationer i deras försök att öka medvetenhet och mätte dess effektivitet. Det slutgiltiga målet med att öka medvetenheten är att uppnå ett ändrat säkerhetsbeteende och forskaren har presenterat en femstegsmodell som denne även utgick ifrån i sin studie. Femstegsmodellen finns representerad i figur 2 nedan.



Figur 2 – Femstegsmodell för att mäta säkerhetsmedvetenhet (Khan *m.fl.*, 2011)

Utav de tekniker som testades i studien genomförd av Khan *m.fl.* (2011) var det enbart två som ändrade säkerhetsbeteendet, nämligen utbildningspresentationer samt gruppdiskussioner. Topp tre av de totalt 7 testade teknikerna var också just utbildningspresentationer, gruppdiskussioner samt även mailutskick. Övriga tekniker som testades var affischering, datorspel, nyhetsbrev och datorbaserad träning. Dessa tekniker visade sig dock enligt undersökningen inte ha samma positiva effekt på medvetenhet. Samtliga tekniker och dess effekt på medvetenhet med utgångspunkt från forskarens femstegsmodell kan ses nedan.

Teknik	Komponent av kunskap	Komponent av attityd	Komponent av normer	Komponent av intentioner	Ändrat beteende	Total effektivitet
Utbildningspresentationer	Ja	Ja	Nej	Ja	Ja	4
Mail	Ja	Ja	Nej	Ja	Nej	3
Gruppdiskussioner	Ja	Ja	Ja	Ja	Ja	5
Nyhetsbrev	Ja	Ja	Nej	Nej	Nej	2
Datorspel	Nej	Ja	Nej	Ja	Nej	2
Datorbaserad träning	Ja	Ja	Nej	Nej	Nej	2
Affischering	Ja	Ja	Nej	Nej	Nej	2

Figur 3 – Metoder för att öka säkerhetsmedvetenhet samt deras effektivitet (Khan *m.fl.*, 2011)

En del i att öka säkerheten inom organisationen är enligt Peltier (2005) genom ett så kallat informationssäkerhetsprogram. Ett informationssäkerhetsprogram som helhet består i sin tur av tre olika delprogram i form av utbildning, träning och medvetenhetsprogram (Peltier, 2005). Informationssäkerhetsprogram är även känt som SETA-program, från engelskans security education, training and awareness (SanNicolas-Rocca, Schooley och Spears, 2014; Burns *m.fl.*, 2015). Ett första steg i ett lyckat informationssäkerhetsprogram är enligt Peltier (2005) ett välarbetat medvetenhetsprogram. Det finns olika synsätt på vad som är en del av just medvetenhetsprogrammet. Peltier (2005) menar att medvetenhetsprogrammets syfte är att sälja in informationssäkerhet och dess program som koncept hos de anställda. Medvetenhetsprogrammet ska förmedla vad som förväntas av de anställda och vart de ska vända sig för assistans samt också se till att de anställda förstår vikten av en god informationssäkerhet. Varken medvetenhetsprogrammet eller informationssäkerhetsprogrammet som helhet ska ses som en engångsföreteelse, utan det är viktigt med årlig uppföljning för att medvetenhetsprogrammet ska uppnå någon effekt. Informationssäkerhetsprogram i form av utbildning, träning och medvetenhet är även ansett som det viktigaste för att lyckas få till en informationssäkerhetskultur (Nasir, Arshah och Ab Hamid, 2017).

De Maeyer (2007) definierar ett medvetenhetsprogram som “an organised and ongoing effort to guide the behaviour and culture of an organisation in regard to security issues”. Vidare förklarar Awawdeh och Tubaishat (2014) att ett medvetenhetsprogram ska motivera och stimulera anställda och påminna dem om de konsekvenser och den inverkan det har om informationssäkerhet inte tas på allvar. Medvetenhetsprogrammet ska uppnå ett ändrat säkerhetsbeteende genom utbildning och påpekandet av viktig information eller relevanta hot. Dessa medvetenhetsprogram kan sedermera också innehålla diverse olika metoder för att förmedla medvetenhet, både formella som informella utbildningsmetoder. Några exempel är bland annat videos, nyhetsbrev, sociala medier, konferenser, föreläsningar, sms, datorbaserad träning, olika tävlingar etc. (Awawdeh and Tubaishat, 2014).

Amankwa, Loock och Kritzinger (2014) har delat upp och särskiljer dessa program baserat på vad de har för syfte, fokus och hur de förmedlas. Fokus av ett medvetenhetsprogram är att rikta uppmärksamhet och påminna de anställda om informationssäkerhet. Syftet är sedermera att de anställda ska förstå sina roller och deras egna ansvar gällande informationssäkerheten för organisationen. Resultatet och uppdelningen som gjordes i studien kan ses i figur 4.

Attribut	Utbildning	Träning	Medvetenhet
Fokus	Insikt och förståelse	Kompetens och kunskap om informationssäkerhet	Rikta uppmärksamhet och påminnelser
Syfte	Göra anställda mer kompetenta gällande informationssäkerhet för att säkerställa konfidentialitet, riktighet och tillgänglighet för organisationens information	Göra anställda mer kompetenta och öka kunskapen baserat på vilka roller och ansvarsområden de har inom organisationen	Säkerställa att varje anställd inser sin roll och det ansvar de har gentemot att skydda organisationens information
Metod för leverans	Teoretiska instruktionsmetoder i form av seminarier, diskussioner i klassrum, och forskning	Praktiska instruktionsmetoder i form av seminarier och studiegrupper	Tryckt och elektronisk media i form av exempelvis videos, flygblad och affischering

Figur 4 – Ramverk för jämförelse av begreppen Informationssäkerhetsutbildning, Informationssäkerhetsträning samt informationssäkerhetsmedvetenhet (Amankwa, Loock och Kritzinger, 2014)

Utöver medvetenhetsprogrammen syftar enligt Amankwa, Loock och Kritzinger (2014) informationssäkerhetsutbildning till att öka den kompetens och kunskap anställda besitter genom att sträva efter en förståelse för de dokument gällande informationssäkerhet som finns. Även informationssäkerhetsträning syftar till att öka kompetensen och kunskapen hos de anställda, men till skillnad från informationssäkerhetsutbildning ska detta enligt Amankwa, Loock och Kritzinger (2014) vara specifikt mot de anställdas roller och de ansvarsområden de har. Informationssäkerhetsutbildning och informationssäkerhetsträning är därav mycket lika varandra, men där det också skiljer sig i att utbildning levereras genom teoretiska metoder och träning levereras genom praktiska metoder.

ISO 27002 (2017) tar upp riktlinjer för informationssäkerhetsåtgärder och i avsnitt 7.2.2 av standarden tas medvetenhet, utbildning och fortbildning vad gäller informationssäkerhet upp. Säkerhetsåtgärden beskrivs som att "alla organisationens anställda och i förekommande fall leverantörer bör erhålla lämplig utbildning och fortbildning för ökad medvetenhet och regelbundna uppdateringar vad gäller organisationens policy, regelverk och rutiner i den omfattning som är relevant för deras befattning". För att uppnå detta bör ett utbildningsprogram fastställas som utöver att policy, regelverk och rutiner, med hänsyn tagen till organisationens informationssäkerhet och de befintliga säkerhetsåtgärder som finns ska ingå, ska det även finnas ett antal kunskapshöjande aktiviteter som exempelvis kampanjer, broschyrer eller nyhetsbrev. Utbildningen ska även ta hänsyn till de olika roller de anställda besitter.

Standarden tar även upp ett antal allmänna aspekter utbildningen bör omfatta:

- Ledningens engagemang för informationssäkerhet inom hela organisationen

- Behovet av att bekanta sig med och följa gällande informationssäkerhetsregler och skyldigheter som är definierade i policy, standarder, författningar, avtal och överenskommelser

- Personligt ansvar för sina egna handlingar och passivitet samt allmänna skyldigheter mot att säkra eller skydda information som tillhör organisationen och externa parter

- Grundläggande informationssäkerhetsrutiner (t.ex. rapportering av informationssäkerhetsincidenter) och grundläggande säkerhetsåtgärder (såsom lösenordsskydd, skydd för skadliga program och renstädat skrivbord)

- Kontaktpunkter och resurser för ytterligare information och råd i frågor gällande informationssäkerhet, inbegripande ytterligare informationssäkerhetsutbildning och utbildningsmaterial

Denna utbildning kan utföras på olika sätt som exempelvis självstudier, webbaserad, distans eller helt enkelt vara klassrumsbaserad som till exempel en föreläsning. Denna utbildning bör sedermera också genomföras regelbundet och när personal är ny eller byter roller.

Hallberg *m.fl.* (2017) menar på att anställdas syn på informationssäkerheten utvecklas genom utbildningar med syfte på att öka medvetenheten och förståelsen för informationssäkerhet inom organisationen. Den gemensamma synen, som uppnås via utbildningar för att öka medvetenheten, anses även vara en viktig del i det som anses vara en informationssäkerhetskultur. Med den definition av säkerhetsmedvetenhet som används i denna studie, tillsammans med tidigare litteratur som finns beskrivet i avsnitt 2.3 samt 2.4, kommer således även utbildningar likaså träning med syfte att öka medvetenhet att räknas in som aktiviteter för ökad säkerhetsmedvetenhet under denna studie. Att medvetenhet innefattar både utbildning och träning är något som även stöds av Siponen (1991) som påpekar att både utbildning och träning är en del i att öka medvetenheten.

Ghazvini och Shukur (2018) tar upp att säkerhetsmedvetenheten i en organisation som en stort bidragande faktor i hur effektiv informationssäkerheten är och säkerhetsmedvetenheten ökas just genom dessa medvetenhetsprogram. För att verkligen ändra på användares attityd behöver dessa program utföras flera gånger samt uppdateras och förbättras, och inte vara en engångsföreteelse, något som det i många fall är (Ghazvini och Shukur, 2018).

Det huvudsakliga innehållet i ett medvetenhetsprogram bör vara organisationens interna säkerhetspolicy, de huvudsakliga hoten mot informationstillgångar, grundläggande skyddsåtgärder samt incidenthantering. Samtidigt är det viktigt att innehållet förstås för att i slutändan kunna uppnå ett ändrat beteende, vilket leder till att feedback blir extra viktigt för att kunna se att anställda faktiskt har förstått det som förmedlas (Ghazvini och Shukur, 2018). Med ett effektivt medvetenhetsprogram kan en förändring i beteende enligt Ghazvini och Shukur (2018) ses redan efter några veckor, men där det kan ta upp emot 3–5 år innan en förändring i kulturen kan ses, vilket även

kräver årlig översikt och uppdatering av programmet för att det hela tiden ska hållas relevant.

Det är enligt Johnson (2006) viktigt att få ledningens engagemang att investera i informationssäkerheten och dessa medvetenhetsprogram. Ett medvetenhetsprogram medför även vissa kostnader, vilket är bra att känna till. Huvudsakligen består dessa kostnader i form av löner för de som jobbar med organisationens säkerhetsmedvetenhet, materialet som krävs men även lärare och lokalkostnader som används. Johnson (2006) tar också upp indirekta kostnader i form av den tid som anställda lägger på att antingen marknadsföra programmen eller helt enkelt den tid som anställda faktiskt spenderar på till exempel kurser. Men Johnson (2006) menar att om fokus väl läggs på att öka medvetenheten finns det ett antal fördelar som kan uppnås för organisationen. Dessa fördelar är bland annat ökat förtroende hos potentiella kunder, ökad trovärdighet och korrekthet av information samt en ökad moral hos anställda vilket i sin tur påverkar produktiviteten i positiv bemärkelse.

3 Problemområde

Ofta är det människan själv som är ansedd som den svagaste länken när det gäller informationssäkerhet. Organisationer kan fokusera hur mycket de vill på tekniska lösningar, de kommer inte komma undan det faktum att människan alltid kommer att stå i centrum när det gäller informationssäkerhet. Nohlberg (2009) menar att oavsett vilken metod som väljs för en attack, kommer det alltid börja och sluta med människan. Vidare menar han även på att många utav de säkerhetsincidenter som skett hade kunnat förhindras om de involverade personerna hade varit mer säkerhetsmedvetna. Detta till trots tenderar organisationer till att fokusera mer på tekniska lösningar utan att i många fall reflektera över den stora del vi människor faktiskt har i informationssäkerhetsarbetet.

Det finns statistik som tyder på att upp mot 75 % av alla säkerhetsincidenter sker inom den egna organisationen av egen personal (D'Arcy, Hovav och Galletta, 2009). Samtidigt finns det studier som visar på att medvetenheten gällande informationssäkerhet har en direkt positiv koppling när det gäller säkerhetsbeteendet hos användarna och följandet av organisationens säkerhetspolicy, både på organisatorisk och individnivå (Alotaibi, Furnell och Clarke, 2017). För att en säkerhetspolicy ska ha någon effekt för organisationen och dess anställda menar forskaren även på att all personal behöver bli kontinuerligt uppdaterade gällande medvetenheten genom medvetenhetsträning och utbildning.

Det är alltså viktigt att alla organisationer jobbar med sina medarbetares säkerhetsmedvetenhet. En undersökning av Ernst & Young (2009) visar att trots att en majoritet av organisationerna har medvetenhetsprogram, har mindre än hälften inkluderat delar i sina program som berör exempelvis uppdateringar av aktuella hot, heta ämnen eller speciella aktiviteter för högriskgrupper inom organisationen. Med andra ord är dessa medvetenhetsprogram inte på den nivå de hade kunnat vara för att uppnå den önskade effektiviteten. Samtidigt är det enbart 20% av de deltagande i undersökningen som faktiskt mäter effektiviteten av sina program och utför modifieringar därefter. De hot som finns är inte statiska, de ändras, precis som teknologi. Därför är det viktigt att inte enbart luta sig mot gammal kunskap utan att hela tiden öka medvetenheten. Om inget görs för att öka medvetenheten eller att uppdatera medarbetare genom medvetenhetsprogram som faktiskt är aktuella för dagens hot kommer det tillslut enbart vara utdaterad kunskap människorna besitter och i och med det kan medvetenheten i slutändan försvinna.

3.1 Syfte och frågeställning

Syftet med studien är att få en ökad kunskap i hur säkerhetsföretag jobbar för att öka den egna interna medvetenheten. De företag som arbetar inom säkerhetsbranschen bör ha både kunskapen och resurserna för att ligga i framkant när det gäller ökandet av den egna personalens interna medvetenhet. Det handlar bland annat om vilka metoder de använder för att göra personalen medvetna om den informationssäkerhetspolicy som finns, men också allmänt om hur de får sina medarbetare till att ha ett större säkerhetstänk rent generellt, då medvetenhet som tidigare nämnts definieras som förståelse, kunskap och attityd gentemot informationssäkerhet. Om viktiga aktiviteter kan hittas från företag som rent hypotetiskt bör ha bättre kunskaper om

informationssäkerhet och därigenom också förutsättningar för att lyckas med att på ett effektivt sätt upprätthålla medvetenheten inom organisationen, kan också dessa aktiviteter eventuellt bli grundstenar att utgå från för övriga organisationer som inte haft samma förutsättningar att komma lika långt i processen.

Kan viktiga parametrar på hur ökandet av medvetenhet hittas kan ekonomiska förluster även undvikas. Det kostar att göra fel, så gör rätt från början.

Med utgångspunkt i syftet med arbetet har följande frågeställning formulerats:

- Hur arbetar säkerhetsföretag med att höja sina medarbetares säkerhetsmedvetenhet?

3.2 Avgränsningar

Denna studie kommer att rikta sig mot företag som på ett eller annat sätt arbetar med informationssäkerhet. Anledningen till att avgränsningen görs mot just säkerhetsföretag är av den anledningen att de rent hypotetiskt borde ha kunskapen för att göra ett bra jobb då de arbetar inom säkerhetsområdet. Med säkerhetsföretag och säkerhetsområdet menas företag som jobbar med informationssäkerhet på det sättet som beskrivs i kapitel 2.1 och som finns illustrerat i informationssäkerhetsmodellen i figur 1. Hypotetiskt bör dessa företag också ha större krav på sig då de eventuellt arbetar med klassificerad information vilket gör att ett effektivt informationssäkerhetsarbete är av stor vikt, där medvetenhet som tidigare klargjorts är en stor del. För att också öka sannolikheten att kompetenta företag undersöks kommer avgränsningen mot större företag att göras. Chansen att lite större företag med många anställda på många olika avdelningar har både behovet men också svårigheten att uppnå en medvetenhet gör just större företag intressant.

Medvetenhet handlar om människor och beteenden och därav kommer undersökningen också befinna sig i den administrativa delen gällande informationssäkerhet. Tekniska detaljer som inte har med medvetenhet att göra kommer därför inte att tas hänsyn till.

3.3 Förväntat resultat

Det förväntade resultatet av denna studie är en sammanställning av de aktiviteter som säkerhetsföretag jobbar med för att öka den egna interna medvetenheten inom organisationen. Om säkerhetsföretag är bättre på att jobba med den interna medvetenheten kanske dessa aktiviteter kan tillämpas även på organisationer inom andra typer av branscher. Detta kan bidra till att dessa företag får både inspiration och viss vägledning i sitt eget arbete när det gäller att öka sin säkerhetsmedvetenhet. Antingen kan andra organisationer lära sig av dessa resultat och ta lärdomar från experter för att öka sina egna resultat inom sina egna verksamheter, alternativt kan det vara bra med förståelsen för att det finns en väg att gå även för de som jobbar inom området.

4 Metod

Detta kapitel berör de metoder som har valts och argumentering bakom valen. Kapitlet berör även den egna tillämpningen och hur genomförandet sedan har skett utifrån de valda metoderna.

4.1 Val av metod

Det finns i huvudsak två olika metoder för att utföra forskningsstudier på. Dessa är den kvalitativa samt den kvantitativa metoden. Den kvalitativa forskningsmetoden syftar till att få en helhetsförståelse och söker efter beskrivande data, det handlar om att systematisera kunskap om något som kännetecknar ett fenomen (Olsson och Sörensen, 2007). Det handlar även om ett inifrånperspektiv med en närhet till undersökningsproblemet och försökspersonerna, där resultaten går in på djupet av ett problem. Kvantitativ metod däremot har ett utifrånperspektiv med en distans och oftast kortvarig eller ingen kontakt alls med försökspersonerna, där resultaten är generella. Kvantitativ forskning är oftast hypotesprövande som utgår från en teori grundad på tidigare forskning (Olsson och Sörensen, 2007).

Frågeställningen grundar sig i att ta reda på hur säkerhetsföretag arbetar för att öka medvetenheten, vilket kräver en djupare kunskap och en helhetsförståelse. Därför har denna studie utgått från en kvalitativ forskningsmetod. Utöver att den kvalitativa forskningsmetoden har tillämpats, har studien även fokuserat på en induktiv ansats, även kallad upptäcktens väg (Holme och Solvang, 1997). Detta är också det som normalt är ansett som den kvalitativa ansatsen, medan en deduktiv ansats är ansett som mer kvantitativ (Patton, 2002). Detta innebär att forskningsarbetet har utgått från empirisk data för att sedan sammanföra och sammanställa upptäckterna till de olika aktiviteter som används för att öka medvetenheten i säkerhetsföretag.

4.1.1 Datainsamlingsmetod

En kvalitativ metod innebär i sin tur olika datainsamlingstekniker. I den här studien har valet fallit på att utföra en intervjustudie för att samla in den data som krävs. Det finns enligt Denscombe (2010) tre olika typer av intervjustrukturer i form av strukturerade, semistrukturerade samt ostrukturerade intervjuer.

- Strukturerade intervjuer innebär en hög kontroll av både de frågor som ställs och de svar som söks. Mycket likt den kvantitativa enkäten är samtliga frågor fördefinierade. Det är också mer kvantitativ data som söks och en strukturerad intervju kan ses som standardiserad.

- Semistrukturerade intervjuer är mer flexibel än den strukturerade intervjun. Här finns dock fortfarande fördefinierade frågor som forskaren vill ha svar på, men där fokus ligger på den intervjuade personen att kunna utveckla och gå in djupare på områden som är av specifikt intresse. Även följdfrågor kan med fördel ställas i en semistrukturerad intervju baserat på de svar som erhålls för att få tag på än djupare kunskap.

- Ostrukturerade intervjuer är den intervjutypen som logiskt nog har minst struktur. Här kan intervjuaren starta samtalet med ett övergripande tema och sedan får respondenten prata fritt utifrån temat och intervjun får utveckla sig själv.

Denscombe (2010) menar också på att både den semistrukturerade och den ostrukturerade intervjun har ett upptäckande syfte, medan den strukturerade intervjun har ett mer granskande syfte. Studien utgår från att upptäcka aktiviteter som säkerhetsföretag jobbar med, vilket innebär att semistrukturerade intervjuer med ett upptäckande syfte varit önskvärt (se kapitel 4.2.4). Vidare har dessa aktiviteter samlats in från olika företag, vilket innebär att en viss struktur kan vara fördelaktig för att säkerställa att alla önskade punkter tas upp vid varje enskild intervju. Samtidigt är det viktigt att de svaren som söks samt de frågor som ställs inte är helt standardiserade för att garantera att nya upptäckter faktiskt kan göras och de intervjuade personerna kan gå in djupare på de delar som de faktiskt fokuserar mest på. Med den bakgrunden har semistrukturerade intervjuer använts för datainsamling.

4.2 Genomförande

4.2.1 Litteratursökning

För att få en grund att stå på har litteratursökning genomförts där information samlas in från flertalet olika källor som exempelvis böcker och vetenskapliga artiklar. Den litteratur som har samlats in har blivit underlag för den bakgrund som studien har utgått från samt de intervjuer och den analys som har genomförts.
När litteratur samlas in och analyseras är det enligt Webster och Watson (2002) viktigt att använda sig av relevant litteratur och inte begränsa sig till att söka artiklar från en forskningsmetod, en uppsättning tidskrifter eller att begränsa sig till en geografisk plats. Vidare menar Berndtsson *m.fl.* (2008) att en kombination av referensdatabaser samt tidskrifter och konferensbidrag kan användas för att säkerställa att relevant litteratur används.
De databaser som har använts vid litteratursökningen är framförallt IEEE Xplore samt ACM Digital Library, men där även Google Scholar har använts. Sökord som använts för att få fram artiklar av relevans har varierat men där informationssäkerhet allt som oftast varit grunden i kombination med sökord som exempelvis medvetenhet, beteende, mänsklig faktor samt deras engelska översättningar. Samtidigt har ingen begränsning gjorts till den litteratur som eftersöks när det gäller geografiska platser eller forskningsmetoder.

4.2.2 Frågekonstruktion

För att säkerställa att den kvalitativa data som samlas in från intervjuerna också är av kvalitet är det viktigt att konstruera frågorna på ett sådant sätt att de möjliggör svar som går in på djupet och är förklarande. Om frågor ställs där svaren enbart blir "ja" eller "nej" blir det heller inga svar som kommer gå att göra någon vidare kvalitativ analys på. Enligt Patton (2002) är det därför viktigt att använda sig utav så kallade öppna frågor för att få ut mer beskrivande svar från intervjupersonen. En öppen fråga är en sådan fråga som helt enkelt ger möjligheter till ett djupare svar och reflektioner från den intervjuade personens sida. Snarare att fråga "gör ni det här?", som inte uppmanar personen att ge ett utförligt svar, kan en öppen fråga som exempelvis "hur gör ni det här?" eller "varför

gör ni det här?" användas istället. Detta kommer uppmana intervjupersonen att återge sin egen erfarenhet och förståelse med sina egna ord, vilket är precis det som eftersöks i den kvalitativa intervjun (Patton, 2002). Detta sätt att utforma frågor på tillsammans med den litteratursökning som genomförts är det som använts för att konstruera de frågor som använts under denna studie. Samtliga intervjuer som förkonstruerats inför intervjuerna kan ses i bilaga 1.

4.2.3 Urval

Målet med intervjuerna är att få en klar bild över hur företagen jobbar för att öka medvetenheten. Därför har det varit viktigt att minst en person inom varje företag som deltar i intervjun har något typ av ansvar eller kunskap när det gäller informationssäkerheten inom organisationen. Dessutom är det en fördel om personer på olika nivåer inom företaget kan intervjuas, då perspektivet utifrån de olika rollerna kan skilja och att de också uppfattar saker olika. Intervjuer med personer utöver de med inblick i informationssäkerhetsarbetet kan ses som komplementära intervjuer då huvudsaken har varit att samla in data om hur de, officiellt, men kanske också inofficiellt, arbetar för att öka säkerhetsmedvetenheten. Dessa komplementära intervjuer kan dock bidra positivt i syftet att analysera den insamlade data då det i vissa fall kan skilja mellan den planen företagen har och hur det faktiskt uppfattas och tas emot av resterande anställda. Sammanlagt har fem respondenter intervjuats från tre olika företag där deras roller varit bland annat informationssäkerhetskoordinator, lokalt säkerhetsansvarig, informationssäkerhetskonsult, gruppchef och regionchef.

Vidare har intervjuerna även skett med endast en person åt gången. Det finns enligt Denscombe (2010) ett antal fördelar med att utföra intervjuer en och en och tar upp fyra olika fördelar. Bland annat är det lättare att få till intervjuer då endast en person behöver planeras in åt gången. En annan fördel är att åsikterna endast kommer från en person och de påverkar inte varandra i deras svar eller åsikter, vilket gör det enkelt att särskilja på vad som kommer från vilken person. Det blir även lättare att genomföra intervjun av den anledningen att endast en person behöver tas hänsyn till vilket bidrar till att intervjun som helhet blir lättare att kontrollera. Den sista fördelen som tas upp handlar om när intervjun är klar och transkribering ska ske. Det blir betydligt enklare att transkribera en intervju om det enbart finns en intervjuperson. Är intervjun exempelvis inspelad finns endast en röst utöver sin egen att ta hänsyn till. Därav behöver problemet att urskilja från vem ett svar kommer från aldrig uppstå.

Även om det rent praktiskt hade varit möjligt att genomföra gruppintervjuer inom någon organisation har detta inte genomförts av den anledningen att svaren blir svårare att sammanställa då det kan bidra till skillnader i typen av svar som samlas in. Det skulle även kunna leda till svårigheter att utföra analysen då datainsamling har skett på olika sätt vilket i sin tur kommer påverka trovärdigheten negativt.

4.2.4 Datainsamling

Som nämnts i kapitel 4.1.1 har semistrukturerade intervjuer genomförts. Sammanlagt har fem olika intervjuer genomförts på tre olika företag. Intervjuerna har tagit mellan 30–70 minuter. De allra flesta intervjuer har skett på plats hos företagen för att göra det så enkelt som möjligt för den intervjuade personen. Samtidigt har det varit fördelaktigt då samtliga företag har haft ett avskilt rum som har gått att stänga vilket har undvikit

onödigt buller som stör intervjun. Under ett fall har respondenten dock inte varit tillgänglig för att genomföra intervju på plats och i detta fall har Skype använts som hjälpmedel. För att förenkla analys har de flesta intervjuer spelats in förutom vid de tillfällen då respondenten har uttryckt en önskan om att inte bli inspelad. I de tillfällen då inspelning inte varit möjligt har fältanteckningar tagits istället för att använda teknologiska hjälpmedel. Vid de tillfällen där det tillkommit frågetecken eller där det under analystillfället har märkts att något skulle kunna förklaras ytterligare har kompletterande frågor skickats via mail.

4.3 Analys av data

För att analysera den data som har samlats in har en innehållsanalys genomförts. Denscombe (2010) menar att en innehållsanalys generellt följer en logisk och relativt okomplicerad process. Denna processen består av att först välja ut den text som ska analyseras för att sedan brytas ner och välja ut mindre komponenter som exempelvis ord eller meningar i texten som är grund för analysen. Därefter ska relevanta kategorier skapas utifrån vad syftet med analysen är för att sedan koda texten och välja ut de ord eller meningar som har betydelse och kategorisera dessa som blir enheter för analys. Därefter sker en notering av hur ofta dessa noteringar förekommer för att sedan analysera dessa kategorier mer i detalj.
Efter att intervjuerna hade skett påbörjades transkribering av det inspelade materialet. Vid de tillfällen då inspelning inte var möjligt har ingen transkribering skett utan då har enbart fältanteckningar använts för analys, i och med att det inte funnits något inspelat material att transkribera. Efter att intervjun transkriberats påbörjades kodningen där ord eller meningar som varit av betydelse har markerats.

4.4 Etiska aspekter

När forskning genomförs är det viktigt att ta hänsyn till de etiska aspekter som finns. Olsson och Sörensen (2007) förklarar att personer som ingår i forskningsprojekt skyddas av olika regelverk där konfidentialitet, sekretess och anonymitet är viktiga aspekter att ta hänsyn till. Konfidentialitet och sekretess syftar till säkerhet för personer som ingår i undersökningen genom att säkerställa att obehöriga inte ska kunna ta del av informationen. Anonymitet finns om data som framtagits inte kan kopplas till enskilda individer. Utöver dessa aspekter tar Olsson och Sörensen (2007) även upp fyra principer för etik gällande forskning i form av autonomiprincipen, godhetsprincipen, principen att inte skada samt rättviseprincipen. Autonomiprincipen innebär att deltagare har rätt till självbestämmande samt förmågan att självständigt ta ställning till information och handlingsalternativ. Godhetsprincipen innebär en strävan efter att göra gott och förebygga eller förhindra skada. Principen att inte skada innebär att inte utsätta någon för skada både vad gäller psykisk eller fysisk skada. Rättviseprincipen innebär att alla personer som deltar i studien ska behandlas lika i den mån det är möjligt.
Att studien har genomförts inom säkerhetsbranschen innebär i sin tur ökad vikt av de krav gentemot de etiska aspekter som finns. För att säkerställa att etiska aspekter har följts har alla företag samt personer som deltagit i studien varit anonyma, samtidigt som de inför varje intervju har blivit meddelande om de etiska aspekter som gäller. Att nämna personer eller företag vid namn är inte relevant för att kunna ge svar på den frågeställning som finns och därefter även förstå resultatet. Därför kommer inga namn på varken respondenter eller företag att användas, samtidigt som citat som kan kopplas till en specifik individ inte kommer att skrivas ut. Syftet med studien har även förklarats tydligt för alla som har ett deltagande i studien för att säkerställa att de vetat om vad

som förväntats av dem samt hur svaren kan komma att användas. Förmedlingen av syftet med studien har först delgivits vid den initiala kontakten via mail för att sedan upprepas väl på plats inför varje intervju. Deltagarna har alltid haft rätten att neka inspelning av intervjuer, vilket i vissa fall har skett, och i slutändan har det alltid varit deltagarna själva som har haft ett eget självbestämmande om hur deras inblandning ska gå till.

Även Vetenskapsrådet (2002) tar upp etiska principer som är viktiga att följa under forskningsstudier. Fyra huvudkrav beskrivs i form av informationskravet, samtyckeskravet, konfidentialitetskravet samt nyttjandekravet. Informationskravet innebär att forskaren ska informera de som deltar i studien om syftet av studien, vilket följs då syftet av studien både beskrivs i den inledande kontakten samt innan intervjutillfälle. Samtyckeskravet innebär att de som deltar i undersökningen har rätt att själva bestämma över sin medverkan. Detta följs genom att respondenterna hela tiden haft ett eget bestämmande om både att delta och hur deltagandet sker, exempelvis gällande inspelning av intervjuer. Konfidentialitetskravet innebär att deltagande personers uppgifter ska hållas konfidentiellt. I och med att varken deltagande företag eller respondenter nämns vid namn uppfylls detta krav. Nyttjandekravet innebär att de uppgifter som samlas in om enskilda personer enbart får användas i forskningssyfte. Den information som samlas in angående både företag och personer kommer att förstöras efter studiens avslut och kommer enbart användas i den mån det är nödvändigt för studiens syfte.

5 Materialpresentation

5.1 Företag A

I företag A har en respondent intervjuats. Respondenten är lokalt säkerhetsansvarig och ansvarar för den säkerhet som finns på det lokala kontoret. Samtidigt ansvarar respondenten för att rapportera till säkerhetschefen samt se till att den personal som finns på kontoret har gått de utbildningar som krävs.

5.1.1 Informationssäkerhet

Respondent 1 förklarar att det som är sagt inom organisationen gällande externa och interna hot är att de största hoten mot organisationen beror på vad de gör, men de allra svåraste hoten att komma åt för organisationen är de interna hoten som finns. För att minska risken för interna hot med uppsåt, genomför de säkerhetsintervjuer samt registerkontroller på varje person de anställer. Detta görs enligt respondent 1 för att säkerställa att det inte är en person som har fog för att bli utsatt för påtryckningar, utan att det är en person de faktiskt kan lita på.

> *"På det här företaget så har vi i och med att vi anser att även ett internt hot är ett hot, säkerhetsintervjuer med alla människor som vi anställer och de flesta, i alla fall på det här kontoret, genomför vi även en registerkontroll på. Blir man underkänd på den registerkontrollen så är det inte särskilt troligt att man blir anställd här, beroende på vilka uppdrag man ska jobba mot. Men vi har många kunder som kräver att man har någon typ av riskkontroll på olika nivåer."* - Respondent 1

5.1.1.1 Uppdatering

Respondent 1 säger att de för att uppdatera sig om nya hot har inom koncernen en stor säkerhetsorganisation med representanter från de olika företagen. Denna har i sin tur en omvärldsspaning och mycket utav de hoten som är omhändertas i den. Respondent 1 säger även att de utöver säkerhetsorganisationen även har en koncerngemensam IT-organisation som även den har ett visst ansvar när det gäller uppkomsten av nya hot.

> *"Vi har en ganska stor säkerhetsorganisation inom koncernen som vi tillhör och där finns ett ganska tätt samarbete mellan de olika delarna. Så de har ju en omvärldsspaning. Mycket utav de hoten som är omhändertas i den. Vi har en IT-organisation som också är koncerngemensam, ganska mycket omhändertas där."* - Respondent 1

5.1.1.2 Prioritering

Det finns enligt respondent 1 inte någon upplevd prioritering på något specifikt område när det gäller informationssäkerheten. Däremot påpekar respondent 1 att det från högsta ledningshåll säkert finns en prioritering, men där det inte upplevs som att det finns någon prioritering. Detta är medvetet då de inte vill säga att något inom informationssäkerhetsområdet är mindre viktigt. Det skyltas dock inte med de tekniska

lösningarna, utan om någon egentligen fokusering sker är det i sådant fall mot människorna.

> *"Jag tror man ska säga att det inte är någon fokusering på någon del utan det är lika viktigt."* - Respondent 1

> *"Om du frågar någon som är IT-säkerhetschef så säger de säkert att det finns en prioritering men vi upplever inte att det är det egentligen för då säger vi också att om vi prioriterar någonting så säger vi också att någonting inte är lika viktigt."* - Respondent 1

> *"... vi skyltar inte så mycket med de tekniska lösningarna utan de vi i så fall fokuserar på är personerna. Men jag skulle säga att vi egentligen inte fokuserar på något utan tycker det är lika viktigt att vi får med både den tekniska lösningen och handhavaren."* - Respondent 1

5.1.1.3 Ansvar

Respondent 1 berättar att det formella ansvaret kring informationssäkerhet är en ansvarig på koncernnivå, samt en informationssäkerhetschef för varje företag. Inom företag ingår informationssäkerhetschefen sedan i en säkerhetsgrupp där bland annat en säkerhetschef ingår, men för informationssäkerhet är det enbart en som är formellt huvudansvarig på företagsnivå, vilket är informationssäkerhetschefen. Företaget trycker enligt respondent 1 väldigt mycket på att det inte är en persons ansvar att hålla säkerheten, utan att varje individ har sitt egna ansvar. Detta innebär att även om den formella fördelningen är att det finns en informationssäkerhetschef, är det informellt allas ansvar att se till att det finns en god informationssäkerhet i företaget. Respondent 1 utvecklar att just det här individuella ansvaret är något de inom företaget trycker mycket på, bland annat i de utbildningar de genomför, för att få alla att förstå att alla har sitt eget ansvar i att skydda företagets information.

> *"På koncernnivå finns det en som är ansvarig, sen har respektive företag en informationssäkerhetschef och det är egentligen han som är i huvudsak ansvarig för att vi följer de bestämmelser som är. Men sen finns det ett ansvar hos den enskilde medarbetaren också. Dels att faktiskt göra rätt men också att anmäla när man upptäcker att det är något som är fel."* - Respondent 1

5.1.1.4 Konsekvenser

Om säkerhetsregler bryts beskriver respondent 1 att det finns vissa disciplinära åtgärder som kan tas tillhanda. Just nivåerna av dessa åtgärder är enligt respondent 1 troligtvis inte kända för samtliga anställda utan det som är känt är att det faktiskt finns åtgärder. Om det är något mindre fel som görs kan varningar ges ut vilket i sin tur skulle kunna leda till ett visst löneavdrag. Är det dock något större skulle en polisanmälan kunna göras, beroende på vad det är för något som görs. Respondent 1 förklarar att om något i säkerhetsreglerna bryts görs först en utredning för att sedan komma fram till vilken typ av åtgärd som är passande i just det specifika fallet.

> *"Vi kan ge varningar för olika saker och det kan innebära olika saker,*

löneavdrag kan vara en del. Men är det tillräckligt tydligt och inte bara något litet slarv då är det polisanmälan för då har man brutit mot regler och vi är ganska noga med det här eftersom många av våra affärer som vi gör, vi har ett stort krav på oss att följa säkerheten och gör vi inte det så har ju vi brutit." - Respondent 1

5.1.1.5 Ökat engagemang

Respondent 1 säger att en del i att få anställda mer engagerade när det gäller informationssäkerheten ligger i de utbildningar som företag har. Sedan kommer det ut vissa informationsfilmer med jämna mellanrum. Ibland körs vissa kampanjer, eller så kommer allmän information ut på intranätet i syfte att påminna anställda som kanske inte jobbar dagligen med informationssäkerhet att tänka på vissa saker som har med informationssäkerhet att göra. Sedan påpekar respondent 1 att de begränsningar och tekniska åtgärder som finns påminner anställda om att säkerheten faktiskt är viktig. Till exempel övervakas allt de gör på datorerna, vilket alla vet om samtidigt som det framgår att övervakning sker när anställda bland annat går ut på internet på deras jobbdatorer.

"En del i det är att man genomför utbildning. Sen tror jag vi gör på olika sätt inom företaget. På just den här delen där vi sitter på det här kontoret där väldigt många håller på med mjukvaruutveckling i säkerhetskritiska system är den del av vardagen, då vet man att det finns krav på riktighet och annat sånt där." - Respondent 1

"... vi kör med jämna mellanrum nya informationsfilmer. Till exempel som vi har haft nu i höstas, där vi kör en uppsnäppning på det här. Det brukar komma ut, ibland regelbunden information på vårt intranät att glöm inte det här eller man kör någon kampanj, just för att de som normalt sett inte jobbar med det ska påminnas hur det är." - Respondent 1

5.1.2 Säkerhetsmedvetenhet

En hög medvetenhet hos anställda anses enligt respondent 1 vara av största vikt då tekniska lösningar löser en del, men att det ibland inte spelar någon roll om människan bakom gör fel, då det oftast går att komma runt den tekniska lösningen. En del i att göra anställda mer säkerhetsmedvetna tror respondent 1 är just begränsningar som tidigare nämnts. Ett annat exempel utöver övervakning är det faktum att samtliga personer som befinner sig i lokalerna behöver registrera sig. Det leder till att budskapet om att säkerheten är viktig kommer fram direkt. Finns det väldigt tydliga begränsningar som i fallet med registrering för att ta sig in i lokalen eller övervakning av vad som görs på internet, får det personalen att tänka till varför det behöver vara lite krångligt.

"Jag tror att ibland så höjer man säkerhetsmedvetenheten genom att göra begränsningar så att man vet om att allting inte är tillåtet. Som hos oss här till exempel så måste du registrera dig, då höjer vi din säkerhetsmedvetenhet, det är inte bara att komma och gå." - Respondent 1

5.1.2.1 Säkerhetskultur

Att låsa igen lokalerna lite extra tillsammans med utbildningar är något som respondent 1 tror är en bidragande orsak till att få till en säkerhetskultur vilket i sin tur ökar

medvetenheten. Att ha en säkerhetskultur anses i vissa fall vara ett varumärke för att kunna påvisa hur säkra de är. Utöver det fysiska som exempelvis låsta lokaler anses en sådan sak som utbildningar bidra till en ökad säkerhetskultur, då det är människan som krävs för att kunna förändra kulturen. Sedan förklarar respondent 1 att de till varje nyanställd har en introduktion där en utav punkterna är just säkerheten. På det här kontoret går de igenom den väldigt noga, med uppföljningskontroller de första veckorna eller månaderna av en anställning, för att säkerställa att personen förstår tillämpningen av bestämmelser. Detta är ytterligare en sak som enligt respondent 1 både ökar säkerhetsmedvetenheten, men även får in nyanställda i den kultur som finns direkt.

> *"Jag kan bara svara för det här kontoret, men vi har till varje nyanställd en intro. Det är centralt och där är en av punkterna säkerhet. På det här kontoret går jag igenom den punkten väldigt noga och dessutom har en uppföljningskontroll på det de närmaste veckorna, månaderna så man förstår att personen har fattat tillämpningen av bestämmelser och gör det på ett acceptabelt sätt. På det sättet får man in folk i den kultur som det ska vara."* - Respondent 1

5.1.2.2 Standard och policy

Respondent 1 berättar att den del av företag som de tillhör är certifierade enligt ISO 27000 serien och företaget som helhet är igång med att bli certifierade. Att följa standarden innebär för den vanlige anställda att helt enkelt gör som de blir tillsagda. Skillnaden ligger mer på ledningshåll att ha en process för bland annat risk och konsekvensanalyser, vilket inte alla är en del av. I övrigt är det att göra det till en naturlig del i övrig verksamhetsledning.

> *"För vissa delar på företaget här så är det bara att göra som du är tillsagd att göra egentligen. Det är mer att vi har grepp på vilka informationstillgångar vi har, hur vi ska skydda dem, hur vi gör idag, vad är risk, alltså det här med risk och konsekvensanalyser, sen det här med förbättringar. Men att man har en process för det där."* - Respondent 1

Den säkerhetspolicy som finns menar respondent 1 att det är viktigt att inte bara delge som den är, utan att göra någon typ av sammanfattning för att det inte ska bli för svårt att förstå den. respondent 1 förklarar att det innebär att det inte är policyn som sådan som förmedlas, utan tillämpningen av hur den ska följas som förmedlas. Vad policyn innebär är en del av den utbildningen som finns. Om det är några ändringar som sker i policyn vilket innebär att de behöver tänka eller göra på något annat sätt för att uppfylla den har de enligt respondent 1 tre olika kanaler för att sprida informationen om detta. Det som är standardiserat är intranätet, men utöver det går de även ut med mail samt sätter upp lappar i fikarummet där innebörden av förändringen förmedlas. Utöver det är även en sammanfattning av policyn en del av den säkerhetsutbildning som finns.

> *"Ibland när det blir förändringar, antingen går man ut på intranätet eller som ibland på det här kontoret sitter det en lapp på fikarummet att nu är det så här och nu måste vi göra på det här sättet."* - Respondent 1

"... vi har tre sätt, jag går ut med mail, vi tar intranätet och vi kör papper, det är liksom de tre." - Respondent 1

5.1.2.3 Informationsspridning

Respondent 1 säger att den stora informationsspridningskällan är intranätet, men det kan skilja sig åt beroende på vilken information som ska spridas vilken kanal de använder. På intranätet finns bland annat regelverk som de är, men det finns även beskrivet i text hur tillämpning sker. Respondent 1 är tydlig med att det är viktigt att bryta ner regelverk, policys eller andra bestämmelser för att minska graden av tolkning och göra det tydligare vad dessa olika dokument i praktiken faktiskt innebär för de anställda. Samtidigt som det finns en nedbruten, tydligare text med en beskrivning av hur tillämpningen sker av regelverk eller policy, finns dessa även i sin helhet att tillgå på intranätet. Sker större förändringar kan en ändring av säkerhetsutbildningarna ske eller så kan de gå ut med en ny säkerhetsfilm. Just säkerhetsfilmer är även något de använder sig av. Ibland skickar det ut vissa säkerhetsfilmer som alla måste se och senaste gången en sådan kom ut skulle de även diskutera den i grupp efter att ha sett den. Dessa videoklipp är oftast 10–15 minuter långa och fokuserar specifikt på att öka just säkerhetsmedvetenheten. Förutom intranätet använder de enligt respondent 1 som tidigare nämnts i kapitel 5.1.2.2 även mail och affischering i form av de lappar de sätter upp i fikarummet samt att de som jobbar centralt med säkerheten och alla lokalt säkerhetsansvarig har månadsmöten där alla samlas, vilket även det är ett sätt att sprida information enligt respondent 1.

"Den stora informationsspridningskällan är vårt intranät. Det är att man för till exempel säkerhet eller informationssäkerhet, på den sidan, dels har de regelverken som finns men också skriver i text hur tillämpar vi regelverket i så fall. Man behöver bryta ner dem för att se, hur gör vi? För en del regelverk kan man tolka på flera sätt, så därför behöver man då bryta ner och säga, för att följa det här regelverket ska vi göra på följande sätt, och då har vi framförallt intranätet." - Respondent 1

5.1.2.4 Utbildningar

När det gäller utbildningar berättar respondent 1 att det finns ett grundpaket som alla måste gå. Beroende på befattning finns det även ytterligare utbildningar som behöver genomföras, exempelvis finns det en säkerhetsutbildning för de som är chefer. Respondent 1 förklarar att de mesta av utbildningarna är E-learning, men två gånger per år genomförs något som kallas för kursveckan där det genomförs utbildningar med olika fokus. Dessa utbildningar är lärarledda och i sal. En utav de utbildningar som finns kallas enligt respondent 1 för just informationssäkerhet och pågår under två dagar. Respondent 1 förtydligar att detta dock är en fördjupad kurs och något som personalen kan gå för att fördjupa sina kunskaper efter att de gått de grundläggande utbildningarna. Med andra ord är de inte obligatoriska. På kontoret där intervjun genomfördes har väldigt många gått den enligt respondent 1, då de jobbar mycket mot just informationssäkerhet.

"I vårt utbud av utbildningar finns ett grundpaket som alla ska gå. Sedan beror det till exempel på vad man har för befattning, så finns det andra utbildningar

som du också måste gå. Sen har vi vissa ställen där vi säger att vi ska gå fördjupade informationssäkerhetsutbildningen. Då pratar vi mest E-learningdelar." - Respondent 1

Enligt respondent 1 har de utbildningar som är E-learning efter att den är genomförd ett antal frågor som måste besvaras och klaras för att bli godkänd. Dessa resultat sparas sedan för att kunna se hur många det är som är godkända samt hur ofta personalen har gått utbildningarna. Respondent 1 utvecklar att det sedan finns fördjupningskurser även inom E-learning som personalen kan gå om de är intresserade av att ytterligare fördjupa sina kunskaper efter de obligatoriska utbildningarna. Dessa utbildningar behöver generellt göras om på nytt inom ett, två eller tre-årsintervall, beroende på vilken kurs det är. Kurserna kan som tidigare nämnts utföras när de har tid eller själva känner för det, vilket skapar ett rullande och att konversationer angående utbildningarna får en kontinuitet. Det är enligt respondent 1 linjechefernas ansvar att se till att de anställda genomför utbildningarna med de intervall som krävs. En översyn av utbildningarna genomförs med jämna mellanrum för att säkerställa att innehållet är relevant. Samma sak gäller resultaten som kommer från utbildningarna med hur många det är som har genomfört och blivit godkända på utbildningarna.

"... dels blir det ju det här att vi gör en översyn av utbildningarna, av vad det är som har ändrats och vad som är relevant. Det behöver man göra med jämna mellanrum så att dem ändras. Sen blir det en utvärdering kopplat till hur många det är som har genomfört och om dem är godkända. Där är det också så att det flesta av de här kopplat till säkerheten så behöver man göra dem, det räcker inte med att man gjorde dem första veckan och blev anställd utan man ska förnya dem här. Då har vi ett rapportsystem för det så att man vet när dem genomfördes senast och om det är två års, tre års eller varje årsintervall på den kursen. Det beror lite på vad det är för någonting." - Respondent 1

Den säkerhetskurs som är obligatorisk för samtliga anställda innehåller enligt respondent 1 delarna informationssäkerhet, anläggningssäkerhet, personalsäkerhet, resesäkerhet samt incidenthantering. Den delen som handlar om informationssäkerhet tar upp tillgänglighet, riktighet, sekretess och spårbarhet och hur de kan tillämpa dessa för att på bästa sätt skydda sin information. Utöver den mest grundläggande säkerhetskursen förklarar respondent 1 att det finns vissa andra kurser som även är obligatoriska och som rör informationssäkerhet. Dessa är kurserna "E-post & anti-phishing", "Out of office security" samt "Security on the Web". I utbildningsmaterialet finns även företagets säkerhetspolicy, där de har gjort en sammanfattning av den för att den lättare ska förstås. Sedan finns det även en fördjupad informationssäkerhetsutbildning som innehåller fyra olika block i form av varför de ska säkra sin information, vad är informationssäkerhet, företagets ledningssystem för informationssäkerhet och slutligen tips för medarbetarna. Den fysiska kursen som sker under två dagar med fokus på informationssäkerhet innehåller bland annat delar om angrepp och hot, digitala spår, internet och sociala medier, kryptering, mobila enheter, skydd samt säkerhet i utvecklingsprocessen. Respondent 1 berättar att utbildningen av personal gällande informationssäkerheten börjar från den första dagen att den är anställd i och med att säkerheten är en stor del i det introduktionsprogram som finns.

Just utbildningarna anses enligt respondent 1 vara den viktigaste aktiviteten som görs för att öka medvetenheten. Anledningen är att det blir ett rullande och att diskussioner sätts igång i och med det faktum att inte alla anställda gör dessa samtidigt. Även fördjupningarna görs på ett rullande sätt vilket gör att diskussionen på det sättet blir levande inom företaget.

> *"En del är den här utbildningen och där är det så att i och med att man gör dem vid olika tillfällen så kommer ibland samtal upp i fikarummet kopplat till det. För nu har någon gått den här utbildningen och så säger någon till någon annan, den här frågan, kommer du ihåg den? Och där är diskussionen igång på det sättet."* - Respondent 1

5.1.2.5 Framtid

För framtiden tror respondent 1 det är viktigt att tänka på att inte mer information automatiskt ger en högre säkerhetsmedvetenhet, utan att det då istället kan leda till informationsöverbelastning. Att inte tillåta alternativa sätt att kringgå säkerhetslösningar som exempelvis tvåfaktorsautentisering är en annan sak som är viktig att ha med sig. Att helt enkelt ibland göra det lite krångligt och tydligt att allt inte är tillgängligt för alla, vilket kommer göra folk mer medvetna då det är någon som kräver det av personalen. En annan sak respondent 1 tror blir viktig i framtiden är att verkligen förmedla varför det är viktigt att följa de bestämmelser som finns. Detta för att få den acceptansen att följa samtliga bestämmelser och inte bara de som personal tycker är värt att följa.

> *"Man kan alltid bli bättre, men det är en sak att vara medveten men det är inte alltid säkert att bara för att jag med lite mer information ökar medvetenheten. En del tror ju det, jag tror inte på det. Man får sådan information overload och till sist så läser man inte ens, man tar inte åt sig det."* - Respondent 1

5.2 Företag B

Två respondenter har intervjuats i företag B, en gruppchef för säkerhetsskydd och informationssäkerhet, benämnd som respondent 2, samt en informationssäkerhetskonsult som även agerar som koncernens handgångne man när det gäller säkerhetsfrågor inom organisationen, benämnd som respondent 3. Respondent 3 som är informationssäkerhetskonsult ansvarar även internt för att implementera ett ledningssystem för informationssäkerhet. Respondent 2 ville inte bli inspelad och därför kommer inga direkta citat från respondent 2 att kunna användas.

5.2.1 Informationssäkerhet

Enligt både respondent 2 och 3 är de största historiska hoten trendmässigt de som varit externa, åtminstone med vad som de känner till. Respondent 3 menar att de interna hoten har varit få men har inte varit med uppsåt utan har snarare handlat om att personalen inte tänkte på vad de fick eller inte fick göra, eller att de helt enkelt inte visste om den policy som fanns.

"Tittar man på vad som hänt så är de externa hoten de största trendmässigt, det vill säga det vi känner till. Man får inte vara helt naiv och tro att vi inte har någon som utöver hot mot oss, det är bara en fråga när man upptäcker det. Interna hot har varit få och de har naturligtvis varit aktörsdrivna men de har inte varit med uppsåt, utan vi snackar om 'tänkte inte på det', eller vara lite för ambitiös eller kände inte till policys etc." - Respondent 3

5.2.1.1 Uppdatering

Det finns enligt respondent 2 och 3 en intern säkerhetsgrupp inom organisationen som har i ansvar att uppdatera sig gällande informationssäkerhet. Enligt respondent 3 har de en gemensam Sharepoint sida där saker av intresse läggs upp. Respondent 3 menar även att det finns gott om information både internt och externt att samla in vilket inte gör det svårt att hålla sig uppdaterad. Det är just den här säkerhetsgruppen som har ansvaret att hålla sig uppdaterad om nya hot. Enligt respondent 2 förmedlas det till anställda från den här säkerhetsgruppen framförallt via intranätet eller mail och ibland som information på möten.

5.2.1.2 Prioritering

Fokus och prioritering ligger både enligt respondent 2 och 3 mer mot människan när det gäller informationssäkerhet av den anledning att det överlag handlar om människor. Teknisk säkerhet ses enligt respondent 3 mer som skyddsåtgärder.

"Jag skulle nog vilja påstå att vi prioriterar människan. Därför att det är det som det handlar om. Security överlag handlar om människor. Det är därför det är så svårt. Tekniska prylar såsom antivirusskydd, brandväggar och allt det där, för min del i alla fall, det är skyddsåtgärder. Det är inte det första jag tänker på utan det får man välja med omsorg när man har lärt sig de grundläggande delarna." - Respondent 3

5.2.1.3 Ansvar

Respondent 2 och 3 säger att det endast finns en informationssäkerhetschef på koncernnivå och att det sedan finns en underställd säkerhetschef inom varje division inom koncernen. Respondent 3 påpekar även att det finns företrädare på lokal nivå, åtminstone i de större städerna och de större kontoren.

5.2.1.4 Konsekvenser

Respondent 3 är lite osäker på vilka konsekvenser det finns om en anställd bryter mot säkerhetsreglerna då det inte varit så vanligt att något har blivit väldigt stort. Den ultimata konsekvensen skulle vara avsked, men där respondenten inte känner till något fall när någon anställd har brutit så pass att avsked har blivit aktuellt. En annan disciplinär åtgärd som respondenten tänker sig skulle ske i första hand är löneavdrag.

"... jag skulle kunna tänka mig löneavdrag i första hand, någon form av disciplinär åtgärd. Det ultimata är naturligtvis avsked men det ska nog mycket

till. Jag känner inte till något exempel där någon har fått lämna företaget." - Respondent 3

5.2.1.5 Ökat engagemang

För att få anställda mer engagerade menar respondent 3 att när det väl sker något som får medial uppmärksamhet, kopplar de till det när de pratar med anställda som behöver få en större förståelse för vad en dålig informationssäkerhet kan leda till. Respondent 2 påpekar att det egentligen är ganska reaktivt.

> *"Det vi försöker göra är ju att när det sker någonting som får medial uppmärksamhet att knyta an till det när man pratar med de anställda eller kollegorna som behöver få lite större förståelse för vilka konsekvenser dålig informationssäkerhet kan få."* - Respondent 3

Respondent 3 menar även att det är en svår balansgång i det att utbildningar innebär inkomstbortfall då det inte är speciellt produktiv tid. Att få igenom en förståelse på chefsnivå att god informationssäkerhet faktiskt lönar sig är därför en utmaning. De vet enligt respondent 3 om att de behöver höja sin säkerhetsmedvetenhet, men det finns ingen aktiv kampanj de jobbar med i nuläget för att få anställda mer engagerade. De är dock på gång med en ny kampanj, men val av metod är ännu inte fastställt. Samtidigt tror respondent 3 att det är lite olyckligt att alla nya regelverk kommer på en och samma gång då det kan bli lite för mycket på en och samma gång för anställda, vilket gör att anställda helt enkelt inte tar åt sig till slut.

> *"Jag tror att det blir lite för mycket, det är min rädsla. Det är inget snack om att de här regelverken, förordningarna behövs, tveklöst. All regelverk är en reaktion på någonsting som har hänt och det har hänt mycket, därför kommer alla de här sakerna. Det är olyckligt att det kommer i skov."* - Respondent 3

> *"... generellt tror jag det kan bli att man känner sig chokad och kommer att ha en 'vänta och se' approach till hur man ska ta sig an och välja hur man ska börja arbeta med att bli compliant med de här regelverken."* - Respondent 3

5.2.2 Säkerhetsmedvetenhet

Att ha en hög säkerhetsmedvetenhet anses av både respondent 2 och 3 vara det absolut viktigaste.Respondent 2 menar att information och kompetens är deras produkt, därav blir säkerhetsmedvetenheten avgörande för företaget. Enligt respondent 3 finns inga bättre indikatorer än just de anställda, då det är de som varnar om någonting inte står rätt till. Respondent 3 fortsätter förklara att anställda kan ses som sensorer, som underhålls genom att öka medvetenheten hos de anställda. Under tidigare arbete för respondent 3 kunde det märkas att säkerhetsrapportering kunde vara på rekordlåga nivåer, för att sedan utföra en utbildningsinsats och kunde där se att benägenheten att rapportera säkerhetsincidenter ökade. Efter ett halvt år till ett år börjar dessa rapporterade säkerhetsincidenter att minska, vilket är en bra indikator på att någon mer åtgärd gällande medvetenheten kan behövas. Det önskvärda är att hålla den kurvan på en jämnare nivå. Respondent 3 förklarar att det dock är svårt att hålla den exakt jämn då det finns mer än säkerhet som behöver utbildas inom en organisation.

"...alla anställda är sensorer så har jag betraktat dem. Sensorer som varnar mig för eller ger mig indikationer på att någonting inte står rätt till och sensorer måste underhållas. För en sensor som inte fungerar larmar inte." - Respondent 3

5.2.2.1 Säkerhetskultur

Även om de enligt respondent 3 är något sena med att arbeta med säkerhetskulturen är det ändå något som de precis påbörjat. Det är dock i ett tidigt skede där GDPR blev en ögonöppnare och där de försöker utnyttja den vågen för att få till en säkerhetskultur. I grund och botten handlar det enligt respondent 3 om ledningens inställning och medvetenhet för att anamma en policy och sätta en kultur. I nuläget finns dock ingen aktiv plan på hur de ska lyfta upp användarna i det hela utan det måste börja uppifrån och ner. Respondent 3 menar även att det är via policyn som kulturen sätts och att det är den som ledningen måste förespråka och stå för. Respondent 2 menar att företagets e-kurser hjälper till att bidra till att få till en säkerhetskultur.

"GDPR var en ögonöppnare och det försöker vi utnyttja den vågen så att säga. Men i grund och botten så handlar det faktiskt om ledningens medvetande och ledningens inställning. Utan ledningen i ryggen så är det liksom ingen idé." - Respondent 3

"... det är ledningen som ska stå för kulturen. Det är ledningen som ska slå an tonen för koncernen och det gör man med policyn, för policyn är en viljeinriktning." - Respondent 3

5.2.2.2 Standard och policy

Respondent 3 förklarar att samma sak som med säkerhetskulturen gäller arbetet med standarden ISO 27000. De är precis i uppstarten av att implementera ett ledningssystem enligt ISO 27000 serien. Det finns mål och visioner men i dessa finns det inte ännu specificerat om de ska gå hela vägen och certifiera sig eller inte. Förståelsen för att de behöver ha ett ledningssystem finns, men hur ambitiöst och hur långt de ska ta det är ännu inte bestämt utan där väntar de på svar från ledningen om vad de vill. I arbetet med säkerhetspolicyn finns det en ny reviderad policy som ännu inte är fastställd och planerna med hur den ska marknadsföras är för respondenterna ännu okänt. I övrigt säger både respondent 2 och 3 att den nuvarande policyn finns att tillgå på deras intranät.

"... vi startade i somras att börja med att införa ett ledningssystem enligt ISO 27000, men det arbetet är i praktiken bara påbörjat. Det finns visioner, det finns mål, men varken i vision eller målen finns det till exempel upptaget om vi ska certifiera oss eller ej." - Respondent 3

"Jag tror det finns en förståelse för att, okej, vi måste ha ett ledningssystem för informationssäkerhet. Men hur högt, hur ambitiöst ska det vara? Där är det ingen som har satt ned foten än." - Respondent 3

5.2.2.3 Informationsspridning

Den stora informationsspridningskällan är enligt respondent 2 intranätet, där det som är allmänt sprids. Sker det ändringar i policys eller rutiner kommer den här informationen framförallt att spridas via mail och kompletteras ibland även på möten. Samma sak gäller om det sker organisationsförändringar som berör en vissa enheter skickas detta på mail och tas ibland upp på möten för de enheter de gäller.

5.2.2.4 Utbildningar

Respondent 3 säger att det finns ett utbildningssystem där personal kan anmäla sig och gå utbildningar via internet var och en för sig. I nuläget finns inga lärarledda utbildningar även om det är något som respondent 3 hade velat se i framtiden. Respondent 3 menar på att det hade varit önskvärt att säkerhetscheferna hade varit ute i verksamheterna och haft hand om utbildningar, då det hade varit viktigt för anställda att få ett ansikte på de som ansvarar. Detta tror respondent 3 hade bidragit till att det hade känts mer naturligt för anställda att säkerhetsrapportera och höra av sig till de som är ansvariga.

> *"Jag skulle vilja se om jag får önska att alla divisionernas säkerhetschefer, minst, är ute i verksamheterna och kör de här utbildningarna. Det är så viktigt att man får ett ansikte på de som företräder säkerhetstjänsten eller bedriver säkerhetsarbetet för då blir det mer naturligt för någon, tror jag i alla fall, att göra säkerhetsrapporter, att höra av sig till de som är ansvariga."* - Respondent 3

Respondent 3 förklarar att det för nyanställda finns ett program som de måste gå där vissa delar angående informationssäkerhet tas upp. Delar som GDPR, där hur det ska handskas med personuppgifter, tas upp samt att den policy som finns blir känd för alla nyanställda. Utöver GDPR och organisationens policy går utbildningen igenom grundläggande informationssäkerhet med konfidentialitet, riktighet och tillgänglighet som grund. Mer än just det grundläggande finns inte men det viktigaste enligt respondent 3 är att just alla får en grundläggande förståelse och att de sedan får utbildningar anpassade efter det arbete som de faktiskt ska utföra. Den grundläggande förståelsen för informationssäkerhet anser respondent 3 dock vara viktigt oavsett vad som ska göras, då alla ska ha en basnivå när det kommer till kunskaper inom informationssäkerhetsområdet.

Enligt respondent 3 utförde de utbildningar specifikt för GDPR när det var nytt. Dessa skickade de ut som små lektioner som de kunde göra när de hade tid och på vilken utrustning de kände för. De skickade sedan ut en ny lektion per vecka, där varje lektion tog ungefär 5 minuter.

> *"Jag hittar på nya utbildningar i form av att göra lite roligare typ comics eller enkla små nanolearningar. Så gjorde vi med GDPR till exempel. Vi portionerade ut i fem minuters små lektioner en gång i veckan, så att folk kunde sitta på tunnelbanan eller bussen och swipa på sin padda eller vilken device man nu använde för att inte stjäla för mycket arbetstid från dem"* - Respondent 3

Ungefär fyra gånger per år sker det enligt respondent 3 en heldag med utbildningar för nyanställda på huvudkontoret. När respondenten var nyanställd var det organisationens HR chef och CIO som pratade ytterst kort om just informationssäkerhet, något som respondent 3 hoppas det finns mer tid för på dessa utbildningar i dagens läge, utan att ha något större koll på hur det faktiskt i praktiken ser ut idag.

> *"Sen finns det ju, jag tror det är två, säg att det är fyra gånger per år som det finns en kurs då man åker upp till huvudkontoret i Stockholm och har en heldag. Det brukar vara ett hundratal personer på de här utbildningarna. När jag var ny så var det chefen HR och chefen IT alltså CIO som pratade om informationssäkerhet i kanske 30 sekunder. Jag känner inte till om det finns någon plats för säkerhetschefen eller informationssäkerhetschefen på den här kursen idag, jag har ingen aning. Skulle gärna sett det naturligtvis, jag tycker det borde varit det."* - Respondent 3

I övrigt finns det enligt respondent 3 inga återkommande utbildningar som måste göras med jämna mellanrum för att uppdatera kunskaperna. De utbildningar som finns gällande informationssäkerhet är de för nyanställda, inga kontinuerliga utbildningar för personal sker.

Respondent 3 anser att utbildningarna kan ses som det viktigaste som organisationen gör för att öka säkerhetsmedvetenheten. Respondent 2 anser att den viktigaste aktiviteten är de möten som sker. När det sker gruppmöten kan de ta upp om saker har hänt, exempelvis om det kommit en virusvarning.

5.2.2.5 Framtid

För framtiden hade respondent 2 velat se ett bra utbildningspaket vid nyanställning som är riktad mot typen av uppdrag personen ska ha, samtidigt som det sker en årlig uppdatering för samtliga via exempelvis en föreläsning eller en e-kurs. Respondent 3 hade velat se att informationssäkerhet görs mer lättillgängligt via användning av exempelvis figur i form av en fiktiv medarbetare på företaget som anställda vill följa. Denna figuren kan sedan utsättas för olika saker som exempelvis frågeställningar. Detta skulle bidra till att anställda lättare kan ta till sig av informationen samtidigt som det inte blir riktigt så tungt, att informationssäkerhet förmedlas på ett roligare sätt som samtidigt kan kopplas mycket till privatlivet. Dessa bör framföras i korta filmklipp för att undvika för mycket information på en och samma gång.

> *"Jag personligen skulle absolut vilja se att vi gjorde informationssäkerhet mycket mer lättillgängligt, att inte göra det så tungt. Inte dra ner allvaret i det på det sättet utan att göra det mer lättillgängligt genom att använda kanske serier, att hitta på någon slags figur, någon form av fiktiv medarbetare på företaget som man gärna vill följa, där han eller hon kan tänkas råka ut för frågeställningar och allt sånt där. Någon form av enklare animerade filmsnuttar som på något sätt är roliga men ändå naturligtvis har med sig ett lärande budskap. Det är vad jag skulle vilja se. De ska heller inte vara längre än fem minuter max."* - Respondent 3

5.3 Företag C

Även i företag C har två respondenter intervjuats varav en regionchef som benämns som respondent 4. Respondent 4 jobbar med att utveckla regionen och i huvudsak se till att de utvecklar kunder och medarbetare på den geografiska yta som respondent 4 ansvarar för, men jobbar inte specifikt mot informationssäkerhet. Den andre respondenten som har intervjuats benämns som respondent 5 och har två roller inom företaget. Den ena rollen är som data protection officer (DPO) med ett ansvar i att kontrollera och stötta företaget i efterlevnaden av GDPR. Andra rollen är som informationssäkerhetskoordinator där de mesta initiativen inom informationssäkerhet ingår med ansvar för att bland annat se till att ta emot alla olika krav i förhållande till informationssäkerhet och implementera det i verksamheten.

5.3.1 Informationssäkerhet

Både respondent 4 och 5 anser de externa hoten vara de största mot organisation. Respondent 5 påpekar dock att sårbarheterna kan komma från internt inom organisationen, men att just hoten i huvudsak kommer från externa källor.

> *"Bra fråga, väldigt bra fråga. Det måste vara externa hot. Sårbarheten kan ju vara internt, mänskliga faktorn, det kan vara interna svagheter i systeminfrastruktur och applikationer men hoten kommer externt ifrån."* - Respondent 5

5.3.1.1 Uppdatering

Respondent 5 berättar att det finns en omvärldsbevakning i form av hundratalet säkerhetskonsulter som jobbar ute hos kunder. Internt menar respondent 5 att de som jobbar med informationssäkerhet håller sig uppdaterade via nyhetssidor. Är det något som upptäcks skickas detta vidare till relevanta personer, vilket oftast är respondent 5 i sin roll som informationssäkerhetskoordinator eller IT-chefen att det finns en sårbarhet. Därefter menar respondent 5 att det är deras uppgift att skicka det vidare till de personer som ska lösa det. Är det dock något som berör alla, som exempelvis att det florerar något med phishing, kan de lägga upp det som en nyhet på intranätet.

> *"Där har vi omvärldsbevakning dels i form av att vi har ett hundratal säkerhetskonsulter som jobbar med säkerhet som konsulter ute hos kunder. Intern så håller vi oss uppdaterade genom nyhetssidor."* - Respondent 5

> *"... kan komma från vår group CISO och då skickas det antingen till mig eller IT-chefen att nu har vi hittat en sårbarhet, vänligen kontrollera hur det ser ut inom landet. Så det brukar vara den som identifierar, det är en person som kan säkerhet och vet hur vi jobbar med säkerhet så den skickar det vidare till relevanta personer."* - Respondent 5

> *"... Är det något som pågår med phishing eller liknande då kan det vara att vi lägger ut en nyhet på intranätet om det är någonting som påverkar alla våra anställda, så att de är uppmärksamma"* - Respondent 5

5.3.1.2 Prioritering

Det fokuseras enligt respondent 4 och 5 inte på något specifikt område inom informationssäkerhet, utan både människan och det tekniska anses som viktigt att fokusera på. Respondent 5 menar att medvetenhet är en konstant bit medans de gör kontinuerliga kontroller på de tekniska bitarna

> *"Awareness med människorna, det är som en konstant bit medans de tekniska bitarna, då gör vi kontroller regelbundet för att se hur våra infrastrukturer och applikationer ser ut och står emot kraft och hot utifrån. Så vi fokuserar på både och, jag kan nog inte säga att vi fokuserar på det ena mer än det andra."* - Respondent 5

5.3.1.3 Ansvar

Både respondent 4 och 5 påpekar att det yttersta ansvaret ligger på VD, men där respondent 4 utvecklar och menar att det formella informationssäkerhetsansvaret ligger på företagets CIO. Bland annat står det enligt respondent 5 i företagets säkerhetspolicy att det är CIO som har ansvaret för informationssäkerheten. De som arbetar med företagets informationssäkerhet är sedermera respondent 5 och en till person, men där de har mycket hjälp från koncernen som ställer krav på de olika länderna som de är verksamma i. Respondent 4 menar också att alla i organisationen har ett personligt ansvar för att hålla organisationens information säker.

> *"Just nu står vi i en väldigt spännande situation med ansvaret. Vi hade tidigare en riktig informationssäkerhetschef, sen för två år sedan flyttade han och blev vår group CISO. Så här i Sverige, den som tog över efter honom med informationssäkerhetsansvaret det var vår dåvarande IT-chef och när hon sedan slutade så fick CIO ta över informationssäkerhetsansvaret. Så vi har fortfarande CIO som är CISO i och med att vi inte har pekat ut en riktig CISO. Så där ligger det formella ansvaret."* - Respondent 5

> *"Dels har vi ett personligt ansvar. Det är svårt för mig som chef och det är klart att VD har ett ytterst ansvar för hela bolaget. Men det ligger väldigt mycket på det personliga planet att vi både håller oss utbildade och uppdaterade men också att vi agerar enligt de processer och rutiner som finns så att vi inte utsätter oss för större risk. Eller när någonting händer att vi agerar på rätt sätt och så vidare."* - Respondent 4

> *"Ansvarar gör CIO, arbetar med det är, om man tittar på informationssäkerhet så är det jag och en till. Tittar man på IT-säkerhet så är det fem stycken inom IT-avdelningen. Sen får man också tänka på att vi har rätt mycket stöd och beslut från gruppnivå där de nu är tre personer som ställer krav på oss länder."* - Respondent 5

5.3.1.4 Konsekvenser

Respondent 5 menar att de konsekvenser anställda råkar ut för beror på hur mycket de har brutit mot säkerhetsreglerna. Respondent 5 fortsätter och berättar om att de hade en situation där en person fick gå på dagen för att den inte skött sig, men där det

handlade om att det var mycket fel. I de vanligaste fallen är det enligt respondent 5 en tillsägelse som gäller och att närmaste chef blir informerad. Bryter anställda mot företagets policy är det i första hand en varning som utges. Om det blir upprepade brott är det upp till chefen vad för typ av åtgärd som ska ske.

> *"Sen har vi disciplinära åtgärder hos HR om man bryter mot våra policys eller liknande. Det är varning i första hand och i värsta fall uppsägning. Det blir först en varning och varning till närmaste chef. Blir det upprepade brott mot våra policys så blir det ett samtal med chefen. Sen är det upp till chefen."* - Respondent 5

5.3.1.5 Ökat engagemang

Respondent 4 anser att de har det lättare att få ett engagemang kring informationssäkerheten på grund av att det är ett IT-bolag där säkerheten hela tiden är en viktig del i det de gör. I övrigt anser respondent 4 att de via utbildningar och att det faktum att det har det högt på agendan leder till ett ökat engagemang. Respondent 5 menar att det är en utmaning att få anställda att tycka det är roligt och påpekar att sättet de förmedlar informationssäkerhet på är det viktigaste. Att inte enbart prata om krav som ska uppfyllas, utan risker och hur anställda bör tänka för att skydda informationen de hanterar.

> *"Dels har vi det lite lättare i och med att vi är ett IT-bolag, för vi lever ju av de här grejerna och säkerhet är som en våt filt. Oavsett vad vi håller på med så är säkerheten en viktig del, oavsett om vi kopplar upp sensorer till en lyktstolpe eller om vi pratar om klientskydd eller vad det är för någonting. Där har vi det lite lättare i och med att vi jobbar med de grejerna. Men det handlar mycket om att vi utbildar och att vi pratar om det här grejerna och vi har det högt upp på agendan."* - Respondent 4

> *"Det är en utmaning som jag tror de flesta företag står för, att anställda ska tycka det är roligt och inte bara se det som någonting de måste följa och sucka åt det. Där ser jag på sättet man lägger fram det, att det hjälper inte att säga: det här får du inte göra och det här får du inte göra, utan istället lyfta upp vilka risker vi ser med varför de inte ska göra som de ska göra och vad de ska göra istället."* - Respondent 5

> *"Så sättet man kommunicerar på skulle jag säga är det viktigaste. Vi har till exempel en 'medarbetarens guide till informationssäkerhet' och det är ett papper vi utformat just för medarbetarna. I början när det togs fram så innehöll det bara, du får inte göra så här… du får inte göra så här. Nu har vi istället gjort om det helt och hållet så att det står vilka risker som finns och hur man som anställd ska tänka för att skydda företagets och vår information."* - Respondent 5

5.3.2 Säkerhetsmedvetenhet

Respondent 4 anser att säkerhetsmedvetenheten är väldigt viktig, då det bland annat handlar om en trovärdighetsfråga gentemot kunder. Även respondent 5 anser

säkerhetsmedvetenheten vara mycket viktig då de flesta incidenter beror på den mänskliga faktorn. Samtidigt ser respondent 5 säkerhetsmedvetenhet som att ha en verksamhet där folk känner till de risker som finns samt hur de ska agera.

> *"... det är också en trovärdighetsfråga när vi jobbar med de här sakerna. Vi själva vill inte vara skomakarens barn att vi pratar hur viktigt det här är för våra kunder men själva så lever vi inte riktigt som vi lär så det är jätteviktigt."* - Respondent 4

> *"Det är jätteviktigt, för de flesta incidenter beror ofta på den mänskliga faktorn. Det är nästan alltid dit man kan spåra tillbaka, att någon har glömt göra någonting, en process har brustit, någon har gått en smitväg istället för att följa våra processer, eller bara slarvat."* - Respondent 5

> *"Jag ser det som att ha en verksamhet där folk känner till vilka risker vi har och hur de ska agera. Att man tänker på det i sin vardag."* - Respondent 5

Det viktigaste med säkerhetsmedvetenhet tror respondent 5 är att det inte får bli för mycket information och att hålla det intressant genom att referera till situationer som alla kan relatera till.

> *"Jag tror att det viktigaste med säkerhetsmedvetandet är att inte ta för mycket information på en gång, utan hålla det intressant så att man kan ta till sig det och fortfarande tänka in i sin vardag. Så man inte tar för specifika situationer som bara en viss typ av människor kan ta in utan jag tror framgången är att hålla det generellt till någonting som alla kan referera till."* - Respondent 5

5.3.2.1 Säkerhetskultur

Respondent 5 tycker att de arbetar aktivt för att få till en säkerhetskultur i och med att de har pratat om det och för två år sedan tagit fram en process för hur de ska hantera säkerhetsutbildningarna och att det ska vara en årlig process. Respondent 5 berättar även att de nyligen bytte färg på banden till sina passerkort för att förtydliga om de är anställda, inhyrda konsulter eller om det är lånekort. När den här ändringen gjordes satte de enligt respondent 5 upp skyltar vid varje ingång samt inne på toaletterna för att öka medvetenheten av att dessa band var betydelsefulla. Förutom de årliga utbildningarna anser respondent 5 att en del är de punktinsatser som de gör. En utav punktinsatserna var en phishing kampanj där de själva skapade phishingmail och testade sina anställda. Inom en snar framtid menar respondent 5 att de kommer genomföra punktinsatser gällande VD bedrägerimail för ledning och de som sitter i ekonomi.

> *"Jag skulle vilja säga ja, i och med att vi har pratat om det och först för två år sedan tagit fram en process för hur vi ska hantera våra säkerhetsutbildningar som vi genomför då och då. Att det nu är en årlig process där vi går igenom vilka områden vi vill fokusera på och sen punktinsatser vid behov."* - Respondent 5

> *"En del är årlig obligatorisk utbildning i informationssäkerhet och sen*

punktinsatser. Vi har nyligen genomfört phishing-kampanjer, där vi själva har skapat phishingmail som vi har skickat ut till våra anställda." - Respondent 5

5.3.2.2 Standard och policy

Respondent 5 menar att de delvis följer standarden ISO 27000. Deras outsourcingavdelning är certifierade där de har ett datacenter med kundernas information. Sedan har de även enligt respondent 5 bestämt sig för att arbeta mer i enlighet med ISO 27000 standarden än vad de gör idag och inom tre år ska större delar av företaget vara certifierade. De är dock inte helt klara med att besluta vilka avdelningar som ska respektive inte ska vara certifierade, då alla avdelningar inte har behovet av att vara certifierade. Den avdelning som är certifierad har specifika resurser som jobbar med att upprätthålla certifieringen samtidigt som de har väl inarbetade processer. Just på grund av att det är kundinformation och att den avdelningen är väldigt processtyrd tror respondent 5 gör det lättare att efterleva standarden. Samtidigt menar respondent 5 att de har märkt att det är en konkurrensfördel om de sköter det på rätt sätt och följer standarden.

"Vi har en avdelning inom företaget som är ISO 27001 certifierade. Det är vår outsourcingavdelning där vi har datacenter där vi har kundernas information som de outsourcar till oss. Sen har vi flera datacenter som är certifierade och vi själva har bestämt oss för att arbeta mer i enlighet med ISO 27001 standarden än vad vi gör idag, så det ligger i vår treårsplan" - Respondent 5

"Den avdelning som är certifierade de har specifika resurser som jobbar med certifieringen att upprätthålla, informera och de har väl inarbetade processer. Så den avdelningen är väldigt processtyrd och i och med att det bara är kundinformation som finns där, så tror jag att det är lättare där än på vissa andra avdelningar att få till certifieringen och få att den efterlevs." - Respondent 5

Gällande företagets säkerhetspolicy förklarar både respondent 4 och 5 att den är en del av introduktionsplanen för nyanställda, där de måste läsa igenom den. Respondent 5 menar även att de gör en överblick av policyn årligen och ändrar den vid behov, sker ändringar lägger de upp en nyhet på intranätet att det har skett en uppdatering av säkerhetspolicyn. I övrigt är säkerhetspolicyn inte en del av det utbildningsmaterial som återfinns i utbildningarna.

"Den finns med i listan som man ska gå igenom när man nyanställs, då ska alla läsa igenom vår säkerhetspolicy. Sen har vi nyligen kommit på att vi ska gå ut på intranätet när vi gör uppdateringar i den vilket sker årligen." - Respondent 5

5.3.2.3 Informationsspridning

De primära kanalerna för informationsspridning är enligt respondent 5 intranätet och mail. De har även plats på toalettdörrarna för att sätta upp lappar samt skärmar ute i lokalerna, bland annat vid kaffeautomaterna, där de kan lägga upp information. Skärmarna eller lapparna används dock för mindre viktig information då det inte kan

garanteras att det läses. Är det något större som har påverkan på flera personer och de måste få ut informationen snabbt kan de även använda sig av sms.

> *"Är det viktig information då blir det antingen mail eller nyhet på intranätet. Är det mindre viktig information kan man ta någon av skärmarna eller lappar någonstans."* - Respondent 5

> *"Sms skickar vi ut om det är någonting större som har påverkan på flera personer och vi behöver få ut informationen snabbt, exempelvis "Just nu cirkulerar ett mail med rubriken "[…]". Radera mailet, klicka inte på länken… om du har klickat på länken, kontakta "[…]"."* - Respondent 5

5.3.2.4 Utbildningar

Respondent 4 berättar att de i utbildningsväg kör E-learning som alla medarbetare har gått. Respondent 5 förklarar att det sker utbildningar via nätet för samtliga anställda och att de görs en gång per år, samtidigt som det för nyanställda finns en egen, grundläggande utbildning som samtliga måste genomgå när de anställs, som ingår i det program som alla nyanställda måste genomföra. Respondent 5 berättar att det kan bli att nyanställda får gå två kurser parallellt, i och med att de har en informationssäkerhetsutbildning för samtliga nyanställda, samtidigt som de genomför en årlig informationssäkerhetsutbildning för alla i hela företaget.

> *"Det ligger i vårt onboardingprogram för nyanställda. Så när man börjar på företaget så har man en lång lista på saker att göra, allt från att skicka in kontouppgifter till löneavdelningen till att gå igenom informationssäkerhetsutbildningen."* - Respondent 5

> *"Just nu har vi en som rullar för nyanställda som tar upp i princip alla områden och sen blir det en årlig för allihop. Så nyanställs man precis innan så kan det vara att man får gå två kurser parallellt."* - Respondent 5

Just nu skiljer det sig enligt respondent 5 inte på utbildningsmaterial beroende på vilken roll de utbildar. Däremot påpekar respondent 5 att de gjorde en extra utbildning för chefer när de utförde en utbildning gällande GDPR. Den senaste utbildningen de utförde handlade om just GDPR och säkerhet. Inga lärarledda utbildningar sker enligt respondent 5 gällande informationssäkerhet, men där det kommer att komma i och med det arbete de genomför med ISO 27000. Respondent 5 har däremot genomfört föreläsningar och berättat om GDPR.

> *"Just nu gör det inte det utan det vi har gjort med de tidigare utbildningarna är att vi har gjort en för allihop med vilka risker alla behöver känna till och vad alla behöver veta. Så då har vi inte gjort någon skillnad på roll."* - Respondent 5

> *"För GDPR gjorde vi en extra utbildning för chefer för att ta upp allting med CVn och hur vi hanterar dokument om anställda och vad man behöver tänka på. Också att se till att alla i din avdelning har läst*

informationssäkerhetspolicyn och medarbetarens guide till informationssäkerhet." - Respondent 5

"Jag har haft massor med lärarledda föreläsningar där jag har berättat om GDPR, men inom informationssäkerhet så har vi inte haft det. Det kommer dock komma i och med det arbetet vi påbörjar nu med ISO 27001 certifiering." - Resondent 5

Respondent 5 berättar att den utbildning som görs av alla nyanställda har ett antal moduler i form av "Sekretess", "Skydda din mobil", "Skydda din dator", "Nätverk", "Surfa säkert", "Facebook och sociala sajter", "Nätfiske och social engineering", "Ransomware", "Lösenord", "Säker identitet", "Lagra säkert" samt "Våra lokaler". Utbildningen för nyanställda behöver enligt respondent 5 uppdateras, då den har varit likadan i flera år.

"Den för nyanställda den skulle behöva uppdateras, den för nyanställda. Men det är sånt som ligger på den långa listan." - Respondent 5

När det gäller utbildningen som görs av samtliga anställda på företaget skiljer det sig enligt respondent 5 åt varje år vad innehållet är, men där grunden är densamma. Därefter ändrar de utbildningen beroende på vad som är relevant och om det finns en extra risk som det behöver fokuseras extra mycket på. Moduler i den planerade utbildningen för 2019 är enligt respondent 5 "Confidentiality and privacy", "Working in a secure way", "Actual threats, phishing" och "Physical security" med tillhörande dellektioner för varje modul.

"Grunden är väl hyfsat densamma med områden som klassificering, hur man ska tänka runt mail, våra lokaler." - Respondent 5

"... men man justerar lite grann. Sen tittar man också på om det är någon extra risk som vi ser nu som vi behöver lägga extra fokus på som vi inte hade med förra utbildningen." - Respondent 5

När de utformar utbildningarna som görs för samtliga anställda försöker de enligt respondent 5 koppla det till vardagliga händelser för att göra det lättare för anställda att förstå vad som förmedlas.

"Då försöker vi när vi utformar utbildningarna att koppla det till vardagliga händelser så att man tar exempel ur vardagen så att folk kan tänka sig in i situationen." - Respondent 5

Efter en avklarad modul får du enligt respondent 4 och 5 svara på frågor.

"Du får svara på ett antal frågor och ställas inför ett antal saker i den här interaktiva utbildningen" - Respondent 4

Respondent 5 förklarar att det inte är frågor för att en anställd ska bli godkänd eller inte godkänd. Frågorna är till för att få personen som gör utbildningen att tänka till, svarar personen fel kommer rätt svar upp med en förklaring.

> *"Jag tror man kan svara fel på alla och ändå bli godkänd. För svarar man fel kommer det upp en ruta med vad det rätta svaret var och varför man lär sig på det sättet också."* - Respondent 5

Varje modul i utbildningen är enligt respondent 5 väldigt korta samtidigt som de kan göras på vilken enhet de känner för. Detta är något som görs för att det inte ska låsa anställda under för lång tid. Samtidigt menar respondent 5 att dessa utbildningar inte är fakta tunga, utan fokuserar på att koppla det till risk och få anställda att tänka själva.

"Tidigare har vi gjort i nano-learning format, så vi har haft olika moduler. En modul om fysisk säkerhet som är väldigt enkelt att relatera till och då är det små korta lektioner inom det området och sen frågor på slutet, efter hela fysiska säkerheten. Då är det kanske, hela fysiska säkerhetsmodulen kanske tar fem minuter att läsa igenom. Så det ska inte vara för långt utan kort så man ändå kan göra det när man sitter på tåget på väg till jobbet eller liknande. Att det inte är någon utbildning som man måste påbörja och sen ska man avsätta en timme och kan inte avbryta. Då tror jag man får svårare att få utbildningarna genomförda." - Respondent 5

> *"Under våra årliga utbildningar så har vi inte så mycket faktabaserat utan vi kopplar det till risk och vill att folk ska bli medvetna om riskerna och tänka innan."* - Respondent 5

De viktigaste aktiviteterna som genomförs för att öka medvetenheten ser respondent 4 som det faktum att de lever i den miljön som de gör som IT-bolag.

> *"Det är att vi lever med det här så det här är ju saker som vi hela tiden jobbar med."* - Respondent 4

Respondent 5 anser just utbildningarna tillsammans med punktinsatserna vara de allra viktigaste aktiviteterna som de genomför för att öka medvetenheten. Detta beror på att det är något som sker kontinuerligt på en årsbasis och därför bidrar till att det pratas om det bland anställda.

> *"Jag tror att det är de här punktinsatserna tillsammans med den årliga utbildningen. I och med att den bara är årlig så blir det ändå någonting som det pratas om i korridorerna också, och punktinsatserna."* - Respondent 5

5.3.2.5 Framtid

För framtiden anser respondent 4 att det är viktigt att hålla en grundnivå på samtliga anställda samtidigt som det är viktigt att hela tiden uppdatera och hålla saker relevant.

> *"Jag tror det är viktigt att det finns en grundnivå där alla går igenom och att den inte är frivillig utan den går man igenom. Sen tror jag man behöver fräscha upp saker vart eftersom saker och ting förändras."* - Respondent 4

Respondent 5 tycker att de som företag borde jobba mer med medvetenheten samt utföra mer utav de punktinsatserna som de genomför. Samtidigt menar respondent 5 att

det är viktigt att det inte blir för mycket, utan att det måste hållas på en bra nivå för att det inte ska bli för tjatigt.

> *"Mer punktinsatser och mer medvetenhet. Sen får det inte bli för mycket heller så att våra anställda tycker det är jobbigt när man hela tiden kommer och tjatar om säkerhet"* - Respondent 5

Det har även enligt respondent 5 talats om att det ska ingå en obligatorisk utbildning för de som klickar på ett utav de phishing mail som kommer från företaget själva i de punktinsatser det genomför. Det är inget som finns idag men de har pratat om det och det kanske kommer i framtiden.

> *"Den senaste kampanjen då kom det upp information om att det här är phishing och klickade på det, så här ska du tänka när du får ett mail. Det finns sådana phishing kampanjer med en tillhörande utbildning också att klickar man på ett phishing mail från verksamheten så får man gå en obligatorisk utbildning"* - Respondent 5

> *"... så har vi inte gjort, men vi har pratat om det, så det kanske kommer."* - Respondent 5

6 Analys

6.1 Informationssäkerhet

D'arcy, Hovav och Galletta (2009) tar upp interna hot som de mest vanliga och Alotaibi, Furnell och Clarke (2017) samt Nohlberg (2009) tar upp människan och den mänskliga faktorn som den svagaste länken i att skydda sin information. Ändå har de flesta respondenter ansett de externa hoten som störst mot deras verksamheter, där respondent 1 ändå påpekat att det beror på vad de gör, men där de svåraste hoten att komma åt är just de interna. Respondent 5 menar även att sårbarheterna kan vara interna, men där hoten är externa. Att sårbarheterna är interna är något som stämmer överens med litteraturen, som menar att det är just människan som är den svagaste länken (Nohlberg, 2009; Alotaibi, Furnell och Clarke, 2017). Att det skiljer sig något från litteraturen kan eventuellt vara en definitionsfråga. Det är möjligt att de intervjuade personerna ser dessa hot som enbart de som varit medvetna hot. Här förklarar dock respondent 3 att de flesta incidenter som varit internt har handlat om att personal inte visste om säkerhetspolicy eller inte tänkte på vad de egentligen borde gjort. Detta är i paritet med vad Doherty och Fulford (2009) nämner som de allra vanligaste övergripande hoten, men ändå nämner externa hot som de största av vad de känner till. En annan anledning till varför det skiljer sig kan vara att de ser hoten utifrån risk och konsekvens. Ett litet småfel av en anställd utan motiv kanske inte kostar organisationen på samma sätt som ett eventuellt intrång från en extern källa hade gjort. I och med att enbart stora företag intervjuats kan även detta ha påverkat då de eventuellt är extra utsatta för externa hot då deras information möjligen ses som mer attraktiv från externa källor sett. Faktum kvarstår att det generellt skiljer sig något i synen på vilka de största hoten är mot vad litteraturen säger.

Sammanfattning:

- Externa hot ses som största hoten mot verksamheten
- Interna sårbarheter men största hoten kommer från externa källor
- Svåraste hoten att komma åt är de interna

6.1.1 Uppdatering

Enligt Ghazvini och Shukur (2018) är det viktigt att anställda är medvetna om potentiella hot och konsekvenserna av deras handlingar. Awawdeh och Tubaishat (2014) tar upp att ett medvetenhetsprogram bland annat ska innehålla viktig information och relevanta hot. Ernst och Young (2009) tar upp att medvetenhetsprogrammen oftast inte är tillräckligt bra då de bland annat inte innehåller aktuella hot. Det är alltså enligt litteraturen viktigt att organisationer håller sig uppdaterade om relevanta hot och vad som sker för att på riktigt kunna erhålla en ökad medvetenhet. Samtliga organisationer som deltagit i studien har grupper av något slag som jobbar med att hålla sig uppdaterade. Detta blir något lättare när det är stora organisationer då de har resurserna till att kunna ha dessa grupper vars syfte är att uppdatera sig. Samtliga företag har även ett antal säkerhetskonsulter som jobbar ute hos kunder vilket gör att de kan hålla sig uppdaterade via en omvärldsspaning. De uppdaterar sig först och främst via nyhetssidor för informationssäkerhet. Om något nytt

hot eller något annat av värde förmedlas detta framförallt via företagens intranät, förutsatt att det berör alla anställda. Respondenterna har varit tydliga med att inte förmedla saker till personer som inte kan påverka. Något som även är återkommande hos samtliga respondenter är att det är viktigt att inte ge för mycket information då det kan ge motsatt effekt. Respondent 1 och 2 menar även på att de i företag A och B även använder sig av mail för att förmedla den här informationen. I företag B använder de ibland även möten för att ta upp frågor kring sådan information enligt respondent 2. Är det något som cirkulerar som har påverkan på flera personer och informationen måste ut snabbt kan de även enligt respondent 5 använda sig av sms.

Sammanfattning:

- Samtliga företag har säkerhetsgrupper som jobbar specifikt med att uppdatera sig om uppkommande hot
- Uppdaterar sig via nyhetssidor och omvärldsspaning
- Analyserar upptäckter om vilka informationen gäller för att inte utge onödig information
- Intranätet används i huvudsak om det gäller samtliga anställda, som exempelvis phishing mail

6.1.2 Prioritering

Endast företag B med respondent 2 och 3 antydde att de fokuserar mer mot människan när det gäller informationssäkerhet. Respondent 1 påpekar att de inte skyltar så mycket med deras tekniska lösningar och att det eventuellt kan finnas en prioritering från ledningshåll, men att de inte upplever det som någon specifik prioritering. Respondent 4 och 5 menar att de helt enkelt fokuserar på båda där människan är den mest konstanta delen som det jobbas på. Samtliga respondenter var tydliga med att de åtminstone fokuserar på människan och inte enbart på den tekniska säkerheten. Detta går hand i hand med vad litteraturen uppmärksammat som en viktig del för att lyckas hålla information säker. Historiskt har mycket fokus lagts på de tekniska säkerhetsåtgärderna för att hålla information säker (Crossler *m.fl.*, 2013). Herath och Rao (2009) beskriver dock teknologi som en utav tre komponenter för att skydda organisationens tillgångar där människan och processerna är de andra. Samtidigt har litteraturen antytt att människan är något som organisationer tenderar att glömma bort eller ignorera (Bashorun, Worwui och Parker, 2013). Detta trots att Ghazvini och Shukur (2018) även antytt att informationssäkerhet som helhet är ett människoproblem och inte ett tekniskt problem. Nohlberg (2009) menar också att människan alltid kommer stå i centrum oavsett vilken metod av attack som sker och D'arcy, Hovav och Galettas (2009) undersökning har visat att de allra flesta incidenter också sker av egen personal. Det är med andra ord enligt litteraturen av största vikt att organisationer lägger stort fokus och en prioritet även på människan inom informationssäkerhet och inte enbart på de tekniska lösningarna. Samtliga företag som ingått i den här studien har varit tydliga med att de prioriterat människan och deras anställda högt i arbetet om informationssäkerhet även om endast Företag B var tydliga med att de prioriterade människan högst. Resterande respondenter valde att påpeka att de fokuserar och prioriterar båda och att de inte vill sätta något mer fokus på det ena över det andra. Att människan är högt prioriterat går dock inte undkomma och detta är med andra ord en skillnad från vad litteraturen antytt att människan är något som ofta ignoreras, då människan varit en utav de absolut största prioriteringarna för både företag A, B och C.

Sammanfattning:

- Fokus ligger på både tekniska och mänskliga åtgärder i företag A och C
- Prioritet på människan i företag B

6.1.3 Ansvar

Khan *M.fl.* (2011) tar upp information som en väsentlig del för organisationer och något som de är högst beroende av. Det blir därav viktigt att även ha ett formellt ansvar kring att skydda just sin information. Samtliga företag som deltagit i studien är delar av en koncern och samtliga har också visst ansvar och krav som tillkommer från den. Däremot skiljer det sig något mellan företagen när det kommer till vad de väljer att benämna och hur de delar upp ansvaret. Både företag A och B har en person som är i huvudsak ansvarig på koncernnivå. Sedan har båda dessa företag en egen ansvarig där respondent 1 menar att det i företag A benämns som informationssäkerhetschef och respondent 3 menar att de benämner den personen som enbart säkerhetschef. Respondent 5 förklarar att de i företag C har tre personer från koncernnivå som ställer krav och en CIO som ansvarar för informationssäkerheten inom företaget. Respondent 3 påpekar också att de har lokalt säkerhetsansvariga ute i verksamheterna. Respondent 1 i företag A är lokalt säkerhetsansvarig, vilket tyder på att även den ansvarsfördelningen kan appliceras på företag A. I företag C talar respondent 5 om att även om de har en person som är formellt ansvarig i form av deras CIO, är det respondent 5 tillsammans med en kollega som även jobbar med företagets informationssäkerhet. Detta tyder på att ett visst ansvar ligger hos dessa, även om det rent formellt är enbart CIO som ansvarar. Samma sak gäller i företag A och B med deras lokala säkerhetsansvariga. Enligt Chang och Lin (2007) krävs det att informationssäkerhet är en nyckelkomponent i företagets planering och ledning för att lyckas säkerställa god informationssäkerhet. Martins och Eloff (2002) tar upp vikten av att ha en dedikerad grupp eller person som ansvarar för informationssäkerheten. Samtliga företag som deltagit i studien har haft både dedikerade grupper och personer som ansvarar för säkerheten i form av grupper eller personer från koncernnivå samt en huvudansvarig på företagen i form av CIO, säkerhetschef eller informationssäkerhetschef. Samtidigt har dessa huvudansvariga haft underställda som har i uppgift att arbeta med företagens informationssäkerhet, som till exempel lokalt säkerhetsansvariga eller informationssäkerhetskoordinatorer. Amankwa, Loock och Kritzinger (2014) menar i sin tur att syftet med ett medvetenhetsprogram är att få anställda att förstå sitt eget ansvar gällande informationssäkerheten. Just det egna ansvaret är något som har påpekats av respondent 1 och 4 i företag A respektive C. Dessa har påpekat att det är väldigt viktigt att förstå att samtliga anställda har ett eget ansvar, även om det formella ansvaret ligger hos en person.

Sammanfattning:

- Krav från koncernnivå
- En person med huvudsakligt ansvar för informationssäkerhet specifikt
- Flertalet personer som arbetar med företagets egen informationssäkerhet
- Samtliga anställda har personligt ansvar

6.1.4 Konsekvenser

Om anställda bryter mot företagets säkerhetsregler ger företag A och C ut varningar där respondent 1 menar att det i företag A kan innebära disciplinära åtgärder i form av löneavdrag. I företag C innebär inte varningarna disciplinära åtgärder i form av löneavdrag utan vid upprepade varningar blir det samtal med närmaste chef där det är upp till chefen vad som sker. I företag B är både respondent 2 och 3 osäkra på vad de har för konsekvenser men där respondent 3 kan tänka sig att det i så fall rör sig om löneavdrag i första hand. Generellt verkar det som att anställda inte känner till just de konsekvenser som blir om de bryter mot säkerhetsreglerna.

Sammanfattning

- Varningar om anställda bryter
- Löneavdrag i företag A och B
- Är det grova brott mot säkerhetsreglerna är den ultimata konsekvensen avsked eller polisanmälan

6.1.5 Ökat engagemang

För att få anställda mer engagerade när det gäller informationssäkerhet talar samtliga respondenter om vikten av att kommunicera på rätt sätt. Respondent 1 menar även att en del i att få ett ökat engagemang är de utbildningar de genomför samt att de ibland går ut med informationssäkerhetsfilmer. I företag B försöker de koppla händelser som skett och fått medial uppmärksamhet för att få en förståelse för att informationssäkerhet är viktig, vilket gör det lättare för anställda att greppa konceptet informationssäkerhet. Företag C och respondent 5 anser att det är just sättet de kommunicerar på som är viktigast för att få till ett ökat engagemang hos anställda. Att de istället för att säga vad de inte får göra, vilket kan göra att anställda blir mindre engagerade då det enbart är massor av krav och begränsningar, istället kommunicerar ut de risker som finns och hur en anställd bör tänka. Respondent 4 anser utbildningarna samt att de som företag har informationssäkerhet högt upp på agendan och helt enkelt pratar om säkerhetsfrågor som en bidragande orsak till hur de får anställda mer engagerade.

Det har fastställts att människan är en viktig del av säkerheten där bland annat Nohlberg (2009) påpekat att människan står i centrum oavsett vilken attack som sker och Ghazvini och Shukur (2018) menar att informationssäkerhet i huvudsak är ett människoproblem. Därför blir det också viktigt att anställda har ett engagemang när det gäller informationssäkerheten i organisationerna. Att samtliga respondenter talat om olika sätt att kommunicera på är även i linje med Martins och Eloff (2002) som menar att kommunikation bör vara en del av just informationssäkerheten tillsammans med människorna, träning och processerna. Respondent 3 och 5 i företag B respektive C har talat specifikt om vikten av att kommunicera på rätt sätt för att göra det lätt för anställda att greppa vad som kommuniceras ut. Detta är något som Ghazvini och Shukur (2018) påpekat som väldigt viktigt för att kunna uppnå ett ändrat beteende, att anställda förstår det som kommuniceras.

Sammanfattning:

- Kommunikation - inte kommunicera ut informationssäkerhet som en lång lista med vad som inte är tillåtet, utan kommunicera ut de risker som finns och hur en anställd bör tänka för att skydda informationen.

- Utbildningar
- Informationsfilmer kopplat till informationssäkerhet
- Koppla information till verkliga händelser som fått medial uppmärksamhet
- Att de som företag har informationssäkerhet högt upp på agendan och pratar mycket om det

6.2 Säkerhetsmedvetenhet

Samtliga respondenter har påstått att säkerhetsmedvetenheten är viktig och respondent 2 och 3 menar att det är det absolut viktigaste. Alotaibi, Furnell och Clarke (2017) har påpekat att medvetenheten hos anställda har en direkt positiv koppling till anställdas säkerhetsbeteende och följandet av organisationens säkerhetspolicy. Bashorun, Worwui och Parker (2013) antyder att människan ofta ignoreras i informationssäkerhetsarbetet. I och med att samtliga företag har både informationssäkerhet och människan väldigt högt upp på agendan i deras arbete med informationssäkerheten är det inget som kan appliceras på de företag som deltagit i denna studie. En sak som skiljer sig från litteraturen är att ingen av respondenterna har pratat i termer om att de använder sig av ett medvetenhetsprogram. I företag A och C har de dock en kontinuerlig plan när det gäller framförallt utbildningar, men även andra sätt att öka medvetenheten på med bland annat punktinsatser i företag C och informationsfilmer i företag A. Utbildningar samt punktinsatserna och informationsfilmer är något som med jämna mellanrum genomförs. Med andra ord är det ingen engångsföreteelse. Just att det är ett kontinuerligt arbete är precis det som Peltier (2005) tar upp som viktigt för att uppnå effekt. Även Ghazvini och Shukur (2018) tar upp vikten av att programmen måste utföras flertalet gånger för att kunna ändra på anställdas attityd samtidigt som det i många fall är just en engångsföreteelse. Företagen som deltagit i den här studien har samtliga haft ett kontinuerligt arbete när det gäller att öka säkerhetsmedvetenheten. Dock har enbart företag A och C haft kontinuerliga utbildningar.

Sammanfattning:

- Säkerhetsmedvetenheten är av företagen ansedda som en extremt viktig del i att hålla informationen säker
- Talar inte i termer om medvetenhetsprogram
- Samtliga företag arbetar specifikt mot en ökad säkerhetsmedvetenhet
- Kontinuerligt arbete

6.2.1 Säkerhetskultur

Samtliga företag menar att de jobbar med säkerhetskulturen inom organisationen. Martins och Eloff (2002) menar att informationssäkerhet bör vara en del av organisationskulturen samtidigt som det handlar om vad som är accepterat och inte accepterat inom organisationen. De menar även att det är viktigt att organisationen har informationssäkerhet som prioritet och ett ansvar kring informationssäkerhet och att anställda får vägledning i vad som är accepterat eller inte accepterat. Att samtliga företag har informationssäkerhet och framförallt människan som en prioritet finns beskrivet i kapitel 6.1.2 och att de har ett formellt ansvar kan läsas i kapitel 6.1.3. Respondent 1 menar att de begränsningar de gör tillsammans med utbildningarna är något som bidrar till en säkerhetskultur samtidigt som de noggrant går igenom introduktionen där informationssäkerheten är en viktig del med samtliga nyanställda.

Respondent 3 menar att de inte har en aktiv plan i dagsläget med hur de ska jobba med kulturen men där det måste börja med ledningen och säkerhetspolicyn. Detta är något som även går hand i hand med Martins och Eloff (2002) som menar att ledningen måste ha informationssäkerhet och visa sitt engagemang i att implementera informationssäkerhet i organisationen. I samtliga företag har utbildningar påpekats som ett bidrag i att öka säkerhetsmedvetenheten och respondent 5 påpekar även de punktinsatser de utför som ytterligare en bidragande orsak till att få in en säkerhetskultur. Martins och Eloff menar att det är anställdas beteende som är en faktor i en informationssäkerhetskultur. Att samtliga företag tagit upp utbildningar som en bidragande faktor till en säkerhetskultur är därför i linje med litteraturen med det faktum att Khan *m.fl.* (2011) tagit upp just utbildningspresentationer som en teknik i att faktiskt uppnå ett ändrat beteende hos anställda. Ghazvini och Shukur (2018) tar upp årlig översikt och uppdatering av programmen för att hålla det relevant som ett krav i att lyckas uppnå en förändring i kulturen. Företag A och C har påpekat att de jobbar kontinuerligt med att uppdatera sina utbildningar och punktinsatser vilket därav går i linje med det som Ghazvini och Shukur (2018) har som krav för en förändrad kultur.

Sammanfattning:

- Informationssäkerhet prioritet
- Tydligt ansvar inom informationssäkerhet
- Begränsningar av vad som är tillåtet bidrar till kulturen
- Introduktion för nyanställda där informationssäkerheten är en viktig del
- Kontinuerliga utbildningar bidrar till en säkerhetskultur
- Kontinuerliga punktinsatser bidrar till en säkerhetskultur
- Kontinuerliga uppdateringar av utbildningsmaterial och punktinsatser för att hålla det relevant

6.2.2 Standard och policy

Samtliga intervjuade företag har haft delar i organisationen som är certifierade enligt ISO 27000 serien. Respondent 1 menar att den del som de tillhör i företag A är certifierade. Respondent 3 menar att de är precis i uppstarten av att bli certifierade och Respondent 5 menar att deras outsourcingavdelning är certifierad enligt ISO 27000. ISO 27002 (2017) tar bland annat upp att de utbildningar som sker bör omfatta de säkerhetsregler och skyldigheter som finns definierade i bland annat standarder. Att de regler som kommer från deras certifieringar från ISO 27000 finns med i deras utbildningar är inte något som framkommit. Respondent 5 menar däremot att de ser till att standarden följs genom att den avdelning som är certifierad är väldigt processtyrd. Det framkommer även av respondent 1 att deras fördjupade informationssäkerhetsutbildning har ett block gällande företagets ledningssystem för informationssäkerhet. Detta skulle kunna ses som att de tagit med bestämmelser från standarden in i utbildning, men då det endast är i den fördjupade kursen är det inte något som förmedlas till samtliga anställda. Samtliga respondenter har även varit tydliga med att inte delge onödig information. Detta kan vara en anledning till att de inte tar med de krav som kommer från standarden i utbildningen då det enbart är vissa avdelningar som är certifierade och inte alla.

När det gäller företagens säkerhetspolicy överblickar samtliga företag sin policy och gör uppdateringar när det behövs. Bland annat är det enligt Martins och Eloff (2002) viktigt

att granska sin informationssäkerhetspolicy och göra den till en del i det vardagliga arbetet. Ghazvini och Shukur (2018) menar att en del utav det huvudsakliga innehållet i ett medvetenhetsprogram är just säkerhetspolicyn. I ISO 27001 menar de att ett av de krav som finns för medvetenhet är att anställda ska vara medvetna om just informationssäkerhetspolicyn. I företag A talar respondent 1 om vikten av att göra en sammanfattning och att sprida information om policyn som hur de tillämpar den för att den ska förstås. Respondent 1 menar att de i företag A har säkerhetspolicyn med i de utbildningar de utför, men i sammanfattad form. Att göra en sammanfattning av policyn för att den lättare ska förstås går i linje med vad Ghazvini och Shukur (2018) säger om att det är viktigt att innehållet i ett medvetenhetsprogram förstås för att kunna uppnå ett ändrat beteende. Samtliga företag har även säkerhetspolicyn på intranätet att tillgå för alla anställda. Respondent 3 påpekar att de har en uppdaterad säkerhetspolicy men där de inte är riktigt klara med hur den ska marknadsföras. Respondent 1 menar att de sprider ändringar i policyn via intranätet, affischering och mail. I företag C menar respondent 5 att de främst sprider säkerhetspolicyn via intranätet. Respondent 5 är även tydlig med att den inte är en del av utbildningen, men att de går igenom den och uppdaterar den vid behov en gång per år. När den väl uppdateras läggs en nyhet upp på intranätet. Att policyn granskas är med andra ord något som samtliga företag gör. Respondent 5 påpekar även att deras säkerhetspolicy är en del i deras introduktionsprogram för nyanställda, där det är ett krav att de läser igenom den. Amankwa, Loock och Kritzinger (2014) tar upp att utbildningen ska sträva efter en förståelse för de dokument gällande informationssäkerhet som finns. I företag B och C har säkerhetspolicyn inte varit ett av de dokument som ingår i utbildningen och därav skiljer det sig något från litteraturen. Ghazvini och Shukur (2018) samt standarden ISO 27001 (2017) tar upp att det enbart är viktigt att anställda är medvetna om policyn och beskriver inte att det är ett krav i den utbildning som sker. Detta är däremot något som samtliga företag som deltagit i studien gör då policyn finns att tillgå på intranätet samtidigt som de uppdateringar som görs förmedlas ut till anställda.

Sammanfattning:

- Delar är certifierade enligt ISO 27000
- Standarden följs genom väl inarbetade processer
- Säkerhetspolicyn i sammanfattad form i utbildningar med förmedlingen om hur den ska tillämpas
- Säkerhetspolicyn finns att tillgå på intranätet
- Viktigt att förmedla en sammanfattning av säkerhetspolicyn för att anställda lättare ska förstå
- Samtliga nyanställda måste läsa företagets säkerhetspolicy
- Årlig överblick och uppdatering av policyn vid behov
- Förändringar i säkerhetspolicyn förmedlas antingen via nyhet på intranätet, mail eller affischering

6.2.3 Informationsspridning

Awawdeh och Tubaishat (2014) menar att ett medvetenhetsprogram ska motivera och stimulera anställda och påminna dem om de konsekvenser och inverkan det har om informationssäkerhet inte tas på allvar. Samtidigt menar de även att ett medvetenhetsprogram uppnår ett ändrat säkerhetsbeteende genom att påpeka viktig information eller relevanta hot och tar upp ett antal exempel som bland annat videos,

nyhetsbrev, sociala medier, konferenser, föreläsningar, sms, datorbaserad träning och olika tävlingar. Amankwa, Loock och Kritzinger (2014) delade upp ett informationssäkerhetsprogram i olika delar där ett medvetenhetsprogram hade fokus att rikta uppmärksamhet och påminna anställda om informationssäkerhet. Ramverket för jämförelse av begreppen informationssäkerhetsutbildning, informationssäkerhetsträning och informationssäkerhetsmedvetenhet kan ses i figur 4. Informationsspridning skulle i det här fallet befinna sig inom begreppet informationssäkerhetsmedvetenhet. Begreppen utbildning och träning tas upp i kapitel 6.2.4. Metoder för förmedling av informationssäkerhetsmedvetenhet enligt Amankwa, Loock och Kritzinger (2014) är tryckt och elektronisk media som exempelvis videos, flygblad eller affischering. Khan *m.fl.* testade olika tekniker där topp tre var gruppdiskussioner, utbildningspresentationer och mail.

De informationsspridningskanaler som i huvudsak används av de deltagande företagen menar samtliga respondenter är intranätet, där de sprider den mesta informationen gällande informationssäkerhet. Att arbeta med medvetenheten via ett intranät är inget som har tagits upp i litteraturen vilket är något som skiljer sig. Respondent 1 menar att utöver att använda sig av intranätet för informationsspridning använder de i företag A även mail och affischering, vilket även respondent 5 påpekar att de gör i företag C. Mail och affischering var en del av den undersökning Khan *m.fl.* (2011) genomfört där mail var det tredje mest effektiva sättet att öka medvetenhet på. Mail var en komponent av kunskap, attityd samt intention. Affischering var i sin tur enbart en komponent av kunskap och attityd. Att de använder sig av affischering och mail är något som enligt Khan *m.fl.* (2011) bidrar till en ökad medvetenhet. Respondent 1 menar även att de använder sig av videos för att förmedla information om det är någon större ändring som har skett. Videos var inte en del av Khan *m.fl.* (2011) undersökning och effekten av just videos på medvetenheten är därför okänd. Däremot nämner både Amankwa, Loock och Kritzinger (2014) samt Awawdeh och Tubaishat (2014) att videos är en utav de tekniker som används för ökad medvetenhet.

Respondent 1 och 2 tar även upp möten som ett sätt de sprider information på. Möten är något som inte funnits som exempel i litteraturen som en teknik för ökad medvetenhet, möjligen för att det endast är internt för de som deltar i mötet och inte ut mot samtliga anställda. Respondent 5 tar även upp att även om intranät och mail är de primära kanalerna för informationsspridning samtidigt som de använder affischering, använder de även sms om det är något större som påverkar många människor och som behöver komma ut snabbt. Användandet av sms påpekar även Awawdeh och Tubaishat (2014) som en utav teknikerna för att öka medvetenheten. Många utav de tekniker som nämnts i litteraturen används alltså av företagen som deltagit i denna studie.

Sammanfattning:

- Primärt är det intranätet och mail som används för informationsspridning
- Affischering i form av lappar eller skärmar ute i lokalerna
- Informationsfilmer om större ändringar sker
- Möten används till viss del för att sprida information
- Sms om något större sker som påverkar många människor och informationen behöver komma ut snabbt

6.2.4 Utbildningar

Khan *m.fl.* (2011) tar upp i sin femstegsmodell att målet med att öka medvetenheten är att tillslut uppnå ett ändrat beteende. I sin studie var det enbart två tekniker utav de tekniker som testats som faktiskt var tillräckligt effektiva att uppnå ett ändrat beteende, vilket var utbildningspresentationer och gruppdiskussioner. Awawdeh och Tubaishat (2014) tar upp att för att uppnå ett ändrat säkerhetsbeteende behöver utbildning och påpekandet av viktig information eller relevanta hot genomföras. Även ISO 27002 (2017) tar upp att alla organisationens anställda och leverantörer bör erhålla lämplig utbildning och fortbildning för ökad medvetenhet. Standarden tar också upp att dessa kan utföras på olika sätt som till exempel självstudier, webbaserad, distans eller klassrumsbaserad. Vidare menar även Hallberg *m.fl.* (2017) att anställdas syn på informationssäkerhet utvecklas genom utbildningar med syfte att öka medvetenheten och förståelsen för informationssäkerhet inom organisationen.

I litteraturen är med andra ord utbildningar en viktig del om en ökad medvetenhet ska kunna uppnås och i slutändan ett ändrat säkerhetsbeteende. Samtliga respondenter har varit tydliga med att de utför utbildningar på ett eller annat sätt samt att respondent 1, 3 och 5 ansett just utbildningar som det viktigaste för att öka medvetenheten hos anställda. I samtliga företag som deltagit i studien har de även använt sig av webbaserade utbildningar i första hand via E-learning. Att utbildningar sker och även är en stor del i arbetet att öka medvetenheten går därför i linje med det som litteraturen påpekat som en viktig faktor i ökad medvetenhet. Däremot är det endast i företag A där de har extra utbildningsmaterial och skiljer på utbildning baserat på vilken roll i företaget de har. Där berättar dock respondent 5 att de gällande utbildningen för GDPR skiljde på utbildningsmaterial och hade en extra kurs för chefer. Dock är det inget som generellt gäller för de årliga obligatoriska utbildningar de genomför. Något som ISO 27002 (2017) beskrivit att utbildningen ska göra, samtidigt som utbildningen ska ske regelbundet och när personal är ny eller byter roller. Att skilja på utbildningsmaterial baserat på roll är med andra ord inte något som görs i stor bemärkelse, då det enbart är i företag A detta sker. Däremot påpekar samtliga respondenter att de har specifika utbildningar och att de är en viktig del för ny personal, vilket också standarden antyder. Att utbilda ny personal inom informationssäkerhet är med andra ord något som samtliga företag tar på största allvar, något som även går i linje med litteraturen. I företag A berättar även respondent 1 att de två gånger per år även har lärarledda utbildningar i sal, som dock inte är obligatoriska och som anställda kan gå om de vill fördjupa sina kunskaper, där kursen angående informationssäkerhet pågår i två dagar. Det finns med andra ord möjligheter även till klassrumsbaserade utbildningar även om det inte är det som ses som standard. Respondent 5 menar att de i dagsläget inte har några lärarledda utbildningar, men att det kommer att komma framöver i och med arbetet de gör med ISO 27000.

Peltier (2005) menar även att det är viktigt att ett informationssäkerhetsprogram sker kontinuerligt med årlig uppföljning för att kunna uppnå effekt. Även Ghazvini och Shukur (2018) menar att ett program för att öka medvetenhet behöver utföras fortlöpande, samt också kontinuerligt uppdateras och förbättras för att ge önskad effekt. Det är egentligen bara i företag B där det inte sker utbildningar kontinuerligt. I övrigt har de både i företag A och C både kontinuerliga utbildningar som behöver genomföras inom ett visst årsintervall men de genomför även kontinuerligt en översyn av utbildningar för att de hela tiden ska vara relevanta. Detta är alltså något som går i linje

med vad litteraturen påpekat som viktigt för att utbildningarna och programmen som helhet ska lyckas ge någon effekt.

När det gäller innehåll i utbildningar har bland annat respondent 1 förklarat att deras mest grundläggande kurs innehåller delar om informationssäkerhet, anläggningssäkerhet, personalsäkerhet, resesäkerhet samt incidenthantering. Även företagets säkerhetspolicy är en del av utbildningsmaterialet enligt respondent 1. Det huvudsakliga innehållet i ett medvetenhetsprogram bör enligt Ghazvini och Shukur (2018) vara den interna säkerhetspolicyn, de huvudsakliga hoten mot informationstillgångar, grundläggande skyddsåtgärder samt incidenthantering. Utbildningsmaterialet i företag A är mycket omfattande och täcker gott och väl de delar som litteraturen antyder som viktig. Respondent 5 menar att de i företag C inte har säkerhetspolicyn som en del i utbildningsmaterialet som sker kontinuerligt, dock är den en viktig del i programmet för nyanställda, då de måste läsa den. Företag B genomför inte kontinuerliga utbildningar, dock är säkerhetspolicyn även där en del av programmet för nyanställda. Här skiljer det sig något med hur företagen förmedlar policyn, då den inte är en del av just utbildningen i samtliga företag. Litteraturen tar dock inte upp i klartext att det bästa är att policyn ska vara del av just utbildningen, utan enbart att den ingår i programmet och förmedlas. Enligt Amankwa, Loock och Kritzinger (2014) är fokuset med utbildningar att ge en insikt och förståelse angående informationssäkerhet. Syftet med utbildningarna är sedermera att göra anställda mer kompetenta gällande informationssäkerhet. Både i företag A och C har de kontinuerliga utbildningar med ett brett utbud, vilket logiskt borde bidra till att göra anställda mer kompetenta gällande informationssäkerhet och är därför i enlighet med litteraturen. Den utbildning som sker i företag B för nyanställda tar upp de grundläggande inom informationssäkerhet för att samtliga anställda ska ha en grundförståelse, vilket också gör anställda mer kompetent. I företag B genomför de dock inte kontinuerliga utbildningar, vilket Peltier (2005) och Ghazvini och Shukur påpekat som viktigt.

Något som samtliga respondenter tagit upp som inte påpekats i litteraturen är det faktum att de ansett att det är av stor vikt att utbildningarna är korta och effektiva. Respondenterna menar att långa utbildningar och mycket information tillslut kan leda till mindre motivation att följa bestämmelser, då informationssäkerhet istället blir något negativt och tråkigt. En annan sak är att utbildningarna kan göras på vilken enhet som helst, då det leder till att inte mycket av anställdas arbetstid behöver tas. Johnson (2006) tar upp tiden som anställda lägger på kurser som en av de kostnader som medvetenhetsprogrammen medför. Att de är korta och kan göras vart som helst är ett sätt som företagen som deltagit i studien kommer undan det problemet. Efter avklarade kurser behöver de även i företag A och C svara på frågor, vilket även det är kunskapshöjande då det får anställda att tänka till. En annan sak som respondenterna tagit upp som inte framkommer i litteraturen är att de även är noga med hur saker i utbildningarna, men även generellt hur information gällande informationssäkerheten bör förmedlas. Respondent 5 påpekar att de utformar sina utbildningar för att få anställda att tänka till själva, istället för att låta utbildningarna vara faktatunga. De fokuserar på att koppla innehållet i utbildningarna till vardagliga händelser, för att göra det lättare för anställda att förstå det som förmedlas. Även detta är en sak som görs för att inte utbildningarna ska ha motsatt effekt på motivationen mot informationssäkerhet för anställda, och för att öka förståelsen.

Respondent 5 tar också upp att de med jämna mellanrum genomför punktinsatser där de bland annat skickar ut phishingmail till anställda för att testa sina anställda. I nästa punktinsats planerar de en punktinsats specifikt för ledning och ekonomiavdelningen. ISO 27002 (2017) tar upp att ett utbildningsprogram även bör ta upp ett antal kunskapshöjande aktiviteter som exempelvis kampanjer, broschyrer eller nyhetsbrev. Dessa punktinsatser kan ses som detsamma som kampanjer och stämmer därför överens med det som standarden tar upp som kunskapshöjande aktivitet.

Sammanfattning:

- Utbildningar i form av E-learning
- Grundläggande material som bas för samtliga anställda
- Extra utbildningar baserat på roll
- Specifik utbildning för nyanställda
- Utbildningar behöver göras om inom angivet årsintervall
- Kontinuerlig översikt och förbättring av utbildningsmaterial
- Säkerhetspolicy i sammanfattad form med i utbildningsmaterial
- Möjlighet till fördjupade kurser, både inom E-learning och lärarledda kursdagar
- Korta och effektiva utbildningar, för att inte ta för mycket tid från anställda
- Kan göras på vilken enhet som helst, för att vidare öka effektiviteten
- Frågor efter avklarad kurs
- Utformade utbildningar utifrån vardagliga händelser och som får anställda att tänka efter
- Inte faktatunga, för att undvika motsatt effekt på attityd mot informationssäkerhet
- Kontinuerliga punktinsatser, exempelvis phishingmail för att testa anställda
- Specifika punktinsatser för extra utsatta grupper, exempelvis VD-bedrägerimail till ledning eller ekonomiavdelning

6.2.5 Framtid

När respondenterna pratar om vad de tror blir viktigt för framtiden tror respondent 1 att det bland annat blir viktigt att tänka på att mer information inte automatiskt ger högre säkerhetsmedvetenhet, utan att det i slutändan kan leda till informationsöverbelastning. Även respondent 3 och 5 talar om vikten av att inte göra informationssäkerhet för tungt. Just att inte delge för mycket information är inte något som är återkommande i litteraturen. Litteraturen har mer fokuserat på vad som behöver göras mer, snarare än det faktum att det faktiskt också kan bli för mycket och att det i sådant fall kan ge motsatt effekt. Detta är alltså något som respondenterna påpekat som viktigt att tänka på för framtiden. Respondent 1 har även påpekat begränsningar ibland gör anställda mer medvetna, och att därför inte tillåta alternativa sätt att kringgå säkerhetslösningar, då dessa säkerhetslösningar kan få anställda att tänka till extra. Även detta är något som det inte finns mycket om i litteraturen gällande just säkerhetsmedvetenheten.

Respondent 1 fortsätter även med att det är viktigt att förmedla varför det är viktigt att följa bestämmelser för att lyckas få den acceptansen som behövs från anställda. Detta kan kopplas till det Amankwa, Loock och Kritzinger (2014) tar upp om att informationssäkerhetsutbildning syftar till att öka kompetens och kunskap anställda besitter genom att sträva efter en förståelse för de dokument gällande

informationssäkerhet som finns. Även Hallberg m.fl. (2017) menar att synen på informationssäkerhet utvecklas genom utbildningar med syfte att öka medvetenheten och förståelsen för informationssäkerhet. Just förståelsen är precis det som det handlar om när förmedlingen om varför det är viktigt sker, vilket är i linje med en utav de faktorer som är viktiga när det arbetas med medvetenheten, just förståelsen. Den definitionen som använts i den här studien för säkerhetsmedvetenhet är just den förståelse, kunskap och attityd anställda besitter gentemot området informationssäkerhet. Även den definitionen tar upp förståelse. Litteraturen tar med andra ord upp förståelse som en komponent av medvetenhet och det är även det som uppnås när förmedlingen om varför det är viktigt görs.

Respondent 2 hade för deras företag velat se ett bra utbildningspaket vid nyanställning som är specifikt riktat mot den tjänst den anställde ska ha samt en årlig uppdatering via antingen en föreläsning eller E-kurs. Att det ska vara riktat mot den tjänst den anställde ska ha tar ISO 27002 (2017) upp som något en utbildning bör göra samtidigt som den bör genomföras regelbundet. Även Peltier (2005) och Ghazvini och Shukur (2018) tar upp vikten av att arbetet med informationssäkerheten sker kontinuerligt. Deras önskemål om framtiden är därav något som går hand i hand med det som litteraturen påpekar som viktigt. Även respondent 4 menar att det är viktigt att ha en bra grund hos samtliga anställda samt att de fortsätter fräscha upp och uppdatera sig för att hålla saker relevant.

Respondent 5 tycker att de kan göra än mer med medvetenheten samt att de kan utföra fler av de punktinsatser som de genomfört, då de ansett detta gett positiva och intressanta resultat. Samtidigt har de talat om att eventuellt utföra obligatoriska utbildningar för de som klickar på ett utav företagets eget phishingmail. Detta är något som kan kopplas tillbaka till det som diskuterats tidigare om att inte ge ut för mycket information, då detta är något som innebär att endast de som råkat ut för det och gjort misstaget själva som behöver gå utbildningen. Detta är möjligen ett relativt nytt koncept, då det inte finns mycket skrivet i litteraturen om dessa typer av punktinsatser.

Sammanfattning:

- Viktigt att inte ge ut för mycket information, då detta kan leda till informationsöverbelastning
- Göra begränsningar utan möjlighet att kringgå säkerhetslösningar, vilket kan öka medvetenheten då det får anställda att tänka till varför det är begränsningar
- Viktigt att förmedla varför det är viktigt att följa bestämmelser, för att öka förståelsen för varför exempelvis vissa regelverk eller begränsningar finns
- Grundpaket för nyanställda riktade mot den tjänst de ska ha
- Viktigt att uppdatera kunskaperna med jämna mellanrum
- Jobbas mer med anställdas medvetenhet
- Mer punktinsatser
- Obligatoriska utbildningar för de som faller för exempelvis phishingmail anordnade av företaget själva

7 Resultat och slutsatser

Resultatet har uppkommit utifrån den analys som har gjort och kan ses i sin helhet i tabell 1. De säkerhetsföretag som deltagit i studien har haft människorna och deras medvetenhet högt upp på agendan. Framförallt har utbildningar varit en stor del av arbetet mot en ökad medvetenhet. Precis det som Awawdeh och Tubaishat (2014) tar upp är utbildningar, tillsammans med påpekandet av viktig information eller relevanta hot viktigt för att ändra ett säkerhetsbeteende. Samtliga av dessa delar är något som resultatet också visar att de faktiskt jobbar med. De utför utbildningar kontinuerligt, de uppdaterar sig ständigt om relevanta hot eller information som florerar ute i världen kring området informationssäkerhet. Samtidigt visar resultatet också hur dessa företag ser hur förmedlingen sker av information som en viktig faktor i deras arbete för ökad medvetenhet. Ghazvini och Shukur (2018) har påpekat vikten av att anställda förstår det som förmedlas, vilket också resultatet av den här studien visar att de deltagande företagen jobbar målmedvetet med. Samtliga identifierade kategorier tillsammans med sammanfattat material finns presenterat i tabell 1 nedan.

Tabell 1 - Resultat

Kategori	Sammanfattning
Informationssäkerhet	• Externa hot ses som största hoten mot verksamheten • Interna sårbarheter men största hoten kommer från externa källor • Svåraste hoten att komma åt är de interna
Uppdatering	• Samtliga företag har säkerhetsgrupper som jobbar specifikt med att uppdatera sig om uppkommande hot • Uppdaterar sig via nyhetssidor och omvärldsspaning • Analyserar upptäckter om vilka informationen gäller för att inte utge onödig information • Intranätet används i huvudsak om det gäller samtliga anställda, som exempelvis phishing mail
Prioritering	• Fokus ligger på både tekniska och mänskliga åtgärder i företag A och C • Prioritet på människan i företag B
Ansvar	• Krav från koncernnivå • En person med huvudsakligt ansvar för informationssäkerhet specifikt • Flertalet personer som arbetar med företagets egen informationssäkerhet • Samtliga anställda har personligt ansvar
Konsekvenser	• Varningar om anställda bryter

	• Löneavdrag • Är det grova brott mot säkerhetsreglerna är den ultimata konsekvensen avsked eller polisanmälan
Ökat engagemang	• Kommunikation - inte kommunicera ut informationssäkerhet som en lång lista med vad som inte är tillåtet, utan kommunicera ut de risker som finns och hur en anställd bör tänka för att skydda informationen. • Utbildningar • Informationsfilmer kopplat till informationssäkerhet • Koppla information till verkliga händelser som fått medial uppmärksamhet • Att de som företag har informationssäkerhet högt upp på agendan och pratar mycket om det
Säkerhetsmedvetenhet	• Säkerhetsmedvetenheten är av företagen ansedda som en extremt viktig del i att hålla informationen säker • Talar inte i termer om medvetenhetsprogram • Samtliga företag arbetar specifikt mot en ökad säkerhetsmedvetenhet • Kontinuerligt arbete
Säkerhetskultur	• Informationssäkerhet prioritet • Tydligt ansvar inom informationssäkerhet • Begränsningar av vad som är tillåtet bidrar till kulturen • Introduktion för nyanställda där informationssäkerheten är en viktig del • Kontinuerliga utbildningar bidrar till en säkerhetskultur • Kontinuerliga punktinsatser bidrar till en säkerhetskultur • Kontinuerliga uppdateringar av utbildningsmaterial och punktinsatser för att hålla det relevant
Standard och Policy	• Delar är certifierade enligt ISO 27000 • Standarden följs genom väl inarbetade processer • Säkerhetspolicyn i sammanfattad form i utbildningar med förmedlingen om hur den ska tillämpas • Säkerhetspolicyn finns att tillgå på intranätet • Viktigt att förmedla en sammanfattning av säkerhetspolicyn för att anställda lättare ska förstå • Samtliga nyanställda måste läsa företagets

	säkerhetspolicy • Årlig överblick och uppdatering av policyn vid behov • Förändringar i säkerhetspolicyn förmedlas antingen via nyhet på intranätet, mail eller affischering
Informationsspridning	• Primärt är det intranätet och mail som används för informationsspridning • Affischering i form av lappar eller skärmar ute i lokalerna • Informationsfilmer om större ändringar sker • Möten används till viss del för att sprida information • Sms om något större sker som påverkar många människor och informationen behöver komma ut snabbt
Utbildningar	• Utbildningar i form av E-learning • Grundläggande material som bas för samtliga anställda • Extra utbildningar baserat på roll • Specifik utbildning för nyanställda • Utbildningar behöver göras om inom angivet årsintervall • Kontinuerlig översikt och förbättring av utbildningsmaterial • Säkerhetspolicy i sammanfattad form med i utbildningsmaterial • Möjlighet till fördjupade kurser, både inom E-learning och lärarledda kursdagar • Korta och effektiva utbildningar, för att inte ta för mycket tid från anställda • Kan göras på vilken enhet som helst, för att vidare öka effektiviteten • Frågor efter avklarad kurs • Utformade utbildningar utifrån vardagliga händelser och som får anställda att tänka efter • Inte faktatunga, för att undvika motsatt effekt på attityd mot informationssäkerhet • Kontinuerliga punktinsatser, exempelvis phishingmail för att testa anställda • Specifika punktinsatser för extra utsatta grupper, exempelvis VD bedrägerimail till ledning eller ekonomiavdelning
Framtid	• Viktigt att inte ge ut för mycket information, då detta kan leda till informationsöverbelastning • Göra begränsningar utan möjlighet att kringgå

	säkerhetslösningar, vilket kan öka medvetenheten då det får anställda att tänka till varför det är begränsningar • Viktigt att förmedla varför det är viktigt att följa bestämmelser, för att öka förståelsen för varför exempelvis vissa regelverk eller begränsningar finns • Grundpaket för nyanställda riktade mot den tjänst de ska ha • Viktigt att uppdatera kunskaperna med jämna mellanrum • Jobbas mer med anställdas medvetenhet • Mer punktinsatser • Obligatoriska utbildningar för de som faller för exempelvis phishingmail anordnade av företaget själva

Följande frågeställning har behandlats i denna studie: ”Hur arbetar säkerhetsföretag med att höja sina medarbetares säkerhetsmedvetenhet”.

Resultatet av denna studie visar att företagen prioriterar säkerhetsmedvetenheten och därmed arbetar specifikt med målet att öka sina anställdas medvetenhet. Företagen har ett tydligt formellt ansvar när det gäller informationssäkerhet och har det högt på agendan i företagsledningen. För att hålla sig uppdaterade om nya hot som tillkommer har de grupper inom organisationen som håller sig uppdaterade främst via nyhetssidor, samtidigt som de har en omvärldsspaning i form av säkerhetskonsulter. Om anställda bryter mot säkerhetsregler ger de ut varningar vilket i första hand kan innebära löneavdrag.

För att få anställda mer engagerade när det gäller organisationens informationssäkerhet fokuserar de mycket på hur information kommuniceras ut. De försöker att inte kommunicera ut informationssäkerhet som en lång lista med vad som inte är tillåtet, utan att istället informera om de risker som finns och hur en anställd bör tänka för att skydda informationen. De kopplar information till händelser som fått stor medial uppmärksamhet för att öka förståelsen. Företagen som deltagit i studien utför utbildningar och vissa går även ut med informationsfilmer med jämna mellanrum, samtidigt som de pratar mycket om det utåt vilket sänder signaler om att det är viktigt.

För att jobba mot att nå och bibehålla en säkerhetskultur inom organisationen, vilket påverkar medvetenheten, är en bidragande faktor att informationssäkerhet är en prioritet med ett tydligt ansvar kring informationssäkerheten. De gör begränsningar, bland annat i lokalerna vilket ytterligare påpekar vikten av informationssäkerhet. De har en noggrann introduktion till nyanställda där informationssäkerhet är en viktig del. De utför kontinuerligt utbildningar och punktinsatser samtidigt som de ständigt utför uppdateringar av dessa för att de hela tiden ska vara relevanta.

De delar som är certifierade enligt ISO 27000 serien är väldigt processtyrda och följs genom att egentligen följa de processer de satt upp. Säkerhetspolicyn finns som den är

att tillgå på intranätet och i sammanfattad form i utbildningar. Det är önskvärt att förmedla den i sammanfattad form med hur tillämpningen sker för att göra det lättare för anställda att förstå vad det faktiskt innebär. I introduktionsprogrammet för nyanställda måste samtliga läsa igenom policyn i samband med anställning. Det sker årlig översyn av policyn med ändringar vid behov. Sker ändringar förmedlas detta antingen via intranätet, mail eller affischering i form av lappar eller skärmar ute i lokalerna.

För generell informationsspridning gällande informationssäkerhet är det i huvudsak intranätet och mail som används. Är det mindre viktig information kan affischering användas med lappar eller skärmar ute i lokalerna och sker större ändringar kan en ny informationsfilm komma ut. Till viss del sprids även information på gruppmöten. Om något större sker som påverkar många människor och som behöver komma ut snabbt kan sms användas för att sprida information om informationssäkerhetsfrågor.

Det stora arbetet sker med utbildningar vilket även ses som den viktigaste aktiviteten som genomförs för att öka medvetenheten. De utbildningar som sker är i huvudsak via E-learning med ett grundläggande material för samtliga anställda med skillnader baserat på roll. Nyanställda får en specifik utbildning som del i introduktionsprogrammet. Det finns fördjupade kurser både inom E-learning samt kursdagar där anställda kan åka till där det är lärarledda föreläsningar om informationssäkerhet i två dagar. Säkerhetspolicyn finns som kursmaterial i sammanfattad form. Utbildningsmaterialet är inte faktatungt för att undvika att det leder till motsatt effekt på attityden mot informationssäkerhet. Utbildningarna är fokuserade på att koppla till vardagliga händelser för att anställda lättare ska kunna förstå det som förmedlas och som får anställda att tänka efter. De kurser som genomförs har ett antal moduler som fokuserar på olika områden inom informationssäkerhet. Modulerna är korta för att inte ta för mycket tid och låsa anställda under lång tid, samtidigt som det bidrar till att inte göra det lika tungt med för mycket på samma gång. Dessutom kan dessa kurser utföras på vilken enhet som helst. Efter avklarad kurs behöver anställda svara på ett antal frågor. De utbildningar som genomförs behöver göras om inom ett visst årsintervall och det sker en kontinuerlig översikt och uppdatering av utbildningarna för att de hela tiden ska hållas relevanta.

Utöver utbildningar sker även kontinuerliga punktinsatser i form av exempelvis phishingmail som skickas ut för att testa anställda. Specifika punktinsatser för specifika grupper sker, med exempelvis bedrägerimail som ser ut att komma från VD till ledning eller ekonomiavdelningen.

Med blickarna framåt finns det ändå saker som de vill göra mer av, men även ser som viktigt att de fortsätter med. Bland annat är det viktigt att tänka på att inte ge ut för mycket information då det kan ge motsatt effekt och informationsöverbelastning. Samtidigt blir det viktigt att också förmedla varför det är viktigt att följa bestämmelser, för att öka förståelsen för varför saker behöver göras som det gör. Att inte tillåta alternativa sätt att kringgå säkerhetslösningar är en annan viktig sak för att öka medvetenheten då det får anställda att tänka till varför det är som det är. För att hålla medvetenheten är det viktigt att uppdatera kunskaperna med jämna mellanrum samt ett bra grundpaket för nyanställda inriktat mot typen av tjänst den ska ha. Det kan jobbas mer med medvetenheten och fler punktinsatser är önskvärt. Det har även diskuterats

om en obligatorisk utbildning för de anställda som faller för punktinsatser som exempelvis phishingmail som företaget skickar ut, som kanske kommer att ses i framtiden.

8 Diskussion

8.1 Resultat

Syftet med studien var att ta reda på hur säkerhetsföretag arbetar för att öka säkerhetsmedvetenheten inom sin organisation. Resultaten har också påvisat hur de som har deltagit i studien faktiskt har jobbat. Mycket har stämt överens med det som ansetts som viktigt i litteraturen, men de har även påpekat saker som varit viktiga för dem som litteraturen inte har påpekat. Det som av Awankwa, Loock och Kritzinger (2014) benämnt som informationssäkerhetsträning har inte varit vanligt hos de företag som deltagit i den här studien. Samtidigt har samtliga respondenter som deltagit i studien påpekat vikten av att inte ta för mycket tid från de anställda. Informationssäkerhetsträning känns som en sådan sak som kräver mycket tid och framförallt flertalet anställda på samma gång för att kunna genomföras, i och med att det handlar om bland annat seminarier och studiegrupper.

När det rådde tveksamheter kring det insamlade materialet kunde respondenten kontaktas igen på mail för att förtydliga vissa saker. Det är därför möjligt att det finns en del av materialet i resultatet som inte är helt rättvisande eller vissa saker som de gör men som de kanske inte själva tänkte på vid intervjutillfället. Att endast 5 respondenter och 3 företag deltog i studien är även det en sak som kan ha kommit att påverka utgången av resultatet. Möjligen hade andra svar kunnat uppnås eller andra upptäckter kunnat göras om fler hade deltagit i studien.

8.2 Vetenskapliga aspekter och framtida forskning

Det har skett betydande forskning inom området säkerhetsmedvetenhet som helhet. Men inte många studier har gjorts som undersökt just företag som jobbar med informationssäkerhet. Mycket av de tidigare studier som gjorts inom organisationer har fokuserat på att hitta problem och svårigheter med säkerhetsmedvetenhet. Denna studie fokuserar på ett försök till att hitta en lösning. De studier som gjorts som fokuserat på medvetenhetsprogram och dess innehåll har förvisso kommit fram till viktiga aspekter i arbetet med en ökad säkerhetsmedvetenhet, men har oftast inte beskrivit hur detta används i praktiken av olika organisationer. Denna studie kan därför även verifiera hur väl företag inom informationssäkerhetsområdet faktiskt applicerar dessa aspekter i sitt eget arbete gentemot säkerhetsmedvetenheten. Bland annat visar det sig att de använder sig mycket av vad som anses vara viktigt, medan vissa saker inte är riktigt lika vanligt förekommande, detta finns även beskrivet i 8.1. Samtidigt som deltagande företag i studien gör saker som de tycker är viktiga som inte är nämnda i litteraturen, vilket kan tyda på att det finns ytterligare saker att tänka på och ta till sig i arbetet mot en ökad säkerhetsmedvetenhet.

Resultaten från denna studie baseras på hur säkerhetsföretag jobbar för att öka sin säkerhetsmedvetenhet och studien har även avgränsats mot större företag. Det hade kunnat vara av intresse att även undersöka små eller medelstora säkerhetsföretag och se hur de gör, då de troligtvis inte har samma formella krav på sig. De resultat som skulle komma från dessa studier skulle då kunna jämföras med resultatet från denna studie, för att se vilka skillnader det finns baserat på storlek på företag. Delar av resultaten från denna studie hade även kunnat testas på andra företag i andra branscher, med andra ord som inte jobbar med informationssäkerhet, för att se om undersökningen även kan

appliceras med goda resultat för dem. Något som skulle vara intressant, baserat på resultatet från den här studien, är att testa kategorier eller delar av kategorier på andra företag och mäta påverkan på säkerhetsmedvetenheten av dessa. Bara för att de företag som deltagit i studien gör på vissa sätt behöver inte det betyda att det är en exakt sanning om att detta är saker som alla påverkar säkerhetsmedvetenheten positivt. Att exempelvis mäta säkerhetsmedvetenheten i en organisation, implementera en viss kategori eller del av kategori, för att sedan göra en ny mätning efteråt. Detta skulle ge ett exakt svar av den påverkan dessa kategorier faktiskt har på säkerhetsmedvetenheten. Vidare skulle eventuellt även en kombination av kategorier kunna testas, för att i slutändan, om möjligt, eventuellt kunna hitta vad som är en optimal kombination av aktiviteter och tillvägagångssätt för att öka säkerhetsmedvetenheten inom organisationer.

8.3 Val av metod

Valet av metod för att besvara studiens frågeställning föll på en kvalitativ metod med semistrukturerade intervjuer som datainsamling. Eftersom frågeställningen syftat till att ta reda på hur företagen arbetat för att öka sin medvetenhet krävs det ett utforskande angreppsätt, vilket är just den kvalitativa metoden. En kvantitativ metod hade inte gett möjligheten att ta sig in på djupet på samma sätt som den kvalitativa metoden har gjort. Dock hade en kvantitativ metod kunnat funka för att exempelvis jämföra företagen mot litteraturen eller liknande. Men den kvalitativa metoden som tillämpats fungerade väldigt bra och gav möjligheten till en närhet av de företagen som undersöktes, vilket även det är en fördel över den kvantitativa metoden. Intervjuer var lämpligast eftersom det ger möjlighet till att verkligen ta reda på, från respondenter som på ett eller annat sätt haft inblick, hur de arbetar och att verkligen kunna samla in mycket data som bidragit till att en djupare analys kunnat genomföras. Semistrukturerade intervjuer var också mest fördelaktigt i och med att det var viktigt att kunna få reda på hur just de jobbar, samtidigt som en viss struktur var viktig för att ändå hålla sig till ämnet och få de svar som faktiskt bidrar till att besvara frågeställningen.

Den kvalitativa metoden med intervjuer som datainsamling var alltså det som passade bäst. Observationer hade kunnat ge svar på vissa frågor, men eftersom arbetet med att öka medvetenheten är ett kontinuerligt arbete som sker över loppet om ett eller flera år hade det varit svårt att faktiskt förstå helheten med observationer. Samtidigt hade observationer varit svårt att få igenom, då det är mycket konfidentiell information som cirkulerar i dessa organisationer och att få tillgång till en insyn på det sättet som en observation eventuellt hade krävt hade därför varit komplicerat.

När respondenter valdes ut har det varit viktigt att åtminstone någon i varje företag som deltagit i studien har arbetat med företagets medvetenhet på ett eller annat sätt. Detta för att säkerställa att de svar som krävs för att besvara frågeställningen kan göras. För att också säkerställa att samtlig information som respondenterna ger också finns att tillgå vid analys och fastställandet av resultat har de spelats in. Svaren har sedan transkriberats och analyserats genom en innehållsanalys vilket har bidragit till att säkerställa att minska misstag om svar som förbises i det insamlade materialet. Vid presentation av materialet har även citat från respondenterna använts för att bekräfta att det material som presenteras också stämmer överens med vad de sagt.

8.4 Etiska aspekter

Det är viktigt att följa de etiska aspekterna under en forskningsstudie där Olsson och Sörensen (2007) tar upp konfidentialitet, sekretess och anonymitet som viktiga aspekter. Olsson och Sörensen (2007) tar även upp fyra principer som är viktiga att följa under forskningsstudier och dessa kan läsas mer i detalj i kapitel 4.4. Även de krav som Vetenskapsrådet (2002) tagit fram är viktiga att följa. För att samtliga dessa ska uppfyllas har samtliga respondenter alltid haft sista ordet när det gäller deras typ av involvering i studien. Innan de deltar presenteras syftet med studien och hur deras information kommer att användas. Under studiens gång har de bland annat haft rätten att neka till inspelning av intervju vilket i förekommande fall har antecknats via fältanteckningar. Samtliga respondenter och företag som deltagit i studien har varit anonyma. Vid de tillfällen de nämnt företag vid namn har det i materialpresentationen istället benämnts som företaget istället för att nämna företaget vid namn.

Första kontakten med respondenterna har gjorts via mail, där syfte med studien samt också hur intervjutillfället kommer att se ut. Detta har gett respondenterna tid att reflektera över deras egen inblandning i studien. Samma sak har meddelats väl på plats innan intervjuns start. Samtidigt har ingen information som samlats in under intervjuerna använts till något annat än just denna studie och för att besvara frågeställningen.

8.5 Samhälleliga aspekter

Att medvetenheten hos anställda inom informationssäkerhetsområdet är viktigt råder det ingen tvekan om. Det kommer ständigt nya regelverk som berör informationssäkerhet och det är viktigt att hela tiden bli bättre. Studien har fokuserat på att ta reda på hur just säkerhetsföretag jobbar för att öka medvetenheten och avgränsat sig mot större företag med hypotesen att dessa helt enkelt är i toppskiktet när det gäller att jobba med säkerhetsmedvetenheten. Bidraget av studien är just resultatet och svaret på hur större säkerhetsföretag jobbar för att öka sin medvetenhet. Andra branscher och mindre företag kan därför kolla på detta resultatet och eventuellt också tillämpa de saker som passar och fungerar in i sin egen verksamhet. Detta skulle bidra till att företag som inte har samma förutsättningar eller kompetens inom området kan ta till sig dessa resultat och på ett effektivt sätt ta sig vidare i processen i arbetet med säkerhetsmedvetenhet. Men det har även skiljt en del mellan hur de olika företagen som deltagit i studien har jobbat med att öka medvetenheten. Trots att dessa är stora företag med höga krav på sig att ha en bra informationssäkerhet finns det vissa saker som kan förbättras. Dessa företag skulle därför kunna se dessa resultaten som inspiration även för att lära sig av varandra och förbättra sitt eget arbete med en ökad säkerhetsmedvetenhet.

Referenser

Alotaibi, M., Furnell, S. och Clarke, N. (2017) ”Information security policies: A review of challenges and influencing factors”, *2016 11th International Conference for Internet Technology and Secured Transactions, ICITST 2016*. Infonomics Society, s. 352–358. doi: 10.1109/ICITST.2016.7856729.

Amankwa, E., Loock, M. och Kritzinger, E. (2014) ”A conceptual analysis of information security education, information security training and information security awareness definitions”, *2014 9th International Conference for Internet Technology and Secured Transactions, ICITST 2014*. Infonomics Society, s. 248–252. doi: 10.1109/ICITST.2014.7038814.

Al Awawdeh, S. och Tubaishat, A. (2014) ”An information security awareness program to address common security concerns in IT unit”, *ITNG 2014 - Proceedings of the 11th International Conference on Information Technology: New Generations*. IEEE, s. 273–278. doi: 10.1109/ITNG.2014.67.

Bashorun, A., Worwui, A. och Parker, D. (2013) ”Information security: To determine its level of awareness in an organization”, *AICT 2013 - 7th International Conference on Application of Information and Communication Technologies, Conference Proceedings*. IEEE, s. 1–5. doi: 10.1109/ICAICT.2013.6722704.

Berndtsson, M. *m.fl.* (2008) *Thesis Projects: A Guide for Students in Computer Science and Information Systems*. 2:a uppl. London: Springer-Verlag.

Burns, A. J. *m.fl.* (2015) ”Assessing the role of security education, training, and awareness on insiders’ security-related behavior: An expectancy theory approach”, *Proceedings of the Annual Hawaii International Conference on System Sciences*. IEEE, 2015–March, s. 3930–3940. doi: 10.1109/HICSS.2015.471.

Chang, S. E. och Lin, C. S. (2007) *Exploring organizational culture for information security management*, *Industrial Management and Data Systems*. doi: 10.1108/02635570710734316.

Crossler, R. E. *m.fl.* (2013) ”Future directions for behavioral information security research”, *Computers and Security*, 32, s. 90–101. doi: 10.1016/j.cose.2012.09.010.

D’Arcy, J., Hovav, A. och Galletta, D. (2009) ”User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach”, *Information Systems Research*, 20(1), s. 79–98. doi: 10.1287/isre.1070.0160.

Denscombe, M. (2010) *The Good Research Guide: for small-scale social research projects*. 4:e uppl. Maidenhead: Open University Press.

Doherty, N. F. och Fulford, H. (2009) ”Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis”, i *Social and Human Elements of Information Security: Emerging Trends and Countermeasures*, s. 326–342.

Ernst & Young (2009) ”Outpacing Change: Ernst & Young’s 12th annual global information security survey”.

F.W. Guldenmund (2000) ”The nature of safety culture : a review of theory and research”, *Safety Science*, 34, s. 215–257. doi: 10.1016/S0925-7535(00)00014-X.

Ghazvini, A. och Shukur, Z. (2018) ”Review of information security guidelines for awareness training program in healthcare industry”, *Proceedings of the 2017 6th International Conference on Electrical Engineering and Informatics: Sustainable Society Through Digital Innovation, ICEEI 2017*, 2017–Novem, s. 1–6. doi: 10.1109/ICEEI.2017.8312399.

Hallberg, J. *m.fl.* (2017) *Informationssäkerhet och organisationskultur*. Lund: Studenlitteratur AB.

Herath, T. och Rao, H. R. (2009) ”Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness”, *Decision Support Systems*. Elsevier B.V., 47(2), s. 154–165. doi: 10.1016/j.dss.2009.02.005.

Holme, I. M. och Solvang, B. K. (1997) *Forskningsmetodik: Om kvalitativa och kvantitativa metoder*. 2:a uppl. Lund: Studentlitteratur.

ISO/IEC 27001:2017 (2017) ”Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Krav”. Sverige.

ISO/IEC 27002:2017 (2017) ”Informationsteknik – Säkerhetstekniker – Riktlinjer för informationssäkerhetsåtgärder”. Sverige.

Johnson, E. C. (2006) ”Security awareness: switch to a better programme”, *Network Security*, 2006(2), s. 15–18. doi: 10.1016/s1353-4858(06)70337-3.

Khan, B. *m.fl.* (2011) ”Effectiveness of information security awareness methods based on psychological theories”, *African Journal of Business Management*, 5(26), s. 10862–10868. doi: 10.5897/ajbm11.067.

De Maeyer, D. (2007) ”Setting up an Effective Information Security Awareness Programme”, i *ISSE/SECURE 2007 Securing Electronic Business Processes*, s. 49–58.

Martins, A. och Eloff, J. (2002) ”Information Security Culture”, i Ghonaimy, M. A., El-Hadidi, M. T., och Aslan, H. K. (red.) *Security in the Information Society*. Boston, MA: IFIP Advances in Information and Communication Technology, s. 203–214.

Nasir, A., Arshah, R. A. och Ab Hamid, M. R. (2017) ”Information Security Policy Compliance Behavior Based on Comprehensive Dimensions of Information Security Culture”, s. 56–60. doi: 10.1145/3077584.3077593.

Nationalencyklopedin (2019) ”Medvetenhet”. Tillgänglig vid: http://www.ne.se/uppslagsverk/ordbok/svensk/medvetenhet.

Nohlberg, M. (2009) ”Why Humans are the Weakest Link”, i Gupta, M. och Sharman, R. (red.) *Social and Human Elements of Information Security: Emerging Trends and Countermeasures*. Hershey: Information Science Reference, s. 15–26. doi: 978-1-60566-037-0.

Olsson, H. och Sörensen, S. (2007) *Forskningsprocessen: kvalitativa och kvantitativa perspektiv*. 2:a uppl. Stockholm: Liber AB.

Patton, M. Q. (2002) *Qualitative Research & Evaluation Methods*. 3:e uppl. Thousand Oaks: Sage Publications, Inc.

Peltier, T. R. (2005) ”Implementing an Information Security Awareness Program”, *Information Systems Security*, 14(2), s. 37–49.

Pfleeger, C. P., Pfleeger, S. L. och Margulies, J. (2015) *Security in Computing*. 5th uppl. Upper Saddle River, NJ: Prentice Hall.

SanNicolas-Rocca, T., Schooley, B. och Spears, J. L. (2014) ”Designing effective knowledge transfer practices to improve is security awareness and compliance”, *Proceedings of the Annual Hawaii International Conference on System Sciences*. IEEE, s. 3432–3441. doi: 10.1109/HICSS.2014.427.

Schneider, B. *m.fl.* (2017) ”Organizational Climate and Culture: Reflections on the History of the Constructs in JAP”, *Journal of Applied Psychology*. doi: 10.1016/j.jbiomech.2007.12.017.

Siponen, M. T. (1991) ”A conceptual foundation for organizational information security awareness - ABI/INFORM Complete - ProQuest”, (Table I), s. 31–41. Tillgänglig vid: http://search.proquest.com.librarylogin-ue.suagm.edu:85/abicomplete/docview/212301357/AD4BABC8AB0146BDPQ/15?accountid=130249#.

SIS (2015) *Teknisk rapport: Terminologi för informationssäkerhet*. Stockholm, Sverige: SIS Förlag AB.

Tsohou, A. *m.fl.* (2015) ”Managing the introduction of information security awareness programmes in organisations”, *European Journal of Information Systems*, 24(1), s. 38–58. doi: 10.1057/ejis.2013.27.

Vetenskapsrådet (2002). *Forskningsetiska principer inom humanistisk-samhällsvetenskaplig forskning*. Stockholm: Vetenskapsrådet. Tillgänglig vid: http://www.codex.vr.se/texts/HSFR.pdf.

Webster, J. och Watson, R. T. (2002) ”Analyzing the Past to Prepare for the Future: Writing a Literature Review”, *MIS Quarterly*, 26(2).

Åhlfeldt, R. M., Spagnoletti, P. och Sindre, G. (2007) ”Improving the information security model by using TFI”, *IFIP International Federation for Information Processing*, 232, s. 73–84. doi: 10.1007/978-0-387-72367-9_7.

Bilaga 1 – Intervjufrågor

Om respondenten:

1. Roll i företaget

2. Arbetsuppgifter
    a. På vilket sätt jobbar du med informationssäkerhet?

Generell informationssäkerhet:

1. Anser ni era största hot vara externa eller interna?

2. Hur uppdaterar ni er själva om de relevanta hot som finns?
    a. Hur förmedlas detta till de anställda?

3. Vilket område inom informationssäkerhet prioriterar eller fokuserar ni mest på?

4. Hur är ansvaret gällande informationssäkerheten fördelat inom organisationen?
    a. Hur många ansvarar för organisationens informationssäkerhet?

5. Vad är konsekvenserna om anställda bryter mot säkerhetsreglerna?
    a. Hur förmedlas dessa konsekvenser?

6. Hur gör ni för att få era anställda mer engagerade gällande informationssäkerheten?

Säkerhetsmedvetenhet:

1. Hur ser du på begreppet säkerhetsmedvetenhet?

2. Hur viktigt anser ni det är, att medvetenheten hos era anställda är hög?
    a. Varför?

3. Mäter ni hur medvetna era anställda är gällande informationssäkerhet?
    a. Om ja: hur?

4. Jobbar ni aktivt för att få till en säkerhetskultur?
    a. Om ja: hur?

5. Följer ni någon standard?
    a. Om ja: hur ser ni till att den förstås och efterlevs?

6. Hur ser ni till att personal vet om den säkerhetspolicy som finns?
    a. Hur ser ni till att den förstås och efterlevs?

7. Skiljer ni något i förmedlingen av olika dokument som exempelvis standarder, policys eller avtal etc?

8. Har ni något medvetenhetsprogram?
    a. Om ja: hur är det uppstyrt? Vad ingår?
    b. Utvärderar ni resultatet av programmet?

9. Utför ni utbildningar i syfte att öka medvetenheten?
    a. Om ja: skiljer det sig på utbildningsmaterial beroende på vilken roll inom organisationen ni utbildar?
    b. Vad är utbildningsmaterialet?
    c. Hur tidigt utbildar ni ny personal inom säkerhet?
    d. Hur ofta sker utbildningarna?

10. Utför ni någon typ av praktisk träning för att öka säkerhetsmedvetenheten?
    a. Om ja: exempel på metoder?

11. Vilka anser ni vara era viktigaste aktiviteter ni utför för att öka medvetenheten?

12. Finns det något ni vill göra annorlunda i framtiden gällande medvetenheten?

13. Något som inte har tagits upp under den här intervjun som ni vill ta upp eller som hade varit bra för mig att veta?