LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

Informationssäkerhetsutmaningar vid storskaligt distansarbete

Kandidatuppsats 15 hp, kurs SYSK16 i Informatik

Författare: Andreas Berg
Rasmus Holmqvist
Jakob Andersson

Handledare: Nicklas Holmberg

Rättande lärare: Benjamin Weaver
Markus Lahtinen

Informationssäkerhetsutmaningar vid storskaligt distansarbete

ENGELSK TITEL: Challenges within information security during large scale remote work.

FÖRFATTARE: Andreas Berg, Jakob Andersson och Rasmus Holmqvist

UTGIVARE: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

EXAMINATOR: Benjamin Weaver, Markus Lahtinen

FRAMLAGD: maj, 2021

DOKUMENTTYP: Kandidatuppsats

ANTAL SIDOR: 68

NYCKELORD: Informationssäkerhet, Distansarbete, Mänskliga faktorn

SAMMANFATTNING (MAX. 200 ORD):

Under 2020 och 2021 har en stor del av organisationer i Sverige och runt om i världen tvingats lägga om sin verksamhet till arbete på distans till följd av Covid-19 pandemin. Detta har lett till nya utmaningar inom inte minst informationssäkerhet, där policys och riktlinjer i många fall varit anpassade för arbete i organisationernas lokaler. Då den största risken inom informationssäkerhet är den mänskliga faktorn innebär den nya situationen att organisationer behöver identifiera vilka utmaningar distansarbetet medför, och hur dessa ska hanteras. Vi ämnar därför i denna uppsats att närmare undersöka vilka upplevda utmaningar detta är och hur organisationer hanterar dem. Vi har genomfört en kvalitativ undersökning bestående av fyra intervjuer med personer i ledande position inom informationssäkerhet på respektive organisation. Även om vissa aspekter av arbetet med informationssäkerhet förblivit oförändrade, visar vår undersökning att det storskaliga distansarbetet har medfört ett flertal utmaningar som organisationerna behövt hantera. Resultatet visar att säkerhetskulturen i flera fall blivit lidande och insynen i personalens medvetenhet om policys och risker minskat.

Innehåll

Figurer

Tabeller

1 Introduktion

I detta kapitlet redogör vi för läsaren vad bakgrunden och problemområdet är. Därefter introduceras frågeställningen, syftet med uppsatsen samt vilka avgränsningar som har gjorts.

1.1 Bakgrund

Informationssäkerhet handlar om att skydda integriteten, tillgängligheten och sekretessen av informationstillgångar (Mattord & Whitman, 2011). Arbetet kring informationssäkerhet utvecklas kontinuerligt i takt med att hoten och omvärlden förändras (Mattord & Whitman, 2011; Popescu, 2018). En sådan stor förändring är den ökade mängden distansarbete som började under år 2020 (Bloom, 2020).

Den 11 Mars 2020 gjorde världshälsoorganisationen WHO klart att Covid-19 skulle klassificeras som en pandemi (BBC, 2020). För att minska smittspridningen gjorde regeringar världen över klart att länder skulle beläggas med restriktioner av olika grad, främst genom social distansering (Mahase, 2020; Centers for Disease Control and Prevention, 2020). Vid symptom på Covid-19 är rekommendationen från sjukvården att sätta sig i karantän och minimera mängden sociala kontakter (Folkhälsomyndigheten, 2020; Centers for Disease Control and Prevention, 2021). På arbetsplatser runt om i Sverige och världen ledde dessa restriktioner till att många organisationer valde att i stor utsträckning övergå till distansarbete, där personal utförde sina dagliga uppgifter på distans, i stället för på arbetsplatsen (Europakommissionen, 2020).

Distansarbete, även känt som remote work eller telework, syftar i den här uppsatsen på arbete som utförs digitalt på en annan plats än en central arbetsplats, till exempel ett kontor. Ordet distansarbete uttrycktes som en term redan 1972 av den NASA-anställda Jack Nilles (Allied Telecom, 2016). Den första konferensen inom ämnet hölls 1980 efter att författaren Frank Schiff skrev en artikel vid namn ”Working From Home Can Save Gasoline” (Allied Telecom, 2016). Med teknologins framfart och utvecklingen av digitala verktyg ökade även mängden och intresset av distansarbete (Global Workplace Analytics, 2020). Tidigare har organisationer självmant kunna välja att arbeta på distans och därmed haft tid att planera för detta. Som en följd av Covid-19 blev dock organisationer som inte var anpassade till distansarbete sedan tidigare tvingade att på kort tid lägga om sin strategi för att göra detta möjligt.

Hela 2.7 miljarder anställda har blivit påverkade av nedstängningarna världen över (International Labour Organization, 2020). Som ett exempel utfördes ungefär 5% av den totala arbetstiden i USA på distans innan pandemin (Bloom, 2020). Även i Europa arbetade ungefär 5% av arbetsstyrkan heltid på distans innan pandemin (Eurostat, 2020). I både Europa och i USA höjdes de siffrorna till ca 40 % under pandemin (Bloom, 2020; Eurofound, 2020). Även om förändringen har varit problematisk på sina sätt har den även lett till att många organisationer har insett att distansarbete kan fungera och enligt en rapport från Gartner (2020) svarade 82% av de 127 tillfrågade organisationsledarna att de hade planer på att

fortsätta med distansarbete i viss mån efter pandemin. I samma studie svarade 47% av de tillfrågade organisationsledarna att de har planer på att tillåta distansarbete på heltid efter pandemin (Gartner, 2020). Distansarbete är alltså här för att stanna i en större skala (Bloom, 2020; Gartner, 2020).

Man kan redan se effekterna av det storskaliga distansarbetet och vilka följder detta har haft för informationssäkerhet. Enligt en rapport av Europol har mängden attackvektorer i nätverken blivit fler på grund av distansarbetet (Europol, 2020). Den mänskliga faktorn är den svagaste länken när det gäller informationssäkerhet (Skrodelis, Strebko & Romanovs, 2020; Hughes-Lartey, Li, Botchey & Qin, 2021), och distansarbete minskar ytterligare IT-avdelningars förmåga att övervaka anställdas beteenden (Borkovich & Skovira, 2020). Upp till 90% av cyberattacker kan härledas till den mänskliga faktorn (Borkovich & Skovira, 2020). Sedan pandemins start har antalet lyckade cyberattacker ökat med 300% jorden runt (Federal Bureau of Investigation, 2020). Även konsekvenserna av ett dataintrång försvåras av distansarbete. I en rapport från IBM rapporteras det att 70% av organisationer påstår att distansarbete skulle leda till ökade kostnader vid ett dataintrång och 76% av organisationer påstår även att det skulle leda till en ökad tid för att identifiera och tygla ett dataintrång (IBM, 2020). Förändringsarbetet vid distansarbete till följd av Covid-19 pandemin leder alltså till nya utmaningar och tillvägagångssätt inom arbetet kring informationssäkerhet (Deloitte, n.d).

1.2 Problemformulering

Det storskaligt påtvingade distansarbetet till följd av Covid-19 pandemin är en av de största arbetssättsförändringarna på flera år och har påverkat en mängd organisationer. Distansarbete har länge varit ett etablerat arbetssätt och ett relativt välutforskat ämne (Wang, Liu, Qian, & Parker, 2021). En majoritet av de studier som har gjorts har dock utförts inom ramarna för distansarbete i en mycket mindre skala än den vi ser idag (Wang et. al, 2021). Då distansarbete i den skala vi ser idag är ett helt nytt fenomen är det svårt att säga om forskningen är applicerbar på en så mycket större skala av distansarbete (Wang et. al, 2021).

Policys, utbildning och träning tillsammans med god medvetenhet är de vanligaste åtgärderna och metoderna som organisationer använder sig av för att försöka minska den mänskliga faktorns negativa säkerhetspåverkan (Puhakainen & Siponen, 2010). Studier visar dock på att det finns problem med att upprätthålla vissa av dessa metoder vid distansarbete. Wang et. al (2021) visar i en studie att människor som arbetar på distans har svårare att hålla sig till rutiner och att behålla fokus på arbetet jämfört med om man arbetar på kontoret. Det visar sig också att anställda som arbetar hemifrån har en tendens att överge de vanliga säkerhetspolicys som finns på ett kontor (Borkovich & Skovira, 2020). Saker som att vidarebefordra misstänksamma länkar och emails till kollegor, eller att vidarebefordra känsligt arbetsmaterial till hemdatorer är några exempel på överskridande av vanliga säkerhetspolicys som distansarbetare ofta är skyldiga till (Borkovich & Skovira, 2020).

När det gäller policys och riktlinjer visar en studie av Georgiadou, Mouzakitis och Askounis (2021) att det även här finns problem vid distansarbete. I studien rapporterades det att av de 264 medverkande hade 53% av deltagarna inte fått några säkerhetsriktlinjer att följa vid övergången till distansarbete. Studien visade även på att av deltagarna som innan pandemin inte hade haft någon möjlighet eller erfarenhet av att arbeta hemifrån, men som var tvungna att göra det nu, var det 44% som inte hade fått några riktlinjer eller råd alls gällande säkerhet (Georgiadou, Mouzakitis & Askounis, 2021).

Vi vet att organisationer lägger vikt och resurser vid att upprätthålla informationssäkerheten (Crossler, Johnston, Lowry, Hu, Warkentin, & Baskerville, 2013). Det har däremot visat sig svårt att hitta forskning kring hur organisationer tar sig an detta vid storskaligt distansarbete. Informationssäkerhet är ett viktigt område för organisationer och det är därför kritiskt att de identifierar de aspekter som blir utmanande vid storskaligt distansarbete samt hur dessa utmaningar ska hanteras.

1.3 Forskningsfråga

Utifrån det formulerade problemområdet har vi valt nedanstående frågeställning. Frågeställningen syftar främst till att belysa och få ökad förståelse om vilka eventuella utmaningar med informationssäkerhet organisationer stöter på med storskaligt distansarbete samt hur organisationer går tillväga för att hantera dessa.

Vilka aspekter av informationssäkerhet är utmanande för organisationer vid storskaligt distansarbete och hur hanteras dessa?

1.4 Syfte

Syftet med uppsatsen är att undersöka utmaningar gällande informationssäkerhet som uppstår vid distansarbete i en större skala. Vidare ämnar uppsatsen att undersöka hur organisationer tar sig an och hanterar dessa utmaningar. Detta är ett särskilt viktigt forskningsområde då det finns indikationer som visar på att storskaligt distansarbete kommer finnas kvar även efter pandemin.

1.5 Avgränsningar

Då informationssäkerhet är ett brett område har vi valt i vår undersökning att avgränsa oss till aspekter kring den mänskliga faktorn. Inom detta område har vi valt att avgränsa oss baserat på de aspekter och utmaningar som är vanligt förekommande i litteraturen. Aspekterna som vi har identifierat som de vanligast förekommande och kommer att behandla är: policys och riktlinjer, utbildning och träning, medvetenhet, compliance samt ledningens roll.

2 Litteraturgenomgång

I kapitel 2.1 redogörs begreppet informationssäkerhet och de modeller som ligger till grund för informationssäkerhet. I kapitel 2.2 presenteras den mänskliga faktorns roll inom informationssäkerhet och de olika aspekter som organisationer enligt litteraturen bör beakta för att uppnå en god informationssäkerhet.

2.1 Informationssäkerhet

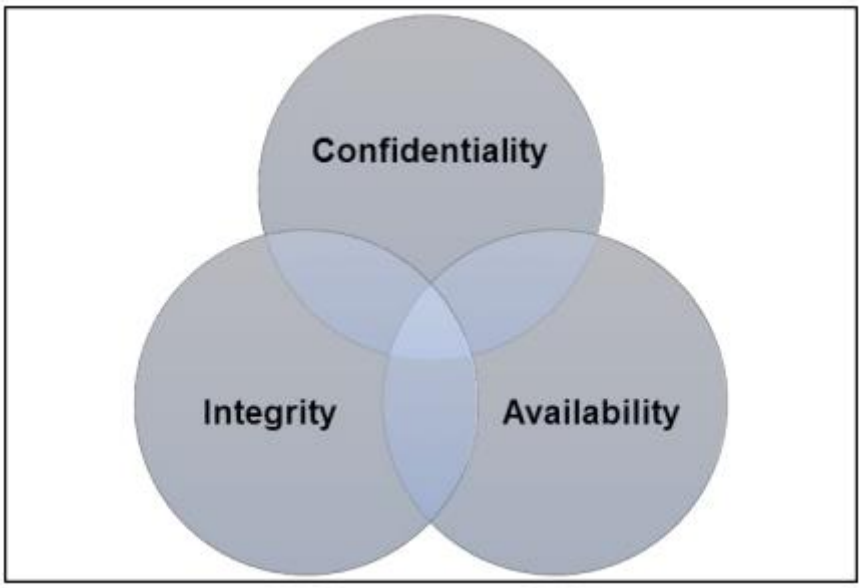
Ett informationssystem kan delas upp i komponenterna: mjukvara, hårdvara, data, människor, procedurer och nätverk (Mattord & Whitman, 2011). Med varje komponent förekommer det olika säkerhetshot som behöver adresseras. Informationssäkerhet handlar om att skydda integriteten, tillgängligheten och sekretessen av dessa komponenter (Mattord & Whitman, 2011). För att uppnå och bibehålla en god informationssäkerhet är det rekommenderat att organisationer implementerar säkerhetspolicys, tränar och utbildar sin personal inom informationssäkerhet samt fokuserar på att uppnå en god säkerhetskultur och medvetenhet (Mattord & Whitman, 2011; Puhakainen & Siponen, 2010; Lebek, Uffen, Neumann, Hohler & Breitner, 2014).

Det är först när något händer, till exempel att obehöriga får åtkomst till systemet eller att organisationens data eller arbete går förlorat, som en organisation generellt inser vikten av informationssäkerhet (Kraemer & Carayon, 2007). Ett av de vanligaste sätten för obehöriga att komma åt information är genom att utnyttja de mänskliga svagheterna hos de anställda på en organisation (Krombholz, Hobel, Huber & Weippl, 2015). Ett sätt att göra detta genom är så kallad social engineering och tekniska redskap är ofta ineffektiva mot detta hot (Krombholz et. al, 2015). Vid Social Engineering är det människor, de anställda, som är måltavlorna för en attack. I stället för tekniska attacker så manipuleras eller övertalas anställda att lämna ut viktig information. Människor har även generellt ett troende om att de är bra på att upptäcka och identifiera ”Social Engineering-attacker”, men forskning visar på det är falskt och att människor har svårt för att upptäcka lögn och bedrägeri (Qin & Burgoon, 2007).

2.1.1 CIA-triaden

Grundpelarna för informationssäkerhet är confidentiality, integrity och availability som tillsammans bildar modellen som kallas för CIA-triaden (Andress, 2014). Denna modell har under lång tid varit industristandarden för informationssäkerhet och varit till grund för många informationssäkerhetsmodeller (Mattord & Whitman, 2011; Gollman, 2011). Den ligger även som bas för mycket av det teoretiska material som finns inom informationssäkerhet samt underlag till hur organisationer arbetar med det (Samonas & Coss, 2014). Beroende på var modellen appliceras skiljer det sig mellan hur stor betydelse det läggs på de olika grundpelarna (Baybulatov & Promyslov, 2020). Information som kräver en hög korrekthet, men som alla får ta del av skulle förslagsvis väga tungt på integrity men confidentiality skulle

inte vara av stor vikt, det är alltså den berörda informationen som styr vilka element som är viktiga (Von Solms & Van Niekerk, 2013).



Figur 1: Modell över CIA-triaden (Samonas & Coss, 2014, s. 31)

Confidentiality har för avsikt att skydda informationen och göra den oåtkomlig för obehöriga. (Andress, 2014). Endast de som har rättighet att ta del av informationen ska få göra det (Mattord & Whitman, 2011). All information är till exempel inte beroende av hög confidentiality och på grund av detta kan åtgärder vidtas i proportion till hur känslig information är (Cherdantseva & Hilton, 2013).

Integritet ämnar att försäkra att informationen inte har blivit manipulerad eller andra sätt ändrad på ett otillåtet vis medan den lagras eller under tiden den skickas (Mattord & Whitman, 2011). Det innefattar både ändringar och manipulation gjorda av obehöriga, eller oönskad radering och ändringar gjorda av behöriga (Andress, 2014). Detta för att försäkra att informationen är korrekt och tillförlitlig (Firdhous & Hussien, 2018).

Availability syftar på att informationen ska vara tillgänglig och kunna nås när det behövs (Agarwal & Agarwal, 2011). Informationen ska ges i korrekt format och tillgängligheten gäller behöriga användare, vilka kan vara både personer och datasystem (Mattord & Whitman, 2011). Nätverksfel, systemfel och strömavbrott är exempel på faktorer som kan göra att informationen inte blir tillgänglig och på det viset kompromissa availability (Andress, 2014).

2.2 Mänskliga faktorn

Organisationer lägger stor vikt på informationssäkerhet och utvecklingen av denna (Crossler et. al, 2013). När det kommer till säkerhetsbrister och incidenter är det människor och den mänskliga faktorn som står för en majoritet av dessa (Skrodelis, Strebko & Romanovs, 2020). Alla misstag och fel som en människa gör räknas till den mänskliga faktorn, oavsett om de är medvetna eller icke-medvetna, illvilliga eller utförda i god tro (Kraemer & Carayon, 2007).

Den mänskliga faktorn är oundviklig, men det går att minska antalet fel som uppstår på grund av den mänskliga faktorn (Wood & Banks, 1993).

2.2.1 Policys och riktlinjer

En säkerhetspolicy är de riktlinjer som anställda förväntas efterfölja för att bibehålla ett säkert arbetssätt (Alhosani, Khalid, Samsudin, Jamel & bin Mohamad, 2019; Alotaibi, Furnell & Clarke, 2019). Att anställda följer säkerhetspolicys är en viktig faktor inom informationssäkerhet (Puhakainen & Siponen, 2010). En policy ska sträva mot att vara en naturlig och självklar del i en organisations vardagliga arbetsliv (Mattord & Whitman, 2011).

Kraemer & Carayon (2007) beskriver att ett problem som kan uppstår vid framtagandet av säkerhetspolicys är att riktlinjerna inte tar hänsyn till de anställdas dagliga arbete och behov och hur dessa kommer att påverkas. Detta kan i sin tur leda till att riktlinjerna delvis, eller inte alls, kommer att följas (Kraemer & Carayon, 2007). Det är även viktig att riktlinjerna kring säkerhet inte skapar för stora svårigheter i det vardagliga arbetet och sätter produktiviteten på spel (Samonas & Coss, 2014). Om riktlinjerna anses vara krångliga och för tidskrävande för de anställda finns det en risk att de anställda kringgår riktlinjerna (Samonas & Coss, 2014). En undermåligt konstruerad säkerhetspolicy är en stor bidragande faktor till att personalen inte kommer att följa den (Bada, Sasse & Nurse, 2019).

2.2.2 Utbildning och träning

Enligt Puhakainen och Siponen (2010) säger tidigare litteratur att utbildning och träning är de vanligaste tillvägagångssätten organisationer använder sig av för att anställda ska följa säkerhetspolicys. Hughes-Lartey et. al (2021) hävdar att en policy måste innehålla ett fokus på att träna och utbilda personalen i att skydda sig själva. För att de anställda lättare ska komma ihåg träningen de får ska den vara direkt riktade till dem (Caldwell, 2012). Nyanställda bör bli informerade om vilka säkerhetspolicys som finns för att bli medvetna om vilka de är och vikten av dessa samt hur lämpligt säkerhetsbeteende ska vara (Nykodym, Kahle-Piasecki & Marsillac, 2010). Mattord och Whitman (2011) menar på att detta även är viktigt för att de nyanställda inte ska bilda sig en egen uppfattning om säkerhetskulturen innan de har blivit utbildade i den officiella säkerhetspolicyn.

Eftersom policys behöver följas av de anställda för att vara effektiva är det viktigt att förstå vad det är som motiverar de anställda till att följa de satta riktlinjerna (Bulgurcu, Cavusoglu & Benbasat, 2010). För att säkerhetspolicys och de moment som krävs för att uppfylla dessa inte ska bli åsidosatta till fördel för andra arbetsuppgifter bör organisationer avsätta specifik tid till dessa säkerhetsmoment (Bulgurcu, Cavusoglu & Benbasat, 2010). Utbildningen och träningen bör vara fokuserad på att göra det enklare för de anställda att utföra säkerhetsmomenten som säkerhetspolicyn kräver (Bulgurcu, Cavusoglu & Benbasat, 2010). Genom att underlätta för de anställda kommer kraven säkerhetspolicyn specificerar inte ses lika betungande (Bulgurcu, Cavusoglu & Benbasat, 2010). Genom att undersöka de anställdas säkerhetsbetende kan organisationer se hur väl policys efterföljs och var det finns bristande kunskap eller motivation (Stanton, Stam, Mastrangelo, & Jolton, 2005). Efter en sådan undersökning kan organisationerna mer effektivt styra utbildningen i rätt riktning.

Bulgurcu, Cavusoglu & Benbasat (2010) argumenterar för att en ökad medvetenhet om informationssäkerhet kan ändra anställdas attityd och acceptans gentemot säkerhetspolicys på

ett positivt sätt. Därför bör träning och utbildning fokusera på att öka anställdas medvetenhet och på det viset samtidigt även öka deras compliance mot säkerhetspolicys (Bulgurcu, Cavusoglu & Benbasat, 2010). Säkerhet kan bli mer intressant för de anställda ifall de känner att de kan ha användning för det och applicera det även utanför arbetet (Haney & Lutters, 2020). Att lära anställda om hur man säkert använder appar och social media är exempel på några saker som är användbara för de anställda även utanför arbetet och som ökar deras generella säkerhetsmedvetenhet (Haney & Lutters, 2020).

2.2.3 Medvetenhet

För att reducera antalet intrång orsakade av den mänskliga faktorn är det viktigt att öka personalens medvetenhet (Metalidou, Marinagi, Trivellas, Eberhagen, Skourlas & Giannakopoulos 2014). Medvetenhet kring informationssäkerhet syftar till att anställda är medvetna om vilka risker som finns och hur dessa ska hanteras samt deras roll i det hela (Siponen, 2000). En ökad medvetenhet och kunskap kring säkerheten menar tidigare forskning är lösningen på att minska detta problem (Hughes-Lartey et.al, 2021; Metalidou et. al, 2014). Ökad medvetenhet ska åstadkommas genom tydliga och lättillgängliga policys (Metalidou et. al, 2014).

Att endast göra personalen medveten om vilka säkerhetsrisker som finns är bara en del av problemet, det är även väsentligt att utbilda och berätta för personalen hur de ska gå tillväga och hantera riskerna (Haney & Lutters, 2020). Det räcker att en enda av användarna på ett nätverk blir utsatt för bedrägeri och lurad av gärningsmännen för att ett helt nätverk äventyras eller ger obehöriga åtkomst (Campean, 2019). Det är därför viktigt att varje enskild anställd är medveten om sin del i det hela och på vilket sätt deras handlingar speglar sig i det stora hela (Aminzade, 2018).

2.2.4 Compliance

Ett sätt att förbättra säkerheten är att fokusera på att få de anställda till att följa de säkerhetspolicys man har (Bulgurcu, Cavusoglu & Benbasat, 2010). Ifall de inte följs tappar de sin effekt (Puhakainen & Siponen, 2010). Siponen, Pahnila, & Mahmood (2010) förklarar att den sociala aspekten och människorna runt omkring den anställda och deras attityd gentemot policyn och deras förväntningar på den anställda spelar en stor roll i hur väl policyn kommer att följas. Organisationer bör därför lägga fokus på att utbilda anställda, chefer som medarbetare, om informationssäkerhet och ge dem en tydlig uppfattning om varför det är viktigt (Siponen, Pahnila, & Mahmood, 2010). Genom detta kan organisationer främja anställdas beteende att följa säkerhetspolicyn genom att skapa ett socialt tryck (Siponen, Pahnila, & Mahmood, 2010). Puhakainen och Siponen (2010) har i sin undersökning konstaterat att fortsatt kommunikation och utbildning till de anställda om säkerhetspolicys är en viktig faktor för att dessa policys ska följas.

2.2.5 Ledningens roll för informationssäkerhet och organisationsförändringar

Inom en organisation är de anställdas värderingar, tankar och handlingar vägledda av gemensamma idéer och tankesätt som finns inom organisationen (Alvesson, 2013). Dessa gemensamma värderingar och beteendemönster samlas i begreppet organisationskultur (Schneider, Brief & Guzzo, 1996; Alvesson, 2013). När man pratar om organisationskultur brukar inte aspekten om relevant kunskap för arbetsrollen vara med, utan man antar att

personalen har den relevanta kunskapen som ens arbetsroll kräver (Van Niekerk & Von Solms, 2010). Man kan däremot inte anta att personalen har tillräckligt god kunskap om informationssäkerhet för att på ett säkert sätt utföra sin dagliga verksamhet (Van Niekerk & Von Solms, 2010). Vidare skriver Van Niekerk & von Solms (2010) att upprättandet av en informationssäkerhetskultur är kritiskt för att hantera den mänskliga faktorn inom informationssäkerhet.

Eftersom anställda blir influerade av vilken attityd som personer runt omkring de har gentemot säkerhet, kan organisationer påverka och forma de anställdas säkerhetsbeteende genom att arbeta mot en stark informationssäkerhetskultur (Leach, 2003). Det är ledningen och befattningshavare som lägger grunden för denna informationssäkerhetskultur genom att föregå med gott exempel (Aminzade 2018; Leach, 2003; Puhakainen & Siponen, 2010). Vidare är det även viktigt att det finns ett tydligt och synligt stöd från huvudledningen inom organisationen för att säkerhetspolicys ska följas (Puhakainen & Siponen, 2010).

Ledningens handlingar spelar inte bara roll för att uppnå en god säkerhetskultur utan det är även en av de viktigaste framgångsfaktorerna vid en organisationsförändring (Paton & McCalman, 2008; Anderson & Anderson 2010; Burnes, 2011; Gill 2002). Organisationsförändringar kan blanda annat innebära införandet av nya policys och riktlinjer eller omorganiseringar, men det kan även innebära sådant som förändrade organisationskulturer (Anderson & Anderson, 2010). Organisationsförändringar är svåra att lyckas med och cirka 60-90% av alla förändringsprojekt misslyckas (Burnes & Jackson, 2011; Todnem By, 2005; Burnes, 2011). Ett misstag som många organisationer gör vid förändringar är att de misslyckas med att förankra förändringarna i organisationskulturen (Kotter, 2012). Kotter (2012) menar på att en förändring behöver bli en del av det naturliga arbetssättet och om det inte blir det finns det en risk att de anställda kommer att gå tillbaka till hur det var innan förändringen. En annat misstag som Kotter (2012) tar upp vid organisationsförändringar är att organisationer ofta förkunnar sig klara med en förändring för tidigt. Kotter (2012) tar upp att organisationer har en tendens att fira och förkunna sig klara med en förändring efter att den första förbättringen är synlig eller när det första projektet efter förändringen är klart. Det kan dock ta tre till tio år innan en förändring har satts i organisationskulturen och om man inte kontinuerligt fortsätter att arbeta med förändringen är det vanligt att det så småningom går tillbaka till hur det var innan förändringen (Kotter, 2012).

2.3 Litteratursammanfattning

Nedan presenteras en tabell av de områden som har redovisats i litteraturgenomgången. Först har informationssäkerhet och CIA-triaden introducerats för att ge läsaren en förståelse för informationssäkerhet och CIA-triadens betydelse. Därefter har vi identifierat de aspekter inom arbetet med informationssäkerhet som enligt tidigare forskning och litteratur har störst betydelse för framgång. Vi har identifierat två övergripande områden. Ett av områdena innefattar säkerhetspolicys och riktlinjer, utbildning och träning samt ledningens roll, vilka ligger till grund för att uppnå aspekterna i det andra området. Det andra området innefattar aspekterna compliance, medvetenhet och säkerhetskultur och det är detta organisationer ska eftersträva att ha en hög nivå av.

Kategori	**Sammanfattning/Innehåll**	**Litteratur**
Informationssäkerhet	● Begreppet informationssäkerhet och vad det innebär. ● Aspekter som är rekommenderade att bejaka för att vidhålla en god informationssäkerhet	Kraemer & Carayon (2007) Krombholz et. al (2015) Lebek et. al (2014) Mattord & Whitman (2011) Puhakainen & Siponen (2010) Qin & Burgoon (2007)
CIA-triad	● Förklarar CIA-triadens betydelse för informationssäkerhet och dess grundläggande element.	Agarwal & Agarwal (2011) Andress (2014) Baybulatov & Promyslov (2020) Cherdantseva & Hilton (2013) Firdhous & Hussien (2018) Gollman (2011) Mattord & Whitman (2011) Samonas & Coss (2014) Von Solms & Van Niekerk (2013)
Mänskliga faktorn	● Mänskliga faktorns inverkan på informationssäkerhen och vilka risker detta medför.	Crossler et. al (2013) Kraemer & Carayon (2007) Skrodelis, Strekbo & Romanovs (2020) Wood & Banks (1993)

Policys och riktlinjer	• Betydelsen av att ha väl utformade och relevanta policys. • Problematik som kan uppstå med policys	Alhosani et. al (2019) Alotaibi, Furnell & Clarke (2019) Bada, Sasse & Nurse (2019) Kraemer & Carayon (2007) Mattord & Whitman (2011) Puhakainen & Siponen (2010) Samonas & Coss (2014)
Utbildning och träning	• Vikten av att ge anställda relevant utbildning och träning • Tillvägagångssätt vid utbildning	Bulgurcu, Cavusoglu & Benbasat (2010) Caldwell (2012) Haney & Lutters (2020) Hughes-Lartey et. al (2021) Mattord & Whitman (2011) Nykodym, Kahle-Piasecki & Marsillac (2010) Puhakainen & Siponen (2010) Stanton et. al (2005)
Medvetenhet	• Begreppet medvetenhet samt hur denna kan höjas inom organisationen • Betydelsen av att hålla en god medvetenhet	Aminzade (2018) Campean(2019) Haney & Lutters (2020) Hughes-Lartey et.al (2021) Metaldiou et. al (2014) Siponen (2000)
Compliance	• Förklaring till begreppet compliance och hur detta kan uppnås	Bulgurcu, Cavusoglu & Benbasat (2010) Puhakainen & Siponen (2010) Siponen, Pahnila, & Mahmood (2010)
Ledningens roll för informationssäkerhet och organisationsförändringar	• Ledningens roll i att forma organisationskulturen • Ledningens roll vid organisationsförändringar • Samspelet mellan	Alvesson (2013) Aminzade (2018) Anderson & Anderson (2010) Burnes (2011) Gill (2002)

	organisationsförändring och organisationskultur	Kotter (2012) (Leach, 2003) Paton & McCalman (2008) Puhakainen & Siponen (2010) Schneider, Brief & Guzzo (1996) Van Niekerk & Von Solms (2010)

Tabell 1: Litteratursammanfattning

3 Metod

I följande kapitel går vi igenom den metodik som använts för att genomföra inhämtningen av empiriska data för vår undersökning. Kapitlet informerar även läsaren om de olika intervjuobjekt som delat med sig av information, och på vilket sätt deras befattning och kompetens är intressant för vår studie.

3.1 Metodval

Då vi i vår studie är ute efter detaljerade svar med möjlighet till följdfrågor, stod det tidigt klart att vår empiriska data behövde vara av kvalitativ art. Vi anser att denna typ av data ger oss en ökad chans att kunna besvara vår frågeställning på ett tillfredsställande sätt. Detta styrks även av Jacobsen (2002) samt Oates (2006), då de menar att kvalitativa studier är mer lämpade för forskning som syftar till att besvara explorativa frågeställningar. Jacobsen utvecklar denna tes med att påpeka att närheten till intervjuobjektet stärks av denna typ av undersökning, vilket i sin tur leder till ökad förståelse kring de tillfrågades syn på verkligheten (Jacobsen, 2002). Dessutom kan våra frågor uppfattas att vara av en känslig natur, vilket är något som Oates (2006) menar på är mer lämpade för kvalitativa undersökningar eftersom intervjupersoner kan vara mer restriktiva i sina svar gällande känsliga frågor vid en enkätundersökning.

3.2 Litteraturinsamling

Utöver intervjuerna, har vi använt sökmotorerna Google Scholar och LUBsearch för att hitta tidigare publikationer inom olika relevanta ämnen. Vi har även använt oss av IEEE Xplore för att hitta relevanta publikationer då Oates (2005) beskriver detta som en tillförlitlig källa. När vi har hittat en artikel vi har tyckt varit av intresse har vi läst igenom den och sedan undersökt vilka referenser som har använts. Vi har sedan gått igenom dessa referenser och på så vis både hittat mer litteratur och säkerställt var informationen kommit ifrån. Sökord vi använt oss av har bland annat varit:

“information security compliance”, “information security remote work”, “information security during Covid-19 pandemic”, “information security policy”, information security human factor”, “information security”, “informationssäkerhet”, “information security culture”

3.3 Intervjuer

Frågorna i vår undersökning (bilaga 8.1) skapades utefter de aspekter av informationssäkerhet som hade identifierats i litteraturgenomgången. Jacobsen (2002) betonar vikten av att inte ha en för strukturerad intervju då den kvalitativa ansatsen kan försvinna. Det är dock viktigt att en viss struktur finns då viktiga ämnen annars kan glömmas bort (Jacobsen, 2002).

Intervjuguiden som har använts har därför fungerat som en guide för att försöka få en så öppen dialog som möjligt, utan att något område ska glömmas bort. Om vi ansåg att en intervjuperson redan hade svarat på en fråga i ett tidigare svar kunde det därför hända att vi hoppade över den frågan senare. På liknande sätt kan frågorna i intervjuerna skilja sig något beroende på hur eller vad intervjupersonerna har svarat i tidigare frågor.

Den rådande pandemisituationen, samt det faktum att en stor del av våra intervjuobjekt arbetar hemifrån i dagsläget, gjorde att vi var tvungna att utföra intervjuerna via videosamtals-applikationerna Microsoft Teams och Zoom. Jacobsen (2002) menar att så kallade besöksintervjuer är mer givande med hänsyn till svaren då det leder till mindre begränsningar än telefonintervjuer (Jacobsen, 2002). Då den teknologi vi använde tillät oss att se den svarande personen under intervjun genom webkamera, anser vi oss ha medierat den effekten i den mån som var möjlig, givet den rådande pandemin. För att underlätta transkribering samt som ett underlag för oss att gå tillbaka till vid analys, valde vi att spela in samtliga intervjuer. Innan vi började spela in intervjun har vi haft en kort dialog med personen i fråga, där vi presenterade oss samt säkerställt att personen sett och hört oss väl. I intervjun med Organisation 3 uppstod det tekniska problem vilket ledde till att intervjun genomfördes utan webbkameror.

3.4 Urval

I urvalsprocessen har våra kriterier varit att intervjua personer som ansvarar för eller har en god översikt av arbetet med informationssäkerhet på organisationerna. Detta på grund av att våra frågor till stor del handlar om upplevda utmaningar och de potentiella åtgärder som organisationer har gjort kring arbetet inom informationssäkerhet vid storskaligt distansarbete. Det var även ett kriterium att organisationerna arbetade på distans i en stor skala. För att få kontakt med personer som uppnådde dessa kriterier skickade vi ut mail till ett 30-tal organisationer. Vid urvalet av organisationer har inte någon speciell bransch varit i fokus. Det väsentliga för vår studie anser vi vara att organisationen hanterar information som behöver skyddas. Vi skickade därför enbart ut mail till organisationen där vi kunde tänka oss att de hade personal i en arbetsroll som passade våra kriterier.

Kontakt med organisationerna skedde först genom organisationernas info-mail där vi sedan blev vidarebefordrade till en person inom det ansvarsområde vi sökte. I vårt mail beskrev vi vad vår undersökning handlade om och vilka ämnen som kommer att diskuteras samt ungefärlig längd på intervjun och deras rättigheter angående anonymitet och att intervjun kommer att spelas in. Vid eventuella svar om tänkbar medverkan bestämdes en tid för intervjun samt mer information om hur inspelningsprocessen kommer att se ut angående transkribering, anonymitet och återkoppling.

Vi såg till att upplysa alla våra intervjupersoner om att både deras och organisationens identitet kommer att vara anonyma. Vi valde att anonymisera våra intervjupersoner dels för att undersökningen kan anses hantera känsliga frågor och dels för att Jacobsen (2002) skriver att anonymisering kan minska risken för att intervjupersoner ska tala osanning.

Informant 1 - I1 **Genomförd** 03-05-2021 **Samtalslängd** 27:01	**Roll** Säkerhetsskyddschef. **Organisation 1 - O1** Företag inom kärnkraftsbranschen. Cirka 170 anställda. **Relevant erfarenhet** Har haft rollen som säkerhetsskyddschef i 5 år.
Informant 2 - I2 **Genomförd** 03-05-2021 **Samtalslängd** 24:49	**Roll** Chief Security Officer (CSO). **Organisation 2 - O2** Internationellt IT-konsultbolag. Cirka 1300 anställda. **Relevant erfarenhet** 10 års erfarenhet inom IT-branschen.
Informant 3 - I3 **Genomförd** 12-05-2021 **Samtalslängd** 22:42	**Roll** IT-chef. Ansvarig för IT- och informationssäkerhet. **Organisation 3 - O3** Biotech-företag. Cirka 100 anställda. **Relevant erfarenhet** Cirka 10 års erfarenhet inom sin roll.
Informant 4 - I4 **Genomförd** 17-05-2021 **Samtalslängd** 24:57	**Roll** Chief Information Security Officer **Organisation 4 - O4** 500+ anställda **Relevant erfarenhet** 10 års erfarenhet inom informationssäkerhet.

Tabell 2: Tabell över informanter

3.5 Validitet och Reliabilitet

För att bedöma kvaliteten på den data som samlas in bör den bedömas utifrån validitet och reliabilitet (Jacobsen, 2002). Med validitet och reliabilitet menas att empirin är tillförlitlig, trovärdig och giltig (Jacobsen, 2002). För att stärka validiteten gav vi våra intervjuobjekt möjlighet att själva läsa igenom våra transkriberingar av intervjuerna, och kommentera om de kände att deras svar inte hade presenterats på ett korrekt sätt (Jacobsen, 2002). I mailet vi skickade ut till organisationerna beskrev vi vilka övergripande områden som intervjun skulle behandla och vad syftet med intervjun var. Då vi önskade att våra informanter skulle svara naturligt och spontant på våra frågor valde vi dock att inte ge dem tillgång till våra specifika

frågor på förhand. Detta är ett steg i att stärka validiteten i undersökningen enligt Jacobsen (2002). För att svaren vi fick av informanterna inte skulle vara partiska var de väl informerade om att de blev anonymiserade och på det viset kunde svara utifrån vad de tyckte och inte utifrån vad som speglade deras organisation på bästa sätt.

3.6 Etik

Vid säkerställandet av en etiskt korrekt intervjuprocess har vi utgått från de tre områden som Jacobsen (2002) beskriver är viktiga att ta i beaktning.

Vi har varit tydliga med att intervjuerna är frivilliga och kan avbrytas av informanter om de så önskar, för att säkerställa *informerat samtycke* (Jacobsen, 2002). För att vidare styrka kravet på informerat samtycke har informanterna i ett tidigt skede fått information om vad intervjun kommer att handla om och möjlighet till att ställa frågor till oss angående intervjun. Då vi genomför dessa intervjuer för att förstå organisationers arbete med informationssäkerhet vid distansarbete, är frågorna inte personliga eller inkräktande och säkerställer därigenom *rätten till privatliv* (Jacobsen, 2002). Detta styrks ytterligare av det faktum att samtliga informanter och organisationer i vår studie är anonyma. Vi har spelat in intervjuerna för att underlätta transkribering, och tydliggjort för samtliga informanter att de kommer att få tillgång till transkriberingen och har möjlighet till invändningar ifall något inte stämmer. Detta anser vi säkerställer Jacobsens (2002) tredje aspekt, *kravet på riktig presentation.* Ifall informanterna skulle säga något de anser är känsligt och inte vill ha med i transkriberingen har de haft möjlighet att korrigera den. Detta beskriver Oates (2005) som att informanterna ska ha rätt till sekretess, där information informanten anser vara känslig inte ska tas med.

3.7 Transkribering

För att underlätta läsningen av de transkriberade intervjuerna har vi valt att inte skriva ut olika ljud som inte tillför något värdefullt för läsaren. Exempel på sådana ljud är till exempel utfyllnadsord som “eh” och “öh” samt upprepningar eller stamning från intervjupersonerna. Vi har däremot valt att ha kvar jakande ord som “mm”. Längre pauser har kodats som tre punkter i transkriberingen då vi anser att det kan vara värdefullt för att få en förståelse för intervjupersonens svar. För att informera läsaren har vi gjort en kort guide till vår kodning av transkriberingarna. Guiden återfinns även i bilagan till varje transkribering.

Kodord	**Betydelse**
(xx)	Svårt att urskilja exakt vad som sägs i inspelningen.
(osäkert ord?)	Något osäker på exakt vilket ord som sägs men har skrivit ut vad vi tycks höra.
****	Anonymisering av namn eller andra identifierande ord.

…	Längre paus.

Tabell 3: Transkiberingsguide

För att analysera datan har vi utgått ifrån Jacobsens (2002) tre steg: beskrivning, systematisering och kategorisering samt kombination. Först har datan behandlats grundligt i det som Jacobsen (2002) kallar för beskrivningsfasen. Därefter har datan systematiersats genom att förenkla och ta fram den information som är av relevans för undersökningen. Jacobsen (2002) kallar detta för systematisering av datan vilket är viktigt för att få en överblick över relevant data. I den sista fasen kan datan börja tolkas genom att generalisera informationen för att hitta samband och mönster (Jacobsen, 2002).

4 Resultat

I kapitel 4 presenteras resultatet av den empiriska undersökningen. Empirin utgår ifrån de områden som tidigare har identifierats och presenterats i litteraturkapitlet.

4.1 Policys och riktlinjer

Alla de tillfrågade svarade att de i någon mån arbetar med säkerhetspolicys och riktlinjer som de anställda ska följa. Informant 1 svarade att deras policy är skapad utifrån regler de får från koncernen och att mycket av deras arbete är styrt av dessa regler. Informant 2 berättar att de arbetar enligt ISO-27001 standarden och generellt har ett stort fokus på säkerhet.

> *"Vi har alltid haft ett stort fokus på säkerhet. Alltså våra kontor har, vi har alltid haft clean desk, du har inget eget skrivbord, det är aktivitetsbaserat så du rensar skrivbordet när du går på lunch, du lämnar inte kvar någonting framme, någonsin. Vilket är jobbigt, men också bidragande till att det inte byggs hemliga pappershögar som man behöver gå och fundera på."* - (I2, 2021, rad 19)

Informant 3 som arbetade på en organisation i mindre storlek förklarade att de tidigare inte hade arbetat aktivt med säkerhetspolicys då de inte haft behov för det. I takt med att organisationen växte till sig och mognade märkte de behovet av att aktivt arbeta med det.

> *"Vi har inte arbetat så aktivt med säkerhetspolicys förrän nyligen. Vi har kommit upp i en nivå där vi har liksom… där vi känner att de här grejerna behövs att man kan inte hålla koll på allting liksom, det är så mycket som händer så man kan inte hålla koll på allting själva så då har vi kommit till en nivå där vi verkligen behöver ha policys i säkerhetsarbetet."* - (I3, 2021, rad 15)

Vid frågan om organisationerna har behövt anpassa sina policys eller riktlinjer för distansarbete svarade informant 2 och 4 att de inte har gjort några ändringar i sina övergripande policys men att de har gjort förtydliganden i sina riktlinjer och guidelines.

> *"Ja, det har vi gjort. Men på ganska operativ nivå skulle jag säga. Vi har inte ändrat det stora övergripande ramverket för informationssäkerhet på grund av pandemin utan det har varit på mycket praktisk nivå att gå ut och kommunicera."* - (I4, 2021, rad 12).

Likadant svarade informant 1 att det inte har skett några ändringar i deras policys eller riktlinjer men att det har uppstått situationer på grund av distansarbetet där personalen har varit osäker på hur de säkert ska gå tillväga. Vid sådana situationer har bedömningar fått göras från fall till fall.

> *"[...] Men jag vet ju att det har hänt vid vissa tillfällen att personer har behövt den här fysiska information i sitt dagliga arbete under vissa tillfällen och då blir det ju lite problematiskt för vi har ju inte samma fysiska skydd i hemmet som vi har på kontoret. Så då har vi ju liksom fått göra vissa bedömningar huruvida man kan låna hem det här materialet och hur man ska hantera det då för att man ska kan känna sig säker så att säga att det sköts på ett bra sätt."* - (I1, 2021, rad 16)

Informant 3 berättar att hen inte ser att det skulle uppstå ytterligare svårigheter eller problem att följa riktlinjerna för de anställda vid distansarbete. Informant 3 berättar vidare att deras arbetssätt sedan tidigare har varit anpassat för distansarbete och de har därför inte behövt göra några förändringar.

> *"Men vår approach till det här har ju egentligen sen många år tillbaka har vår approach varit remote first. Inte nödvändigtvis för att det skulle komma en pandemi men för att, ja vara moderna helt enkelt och kunna erbjuda folk att arbeta på den annan plats."* - (I3, 2021, rad 21)

4.2 Utbildning och träning

Vid frågor angående arbetet kring utbildning och träning av de anställda svarade informant 3 att de inte hade någon utbildning för de anställda utan att de på Organisation 3 istället gjorde kontinuerliga utskick av information. Informant 4 svarade att det finns en utbildning på intranätet som anställda måste göra samt kontinuerliga utskick av information efter det. Både informant 1 och informant 2 uppgav att utbildning ges till nyanställda och att det sedan är något deras organisationer kontinuerligt följer upp. För att hela tiden hålla utbildningsmaterialet uppdaterat bearbetar man det mellan utbildningstillfällena och korrigerar materialet.

> *"Det är allt ifrån fysskydd , infosäk, brandskydd och så vidare och det är en kravutbildning, eller det har varit en kravutbildning då och det är en sån här e-modulsutbildning då, där varje block då, om vi säger infosäk är ett block, tar kanske 15 minuter att genomföra, med flervalsfrågor och så vidare. Det är en kravkurs, det vill säga när du börjar på O1 så måste du genomföra den innan du får ditt passerkort och sen återkommer den, tanken är att den ska återkomma vart tredje år"* - **(**I1, 2021, rad 33)

> *"Alltså vi har ju i vårt löpande säkerhetsarbete så har vi ju löpande årligen uppdateringar, nyanställda gör utbildningar och varje år ska man genomgå en uppdaterad version så att man håller sig ajour med vad vi ser som dom största hoten och dom senaste åren, ja det har ju varit, ja men det är ju phishing liksom."* - (I2, 2021, rad 27)

På frågor angående om de anställda har fått någon specifik utbildning om distansarbete och informationssäkerhet utöver den vanliga utbildningen svarade samtliga informanter att de inte har haft någon specifik utbildning för just detta, men att de använder sig av deras intranät och liknande för att påminna och upplysa de anställda om att tänka extra på informationssäkerhet.

> *"[...] har jag tryckt lite på just det här med infosäkerhet att det är extra, så att säga, viktigt, det är alltid viktigt, men nu är det liksom extra viktigt nu när ni sitter*

hemifrån och jobbar för det är inte riktigt samma, till exempel samma fysskydd som det är på arbetsplatsen och så vidare." - (I1, 2021, rad 39)

4.3 Medvetenhet

Gällande frågor som berörde hur medvetna personalen är om arbetet med informationssäkerhet skilde sig svaren åt. Informant 2 berättar att med tanke på hur många anställda det är hos organisationen finns det därför också en bred variation av medvetenhet och attityd gentemot informationssäkerhet och det är svårt att ge ett gemensamt svar för alla de anställda. Men i och med att de satsar mycket på säkerhet har de flesta anställda en god säkerhetsmedvetenhet. Även i de andra intervjuerna uppgav de intervjuade att de generellt sett tycker medvetenheten och attityden gentemot informationssäkerhet är god. Informant 4 berättar att de har en så stor omsättning av personal att medvetenheten är svår att mäta och kan skifta från år till år beroende på vilken bakgrund de anställda har. De anställdas ålder är något både Informant 2 och Informant 3 nämner. Informant 3 förklarar att snittåldern hos de anställda på Organisation 3 ligger mellan 35-40 års ålder och tror därför inte att förståelsen för informationssäkerhet är något problem. Däremot framhäver hen utmaningen med att se till att de anställda, speciellt de som känner sig osäkra och är rädda att något ska gå fel, ska få rätt information och utbildning för att känna sig bekväma.

"Men jag tror att den största utmaningen där är att liksom se till att de får rätt information och vad de ska göra och vad de ska tänka på. Så man inte blir orolig för allting som händer." - (I3, 2021, rad 52)

Vid frågor rörande huruvida attityden och medvetenheten vid distansarbete har förändrats och om det är en utmaning skiljer sig informanternas svar åt. Informant 1 säger sig inte ha sett någon större skillnad i attityd och medvetenhet hos de anställda sen de gick över till distansarbete. Informant 1 tror dock att bibehållning av en fortsatt hög medvetenhet kring informationssäkerhet är en långsiktig utmaning vid distansarbete. Informant 2 svarar på liknande sätt.

"Och det är lite på något vis, det är ju ganska enkelt så länge man hanterar det på kontoret och så vidare då. Men det är klart att då blir det att det sker lite på automatik. Men sitter man då mycket på distans så gäller det liksom att hela tiden ha den där medvetenheten då så det inte blir att man slentrianmässigt och så glömmer man bort och sådär." - (I1, 2021, rad 86)

Informant 3 påpekar att deras arbetssätt kring att öka medvetenheten är oförändrat. De utför månadsmöten där viktiga saker diskuteras för att öka medvetenheten. Däremot berättar informant 3 och 4 att eftersom kulturella aspekter försvinner vid distansarbete blir det en utmaning att långsiktigt bibehålla medvetenheten bland de anställda.

"Den största utmaningen där är väl egentligen den kulturella utmaningen och awareness-utmaningen liksom att nu är man inte längre on site och man kan inte möta på oss i korridorerna och snacka om en grej man såg på internet eller ett mail man fick som såg konstigt ut" - (I3, 2021, rad 72)

Informant 4 understryker även att den enskilde medarbetaren rent praktiskt får ett mycket större ansvar.

Trots att det inte fanns någon direkt fråga om de kulturella aspekterna var detta något som alla organisationer tog upp som en utmaning vid distansarbete. Alla informanter var eniga om att bibehålla en god medvetenhet vid distansarbete, särskilt långsiktigt, var en utmaning eftersom många kulturella aspekter försvinner. Informant 2 berättar att hen redan har sett konsekvenserna av distansarbetet ur ett kulturellt perspektiv. De gånger hen har varit inne på kontoret så har det funnits nyanställda som informant 2 aldrig har sett innan samt att policys har påverkats gällande till exempel att ha synliga nyckelband vilket är ett krav enligt deras policys.

> *"[...] jag ska kunna se på dig utan att fråga om du ska vara här eller inte. Det märker man också den tappar man ju också när man bara sitter fem pers där, och varför ska jag ha på mig den liksom? Ja men det är ju för att den ska vara på liksom. Det är ju dom aspekterna som är dom läskiga."* - (I2, 2021, rad 43)

Vidare svarade informant 2 följande på frågan vilka långsiktiga utmaningar kring informationssäkerhet vid distansarbete hen ser.

> *"Informationssäkerhetsmässigt så kommer utmaningen att vara att hålla ihop en miljö liksom."* - (I2, 2021, rad 55)

Informant 3 svarade enligt liknande att eftersom de har arbetat enligt remote first är den tekniska biten lika säker oberoende på var man befinner sig utan istället är den stora långsiktiga utmaningen medvetenhet och det kulturella.

> *"Men angående remote arbetet tror jag absolut att det kulturella är det stora."* - (I3, 2021, rad 74)

Vidare svarade informant 3 vid en fråga om policys och riktlinjer att hen absolut tror att det är viktigt med skrivna policys men slutgiltigen är det viktiga att få in innehållet i policyn in i det vardagliga arbetet och organisationskulturen.

> *"Även om jag liksom, jag tror att det är viktigt att ha policys skrivna för saker så är det ju så att culture eats policy for breakfast liksom haha."* - (I3, 2021, rad 21)

Informant 4 berättade att bibehålla en god medvetenhet är utmanande på grund av att vissa kulturella aspekter försvinner vid distansarbete.

> *"Jag tror fortfarande att medvetenheten är den viktiga, för det är en kulturförändring som du själv nämnde här om man sitter hemma. Hur ska man nå sina kollegor och medarbetare ute när de inte ens är vid kaffemaskinen som jag brukar säga."* - (I4, 2021, rad 62)

4.4 Compliance

Gällande att mäta compliance och uppfattningen om hur väl anställda följer utsatta policys och riktlinjer vid distansarbete hade organisationerna olika uppfattningar och tillvägagångssätt. Både organisation 1,2 och 4 utför kontinuerliga kontroller av efterlevnad.

När det gäller distansarbete och att mäta compliance uttrycker informant 2 att det är en utmaning eftersom att organisationen inte har någon möjlighet att utföra kontroller vid distansarbete.

> *"Nej, det kan vi ju inte göra. Utan vi gör vad vi kan. Vi kan, vi ser vilka som är online på VPN och hur dom bitarna efterlevs, men nej som sagt vi kan ju inte göra några hembesök och tittar efter om dom har låst in papperna."* - (I2, 2021, rad 33)

> *"Men compliance är ju svårt att mäta hemma liksom, vi lever fortfarande i Sverige liksom, inte Östberlin så vi kommer inte att göra hembesök. "* - (I2, 2021, rad 55)

Informant 4 berättar att det har skett extra åtgärder för att upplysa de anställda om att följa riktlinjerna vid distansarbete. Vidare poängterar informant 4 att det kan vara en utmaning för de anställda att följa riktlinjerna vid distansarbete på grund av olika hemsituationer.

> *Och sen är det just det här också att vad gör jag med mitt eget nätverk hemma liksom? Hur skyddar jag det när jag inte sitter på jobbet. Det är också… ja helt plötsligt blir man helt beroende av sin hemsituation.* - (I4, 2021, rad 16)

Informant 1 poängterar att det finns en god säkerhetskultur inom organisationen och att hen inte har uppmärksammat några problem eller utmaningar gällande compliance och distansarbete. Vid en fråga om att följa policys vid distansarbete svarade informant 1 följande.

> *"[..] jag hade nog inte fått de frågorna om man inte efterlever så att säga policys och instruktioner. Så jag vill nog sticka ut hakan lite och säga att den, liksom, ansvarskänslan för att följa det är hög, den är på den övre skalan skulle jag säga då, utan att veta då, utan att veta liksom ingen exakt sådär."* - (I1, 2021, rad 26)

Informant 3 däremot berättar att de inte mäter compliance på något sätt, varken vid distansarbete eller vid normalt arbete på kontoret. Hen poängterar dock att det inte borde vara några problem för dem anställda att följa de uppsatta riktlinjerna vid distansarbete då riktlinjerna redan innan pandemin har varit anpassade för ett modernt arbetssätt där distansarbete har varit tilltänkt.

4.5 Ledningen

På frågan om hur ledningens förhållande till arbetet med informationssäkerhet ser ut var svaren skiftande. Informant 2 svarade att på grund av deras bransch och verksamhetsområde så var ledningen väldigt medveten om hur viktigt informationssäkerhet är. Vidare berättar informant 2 att vid förändringar och nya påbud kring riktlinjer, såsom vid det påtvingade distansarbetet, så skickar ledningen ut det med deras stämpel så att de anställda ska förstå att det är ett centralt direktiv direkt från ledningen som ska efterföljas. Även informant 1 och 4 svarade att medvetenheten och inställningen från ledningen gällande informationssäkerhetsarbetet var god, men att de kan sakna en förståelse för vissa saker.

> *"Den starkaste medvetenheten är på styrelsenivån"* - (I4, 2021, rad 46)

Informant 1, 2 och 4 berättar att ledningen aktivt har förmedlat om informationssäkerhet vid distansarbete.

Informant 3 svarade att ledningen har haft en "låt gå" attityd, men när de fick mer kunskap inom ämnet insåg de vikten av att förbättra säkerheten.

> *"Det har varit ganska… Låt gå attityd haha, fram tills typ nu. Vi har lyckats få igenom att vi skulle göra en fullständig cyber security review, [...] Jag tror detta har blivit en ganska bra väckarklocka för ledningen, att nu är det dags att ta tag i det här."* - (I3, 2021, rad 55)

5. Diskussion

I kapitel 5 diskuteras de resultat som har presenterats i kapitel 4. De utmaningar som har presenterats i empirin diskuteras med en grund i den litteratur som har presenterats i kapitel 2. Diskussionskapitlet syftar till att analysera de utmaningar som har uppkommit samt att jämföra organisationernas hanterande av dessa med vad litteraturen påstår är viktiga faktorer.

5.1 Policys och riktlinjer

Gällande policys och riktlinjer kunde vi utifrån datainsamlingen konstatera ett antal olika tillvägagångssätt mellan organisationerna. Ingen av organisationerna hade gjort några ändringar i sina övergripande policys. Två av organisationerna hade gjort förtydliganden i sina riktlinjer kring distansarbete och även om den generella inställningen från organisationerna var att arbetet kring säkerhetspolicys och riktlinjer fungerade bra vid distansarbete kan vi, utifrån teorin, urskilja några problematiska aspekter som uppstår vid distansarbete.

Ett exempel är det som informant 1 beskrev om att det har uppkommit situationer där personalen har behövt säkerhetsklassat material till deras arbete, men enligt säkerhetspolicyn får materialet inte lämna kontoret. Sådana aspekter kan härledas till vad Samonas och Coss (2014) samt Kraemer och Carayon (2007) skriver om att riktlinjer som anses vara för krångliga, tidskrävande eller på andra sätt skapar för stora svårigheter i det vardagliga arbetet riskerar att inte följas.

Sådan information som behövt hålla en hög grad confidentiality har kunnat skyddas fysiskt inom organisationers väggar, med begränsning på availability, då den endast har varit tillgänglig på plats hos organisationen. Med distansarbetet har denna information nu istället behövt komma in i de anställdas hem. Precis som Baybulatov och Promyslov (2020) skriver, skiljer det sig vilka grundpelare på CIA-triaden det läggs störst vikt vid beroende på var den appliceras. Samtidigt som organisationer började arbeta på distans blev de tvungna att lägga mer vikt på availability då de anställda behöver ha tillgång till materialet oberoende av var de befinner sig för att kunna utföra sitt arbete.

I vår undersökning kunde det märkas en viss skillnad mellan organisationer och hur ingående de arbetar med informationssäkerhet. Några organisationer behandlar information som omfattas av säkerhetsskyddslagen och extra åtgärder behöver då vidtas för att just denna information ska hållas säker och skyddas. Detta överensstämmer med vad Cherdantseva och Hilton (2013) skriver om att all information inte är lika känslig och åtgärder kan vidtas i proportion till detta. Organisationer som behandlar denna känsliga information står således inför en större utmaning att följa säkerhetskraven när informationen ska finnas i anställdas hem, vilket även kommer att försvåra arbetet med att utforma policys som är lätta att efterfölja.

Vidare har alla informanter uttryckt att det är en utmaning i att bibehålla en god säkerhetskultur då organisationskulturen påverkas vid distansarbete. Exempel på detta är problematiken som informant 2 uttryckte om att personalens attityd mot att följa kravet på att alltid ha på sig sitt nyckelband när de faktiskt är på kontoret har försämrats. Vi anser då att det som Mattord och Whitman (2011) tar upp med att en policy ska sträva mot att bli en naturlig del i organisationskulturen försvåras ännu mer vid distansarbete. Informant 3 uttrycker det på ett bra sätt:

> *"[...] culture eats policy for breakfast liksom"* - (I3, 2021, rad 21)

5.2 Utbildning

Den aspekt av utbildning som har behandlats i den här uppsatsen handlar inte om huruvida det är en utmaning att utbilda de anställda vid distansarbete. Istället har vi frågat informanterna i vilken mån de anställda utbildas och i vilken mån de har fått information om informationssäkerhet vid distansarbete. Alla organisationer har sedan det storskaliga distansarbetet inletts haft en kontinuerlig kommunikation med sina anställda om informationssäkerhet via diverse intranät och informationsutskick, vilket är precis vad Puhakainen och Siponen (2010) samt Bulgurcu, Cavusoglu & Benbasat (2010) menar på är en viktig faktor för att öka compliance och medvetenhet.

Det var vanligt att utbildning av de anställda gjordes första gången vid nyanställningar. Att de anställda direkt får information och lärdom om hur de bör arbeta utifrån organisationens riktlinjer och värderingar medför att organisationen kan forma deras säkerhetstänk direkt. Detta är precis i linje med vad flera författare i teorin också beskriver (Nykodym, Kahle-Piasecki & Marsillac, 2010; Mattord & Whitman 2011). Genom att kontinuerligt uppdatera och ha fortsatt utbildning bistår organisationer sina anställda med det stöd de behöver för att ha goda förutsättningar att hantera de hot och problem som uppstår allt eftersom omvärlden förändras.

5.3 Medvetenhet

Samtliga informanter menar på att den generella medvetenheten bland organisationerna är god. Däremot har även alla informanter berättat att bibehållandet av medvetenheten vid distansarbete är en stor utmaning, särskilt eftersom vissa kulturella aspekter försvinner vid distansarbete.

Leach (2003) skriver att anställda blir influerade av vilken attityd som personer runt omkring dem har gentemot säkerhet. Vid distansarbete försvinner delar av denna aspekt. Även om personal fortfarande har kontakt med varandra via diverse tekniska program så försvinner mindre konversationer mellan personalen, och särskilt mellan personalen och informationssäkerhetspersonal. Även om denna aspekt kan verkas vara liten är det något som två av informanterna uttryckligen har beskrivit som viktigt inom arbetet för medvetenhet.

Informant 2 beskriver även utmaningar med att den enskilde anställde behöver ha en hög medvetenhet om de tekniska aspekterna vid distansarbete. Olika smarta produkter som kan återfinnas i de anställdas hem kan vara lätta byten för obehöriga att få ankomst till. Detta kan

ses som en säkerhetsrisk då Campeon (2019) berättar att det räcker med en enda användare för att äventyra ett helt nätverk. Det är alltså ännu mer ansvar på varje anställd, vilket även är något som informant 4 berättar om. Detta faller även i linje med vad Aminzade (2018) berättar om att det är viktigt för varje individ att vara medveten om hur ens handlingar kan påverka det stora sammanhanget.

5.4 Compliance

Precis som Puhakainen och Siponen (2010) skriver är den faktiska akten att efterfölja policys en av de viktigaste faktorerna för att uppnå en god informationssäkerhet. Vid distansarbete skiljer sig uppfattningen om huruvida compliance är mer av en utmaning än vid arbete på plats. Informant 1 berättar att det finns en hög ansvarskänsla inom organisationen och att hen inte ser några större problem med compliance vid distansarbete. På liknande sätt svarar informant 3 att de från grunden har haft ett remote first tänk och därför ser informanten inte några större problem kring compliance vid distans jämfört med på plats.

Informant 2 uttrycker problemet med att de vid distansarbete inte har något sätt att mäta eller se till så att deras policys efterföljs. Som ett exempel berättar informanten om att de arbetar med en strikt clean-desk policy. Vidare uttrycker informanten problemet med att den policyn förmodligen inte alls efterföljs lika väl vid distansarbete, vilket är vad Siponen, Pahnila och Mahmood (2010) syftar på med att den sociala aspekten och människors attityd runt omkring en påverkar hur väl anställda kommer att följa säkerhetspolicys. Siponen, Pahnila och Mahmood (2010) berättar att organisationer kan skapa ett socialt tryck för att främja de anställdas beteenden, men som informant 2 säger så försvinner det sociala trycket vid distansarbete. En liknande aspekt som både informant 2 och 4 tar upp är att de anställdas förmåga att följa riktlinjer varierar beroende på deras hemsituation. På kontoret finns förutsättningarna för att följa alla riktlinjer men vid distansarbetet är det upp till den enskilde medarbetaren att säkerställa att allting är säkert.

5.5 Ledningen

Enligt en majoritet av informanterna var ledningens engagemang och medvetenhet gentemot informationssäkerhet generellt god, men några av informanterna uttryckte att det kan saknas förståelse och en viss kunskap om vissa ämnen. Informant 4 uttryckte att inställningen hos ledningen var god men att förståelsen inom vissa områden kan göras bättre, vilket var något de aktivt arbetade med. Detta går i linje med vad Siponen, Pahnila & Mahmood (2010) påpekar om att det är viktigt att även utbilda ledningen. På ett liknande sätt berättade informant 3 att en säkerhetsreview nyligen har genomförts för att bättre kunna visa och utbilda ledningen om varför det behövs mer fokus på informationssäkerhet.

Gällande distansarbete och ledningens roll vid organisationsförändringen under Covid-19 pandemin svarade en majoritet av organisationerna att ledningen aktivt hade engagerat sig i frågan om informationssäkerhet. Informant 2 berättade att direktiv som skickats ut haft ledningens stämpel för att påvisa att besluten kom uppifrån. Detta visar hela organisationen att det är ledningen som lägger grunden och stödjer direktiven, vilket är viktigt för att de ska efterföljas (Puhakainen & Siponen, 2010). Det faller även i linje med vad tidigare forskning

anser att ledningen bör göra för att lyckas med organisationsförändringar (Paton & McCalman, 2008; Anderson & Anderson 2010; Burnes, 2011; Gill 2002).

6 Slutsats

Det huvudsakliga syftet med denna uppsats var att undersöka vilka aspekter av informationssäkerhet som anses vara utmanande vid storskaligt distansarbete samt att undersöka på vilka sätt organisationer eventuellt har hanterat dessa utmaningar. Därav löd forskningsfrågan enligt följande:

Vilka aspekter av informationssäkerhet är utmanande för organisationer vid storskaligt distansarbete och hur hanteras dessa?

Undersökningen har visat på att storskaligt distansarbete innebär flera utmaningar kring arbetet med informationssäkerhet. Vi kan konstatera att arbetet med att bibehålla en god medvetenhet är en av de största utmaningar som organisationer upplever. På grund av att vissa kulturella aspekter försvinner blir det svårare för organisationer att underhålla säkerhetskulturen. Samtliga informanter uppger att arbetet med säkerhetskultur är viktigt för att upprätthålla en god medvetenhet kring informationssäkerhet.

Vidare har undersökningen konstaterat att organisationernas förmåga att mäta compliance försvåras vid distansarbete. Med grund i teorin och av informanternas svar argumenterar vi även för att compliance försvåras i den mån att påtryck från människor och miljö runt omkring en minskas vid distansarbete, vilket leder till en ökad risk för att anställda inte kommer att följa den utsatta säkerhetspolicyn.

Vi kan även konstatera att organisationernas arbetssätt kring utbildning och policys inte förändras på några större sätt vid distansarbete. Organisationerna arbetade i olika grad med utbildning och policys, men något som är gemensamt är att alla organisationer kontinuerligt påminner de anställda för att höja medvetenheten vid distansarbete.

Ledning är enligt teorin en viktig faktor både för att uppnå en god säkerhetskultur och för att lyckas med organisationsförändringar. Vår undersökning visar på att ledningen hos organisationerna generellt har ett bra engagemang, även om det har framkommit att ledningen i vissa fall saknar en viss kunskap om informationssäkerhet. Undersökningen visar även på att ledningen hos en majoritet av organisationerna har varit aktiva vid förmedlandet av information och riktlinjer vid distansarbete.

Vidare kan vi genom undersökningen konstatera att organisationernas storlek, bransch och säkerhetskultur har haft en betydelse för upplevda utmaningar. De av informanterna som ansvarar för större organisationer med mycket säkerhetsklassat material har generellt sett distansarbetet som mer utmanande än de andra informanterna.

6.1 Förslag på fortsatt forskning

Vi har genom vår undersökning kunnat konstatera att det har uppkommit ett flertal utmaningar vid distansarbete. Av dessa utmaningar var svårigheten att bibehålla medvetenhet på grund av att säkerhetskulturella aspekter försvinner den mest uttalade. Då denna undersökning har haft en bred utforskande modell som har undersökt flera aspekter hade fortsatt forskning enbart fokuserad på denna utmaning varit av intresse. Denna undersökning är utförd ungefär ett år efter att organisationerna tvingades till storskaligt distansarbete och det hade även varit av intresse att se hur denna utmaning hanteras efter en ännu längre period.

7 Referenser

Agarwal, A. & Agarwal, A. (2011). The security risks associated with cloud computing. *International Journal of Computer Applications in Engineering Sciences*, *1*, pp. 257-259.

Alhosani, K.E.H.A., Khalid, S.K.A., Samsudin, N.A., Jamel, S. & bin Mohamad, K.M., (2019), November. A policy driven, human oriented information security model: a case study in UAE banking sector. *2019 IEEE Conference on Application, Information and Network Security (AINS)* pp. 12-17.

Allied Telecom. (2016). The History of Telecommuting. Tillgänglig på: https://www.alliedtelecom.net/the-history-of-telecommuting/ [Hämtad 20 april 2021]

Alotaibi, M.J., Furnell, S. & Clarke, N. (2019). A framework for reporting and dealing with end-user security policy compliance. *Information & Computer Security*.

Alvesson, M. (2013). Understanding Organizational Culture, 2nd edn, London: SAGE Publications Ltd.

Aminzade, M., (2018). Confidentiality, integrity and availability–finding a balanced IT framework. *Network Security*, vol. *2018*, no. 5, pp. 9-11

Anderson, D. & Anderson, L.A. (2010). Beyond Change Management How to achieve breakthrough results through conscious change leadership. San Fransisco, Pfeiffer

Andress, J. (2014). The basics of information security: understanding the fundamentals of InfoSec in theory and practice. Syngress.

Bada, M., Sasse, A.M. & Nurse, J.R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour?. *arXiv preprint arXiv:1901.02672*.

Baybulatov, A.A. & Promyslov, V.G. (2020). October. Cybersecurity Assessment Using Delay from Backlog Bound Calculation. In *2020 IEEE 14th International Conference on Application of Information and Communication Technologies (AICT)* pp. 1-6.

BBC. (2020). Coronavirus confirmed as pandemic by World Health Organization, 11 Mars. Tillgänglig på: https://www.bbc.com/news/world-51839944 [Hämtad 24 Mars 2021]

Bloom, N. (2020). How working from home works out. *Institute for Economic Policy Research (SIEPR). Policy Brief June*

Borkovich, D. & Skovira, R. (2020). Working from home: Cybersecurity in the age of Covid-19. *Issues in Information Systems*, vol. 21, no 4, pp. 234-246.

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

Burnes, B. (2011). Introduction: Why Does Change Fail, and What Can We Do About It?, *Journal of Change Management*, vol. 11, no. 4, pp. 445-450

Burnes, B. & Jackson, P. (2011). Success and Failure In Organizational Change: An Exploration of the Role of Values, *Journal of Change Management*, vol. 11, no. 2, pp. 133-162

Caldwell, T. (2012). Training–the weakest link. *Computer Fraud & Security*, vol. 2012, no. 9, pp.8-14.

Campean, S. (2019). The Human Factor at the Center of a Cyber Security Culture. *International Journal of Information Security and Cybercrime (IJISC)*, vol. *8*, *no.*1, pp. 51-58.

Centers for Disease Control and Prevention. (2020). United States Coronavirus (COVID-19) Death Toll Surpasses 100,000. Tillgänglig på: https://www.cdc.gov/media/releases/2020/s0528-coronavirus-death-toll.html [Hämtad 17 april 2021]

Centers for Disease Control and Prevention. (2021). When You Can be Around Others After You Had or Likely Had COVID-19. Tillgänglig på: https://www.cdc.gov/coronavirus/2019-ncov/if-you-are-sick/end-home-isolation.html [Hämtad 17 april 2021]

Cherdantseva, Y. & Hilton, J. (2013). September. A reference model of information assurance & security. In *2013 International Conference on Availability, Reliability and Security*. pp. 546-555. IEEE.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. & Baskerville, R., (2013). Future directions for behavioral information security research. *Computers & security*, *32*, pp.90-101.

Deloitte, (n.d). COVID-19: Cyber and the remote workforce. Tillgänglig på: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-covid-19-cyber-and-the-remote-workforce.pdf [Hämtad 24 april 2021]

Eurofound. (2020), Living, working and COVID-19, COVID-19 series, Publications Office of the European Union, Luxembourg. Tillgänglig på: https://www.eurofound.europa.eu/sites/default/files/ef_publication/field_ef_document/ef20059en.pdf [Hämtad 24 april 2021]

Europakommissionen. (2020). Telework in the EU before and after the COVID-19: where we were, where we head to. Tillgänglig på: https://ec.europa.eu/jrc/sites/jrcsh/files/jrc120945_policy_brief_-_covid_and_telework_final.pdf [Hämtad 24 Mars 2021]

Europol, (2020). Pandemic profiteering: how criminals exploit the COVID-19 crisis. Tillgänglig på: https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis [Hämtad 24 Mars 2021]

Eurostat. (2020). How usual is it to work from home?. Tillgänglig på: https://ec.europa.eu/eurostat/web/products-eurostat-news/-/DDN-20200424-1 [Hämtad 24 april 2021]

Federal Bureau of Investigation. (2020). 2020 Internet Crime Report. Tillgänglig på: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf [Hämtad 22 april 2021]

Firdhous, M.F.M. & Hussien, N.A. (2018). December. Data Security Implementations in Cloud Computing: A Critical Review. In *2018 3rd International Conference on Information Technology Research (ICITR)*, pp. 1-5. IEEE.

Folkhälsomyndigheten. (2020). Protect yourself and others from spread of infection. Tillgänglig på: https://www.folkhalsomyndigheten.se/the-public-health-agency-of-sweden/communicable-disease-control/covid-19/protect-yourself-and-others-from-spread-of-infection/ [Hämtad 17 april 2021]

Gartner. (2020). Gartner Survey Reveals 82% of Company Leaders Plan to Allow Employees to Work Remotely Some of the Time. Tillgänglig på: https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time [Hämtad 24 Mars 2021]

Georgiadou, A., Mouzakitis, S. & Askounis, D. (2021). Working from home during COVID-19 crisis: a cyber security culture assessment survey. *Security Journal*, pp. 1-20

Gill, R. (2002). Change management--or change leadership?, *Journal of Change Management*, vol. 3, no. 4, pp. 307-318

Global Workplace Analytics. (2020). Latest Latest Work-at-Home/Telecommuting/Mobile Work/Remote Work Statistics. Tillgänglig på: https://globalworkplaceanalytics.com/telecommuting-statistics [Hämtad: 27 april 2021]

Gollman, D. (2011). Computer Security, 3rd edn, Wiley

Haney, J. & Lutters, W. (2020). Security Awareness Training for the Workforce: Moving Beyond. *IEEE Annals of the History of Computing*, *53*(10), pp.91-95.

Hughes-Lartey, K., Li, M., Botchey, F.E. & Qin, Z., (2021). Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyon*, vol. 7, no 3, p. e06522.

IBM Security. (2020). Cost of a Data Breach Report. Tillgänglig på: https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf [Hämtad: 22 april 2021]

International Labor Organisation, (2020). Covid-19 and the world of work. Second edition. Tillgänglig på: https://www.ilo.org/wcmsp5/groups/public/---dgreports/---dcomm/documents/briefingnote/wcms_740877.pdf [Hämtad 27 april 2021]

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

Kotter, J.P., (2012). *Leading change*. Harvard business press.

Kraemer, S. & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied ergonomics*, vol. 38, no. 2, pp.143-154.

Krombholz, K., Hobel, H., Huber, M. & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and applications*, vol. *22*, pp. 113-122.

Leach, J. (2003). Improving user security behaviour. *Computers & Security*, vol. *22*, no. 8, pp. 685-692.

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

Mahase, E. (2020). Covid-19: UK starts social distancing after new model points to 260 000 potential deaths. *BMJ*, *368*, p.m1089.

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C. & Giannakopoulos, G. (2014). The human factor of information security: Unintentional damage perspective. *Procedia-Social and Behavioral Sciences*, vol. 147, pp. 424-428.

Nykodym, N., Kahle-Piasecki, L. & Marsillac, E.L., 2010. The managers guide to understanding, detecting, and thwarting computer crime: An international performance issue. *Performance Improvement*, vol. 49, no. 5, pp. 42-47.

Oates, B. J. (2005). Researching information systems and computing. Sage.

Paton, R.A. & McCalman, J. (2008). Change Management A Guide to Effective Implementation, 3rd edn, London: SAGE Publications Ltd

Popescu, I., (2018). The Influence of Vulnerabilities on the Information Systems and Methods of Prevention. *International Journal of Information Security and Cybercrime (IJISC)*, vol. 7, no. 2, pp.25-32.

Puhakainen, P. & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study, *MIS Quarterly*, vol. 34, no. 4, pp. 757-778

Qin, T. & Burgoon, J.K. (2007). May. An investigation of heuristics of human judgment in detecting deception and potential implications in countering social engineering. In *2007 IEEE Intelligence and Security Informatics*. pp. 152-159. IEEE.

Samonas, S. & Coss, D. (2014). THE CIA STRIKES BACK: REDEFINING CONFIDENTIALITY, INTEGRITY AND AVAILABILITY IN SECURITY. *Journal of Information System Security*, vol. 10, no. 3.

Schneider, B., Brief, A. P., & Guzzo, R. A. (1996). Creating a climate and culture for sustainable organizational change. *Organizational Dynamics*, vol. 24, no. 4. pp. 7–19.

Skrodelis, H.K., Strebko, J. & Romanovs, A. (2020). October. The Information System Security Governance Tasks in Small and Medium Enterprises. In *2020 61st International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS)*. pp. 1-4. IEEE.

Siponen, M. (2000). A conceptual foundation for organizational information security awareness, *Information Management & Computer Security*, vol. 8, no 1, pp. 31-41.

Siponen, M., Pahnila, S. & Mahmood, M.A. 2010. Compliance with information security policies: An empirical investigation. *Computer*, vol. 43, no. 2, pp.64-7

Stanton, J.M., Stam, K.R., Mastrangelo, P. & Jolton, J., (2005). Analysis of end user security behaviors. *Computers & security*, vol. 24, no. 2, pp.124-133.

Todnem By, R. (2005). Organisational Change Management: A Critical Review, *Journal of Change Management*, vol. 5, no. 4, pp. 369-390

Van Niekerk, J. & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & security*, vol. 29, no. 4, pp. 476-486.

Von Solms, R. & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, vol 38, pp.97-10

Wang, B., Liu, Y., Qian, J. & Parker, S.K. (2021). Achieving effective remote working during the COVID-19 pandemic: A work design perspective. *Applied psychology*, vol. 70, no. 1, pp.16-59.

Whitman, M.E. & Mattord, H.J. (2011). *Principles of information security*. Cengage Learning.

Wood, C.C. & Banks Jr, W.W., (1993). Human error: an overlooked but significant information security problem. *Computers & Security*, vol. 12, no. 1, pp. 51-60

8 Bilagor

8.1 Intervjuguide

- **Inledande frågor**
  - Skulle du kortfattat vilja beskriva vad ert företag gör för någonting?
  - Vilken är din roll på företaget och vilket arbetsområde är du verksam inom?
  - Hur lång erfarenhet har du inom informationssäkerhet?
  - I vilken utsträckning och hur länge har ni arbetat på distans?
- **Policys**
  - Hur ser ert arbete angående säkerhetspolicys och riktlinjer ut?
  - Har ni behövt anpassa era policys eller riktlinjer för distansarbete?
  - Har anställda enkel tillgång till säkerhetspolicyn/riktlinjerna?
  - På vilka sätt, om några, kan riktlinjerna vara svårare att efterfölja vid distansarbete?
- **Compliance**
  - I vilken mån ser ni till att policyn efterföljs?
  - Har det på något sätt varit en utmaning att se till så att riktlinjerna följs vid distansarbete?
  - Har ni gjort något utöver det vanliga för att se till så att de följs?
- **Utbildning**
  - I vilken mån utbildas anställda om informationssäkerhet och era riktlinjer?
  - Har ni en fortsatt kontinuerlig utbildning och kommunikation om informationssäkerhet?
  - Har de fått någon specifik utbildning eller information om hur man arbetar säkert vid distans?
- **Medvetenhet**
  - Hur skulle du säga att personalens attityd och medvetenhet gentemot informationssäkerhet är?
  - På vilka sätt kan det vara utmanande att bibehålla en god medvetenhet på distans jämfört med på plats?
- **Ledning och övriga utmaningar**
  - Hur skulle du säga att ledningens förhållande till arbetet med informationssäkerhet är?
  - Har de aktivt förmedlat om informationssäkerhet vid distansarbete?
  - Har distansarbetet skapat några större utmaningar för er organisation gällande informationssäkerhet som vi inte har tagit upp?
  - Vilka, om några, långsiktiga utmaningar ser du med informationssäkerhet vid distansarbete?

8.2 Intervju med Organisation 1

(xx) = Svårt att urskilja exakt vad som sägs i inspelningen.
(osäkert ord?) = Något osäker på exakt vilket ord som sägs men har skrivit ut vad vi tycks höra.
**** = Anonymisering av namn eller andra identifierande ord.
… = Längre paus.

Intervjuare 1 (JA) – Jakob Andersson (intervjuledare)
Intervjuare 2 (AB) – Andreas Berg
Intervjuare 3 (RH) – Rasmus Holmqvist
Informant 1 (I1) – Säkerhetsskyddschef på 1 (O1)

1. JA: Kan du berätta lite om din roll? Vilket arbetsområde är du verksam inom?

2. I1: Ja, då är jag så kallat säkerhetsskyddschef på O1 och då kan man undra, jaha okej behöver man ha en sån, lyder ni under säkerhetsskyddslagen? Och det gör vi inte direkt, utan det gör vi indirekt på så sätt att vi hanterar verkens rätt så stora mängder information från kärnkraftsverken och kärnkraftverken i sig är skyddsobjekt och faller in under säkerhetsskyddslagen då. Det kom ju ut en ny uppdaterad version nu här som man hade, ja som man har skärpt till ganska avsevärt för 2 år sedan är det nu väl lite styvt, 2019 tror jag att det var. Som sagt, vi hanterar då väldigt stora aggregerade mängder information, både för att kunna genomföra utbildning och det handlar mest om teknisk instruktion som instruktioner, bygglayouter, logikscheman, kretsscheman. Men även för att kunna bygga våra simulatorer och utveckla och hålla dem uppdaterade för de är ju byggda utefter kretsscheman, precis som att, ja, man bygger en byggsats så bygger man utifrån en ritning på samma sätt bygger man simulatorerna så de är liksom inte kopierade från verkat utan man har fått informationen då att konstruera de utifrån logikscheman och kretsscheman och motsvarande. Det har till och med hänt att simulatorerna är mer rätt än verkligheten i sig för de är byggda på pappret.

3. JA: Mm, vad bra. Hur lång erfarenhet har du inom den här rollen?

4. I1: Ja, just inom säkerhetsskyddschefs rollen på O1 så fick jag möjlighet att börja jobba med den 2015, så det är lite styvt, ja 5-6 år där någonting.

5. JA: Ja

6. I1: Jag fick möjlighet och utbilda mig, eller genomföra en utbildning också då, säkerhetschefsutbildning via företagsuniversitet då. Jag tror till och med att den hette diplomerad säkerhetsskyddschef så det kändes bra, då får man liksom en bra grund att stå på. Så säg 5-6 år där någonting.

7. JA: Ja jättebra, och när det gäller distansarbete i vilken utsträckning och hur länge har ni arbetat på distans?

8. I1: Ja, det har vi gjort, höll på att säga ganska länge, jag skulle nog säga att vi har haft den möjligheten att kunna jobba på distans i varje fall i 10 år. Men det som hände oss, det hände ju många andra också i samband med pandemiutbrottet då att

vi ställde ju liksom nästan om över en natt från att man hade möjligheten att jobba på distans och då fungerade det ofta så att de flesta var på kontoret varje dag i veckan och sen händer det ju ibland att man behöver kanske gå till tandläkaren eller någonting och då tog man och jobbade hemifrån och så hade du då liksom möjligheten att gå ifrån och göra dina, vad det nu var för ärenden och sådär. Men det var enstaka dagar i månaden så snittmedarbetaren jobbade på distans, säg max 2, möjligen 3 dagar på en månad då. Nu har det ju slagit om helt så nu jobbar stora delar av personalen, jag skulle säga 70, 60-70% jobbar ju distans kontinuerligt då va.

9. JA: Ja

10. I1: Och nu är det ju på grund av pandemin.

11. JA: Ja, precis. Ja, vad bra. Då går vi in på lite mer säkerhetsfrågor då.

12. I1: Ja

13. JA: Hur ser ert arbete ut angående säkerhetspolicys och riktlinjer?

14. I1: Ja, då är det så att vi måste så att säga följa de krav och regler som kärnkraftverken ställer på oss för det är ju deras information som vi hanterar och sen så utifrån den informationen så skapar vi egen information då va. Typ vi gör ju liksom utbildningsmaterial, typ kompendier och liknande. Som bygger ursprungligen på deras information så då måste vi hantera den utefter deras regler så utifrån det som de har satt upp som regler det har vi ju då liksom fått skruva om och merga om till vår verksamhet. Så vi har ju då liksom ja, instruktioner för hur man får hantera, hur man ska klassificera och sprida information då i olika format, i vårt ledningssystem då va, så att den typen utav instruktioner ligger ju då i ledningssystemet då.

15. JA: Ja, vad bra. Skulle du säga att arbetssättet kring detta har förändrats på något sätt vid distansarbetet?

16. I1: Nej inte, ja, på det stora hela så har det väl inte det, men sen så i vissa delar får man väl ändå säga att det har det därför att vi har ju liksom ett fysiskt skydd i de lokaler där vi har våra kontor för att mycket av den informationen finns fysiskt på papper så att säga. Och då är vi ju trygga med att har vi den innanför skalskyddet så är det ju bra. Men jag vet ju att det har hänt vid vissa tillfällen att personer har behövt den här fysiska information i sitt dagliga arbete under vissa tillfällen och då blir det ju lite problematiskt för vi har ju inte samma fysiska skydd i hemmet som vi har på kontoret. Så då har vi ju liksom fått göra vissa bedömningar huruvida man kan låna hem det här materialet och hur man ska hantera det då för att man ska kan känna sig säker så att säga att det sköts på ett bra sätt. Så det är väl egentligen den som jag ser det, egentligen den mest påtagliga stora förändringen i vårt arbetssätt.

17. JA: Ja, men de bedömningar som görs då

18. I1: Ja

19. JA: De har liksom skett på, on the spot nu lite, det finns ingen satt policy än?

20. I1: Nej, det finns, nej det kan man säga att det har skett liksom, chefens vetskap, sen så har man tagit kontakt med mig. Så har vi gjort en bedömning utifrån det.

21. JA: Mm ja, vad bra. I vilken mån ser ni till att era policys efterföljs?

22. I1: Ja, det skulle jag väl säga att på det sätt vi följer upp det är väl egentligen i samband med, skulle jag säga, internrevisioner då. Man genomför en internrevison på ledningssystemet och hur man jobbar i ledningssystemet. Det är väl, liksom, det strukturerade sättet vi gör för att följa upp att det fungerar.

23. JA: Ja

24. I1: Sen är det väl lite upp till varje chef också. Alltså ytterst så, jag skulle säga på O1, och så är det ju på många arbetsplatser men, det vilar ju ett stort ansvar hos den enskilda medarbetaren att man följer de regler som gäller. Sen är det ju ett ansvar för chefen att liksom också på något vis ha ett litet, ja ha lite kontroll över hur pass medvetna är mina medarbetare och så vidare och att det fungerar inom gruppen och så.

25. JA: Ja, vad bra. Tror du att det är skillnad på om policyn efterföljs vid distansarbete jämfört med kontorsarbete?

26. I1: Njää, jag skulle nog ändå säga, det låter kanske lite förmätet då, men jag skulle säga att man har en hög ansvarskänsla, och jag märker det. Anledningen till att jag kan säga det är att jag märker för jag får samtal både från enskilda medarbetare men även från chefer där man undrar just liksom, ja som det här exemplet jag tog upp då, det har hänt några gånger att man velat ta hem pärmar med material och så vidare och jag bedömer det lite som att, ja, jag hade nog inte fått de frågorna om man inte efterlevde så att säga policys och instruktioner. Så jag vill nog sticka ut hakan lite och säga att den, liksom, ansvarskänslan för att följa det är hög, den är på den övre skalan skulle jag säga då, utan att veta då, utan att veta liksom ingen exakt sådär. Men det är min känsla åtminstone.

27. JA: Vad bra.

28. AB: Så alla tar verkligen säkerhet på stort, ansvar eller allvar, och tycker det är viktigt?

29. I1: Ja, men jag tycker det! Vi har till och med ordet säkerhet i vårt företagsnamn så att det är lite sådär att, vad ska man säga, ja det tillhör liksom, det blir en dygd på något sätt. Jag vet inte hur jag ska uttrycka det. Men det är en viktigt del. Sen är det många som jobbar på O1, har ju jobbat inom branschen väldigt länge, det är ju bara att titta på ****, alltså många har liksom, jag höll på att säga, har det sen bröstmjölken då, säkerheten, det är en ledstjärna, sen så gäller det inom alla områden i princip.

30. AB: Mm, okej

31. I1: Så att, jag tycker den är, medvetenheten är ganska hög faktiskt.

32. JA: Och gällande utbildning, i vilken mån utbildar ni era anställda om informationssäkerhet och de riktlinjer ni har?

33. I1: Ja det har vi, det var faktiskt bland det första jag tog fram där, en utbildning för, den heter just: ökad säkerhetsmedvetenhet inom O1, och den bygger på olika moduler. Det är allt ifrån fysskydd , infosäk, brandskydd och så vidare och det är en kravutbildning, eller det har varit en kravutbildning då och det är en sån här e-modulsutbildning då, där varje block då, om vi säger infosäk är ett block, tar kanske 15 minuter att genomföra, med flervalsfrågor och så vidare. Det är en kravkurs, det vill säga när du börjar på O1 så måste du genomföra den innan du får ditt passerkort och sen återkommer den, tanken är att den ska återkomma vart tredje år, det är faktiskt ett sånt år i år så jag håller just i detta nu, det låter ju lite ologiskt, men just nu så i dessa tider håller jag på att titta igenom faktainnehållet för att vi ska uppdatera kursen. Och sen så ska vi rulla ut den nu i september under hösten.

34. JA: Mm, okej

35. I1: Och så får man 3 månader på sig att genomföra och då följer vi ju upp att alla har gjort den då. Så det är så vi gör på företaget. Sen så ingår ju O1 i ****koncernen och **** har ju också krav då och då kommer det ifrån koncernnivån så det kan hända ibland att det kommer då, men det är lite mer såhär, randomized, att nu kör man en kampanj då om infosäk till exempel eller om det är GDPR eller vad det kan vara och så rullar man ut det brett över koncernen och då får man genomföra de kurserna också. Men det är väl så vi har lagt nivån när det gäller utbildning.

36. JA: Ja, där svarade du på nästa fråga om kontinuerlig utbildning också, så då kan vi hoppa över den.

37. I1: Ja

38. JA: Har de anställda fått någon specifik utbildning om just distansarbete och informationssäkerhet?

39. I1: Nä, det har de inte. Ingen specifik utbildning. Däremot så har väl jag på förekommen anledning känt att det är viktigt, alltså i samband med pandemin så var det en allmän, alltså i nyhetsflödet i den stora världen, så var det allmänt känt att många försökte liksom utnyttja situationen då. Och, så att just då i samband med det gick vi ut och skrev, eller jag skrev just om de här bitarna att var nu observant på liksom olika typer av mail man får och olika sådana här försök, scamförsök. Som är populärt då. Och sen så även då tryckte just på det här att glöm inte hanteringsreglerna för information och allt vad som innebär med det och titta gärna igenom instruktionen och så vidare. För vi har ju sådana här veckoutskick då, de kopplar egentligen mer till pandemin, alltså här är läget inom företaget och så vidare och i det sammanhanget, det skriver vi på vår interna intranätsida då och i de sammanhangen så har jag tryckt lite på just det här med infosäkerhet att det är extra, så att säga, viktigt, det är alltid viktigt, men nu är det liksom extra viktigt nu

när ni sitter hemifrån och jobbar för det är inte riktigt samma, till exempel samma fysskydd som det är på arbetsplatsen och så vidare.

40. JA: Nä, precis.

41. I1: Nä, men någon specifik utbildning så, det har vi inte haft för just distansarbete.

42. JA: Nä, men det är bra. Ja men det är precis så som du säger, eller mycket av teorin säger ju att företagskultur och säkerhetskultur är ju en stor del i att liksom förebygga. Lite av de aspekterna försvinner ju vid distansarbete kan man tänka sig.

43. I1: Jo, men precis.

44. JA: Ja, och då går vi vidare. Hur skulle du säga att ledningens förhållande till informationssäkerhet är?

45. I1: Ja, den är väl också, väl men, den är god. Precis som den är på medarbetarnivå. Det jag kan däremot ändå lite så där, nu när du tar upp det, sakna så, det är väl kanske, höll på att säga intresset, men känslan för att det här med att, man ser, om jag ska göra en lång historia kort så, informationssäkerhet, frågar du vilken chef, eller vilken person som helst i ledningen så kommer de väl kanske nämna mitt namn då. Men jag menar, jag är inte ansvarig för all information på O1.

46. JA: Nej

47. I1: Men jag kan känna att, hur ska jag säga, att kunskap eller medvetenhetsnivån inom ledningen kanske inte alltid är så där jätteutvecklad just kring det här med ägarskapet kring informationen. Många gånger är ju chefer ägare utav en hel del information som de knappt är medvetna om. Det kan jag väl känna att vi har en del att göra inom företaget att höja graden av ansvarskänsla hos, till att börja med, chefskollektivet då, och det är inte alltid det bara är chefer som äger information men att de liksom är medvetna om att det finns ju ett ansvar kopplat till att man äger information och det börjar med att man är medveten om att man äger informationen. Men många tror jag, eller får jag känslan av många gånger när vi diskuterar, till exempel när vi diskuterar olika applikationer och system som innehåller mycket information, och då tycker cheferna att det berör inte mig så mycket, ja men du äger ju stora delar av innehållet i den här databasen eller vad det nu är. Ja, det har de knappt reflekterat över.

48. JA: Nej

49. I1: Så där skulle jag nog säga, att det är väl egentligen där man skulle behöva sätta in mest, fokus och arbetsinsats att liksom höja den medvetenhetsnivån för ägarskapet.

50. JA: Ja precis, ja.

51. AB: Är det något speciellt du tror man hade kunnat göra för att öka medvetenheten hos ledningen?

52. I1: Ja det tror jag, inom **** har vi fått en, vi har fått tillgång till ett system där man klassar, eller en applikation, som heter iFacts, ni känner kanske till just det namnet eller applikationen, men där klassar man olika system inom företaget som innehåller information och där ska man klassa systemen utifrån den informationen den innehåller. Och där ser jag väl en möjlighet att man engagerar cheferna i det arbetet med att de får vara med och klassa den här informationen för att de som äger informationen är ju också de mest lämpade till att klassa informationen.

53. AB: Ja

54. I1: Så där hade jag, det är väl en sån aktivitet där jag ser att man skulle kunna höja engagemanget hos chefskollektivet då.

55. AB: Ja okej

56. JA: Mm. Har ledningen, har ledningen aktivt förmedlat om informationssäkerhet vid distansarbete. Eller har de lämpat över det på dig?

57. I1: Ja det får jag nog säga, haha, de lät drastiskt som du uttryckte dig där.

58. JA: Haha, ja.

59. I1: Ja men det får jag nog säga att det är väl jag som står för det. Det blir lite så tror jag på ett företag i den storleksordningen som vårt är så tycker man att vi har en som ansvarar för det här så ser man då liksom mig som, jag som är fanbärare inom informationssäkerhet och då blir det gärna att man tittar på mig liksom det har du väl tagit hand om, sådär lite va, och så skulle jag nog säga att det är i det här fallet. Det är ingen annan som går och bekymrar sig över informationssäkerhet eller ligger sömnlös på nätterna, utan det tycker man, men ja det fixar I1 så.

60. JA: Ja, det var kanske lite drastiskt uttryckt.

61. I1: Haha, ja men det stämde ganska väl tyckte jag, men det är min uppfattning iallafall.

62. AB: Så det finns liksom ingen tydlig roll för vem det är, utan det är lite mer förutsatt att det är du som tar ansvar för det?

63. I1: Ja, sen är det ju också, sen får jag ju säga också att både chefskollektivet och medarbetarna, som jag sa tidigare, de har en hög så att säga ansvarskänsla och en hög säkerhetsmedvetenhet, så det är ingen jättestor sådär fråga och jag tycker som sagt att man tar ansvar för jag får frågor ibland, som jag känner att, ja den där frågan uppstår på grund av att man känner ett ansvar för att man vill göra rätt.

64. AB, JA: Mm

65. I1: Och då pratar jag både om chefer och medarbetare så att, ja.

66. JA: På tal om medvetenhet. Har du, skulle du säga att du har sett någon förändring kring attityd och medvetenhet vid distansarbete gentemot innan?

67. I1: Nej, och då menar du medvetenhet kopplat till informationssäkerhet?

68. JA: Ja, precis.

69. I1: Nej, jag har inte märkt av någon större skillnad så, det kan jag inte påstå faktiskt.

70. JA: Nej, okej

71. I1: Utan den är, jag upplever det som att nu har vi jobbat såhär i över 1 år. Men jag tycker det känns som det gjorde innan vi hamnade i den här situationen faktiskt.

72. AB: Ja, okej

73. JA: Nej, men det är jättebra. Mm, då är det nog bara några slutfrågor här.

74. I1: Ja

75. JA: Då ska vi se, ja, jo men studier visar ju också på att distansarbete är här för att stanna. Kanske inte på er organisation, men generellt.

76. I1: Ja, jo

77. JA: Finns det några andra långsiktiga utmaningar kring informationssäkerhet som du kan tänka detta medför?

78. I1: Ja, men då är det vissa bitar just kring som jag nämnde tidigare det här med att vissa roller behöver ha fysisk tillgång till en viss typ av information. Där måste man då se på hur man ska hantera det. Och, nej annars så ser jag väl inga större konstigheter annat än att man måste hela tiden vidmakthålla denna höga kunskapsnivån kring hur man hanterar information, det är liksom lika viktigt hemma som på kontoret och så att det är väl just den här fysiska delen.

79. JA: Den fysiska biten och sen att ha en fortsatt hög medvetenhet och kultur liksom.

80. I1: Ja. Sen är det ju, det är faktiskt en annan grej som slog mig nu, det är just det vi pysslar med nu när vi sitter på Teams då. För då är vi ju liksom ute i den stora i liksom molnvärlden och så och där kan jag ju se kanske att verken, kärnkraftverken har inte bestämt fullt ut ännu vad de kommer tillåta, vad vill säga, vad som får visas över Teams för det finns ju ett tryck då på att man vill utföra utbildning över Teams och det är ju jättebra och det finns ju alla möjligheter då att dela in i olika klassrum och man samlas i olika rum och återsamlas och så vidare, så det finns ju hur mycket finesser med det som helst men samtidigt så är det som sagt säkerhetsklassad information en hel del av det vi hanterar och då kan man inte bara skicka upp det i molnet hur som helst då. Nu är inte jag någon IT-expert så, men där finns ju liksom begränsningar där som man måste kunna hantera helt tekniskt då.

81. JA: Ja

82. I1: Det är ju också en sån aspekt på det hela. Men samtidigt är den ju aktuell om du sitter på kontoret, om du nyttjar Teams via kontoret eller hemma, det spelar ingen roll, du är lika mycket i molnet ändå så att säga.

83. JA: Ja... Nej men den tekniska biten är ju också en utmaning.

84. I1: Ja absolut, absolut är den det.

85. JA: Sista frågan då. Finns det några andra utmaningar för er organisation, förutom de vi tagit upp, som du kan komma på när det gäller informationssäkerhet?

86. I1: Ja, ja men det är väl lite, att det inte blir en slentrian eller hur jag ska uttrycka mig utan att man liksom, är medveten om det, alltså man är medvetet medveten om det så att säga. Vi jobbar ju väldigt mycket med, alltså mycket utav vårt utbildningsmaterial, jag skulle säga 80-90% av utbildningsmaterialet är ju säkerhetsklassat så det är rätt så mycket begränsningar runt omkring det, vad du får göra, och hur du får hantera det och så vidare. Och det är lite på något vis, det är ju ganska enkelt så länge man hanterar det på kontoret och så vidare då. Men det är klart att då blir det att det sker lite på automatik. Men sitter man då mycket på distans så gäller det liksom att hela tiden ha den där medvetenheten då så det inte blir att man slentrianmässigt och så glömmer man bort och sådär… Det kanske som jag ser är en utmaning, just det här när man hela tiden växlar mellan att jobba hemma och jobba på kontoret, i större utsträckning.

87. JA: Ja

88. I1: Att man behåller skärpan hela tiden så att säga.

89. JA: Ja precis. För vi har ju hittat lite studier som då visar på att det är lätt att tappa rutiner när man arbetar på distans.

90. I1: Ja, ja men precis. Så det är det då kanske som jag skulle att man kan göra då därför man är van och så att jobba så på kontoret men just när man sitter på distans så, ja. Men än så länge har jag som sagt inte märkt av det som jag sa tidigare, utan jag tycker det har fungerat väldigt väl så här långt, men sen vet inte jag allt, jag menar jag sitter ju i min lilla lya.

91. JA: Ja, men det har det säkert gjort.

92. I1: Ja, ja

93. JA: Ja, men då var vi nog klara.

94. I1: Ja okej. men vad härligt

8.3 Intervju med Organisation 2

(xx) = Svårt att urskilja exakt vad som sägs i inspelningen.
(osäkert ord?) = Något osäker på exakt vilket ord som sägs men har skrivit ut vad vi tycks höra.
**** = Anonymisering av namn eller andra identifierande ord.
… = Längre paus.

Intervjuare 1 (RH) – Rasmus Holmqvist (intervjuledare)
Intervjuare 2 (AB) – Andreas Berg
Intervjuare 3 (JA) – Jakob Andersson
Informant 2 (I2) – Chief Security Officer på Organisation 2 (O2).

1. RH: Lite först om företaget du jobbar på och din position, först kanske en liten beskrivning av vad ert företag gör?

2. I2: Ja alltså, O2, vi är ju digitaliseringskonsulter, alltså managementkonstulter med stort fokus på digitalisering och att hjälpa våra kunder att anamma digitalisering i allt dem gör. För att vi stöttar med framför allt utveckling med projektledning, change management, de bitarna. Vi har ett stort fokus också på just liksom cybersecurity och secure consulting och hur vi kan göra det. Så det är vad vi gör. Vi finns i Sverige på flera orter, i Finland, Danmark och Polen och är väl strax under 1300.

3. RH: Okej. Och din roll mer specifikt, eller ditt verksamhetsområde där?

4. I2: Ja, jag sitter som CSO det vill säga Chief Security Officer och där har vi bakat ihop, alltså, all den koordinerade, allt säkerhetsarbete där pratar vi liksom IT-säkerhet ner till vilken brandvägg har vi, vad har vi liksom, hur tänker vi liksom rent (xx) med brandvägg, informationssäkerhet, hur jobbar vi med säkerhet, hur klassificerar vi dokument, hur ser vi till att vi har rätt status på grejerna. Även fysisk säkerhet på våra kontor, vad har vi för försvarssystem, hur följer vi upp det, larm allt sånt. Sen gör vi också en hel del arbete där vi har konsulter som är placerade i säkerhetsklass, det vill säga där kunden är en för riket central verksamhet, ehm där min roll är att säkerställa, där vi gör liksom utöver en kompetensprövning även gör en lämplighetsprövning av konsulten. Är du lämplig? Förstår du nu att du inte är lojal mot oss utan mot konungariket. Det är liksom dom fyra benen som är min roll. Sen har vi på alla våra siter, eller orter, lokala ansvariga som liksom då ska få ut det här budskapet och hålla någon typ av lokalt fokus, men allting här ligger liksom i mitt knä eller hur man ska säga.

5. JA: Arbetar du bara internt då så att säga? Eller är du också ute som konsult?

6. I2: Nej jag är inte ute som konsult, utan jag är 100% intern. Sen är jag ibland exponerad mot kundleveranser, framför allt i försäljningsarbeten, framför allt där kunden vill veta hur vi jobbar själva med säkerhet. Vi har... vår finska gren, i Finland, som gör mycket av vår egna IT-drift är ISO-27001 certifierade medans vi i Sverige inte är det, så där har vi en mer pedagogisk roll att förklara att jo men vi är faktiskt lika bra men får förklara mer än när de har stämpeln i boken. Så där är jag mer, men det är ju inte som konsult, utan mer som de faktum att svara upp för hur vi sköter oss.

7. RH: Okej. Hur länge har du arbetat med informationssäkerhet och liknande frågor?

8. I2: Jag har en bakgrund i finans, IT-branschen de senaste 10 åren i olika bolag. Så att jag har alltid jobbat regelstyrt, med externa regelverk, lagkrav och alltid i branscher där man ... Alltså i min värld så är, alltså, säkerhet har alltid. Mitt bekymmer är snarare att jag är för paranoid än mina kollegor, alltså jag har inga bekymmer med att saker inte går att använda. Ett säkert system är ett avstängt system liksom. Det är min bakgrund... man är van… Det ska inte vara enkelt. Ju enklare det är för mig, desto enklare är det för er och det ska inte vara enkelt.

9. RH: Nej, jag förstår. När det kommer till distansarbete, i vilken utsträckning arbetar ni på distans?

10. I2: Vi kan säga så här. De av oss som har då interna funktioner, vi jobbar väl ja sen 1.5 år tillbaka 100% hemma.

11. RH: Okej

12. I2: Våra konsulter jobbar där våra kunder vill att dom ska vara. Majoriteten där är ju också hemma, men som sagt dom som sitter på uppdrag som är säkerhetsklassade i någon mening, eller ja i någon formell mening på den här säkerhetklassningsskalan som SÄPO har så sitter man i en av kunden anvisad lokal som bedöms vara säker.

13. RH: Okej

14. I2: Så att där styrs vi av, alltså, våra konsulter... alltså det där är ett kommersiellt krav. Sen så vill vi ju givetvis att vår personal ska undvika att, vi följer alla rekommendationer och riktlinjer, men ytterst så är det en kommersiell fråga och vi ser en stor lättnad i många restriktioner som vi har haft på oss så ser vi ju att den har (blivit?) flexibla också för hemjobb liksom.

15. RH: Ja. Har det varit en stor ökning av distansarbete så att säga från före pandemin till dagsläget?

16. I2: Oh ja, vi har ju alltså en ambition om att, före pandemin var våra kontor fullbelagda, då var kontoren byggda för att vi skulle sitta där tillsammans och samarbeta och ha det bra och mysigt och dricka kaffe. Nu är det väldigt tomma ytor som vi inte använder. Vi håller på att växla tillbaka i någon mening med liksom platsbokningssystem för att inte fylla upp för mycket och så där. Men vi ser ju definitivt att ingen kommer gå tillbaks till att jobba 100% på kontoret.

17. AB: Okej

18. RH: Okej. Om vi går vidare till policies. I den mån du har möjlighet att svara, lite övergripande hur ert arbete kring säkerhetspolicies och riktlinjer ser ut?

19. I2: Alltså vi har ju... alltså komprimerat som jag sa, vi i Sverige (xx) utom i Finland är inte certifierade enligt ISO-27001 vi jobbar enligt regelverket, eller vad heter det, standarden. Vi har alltid haft ett stort fokus på säkerhet. Alltså våra kontor har, vi har alltid haft clean desk, du har inget eget skrivbord, det är aktivitetsbaserat så du rensar skrivbordet när du går på lunch, du lämnar inte kvar någonting framme, någonsin. Vilket är jobbigt, men också bidragande till att det inte byggs hemliga pappershögar som man behöver gå och fundera på. Så där har vi alltid jobbat ganska effektivt. Med distansarbetet trädde in helt andra aspekter det vill säga... alla våra laptops, alltså den...

IT-mässigt så har vi nog ingen skillnad alls. För alla laptops är fortfarande krypterade, alla mobiltelefoner är fortfarande centralt managerade, vi kan wipea allt när det behövs. Bekymret är ju att vi inte kan göra någon audit hemma hos dig. Har du lagt några papper på skrivbordet? Det vet ju inte jag.

20. RH: Nä, just det.

21. I2: Så det har vi bara tagit upp liksom, vi har gjort förtydliganden både i våra guidelines och riktlinjer då. Vi jobbar enligt en klassisk styrdokumentstrappa med övergripande policys som är oförändrade, vi ska jobba säkert typ, men i våra riktlinjer har vi mer tagit höjd för ja men hemjobb. Tänk på vilka som är hemma, har du städhjälp? Tänk på att det är en person som är i ditt hem. Har du liksom, sitter dina barn och spelar spel på samma nätverk? Beroende på vad gör, kan vi segmentera ditt hemnätverk?

22. RH: Mm, okej.

23. I2: Där försöker vi också tvinga in så många som möjligt att vi har ju en splittad miljö där en del av våra grejer, alltså våra interna tjänster och system som vi använder står on prem hos oss och vissa grejer kör vi liksom moln. Vi kör liksom exempelvis kör vi Teams, vi kör Office 365 så att det är ingen som (xx) vårt syfte. Men allting som kräver, allting för att komma åt vårt system krävs vpn och där tvingar vi i princip in nu alla anställda ska vara online på vpn oavsett om det behövs eller inte. Just för att ja men du kanske inte har världens ballaste brandvägg hemma liksom. Utan då styr vi all trafik vi kan in i vår brandvägg och så försöker vi hantera så mycket vi kan där, för det är vad vi kan göra. Om man tittar ute i branchsen så är det liksom, hotbilden mot företag är ju 99% phishing och sen är det en liten skön ransomware grej, allting kokar ju ner till, det är precis som ni säger… Ingen fokuserar på IT-stöd, alltså IT-stöd gör vad dom kan, men så länge någon tycker att ”ah det här verkar vara en skön länk” då spelar det liksom ingen roll vad som... vad du har för järn liksom.

24. RH: Där gick du in lite också på vår nästa fråga där, om ert arbetssätt kring säkerhetspolicys har förändrats vid mer distansarbete, men som vi förstår det då är det svårkontrollerade miljön den så att säga fysiska hemmamiljön?

25. I2: Den är ju ny i någon mening, tidigare när man har jobbat hemma då har man tagit hem laptopen när man har gjort klart någonting typ om man ska hårddra det, men nu när man har ett byggt hemmakontor då ja men då vet vi ju att då lägger man pappret framme, inte fan går jag och städar undan alla mina papper bara för att klockan är 5 liksom. Utan har jag ett kontor hemma, jag gör det för jag jobbar i köket så då rensar jag haha, men bor man större så är det klart som fan att man har ett kontor och då ligger pappret framme. Och kommer dom, det vi säger, det här är ju också en kulturkrock beroende på vart ifrån man kommer... Har man det naturligt i sig att man faktiskt ska misstro alla, alla är fiender men då är det inte så konstigt att man låser datorn när man går på muggen, att man låser dörren när man går ut med soporna. Men om man inte har det till vardags, då är det klart som fan att man litar på människan som kommer hem och städar. Så att det handlar om, vi jobbar mycket med utbildning och awareness training för att få människor, eller våra kollegor, att förstå att det är faktiskt människor du inte känner och det betyder inte per definition inte att dom är onda men det betyder att du inte känner dom. Om man tittar på social engineering så är det ganska enkelt att kartlägga, tittar ni på min linkedIn kan ni jaga vem som är

mina närmsta kollegor och då är det ganska enkelt att göra en riktad attack. Så att lyfta just att du är inte på kontoret utan du är själv nu och då måste du själv göra dom här åtgärderna som man automatiskt gör på kontoret.

26. AB: Har ni haft sådan utbildning innan också, fysiskt när ni var på plats, eller har det kommit mer nu?

27. I2: Alltså vi har ju i vårt löpande säkerhetsarbete så har vi ju löpande årligen uppdateringar, nyanställda gör utbildningar och varje år ska man genomgå en uppdaterad version så att man håller sig ajour med vad vi ser som dom största hoten och dom senaste åren, ja det har ju varit, ja men det är ju phishing liksom.

28. RH: Ja precis. Har ni utfört någon extra eller specialiserad utbildning nu på grund av situationen med så mycket distansarbete?

29. I2: Vi hade ju förmånen, nu har vi den pågående, kan jag bara berätta då, den årliga utbildningen inföll här för någon månad sen så den var ju ganska riktad mot det.

30. RH: Aha okej.

31. I2: Men vi har liksom inte gjort något extra mer, vi trycker ju ut nya liksom push notiser på intranätet och så vidare där vi upplyser om tänk på det här. Nu har det ju gått så pass långt också att nu är ju dom flesta vana vid situationen liksom, nu handlar det mer om att vänja sig tillbaka till att komma tillbaka till kontoret.

32. RH: Just det. Har ni någon statistik eller har ni någon koll på, alltså hur väl policies efterföljs vid distansarbete. Om det är någon skillnad på hur folk, hur duktiga folk är på att skydda informationen?

33. I2: Nej, det kan vi ju inte göra. Utan vi gör vad vi kan. Vi kan, vi ser vilka som är online på VPN och hur dom bitarna efterlevs, men nej som sagt vi kan ju inte göra några hembesök och tittar efter om dom har låst in papperna.

34. RH: Har ni upplevt någon ökad mängd phisingförsök eller att saker har hänt osv?

35. I2: Nej phishing ligger som ett konstant, som ett konstant liksom flow. Det tar aldrig slut, det spelar ingen roll om du jobbar hemma eller på kontoret. Framför allt inte eftersom vi kör Office 365 så är vi ju...mainservern står där den står, där får vi ju så mycket hjälp som vi kan liksom av våra premium office licenser så att dom tar ju, ja jag vet inte hur mycket dom tar, men dom tar säkert 99 komma nånting % men det slinker ju alltid igenom nånting liksom. Med Ai och alla Machine learning kan man ju själv bygga sig själv en sån snurra på en eftermiddag liksom.

36. AB: Okej. Hur skulle du säga att personalens attityd och medvetenhet gentemot informationssäkerhet är?

37. I2: Det går inte att säga, vi är ju 1300. Den är såhär (gestikulerar stor bredd med händerna).

38. AB: Ja, okej

39. I2: Den blir väl bättre. Det beror ju klart på. Man kan väl vara åldersrasist också, men givetvis i och med att vi satsar mycket på secure, där har vi visst... ja men där är det ju dom som faktiskt själva kommer på att får jag ett mail om en inbjudan till en konferens från ett företag som jag inte har bett om, givetvis är den farligaste länken i det mailet unsubscribe. Medans andra tycker att det är jättebra att man kan trycka på unsubscribe. Det är den nivån som vi jobbar med liksom. Dom allra flesta har bra koll, en del tycker att det är märkligt när man får ett riktat mail från VDn som ber om pengar, men... det är ju mer så att det rapporteras. Jag vill ju att vi ska sluta rapportera dom, att vi ska acceptera att det kommer att hända, vi blockar nästan allt, det som inte blockas, tryck på delete själv liksom, du behöver inte göra ett supportcase av det liksom. Så med det skulle jag säga att vi har en ganska god säkerhetsmognad, men inom den är det fortfarande ganska spritt liksom.

40. RH: Har ni märkt att det har varit ökat antalet lyckade försök eller att ni har stött på mer problem så att säga?

41. I2: Nej, jag har inte haft några incidenter som går att härleda till hemjobb utan, i regel så är det ju inte hemjobbet som är liksom, utan det handlar ju om att komma åt någonting annat.

42. JA: Ja, vi har ju läst ganska mycket om att säkerhetskultur och företagskulturen spelar en stor roll för säkerhetsattityden med människor runt omkring en, att anställda påverkas av beteendet av dom runt omkring en och då kan man ju tänka att många aspekter av det försvinner vid distansarbete.

43. I2: Jo det som man märker nu, dom få gångerna som man är inne på kontoret, jag är inne på kontoret en gång i veckan ungefär, det är att man har jättemånga nya kollegor som man aldrig har träffat och man märker ju då sitter man själv så kontoret ja men då kanske man slarvar med att ha på sig sitt nyckelband liksom. Det har vi också krav på i våra policys, den ska vara på, jag ska kunna se på dig utan att fråga om du ska vara här eller inte. Det märker man också den tappar man ju också när man bara sitter fem pers där, och varför ska jag ha på mig den liksom? Ja men det är ju för att den ska vara på liksom. Det är ju dom aspekterna som är dom läskiga. Jag menar, hur många gånger, jag har en gång i mitt liv blivit nekad av en person att gå in bakom en person i en låst dörr. Säger man bara tack och ursäkta jag har glömt min nyckel så är det bara javisst kom in. En person har sagt nej. Jag blev så jävla arg samtidigt som jag bara fan, du gjorde helt rätt men helvete haha.

44. JA: Haha ja det är ju helt logiskt egentligen. Om vi går vidare, hur skulle du säga att ledningens förhållande till arbetet med informationssäkerhet är?

45. I2: I och med att vi har så många kunder som sitter då med säkerhetsklassning så är vi väl införstådda med att det är jätteviktigt. Så vi har inga tractionproblem i ledningen med att få gehör för våra policys, utan vi har en god förståelse och vi jobbar väldigt synkroniserat i alla våra länder. Sen är det ju alltid en avvägning liksom, kommersiellt, vad som är rimligt och vad som är praktiskt. Men det, är inga bekymmer att... typ som än så länge är det försvarbart ekonomiskt att inte vara ISO 27000 certifierade 100% hela koncernen, snart kommer det nog inte vara det för att vi ser en ganska stor ökning av, alltså det går ganska bra för oss. Så att, då kostar det mer att sälja när man måste förklara än när man kan visa upp en stämpel i boken. Så att det är väl dom aspekterna mer än att någon ska tycka att det vi gör är onödigt.

46. JA: Har ledningen aktivt förmedlat om informationssäkerhet vid övergången till distansarbete, har de engagerat sig?

47. I2: Alltså, jag är väl ledningen i någon mening. Separerad från VD:n med ett steg eller två, så det har ledningen gjort. Det är ju så vi gör när vi jobbar rent operativt, med liksom förändringar som görs liksom längre ner i organisationen så lyfter jag upp det och kommunicerar ut det med min stämpel så att det här är liksom ingenting som kommer från någon drifts-Kalle nere i hörnet utan det här är faktiskt ett centralt direktiv så det gäller liksom.

48. JA: Ja, men jättebra, då är vi snart klara, en fråga kvar. Är det några utmaningar vi har missat som har varit svårt vid distansarbete när det gäller informationssäkerhet?

49. I2: Då är det det som jag nämnde i början, det är just det här med vad som händer hemma. Alltså, man behöver ha en förståelse, beroende på vad man gör givetvis. Men jobbar man mycket med papper, det beror väl på vad man gör. Men alltså i min roll med säkerhetsklassificering och den typen av uppdrag så har jag mycket papper. Och jag försöker undvika att ta hem dom för att mitt hem inte är säkerhetsklassat av SÄPO, och det vill jag inte heller. Det är ju där utmaningen blir. Hur man jobbar, man tar anteckningar. Också dom här, det beror på vilken nivå man lägger sig på. Har du en printer hemma också har du en lite ball printer som du sätter på nätet. Läser man om hur attacker går till så är det liksom via den utrustningen man tar sig in, det är termostaten, det är dina smarta lampor. Ni har säkert läst det här också, hur lätt det är att hacka en IKEA lampa och så tar man sig in i nätverket. Ofta är det ju där hemma, ofta finns det ju någonting coolare att komma åt än den här lampan liksom för det är bara kul att blinka så länge.

50. JA: Ja vi har ju försökt avgränsa oss mycket eftersom informationssäkerhet är ett så stort ämne, men vi har ju läst om Internet of Things och riskerna där.

51. I2: Ja och det är ju bara att titta på, det är ju så det händer liksom. Ju enklare det är, det här kasinot i Las Vegas som är ett klassiskt exempel som blev hackade via termostaterna liksom. En nest-termostat som var lite skönt att man skulle slippa att gå och vrida manuellt, men dom kom ju åt hela skiten sen. Och det är ju, beroende på hur du bygger hemma, är du teknikintresserad, men bara av tekniken och inte risken av tekniken då har du byggt en ganska fin verkstad för en angripare. Så det är väl där liksom, man behöver fokusera lite grann på hemmamiljön beroende på vem det är liksom... som jag tycker är viktigt att komma ihåg. Sen kommer man ju också in på det här med att man är hemma, med kan jag använda min egen dator. Allt det här liksom, Bring your own device tänket, som blir mer aktuellt om man kanske har en fetare hoj hemma liksom, om man sitter och utvecklar och man inte vill, det går ju snabbare att kompilera eller whatever.

52. JA: Ja det är också en sak som vi var inne på ett tag men som vi valde att avgränsa, det här med reverse Bring your own device. Vi hittade till och med några studier som visade på att anställda vid distansarbete har enklare för att vidarebefordra känsligt material till sina privata enheter och så vidare.

53. I2: Ja jag skulle säga att det viktigaste alltid är personalen och medarbetare att man måste ha en naturlig inställning att, ja men vi ska vara lite försiktiga, vi ska inte liksom lita på saker bara för att någon säger det, det är där vi hamnar.

54. AB: Skulle du säga att det finns några andra långsiktiga utmaningar med informationssäkerhet vid distansarbete?

55. I2: Informationssäkerhetsmässigt så kommer utmaningen att vara att hålla ihop en miljö liksom. Jag är för gammal inser jag, för vi har ett ganska stort (xx) internt på just Bring your own device, och jag kan ju inte för mitt liv förstå det. Jag kan ju inte förstå hur jag skulle vilja ha min egen dator alltså, och sen å andra sidan så vill jag ju inte heller för att vi har ett åtagande att skydda, är det kunduppgifter, det får du ju inte ha på din privata dator. Vad utsätter du oss för med din privata dator? Det är ju så jäkla svårt, där har vi, där är utmaningen, men den är ju inte bara hemarbete det vill ju folk ha med sig på kontoret också. Men det blir ju svårare att argumentera emot det när man sitter hemma. Också när man kör mycket cloud, vi kör jättemycket cloud, vi är jätte cloud-vänliga liksom, då spelar det ingen roll. Så att vår avgränsning där är ju att, så mycket du vill på din egen dator det som du når utan vpn, men aldrig kunduppgifter liksom. Men compliance är ju svårt att mäta hemma liksom, vi lever fortfarande i Sverige liksom, inte Östberlin så vi kommer inte att göra hembesök.

56. JA: Nej precis. Nej det är en utmaning. Men då tror jag vi var klara där.

8.4 Intervju med Organisation 3

(xx) = Svårt att urskilja exakt vad som sägs i inspelningen.
(osäkert ord?) = Något osäker på exakt vilket ord som sägs men har skrivit ut vad vi tycks höra.
**** = Anonymisering av namn eller andra identifierande ord.
… = Längre paus.

Intervjuare 1 (JA) – Jakob Andersson (intervjuledare)
Intervjuare 2 (AB) – Andreas Berg
Intervjuare 3 (RH) – Rasmus Holmqvist
Informant 3 (I3) – IT-chef på Organisation 3 (O3)

1. Vilken är din roll inom företaget och vilka områden är du verksam inom?

2. I3: Ja jag är IT-chef så jag är egentligen ansvarig för hela IT-leveransen. Inklusive säkerhet och inklusive allting.

3. AB: Och hur lång erfarenhet har du inom informationssäkerhet?

4. I3: Jag har väl… Jag har egentligen en bakgrund inom, en utbildning inom informationssäkerhet, men jag har inte praktiserat det liksom ordentlighet, eller jag har inte praktiserat det djupt utan på företaget jag jobbar på nu där är jag IT-chef så har jag liksom de kunskarperna för att applicera en bred säkerhetstänk på företaget men vi har inte någon specifik IT-säkerhetsansvarig i och med att vi är så pass små och har växt på (på det sättet?).

5. AB: Mm och nu med pandemin, i vilken utsträckning och hur länge har ni arbetat på distans?

6. I3: Ja, precis. Men det här försöker jag alltid komma ihåg, när det kom till Sverige, då gick vi hem allihopa. Jag tror det var slutet av Mars, mitten av Mars, då all började gå hem, då gick vi hem också.

7. AB: Okej, så det var 100% distans då för alla?

8. I3: Nej, det har varit, alla som kan gå hem gick hem och jobbade hemifrån. De som… I och med att vi är ett tillverkningsföretag så har vi liksom laboratorium i lokalerna där folk behöver vara. Så vi har dels produktion, (kvalitetskontroll?) och logistik som alla egentligen behöver vara på plats.

9. AB: Ja, okej… Och då hoppar vi

10. I3: Så de som gick hem var egentligen, det var IT som gick hem, det var försäljning det var marknadsföring, det var finans och alla de funktioner som inte behöver, inte

måste vara på plats, de gick hem. Och just exakt det var regeln också, att alla som inte måste vara där behöver vara hemma.

11. JA: Okej

12. AB: Okej, och om vi går in på policys lite. Hur ser ert arbete kring policys och riktlinjer ut?

13. I3: Hur ser vadå ut sa du?

14. AB: Hur ser arbetet med säkerhetspolicys och riktlinjer ut?

15. I3: Ja, precis. Vi är ju i en tillväxtfas för företaget så vi har egentligen gått från att vara i… från garage till industri egentligen. Vi har inte arbetat så aktivt med säkerhetspolicys förrän nyligen. Vi har kommit upp i en nivå där vi har liksom… där vi känner att de här grejerna behövs att man kan inte hålla koll på allting liksom, det är så mycket som händer så man kan inte hålla koll på allting själva så då har vi kommit till en nivå där vi verkligen behöver ha policys i säkerhetsarbetet. Vi har precis gjort en säkerhetsreview på alla våra processor med hjälp av…tror det var Nist… Nist cybersecurity framework som vi har gått genom hela vårt företag, hur mogna vi är. Och vi är ganska omogna egentligen. Så vi saknar en hel del saker inklusive liksom, vi har i och försig en uttalat IT-säkerhetspolicy som vi arbetar med, men den har vi tagit fram en gång bara för att fungera som en ISO-standarden, ISO-cerifitierng, men vi behöver se till att få upp det här på kartan och ha liksom… löpande arbete med det här. Och det har vi inte idag men det är något vi skulle behöva. Så vi liksom ligger i startgroparna för att börja arbete med det här.

16. AB: Ja okej. Har ni behövt anpassa policyn eller riktlinjerna nu inför, eller för distansarbetet?

17. I3: Nej, inte egentligen... Vi har…Det får vi se hur det, vad vi upptäcker när vi arbetar ännu djupare med det här. Men vår approach till det här har ju egentligen sen många år tillbaka har vår approach varit remote first. Inte nödvändigtvis för att det skulle komma en pandemi men för att, ja vara moderna helt enkelt och kunna erbjuda folk att arbeta på den annan plats. Nu har vi fortfarande så att vi har fortfarande så här… så kallade säkra nätverk on site, (xx) man får göra lite som man vill, men majoriteten av de tjänster vi kör är webanpassade liksom och körs i webben och via en browser så all säkerhet kommer därifrån.

18. JA: Mm okej. Med VPN då också? För remote.

19. I3: Ja, VPN behövs när man liksom ska nå resurser som är on site. Som filservrar för specifikt ändamål på laboratoriumet. Men annars så kör vi Microsoft 365 så vi har... vi har väl office, microsoft onlinetjänster, inklusive sharepoint och Teams, så allting ligger liksom i molnet. Sen har vi affärssystem som ligger i molnet också och så har vi lite andra system. Majoriteten av systemen ligger i molnet egentligen. Så VPN behövs

nästan aldrig om man liksom inte är en person som egentligen ska stå på labb men jobbar hemifrån den dagen.

20. AB: Okej. Har de anställda lätt tillgång till säkerhetspolicyn? Så de är medvetna om vad som står där och vad som gäller?

21. I3: Nej, det skulle jag inte säga att de har. Vi har ett kvalitetssystem som har policys och man får skriva på att man har läst de här grejerna men jag tror inte den här är tillgänglig… Den är inte med i dagligdags egentligen som den skulle behöva vara. Det finns ju många policys som kanske är mer dagligdags om hur man ska arbete när de faktiskt arbetar och det kan vara relevant de policys. Men det här tror jag är kulturellt arbete som vi behöver göra… för att få in innehållet policyn i det dagliga arbetet och inte bara ha det i en policys liggande sidan om. Även om jag liksom, jag tror att det är viktigt att ha policys skrivna för saker så är det ju så att culture eats policy for breakfast liksom haha.

22. AB: Ja det är ju klart.

23. I3: För att liksom arbete in det här i företaget och kulturen.

24. JA: Haha, ja det är intressant att du säger det för det är väl det vi spenderat de senaste dagarna att skriva om.

25. I3: Haha, ja

26. AB: Men skulle du säga att det är svårare för de anställda att följa, alltså riktlinjerna just vid distansarbete?

27. I3: Om det är svårt att följa?

28. AB: Om det blir några större problem för de anställda just vid distansarbete att följa säkerhetsriktlinjer och arbeta på det säkert sätt?

29. I3: Nej, det tror jag inte egentligen. Jag tror många av de sakerna… Vi får ju ganska mycket av de här grejerna gratis i och med att vi kör allt webbaserad. Så hela liksom, hela, alla tjänster, nästan alla tjänster är webbaserade och körs via en browser och sen har vi alla endpoints som folk tar med sig hem är liksom kontrollerade i form av microsoft intune och med… microsoft ems så det är ganska, vi har ganska bra kolla på de grejerna som åker med hem. Så det viktigast för vår personal är egentligen att inte klicka på massa dumma länkar. Och det är något vi snackar en del om, även om vi naturligtvis skulle behöva snacka ännu mer om, för det här är ju en av de största vägarna in idag.

30. AB: Ser ni till att policyn efterföljs?

31. I3: Nej, det gör vi inte. Vi har, det är väl också en grej som vi behöver få in lite i löpande arbetet att följa upp policyn. Och vi har inte heller något bra sätt att upptäcka

om man bryter mot policyn. För säg att man klickar på en länk någonstans som man inte ska, om det står tydligt i policyn, du ska inte göra den här saken, då blir det nästan upp till den personen att erkänna att de har gjort fel snarare än att vi kontrollerar allting.

32. JA: Okej

33. AB: Men ni kör inte några typ stickprover eller tester… Skickar ut några låtsaslänkar och ser så de inte trycker på de?

34. I3: Haha, nej det har vi inte gjort än, men det är definitivt ett bra sätt att göra det på, att testa så. Vi har ju… Vi är ju i en resa där vi kommer göra alla de här sakerna. I höst kommer vi starta upp mycket mer, bland annat ett cyber security awareness-program, men i dagsläget så har vi inte arbetet så mycket med det. Jag tror vi har levt ganska mycket på, säkerheten har levt ganska mycket på att vi har liksom bra system konfigurerade på standard och sen liksom moderna miljöer. Men jag tror också att det blir ju bara värre och värre det här så det gäller ju verkligen att få med awareness för alla.

35. AB: Ja. Tror du att det blir några svårigheter just vid distansarbete? Det här arbetet… just med awareness.

36. I3: Ja, det lär det bli. Man får se hur det blir liksom, det är ju viktigt att få liksom, att göra awareness program eller utbildningsprogram så är det ju en utmaning att göra det fungerande på distans. Det är ju alltid jättebra att göra det lokalt, om det går.

37. JA: Ja, precis.

38. I3: Men vi får se lite hur vi gör där egentligen, det är inte bestämt riktigt. Men det är något vi ska arbeta fram under hösten också.

39. AB: Yes. Och vidare till utbildning här. I vilken mån utbildas anställda i informationssäkerhet och era riktlinjer?

40. I3: Ingen utbildning. Utan det är bara spontaninformation som skickas ut.

41. JA: För att höja medvetenheten då alltså?

42. I3: Ja precis. Mycket så här att vi skickar ut information säg… inför varje sommar och inför varje jul och tänk på det här nu. Ni kommer vara trötta efter en höst eller en vår liksom och tänk nu på att ni inte ska göra de här grejerna.

43. AB: Okej, så det är lite kontinuerliga utskick med information?

44. I3: Ja, precis.

45. JA: Mm. På tal om medvetenhet. Hur skulle du säga att den generella attityden och medvetenhet är hos personalen gentemot informationssäkerhet?

46. I3: Jag tror att den är ganska… Den är ganska blandad. Det finns de som är oroliga för att någonting ska gå fel och är ganska ängsliga. Och där utmaningen för oss där blir att vi liksom inte utbildat de ordentligen eller tagit hand om de ordentligt med den här ängsligheten så de känner att de gör rätt saker. Så det är liksom en grupp av det hela. Sen kanske det är en grupp som inte vet, inte förstår och inte bryr sig haha. Och de måste man ju då attackera på ett annat sätt.

47. JA: Ja precis.

48. I3: Så de måste man kanske attackera de med lite mer… Med lite piska och morot haha.

49. JA: Haha ja.

50. I3: Men annars så… Jag tror också det beror på vilken generation man tillhör eller hur gammal man är tror jag. För vi är ett ganska ungt, det är ganska många unga människor som arbetar hos oss. Jag vet inte exakt vilken ålder… snittålderna kanske ligger på 40… 35-40 någonstans. Så jag tror nog att… det är nog inte så många som inte förstår att det är ett problem.

51. JA: Nej okej.

52. I3: Men jag tror att den största utmaningen där är att liksom se till att de får rätt information och vad de ska göra och vad de ska tänka på. Så man inte blir orolig för allting som händer.

53. JA: Nej vad bra. Då går vi över till de sista frågorna tror jag.

54. AB: Yes. Hur skulle du säga att ledningens förhållande till informationssäkerhet är?

55. I3: Det har varit ganska… Låt gå attityd haha, fram tills typ nu. Vi har lyckats få igenom att vi skulle göra en fullständig cyber security review, inte en fullständigt audit utan en review, och gå igenom (xx). Jag tror detta har blivit en ganska bra väckarklocka för ledningen, att nu är det dags att ta tag i det här. Vi har heller aldrig haft något breach. Vi har aldrig haft någon breach. Alls. Vilket är ju såhär också ett sätt liksom att vi (xx) i sin säkerhet (xx) såhär. Men i och med att vi fått de här rekommendationerna och genomlysningen från den här externa parten så belyses de här grejerna på ett sätt som gör att vi kommer kunna få ledningen med oss. Och det här är ju ett arbete som vi kommer komma igång med under hösten också. Att sätta upp det här kontinuerliga strategiska arbetet med ledningen så vi kan få belysning på cyber security över organisationen. Så att de finns med i hela, så det finns med i alla strategier och alla (continuty?) plans.

56. AB: Tror du att det skulle sätt annorlunda ut ifall det hade varit någon breach? Att det skulle varit mer stressigt uppifrån ifrån ledningens håll.

57. Ja det tror jag. Vi har inte haft någon breach så att om vi väl skulle få någon tror jag man skulle tänka mycket mer på det här. Det skulle bli mycket lättare att sälja in det här, att det ska vara överallt. Men i och med, i alla fall tidigare. Men i och med de här reviewsen vi gjorde nu så är det lättare för oss att bara säga nu är det viktigt.

58. AB: Ja, det är ju klart.

59. JA: Jag kom på en fråga om medvetenhet igen.

60. I3: Ja

61. JA: Tror du, eller tycker du… Ser du det som en utmaning att bibehålla en god medvetenhet på distans jämfört med på plats, eller är det likvärdigt?

62. I3: Ja precis, det är en bra fråga… Ja alltså utöver det här kulturella att man inte kan ses och prata face-to-face liksom… Där är det nog ingen skillnad egentligen… Tror jag… Jag tror att, vi har ju återkommande månadsmöten på företaget där vi går igenom såhär viktigaste grejerna som händer. Det här kan man ju… Det är ju ingen skillnad egentligen att prata på ett sådant möte om det är remote eller on site, utöver att man kanske får folk ännu mer fokuserade om man faktiskt är on site.

63. JA: Ja men det är bra.

64. AB: Skulle du säga att ni har en god säkerhetskultur generellt?

65. I3: Nej, det skulle jag inte säga. Jag skulle säga att vi har en, 2 av 5 kanske haha.

66. JA: Haha, okej bra skala.

67. I3: Nä precis, men annars har vi.. Det är om vi jämför med om vi skulle vara ett stort företag. Tittar vi liksom på, skulle vi vara till exempel SAAB, som har state actors efter sig som vill sno deras data, då är vi definitivt på en skala 2 av 5. Vi har liksom, vi behöver arbeta betydligt mer med det här. Och vår bransch är ju ganska intressant för attacker, både information, att stjäla information, men också bara för att störa oss i vår produktion med cryptolockers eller motsvarande

68. JA: Ja, det kan jag tänka mig.

69. AB: Ja det känns lite som en mognadsfas för företagen också att ju större och äldre desto mer blir det fokus på säkerhet och sånt. Mer nya företag är väl mer, då är det väl mer själva affärsprocesserna i början och fullt fokus på att utveckla i början.

70. I3: Ja verkligen, verkligen, verkligen. Det är precis så det är. Jag tror liksom det är, där så har vi från IT-sidan lyckats att enabla detta ganska så bra med genom att ha ganska

sunda standardinställningar och sunda system, liksom att enabla det här. Vi har klarat oss rätt så länge utan att gå rätt hårt på cyber security liksom. Genom vi har bra, vi har vettig teknologi för att hålla den distribuerade arbetskraften säker. Men vi kommer till ett läge nu där vi behöver kolla ännu mer systematiskt nu, vi kan inte göra det ad-hoc längre på det sättet som vi gjort tidigare utan det behövs göras systematsikt.

71. JA: Okej. Har distansarbetet skapat några större utmaningar som vi inte har tagit upp än, som du har tänkt på? För informationssäkerhet då.

72. I3: Nej, jag tror inte det är någon skillnad egentligen… Vi… Nej det tror jag inte. Vi har haft vår setup för liksom för arbetarna med deras datorer har varit (xx) men de beter ju sig som (remote first?), alltså datorerna. Så det finns ju inget som är mindre eller mer säkert bara för att man är off site egentligen. Den största utmaningen där är väl egentligen den kulturella utmaningen och awareness-utmaningen liksom att nu är man inte längre on site och man kan inte möta på oss i korridorerna och snacka om en grej man såg på internet eller ett mail man fick som såg konstigt ut.

73. JA: Nej, precis. Och där besvarade du nog den sista frågan där också om du ser några långsiktiga utmaningar. Men då är det kanske det kulturella som är den första då.

74. I3: Ja jag tror det. Den kulturella och sen så struktureringar, för företaget i stort att få upp struktur. Att vi får upp awareness, inte bara hos de anställda utan även hos ledningen så att vi kan arbeta proaktivt med it-säkerheten genrellt. Men angående remote arbetet tror jag absolut att det kulurella är det stora.

75. JA: JA… Då tror jag vi var klara om det inte var något mer.

76. AB: Nej

77. I3: Nej

8.5 Intervju med Organisation 4

(xx) = Svårt att urskilja exakt vad som sägs i inspelningen.
(osäkert ord?) = Något osäker på exakt vilket ord som sägs men har skrivit ut vad vi tycks höra.
**** = Anonymisering av namn eller andra identifierande ord.
… = Längre paus.

Intervjuare 1 (JA) – Jakob Andersson (intervjuledare)
Intervjuare 2 (AB) – Andreas Berg
Informant 4 (I4) – Chief Information Security Officer på Organisation 4 (O4)

1. JA: Då undrar jag om du kortfattat bara skulle vilja beskriva din roll? Vilket verksamhetsområde du är verksam inom?

2. I4: Just det, precis. Jag tror att ni hade lite koll när ni bjöd in mig så jag hoppas det är samma förväntningar. Jag har en roll som CISO eller Chief Information Security Officer. Ansvarar för att leda, driva och utveckla området kring informationssäkerhet vid O4 i sin helhet. Och har jobbat med det innan jag kom till O4 som global informationssäkerhetschef vid ****. Jag har ju jobbat som IT-chef för ganska många olika organisationer. Har haft roliga jobb, roliga ställen att jobba på, trivts bra.

3. JA: Okej, vad bra. Och i vilken utsträckning och hur länge har ni arbete på distans nu ungefär?

4. I4: Du, jag har de någonstans här… Jag skrev upp det här någonstans… Frågar du mig eller frågar du vi generellt på O4?

5. JA: Generellt vid O4.

6. I4: Ja, jag tror vi kom igång ganska snabbt med det… Jag borde hitta det här någonstans… Ja, mars 2020 skulle jag säga, inte 2019 naturligtvis, 2020 mars har vi jobbat hemifrån i princip så mycket vi har kunnat.

7. JA: Ja, men det är bra då var det nog allt med lite bakgrund där. Om vi går in på policys, så i den mån du kan berätta, hur ser ert arbete angående riktlinjer och policys ut?

8. I4: Tänker du generellt? Inte något kopplade till corona och så?

9. JA: Nej, utan bara generellt.

10. I4: Det finns en del riktlinjer på plats idag på O4. Men det är mitt, min analys när jag kom in är att de behöver bli mer kompletta.

11. JA: Okej, har ni på något sätt behövt anpassa riktlinjerna för distansarbete?

12. I4: Ja, det har vi gjort. Men på ganska operativ nivå skulle jag säga. Vi har inte ändrat det stora övergripande ramverket för informationssäkerhet på grund av pandemin utan det har varit på mycket praktisk nivå att gå ut och kommunicera.

13. JA: Ja men det är bra. Har de anställda enkel tillgång till riktlinjerna? Är de medvetna om vad som står?

14. I4: Ja, både ja och nej. Det som gäller corona och covid, där finns en hel del information för medarbetare generellt och då har vi även stoppat in det som är kopplat till distansarbete där.

15. JA: Ja, och om vi tänker för de anställda, på vilka sätt, om några sätt, kan riktlinjerna anses vara svåra att efterfölja? Vid distansarbete då?

16. I4: Den stora utmaningen tycker jag är att det kommer en hel del andra parallella, nya krav på det och nya riktlinjer och framför allt förändrade arbetssätt på grund av corona. Det som är kopplat till informationssäkerhet, det är ju bara en liten del. Och sen är det just det här också att vad gör jag med mitt eget nätverk hemma liksom? Hur skyddar jag det när jag inte sitter på jobbet. Det är också… ja helt plötsligt blir man helt beroende av sin hemsituation.

17. JA: Ja, precis.

18. I4: Så det tycker jag väl är en stor utmaning att alla inte kan, vad ska jag säga, lika lätt, eller mer eller mindre svårt för personalen att anpassa sig.

19. Okej. Och i vilken mån ser ni till att policyn efterföljs?

20. I4: Ja, det är ju det regelefterlevnad som du säger. Just nu görs det, på lite olika ställen. Man kan väl säga såhär, det är inte bara min funktion då som ska göra detta utan det är väl andra. Så att, när du säger policys, menar du generellt infosec eller menar du kopplat nu till distansarbete?

21. JA: Jag menar generellt.

22. I4: Uppföljning idag sker på chefsnivå. Det är de som ansvarar idag för efterlevnad.

23. JA: Okej, revisioner då?

24. I4: Vi kan också säga att den strukturerade uppföljningen som sker utav de här riktlinjerna eller policyn, den görs till stor del av internrevisionerna.

25. JA: Okej, och vid distans har ni gjort något utöver det vanliga för att se till att det följs eller är det samma arbetssätt?

26. I4: Då skulle jag nog vilja säga så här, att ja det görs, fast det görs ganska utspritt. Så det är varje funktion, sektion eller del inom förvaltningen som gör olika aktiviteter själva. För att just följa upp hur distansarbetet fungerar.

27. JA: Nej, precis. Och vidare till utbildning då. I vilken mån utbildas de anställda om informationssäkerhet och riktlinjer? Generellt.

28. I4: Det finns en, framför allt finns det en generell utbildning som har funnits i några år tillgänglig på intranätet för all personal och den är, det är både högt och lågt, det är en kombination av den typ av utbildning som man bör ha. Så det är allt ifrån lösenord, skydda din dator, så här ser phishing-mail ut ungefär, alltså den typen av awareness. Så där finns det en grundbult kan man säga som alla ska gå.

29. JA: Finns det någon fortsatt kontinuerliga utskick eller träning sedan efter det?

30. I4: Ja, det gör det. Ute i organisationen. Vi måste upp en bit där ser jag det som. Och där är vi ju inte unika kan man väl säga heller.

31. JA: Ja, det är ju något vi har läst om att det krävs ofta en händelse innan.

32. I4: Ja. Jag använder olika verkliga case för att utbilda och informera internt för att få upp medvetenheten först på, eller höja skulle man nog säga, för medveten är man nog, men ge lite mer tryck i de här frågorna kanske på ledningsnivå. Och det går bra faktiskt, det går jättebra. Jag kan ju säga att med tanke på corona, det har ju också påverkat den här pandemin, i och med att cyberhot och cyberattacker har ökat dramatiskt gör det ju mitt arbete både lättare och svårare.

33. JA: Ja verkligen. Ja nu har vi gått in lite grann på det, men när det gäller just distans har det kommit någon speciell utbildning eller information, utskick, för att öka awareness?

34. I4: Ja, den ligger kopplad till det som andra har lagt ut kring just förändrade arbetssätt och rutiner vid distansarbete och på grund av corona. Så man kan säga att corona huvuddel, sen går man in på olika delar, tänk på detta, det här och det här behöver du förändra, det påverkar ditt arbetssätt och så vidare. Och det är en blandning då där bland annat informationssäkerhet är med.

35. JA: Okej. Och generellt, hur skulle du säga att personalens medvetenhet är mot informationssäkerhet?

36. I4: Jag skulle säga att den är allmänt god, men att vi har utmaningar på grund av att vi har en stor genomströmning av personal. Ska man se från medvetenheten kan det svänga ganska mycket från ett år till ett annat för att det är nytt folk och då har det ofta att göra med, vad har de med sig från tidigare var de är ifrån? Men utifrån stickprov och de dialoger jag har så kan jag säga att medvetenheten är god, framför allt på högre nivå för det är där jag mest har jobbat nu. Med tanke på cyberhot och cyberattacker och framförallt social engineering så kan man aldrig göra det här för mycket.

37. AB: Hur ser stickproven ut ungefär i stort?

38. I4: Gjort workshops tillsammans med ledningsgrupper, egentligen intervjuer och hur de ser på det. Och det är olika roller också, cheferna har ju ett ansvar också utöver det man har som enskild medarbetare. Sen gör jag också stickprover genom att jag träffar folk och man sitter med medarbetare. Och det ringer in folk och frågar om saker och rapporterar händelser. Men jag skulle säga att mina stickprov mest är, bland gemene, där ju när jag träffar folk på jobbet helt enkelt.

39. JA: På vilka sätt kan det vara utmanande att bibehålla en god medvetenhet på distans jämfört med på plats?

40. I4: Att bibehålla medvetenheten när du sitter på distans…ja det kan ju vara det här att du träffar inte folk vid kaffemaskinen, du får inte det här dagliga flödet av saker och ting som händer omkring dig. Du kanske är mer beroende av att dina chefer håller lite typ samtal eller medarbetarmöten där man berättar vad som har hänt, eller vad som gäller, att man upprepar. Det är väl en sak, det här just med att kommunicera med medarbetare som sitter på distans är en större utmaning. Men sen tänkte du kanske mer på att upprätthålla, att man tänker på hur man arbetar när man sitter på distans.

41. JA: Ja, det också.

42. I4: Nej det är klart, visst. Som så mycket annat så är det…Återupprepa hela tiden, det är ju svårare när man sitter hemma. Så att den enskilde medarbetaren har ju ett mycket större ansvar rent praktiskt.

43. JA: Så du skulle säga att det är det kulturella helt enkelt? Att det är svårt.

44. I4: Ja, ja det är det.

45. JA: Hur skulle du säga att ledningens förhållande till arbetet med informationssäkerhet är?

46. I4: Väldigt varierande. Och det var framför allt för att man ofta blandar ihop begreppen va. Och det är inget unikt för O4 utan det är snarare ganska vanligt. Att man blandar ihop dom här, vad är IT-säkerhet, vad är informationssäkerhet, vad är riskhantering, vad är cyberrisk, alltså vad är dom här orden. Så jag har jobbat mycket med det, att bara försöka få folk att förstå. Hatten är informationssäkerhet och under det finns det… IT-säkerhetsåtgärder, det finns cyberhot etc etc. Den starkaste medvetenheten är på styrelsenivån.

47. JA: Ah okej.

48. I4: O4s styrelse ber mig att rapportera. Hur det går, vad vi gör, hur det ser ut. Kombinationen av att jag har jobbat rätt hårt med awareness på ledningsnivå och att corona är corona, det har ju gett den effekten med… cyberattacker att man får upp ögonen för det. Men också att vi under 2020 fick nya föreskrifter från MSB och

lagefterlevnad är ju en väldigt viktigt punkt för statliga myndigheter. Så att till hösten 2020 uppdaterades de föreskrifter som MSB har för informationssäkerhet till statliga myndigheter.

49. JA: Okej.

50. I4: Så det gjorde att jag fick en uppdaterad plattform rent lagmässigt att följa då. Så att, jag skulle säga att den sista tiden har jag upplevt en kraftig ökning. Och den har hela tiden funnits som sagt på ledningens agenda. Men sen har man då haft, man har ett behov av att jämna ut…Att man förstår, att man pratar om samma sak. Att man inte riktigt, när jag kommer ut och pratar om vissa ord så måste man vara noga med att förstå att, först fånga upp, förstår alla innebörden av det ordet liksom.

51. JA: Så det är en god medvetenhet, generellt väldigt bra.

52. I4: Ja men det tycker jag, det tycker jag. Sen är det ju en helt annan sak att liksom få igång ett mer omfattande, bredare arbetssätt i nästa nivå. Det finns en god självinsikt om jag säger så.

53. JA: Ja, okej. Det låter ju väldigt bra. Och vid just distansarbete, var ledningen aktiv med arbetet med informationssäkerhet då? Kom det några direktiv eller utskick från ledningens håll?

54. I4: Man kan väl säga att när det började, det som hände då var ju egentligen att man gick in i en krishantering. Och det gjorde ju även många andra företag och organisationer. Att man slog på någon slags krisplan. Och i den krisplanen så handlade det ju mer om smitta, risk, spridning av smitta. Det handlade om just att få i gång det dagliga arbetet på distans. Det handlade också om att arbetsmiljön skulle fungera praktiskt för medarbetare etc etc. Så att dom sakerna kom ju först. Så det var jag tog kontakt och sa att nu vill jag trycka in detta också då, och då var man helt med, det var inget snack.

55. JA: Då har vi bara några frågor kvar här, och det är väl egentligen om det finns någon utmaning med distansarbete och informationssäkerhet som vi inte har tagit upp som du kan komma på?

56. I4: Då är vi mer inne på de tekniska bitarna. Det är ju lite grann det här, hur mycket teknik och hur mycket teknisk säkerhet behöver jag som medarbetare förstå när jag jobbar hemifrån. Och det här med… osäkra nätverk, dina egna uppkopplingar, lite blandad kompott kan man väl säga. Men också det här att jag lämnar min dator utan att kanske stänga ner skärmarna, jag kanske… informationssäkerhet handlar ju inte bara om teknik, utan det är ju också det här, var sitter jag någonstans och jobbar. Har jag liksom halva familjen bredvid mig och sitter och har samtal och möten. Kan jag sitta ostört hemma? Skriver jag ut papper på hemmaskrivaren, nja kanske inte med viss information men kanske med annan. Så att det är en blandning av kanske lite sådana saker också. Men det är ganska många punkter att tänka på, det är det. Så att jag…jag tror nog att vi, vi kommer att lära oss mycket av det här och det kommer

också att… att få negativa konsekvenser och positiva konsekvenser att vi fick sadla om helt när det gäller arbetssätt.

57. JA: Ja, jag kan tänka mig att det måste ha varit svårt när det kom så här, utan någon planering eller någonting över huvud taget.

58. I4: Ja, egentligen är det ju hela digitaliseringsbiten här. Digitaliseringen gick ju liksom i raketfart och… sen finns det då i digitaliseringssammanhang så brukar man säga att utan hållbar säkerhet så får du ingen hållbar digitalisering. Det är inte vi som har liksom drivit det här utan det har bara tvingats fram va. För att just den här situationen var inte så mycket att fundera utan det var ju bara att göra. Och det gäller ju inte bara oss, utan det var ju en mängd naturligtvis, andra organisationer som alla mer eller mindre.

59. JA: Ja precis, det var ju dem flesta. Inklusive oss haha.

60. I4: Ja precis, nej men jag förstår absolut. Därför jag menar lite grann som jag sa förut. Det här var ju, samhället gick ju in i ett krisläge. Informationssäkerhet har väl kanske inte varit punkt ett på agendan, men jag hoppas åtminstone att det var topp 5 i dem flesta organisationer.

61. JA: Ja, egentligen svarade du på den sista frågan här om långsiktiga utmaningar med distansarbete och informationssäkerhet, vad det skulle kunna tänkas vara.

62. I4: Jag tror fortfarande att medvetenheten är den viktiga, för det är en kulturförändring som du själv nämnde här om man sitter hemma. Hur ska man nå sina kollegor och medarbetare ute när de inte ens är vid kaffemaskinen som jag brukar säga. Och det är mycket annan verksamhet som också drabbas negativt ut av det här med att man inte är i kontakt med sina kollegor. Men sen å andra sidan så tror jag väl att, jag gissar att det kommer att plana ut, det kommer att bli mer distansarbete än innan men inte lika mycket som nu naturligtvis. Det är ju förhoppningen i alla fall. Och då hoppas vi att man hittar något mellanläge. Men säkerhetsmässigt så…alltså i och med att distansarbetet i sig har ökat cyberattackerna så kraftigt va… det gör ju att, alltså hotbilden har ju ökat. Samtidigt som corona i sig har skapat jättemycket problem för oss, både samhällsmässigt och hälsomässigt men också distansarbetesbiten va. Så är nog egentligen…ja, den kombon av att vi på köpet fick… det finns en enorm potential för cyberkriminella att uttnyttja här. Och det gör dem ju fortfarande, så att jag studerar ju noga andra organisationer utanför Sverige som har blivit drabbade, och dem är ju ganska många. Så jag tror väl egentligen att, för mig är det ju liksom från flera håll, men tittar man bara på vad gör man för medarbetaren på distans, då är det ju information, information, kommunikation och dialog. Och det var ju jobbet redan innan. I alla organisationer, det är inte unikt för oss. Men det är också viktigt att man anpassar det till kulturen.

63. JA: Ja, jättebra svar, vi är klara där. Tack så mycket.