LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

Mikroföretags arbete med informationssäkerhet

- en kvalitativ studie

Kandidatuppsats 15 hp, kurs SYSK16 i Informationssystem

Författare: Emma Johansson
Michelle Olsson Larsson

Handledare: Björn Svensson

Rättande lärare: Miranda Kajtazi
Paul Pierce

Mikroföretags arbete med informationssäkerhet – en kvalitativ studie

ENGELSK TITEL: Micro Businesses work with information security – a qualitative study

FÖRFATTARE: Emma Johansson och Michelle Olsson Larsson

UTGIVARE: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

EXAMINATOR: Osama Mansour, PhD

FRAMLAGD: maj, 2022

DOKUMENTTYP: Kandidatuppsats

ANTAL SIDOR: 101

NYCKELORD: Mikroföretag, Informationssäkerhet, CIA-triaden

SAMMANFATTNING (MAX. 200 ORD):
För företag är information en viktig tillgång, varav informationssäkerhet är en angelägenhet för alla företag oavsett företagsstorlek. Även mikroföretag drabbas av cyberattacker, men i jämförelse med större företag har de begränsat med resurser att allokera till informationssäkerhet. En konsekvens av detta är att informationssäkerhet i allmänhet hanteras av en lekman. Det förekommer studier som argumenterar för att mikroföretag bör studeras separat på grund av att de har egenskaper som skiljer dem från större företag. Däremot förefaller studier om hur specifikt mikroföretag arbetar med informationssäkerhet saknas. Studiens forskningsfråga ämnar därför att besvara hur mikroföretag arbetar med informationssäkerhet. Definitionen av informationssäkerhet som valts för denna studie är CIA-triaden. I syfte för att samla in kvalitativ data och besvara forskningsfrågan har sex stycken semistrukturerade intervjuer utförts. Resultatet visar att mikroföretag beskriver informationssäkerhet som att framför allt bevara egenskapen konfidentialitet. Vidare tyder studiens resultat på att mikroföretag främst arbetar med fysiska säkerhetsåtgärder, antivirusprogram, brandväggar, åtkomstkontroll samt säkerhetskopiering i syfte för att skydda verksamhetens information. Dessa säkerhetsåtgärder kan alla klassificeras under kategorin teknologi, varav resultatet antyder att mikroföretag huvudsakligen arbetar med tekniska säkerhetsåtgärder.

Innehåll

Tabeller

1 Introduktion

Detta inledande kapitel ämnar huvudsakligen introducera ämnesområdet och presentera, för studien, relevant bakgrundsinformation. Vidare redogör författarna för problemområdet, vilket mynnar ut i studiens forskningsfråga, syfte respektive avgränsningar.

1.1 Bakgrund

I det digitala samhället är det mer regel än undantag för, inte bara stora, utan även små- och medelstora företag (SME) att i större utsträckning nyttja informationssystem (IS) (Sadok, Alter & Bednar, 2020). Detta har resulterat i att information lagras, bearbetas och kommuniceras i IS (Heidenreich, 2017), men också att företag i större omfattning förlitar sig på IS för att bedriva den operativa verksamheten (Bulgurcu, Cavusoglu & Benbasat, 2010; Sajal, Jahn & Nygard, 2019; Watad, Washah & Perez, 2018). Ett ökat beroende kommer dock med risker, vilka resulterar i nya krav på hur företag behöver agera för att skydda verksamhetens information (Bulgurcu, Cavusoglu & Benbasat, 2010; Watad, Washah & Perez, 2018).

Digitalisering och utveckling av ny teknologi har en ofördelaktig sida, vilken är att antalet cyberattacker tilltar (Tsochev, Trifonov, Nakov, Manolov & Pavlova, 2020; Sajal, Jahan & Nygard, 2019). En felaktig bild är dock att det framför allt är stora företag som drabbas av dessa cyberattacker (Watad, Washah & Perez, 2018). Enligt Tsochev et al. (2020) är majoriteten av de intrångsförsök som sker på daglig basis riktade mot de mindre företagen. En uppfattning som delas av Kurpjuhn (2015) som påstår att även SME är i riskzonen för att utsättas för en cyberattack. Detta är problematiskt eftersom en cyberattack kan resultera i flera konsekvenser, inte minst för SME (Paulsen, 2016; Watad, Washah & Perez, 2018). En konsekvens kan exempelvis vara finansiella bortfall (Tsochev et al. 2020), där drabbade företag inte sällan förlorar inkomst (Baker & Wallace, 2007). Här är specifikt SME sårbara eftersom de har sämre förutsättningar att hantera finansiella bortfall (Keller, Powell, Horstmann, Predmore & Crawford, 2005). Vidare argumenterar Watad, Washah och Perez (2018) för att småföretag inte är ett undantag, utan att även de kan drabbas av ekonomiska konsekvenser och försämrat rykte i samband med en cyberattack.

För att bedriva operativ verksamhet är företag i regel beroende av information, vilket resulterar i att information anses vara en dyrbar resurs (MSB, 2015; Rees, 2010; SIS, 2015). Vidare är information grunden till kunskap i ett företag (MSB, 2015; SIS, 2015), varav företag också kan ha information som är viktig för att urskilja sig från konkurrenterna på marknaden (Nyak & Rao, 2014). Alla företag behöver därför skydda information från exempelvis obehöriga och cyberattacker, vilket kan uppnås med *informationssäkerhet* (Nyak & Rao, 2014). Informationssäkerhet ämnar dock inte enbart att skydda information som lagras och kommuniceras med informationsteknik (eng. *Information and communication technology, ICT)*, utan även analog information (von Solms & van Niekerk, 2013). Enligt Sadok, Alter

och Bednar (2020) är informationssäkerhet en angelägenhet för samtliga företag, oberoende av företagsstorlek.

Bland de minsta företagen återfinns *mikroföretag*, vilka enligt Europeiska kommissionens definition är företag med maximalt nio anställda (European Commision, u.å.). Tillsammans med ovan får ett mikroföretag inte uppvisa en årlig omsättning, alternativt en balansomslutning, som överstiger två miljoner euro (European Commision, u.å.). Vidare ingår mikroföretag i kategorin SME, vilken är en kategori som står för 99% av alla företag inom EU (European Commision, u.å.). Eftersom mikroföretag skapar arbetstillfällen, men också erbjuder produkter och tjänster har dessa företag en viktig roll i länders ekonomi (Heidenreich, 2017).

Enligt Talu (2020) drabbas även mikroföretag frekvent av cyberattacker. Svårigheten är dock att mikroföretag, i jämförelse med större företag, har begränsade resurser och därav sämre förutsättningar att hantera informationssäkerhet (Heidenreich, 2019; Talu, 2020). Baker och Wallace (2007) argumenterar dock för att begränsade resurser inte är en acceptabel ursäkt till att småföretag i allmänhet har sämre informationssäkerhet än större företag. Med mindre resurser är de dock mer exponerade för de ekonomiska konsekvenserna av en cyberattack, vilket ökar risken för konkurs om de drabbas (Heidenreich, 2017; Talu, 2020). Ovanstående indikerar således på att informationssäkerhet bör vara en angelägenhet även för mikroföretag, vilket även Heidenreich (2017) samt Talu (2020) båda argumenterar för.

1.2 Problemområde

Heidenreich (2017) påstår att kategorin SME, men specifikt mikroföretag, har sämre informationssäkerhet än andra större företag. Vidare skriver Heidenreich (2017) att mikroföretag i allmänhet underskattar komplexiteten med informationssäkerhet, vilket kan resultera i att mikroföretag får en mer obekymrad inställning till informationssäkerhet. Denna uppfattning delas av Renaud och Weir (2016) som i en studie visar att SME inte tar cyberhot på allvar och att det endast var 15% av företagen som hade en realistisk bild av företagets sårbarhet. En avslappnad inställning till informationssäkerhet, i kombination med en mindre budget, kan resultera i att mikroföretag prioriterar att allokera resurser på andra delar av verksamheten (Heidenreich, 2017).

Heidt, Gerlach och Buxmann (2019) påvisar i en studie att SME ser ekonomiska investeringar på informationssäkerhet som en för stor utgift i relation till företagets begränsade resurser. Tidigare studier har även påvisat att SME, till skillnad från stora företag, i allmänhet saknar dedikerad IT-personal som hanterar företagets informationssäkerhet (Gupta & Hammond, 2005; Heidenreich, 2017; Keller et al. 2005; Kurpjuhn, 2015). Kurpjuhn (2015) påstår att detta troligtvis beror på att SME har begränsat med resurser. Här poängterar Heidenreich (2019) att specifikt mikroföretag har ännu mindre resurser och anställda än SME. Konsekvensen av detta blir att en lekman, vilken i allmänhet saknar IT-kompetens, hanterar informationssäkerhet på mikroföretag (Heidenreich, 2017). Vidare har mikroföretag svårt att finna adekvata informationssäkerhetslösningar (Heidenreich, 2019). Detta för att industrilösningarna är för komplexa och kostsamma, medan de privata lösningarna är för simpla för att täcka hela verksamhetens behov (Heidenreich, 2019).

I en pågående studie poängterar Nagahawatta, Lokuge, Warren och Salzman (2021) att det förekommer få studier som specifikt studerar mikroföretag. Majoriteten väljer i stället att

studera hela gruppen SME, vilket resulterar i slutsatser för SME som helhet (Nagahawatta et al. 2021). Vidare skriver Heidenreich (2017) att flera studier om informationssäkerhet väljer att exkludera mikroföretag från SME-definitionen och därav utesluta dessa företag från studierna. Detta är problematisk eftersom mikro-, små- respektive medelstora företag skiljer sig åt i flera avseende som exempelvis storlek, resurser och organisationsstruktur (Heidt, Gerlach & Buxmann, 2019; Nagahawatta et al. 2021). Eftersom skillnaderna är flera bör mikro-, små- respektive medelstora företag studeras separat (Heidt, Gerlach & Buxmann, 2019; Nagahawatta et al. 2021). Ovanstående bekräftas av Baker och Wallace (2007) som påstår att företagsstorlek är en faktor, som i tidigare studier, har visat sig påverka hur företag arbetar med informationssäkerhet.

Tidigare studier om informationssäkerhet i företag försummar i flera fall SME-perspektivet (Heidt, Gerlach & Buxmann, 2019). Uppfattningen delas av Sadok, Alter och Bednar (2020) som påstår att det förekommer relativt få tidigare studier om informationssäkerhet hos SME. Vidare förefaller det, enligt författarnas kännedom, förekomma få tidigare studier som undersöker informationssäkerhet hos specifikt mikroföretag. Exempelvis studerar Gupta och Hammond (2005) samt Keller et al. (2005) informationssäkerhet hos företag med maximalt 500 anställda. Andra studier undersöker i stället informationssäkerhet hos företag med upp till 100 anställda (jmf. Renaud & Weir, 2016; Watad, Washah & Perez, 2018). En del av de studier som påträffas publicerades dessutom för över 15 år sedan.

Det finns dock visserligen studier som berör delar av informationssäkerhet hos mikroföretag. Dessa fokuserar dock på vilken metod mikroföretag kan tillämpa för att utvärdera företagets nivå av informationssäkerhet (jmf. Heidenreich, 2017; Heidenreich, 2019) samt hur mikroföretag skyddar sig mot cyberattacker (Talu, 2020). Således förefaller tidigare studier inte studerat specifikt hur mikroföretag arbetar med informationssäkerhet.

1.3 Forskningsfråga

Ovanstående problemområde resulterar i följande forskningsfråga:

- *Hur arbetar mikroföretag med informationssäkerhet?*

1.4 Syfte

Studien ämnar ge en beskrivning av hur mikroföretag arbetar med informationssäkerhet.

1.5 Avgränsningar

I studien avgränsas begreppet mikroföretag till de företag som inte har IT eller informationssäkerhet som primärt verksamhetsområde. Detta eftersom företag som bedriver verksamhet inom IT eller informationssäkerhet sannolikt har bättre förmåga att arbeta med informationssäkerhet i den egna verksamheten. De exkluderas således från studien eftersom de troligtvis inte är representativa för alla mikroföretag.

2 Litteraturgenomgång

Följande kapitel ämnar presentera de begrepp och modeller inom ämnesområdet som anses vara av relevans för att besvara studiens forskningsfråga. Kapitlet inleds med en beskrivning av studiens centrala modell, CIA-triaden. Därefter lyfts kritik mot CIA-triaden samt ett urval av alternativa modeller, vilket mynnar ut i en motivering om varför CIA-triaden tillämpas för att beskriva informationssäkerhet hos mikroföretag. Därefter följer en övergripande beskrivning av ett urval av säkerhetsåtgärder, vilka delas in i tre kategorier. Kapitlet avslutas med ett teoretiskt resultat som beskriver vilka egenskaper i CIA-triaden respektive säkerhetsåtgärd avser skydda.

2.1 Informationssäkerhet och CIA-triaden

Säkerhet avser skydda samtliga tillgångar (Andress, 2014; Nyak & Rao, 2014), medan informationssäkerhet specifikt ämnar skydda information (Andress, 2014; Nyak & Rao, 2014; von Solms & van Niekerk, 2013). Detta omfattar all information, vilket således även inkluderar den information som inte lagras och kommuniceras med hjälp av informationsteknik (von Solms & van Niekerk, 2013).

Von Solms och van Niekerk (2013) poängterar att det figurerar flera olika definitioner av informationssäkerhet i litteraturen. I allmänhet definieras dock informationssäkerhet med utgångspunkt i vilka egenskaper *säker information* bör inneha (von Solms & van Niekerk, 2013). En väletablerad definition av informationssäkerhet är att säker information besitter tre grundläggande egenskaper, vilka informationssäkerhet ämnar upprätthålla och säkerställa (von Solms & van Niekerk, 2013). Dessa tre egenskaper är konfidentialitet (eng. *confidentiality)*, integritet (eng. *integrity)* respektive tillgänglighet (eng. *availability)*, vilka tillsammans bildar CIA-triaden (Andress, 2014; Dhillon & Backhouse, 2000; Nyak & Rao, 2014; SIS, 2015; von Solms & van Niekerk, 2013).

Enligt Samonas och Coss (2014) återfinns ovanstående definition av informationssäkerhet även i flera standarder och ramverk, såsom COBIT och ITIL. Ett exempel på en standard som delar denna definition är svenska institutet för standarder (SIS) (SIS, 2015). Detta är också den definition av informationssäkerhet som denna studie tillämpar. Nedan följer en beskrivning av respektive egenskap i CIA-triaden:

2.1.1 Konfidentialitet

Enligt Samonas och Coss (2014) har egenskapen konfidentialitet ursprung i det militära, varav konfidentialitet främst förknippas med kontroll. Detta innebär att konfidentialitet är den egenskap i CIA-triaden som ska säkerställa att obehöriga inte ges åtkomst till att ta del av information som de inte har behörighet till (Andress, 2014; Dhillon & Backhouse, 2000). Vidare poängterar Nyak och Rao (2014) att upprätthållande av konfidentialitet är en av de mest angelägna aspekterna inom informationssäkerhet. Åsikten delas av Samonas och Coss (2014), som dock poängterar att organisationers nya behov kan förändra prioriteringarna gällande vilken egenskap i CIA-triaden som har högst prioritet.

2.1.2 Integritet

Enligt Harley och Cooper (2021) förutsätter effektiv användning av information datakvalitet. Definitionerna av datakvalitet är dock flera, men egenskaper som exempelvis att data ska vara exakt (eng. *accuracy),* aktuell (eng. *timeliness)* samt konsekvent (eng. *consistency)* är alla en del av datakvalitet (Harley & Cooper, 2021). Här argumenterar Harley och Cooper (2021) för att integritet har en viktig roll. Detta eftersom integritet är den egenskap som syftar på att samtliga behöriga användare ska delges riktig information och inte information som, i något avseende, är modifierad eller korrupt (Andress, 2014; Dhillon & Backhouse, 2000; Harley & Cooper, 2021; Nyak & Rao, 2014; SIS, 2015). Integritet säkerställer således att information inte, medvetet eller omedvetet, modifieras eller raderas av användare (Andress, 2014). Detta avser dock inte endast åverkan från obehöriga, utan det kan även vara behöriga användare som bidrar till att integriteten inte kan upprätthållas (Andress, 2014).

2.1.3 Tillgänglighet

Nyak och Rao (2014) hävdar att tillgänglighet är en kritisk egenskap i det föränderliga affärsklimatet som ställer allt högre krav på ett skyndsamt beslutsfattande. Även om företag behöver säkerställa att konfidentialitet samt integritet bevaras bör detta inte ske på bekostnad av informationens tillgänglighet (Nyak & Rao, 2014). Detta eftersom egenskapen tillgänglighet avser säkerställa att information är disponibel för behöriga användare vid samtliga situationer som informationen i fråga erfordras (Andress, 2014; Dhillon & Backhouse, 2000; Nyak & Rao, 2014; SIS, 2015).

2.1.4 Kritik mot CIA-triaden

Inom området informationssäkerhet är CIA-triaden en vedertagen modell (Andress, 2014; Dhillon & Backhouse, 2000; Nyak & Rao, 2014), vilken praktiker tillämpar för att erhålla en förståelse för informationssäkerhet i organisationer (Samonas & Cross, 2014). Oavsett påträffas litteratur som, i något avseende, kritiserar CIA-triaden.

I en artikel redogör Samonas och Coss (2014) för akademikers kritik mot CIA-triaden. De skriver att akademiker påstår att CIA-triaden försummar de sociotekniska aspekterna av informationssäkerhet. Å andra sidan påstår Dhillon och Backhouse (2000) att de tre egenskaperna i CIA-triaden är bra för att beskriva informationssäkerhet i en organisation, men kritiserar modellen för att inte vara heltäckande. I likhet med Samonas och Coss (2014) påstår även Dhillon och Backhouse (2000) att CIA-triaden främst fokuserar på de tekniska säkerhetsåtgärder som kan implementeras för att bevara de tre egenskaperna i CIA-triaden. Ovanstående är problematiskt eftersom informationssäkerhet inte ska anses vara endast ett tekniskt område, utan även inkludera både processer och människor (Baker & Wallace, 2007; Dhillon & Backhouse, 2001; Ghaffari, Gharaee & Arabsorkhi, 2019; Siponen, 2005). Samonas och Coss (2014) poängterar dock att akademiker inte förkastar CIA-triaden, utan att de snarare avser komplettera modellen med ytterligare egenskaper som tar hänsyn till de sociotekniska aspekterna av informationssäkerhet.

2.2 Alternativa modeller till CIA-triaden

Enligt Samonas och Coss (2014) förekommer det framför allt åtta förslag på egenskaper som akademiker hävdar bör komplettera CIA-triaden. Några exempel på dessa egenskaper är autenticitet (eng. *authenticity),* tillit (eng. *trust),* etik (eng. *ethicality),* integritet (eng. *integrity of people)* respektive ansvar (eng. *responsibility)* (Samonas & Coss, 2014). En del av ovanstående egenskaper påträffas i konkurrerande modeller till CIA-triaden (jmf. Dhillon & Backhouse, 2000; Parker, 1998). Nedan presenteras två alternativa modeller till CIA-triaden, vilka påträffas i litteraturen.

2.2.1 Rite

Dhillon och Backhouse (2000) kritiserar CIA-triaden och presenterar RITE, vilket är en modell med fyra egenskaper. Dessa egenskaper är ansvar (eng. *responsibility),* integritet (eng. *integrity),* tillit (eng. *trust)* respektive etik (eng. *ethicality)* (Dhillon och Backhouse, 2000). Vidare hävdar Dhillon och Backhouse (2000) att ansvar samt tillit är egenskaper som är kritiska i framför allt större organisationer, specifikt de som är geografiskt spridda eller inte har en vertikal organisationsstruktur. Detta eftersom direkt kontroll inte är möjligt i dessa organisationer, samtidigt som anställda behöver ta eget ansvar utifrån det ansvarsområde som följer med respektive arbetsroll (Dhillon & Backhouse, 2000). Integritet avser däremot att avgöra vilka anställda som ska ha tillgång till viken information, vilket är viktigt eftersom anställdas lojalitet inte bör tas för givet (Dhillon & Backhouse, 2000). Avslutningsvis omfattar egenskapen etik informella normer, vilka anställda i en organisation förväntas agera efter (Dhillon & Backhouse, 2000).

2.2.2 Parkerian hexad

Ytterligare en alternativ modell till CIA-triaden är Parkerian hexad (Andress, 2014; Nyak & Rao, 2014). Modellen, vilken tar utgångspunkt i CIA-triaden, adderar ytterligare tre egenskaper för en mer omfattande och precis beskrivning av informationssäkerhet (Parker, 1998). Dessa tre egenskaper är ägandeskap (eng. *possession),* autenticitet (eng. *authenticity)* respektive användbarhet (eng. *utility)* (Parker, 1998).

Enligt Parker (1998) har egenskapen integritet i Parkerian hexad en något annan innebörd än integritet i CIA-triaden. Parker (1998) skriver att integritet snarare syftar på att information ska vara komplett, medan autenticitet är den egenskap som säkerställer att information är giltig och genuin. Andress (2014) förtydligar och påstår att autenticitet handlar om att information ska kunna härledas till den som äger, alternativt den person som ursprungligen skapat informationen. Vidare förklarar Parker (1998) att användbarhet syftar på om information är användbar för en användare eller inte. Andress (2014) poängterar att egenskapen är abstrakt, men ger möjlighet att beskriva användbarhet utan att tillgänglighet behöver diskuteras. Avslutningsvis lyfter Parker (1998) ägandeskap, vilket framför allt syftar på stöld av fysisk utrustning. Egenskapen gör det därmed möjligt att mer precist beskriva fysisk förlust av information, utan att andra egenskaper som exempelvis tillgänglighet behöver ha påverkats (Andress, 2014). Enligt Andress (2014) ger hexaden, i jämförelse med CIA-triaden, en mer fullständig beskrivning av informationssäkerhet. Å andra sidan argumenterar Andress (2014) för att Parkerian hexad inte är lika vedertagen som CIA-triaden.

2.2.3 Varför CIA-triaden för informationssäkerhet hos mikroföretag

Nedan följer en motivering till varför CIA-triaden tillämpas i denna studie, trots att det förekommer kritik och alternativa modeller.

Gupta och Hammond (2005) påstår att småföretag med mindre än 500 anställda saknar personal med sakkunskap inom informationssäkerhet, samtidigt som de har begränsade finansiella resurser att allokera på konsulter. Mikroföretag är inget undantag och således är det i allmänhet en lekman med begränsade IT-kunskaper som ansvarar för informationssäkerhet i dessa företag (Heidenreich, 2017). Vidare har mikroföretag en simpel organisationsstruktur (Talu, 2020), samtidigt som de har mindre resurser att spendera på informationssäkerhet (Heidenreich, 2019). Till skillnad från större företag är mikroföretag i allmänhet också beroende av en enskild dator (Heidenreich, 2019). Enligt Monev (2020) specificerar CIA-triaden de mest vitala kraven inom informationssäkerhet, samtidigt som modellen är flexibel och kan expanderas vid behov. Detta innebär att CIA-triaden är lämplig även för de organisationer som har en lägre mognad inom informationssäkerhet och således arbetar med mer grundläggande säkerhetsåtgärder (Monev, 2020). Med ovanstående i åtanke kan en grundläggande modell som CIA-triaden vara tillräcklig för att beskriva hur mikroföretag arbetar med informationssäkerhet.

Vidare kommer Samonas och Coss (2014) fram till slutsatsen att samtliga åtta egenskaper som akademiker föreslår bör expandera CIA-triaden kan betraktas som underkategorier till de tre egenskaperna i CIA-triaden. Exempelvis påstår de att ansvar respektive autenticitet ingår i egenskapen integritet, medan tillit är en underkategori till både integritet och konfidentialitet. Med denna definition kan CIA-triaden därför täcka de sociotekniska aspekterna som modellen kritiserats för att förbise (Samonas & Coss, 2014), vilket motiverar val av modell trots kritik. De egenskaper som RITE innehåller är egenskaper som Samonas och Coss (2014) argumenterar för kan ingå i CIA-triaden. Dessa egenskaper (se avsnitt 2.2.1) är möjligen även mindre relevanta för mikroföretag som har få anställda. Detta eftersom (Dhillon & Backhouse, 2000) beskriver flera av egenskaperna som särskilt viktiga för större organisationer med en geografiskt utspridd verksamhet. Därav tillämpas RITE inte i denna studie.

Avslutningsvis anses en mer omfattande beskrivning av informationssäkerhet med Parkerian hexad inte nödvändigt för att beskriva informationssäkerhet hos mikroföretag. Detta med hänsyn till att CIA-triaden är en grundläggande modell, vilken kan vara tillräcklig för företag med begränsad informationssäkerhet (Kaila & Nyman, 2018; Monev, 2020).

2.3 Informationssäkerhet kopplat till människor, processer och teknologi

Informationssäkerhet är inte något som går att uppnå, utan det är snarare en kontinuerlig process som sker genom förbättringar med hänsyn till de förändringar som sker i en organisation (Ghaffari, Gharaee & Arabsorkhi, 2019). Informationssäkerhetsarbetet kan därför beskrivas som en långsiktig interaktion mellan människor, processer samt teknologi (eng. *people, processes and technology*) (Andress, 2003). För att ta fram adekvata säkerhetsåtgärder som kan bevara egenskaperna i CIA-triaden är det därför viktigt att arbeta med både människor, processer och teknologi (Ghaffari, Gharaee & Arabsorkhi, 2019; Nyak & Rao, 2014). Således bör inget område uteslutas, utan en kombination av säkerhetsåtgärder inom respektive område bör eftersträvas (Ghaffari, Gharaee & Arabsorkhi, 2019).

2.3.1 Människor

Nyak och Rao (2014) påstår att det utan människor varken finns behov av, eller möjlighet till, informationssäkerhet. Ursprungligen fokuserade informationssäkerhet dock framför allt på det tekniska, men när fler människor började interagera med nätverk och teknik uppstod nya behov (Wood, 2004). Här påstår Bulgurcu, Cavusoglu och Benbasat (2010) att människor är en viktig aspekt av informationssäkerhet som inte bör åsidosättas framför de tekniska aspekterna. Detta eftersom det är företagets anställda som dagligen nyttjar verksamhetens information (Bulgurcu, Cavusoglu & Benbasat, 2010). Därmed är det också anställda som får hantera hot, vilket exempelvis kan vara virus (Wood, 2004). Människor kan därför vara en tillgång i arbetet med att reducera risker (Bulgurcu, Cavusoglu & Benbasat, 2010; Nyak & Rao, 2014), men samtidigt är de också den svagaste länken i informationssäkerhet då det är möjligt att utsätta människor för sociala manipuleringsattacker (eng. *social engineering attacks*) (Bulgurcu, Cavusoglu & Benbasat, 2010; Kotkova & Hromada, 2021; Nyak & Rao, 2014).

Sammanfattningsvis har detta område således fokus på hur de anställda i praktiken ska arbeta för att skydda information, men också hur detta arbetssätt ska ligga i linje med de policyer som tidigare etablerats (Nyak & Rao, 2014).

2.3.2 Processer

Processer beskriver planering, implementation samt design av de policyer och processer som relaterar till informationssäkerhetsarbetet i en organisation (Ghaffari, Gharaee & Arabsorkhi, 2019). Initialt tas policyer fram för att beskriva hur en organisation ska arbeta med informationssäkerhet (Nyak & Rao, 2014). Därefter tas processer fram för att guida de anställda i hur deras arbete i praktiken ska utföras för att bevara konfidentialitet, integritet samt tillgänglighet (Nyak & Rao, 2014). Då organisationer är i förändring, samt att omvärlden ställer nya krav, är det viktigt att dessa policyer kontinuerligt uppdateras (Nyak & Rao, 2014).

2.3.3 Teknologi

De tekniska säkerhetsåtgärderna är fortfarande viktiga att implementera för att skydda information (Nyak & Rao, 2014). Gemensamt för dessa är att de ska vara en möjliggörare och således bidra till affärsprocesser och informationssäkerhet, snarare än att styra hur dessa ska verkställas (Ghaffari, Gharaee & Arabsorkhi, 2019; Nyak & Rao, 2014). Teknologierna måste dock väljas utifrån hela organisationen och ska passa in i befintliga affärsprocesser samt de krav som finns på informationssäkerhet (Nyak & Rao, 2014).

2.4 Säkerhetsåtgärder

Renaud och Weir (2016) påstår att tidigare studier indikerar på att SME framför allt implementerar de mest grundläggande säkerhetsåtgärderna inom informationssäkerhet. Med detta i åtanke samt avsikten att inkludera samtliga tre område människor, processer respektive teknologi följer nedan en presentation av ett urval av säkerhetsåtgärder som påträffas i litteraturen. Detta i syfte att öka förståelsen för de säkerhetsåtgärder som mikroföretag möjligtvis implementerat och arbetar med.

2.4.1 Människor

Skydd mot sociala manipuleringsattacker

Sociala manipuleringsattacker utnyttjar i allmänhet människors tillit samt vilja att hjälpa till och lyda order (Nyak & Rao, 2014). Eftersom sociala manipuleringsattacker inte angriper hårdvara och mjukvara direkt, utan riktar in sig på personerna som nyttjar dem, måste säkerhetsåtgärder involvera slutanvändare (Syafitri, Shukur, Mokhtar, Sulaiman & Ibrahim, 2022). Litteraturen lyfter grundläggande säkerhetsåtgärder för att skydda användare från sociala manipuleringsattacker:

> (1) Anslut inte enheter, som till exempel USB, i datorer eller liknande utrustning om de inte kommer från en säker och trovärdig källa (Kotkova & Hromada, 2021).
>
> (2) Kontrollera namnet på hemsidan som besöks i syfte för att säkerställa att det inte skett en omdirigering till en skadlig hemsida (Kotkova & Hromada, 2021).
>
> (3) Öppna inte e-mail eller bifogade filer från okända avsändare (Kotkova & Hromada, 2021). Även om dessa ser ut att ha skickats från bekanta avsändare ska exempelvis adressen kontrolleras (Syafitri et al. 2022). Detta eftersom en avsändare kan försöka utge sig för att vara någon de inte är, exempelvis en högt uppsatt i företaget (Syafitri et al. 2022).
>
> (4) Verifiera alltid att de personer som ges tillgång till företagets område de facto är de som de utger sig för att vara (Nyak & Rao, 2014). Detta eftersom det förekommer sociala manipuleringsattacker där personer utger sig för att vara anställda i ett företag som ska inspektera, alternativt laga, något i företagets lokaler (Nyak & Rao, 2014).

Ovanstående rekommendationer bör en organisation specificera i en policy, samtidigt som de anställda kontinuerligt bör utbildas i att identifiera och hantera sociala manipuleringsattacker (Kotkova & Hromada, 2021; Nyak & Rao, 2014).

Utbildning

När ett företag har tagit fram en, eller flera, policyer gällande informationssäkerhet behöver dessa kommuniceras till företagets anställda (Andress, 2014). Detta görs i allmänhet via ett säkerhetsmedvetenhetsprogram (eng. *security awareness programs*), vilket bör ske nära inpå anställning och därefter vid regelbundna intervall (Andress, 2014). Den utbildning som organisationer tillhandahåller anställda bör inte vara generell för samtliga anställda, utan målet bör vara att alla slutanvändare upplever att de lär sig något nytt (Keller et al. 2005). Vidare är det viktigt att anställda lär sig det som är nödvändigt för att skydda organisationens information utifrån den arbetsroll de besitter (Keller et al. 2005).

2.4.2 Processer

Policy

En informationssäkerhetspolicy, även benämnd för ISP (eng. *Information security policy),* definierar i allmänhet arbetsroller samt vilket ansvar respektive arbetsroll har för att skydda

organisationens information och teknologi (Bulgurcu, Cavusoglu & Benbasat, 2010). En ISP preciserar även instruktioner och riktlinjer för hur anställda i praktiken ska agera för att skydda organisationens informationstillgångar (Bulgurcu, Cavusoglu & Benbasat, 2010; Nyak & Rao, 2014).

Enligt Bhaskar och Kapoor (2013) bör en ISP ha stöd från högsta ledningen, samtidigt som den även behöver accepteras av övriga anställda. Bulgurcu, Cavusoglu och Benbasat (2010) instämmer och poängterar att det är avgörande att anställda också följer den ISP som etablerats. Här lyfter Bulgurcu, Cavusoglu och Benbasat (2010) fram vikten av ISP medvetenhet (eng. *ISP awareness).* Detta syftar på att anställda ska ha kunskap om de riktlinjer som preciserats i företagets ISP, men också förstå varför riktlinjerna behövs för att skydda verksamhetens information (Bulgurcu, Cavusoglu & Benbasat, 2010). Vad som bör stå i en informationssäkerhetspolicy beror dock på en organisations specifika behov (Bhaskar & Kapoor, 2013). Exempelvis påverkar organisationsstorlek samt värdet på informationen vilken typ av policy som är adekvat för organisationen i fråga (Bhaskar & Kapoor, 2013). Nedan följer en kort beskrivning av ett urval policyer som kan etableras:

> (1) En åtkomstkontrollspolicy (eng. *access control policy*) beskriver vilka roller i en organisation som ska ha tillgång till exempelvis olika system och information (Nyak & Rao, 2014). Enligt Watad, Washah och Perez (2018) är ovanstående centralt eftersom alla anställda inte alltid behöver ha tillgång till all information, utan endast den information som är nödvändig för arbetsrollen. Även riktlinjer kring lösenordsstyrka och med vilken frekvens lösenord bör bytas kan ingå i denna typ av policy (Bhaskar & Kapoor, 2013).
>
> (2) En *clean desk policy* är grundläggande för organisationer som hanterar känslig information i pappersformat (Andress, 2014). Denna policy ska exempelvis tydliggöra att information inte får ligga framme på skrivbord (Andress, 2014). Vidare kan denna typ av policy beskriva hur anställda ska kassera information, vilket exempelvis kan vara att alla papper ska strimlas (Andress, 2014).
>
> (3) En säkerhetskopieringspolicy (eng. *backup policy*) kan exempelvis beskriva intervallet för säkerhetskopiering, hur återställning av data ska göras samt hur företaget ska förvara säkerhetskopior (Bhaskar & Kapoor, 2013).
>
> (4) En kommunikationspolicy är en policy som ämnar att beskriva hur de anställda ska kommunicera med hjälp av IS på ett säkert sätt (Bhaskar & Kapoor, 2013).

Riskhantering

Informationssäkerhet i en organisation kan påverkas av flera risker, vilka behöver arbetas med proaktivt via riskhantering (Nyak & Rao, 2014). Alla steg i en riskhantering bygger på varandra och behöver utföras korrekt för att kunna utmynna i ett resultat som är av värde för organisationen (Katsikas, 2013). Det första steget, riskidentifiering, består generellt av att undersöka vilka värdefulla tillgångar organisationen har samt vilka hot det finns mot dessa, ofta utifrån CIA-triaden (Nyak & Rao, 2014). Nästa steg, riskanalys, inkluderar analys av hur stor sannolikhet det är att risken inträffar samt vilka effekter det potentiellt kan ha på organisationen (Nyak & Rao, 2014). Det tredje steget, riskhantering, syftar till att välja ut åtgärder som ska reducera, undvika eller överföra risken samt att skapa en riskhanteringsplan

(Katsikas, 2013). När en riskhanteringsplan är etablerad är nästa steg utförande av riskhanteringsplaner, vilket innebär att de proaktiva åtgärderna implementeras och att de anställda som behöver träning erhåller det (Nyak & Rao, 2014). Avslutningsvis ska riskbedömningar kontinuerlig utföras (Nyak & Rao, 2014). Detta eftersom en organisations infrastruktur, teknologi samt kompetens hos medarbetare kan förändras och därav ställa nya krav på riskhanteringen (Nyak & Rao, 2014).

2.4.3 Teknologi

Antivirusprogram

Antivirusprogram är mjukvara som skyddar mot olika typer av skadlig programvara, vilket exempelvis kan vara virus och spionprogram (Nyak & Rao, 2014). Genom att skanna filer kan dessa program identifiera skadlig programvara (Chen, 2013; Nyak & Rao, 2014). Vidare kan antivirusprogram rensa infekterade enheter samt identifiera, varna och eventuellt åtgärda säkerhetsrisker i ett system (Chen, 2013; Nyak & Rao, 2014). Dessa program kan även exempelvis förhindra att användare besöker osäkra webbsidor (Nyak & Rao, 2014).

Antivirusprogram ger dock inte ett fullständigt skydd mot skadlig programvara (Nyak & Rao, 2014; Tsochev et al. 2020). Detta eftersom nya hot snabbt utvecklas (Tsochev et al. 2020), men även för att människor kan brista i sin användning genom att exempelvis ignorera varningar från antivirusprogram (Nyak & Rao, 2014). För att erhålla ett bättre skydd mot nya typer av hot är det därför viktigt att genomföra de senaste uppdateringarna (Keller et al. 2005; Nyak & Rao, 2014; Watad, Washah & Perez, 2018).

Brandväggar

En grundläggande säkerhetsåtgärd inom nätverkssäkerhet är brandväggar (eng. *firewalls)* (Chen, 2013), vilka ämnar skydda information i ett nätverk (Nyak & Rao, 2014). Detta syfte uppnås genom att brandväggar kontrollerar ingående, men också utgående, trafik (Andress, 2014; Chen, 2013; Fulp, 2013; Nyak & Rao, 2014). Vilken trafik som tillåts i ett nätverk beror på en uppsättning regler, vilka en brandvägg filtrerar all trafik utefter (Keller et al. 2005; Nyak & Rao, 2014).

Det förekommer olika typer av brandväggar, både de som skyddar ett privat nätverk och de som skyddar en enskild dator (Chen, 2013; Fulp, 2013; Nyak & Rao, 2014). En nätverksbrandvägg avser att skydda ett helt nätverk och utgör i allmänhet det första skyddslagret som appliceras mellan ett internt nätverk och ett externt, vilket vanligtvis är internet (Andress, 2014; Chen, 2013; Fulp, 2013; Nyak & Rao, 2014). Utöver nätverksbrandväggar finns även mjukvarubrandväggar, vilket är mjukvara som installeras på en specifik dator för att skydda denna (Fulp, 2013; Nyak & Rao, 2014). Mjukvarubrandväggar finns redan integrerade i de flesta operativsystem (Fulp, 2013), vilka kontinuerligt bör uppdateras (Keller et al. 2005).

Fysiska säkerhetsåtgärder

Fysiska säkerhetsåtgärder ämnar skydda information från fysiska hot som exempelvis, brand, stöld, strömavbrott, naturkatastrofer och sabotage (Nyak & Rao, 2014). I praktiken innebär detta att företag behöver skydda exempelvis lokaler, utrustning, nätverksutrustning samt hårdvara från fysiska hot (Andress, 2014; Nyak & Rao, 2014). Andress (2014) beskriver tre kategorier av fysiska säkerhetsåtgärder, varav första kategorin omfattar avskräckande

säkerhetsåtgärder som exempelvis vakthundar och skyltar om kameraövervakning. Andra kategorin inkluderar säkerhetsåtgärder som ämnar att upptäcka och rapportera, vilket kan vara brandlarm och kameraövervakning (Andress, 2014). Sista kategorin omfattar i stället preventiva åtgärder, vilka exempelvis är staket och lås på dörrar (Andress, 2014). Ytterligare exempel på fysiska säkerhetsåtgärder är att låsa in datorer, anlita vakter samt använda passerkort för anställda (Nyak & Rao, 2014).

Kryptering

Kryptering är en del av kryptografi, vilken ämnar skydda information från de individer som inte bör ta del av informationen i fråga (Andress, 2014; Nyak & Rao, 2014). Kryptering avser därför konvertera läsbar information till en skyddad, icke läsbar, version (Andress, 2014; Nyak & Rao, 2014). Denna kan sedan konverteras tillbaka med hjälp av en krypteringsnyckel, vilket benämns för dekryptering (Andress, 2014; Nyak & Rao, 2014).

Det finns olika typer av kryptering (Andress, 2014; Nyak & Rao, 2014). Symmetrisk kryptering innebär att kryptering respektive dekryptering görs med samma krypteringsnyckel (Andress, 2014; Nyak & Rao, 2014). Vid asymmetrisk kryptering förekommer det två krypteringsnycklar, en för kryptering respektive en för dekryptering (Andress, 2014; Nyak & Rao, 2014). Ytterligare en krypteringsteknik är hashfunktioner, vilket innebär att en matematisk funktion genererar ett specifikt fastställt hashvärde (Andress, 2014; Nyak & Rao, 2014). Om ett meddelande ändras kommer även hashvärdet förändras, vilket resulterar i att hashvärdet inte matchar det förberäknade värdet (Andress, 2014; Nyak & Rao, 2014). Det förekommer olika situationer där kryptering kan användas, men två exempel är digitala signaturer respektive krypterade e-mail (Nyak & Rao, 2014).

Säkerhetskopiering

Målet med säkerhetskopiering är att ta kopior av den information som är essentiell för företagets verksamhet och spara denna på en annan plats än där originalet lagras (Jayadevappa & Soh, 2009). Detta för att göra det möjligt att återställa information som, av någon anledning, blivit korrupt eller raderats (Nyak & Rao, 2014).

Det förekommer olika metoder för att säkerhetskopiera (Nyak & Rao, 2014). Fulla säkerhetskopieringar innebär att det tas en kopia av hela systemet, medan inkrementella fungerar som ett komplement till den fulla och sparar endast de filer som blivit ändrade under dygnet (Nyak & Rao, 2014). Differentiella säkerhetskopieringar är också ett komplement och tar vid varje tillfälle kopior av alla de filer som ändrats sedan den senaste fulla säkerhetskopieringen (Nyak & Rao, 2014). Dessa kopior kan sparas på exempelvis externa hårddiskar eller i molnet (Nyak & Rao, 2014). Vidare bör säkerhetskopieringar genomföras regelbundet (Jayadevappa & Soh, 2009; Nyak & Rao, 2014; Tsochev et al. 2020), men intervallet bör vara realistiskt i förhållande till företagets resurser (Tsochev et al. 2020).

Åtkomstkontroll

Åtkomstkontroll består av autentisering respektive auktorisering, där autentisering syftar på att identifiera användare och auktorisering på att ge eller neka åtkomst baserat på användarens roll (Nyak & Rao, 2014). Åtkomstkontroll ämnar således kontrollera och hanterar vilka användare som ges åtkomst till nätverk, system samt data (Andress, 2014; Nyak & Rao, 2014). Detta kan exempelvis vara att begränsa vem som har åtkomst till datorrum, filer eller resurser som exempelvis skrivare på ett nätverk (Nyak & Rao, 2014).

Ett exempel på en grundläggande åtkomstkontroll är lösenord (Andress, 2014). Starka lösenord som hanteras rätt kan vara en effektiv åtkomstkontroll (Andress, 2014), men dessa får inte skrivas ner eller förvaras åtkomligt för andra (Keller et al. 2005). Ett starkt lösenord bör bestå av både stora och små bokstäver, men också symboler och siffror (Andress, 2014). Samma lösenord ska inte användas för flera olika inloggningar (Andress, 2014). Vidare ska lösenord regelbundet bytas ut (Nyak & Rao, 2014).

2.5 Teoretisk resultat

Nedan presenteras studiens teoretiska resultat, vilket är utgångspunkt för de intervjufrågor som används för insamling av empirisk data i syfte för att besvara studiens forskningsfråga. Syftet med det teoretiska resultatet är att koppla ihop de område och modeller som beskrivits i litteraturgenomgången (se avsnitt 2). Vidare avser avsnittet att motivera varför säkerhetsåtgärderna kan vara relevanta för mikroföretag. Då det, som tidigare nämnt i studiens problemområde (se avsnitt 1.2), finns få studier som beskriver hur mikroföretag bör arbeta med informationssäkerhet använts rekommendationer för SME.

2.5.1 Människor

Skydd mot sociala manipuleringsattacker

Watad, Washah och Perez (2018) rekommenderar småföretag med färre än 100 anställda att informera och utbilda anställda om hur de kan skydda sig mot sociala manipuleringsattacker. Gällande CIA-triaden påstår Nyak och Rao (2014) att denna kategori av säkerhetsåtgärder främst bevarar egenskaperna integritet respektive konfidentialitet. Detta eftersom sociala manipuleringsattacker kan resultera i att känslig och konfidentiell information läcker ut, men även att information modifieras (Nyak & Rao, 2014). Syafitri et al. (2022) påstår å andra sidan att det främst är konfidentialitet som bevaras eftersom attackerna främst ämnar avslöja konfidentiell information. Denna åsikt delas av Kotkova och Hromada (2021) som skriver att de flesta attackers motiv är att få tillgång till information.

Utbildning

Keller et al. (2005) rekommenderar utbildning inom informationssäkerhet för anställda på SME. Rekommendationen delas av Watad, Washah och Perez (2018) som vidare förklarar att utbildning är av sådan vikt att även om det endast genomförs informella utbildningar bör de utföras. Då utbildning kan ske inom flera olika aspekter inom informationssäkerhet kan utbildning potentiellt bevara samtliga egenskaper i CIA-triaden (Nyak & Rao, 2014).

2.5.2 Processer

Policy

Tidigare studier argumenterar för att SME bör etablera policyer som berör företagens informationssäkerhet (Gupta & Hammond, 2005; Keller et al. 2005; Watad, Washah & Perez, 2018). Vilka, eller vilken, typ av policy som krävs beror dock på organisationens specifika behov (Gupta & Hammond, 2005; Keller et al. 2005; Watad, Washah & Perez, 2018). Däremot visar Gupta och Hammond (2005) studie att småföretag, till skillnad från stora, mer

sällan har en nedskriven informationssäkerhetspolicy. Två anledningar till detta kan vara begränsningar av IT-kunskap samt finansiella resurser (Gupta & Hammond, 2005). Eftersom en informationssäkerhetspolicy kan beröra flera områden kan den syfta på att bevara olika egenskaper i CIA-triaden (Nyak & Rao, 2014).

Enligt Watad, Washah och Perez (2018) bör SME åtminstone etablera en åtkomstpolicy. Vidare betonar Keller et al. (2005) vikten av att SME ska ha en lösenordspolicy, vilket Watad, Washah och Perez (2018) påstår är viktigt även för småföretag. Ovanstående två policyer syftar främst på att bevara egenskaperna konfidentialitet respektive integritet (Nyak & Rao, 2014).

Riskhantering

Rees (2010) argumenterar för att riskhantering är fundamentalt för SME att genomföra, vilket även Gupta och Hammond (2005) påstår. Detta eftersom de säkerhetsåtgärder som SME väljer att implementera bör anpassas efter företagets unika riskprofil (Paulsen, 2016). Enligt Heidenreich (2019) är mikroföretag inget undantag, utan även de bör identifiera risker för att implementera de säkerhetsåtgärder som är adekvata för företaget i fråga. Eftersom riskhantering berör alla delar av informationssäkerhet kan riskhantering skydda samtliga egenskaper i CIA-triaden (Nyak & Rao, 2014).

2.5.3 Teknologi

Antivirusprogram

Skadlig programvara kan exempelvis resultera i stulna bankuppgifter, dataförlust, korrupta filer samt kraschade hårddiskar och operativsystem (Nyak & Rao, 2014). Därför ämnar antivirusprogram skydda samtliga tre egenskaper i CIA-triaden (Nyak & Rao, 2014). Vidare är antivirusprogram en grundläggande säkerhetsåtgärd inom informationssäkerhet (Chen, 2013; Nyak & Rao, 2014; Tsochev et al. 2020), vilken även är adekvat för SME (Keller et al. 2005; Rees, 2010; Watad, Washah & Perez, 2018). Antivirusprogram bör därför installeras på samtliga datorer i ett företag (Keller et al. 2005), men även surfplattor och telefoner kan behöva skyddas med antivirusprogram (Tsochev et al. 2020).

Brandväggar

Brandväggar avser att bevara och säkerställa integritet, konfidentialitet samt tillgänglighet (Fulp, 2013; Nyak & Rao, 2017). Brandväggar skyddar således privata nätverk från externa hot (Chen, 2013). Detta kan exempelvis vara *Denial of Service attacker* (DoS-attack) som riskerar att göra ett nätverk otillgängligt och därav påverka tillgängligheten (Nyak & Rao, 2014). Ett annat exempel är att obehöriga kommer åt information, vilket kan resultera i att konfidentialitet inte kan upprätthållas (Nyak & Rao, 2014). Alla företag bör därför implementera brandväggar (Tsochev et al. 2020), vilket är en rekommendation som även gäller för SME (Keller et al. 2005; Kurpjuhn, 2015; Rees, 2010; Watad, Washah & Perez, 2018). Fulp (2013) poängterar dock att vilken typ av brandvägg som är adekvat för ett företag beror på situation samt vilken information ett företag behöver skydda.

Fysiska säkerhetsåtgärder

Enligt Nyak och Rao (2014) kan de fysiska säkerhetsåtgärderna skydda samtliga egenskaper i CIA-triaden. Andress (2014) påstår dock att dessa säkerhetsåtgärder framför allt avser att

säkerställa tillgänglighet. Exempelvis påverkar både bränder, fysisk skada på utrustning samt naturkatastrofer tillgänglighet (Nyak & Rao, 2014). Stöld och sabotage riskerar däremot att inte bara påverka tillgänglighet, utan även konfidentialitet (Nyak & Rao, 2014). Vidare skriver Andress (2014) att information som lagras i fysisk media också behöver skyddas för att säkerställa integritet. Detta eftersom exempelvis temperatur och fukt kan påverka fysisk media, vilket potentiellt kan resultera i att integritet inte kan upprätthållas (Andress, 2014). Företag bör därför vidta fysiska säkerhetsåtgärder i syfte för att skydda information (Tsochev et al. 2020), vilket är en rekommendation även för SME (Keller et al. 2005; Watad, Washah & Perez, 2018).

Kryptering

Eftersom kryptering ska förhindra att obehöriga får tillgång till information ämnar kryptering främst att bevara egenskapen konfidentialitet i CIA-triaden (Andress, 2014; Nyak & Rao, 2014). Även om fokus ligger på konfidentialitet, bevarar kryptering dock även integritet (Andress, 2014; Harley & Cooper, 2021; Nyak & Rao, 2014). Watad, Washah och Perez (2018) påstår dock att småföretag i allmänhet saknar processer för att hantera kryptering. Detta är problematiskt eftersom även småföretag bör använda sig utav kryptering (Watad, Washah & Perez, 2018).

Säkerhetskopiering

Företag som arbetar med säkerhetskopiering kan ha bättre förutsättningar att hantera korrupta filer, manipulerad data, system som kraschar samt förlust av data (Nyak & Rao, 2014). Säkerhetskopiering avser därför att säkerställa tillgänglighet, men också bevara integritet (Nyak & Rao, 2014). Under förutsättning att säkerhetskopiering sker regelbundet är det en effektiv säkerhetsåtgärd (Keller et al. 2005), vilken även SME bör implementera (Keller et al. 2005; Rees 2010; Watad, Washah & Perez, 2018).

Åtkomstkontroll

Åtkomstkontroll avser att förhindra att obehöriga får tillgång till information och således förebygga att information exempelvis stjäls, raderas eller manipuleras (Nyak & Rao, 2014). Således ska åtkomstkontroll bevara egenskaperna konfidentialitet och integritet i CIA-triaden (Nyak & Rao, 2014). Watad, Washah och Perez (2018) rekommenderar att småföretag ska ha i åtanke om alla anställda behöver tillgång till all data och även restriktioner på vem som har fysisk tillgång till hårdvara. Vidare rekommendationer för småföretag är att anställda ska ha starka lösenord där ett lösenord inte får delas av flera anställda (Keller et al. 2005; Watad, Washah & Perez, 2018). Vidare bör även småföretag undvika att använda samma lösenord till ett konto under en längre period (Watad, Washah & Perez, 2018).

2.5.4 Litteratursammanställning

Nedan följer en sammanställning av studiens litteraturgenomgång samt en beskrivning respektive avsnitts syfte.

Tabell 1: Litteratursammanställning

Avsnitt	Syfte med avsnitt	Litteratur
Informationssäkerhet och CIA-triaden (Avsnitt 2.1)	Avsnittet avser att definiera vad informationssäkerhet är, vad det ämnar skydda samt vilken definition som tillämpas i studien. Vidare avser avsnittet att presentera, en för studien, relevant modell.	Andress (2014); Dhillon och Backhouse, (2000); Harley och Cooper (2021); Nyak och Rao (2014); Samonas och Coss, (2014); SIS (2015); Siponen (2005); von Solms och van Niekerk (2013);
Alternativa modeller till CIA-triaden (Avsnitt 2.2)	Avsnittet presenterar alternativa modeller till CIA-triaden i syfte för att belysa vilka övriga modeller som utvärderats. Vidare avser avsnittet att beskriva varför CIA-triaden kan vara adekvat för att beskriva informationssäkerhet hos mikroföretag.	Andress (2014); Dhillon och Backhouse (2000); Gupta och Hammond (2005); Heidenreich (2017); Kaila och Nyman (2018); Monev (2020); Parker (1998); Samonas och Coss (2014); Talu (2020)
Informationssäkerhet kopplat till människor, processer och teknologi (Avsnitt 2.3)	Detta avsnitt avser beskriva vilka olika typer av säkerhetsåtgärder SME bör implementera för att arbeta med informationssäkerhet och bevara egenskaperna i CIA-triaden.	Andress (2003); Bulgurcu, Cavusoglu och Benbasat (2010); Ghaffari, Gharaee och Arabsorkhi (2019); Kotkova och Hromada (2021); Nyak och Rao (2014); Wood (2004)
Säkerhetsåtgärder (Avsnitt 2.4)	Syftet med avsnittet är att kortfattat beskriva ett urval av grundläggande säkerhetsåtgärder. Detta för att öka förståelsen för de säkerhetsåtgärder som mikroföretag möjligtvis kan ha implementerat och arbetar med.	Andress (2014); Bhaskar och Kapoor (2013); Bulgurcu, Cavusoglu och Benbasat, (2010); Chen, (2013); Fulp (2013); Gupta och Hammond (2005); Jayadevappa och Soh (2009); Katsikas (2013); Keller et al. (2005); Kotkova och Hromada, (2021); Nyak och Rao (2014); Renaud och Weir (2016); Syafitri et al. (2022); Tsochev et al. (2020); Watad, Washah & Perez (2018)
Litteraturresultat (Avsnitt 2.5)	Detta avslutande avsnitt ämnar koppla ihop de modeller och område som beskrivits i litteraturgenomgången. Vidare avser avsnittet att presentera vilka säkerhetsåtgärder som SME och mikroföretag rekommenderas att implementera.	Andress (2014); Chen (2013); Fulp (2013); Gupta och Hammond (2005); Harley och Cooper (2021); Heidenreich (2017); Heidenreich (2019); Keller et al. (2005); Kotkova och Hromada (2021); Nyak och Rao (2014); Paulsen (2016); Rees (2010); Syafitri et al. (2022); Tsochev et al. (2020); Watad, Washah och Perez (2018)

Följande tabell sammanfattar studiens teoretiska resultat. Symbolen * indikerar på att vilken, eller vilka, egenskaper som säkerhetsåtgärden avser bevara kan variera beroende på åtgärdens innehåll och omfattning.

Tabell 2: Sammanställning teoretisk resultat

	Konfidentialitet	**Integritet**	**Tillgänglighet**
Skydd mot sociala manipuleringsattacker	x	x	
Utbildning*	x	x	x
Policy*	x	x	x
Riskhantering*	x	x	x
Antivirusprogram	x	x	x
Brandväggar	x	x	x
Fysiska säkerhetsåtgärder	x	x	x
Kryptering	x		
Säkerhetskopiering		x	x
Åtkomstkontroll	x	x	

3 Metod

Följande kapitel avser beskriva, men också motivera, studiens tillvägagångssätt och metodval. Inledningsvis presenteras och motiveras val av kvalitativ data, urval, datainsamling samt tillvägagångssätt för analys av kvalitativ data. Därefter redogörs för studiens litteraturstudie med fokus på söktermer. Avslutningsvis diskuteras studiens kvalitet med fokus på validitet, reliabilitet samt etiska aspekter.

3.1 Metodval

3.1.1 Kvalitativ metod

Oates (2006) skriver att kvalitativa metoder lägger tyngdpunkt på insamling samt analys av icke-numerisk data, medan kvantitativa metoder i stället förknippas med insamling och analys av numerisk data. Nedan följer en motivering till varför en kvalitativ metod anses adekvat för att besvara studiens forskningsfråga.

Jacobsen (2002) redogör för två kategorier av forskningsfrågor, vilka är deskriptiva samt kausala forskningsfrågor. De deskriptiva forskningsfrågorna ämnar beskriva ett område, medan de kausala forskningsfrågorna omfattar mer än en beskrivning och i stället avser att förklara varför något är som det är (Jacobsen, 2002). Beslut om studiens tillvägagångssätt har tagits med hänsyn till studiens forskningsfråga, vilken i linje med Jacobsen (2002) definition är deskriptiv. Detta eftersom studien inte ämnar förklara varför mikroföretag arbetar med informationssäkerhet på ett specifikt sätt, utan endast beskriva hur de arbetar med detta vid en given tidpunkt. Som studiens problemområde (se avsnitt 1.2) antyder förefaller det, enligt vår kännedom, existera få tidigare studier som undersöker hur specifikt mikroföretag arbetar med informationssäkerhet. Avsaknaden av tidigare studier resulterar således i begränsade förkunskaper om det studien ämnar undersöka, vilket enligt Jacobsen (2002) kännetecknar en oklar forskningsfråga.

Till skillnad från kvantitativa metoder förutsätter en kvalitativ metod inte förkunskaper om det som ska studeras, varav någon form av kvalitativ metod är adekvat för oklara forskningsfrågor (Jacobsen, 2002). Eftersom studiens forskningsfråga är oklar motiveras valet av en kvalitativ metod. Vidare ger en kvalitativ metod även förutsättning för att samla in både djupgående och nyanserad data, vilket kan bidra till ökad förståelse för det som studeras (Jacobsen, 2002). Med begränsad kännedom om hur mikroföretag arbetar med informationssäkerhet bedöms kvalitativ data vara adekvat för att undersöka studiens forskningsfråga. Detta eftersom kvalitativ data kan ge en mer detaljerad beskrivning av hur mikroföretag arbetar, snarare än att endast presentera statistik över exempelvis vilka säkerhetsåtgärder de implementerat. Kvalitativa metoder resulterar dock i allmänhet i låg generaliserbarhet (Jacobsen, 2002), vilket inte bedöms som en nackdel för denna studie. Detta eftersom studien ämnar tillhandahålla en beskrivning, varav vi väljer lägga större vikt vid detaljerad data snarare än att eftersträva ett resultat som kan generaliseras.

3.1.2 Intervjuer

Informationssäkerhet är i allmänhet ett känsligt ämne för företag att diskutera med externa parter (Kotulic & Clark, 2004), vilket påverkade val av tillvägagångssätt. För att samla in kvalitativ data genomfördes intervjuer. Detta eftersom Oates (2006) menar att intervjuer är det tillvägagångssätt som passar bäst för att undersöka känsliga ämnen. Vidare pekar Kotulic och Clark (2004) specifikt på att studier om informationssäkerhet bör välja intervjuer framför enkätundersökningar. Detta eftersom flera tidigare studier inom ämnesområdet erhållit låg svarsfrekvens på enkätundersökningar (Kotulic & Clark, 2004). Intervjuer valdes också eftersom de gav oss möjlighet att introducera oss för respondenter. Detta för att bygga förtroende, vilket Kotulic och Clark (2004) menar är kritiskt för studier inom informationssäkerhet. Vidare valdes intervjuer för att ha möjlighet att låta respondenter med ord, utifrån egna erfarenheter, beskriva hur företaget arbetar med informationssäkerhet.

Val av intervjustruktur föll på semistrukturerade intervjuer, vilket Oates (2006) skriver är en intervjustruktur som utgår från en uppsättning fördefinierade intervjufrågor i en intervjuguide. Enligt Oates (2006) behöver en intervjuguide dock inte strikt följas, utan frågor kan både strykas och adderas efter behov. Denna intervjustruktur valdes således för att ha möjlighet att följa en intervjuguide och säkerställa att viktiga frågor berörs, men också för att stryka frågor som exempelvis respondenten redan besvarat. Detta i linje med Oates (2006) som skriver att det är viktigt att ha möjlighet att stryka, men också addera frågor, för att få ett bättre flöde i en intervju. Denna typ av intervju valdes även för att ha möjlighet att ställa följdfrågor anpassade efter varje specifik intervjusituation.

3.1.3 Urval

För att tillfråga, för studien, relevanta respondenter och företag definierades en uppsättning urvalskriterier med utgångspunkt i studiens syfte och forskningsfråga. Vidare anses endast mikroföretag relevanta för att besvara studiens forskningsfråga. I linje med European Commission (u.å.) definition av mikroföretag omfattar studien därför endast företag med maximalt nio anställda samt en balansomslutning, eller årlig omsättning, som understiger två miljoner euro. De bolagsformer som ingår i studiens urval är enskild firma respektive aktiebolag (AB). Gällande urval av respondenter i respektive mikroföretag har ägare av enskilda bolag, alternativt VD i ett AB, intervjuats.

Inledningsvis kontaktades VD, alternativt ägare, till mikroföretag i vårt eget kontaktnät. Dessa kontakter resulterade i vissa fall i kontaktuppgifter till andra mikroföretag som kunde tillfrågas. De respondenter som ingår i studiens slutliga urval är de respondenter som fanns tillgängliga, vilket Jacobsen (2002) beskriver som ett bekvämlighetsurval. I linje med Kotulic och Clark (2004) som hävdar att studier om informationssäkerhet bör fokusera på ett fåtal respondenter för att bygga förtroende, valde vi att intervjua totalt sex respondenter. I nedan tabell presenteras respondenternas roll, antal anställda i företaget samt inom vilket område mikroföretagen är verksamma.

Tabell 3: Presentation respondenter

Respondent	Roll	Antal anställda	Bransch
R1	VD	1	Juridik
R2	VD	1	Redovisning
R3	Ägare	1	Detaljhandel
R4	Ägare	1	Detaljhandel
R5	VD	5	Tillverkning
R6	Ägare	1	Hälso- och sjukvård

3.2 Intervjuer

3.2.1 Utformning av intervjufrågor

Oates (2006) skriver att en intervjuguide ska konstrueras innan semistrukturerade intervjuer genomförs. Därför formulerade vi en intervjuguide (se appendix 3) med utgångspunkt i studiens litteraturgenomgång (se avsnitt 2) innan intervjuprocessen initierades.

I linje med Oates (2006) rekommendationer inleddes respektive intervju med bakgrundsfrågor, alternativt frågor relaterade till medgivande och etiska aspekter. Eftersom informationssäkerhet kan vara ett känsligt ämne för företag (Kotulic & Clark, 2004), var målsättningen att formulera frågor som inte upplevs för specifika. Exempelvis frågor om exakt vilket antivirusprogram företaget använder eller var eventuella övervakningskameror är placerade. Eftersom tidigare studier poängterar att SME i allmänhet saknar IT-personal (Gupta & Hammond, 2005; Heidenreich, 2017; Keller et al. 2005; Kurpjuhn, 2015), var målsättningen även att formulera frågor som en person utan erfarenhet om IT och informationssäkerhet kan förstå. Detta ligger i linje med Oates (2006) rekommendationer om att undvika akademiska termer.

Enligt Oates (2006) bör intervjufrågor vara öppna. I praktiken innebär detta att intervjufrågor exempelvis inleds med "*hur"* och därav erfordrar mer detaljerade svar än endast exempelvis ja eller nej (Oates, 2006). Med hänsyn till studiens syfte och forskningsfråga valde vi att huvudsakligen formulera öppna frågor. Detta för att erhålla en mer detaljerad beskrivning av hur respektive mikroföretag arbetar med informationssäkerhet. Vidare valde vi, i linje med Jacobsens (2002) rekommendationer, att undvika att formulera ledande frågor som potentiellt kan influera respondenternas svar. För flera frågor valde vi dock att förbereda exempel ifall

att respondenten inte skulle förstå vad en fråga syftar på. Dessa exempel har också använts som stöd för att ställa följdfrågor under respektive intervju.

Tabell 4: Intervjufrågor

Exempel på frågor (se appendix 3)	Kategori	Litteraturgenomgång
Har du tagit del av informationen ovan? Vill du ha ett exemplar av transkriberingen?	Medgivande/etik	
Vilken roll har du i detta företag? Hur många personer arbetar i detta företag?	Bakgrundsfrågor	
Hur definierar du informationssäkerhet?	CIA-triaden: Konfidentialitet, integritet & tillgänglighet	Avsnitt 2.1: Informationssäkerhet och CIA-triaden
Vet du vilken information som är viktig att skydda för ditt företag?	CIA-triaden: Konfidentialitet, integritet & tillgänglighet	Avsnitt 2.5.5: Riskhantering
Hur arbetar ni för att säkerställa att obehöriga inte ska få tillgång till företagets information?	CIA-triaden: Konfidentialitet, (integritet)	Avsnitt 2.1.1: Konfidentialitet Avsnitt 2.5.1: Skydd mot sociala manipuleringsattacker
Hur kommunicerar ni och delar känslig information? Hur säkerställer ni att den kommer till rätt mottagare?	CIA-triaden: Konfidentialitet	Avsnitt 2.1.1: Konfidentialitet
Har alla anställda tillgång till all information?	CIA-triaden: Konfidentialitet	Avsnitt 2.1.1 Konfidentialitet Avsnitt 2.5.10 Åtkomstkontroll
Hur arbetar ni för att verksamhetens information alltid är rätt? Dvs att den inte råkar raderas eller att någon går in och ändrar något som inte ska ändras.	CIA-triaden: Integritet	Avsnitt 2.1.2: Integritet Avsnitt 2.5.10 Åtkomstkontroll
Hur arbetar ni med säkerhetskopiering?	CIA-triaden: Integritet, tillgänglighet	Avsnitt 2.5.9: Säkerhetskopiering
Hur arbetar ni för att säkerställa att information alltid finns tillgänglig när den behövs?	CIA-triaden: Tillgänglighet	Avsnitt 2.1.3: Tillgänglighet
Hur avgör ni vilka säkerhetsåtgärder ni behöver tillämpa för att skydda företagets information?	CIA-triaden: Konfidentialitet, integritet & tillgänglighet	Avsnitt 2.5.5: Riskhantering
Har ni etablerat en informationssäkerhetspolicy?	CIA-triaden: Konfidentialitet, integritet & tillgänglighet	Avsnitt 2.5.3: Policy
Utbildar ni på företaget er inom informationssäkerhet på något vis?	CIA-triaden: Konfidentialitet,	Avsnitt 2.5.2: Utbildning

	integritet & tillgänglighet	
Vad använder ni för tekniska säkerhetsåtgärder för skydda er information?	CIA-triaden: Konfidentialitet, integritet & tillgänglighet	Avsnitt 2.5.6 Brandväggar, Avsnitt 2.5.5 Antivirus, Avsnitt 2.5.8 Kryptering Avsnitt 2.5.7 Fysiska säkerhetsåtgärder Avsnitt 2.5.9 Säkerhetskopiering Avsnitt 2.5.10 Åtkomstkontroll
Hur arbetar ni med fysiska säkerhetsåtgärder?	CIA-triaden: Konfidentialitet, integritet & tillgänglighet	Avsnitt 2.5.7 Fysisk säkerhet
Hur är er tanke kring lösenord?	CIA-triaden: Konfidentialitet & integritet	Avsnitt 2.5.3 Policy Avsnitt 2.5.10 Åtkomstkontroll

3.2.2 Intervjuförfarande

Den initiala kontakten med respondenter var via e-mail där vi bifogade en förfrågan om att delta i studien (se appendix 1). Vi valde även att bifoga ett informationsblad (se appendix 2) som vi bad respondenten att läsa igenom inför en eventuell intervjun. Därefter bokades en tid för intervju in.

Vi valde att inte skicka ut intervjufrågorna i förväg. Detta eftersom intervjuerna planerades att vara semistrukturerade. Vi ville därav undvika att respondenterna skulle ställa sig frågande till om inte alla frågorna de informerats om kom med eller om det adderades frågor som inte hade skickats till dem. Dock var vi noga med att informera om ämnet och syftet med intervjuerna. Detta ligger i linje med Oates (2006) rekommendationer om att skicka ämne, alternativt frågor, innan en intervju för att låta respondenten förbereda sig.

Vi prioriterade att genomföra intervjuerna fysiskt på plats hos företagen, men anpassade tillvägagångssätt utefter respondenternas önskemål. Detta eftersom Jacobsen (2002) redogör för *kontexteffekten,* vilken betyder att respondenter påverkas av omgivningen. Därför bör intervjuer ske på en plats som respondenten känner sig trygg i (Jacobsen, 2002). På grund av avstånd och respondentens önskemål genomfördes dock en intervju digitalt via Zoom.

Båda författarna har varit närvarande vid samtliga intervjuer. Dock har varje författare haft ansvar för olika uppgifter under intervjuerna. En var huvudansvarig för att genomföra intervjun och ställa frågor, medan en i stället hade ansvar för att föra anteckningar och flika in vid behov. Intervjuerna inleddes med att vi presenterade oss samt studiens syfte. Vidare gick vi muntligt igenom informationsbladet (se appendix 2) och frågade om medgivande. Om medgivande gavs av respondenten startades ljudupptagningen och intervjufrågorna började ställas. Vi valde att göra ljudupptagningar för att kunna få en fullständig återgivning av intervjun i efterhand. Detta ligger i linje med Jacobsens (2002) rekommendationer som även belyser att ljudupptagningar är fördelaktiga. Detta eftersom risken för att datainsamlingen formas av intervjuarens intresse eller förmåga att anteckna minskar (Jacobsen, 2002).

Anteckningarna var främst en säkerhetsåtgärd ifall ljudupptagningen blev otydlig på något ställe.

Tabell 5: Sammanställning intervjuer

Respondent	Intervjutyp	Längd	Appendix
R1	Digital	27 min	Appendix 4
R2	Fysisk	20 min	Appendix 5
R3	Fysisk	18 min	Appendix 6
R4	Fysisk	17 min	Appendix 7
R5	Fysisk	33 min	Appendix 8
R6	Fysisk	23 min	Appendix 9

3.2.3 Transkribering och analys av empiri

Det är enklare att analysera kvalitativ data i skriftlig form än i ljudinspelningar (Oates, 2006), varav vi valde att transkribera samtliga ljudinspelningar. Vidare påpekar Oates (2006) vikten av att ordagrant transkribera vad som sägs på ljudinspelningar, samtidigt som ord som exempelvis "ehh" kan raderas under förutsättning att det inte påverkar betydelsen av det som sägs. Vi har valt att ta bort ord som upprepas samt exempelvis "ehh", "hmm" och "öh" i samtliga transkriberingar. I de situationer som skratt anses ha betydelse för sammanhanget markeras detta med [skrattar]. En mening som blir avbruten, alternativt tystnad, markeras med tre punkter. Ovanstående är i syfte för att öka läsbarheten av transkriberingarna. I de fall vi behövt ta bort ord från transkriberingarna markeras detta med [borttaget]. Detta gäller delvis ord som kan härledas till en respondent eller ett mikroföretag, men vi har även valt att ta bort namn på exempelvis virusprogram och larmleverantörer. I övrigt har vi inte ändrat i transkriberingarna, vilket resulterar i att samtliga transkriberingar står i talspråk snarare än i skriftspråk. Detta kan dock påverka läsbarheten negativt, men vi valde att prioritera att ordagrant återge respondenterna framför att översätta till korrekt skriftspråk.

I linje med Oates (2006) rekommendationer initierades analysen med att vi läste igenom allt material i sin helhet samt identifierade, för forskningsfrågan, relevanta segment. Enligt Oates (2006) är kategorisering av kvalitativ data en fördelaktig metod för att strukturera, och därefter analysera materialet. Med utgångspunkt i Oates (2006) rekommendationer har vi därför valt att kategorisera materialet i nio kategorier (se tabell 6), vilka alla associeras med en egen färgkod. Alla kategorier konstruerades med utgångspunkt i studiens teoretiska resultat (se avsnitt 2.5) där respektive färg representerar en specifik säkerhetsåtgärd. För att ha möjlighet att härleda koppling till CIA-triaden har vi även valt att använda koder, en kod för respektive egenskap i CIA-triaden (se tabell 7).

Tabell 6: Färgkoder

Säkerhetsåtgärder	Färgkod
Skydd mot sociala manipuleringsattacker	Blå
Utbildning	Grön
Policy	Röd
Riskhantering	Gul
Antivirusprogram	Orange
Brandväggar	Rosa
Fysiska säkerhetsåtgärder	Mörkblå
Kryptering	Mörkgul
Säkerhetskopiering	Mörkgrön
Åtkomstkontroll	Turkos

Tabell 7: Koder

Huvudområde	Kod
Konfidentialitet	K
Integritet	I
Tillgänglighet	T

3.3 Tillvägagångssätt för litteraturstudie

Utöver datainsamling av kvalitativ data omfattar studien även en litteraturstudie, vilken i linje med Oates (2006) rekommendationer syftar på att erhålla en förståelse för området samt identifiera vad tidigare forskning studerat.

För att hitta artiklar har vi sökt i databaserna *LUBSearch, LUBCat, IEEE Xplore, ACM Digital Library, AIS Digital Library* samt *Google Scholar.* För att finna relevanta artiklar användes olika söktermer, individuellt eller i kombination. Ett urval av de söktermer som tillämpades för att hitta artiklar om informationssäkerhet hos SME är följande: "*Small business", "Information Security", "SME", "SMME", "Small Enterprise", "Information Security Controls",* samt "*Micro Business".* Sökkombinationen "*information security"* AND "*SME"* gav flera, för studien, relevanta artiklar. Efter genomgång av ett antal artiklar inom ämnesområdet påträffades begrepp som "*IT-security", "computer security"* samt *"cyber security".* Eftersom vi initialt fann få studier om informationssäkerhet hos SME breddades vår sökning med dessa termer. Ytterligare söktermer som använts för att hitta artiklar är: "*Information security", "Threats", "Challenges", "CIA triad".* De artiklar som söktes fram

genererade i flera fall ytterligare artiklar via referenslistor. Där blev det även tydligt vilka artiklar som var mer väl citerade inom ämnesområdet.

Artiklar som är "*peer reviewed"* prioriterades i litteratursökningen. Detta för att säkerställa högsta möjliga nivå av kvalitet och reliabilitet i studierna. Vidare utvärderade vi artiklar efter exempelvis publiceringsår samt i vilken tidskrift som artikeln publicerats i. Vi har även försökt hitta information om tidskrifters *"impact factor"* samt konferensers "*rejection rate"*. Vidare försökte vi finna artiklar som publicerats i tidskrifter som omnämns i AIS *"Senior Scholars' Basket of Journals"* (AIS, u.å.), men flera av artiklarna som citeras i denna studie har inte publicerats i tidskrifter som nämns där.

3.4 Etik

Inom forskning är det enligt Oates (2006) essentiellt att göra etiska övervägande samt ta hänsyn till de rättigheter som alla deltagare i en studie har. I syfte för att säkerställa att hela intervjuprocessen, men även studien som helhet, uppfyller etiska krav har vi valt att specifikt följa de fem etiska krav och rekommendationer som Oates (2006) lyfter fram.

De två först rättigheterna som Oates (2006) redogör för är att individer ska delta i en studie av egen fri vilja samt att de när som helst under en process kan återkalla medverkan. I samband med att potentiella deltagare kontaktades informerade vi om att det är frivilligt att delta samt att de kan avbryta medverka under hela processen. Jacobsen (2002) hävdar dock att individer kan känna sig pressade till att delta, även om det explicit inte uttalats något tvång. Innan respektive intervju påbörjades informerades respondenterna återigen muntligt om ovanstående två rättigheter. I informationen som varje deltagare fick läsa innan en intervju informerades de även om att de har rätt att hoppa över frågor, utan att ange anledning till detta. Med detta ville vi återigen belysa för respondenterna att deltagande är frivilligt och att det inte finns några krav på att de ska delge oss information.

Enligt Oates (2006) syftar den tredje rättigheten på informerat samtycke, vilket endast kan ges om en respondent är väl införstådd med vad ett deltagande i en studie innebär för individen i fråga. I praktiken betyder detta att en respondent måste erhålla information om vem som utför studien, studiens syfte samt hur data kommer användas i studien (Oates, 2006). För att uppfylla detta krav har samtliga respondenter fått läsa igenom ett informationsblad (se appendix 2) med den information som Oates (2006) poängterar som viktig. Vi var också noga med att informera om att det rör sig om en kandidatuppsats som skrivs av två studenter på det systemvetenskapliga programmet vid Lunds universitet. Dock skriver Jacobsen (2002) att det i praktiken inte går att säkerställa om en deltagare har förstått vad medverkan i en studie faktiskt innebär. Vi är medvetna om denna risk och valde därför att inleda en intervju med att fråga om respondenten har frågor angående informationsbladet. Detta för att få respondenten att reflektera över informationen och ta upp eventuella tveksamheter.

Enligt Oates (2006) handlar de två sista rättigheterna om konfidentialitet respektive anonymitet. Med hänsyn till att informationssäkerhet kan vara ett känsligt ämne för företag (Kotulic & Clark, 2004), valde vi att lägga särskild vikt vid dessa två aspekter. Detta för att respondenterna ska vara trygga med att den information de delger oss inte ska kunna härledas till vare sig individen eller företaget i fråga. Därför informerades respondenterna redan i förfrågan att information som kan härledas till individen eller företaget inte kommer

inkluderas i studien. Vidare valde vi att lägga vikt vid dessa aspekter för att säkerställa att information som framkommer under intervjuerna inte kan användas av andra personer för att attackera de företag som medverkat. Vi ansåg att varken namn, ålder, kön, företagsnamn samt företagets placering är av intresse för studien och därav har dessa uppgifter utelämnats. Gällande konfidentialitet valde vi att spara samtliga ljudfiler lokalt på våra privata datorer i en lösenordskyddad mapp.

Avslutningsvis tar Jacobsen (2002) upp ytterligare en rättighet som ska tillgodoses i studier, vilken är samtliga deltagares rätt att framställas på ett sätt som är korrekt. För att bidra till att alla respondenter upplever att de framställs på ett rättvisande sätt samt att vi inte har begått misstag i transkriberingarna erbjöd vi varje respondent möjlighet att läsa igenom sin egen transkribering. Detta var också i syfte för att respondenterna ska kunna ta bort information som de inte är bekväma med att delge i denna studie.

3.5 Reliabilitet och validitet

3.5.1 Reliabilitet

Jacobsen (2002) beskriver att begreppet *reliabilitet* syftar på om en undersöknings slutsatser, men även resultat, kan anses vara pålitliga eller inte. En åtgärd som vidtogs i syfte för att öka studiens reliabilitet var att samtliga intervjuer spelades in. Detta eftersom vi bedömer att risken för felaktigheter i datamaterialet hade varit högre om vi endast tagit anteckningar och i stället försöka komma ihåg vad som sagts under respektive intervju. Jacobsen (2002) lyfter ytterligare en anledning till ljudupptagning och transkribering, vilket är möjligheten till att andra kan kontrollera rådata och se om de slutsatser vi dragit är riktiga och trovärdiga.

Jacobsen (2002) beskriver att kvalitativa studier kan drabbas av en *intervjuareffekt*, vilket i praktiken innebär att en respondent influeras av den eller de som genomför en intervju. När intervjuerna genomfördes var vi medvetna om risken. Även om vi försökte agera på liknande sätt under alla intervjuerna var det i praktiken svårt att uppnå, vilket även Jacobsen (2002) bekräftar. För att minska skillnaderna mellan respondenternas intervjuer närvarade båda författarna samt hade samma roller vid samtliga intervjuer som genomfördes. Detta eftersom Jacobsen (2002) argumenterar för att alla respondenter bör utsättas för liknande stimulans, vilket är svårt att uppnå om olika personer intervjuar. Det har även gjorts försök till att inte lägga värdering i frågorna när de ställs då vi ville undvika i den grad det gick att respondenten upplevde att våra frågor antydde att de borde ha en viss säkerhetsåtgärd. Det är dock inte möjligt att utesluta att studiens resultat ändå har påverkats av intervjuareffekten.

3.5.2 Validitet

Begreppet *validitet*, vilket vidare kan delas upp i *extern* respektive *intern validitet*, belyser om en studies resultat kan anses vara giltigt eller inte (Jacobsen, 2002). Jacobsen (2002) förklarar att en studie som har hög *intern validitet* mäter det som studien ämnar undersöka. I syfte för att nå högre intern validitet formulerades därför intervjufrågorna med utgångspunkt i studiens litteraturgenomgång (se avsnitt 2) samt studiens teoretiska resultat (se avsnitt 2.5).

Det föreligger viss risk för att respondenter avsiktligt väljer att undanhålla information, vilket kan påverka en studies validitet (Jacobsen, 2002). Vi har försökt ta hänsyn till konfidentialitet och anonymitet enligt tidigare beskrivning för att respondenterna ska kunna känna att de kan delge oss information. Det går dock inte att utesluta att ovanstående påverkat studiens validitet. Jacobsen (2002) förklarar vidare att *extern validitet* handlar om en studies generaliserbarhet. Detta innebär att slutsatser och resultat från en studie med låg extern validitet inte bör generaliseras till en större population (Jacobsen, 2002). Vi har inte vidtagit några specifika åtgärder för öka studiens externa validitet.

4 Resultat

Följande kapitel ämnar presentera studiens resultat. Kapitlet inleds med en redogörelse av hur respondenterna definierar informationssäkerhet samt övergripande hur de arbetar för att bevara de tre egenskaperna i CIA-triaden. Därefter presenteras vilka säkerhetsåtgärder mikroföretagen implementerat och arbetar med.

4.1 Informationssäkerhet och CIA-triaden

När respondenterna tillfrågas hur de definierar informationssäkerhet erhålls varierande svar. R4 svarar att hen inte har en uppfattning om vad informationssäkerhet är (R4, 20). R3 berättar i stället att hen inte funderat på det, men utvecklar och säger att informationssäkerhet syftar på att skydda datorn från virus (R3, 26). Å andra sidan svarar R6 att informationssäkerhet handlar om att skydda information från obehöriga (R6, 22). En definition som delvis delas av både R1, R2 och R5 (R1, 51; R2, 22). R2 vidareutvecklar och förklarar att informationssäkerhet, utöver att skydda information från obehöriga, även omfattar källkritik och lösenord (R2, 22). Även R1 utvecklar och nämner:

> *"[...] det första man tänker på är ju att någon extern kommer åt mina filer eller låser dem och vill ha betalt för att låsa upp. Det är överhuvudtaget att någon kommer åt det som finns i min dator på ett eller annat vis. Det kan ju vara genom att stjäla datorn också i och för sig." (R1, 50)*

R5 förklarar att informationssäkerhet även handlar om risker (R5, 12).

> *"Informationssäkerhet för mig är…Jag ser det som att det är en risk i första hand. Och att man ska skydda sig emot, var man för sin data helt enkelt. Hur säkert är den plattformen, om det är på webben. Vem ansvarar för den? Hur kan vi på bästa sätt säkra vår information? [...]" (R5, 12)*

Gällande upprätthållande av konfidentialitet berättar ingen respondent om någon säkerhetsåtgärd som inte kan kategoriseras under de tio säkerhetsåtgärder som denna studie specifikt redogör för. När respondenterna i stället tillfrågas hur de säkerställer att information är rätt, det vill säga hur de bevarar egenskapen integritet, säger R2 att hen inte säkerställer det eftersom hen litar på programmen i molnet (R2, 62–64). R1 berättar däremot att hen använder skannade PDF-filer för att säkerställa integritet eftersom de är svårare att redigera än exempelvis Word-filer (R1, 78). R5 säger att de har manuell hantering där information förs över till systemen, varav de kontrollerar att informationen som matats in också blir korrekt (R5, 55–59). Liknande säger R6 att hen kontrollerar viktig information för att säkerställa att den skrivits in på rätt sätt (R6, 48). Senare nämner även R5 att det är viktigt att information är uppdaterad och aktuell, vilket säkerställs genom att ha anställda har olika ansvarsområde om vem som ska uppdatera vad (R5, 75).

Två respondenter uttrycker att de inte arbetar på något specifikt sätt för att säkerställa egenskapen tillgänglighet (R1, 85; R3, 76). R1 berättar att *"jag arbetar inte alls för det, det sköts automatiskt. Alltså man är ju oerhört handlingsförlamad och strandsatt när internet lägger ner. [...] " (R1, 85).* Liknande säger R3 att *"[...] Allt ligger i datorn. Jag har inget speciellt sätt för att säkerställa att det är tillgängligt) (R3, 76).* Vidare berättar R5 att *"vi jobbar ju mest bara med program, så den informationen finns alltid där. [...]" (R5, 75).* En gemensam nämnare är dock att samtliga respondenter uttrycker att de är beroende av internet (R1, 85; R2, 74; R3, 79; R4, 72; R5, 79; R6, 70). Vidare säger fyra respondenter att de är beroende av en enskild dator för att information ska vara tillgänglig (R1, 87; R2, 68; R3, 89; R4, 78). R2, R3 samt R6 vidareutvecklar och förklarar dock att de inte är bundna till sin specifika dator, utan att information finns i molnet och därför kan nås via en annan dator (R2, 86; R3, 89; R6, 68).

4.2 Säkerhetsåtgärder

4.2.1 Människor

Skydd mot sociala manipuleringsattacker

Gällande skydd mot sociala manipuleringsattacker tar majoriteten av respondenterna framför allt upp risken med e-mail och länkar. R2, R5 samt R6 berättar alla att de är uppmärksamma på riskerna med e-mail och länkar, varav de inte klickar på suspekta länkar (R2, 148; R5, 128, 130; R6, 144). R1 förklarar att "[...] *jag avgör själv vilka mail jag öppnar. Om det är något misstänkt skräpmail så får jag avgöra själv om det kan vara något lurt." (R1, 89).* R4 poängterar i stället att alla e-mail som ser konstiga ut raderas (R4, 93).

Tre respondenter tar upp ytterligare säkerhetsåtgärder. R2 berättar att ett antivirusprogram skannar de filer som laddas ner, samt att det finns en motvilja att ansluta USB som kommer från externa parter även om arbetet idag kräver det (R2, 148). Både R3 och R4 nämner i stället bluffakturor och poängterar att de är uppmärksamma på detta (R3, 64; R4, 62).

Utbildning

Gemensamt för samtliga respondenter är att de själv inte har någon tidigare utbildning inom informationssäkerhet. Vidare är det inget av de mikroföretag som intervjuats som säger att de utbildar företagets anställda inom informationssäkerhet. R5 utvecklar och förklarar varför utbildning inte upplevs vara relevant för företaget i fråga:

> *"[...] känslan är nog att vi är lite för få, men samtidigt är det väl också att ju mer vi lägger upp. Igen, jag ser första prioritet som att det är internet som är risken. Och ju mer vi litar på det, eller förlitar oss på det så kan det vara nyttigt att alla får information. Vad, hur och när man ska göra saker och vilka risker man utsätter sig för och kunderna. Och hur man hanterar det på bättre sätt [...]. Så vi kanske kommer dit där, men just nu så är det inte så att vi har lagt tid på det." (R5,103)*

Fyra respondenter berättar dock att de på egen hand tar reda på information gällande informationssäkerhet (R2, 102; R3, 108; R4, 89; R5, 146). R5 inhämtar information om informationssäkerhet, men nämner inte från vilken källa (R5, 146). R2 berättar att "*jag försöker prata med nära vänner och bekanta. [...]. För att ta reda på vad jag kan på eget håll [...]" (R2, 102).* Å andra sidan berättar två respondenter om en mer passiv och osystematisk kunskapsinhämtning. R4 säger här att "*det är ju mest om man läser något i tidningen. [...]" (R4, 89–91).* R3 utvecklar och uttrycker:

> *"Nej, det är slumpmässigt. Det beror på om något dyker upp. Någonting någonstans om ämnet. Då kanske jag undersöker det mer, men inget systematiskt nej. Jag söker inte aktivt efter information om det." (R3, 108)*

4.2.2 Processer

Policy

Inget mikroföretag uppger att de har en nedskriven informationssäkerhetspolicy. R1 säger dock att det finns i bakhuvudet hur information ska skyddas (R1, 91). Även R2 berättar att det finns en tanke om informationssäkerhet, men vill inte benämna det för policy.

> *"Ja, men jag skulle nog aldrig säga att jag har en policy. Men ja, jag har väl en tanke som jag kan utforma från gång till gång. För det är aldrig samma. Man ställs inför många olika situationer, så det blir en ny varje gång." (R2, 88)*

R5 berättar att de inte har något de benämner för policy, men att de inom företaget pratar om informationssäkerhet.

> *"Det har vi bara muntligt. Vi har ingen direkt policy, [...] där är vissa saker som jag tycker, jag har tagit till mig, så då har det kommit ner lite på pränt. Men även om det kommer ner på papper så är det inget vi hade tittat på mer än en gång. Och sen hade vi igen bara trillat tillbaka till rutinerna, men då hade, då finns i alla fall ett papper." (R5, 91)*

Även R6 berättar att det inte finns en informationssäkerhetspolicy i mikroföretaget. Däremot vidareutvecklar R6 och förklarar varför en policy inte upplevs vara relevant.

> *"Det är väldigt liten skala på företaget. Hade jag haft anställda så tror jag att då hade det känts mer viktigt för mig, nu är det bara jag. Och så då. Känns det ja, inte aktuellt helt enkelt." (R6, 86)*

Flera respondenter nämner däremot att de har en tanke kring hur lösenord borde utformas eller inom vilket intervall de ska bytas (R1, 104, 108; R2, 36, 132; R3, 116, 120; R6, 108, 110). R2 säger dock att riktlinjen angående hur ofta lösenord ska bytas inte alltid följs (R2, 36, 128).

De två respondenter (R5 och R6) som har manuella säkerhetskopieringar har etablerat riktlinjer gällande med vilka intervall säkerhetskopieringar ska tas (R5, 67; R6, 64). Det finns även riktlinjer hos R5 som säger vilken information som ska säkerhetskopieras (R5, 69). Dock kunde R4 inte redogöra för vad som säkerhetskopieras eller vilken typ av säkerhetskopiering det rör sig om (R4, 40).

R5 berättar att hen säger till de anställda att papper med information inte får ligga framme med texten uppåt (R5, 95). R5 vidareutvecklar och förklarar att det kan finnas svårigheter med att få anställda att följa dessa riktlinjer (R5, 97–99):

> *"[...]det händer så sällan att folk kommer hit. Då blir det också att, till slut förstår ingen varför man ska göra det, för då gör de det som är lättast för dem. Att alltid ha det uppe. Så det är nog den svåraste delen [...]" (R5, 97).*

R1, R2, R3 och R5 berättar om riktlinjer för hur papper med information ska hanteras. De säger att papper med känslig information som inte längre används ska makuleras, strimlas eller rivas sönder (R1, 118; R2, 80; R3, 126; R5, 19).

Riskhantering

Ingen av respondenterna uttrycker att de gör en formell riskhantering, men flertalet nämner dock steg som finns med i en riskhantering. Gällande att ha kunskap om vilken information som är viktig att skydda anger R1, R4 samt R6 att de vet vilken information som ska skyddas (R1, 58; R4, 30; R6, 24). Däremot svarar R2 att hen inte vet, men att all information som anses vara känslig skyddas (R2, 30). Detta liknar vad R5 säger, vilket är att de inte vet vad de enligt lag är skyldiga att skydda, men att de upplever att de har en sund uppfattning om vilken information som borde skyddas (R5, 19, 25). R3 svarade att *"alltså jag vet inte. Det enda jag har att koncentrera mig på är det här med GDPR eller vad det nu heter. Att man ska skydda information om kunder." (R3, 42).*

Fyra respondenter (R1, R2, R3, R5) nämner GDPR när vilken information som bör skyddas kommer på tal (R1, 95; R2, 30; R3, 42, R5, 142). R1 har valt att ta kontakt med en jurist för att få information om skyldigheter utifrån GDPR (R1, 95). R2 och R5 uppger att de inte vet vad som gäller och att det är svårt att veta var man ska vända sig för att få information (R2, 30; R5, 144). R3 har valt att sluta med e-mailutskick till kunder då det var ett för stort projekt att sätta sig in i GDPR och sedan utföra allt regelrätt (R3, 60).

R1 och R4 berättar att de väljer att överlämna ansvaret gällande val av tekniska säkerhetsåtgärder till andra personer (R1, 46, 89; R4, 38).

> *"[...] Jag har ju en IT-konsult som har hjälpt mig att lägga upp allt jag har och som jag ringer så fort det är någonting. Och det är också han som har gjort de skydd som jag nu har utan att veta om det." (R1, 46*)

För R2 är det däremot en egen analys:

> *"Nej, så jag får själv göra en analys. Vad skulle någon kunna göra med den här informationen? Ja, inte mycket eller ja det kanske inte är så lämpligt. Det är en egen analys jag får göra." (R2, 84)*

R6 berättar att hen själv tar beslut om säkerhetsåtgärder samt att hen går på känsla om vad som bör implementeras, förutom i de fall där det finns lagkrav (R6, 76, 78). R3 nämner att beslut om säkerhetsåtgärder är något som sker efterhand och är reaktivt (R3, 101). I samband med att säkerhetskopiering diskuteras antyder även R4 att val av säkerhetsåtgärder sker reaktivt.

> *"[...] Det var bara i förra veckan igen. Någonting hände med mitt lösenord så jag kom inte in i datorn. Då var det en här och fixade det och då sa han att han även fixade en backup. Det hade jag inte innan." (R4, 38).*

Gällande beslut om vilka säkerhetsåtgärder som ska implementeras berättar R5 att de har tillit till att de försäljare som säljer mjuk- samt hårdvara ger råd om vilka lösningar som passar företagets behov (R5, 87). R5 utvecklar och redogör för en reaktiv beslutsprocess där beslut om vilka säkerhetsåtgärder som ska implementeras kan tas efter att företaget råkat ut för en händelse (R5, 89).

R1, R5 och R6 reflekterar över bristerna de uppfattar att de själva har. R5 säger att de vet att de borde bli bättre på att exempelvis ha starka lösenord och att de ska bytas ut med jämna mellanrum (R5, 119). Förklaring till varför detta inte görs idag, trots medvetenhet om bristen, är att "*...människan är lite bekväm av sig och kör på någon vana.*" (R5, 119). R1 reflekterar över att det inte är bra att ha samma lösenord på flera ställen. Reflektionen blir dock att det är svårt att komma ihåg flera olika lösenord och för att hantera detta kan man skriva ner dem, vilket resulterar i en ny risk (R1, 106). R6 är medveten om risker och lyfter att det finns en medvetenhet om att hen brister i flertalet (R6,26, 80). På följdfrågan om varför riskerna accepteras och inte hanteras berättar R6:

> *"Dels, så kan det vara lite ekonomi. Att köpa in de här grejerna. Sen är det väl att så många andra gör på ungefär samma sätt, liksom att det är lite accepterat på något sätt att ja, man gör sitt bästa, men kanske inte hela vägen. Så jag tror att det är det. Plus att jag också har känt att det är så litet." (R6, 106)*

4.2.3 Teknologi

Antivirusprogram

Samtliga respondenter uppger att de har antivirusprogram installerat på företagets datorer (R1, 74; R2, 106; R3, 30; R4, 23; R5, 27; R6, 92). R1 är dock något osäker, men säger att IT-konsulten som anlitats av företaget sannolikt har installerat ett antivirusprogram (R1, 74). Däremot är det ingen respondent som tar upp om antivirusprogram har installerats på företagets mobiltelefoner eller inte.

R2, R3 och R5 har valt att köpa till ytterligare antivirusprogram (R2, 108; R3, 52; R5, 31), medan R6 i stället har valt att endast ha det antivirusprogram som följer med operativsystemet (R6, 94). För R1 respektive R4 framgår det däremot inte om de har ytterligare antivirusprogram utöver det som följer med datorns operativsystem. Gällande uppdatering av datorer, antivirusprogram samt brandväggar uppger samtliga respondenter, utom R4, att de genomför uppdateringarna (R1, 97; R2, 114; R3, 52; R5, 27; R6, 96). Huruvida uppdateringar genomförs eller inte tas inte upp av R4.

Gällande hur ofta uppdateringar genomförs svarar R1 och R2 att de i allmänhet genomför uppdateringar direkt (R1, 97; R2, 114). R6 förklarar att uppdateringarna görs, men att det kan ta ett tag innan hen väljer att uppdatera (R6, 96). Även R3 och R5 uppdaterar, men berättar att detta sköts automatiskt (R3, 52; R5, 31).

> *"Precis och dessa uppdateras hela tiden, kontinuerligt med det nya. [...]. Jag betalar för det så då släpper jag tanken på det." (R3, 52).*

> *"[...] När det gäller virusprogram och brandvägg, då är det när vi köper tjänsten. När vi köper produkten, då köper vi också tjänsten av licenserna till det och då ska det ju sköta sig själv och uppdateras." (R5, 31)*

Brandväggar

Samtliga respondenter uppger att de har brandväggar installerade på företagets datorer (R1, 62; R2, 112; R3, 28; R4, 24; R5, 27; R6, 92). R5 utvecklar och säger att företagets server, vilken är en separat arbetsstation med en stationär dator, också har både brandvägg och antivirusprogram (R5, 33). Respondenterna diskuterar brandväggar i samband med antivirusprogram, varav fem respondenter nämner att de uppdaterar brandväggen.

Fysiska säkerhetsåtgärder

Samtliga sex mikroföretag uppger att de, i någon omfattning, arbetar med fysiska säkerhetsåtgärder. Alla respondenter säger att det finns lås på arbetsplatsen (R1, 64; R2, 44; R3, 110; R4, 46; R5, 107; R6, 98). Likaså är brandlarm ytterligare ett exempel på en fysisk säkerhetsåtgärd som alla respondenter uppger att de har vidtagit (R1, 64; R2, 120; R3, 114; R4, 104; R5, 115; R6, 102). Vidare har alla respondenter, bortsett från R4, larm på arbetsplatsen (R1, 64; R2, 44; R3, 110; R5, 107; R6, 28). R4 har dock valt att installera en övervakningskamera (R4, 97), vilket även är en fysisk säkerhetsåtgärd som R1 och R5 nämner att de har implementerat (R1, 64; R5, 107). R3 samt R4 berättar dock om en fysisk säkerhetsåtgärd som de övriga respondenterna inte nämner. R3 säger att hunden är på kontoret, vilket gör att obehöriga inte kan gå in där obemärkt (R3, 112). Liknande resonemang för R4:

> "*[...] Men alltså när jag är här i butiken så är det ju ingen som kan gå ut där för då har jag en hund som vaktar och de kommer aldrig förbi henne. Och samma med datorn, den kan dom inte heller komma åt då. Hon skyddar liksom den avdelningen där ute. Det är en levande vakt. [...].*" *(R4, 34).*

R2 berättar att den bärbara datorn låses in i ett skåp vid arbetsdagens slut (R2, 42). Detta är en fysisk säkerhetsåtgärd som även R3 berättar att de vidtar på företaget, dock endast om arbetsplatsen inte ska besökas under en längre tidsperiod (R3, 110). Vidare säger R5 att de låser det rum som den stationära dator, vilken används som server, står i (R5, 33). I motsats berättar dock R4 att de inte låser in företagets bärbara dator (R4, 108). Gällande de externa hårddiskarna berättar både R1 och R5 att de väljer att inte låsa in dessa (R1, 91; R5, 117). R6 har en extern hårddisk (R6, 58), men anger inte om de väljer att låsa in den eller inte.

Samtliga respondenter tar i något avseende upp hur fysisk information, exempelvis papper i pärmar, kan skyddas. Här berättar R2 samt R5 att pärmar och information i pappersform låses in (R2, 46; R5, 19). Skillnaden är dock att R2 inte har ett brandsäkert skåp (R2, 122), medan R5 berättar att de har ett brandsäkert kassavalv där en del information i fysisk form förvaras (R5, 155). R6 säger i stället "*[...] Vi har ju till exempel inget säkerhetsskåp, vilket i den bästa utav världar där jag förvarar mitt material skulle vara både brandsäkert och inbrottssäkert. " (R6, 98).*

Kryptering

Både R2 och R6 uppger att de använder någon form av kryptering, men att det inte handlar om att kryptera e-mail som skickas (R2, 50; R6, 90). R2 berättar att hen krypterar filer, vilket innebär att filer som skickas till kunder krypteras och lösenordskyddas.

> *"Jag lösenordskyddar via Adobe. Alla dokument i PDF eller där som jag anser är känslig information. […] sånt som jag anser att det kan bli dumt om det hamnar i fel händer." (R2, 50)*

R6 nämner däremot att någon form av kryptering sannolikt sker:

> *"Nej, men jag har fått för mig att det finns någon form av kryptering i hur det lagras uppe i Google. Vet inte, men annars krypterar jag ingenting." (R6, 90)*

Säkerhetskopiering

Samtliga respondenter berättar att de i någon omfattning säkerhetskopierar, men på vilket sätt detta görs samt vad som säkerhetskopieras skiljer sig åt mellan mikroföretagen. R1 berättar att filer säkerhetskopieras både till en extern hårddisk samt till en plattform i molnet (R1, 10, 20). Även R2 säkerhetskopierar filer, men dessa säkerhetskopior lagras i molnet och inte på en extern hårddisk (R2, 14). R2 berättar även att hen har allt i molnet, varav de system som används också ligger online (R2, 70). R4 har informerats av en person de får hjälp av att det finns en backup, men vet inte om denna är molnbaserat eller om den ligger på en extern hårddisk (R4, 36–40). R4 säger också att det framför allt är lagersystemet som säkerhetskopieras, vilket är en excelfil (R4, 10, 40–42).

Till skillnad från övriga respondenter berättar R5 om att de säkerhetskopierar till en extra stationär dator, vilken de själva benämner för server (R5, 33). För varje dator i företaget finns även en separat extern hårddisk (R5, 65). R5 berättar även att de endast säkerhetskopierar system och inte enskilda filer på datorn (R5, 65, 69). Ingenting finns på, eller säkerhetskopieras till, molnet (R5, 14). R6 säkerhetskopierar däremot både till extern hårddisk samt till en plattform i molnet (R6, 58). Eftersom systemen är molnbaserade tas dock inte säkerhetskopior på dessa (R6, 60). R6 har även viss information i pappersformat (R6, 60). Detta är även en åtgärd som R3 nämner. R3 säger att kunduppgifter finns på fysiska papper, vilka sedan har överförts till filer på datorn (R3, 66). De fysiska papperna betraktas därför som en säkerhetskopia (R3, 68). R3 har ingen extern hårddisk, men berättar att fotografier sparas både på datorns hårddisk, i molnet samt i mobiltelefonen (R3, 95–97).

R1, R2, R3 och R4 uppger att de har automatiska säkerhetskopieringar (R1, 80; R5, 69; R6, 64). R5 har automatiska överföringar till servern dagligen, men även manuella säkerhetskopieringarna som även de genomförs på daglig basis (R5, 65, 69). Även R6 har en kombination av automatiska överföringar till molnet och manuella säkerhetskopieringar (R6, 64). Säkerhetskopiering till molnet sker dagligen, medan manuella säkerhetskopieringar till en extern hårddisk sker med 50–100 dagars mellanrum (R6, 64).

Två respondenter nämner att de har fått hjälp av någon annan att välja ut metod för säkerhetskopiering, varav de inte är insatta i hur denna fungerar (R1, 48; R4, 38). Sammantaget har hälften av respondenterna (R1, R3, R6) valt att säkerhetskopiera både på externa hårddiskar och i molnet (R1, 10, 20; R3, 95, 97; R6, 58). De respondenter som har

valt olika riktningar är R2 som har allt på molnet och R5 som vill ha så lite information som möjligt i molnet.

> *"Så jag når allting där. Jag har den tanken att händer någonting så kan jag köpa en ny dator och logga in på, vad är det nu. Microsoft, Windows ja där man kan komma åt allting. Där ligger till och med skrivbordet. Alltihopa ligger där." (R2, 70)*

Respondent 5 anser att molnet är en större risk och vill därför undvika system som är molnbaserade eller säkerhetskopior som lagras i molnet.

> *"Jag har ju velat fram till nu och även om programmet också har anpassat sig till att det kan ligga i molnet så har jag ändå valt att hålla det kvar det i datorerna för jag anser att det är lite säkrare." (R5, 14)*

Åtkomstkontroll

Gällande åtkomstkontroll använder samtliga respondenter och mikroföretag lösenord i någon mån. Hur starka lösenord ska vara, med vilken frekvens de ska bytas ut samt om samma lösenord får användas på flera konto skiljer sig dock mellan mikroföretagen.

R1 och R4 berättar att ett lösenord används på mer än ett konto (R1, 108; R4, 112), medan R5 och R6 uppger att snarlika lösenord används för flera konton (R5, 119; R6, 112). Endast R2 och R3 berättar att de har helt olika lösenord till alla konton (R2, 134; R3, 122). Tvåstegsverifiering nämns av två respondenter. R1 använder det vid en inloggning (R1, 110), medan R6 har det på flera system samt betalar extra för att använda tvåstegsverifiering på ett system som inte erbjuder det i grundversionen.

> *"Jag betalar ju lite extra varje månad, till exempel för att ha det, att det skulle gå in med mobilt bankid på journalprogrammet till exempel, för det känns som ett bra val att göra." (R6, 76)*

Lösenordsstyrka varierar mellan respondenterna. R1 och R4 nämner inget om styrkan på deras lösenord, medan R6 förklarar att hen försöker att endast använda starka lösenord (R6, 112). R2 har en lösenordshanterare som även genererar lösenord om minst 16 tecken med specialtecken (R2, 132). R3 går i stället efter de kriterier som systemet rekommenderar när hen väljer lösenord (R3, 120). R5 säger att de är medvetna om att lösenorden borde vara starkare än vad de är idag (R5, 119).

Med vilken frekvens lösenord byts varierar mellan mikroföretagen. R1 byter cirka var tredje år, oftast är det när hen känner att det är samma på för många ställen (R1, 108). R2 har som mål att byta var tredje månad (R2, 36). R3 har däremot inget specificerat intervall utan det är slumpmässigt när R3 väljer att byta ut lösenorden (R3, 118). R4 berättar att hen aldrig byter sina lösenord (R4, 114). Även R5 säger att lösenord inte uppdateras (R5, 119). R6 byter inte lösenord på eget initiativ, utan det är när omständigheter kräver det såsom byte av mobiltelefon (R6, 110).

R5 förklarar att de anställda har tillgång till olika information beroende på deras roll (R5, 19, 49). Informationen i pappersform har endast de på kontoret tillgång till förutom fraktsedlarna som även de på lagret behöver tillgång till (R5, 19). Alla anställda behöver inte arbeta i alla system och i de system som flera anställda behöver tillgång till har alla egna inloggningar med unika lösenord (R5, 27). R2 delar internet med andra företag i samma kontorslokal, men

säger att de inte kan komma åt varandras information. R2 säger att "[...] *vi är ju inne på samma internet, men jag kan inte komma åt någon annans information och ingen kan komma åt min. [...]*" (R2, 142). Som en extra säkerhetsåtgärd är den kombinerade skrivaren och skannern inte uppkopplad via Wifi, utan via en nätverkskabel för att förhindra att någon som sitter på samma Wifi ska komma åt filerna som skannas.

> *"Man kan ju koppla upp sig på Wifi men då når alla ens skrivare. Så nu har jag en nätverkskabel så att jag… alltså att ingen annan kan få det jag skannar. Jag kan inte skanna det fel utan det går via nätverkskabeln in i datorn direkt." (R2, 140)*

4.3 Sammanställning av resultat

I nedan tabell sammanfattas vilka säkerhetsåtgärder som resultatet visar att mikroföretagen arbetar med. De säkerhetsåtgärder som resultatet visar att mikroföretagen delvis arbetar med markeras inte i tabellen.

Tabell 8: Sammanställning resultat

	R1	**R2**	**R3**	**R4**	**R5**	**R6**
Skydd mot sociala manipuleringsattacker						
Utbildning						
Policy						
Riskhantering						
Antivirusprogram	x	x	x	x	x	x
Brandväggar	x	x	x	x	x	x
Fysiska säkerhetsåtgärder	x	x	x	x	x	x
Kryptering		x				
Säkerhetskopiering	x	x	x	x	x	x
Åtkomstkontroll	x	x	x	x	x	x

5 Diskussion

I följande femte kapitel för författarna en diskussion kring de resultat som presenterats i föregående kapitel. Initialt berör diskussionen säkerhetsåtgärderna och sedan informationssäkerhet och CIA-triaden. Avslutningsvis förs en diskussion kring studiens valda metod.

5.1 Säkerhetsåtgärder

5.1.1 Människor

Enligt Watad, Washah och Perez (2018) bör anställda i småföretag utbildas och informeras om hur de ska agera för att skydda sig mot sociala manipuleringsattacker. Studiens resultat tyder dock på att denna typ av utbildning inte genomförs i mikroföretagen. Vidare finns, utifrån resultatet, ingen tydlig indikation på att mikroföretagen aktivt söker efter information angående vilka säkerhetsåtgärder de kan implementera för att skydda sig mot dessa attacker. Å andra sidan antyder dock resultatet att mikroföretagen, i någon omfattning, reflekterar över sociala manipuleringsattacker och hur de ska agera för att skydda sig mot dessa. Här tyder resultatet på att det framför allt handlar om att inte klicka på suspekta länkar och e-mail. Detta ligger i linje med Kotkova och Hromada (2021) rekommendationer om att inte öppna e-mail och filer från okända avsändare. Däremot berörs skydd om sociala manipuleringsattacker inte i större omfattning i studiens empiri. Därför är det inte möjligt att med säkerhet utesluta att mikroföretagen inte arbetar med fler säkerhetsåtgärder för att skydda sig mot dessa attacker.

Gällande utbildning av anställda poängterar Keller et al. (2005) att SME bör utbilda anställda om informationssäkerhet, vilket enligt Watad, Washah och Perez (2018) även inkluderar informella utbildningar. Resultatet tyder dock på att mikroföretagen inte arbetar med utbildning i någon större omfattning eftersom det inte förekommer indikationer på att de genomför formella utbildningar. Däremot tyder resultatet snarare på att ägare, alternativt VD, till mikroföretagen på egen hand inhämtar information om informationssäkerhet. Detta kan indikera på att det, i linje med Watad, Washah och Perez (2018) rekommendationer, snarare sker någon form av informell utbildning i mikroföretagen. Även om studiens resultat visar att mikroföretagen inte arbetar med utbildning i någon större omfattning kan det inte dras slutsatser om att detta är irrelevant för mikroföretag. Detta eftersom resultatet inte presenterar en tydlig anledning till att mikroföretagen inte arbetar med utbildningar, mer än att det kan röra sig om att de har för få anställda. Det kan därför spekuleras i om mikroföretag med fler anställda arbetar med utbildning i större omfattning än de mikroföretagen med endast en anställd.

Ovanstående två säkerhetsåtgärder kan, i den modell som Ghaffari, Gharaee och Arabsorkhi (2019) samt Nyak och Rao (2014) presenterar, klassificeras under kategorin människor. Således tyder resultatet på att mikroföretagen inte arbetar med kategorin människor i större omfattning. Detta går delvis emot Bulgurcu, Cavusoglu och Benbasat (2010) som argumenterar för att människor är en viktig aspekt av informationssäkerhet som således inte bör bortprioriteras.

5.1.2 Processer

SME rekommenderas att etablera en informationssäkerhetspolicy (Gupta & Hammond, 2005; Keller et al. 2005; Watad, Washah & Perez, 2018). Baserat på Bulgurcu, Cavusoglu och Benbasat (2010) samt Nyak och Rao (2014) definition av ISP visar resultatet dock att mikroföretagen inte arbetar med en skriftlig informationssäkerhetspolicy. Detta ligger i linje med de resultat Gupta och Hammond (2005) finner hos småföretag. Däremot tyder resultatet på att företagen ändå har någon form av riktlinjer för hur de vill att företaget ska arbeta med informationssäkerhet. Här är det framför allt riktlinjer för hur lösenord ska hanteras, vilket är en policy som SME rekommenderas att etablera (Keller et al. 2005; Watad, Washah & Perez, 2018). Vidare tyder resultatet på att en del mikroföretagen även har riktlinjer som har likheter med den *clean desk policy* som Andress (2014) beskriver.

Trots att resultatet visar att mikroföretagen inte arbetar med policyer lyfts det att anställda har svårt att följa samt förstå syftet med riktlinjer, vilket delvis kan kopplas till Bulgurcu, Cavusoglu och Benbasat (2010) definition av ISP awareness. Utifrån studiens resultat är det dock inte möjligt att identifiera varför mikroföretagen inte har en nedskriven informationssäkerhetspolicy. Enligt Gupta och Hammond (2005) kan ekonomi samt begränsade IT-kunskaper vara två anledningar till varför det saknas en nedskriven policy. Det finns däremot inget i resultatet som explicit tyder på att detta är fallet för mikroföretagen i denna studie. Dock finns en indikation på att en nedskriven policy inte upplevs som relevant för ett företag av liten skala. Likt utbildning kan det således spekulerats om mikroföretag med fler anställda arbetar med nedskrivna policyer i en annan omfattning än mikroföretag med endast en anställd.

Gällande riskhantering var det ingen av respondenterna som berättade om ett tillvägagångssätt som kan liknas vid den riskhantering som beskrivs i litteraturen (Katsikas, 2013; Nyak & Rao, 2014). Dock antyder resultatet att mikroföretagen utför vissa aktiviteter som har likheter med ett, eller flera, av de delmoment som i en riskhantering. Resultatet visar att alla mikroföretagen reflekterar över vilken information som behöver skyddas. Dock finns indikationer på att det inte reflekteras över vilka specifika risker som förekommer i relation till att hålla informationen säker, vilket Heidenreich (2019) påstår är viktigt för mikroföretag. Risker behöver arbetas med proaktivt (Nyak & Rao, 2014), men resultatet visar att mikroföretagen snarare arbetar reaktivt. Det framkommer dock att en del av mikroföretagen är medvetna om sina brister inom informationssäkerhet, men att de väljer att acceptera dessa snarare än att förebygga.

I likhet med kategorin människor visar resultatet att mikroföretag inte arbetar med säkerhetsåtgärder som, i den modell som Ghaffari, Gharaee och Arabsorkhi, (2019) och Nyak och Rao (2014) presenterar, kan klassificeras under kategorin processer. Studiens resultat antyder således att mikroföretag inte förefaller ha området processer i åtanke när de arbetar med informationssäkerhet.

5.1.3 Teknologi

SME rekommenderas installera antivirusprogram (Keller et al. 2005; Rees, 2010; Watad, Washah & Perez, 2018), samt brandväggar (Keller et al. 2005; Kurpjuhn, 2015; Rees, 2010; Watad, Washah & Perez, 2018). Resultatet indikerar på att mikroföretagen följer ovanstående rekommendationer och således har installerat både brandvägg och antivirusprogram. I linje med Keller et al. (2005) samt Watad, Washah och Perez (2018) rekommendationer visar resultatet även att mikroföretagen uppdaterar dessa.

Ytterligare en säkerhetsåtgärd som samtliga mikroföretag, i någon omfattning, arbetar med är säkerhetskopiering. Detta ligger i linje med tidigare studier som argumenterar för att SME bör arbeta med säkerhetskopiering (Keller et al. 2005; Rees 2010; Watad, Washah & Perez, 2018). Resultatet indikerar dock på att hur mikroföretag arbetar med säkerhetskopiering skiljer sig från företag till företag. Exempelvis visar resultatet att det endast är ett mikroföretag som säkerhetskopierar de system som används i den operativa verksamheten, medan resterande framför allt säkerhetskopierar filer. Nyak och Rao (2014) beskriver fulla, inkrementella samt differentiella säkerhetskopieringar, men utifrån studiens resultat är det inte möjligt att identifiera vilken typ av säkerhetskopiering som sker i det företag som säkerhetskopierar system. Gällande intervallet bör säkerhetskopieringar genomföras regelbundet (Jayadevappa & Soh, 2009; Keller et al. 2005; Nyak & Rao, 2014; Tsochev et al. 2020). Hur ofta mikroföretagen säkerhetskopierar är i flera fall svårt att identifiera eftersom majoriteten arbetar med automatiska uppdateringar och inte redogör för intervallet. Resultatet visar att intervallet för manuella säkerhetskopieringar skiljer sig mellan mikroföretagen. Intervallet för när säkerhetskopiering ska ske bör vara realistiskt till företagets resurser (Tsochev et al. 2020), vilket således kan vara en möjlig förklaring varför intervallet för säkerhetskopiering skiljer sig mellan mikroföretagen.

Även fysiska säkerhetsåtgärder är en kategori som resultatet visar att samtliga av mikroföretagen, i någon omfattning, arbetar med. De säkerhetsåtgärder som majoriteten implementerar, exempelvis larm och brandlarm, kan skydda företagets alla tillgångar och inte enbart information. Således är det inte möjligt att, utifrån resultatet, utesluta att dessa åtgärder kan ha valts ut i syfte för att skydda mer än bara information. Vidare kan fysiska säkerhetsåtgärder skydda samtliga tre egenskaper i CIA-triaden (Nyak & Rao, 2014), men utifrån resultatet finns inte indikationer på att mikroföretagen implementerar dessa åtgärder för att bevara integritet. Detta eftersom respondenterna framför allt reflekterar kring exempelvis stöld, brand samt åtgärder för att förhindra att obehöriga rent fysiskt kan ta del av information.

Åtkomstkontroll kan, som nämnt i 2.4.3, innefatta flera olika åtgärder för att styra vem som får åtkomst till viss information. Enligt Andress (2014) är lösenord en grundläggande åtgärd för att arbeta med åtkomstkontroll. Utifrån resultatet är detta också den åtgärd som mikroföretagen främst använder. Det var dock endast hälften som uttryckte att de använde sig av starka lösenord, vilket rekommenderas för SME av Keller et al. (2005) och Watad, Washah och Perez (2018). Resultatet visar även att hälften av respondenterna inte byter lösenord på eget initiativ och de mikroföretag som uppgav att de byter har inte några likheter i frekvens, utan byte sker med en variation på var tredje månad till var tredje år. Rekommendationerna är dock inte mer specificerade än att lösenord ska bytas ut regelbundet (Watad, Washah & Perez, 2018). Watad, Washah och Perez (2018) har även rekommendationer om att småföretag ska reflektera över om alla anställda behöver tillgång till all information och om de behöver utöva rollbaserad tillgång. Detta gjordes i fallet med mikroföretaget som hade fler en än anställd.

En säkerhetsåtgärd som däremot inte alla mikroföretagen arbetar med är kryptering, vilket Watad, Washah och Perez (2018) påstår är en säkerhetsåtgärd som även småföretag bör vidta. Det var enbart ett mikroföretag som specifikt utnyttjade kryptering när filer skulle delas med kunder. Resultatet antyder att denna kryptering gjordes för att skydda konfidentialitet av dokumentet och nämner inget om att bevara integritet. Detta ligger i linje med litteratur som skriver att kryptering främst avser att bevara konfidentialitet (Andress, 2014; Nyak & Rao, 2014).

Tidigare studier understryker att informationssäkerhet inte enbart är ett tekniskt område, utan att även människor och processer är två viktiga aspekter att beakta (Baker & Wallace, 2007; Dhillon & Backhouse, 2001; Ghaffari, Gharaee & Arabsorkhi, 2019; Siponen, 2005). Studiens resultat tyder dock på att mikroföretagen i synnerhet arbetar med säkerhetsåtgärder som, i den modell Ghaffari, Gharaee och Arabsorkhi (2019) och Nyak och Rao (2014) presenterar, kan klassificeras under kategorin *teknologi.* Således antyder resultatet att mikroföretagen arbetar med tekniska säkerhetsåtgärder, snarare än med processer och människor.

5.2 Informationssäkerhet och CIA-triaden

Enligt litteraturen ämnar informationssäkerhet bevara samt säkerställa konfidentialitet, integritet samt tillgänglighet (Andress, 2014; Dhillon & Backhouse, 2000; Nyak & Rao, 2014; SIS, 2015; von Solms & van Niekerk, 2013). Studiens resultat tyder dock på att samtliga respondenter beskriver informationssäkerhet på ett sätt som i viss mån avviker från den definition litteraturen presenterar. Majoriteten förklarar att informationssäkerhet ska skydda verksamhetens information från obehöriga. Eftersom egenskapen konfidentialitet i CIA-triaden syftar på att förhindra att obehöriga kan ta del av information de inte ska ha tillgång till (Andress, 2014; Dhillon & Backhouse, 2000), kan resultatet tyda på att mikroföretagen framför allt kopplar informationssäkerhet till konfidentialitet. En av definitionerna som framkommer i studiens resultat innefattar dock att informationssäkerhet ska förhindra att virus låser filer, vilket snarare kan kopplas till egenskapen tillgänglighet. Vidare antyder resultatet att respondenterna huvudsakligen kopplar informationssäkerhet till att skydda information som finns lagrad i en dator, alternativt på nätet. Även om respondenternas svar indikerar på att tillgänglighet samt integritet utelämnas från deras definition av informationssäkerhet påvisar resultatet att samtliga mikroföretag implementerar säkerhetsåtgärder för att bevara alla egenskaper i CIA-triaden. Detta gäller även för de mikroföretag som explicit uttrycker att de inte har implementerat säkerhetsåtgärder för att bevara och säkerställa integritet och tillgänglighet.

Vidare visar studiens resultat att samtliga ägare, alternativt VD, till de mikroföretag som intervjuats inte har någon utbildning inom informationssäkerhet. Det mikroföretag som har fler än en anställd nämner inte att de har anställda som hanterar informationssäkerhet eller IT-relaterade frågor. Detta ligger i linje med Heidenreich (2017) som poängterar att mikroföretag saknar IT-kunskap och dedikerad IT-personal, vilket resulterar i att informationssäkerhet hanteras av en lekman. I likhet med Heidenreich (2017) visar även denna studies resultat på att informationssäkerhet i mikroföretagen hanteras av lekmän. Dock framkommer det av resultatet att ett mikroföretag anlitar en IT-konsult, vilket leder till att företagets informationssäkerhet hanteras av en yrkesman. Utifrån resultatet framkommer det inte varför mikroföretagen väljer att inte anlita konsulter med sakkunskap. Däremot hävdar Gupta och

Hammond (2005) att småföretag har begränsad ekonomi och att det saknas ekonomiska resurser till att anlita konsulter. Ovanstående kan möjligtvis även vara en anledning till varför mikroföretag inte anlitar konsulter.

Resultaten visar även skillnad i mikroföretagens inställning till att använda molnbaserade system relaterat till informationssäkerhet. Vissa har både system och filer i molnet för att alltid ha tillgång till det och att ansvaret då ligger hos de företag som levererar tjänsten. Å andra sidan vill vissa av mikroföretagen ha så mycket som möjligt lokalt på datorn för att det finns en vaksamhet gällande om molnbaserade system kan garantera att informationen förvaras säkert.

Konfidentialitet

Konfidentialitet är den egenskap som ska säkerställa att obehöriga inte ska ges åtkomst till information som de inte har behörighet att ta del av (Andress, 2014; Dhillon & Backhouse, 2000). De säkerhetsåtgärder som respondenterna främst använder sig av, som litteraturen skriver bevarar konfidentialitet, är fysiska säkerhetsåtgärder, antivirusprogram, brandväggar samt lösenord. Då flertalet respondenter nämner att obehöriga inte ska få tillgång till information tolkas detta som att säkerhetsåtgärderna implementerats för att bevara just konfidentialitet. Nyak och Rao (2014) påstår att upprätthållande av konfidentialitet är en av de mest angelägna aspekterna inom informationssäkerhet. Resultatet tyder på detta kan vara en uppfattning som delas av mikroföretagen.

Integritet

Integritet säkerställer att information som delges behöriga användare ska vara korrekt (Andress, 2014; Dhillon & Backhouse, 2000; Harley & Cooper, 2021; Nyak & Rao, 2014; SIS, 2015). Utifrån studiens resultat är det svårt att tyda om mikroföretagen arbetar med de kvalitetsdimensioner som Harley och Cooper (2021) beskriver. Däremot tyder resultatet på att det finns en viss tanke på att data ska vara aktuell och således behöver uppdateras. Studiens resultat indikerar däremot på att mikroföretagen framför allt arbetar med åtkomstkontroll, säkerhetskopiering, fysiska säkerhetsåtgärder, brandväggar och antivirusprogram för att bevara integritet. Detta är dock inte möjligt att säkerställa att mikroföretagen implementerat ovanstående säkerhetsåtgärder i syfte för att bevara integritet.

Tillgänglighet

Tillgänglighet ska säkerställa att information finns tillgänglig för samtliga behöriga användare när informationen efterfrågas (Andress, 2014; Dhillon & Backhouse, 2000; Nyak & Rao, 2014; SIS, 2015). För att bevara egenskapen tillgänglighet i CIA-triaden tyder resultatet på att mikroföretagen huvudsakligen arbetar med någon form av säkerhetskopiering, antivirusprogram, brandväggar samt fysiska säkerhetsåtgärder. Utifrån resultatet är det dock inte möjligt att påvisa om mikroföretagen implementerat dessa säkerhetsåtgärder med avsikt att upprätthålla specifikt egenskapen tillgänglighet i CIA-triaden. En anledning till detta är att flera mikroföretag nämner att de inte arbetar för att säkerställa tillgänglighet. Dock visar resultatet att de ändå implementerat säkerhetsåtgärder som enligt litteraturen kan säkerställa tillgänglighet (Andress, 2014; Nyak & Rao, 2014). Vidare påstår Heidenreich (2019) att mikroföretag i allmänhet är beroende av en dator, vilket är ett resultat som även denna studie påvisar. Detta kan möjligen tyda på att mikroföretagen har en sårbarhet och svårt för att säkerställa egenskapen tillgänglighet.

5.3 Metoddiskussion

I linje med Jacobsen (2002) definition tillämpades ett bekvämlighetsurval. Samtliga företag som intervjuats uppfyller studiens urvalskriterier, men bekvämlighetsurvalet resulterade i att fem av sex mikroföretag som intervjuats endast har en anställd. Således kan det ifrågasättas om studiens resultat och slutsatser är representativa för mikroföretag som har fler än en anställd.

Då förhållandevis få mikroföretag har intervjuats i denna studie kan det argumenteras om hur väl studiens resultat och slutsatser representerar realiteten. Enligt Jacobsen (2002) är kvalitativa metoder i allmänhet associerade med lägre generaliserbarhet. Därav menar vi att studiens resultat och slutsatser snarare ger en indikation på hur mikroföretag arbetar med informationssäkerhet. Om vi däremot hade valt att tillfråga ett större antal mikroföretag hade en kvantitativ metod möjligtvis varit mer adekvat. Detta eftersom Jacobsen (2002) poängterar att kvalitativa metoder fordrar mer resurser i jämförelse med kvantitativa metoder. Dock hade en kvantitativ metod inte resulterat i en beskrivning på samma sätt som i denna studie. Detta eftersom Jacobsen (2002) skriver att kvantitativa metoder snarare är lämpliga för att presentera omfattning och således hur ofta ett specifikt fenomen uppträder (Jacobsen, 2002). Därav hade en kvantitativ metod snarare varit lämplig för att undersöka i vilken omfattning mikroföretag arbetar med informationssäkerhet och olika säkerhetsåtgärder. I förhållande till studiens syfte menar vi dock att studiens metodval är adekvat.

6 Slutsats

Detta avslutande kapitel ämnar besvara studiens forskningsfråga och sammanfattar således studiens resultat i en slutsats. Kapitlet avslutas med förslag på vidare studier om informationssäkerhet hos mikroföretag.

Denna studie ämnar undersöka samt ge en beskrivning av hur mikroföretag arbetar med informationssäkerhet. Forskningsfrågan som studien avser att besvara är därför följande.

Hur arbetar mikroföretag med informationssäkerhet?

Studiens resultat tyder på att ägare, alternativt VD, till mikroföretag huvudsakligen beskriver informationssäkerhet som skydd mot att obehöriga ska ta del av företagets information. Med utgångspunkt i CIA-triaden indikerar således resultatet på att mikroföretag främst förknippar informationssäkerhet med att bevara egenskapen konfidentialitet. Däremot antyder resultatet att mikroföretag, trots ovanstående beskrivning av informationssäkerhet, även arbetar med säkerhetsåtgärder som ämnar att bevara och säkerställa egenskaperna integritet respektive tillgänglighet.

Vidare tyder resultatet på att mikroföretag framför allt arbetar med informationssäkerhet på egen hand. Då resultatet visar att ägare, alternativt VD, till mikroföretag saknar utbildning inom informationssäkerhet är det således lekmän som tar beslut om hur företaget ska arbeta med informationssäkerhet för att skydda information. Dock indikerar resultatet på att det förekommer situationer då mikroföretag anlitar en IT-konsult som tar hand om företagets informationssäkerhet och beslutar om vilka säkerhetsåtgärder som ska implementeras.

Avslutningsvis antyder resultatet även att mikroföretag framför allt arbetar med antivirusprogram, brandväggar, fysiska säkerhetsåtgärder, åtkomstkontroll samt säkerhetskopiering. Gällande fysiska säkerhetsåtgärder framgår det att lås samt larm är vanligt förekommande åtgärder, medan resultatet visar att lösenord är den typ av åtkomstkontroll mikroföretag framför allt arbetar med. Ovanstående säkerhetsåtgärder kan alla klassificeras under kategorin teknologi, varav resultatet tyder på att mikroföretag huvudsakligen arbetar med tekniska säkerhetsåtgärder. Således indikerar resultatet på att mikroföretag inte arbetar med säkerhetsåtgärder som faller in under kategorierna människor samt processer i samma omfattning som de säkerhetsåtgärder som klassificeras i kategorin teknologi.

6.1 Förslag på vidare studier

Denna studie ger en indikation på hur mikroföretag arbetar med informationssäkerhet, men då endast sex mikroföretag tillfrågats är det inte möjligt att generalisera studiens slutsatser. Därav ser vi ett behov av ytterligare studier som undersöker fler mikroföretag, förslagsvis med fler än endast en anställd. Vidare kan mikroföretag som är verksamma inom olika branscher studeras. Detta för att undersöka om bransch, och således även typ av information som hanteras i verksamheten, påverkar hur mikroföretag arbetar med informationssäkerhet. Ytterligare ett förslag på vidare forskning är att studera om det finns en anledning till varför mikroföretag väljer att arbeta med informationssäkerhet på ett specifikt sätt.

Appendix 1 - Förfrågan

Förfrågan om att delta i studie om informationssäkerhet

Kandidatuppsats: Ekonomihögskolan vid Lunds universitet

Hej,

Vi är två studenter, Emma Johansson och Michelle Olsson Larsson, som studerar på Systemvetenskapliga programmet vid Lunds universitet. Syftet med vårt examensarbete är att undersöka hur mikroföretag arbetar med informationssäkerhet. Vi söker efter deltagare som vill medverka i en intervju som beräknas ta cirka 45 minuter.

I en intervju, där vi önskar att göra en ljudupptagning, kommer du få frågor om informationssäkerhet. Vi har förståelse för att informationssäkerhet kan vara ett känsligt ämne. Frågorna är därför generella och syftar inte på att ta reda på specifik information om företagets informationssäkerhet.

Som deltagare i studien kommer ditt namn, kön och ålder inte framgå av studien. Företagsnamn, lokalisering och annan information som kan identifiera företaget exkluderas också från studien. Deltagande är frivilligt. Om du väljer att medverka i studien har du rätt att närsomhelst avbryta ditt deltagande. Är du intresserad att delta i studien?

Vid ytterligare frågor om studien är du välkommen att kontakta oss enligt nedan:

Kontaktuppgifter:

Emma Johansson
0703-18 88 13
em4243jo-s@student.lu.se

Michelle Olsson Larsson
0763-077869
mi3061la-s@student.lu.se

Tack på förhand,

Vänligen
Emma och Michelle

Appendix 2 - Informationsblad

Ett stort tack för att du vill medverka i vår studie. I början av juni ges du möjlighet att ta del av studiens resultat samt uppsatsen i sin helhet.

Nedan information beskriver hur vi kommer att använda den information som du delger oss. Vi ber er därför att noggrant läsa igenom följande information:

Intervjuförfarande:

- Din intervju kommer spelas in (endast ljudfil). Om intervjun sker digitalt kommer även en videoupptagning tas på grund av restriktioner i programvarans inställningar. Denna kommer dock raderas direkt när den skapats och det är endast ljudupptagningen som används för transkribering.
- Vi kan komma att ta anteckningar under din intervju.
- Vi kommer efter intervjun att transkribera ljudupptagningen. Du har möjlighet att läsa samt godkänna transkriptionen om du önskar.
- Transkriberingen kommer utgöra en del av studiens empiriska material, vilket i praktiken innebär att transkriptionen i sin helhet kommer presenteras i uppsatsen.
- Efter godkänt betyg kommer uppsatsen publiceras i Lunds universitets databas för uppsatser (https://lup.lub.lu.se/student-papers/search/).
- Det är frivilligt att delta i studien. Du kan närsomhelst avsluta din medverkan.
- Du har rätt att utelämna svar på de frågor du inte vill besvara utan att ange anledning till detta.

Anonymitet:

- Information som kan härledas till dig, eller företaget, kommer tas bort från transkriberingen och inte redovisas i studien.
- Företaget namn och plats kommer inte nämnas i studien. Antal anställda samt din yrkesroll kommer nämnas. Bransch kan komma att nämnas.

Konfidentialitet:

- Ljudfiler kommer sparas i en lösenordskyddad mapp lokalt på våra datorer. Det är endast vi som genomför studien som har tillgång till ljudfilerna.
- Vi kommer att spara ljudfiler fram till att transkriberingen är färdigställd. Därefter kommer alla ljudfiler raderas.

Kontaktuppgifter till oss som genomför studien:

Emma Johansson

0703-18 88 13

em4243jo-s@student.lu.se

Michelle Olsson Larsson

0763077869

mi3061la-s@student.lu.se

Appendix 3 - Intervjuguide

Bakgrundsfrågor:

Medgivande och etiska aspekter

1. Har du tagit del av informationen ovan? Och har du några frågor kring den?
2. Godkänner du ovanstående information? Och vill du medverka i studien?
3. Vill du ha ett exemplar av transkriberingen?
4. Vill du ha ett exemplar av rapporten när den är färdig?

5. Vilken roll har du på detta företag?
6. Hur många personer arbetar i detta företag?
7. Vilka IT-stöd använder ni? *(Exempelvis hårdvara, mjukvara)*
8. Har du gått någon utbildning i informationssäkerhet?

Informationssäkerhet

9. Hur definierar du informationssäkerhet? (Personer)
10. Vet du vilken information som är viktig att skydda för ditt företag?

Konfidentialitet:

11. Hur arbetar ni för att säkerställa att obehöriga inte ska få tillgång till företagets information *(exempelvis e-mails, dokument, fysiska papper, personuppgifter, bankuppgifter, telefon, kunduppgifter, uppgifter om anställda etcetera*)?

12. Hur kommunicerar ni och delar känslig information (*exempelvis personuppgifter, affärshemligheter*)? Hur säkerställer ni att den kommer till rätt mottagare?

13. Har alla anställda tillgång till all information?

Integritet:

14. Hur arbetar ni för att verksamhetens information alltid är rätt (*exempelvis att fakturor stämmer, överensstämmer information som lagras både digitalt och fysiskt*)? Dvs att den inte råkar raderas eller att någon går in och ändrar något som inte ska ändras?

15. Hur arbetar ni med säkerhetskopiering (*exempelvis informationssystem eller filer på datorer*)?

Tillgänglighet:

16. Hur arbetar ni för att säkerställa att information alltid finns tillgänglig när den behövs?

Konfidentialitet, integritet och tillgänglighet:

17. Hur avgör ni vilka säkerhetsåtgärder ni behöver tillämpa för att skydda företagets information?

18. Har ni etablerat en informationssäkerhetspolicy?
    Tex:
    - *Om nej: Varför har ni inte en policy?*
    - *Om ja: Hur säkerställer ni att er policy gällande informationssäkerhet efterföljs?*

19. Utbildar ni på företaget er inom informationssäkerhet på något vis?
    Tex:
    - *Varför inte?*
    - *Hur ofta och i vilken omfattning?*

20. Vad använder ni för tekniska säkerhetsåtgärder *(Exempelvis brandvägg, antivirusprogram, kryptering)* för skydda er information?
    Tex:
    - *Uppdaterar ni eventuella antivirusprogram och brandväggar när nya uppdateringar släpps?*

21. Hur arbetar ni med fysiska säkerhetsåtgärder? *(Till exempel lås, passerkort, larm, låsa in hårddiskar, skydd mot brand etc.)*

22. Hur är er tanke kring lösenord? *(ex: hur ofta lösenord bytas, hur starkt lösenord ska vara)*

Appendix 4 – Intervju Respondent 1

18 april 2022 - Digital intervju
R1 - Respondent, F - Författare, F1 - Författare 2

Rad	Person	Frågor och svar	Kod
1	F	Så och då börjar vi lite enkelt. Vilken roll har du på ditt företag?	
2	R1	Ja, jag är ju helt ensam så jag är, vad ska man säga, enda anställde och VD och ordförande och allt möjligt. Ensam styrelse.	
3	F	Så du har alla roller i princip?	
4	R1	Ja	
5	F	Och ja, då är det bara en person som jobbar på företaget?	
6	R1	Ja	
7	F	Och då är nästa fråga: Vilka IT- stöd använder du? Och det är då hårdvara och mjukvara. Så det är program och de tekniska grejerna.	
8	R1	Ja, och det ska jag veta? Jag har en laptop. Behöver ni veta exakt eller?	
9	F	Nejdå	
10	R1	Det är en laptop som är kopplad till en fristående stor skärm här. Och så har jag en HP skrivare. Den gör allting. Den skannar, kopierar och skriver ut. Och så har jag en separat scanner. En sådan där man matar uppifrån som ger en snabb scan. Och så har jag en extern hårddisk för säkerhetskopiering. Det var nog all hårdvara det. Brukar det vara någonting mer som jag glömmer?	
11	F	Nejdå	
12	R1	Ja och det här headsetet och den här…	
13	F	Kameran? Ja, men det är väl så det brukar se ut på mindre företag ja. Vad använder du för program som du jobbar med på datorn?	
14	R1	Microsoft outlook. Microsoft Word. Adobe.	
15	F	Vad var det sista du sa?	
16	R1	Adobe. Men alltså PDF. Jag jobbar inte med det, bara om jag använder PDF alltså. Sen har jag här något skärmklippverktyg. Vad är det för någonting? Vet ni vad det är? Skärmklippverktyget använder jag.	
17	F	Ja det är när man ska klippa ut saker och dokument och sånt.	
18	R1	Jag vet inte om det ligger i Officepaketet eller vad. Jag har en genväg till den här längst ner på skärmen i alla fall. Den använder jag ofta.	
19	F	Ja	

20	R1	Vad har jag mer? Ja, sen nu för tiden då Teams och Zoom. Och så har jag ju Google chrome för att komma ut på internet. Sen så sparas allting till någonting i molnet som heter Onedrive.	I, T
21	F	Så det är där du har dina dokument?	
22	R1	Ja. Oj nu försvann ni vad gjorde jag nu?	
23	F	Kanske bara råkat trycka ner oss. Förminskat fönstret.	
24	R1	Vänta, ska se här. Där ja. Så. Jag funderar på… Sen har jag ju såklart alla de här programmen som ingår i Office paketet, men jag använder inte excel till exempel.	
25	F	Har du något system…	
26	R1	Och inte Powerpoint använder jag inte heller.	
27	F	Mhm…	
28	R1	Och det är för att jag inte klarar det. [skrattar]	
29	F	Det finns kurser att gå [skrattar]	
30	R1	Ja, men än så länge så har det gått bra utan. Alltså man kan alltid be någon annan eller så där.	
31	F	Ja, smidigt.	
32	R1	Ja, men det är ju mitt viktigaste arbetsredskap.	
33	F	Har du något system eller program där du har koll på dina kunder? Eller klienter kanske du säger istället?	
34	R1	Ja det var så, jag öppnade ju det här företaget [borttaget] och då var det tal om att ha nått sånt tidredovisningssystem som inkluderar allting med tider och fakturering och så där. Men jag sket i det, utan jag kör det i Word. Alltså manuellt.	
35	F	Allt i Word ja	
36	R1	Klient och ärenderegister i Word som jag för manuellt. Och fakturor gör jag manuellt i Word.	
37	F	Så, då går vi vidare till nästa fråga som kan upplevas som ganska svår. Men det är som sagt inget läxförhör. Nej det var inte den frågan än. Innan det. Har du gått någon utbildning i informationssäkerhet?	
38	R1	Nej, det har jag inte gjort. Det enda jag har gjort är som alla företag nu för tiden är man väl skyldig att ha… Jag tänker på GDPR.	
39	F	Ja	
40	R1	Där hade jag någon sittning med någon konsult om vad jag är skyldig att ha och det är väl åt informationssäkerhet hållet eller?	
41	F	Precis	

42	R1	Hon hade ju en massa frågor om hur hur jag skyddade data och så där. Och där var jag också skyldig att ha information om det där i mina e-mails disclaimer och på min hemsida. Men det har jag inte tagit mig tiden att lägga in än så det har jag i default.	K
43	F	Det står på att göra listan?	
44	R1	Ja, Jag har fått allting av henne. Jag har betalt för det också. [borttaget]. Men jag har inte orkat göra… se till så att det kom ut. Det krävde lite insats från mig också för att göra det sista och jag har inte hunnit.	
45	F	Nej jag förstår	
46	R1	Jag väntar på ett föreläggande från myndigheterna. Så annars ingen informationssäkerhetsutbildning. Jag har ju en IT-konsult som har hjälpt mig att lägga upp allt jag har och som jag ringer så fort det är någonting. Och det är också han som har gjort de skydd som jag nu har utan att veta om det.	
47	F	Ja	
48	R1	Han har valt vad jag behöver liksom. Till exempel är det han som har gjort Onedrive lösningen och den här externa hårddisken och att jag ska ha den och så.	
49	F	Tillbaka till den här lite kanske svårare fråga då. Hur definierar du informationssäkerhet?	
50	R1	Ja, det första man tänker på är ju att någon extern kommer åt mina filer eller låser dem och vill ha betalt för att låsa upp. Det är överhuvudtaget att någon kommer åt det som finns i min dator på ett eller annat vis. Det kan ju vara genom att stjäla datorn också i och för sig.	K & T
51	F	Så det är att någon obehörig ska komma åt information som de inte ska?	
52	R1	Ja	
53	F	Och den vetenskapliga och den definitionen som de som jobbar med informationssäkerhet har är att där är tre egenskaper hos ens information som man vill skydda och det är konfidentialitet, integritet och tillgänglighet. Så det är de tre man kollar på. Så det är dem vi kommer att ställa frågor utifrån. Bara för att få med alla aspekter.	
54	R1	Ja	
55	F	Det här med när vi pratar om informationssäkerhet så är det inte bara information som är digitalt utan det kan även vara om där är saker i till exempel pärmarna som står bredvid dig eller att man inte råkar säga någonting man kanske inte ska säga i telefon så andra kan höra och sånt.	
56	R1	Ja, jag fattar	
57	F	Så det kan vara bra om det är med i dina tankar när du svarar på frågorna. Det är det breda perspektivet som vi är ute efter. Vet du vilken information som är viktig att skydda för ditt företag?	
58	R1	Ja eftersom det är en [borttaget] så är det ju ganska lätt. Alltså jag har ju skyldig att hålla allting som har med mina klienter och mina uppdrag att göra hemligt för alla. Så det är ju enkelt.	K
59	F	Ja det är den informationen ja	

60	R1	Ja sen vad finns det mer för information i mitt företag? Det är väl bara företagets ekonomi då. Men den är inte så… den är jag inte skyldig att hålla hemlig och enligt någon lag och det är ju upp till mig hur känslig jag tycker det är och det är ju inte så känsligt. Mycket av det ska man ju ändå publicera en gång om året i årsredovisningen. Så nej det är klientrelaterade ärenden, ärenderelaterad information som är hemligt.	K
61	F	Och hur arbetar du då för att säkerställa att obehöriga inte får tillgång till den här informationen eller all information på företaget?	
62	R1	Ja hur gör jag det? Om vi börjar med det som är i datorn då så har jag ju en skärmsläckare som går igång efter någon halv minut eller vad det är och som kräver lösenord så att om jag lämnar datorn så kan ingen komma förbi och titta i filerna om de inte har det lösenordet. Och sen har jag ju ett annat arbetsredskap, mobilen. Och där har jag ju mail och massa hemligheter och det är samma där. Där har jag alltså att jag måste slå pinkod för att komma in varje gång. Så det är lösenordskyddade skärmsläckare eller vad det heter på både mobilen och datorn då. Jag vet inte om det är skyddat på något… Ja sen ja sen har jag ju säkert skydd då om man tänker angrepp utifrån cyberrymden. Sen har jag ju, vet ju inte knappt vad det heter. Brandvägg och sånt.	K
63	F	Och det var den här IT-killen?	
64	R1	Ja, har ju några ikoner här som har med säkerhet. Windowssäkerhet ingen åtgärd krävs står det här. Så det är väl några Windows paket jag har. Ja, sen så fysiska akter har jag. Vet inte om ni ser det här? Men jag har ju massa pärmar här på kontoret. Kontoret har jag här i bostaden så att det är ju svårt att skydda. Men det är inte så mycket spring här och jag är ju alltid här liksom. Är jag inte det så är [borttaget] här. [borttaget] som bor här. Men det är ju inte så skyddat egentligen. Men jag har ju… på huset finns ju inbrottslarm och så där. Som jag i och för sig inte alltid aktiverar när jag bara lämnar huset i 20 minuter eller så där. Men om jag åker bort någon längre stund så aktiverar vi ju larmet. Så då är ju den fysiska informationen skyddad via inbrottslarm och brandlarm. Och sen har jag… Och det aktiverar jag också när jag åker bort. Övervakningskamera på ett par strategiska ställen här som tar tiosekunders filmsnuttar om någon går förbi kameran och så skickas det upp i molnet. Så det är ju som inbrottsskydd, ja inbrottsskydd är det väl inte för de kan ju göra inbrott även om de blir inspelade.	K & T
65	F	Ja, man blir medveten om det i alla fall.	
66	R1	Nej det är ju inte säkert de ser den. Ja, alltså den tjuter inte utan filmar bara.	
67	F	Jag tänker att du blir medveten.	
68	R1	Ja jag får ju information och då inbrottslarmet är ju kopplat till [borttaget]. De ser i realtid här. Det finns ju kamera där också. Så de ser vad som händer. Det är en särskilt här i företagets kontor. En särskild kamera till [borttaget]. Sen har jag sagt till [borttaget] att det inte får vara fester här. [Borttaget] fyller snart [borttaget]. Jag vill inte ha [borttaget] som springer runt här. För då vet jag inte om de springer in just här där det är hemligheter, på kontoret. Så några riktiga fester har det inte fått vara här. Inga röjarpartyn här inte.	K
69	F	Mhm	
70	R1	För att skydda informationen faktiskt. Ja jag vet inte om det är något jag glömmer?	
71	F	Man brukar kanske ha något antivirus men det finns också inbyggt i datorn om den…	

72	R1	Kan jag hitta… kan jag hitta det genom att klicka här någonstans eller nej för det har jag säkert alltså men jag vet inte vad jag hittar det.	
73	F	Ja, nej det brukar vara inbyggt i datorn och då är det ifall man kanske har köpt något extra.	
74	R1	Ja men det tror jag att han har satt in.	K, I & T
75	F	Men då tror jag att vi har täckt allt på den frågan. Och då är nästa, hur kommunicerar och delar du den här känsliga informationen, och hur säkerställer du att den kommer till rätt mottagare?	
76	R1	Ja nittionio gånger av hundra är det mail och telefon man jobbar med och i yttersta undantagsfall nu för tiden vanlig post. Gällande e-mail är att man använder e-mailadresser som man tror sig veta är de korrekta. Men jag använder inte krypterade mail eller så som en del myndigheter och [borttaget] har börjat att göra men det gör jag inte utan det det skickas som öppna e-mail med outlook.	
77	F	Då går vi vidare till den punkten som kallas integritet och då är frågan: Hur arbetar du för att verksamhetens information alltid är rätt? Med det innebär att den kanske inte råkas raderas eller att någon går in och ändrar eller du, och ändrar någonting som inte ska ändras.?	
78	R1	Den var lite svår, men alltså när jag skickar ett skarpt dokument i verksamheten till exempel en [borttaget] då gör jag ju alltid det som en skannad pdf och då tycker jag att den är skyddad för den är inte så lätt att redigera. Men när jag skickar utkast mellan mig och klienten så är det ju i word och då kan ju klienten eller någon annan vara inne och ändra eller så. Så det är skannade pdf:er.	I
79	F	Du nämnde också lite med säkerhetskopiering?	
80	R1	Ja, men det utgår jag ifrån att det görs automatiskt till den externa hårddisken och sen så ser jag hur det blir en symbol på de här alla de här ikonerna när det har laddats upp i onedrive där i molnet.	I & T
81	F	Så det går både till molnet och till din externa hårddisk så du har dem på två ställen?	
82	R1	Ja om det fungerar som det ska. Jag har aldrig kollat om det ligger något på den där hårddisken, men det måste det väl göra? Den lyser och är inkopplad i alla fall. Jag vet inte om den blir full någon gång.	
83	F	Ja då får du ringa IT-killen	
84	F	Och då nästa fråga. Det är hur arbetar du för att säkerställa att informationen alltid finns tillgänglig när den behövs?	
85	R1	Jag arbetar inte alls för det, det sköts automatiskt. Alltså man är ju oerhört handlingsförlamad och strandsatt när internet lägger ner. Men de gånger det händer, vilket hände nyligen att jag tappade internet ja då blir det ju ett jävla ringande till it-konsulten. Han sitter i [borttaget] men han kan ju gå in på min dator på distans. Men det blir många timmars felsökning och slutar med att någon förstärkare här till routern hade lagt av så hårdvarufel visade sig det i slutändan. Sånt där kan hända men det är ju inget jag kan förebygga eller någonting utan när någonting händer så får man ringa de experter som man kan komma åt. Eller leverantören om det är så. Och det är ju samma med mobilen. Om det händer något med den då får jag då ringa en it-konsult eller leverantören av abonnemanget om det inte fungerar.	T

86	F	Är det så att du har du en extra dator, eller har du flera datorer som en går sönder så har du en annan du kan använda?	
87	R1	Nej det har jag inte eller ja jag har ju min förra dator ligger där uppe i en garderob. Den skulle jag väl kunna använda antar jag om den här la av. Men man känner, alltså det ja, i och för sig det skulle ju kunna hända i ett väldigt tidskritisk läge. Men det har jag ingen beredskap för utan jag tänker väl att när någonting går sönder så ringer jag honom och sen så åker jag och köper det som behövs och så hjälper han mig att koppla in det. Man får bara hoppas att det inte är någonting som måste vara färdigt inom någon dag. Att det inte händer när någonting verkligen måste bli färdigt det har jag ingen beredskap för då får man väl begära anstånd hos den som vänta på något.	T
88	F	Ja då går vi vidare. Hur avgör du vilka säkerhetsåtgärder som du behöver tillämpa? Och då har du nämnt den här IT-killen.	
89	R1	Ja ansvaret har jag överlåtit med varm hand till honom. Att skydda mig mot cyber-angrepp och sånt här. Och sen så är jag som alla nu för tiden, att jag avgör själv vilka mail jag öppnar. Om det är något misstänkt skräpmail så får jag avgöra själv om det kan vara något lurt.	
90	F	Finns det en etablerad informationspolicy? Nu är du ensam så den kanske inte är nedskriven. Men du har en liten plan i ditt huvud?	
91	R1	Alltså jag har ju att förhålla mig till [borttaget] säger och i det ingår ju att att vara hemlig med klientens uppgifter liksom. Det är väl någonting jag har i bakhuvudet hela tiden.	K
92	F	Utbildar du dig någonting inom informationssäkerhet?	
93	R1	Nej.	
94	F	Du nämnde någonting om den här GDPR, så där tar du reda på för det var något som behövde göras?	
95	R1	Nej nej utan det är bottnade i att det finns ett krav från [borttaget] att företagen skulle ha någonting, någon policy och så för detta med GDPR. Och för att uppfylla det kravet så tog jag kontakt med en jurist som är specialiserad på det där och då ingick det rådgivningen att ungefär som vi gör nu ställa massa frågor och så. Så indirekt blev det ju någon form av utbildning för mig men det var ju det var för att uppfylla ett krav. Eller ja egentligen är det väl för att uppfylla de kraven som ställs i GDPR för verksamheten. Så det var ju liksom vad ska jag säga därtill nöd och tvungen. Det var ju ingenting jag sökte upp för att jag vill det och ville få veta mer om GDPR.	
96	F	Ja och bara en lite mindre fråga. Brukar du uppdatera och så när datorn säger att nu är det en ny uppdatering på gång? Brukar du uppdatera den när det kommer upp eller det är någonting du skjuter upp?	
97	R1	Nej det gör jag direkt både i mobilen och i datorn. Om det inte är något obskyrt program som vill uppdateras, men den här vanliga gör jag. Ibland är det något program som jag inte använder som vill uppdateras och då kan jag skita i det men själva datorns uppdateringar gör jag.	
98	F	Du har nämnt det ganska mycket, hur arbetar ni med fysiska säkerhetsåtgärder? Och då tänkte jag så med din hårddisk, är det någonting som låses in eller den står alltid på samma ställe?	
99	R1	Nej, den står på samma ställe tyvärr	
100	F	Ja och sen sa du att du har lås på ditt hem och du hade brandlarm och du har…	

101	R1	Inbrottslarm, övervakningskameror	
102	F	Så det är väl skyddat	
103	F	Hur är din tanke kring lösenord? Är det att de ska vara speciellt långa eller hur ofta du byter dem och så finns det någon tanke kring det?	
104	R1	Tyvärr inte. Man kan säga att jag kanske byter var tredje år men att jag tyvärr kör samma på de ställena som då dyker upp när jag ändrar	
105	F	Det är ganska vanligt	
106	R1	Ja annars blir man tvungen att skriva ner det och då är ju det en risk	
107	F	Precis ja ja men exakt	
108	R1	Att någon kommer åt den lappen. Men det går liksom inte att ha femton olika lösenord. Kanske det går men… Sen på vissa ställen blir man utelåst om man försöker mer än tre gånger och så där. Man skulle kunna köra gör antingen [borttaget], [borttaget] och tre och sådär så att man har femton olika. Men då då kommer man ju inte ihåg på vilket ställe man hade [borttaget]och då måste man ju prova alla femton till slut. Så nej jag kör samma men jag har känt att nej fan nu har jag det här på för många ställen och då byter jag då, och då försöker jag också byta även befintliga då och inte bara nytillkomna ställen som man måste ange ett lösenord på. Men det blir lite överlapp där så jag har väl en två tre lösenord som används på olika ställen.	
109	F	Ibland så finns det att man kan ha tvåstegsverifikation. Som är att man loggar in och sen ska man göra någonting med mobilen för att komma in i datorn är det något du har?	
110	R1	Ja det vill jag minnas att han, konsulten lade in för inte så länge sedan faktiskt bara några månader sedan. Men jag kommer inte ihåg på vilket sätt. Vad fan kan det ha varit? Kan det vara att när man ska in i Windows överhuvudtaget?	
111	F	Vissa har det när de ska in i sin mail. Vissa har det på datorn överhuvudtaget, det är lite olika det finns flera olika.	
112	R1	Ja jaha, men då har jag det men jag vet inte vad det är för. Det kanske är för att komma åt mitt Microsoft konto?	
113	F	Där brukar det de har möjlighet till det ja.	
114	R1	Ja jag vet att han gjorde det. Jag kommer inte ihåg varför men det var inte alls länge sedan vi höll på med det. Men tyvärr jag vet inte säkert vad det är för, men det är inte för att komma in i datorn. Mm jag stänger av datorn och sätter på den då slår jag ju bara mitt vanliga lösenord så är jag inne så det är ju inget tvåstegs.	
115	F	Men jag har inga fler frågor. Har Michelle?	
116	F1	Nej jag har ingenting att tillägga iallafall.	
117	F	Har du någon fråga, eller något du vill berätta som du känner att du inte har fått berätta som du tycker vi har missat?	
118	R1	När det gäller informationssäkerhet i vid mening nej. Det är möjligen fysiska papper för det är jag noga med här, för det vet jag att en [borttaget] har fått disciplinära påföljder för. Alltså sådana papper som man gör sig av med, som har med ärende att	K

		göra och som är känsliga. Men som är skräp för mig men de är känsliga för det är klientmaterial. Det har jag ju en dokumentförstörare till. Men det var en [borttaget] som hade slängt massa papper i en container och så var det någon som hade sett det på en allmän plats, en återvinningsstation och då har det legat avtal och grejer där som då fick han ju disciplinpåföljd för så får inte vi slängde material. Så att vem som helst kan gå och läsa det. Så där försöker jag tänka på att tugga allt som som jag inte ska behålla, allt fysiskt papper.	
119	F	Det var ett jättebra tillägg. Det är sånt man inte alltid tänker på.	
120	R1	Nej uppenbarligen gjorde inte den [borttaget] det.	
121	F	Men då avslutar jag inspelningen.	

Appendix 5 – Intervju respondent 2

22 april 2022 - Fysisk intervju
R2 - Respondent, F - Författare, F1 - Författare 2

Rad	Person	Frågor och svar	Kod
1	F	Hej, då börjar vi lite lätt. Vilken roll har du på detta företag?	
2	R2	Ja, företagsledare	
3	F	Hur många personer arbetar på ditt företag?	
4	R2	Det är bara jag.	
5	F	En person, ja. Vilka IT-stöd använder ni? Såsom hårdvara, mjukvara	
6	R2	Jag har en dator. Dockstation, skärmar.	
7	F	Vilka system sitter du i på datorn?	
8	R2	Det är Excel, om det är det du tänker på?	
9	F	Ja exakt, det är ett jättebra exempel.	
10	R2	Sen är det ju de programmen som… Alltså [Borttaget]. Jag vet inte om det räknas?	
11	F	Jodå, men säg du dom du använder.	
12	R2	[Borttaget], det är [borttaget]. Sen även [borttaget]. Det är nog de som är huvudsak skulle jag säga.	
13	F	Har du någon extern hårddisk eller så?	
14	R2	Nej	
15	F	Det är datorn som är ditt primära arbetsredskap?	
16	R2	Ja	
17	F	Och kanske en telefon?	
18	R2	Ja, telefon definitivt.	
19	F	Har du gått någon utbildning i informationssäkerhet?	
20	R2	Nej	
21	F	Då går vi vidare till en ganska bred fråga. Det kan ta lite tid att svara. Hur definierar du informationssäkerhet?	
22	R2	Ja, det var en bra fråga. Det har jag nog aldrig gjort. Informationssäkerhet. Ja, alltså dels tänker man på källkritik. På vad man får information ifrån och hur säker den är. Men annars så är det lösenord. Alltså hur man skyddar sin information. Det är mest lösenord som jag tänker på.	K

23	F	De som jobbar med informationssäkerhet och vetenskapen brukar dela in informationssäkerhet i tre olika delar och då är det integritet, konfidentialitet och tillgänglighet. Då är det att just de tre egenskaperna ska du bevara på din information. Då är det inte bara information som är digitalt i datorerna utan det kan även vara exempelvis pärmar eller om du sitter och pratar i telefon och vem är det då som hör informationen. Det är egentligen all information som kan vara, ja känsligt.	
24	R2	Det tänker jag omedvetet på. Jag är väldigt noga med vem jag pratar med i telefon till exempel. Jag tänker på personnummer eller vem som kan höra vad jag säger, men jag hade inte kopplat det automatiskt till informationssäkerhet. Men det är någonting jag medveten om när jag gör det.	K
25	F	Vet du vilken information som är viktig att skydda för ditt företag?	
26	R2	För mitt eller alla som jag hanterar?	
27	F	All information som finns på ditt företag. Så det även de som du hanterar ja.	
28	R2	Och vad var frågan sa vi? [Skrattar]	
29	F	Du behöver inte säga exakt vad det är information, men är du medveten om vilken information som är viktigare än någon annan? Och vilken information du måste skydda mer än någon annan information?	
30	R2	Jag vet ju inte om jag vet rätt. För det är vad som går på ryktesvägar och vad folk tror och säger. För att det är ju framför allt GDPR som ingen av småföretagen har koll på. Som man gissar sig till vad det är egentligen. Så nä, det skulle jag inte säga att jag vet. Men jag försöker skydda allt som jag kan anse vara känsligt. Men nej, jag vet inte egentligen vad det är och vad dom säger om det.	
31	F	Det är ett superbra och väldigt ärligt svar. Ja då går vi vidare till den här punkten eller egenskapen som kallas för konfidentialitet. Vi ska prata lite om den. Hur arbetar du för att säkerställa att obehöriga inte ska få tillgång till företagets information?	
32	R2	Ja, alltså jag vet inte om det är….	
33	F	Bara säg vad du tror, det finns inga rätt eller fel här.	
34	R2	Jag låser alltid datorn när jag går härifrån.	
35	F	Ja, precis. Det är en sån sak.	
36	R2	Jag har lösenordshanterare. Hör inte till den kategorin kanske? Och sen så har jag att jag ska byta lösenord var tredje månad. Den påminner mig. Sen är det en annan fråga om jag gör det. Men jag får information om att det är dags att göra det. Så att den ska jag bli bättre på.	
37	F	Men hur ofta blir det att du byter?	
38	R2	Alltså vissa… jag gör utsortering. De som jag använder ofta, de byter jag var tredje månad. Men sen dom andra… jag känner att det inte är jätteviktigt. De får vara. Så de har jag haft i ett halvår.	
39	F	Men det är ändå bara ett halvår.	
40	R2	Ja, alltså nu har jag bara varit i gång[borttaget] så det kan bli längre.	
41	F	Jaha, då förstår jag. Jobbar du på något annat sätt?	

42	R2	Ja, jag låser in datorn på kvällen också. Om det är något att skydda.	
43	F	Låser du dörren?	
44	R2	Ja, definitivt. Här är larm och lås. Och lås på datorn. Och lås på nästan alla pärmar.	
45	F	Lås på pärmarna?	
46	R2	Ja, alltså de står i låsta skåp.	
47	F	Jaha, då förstår jag. Så mycket lösenord, mycket skydd. Och sen är det lås och larm och så?	
48	R2	Ja, i byggnaden.	
49	F	Då går vi vidare på nästa fråga. Hur kommunicerar och delar du känslig information? Och hur säkerställer att den kommer till rätt mottagare?	
50	R2	Jag lösenordsskyddar via Adobe. Alla dokument i PDF eller där som jag anser är känslig information. Till exempel löner. Ja, framför allt löner är det jag lösenordskyddar. [Borttaget] och sånt som jag anser att det kan bli dumt om det hamnar i fel händer.	
51	F	Hur kommunicerar du det? Är det via mejl eller det via USB?	
52	R2	Dokumentet skickar jag via mejl och sen skickar jag lösenordet via sms. Så att jag har två olika källor dom kommer från.	
53	F	Ja, precis. Två olika vägar	
54	R2	Tvåstegsautentisering.	
55	F	Jag tycker vi hoppar över frågan om alla anställda har tillgång till all information. Det känns inte relevant.	
56	R2	Ja	
57	F	Men superbra. Du ser att man gör ganska mycket mer än vad man egentligen tänker är informationssäkerhet. Just det, jag tänkte på att du sa att du tänker på att skydda information när du pratar i telefon. Det är ju också ett sätt att skydda så att obehöriga inte får information. Att du inte pratar om det på ett offentligt ställe.	
58	R2	Och tänker på att man säger kanske kunder i stället för en specifik kund. Jag har dom inom branschen istället för att nämna kunder vid namn. Inte för att det är något sekretess eller nåt sånt men jag tycker ändå att det får de själva berättar för folk i sådana fall.	K
59	F	Ja, då går vi vidare på integritet och då är det hur arbetar du för att verksamhetens information alltid är rätt? Det vill säga att den inte råkas raderas eller att någon går in och ändrar eller du råkar ändra någonting som inte ska ändras.	
60	R2	Mhm fler frågor? Ja, nä… [skrattar]	
61	F	Ett sätt som vissa gör är att de till exempelvis säkerhetskopierar. Att man har sakerna på två ställen eller att man har det i molnet eller…	
62	R3	Alltså [borttaget] är ju redan i molnet. [Borttaget] är också i molnet så nej jag säkerställer inte det.	I

63	F	Nej, men då är det ju att du använder ett system för att säkerställa att informationen är rätt. Du förlitar dig på deras.	
64	R2	Ja, jag förlitar mig på deras.	I
65	F	Då är det tillgänglighet. Hur arbetar du för att säkerställa att information alltid finns tillgänglig när den behövs?	
66	R2	Ja, gör jag det? [skrattar]	
67	F	Exempelvis kan det vara att du ha en dator och om den datorn går sönder då är inte din information tillgänglig.	
68	R2	Nej, då får jag köpa en ny dator helt enkelt.	T
69	F	Du har inte en annan dator i reserv? Men det ligger ändå i molnet…	
70	R2	Så jag når allting där. Jag har den tanken att händer någonting så kan jag köpa en ny dator och logga in på, vad är det nu. Microsoft, Windows ja där man kan komma åt allting. Där ligger till och med skrivbordet. Alltihopa ligger där.	T
71	F	Så det är ju en sån, det är ju säkert. Då kommer du ju in ändå.	
72	R2	Jag behöver köpa en ny dator, men det är det.	T
73	F	Hur är det om exempelvis internet går ner här?	
74	R2	Ja, det är inte bra. Då är jag körd.	T
75	F	Det kan ju också vara att skärmar och sånt går sönder. Då är man fast liksom?	
76	R2	Ja det är ett problem. Men internet hade varit förödande. Alltså det hade inte gått.	
77	F	Du har inte en annan lokal du kan åka till där det finns internet eller så?	
78	R2	Nej, men mobilt internet via telefonen som man kan dela i sådana fall. Är det nere överallt så går det inte.	T
79	F	Och i det här så ingår ju också att man ser till så att sakerna exempel inte stjäls. Och då har du ju redan nämnt lås, larm. Har du dokument och så? Om du slänger dom hur hanteras de då?	
80	R2	Strimlas om det är känslig information.	
81	F	Då lämnar vi den frågan. Hur avgör du vilka säkerhetsåtgärder som du behöver tillämpa för att skydda företagets information?	
82	R2	Ja, jag har en diskussion med mig själv. Så det är vad jag beslutar mig för.	
83	F	Du nämnde innan att det är svårt att få information. Att man inte vet vad man ska inhämta informationen ifrån.	
84	R2	Nej, så jag får själv göra en analys. Vad skulle någon kunna göra med den här informationen? Ja, inte mycket eller ja det kanske inte är så lämpligt. Det är en egen analys jag får göra.	
85	F	En liten riskanalys ja. Är det något du skriver ner?	

86	R2	Nej, det är bara i huvudet.	
87	F	Och där hade jag en fråga. Har du etablerat en informationssäkerhetspolicy? I småföretag så kanske det inte är någonting man har nedskrivet men det finns kanske ändå i huvudet. Och då låter det ju som att du har en viss policy om hur du vill att information ska skyddas.	
88	R2	Ja, men jag skulle nog aldrig säga att jag har en policy. Men ja, jag har väl en tanke som jag kan utforma från gång till gång. För det är aldrig samma. Man ställs inför många olika situationer, så det blir en ny varje gång.	
89	F	Kan du ge ett exempel på en sån situation?	
90	R2	Nej, det tror jag inte egentligen. Alltså vissa mailar ju frågor som är mer omfattande än andra. Till exempel. Och då kan jag tycka att det är dumt redan i första ledet att vissa mailar	
91	F	Ja så det är kunden som..	
92	R2	Brister i det ja.	
93	F	Ja precis. Så redan när det kommer in hos dig så tycker du att informationssäkerheten har brustit?	
94	R2	Ja egentligen är det oftast så ja. De har ofta inte så de kan skydda dokumenten. Alltså småföretag lägger inte ens pengar på Adobe även om det bara kostar typ 150 kr i månaden liksom. Det vill inte folk. De vill inte lära sig. Jag har ju inte heller den yngsta målgruppen. Dom tycker inte det är viktigt och bryr sig liksom inte. Dom blir irriterade när dom får lösenordskyddade dokument.	
95	F	Men du står ändå fast vid att uppfylla dina egna krav?	
96	R2	Ja, för jag tänker att det blir skit för mig. Om det visar sig att det går åt skogen med informationen, ja då var det ju jag som skickade det. Jag känner mig trygg i det här och därför gör jag det. Annars får de komma hit så jag skriver ut papperna i sådana fall. Men det har inte behövts.	
97	F	Dom går med på det efter att du… Ja, men det är intressant att när man har en process som innefattar någon annan så kan det vara att det brister där. Då får man försöka upprätthålla så mycket man kan för att skydda sig själv. Men man vill ju också skydda kunderna, men dom skyddar inte alltid sig själv.	
98	R2	Och de förstår inte när man säger till att du måste, du kan inte skicka sånt på mejl. Nästa dag är det bortglömt igen. De ser inte vikten i det. De bryr sig inte, eller förstår inte.	
99	F	Svårt att veta vilket som är vilket. Om de inte bryr sig eller att de inte förstår.	
100	R2	Ja, precis.	
101	F	Utbildar ni er på företaget inom informationssäkerhet på något vis?	
102	R2	Jag försöker prata med nära vänner och bekanta. [Borttaget] säker källa. För att ta reda på vad jag kan på eget håll eftersom jag inte har någon… jag har inte lyckats hitta någon källa där jag kan få svar på mina frågor. Jag får försöka leta på de håll jag kan. Och då är, ja [borttaget] har haft en lång diskussion för att jag ska få svar på mina frågor. Men visst det finns fler frågor.	

103	F	Så att det saknas tydlighet om var man ska vända sig för att få svar på sina frågor?	
104	R2	Definitivt	
105	F	Då blir vi lite tekniska. Vad använder du för tekniska säkerhetsåtgärder? Och då kan det vara brandvägg, antivirusprogram, kryptering. Du har ju nämnt till exempelvis kryptering. Du krypterar dina filer med lösenord och så. Vad har du mer på din dator?	
106	R2	Där är ett antivirusprogram	
107	F	Är det sånt som var med eller har du köpt till extra?	
108	R2	Ja, jag köpte det extra när jag köpte datorn. [borttaget] om det är någon information ni har nytta av.	
109	F	Ja, men det är intressant. Då vet vi vilken.	
110	R2	Där ingick också en lösenordshanterare, så den har jag använt också.	
111	F	Och så brandvägg är det då den som kom med datorn?	
112	R2	Ja, Windows Defender.	
113	F	Och när det kom upp så här att nu är det ny uppdatering, det kan både vara operativsystemet alltså själva datorn men också kanske på den här [borttaget] som du nämnde. Skjuter du på det eller vill du få det gjort och gör det direkt?	
114	R2	Nu när Windows 11 kom, den har jag inte gjort för jag är rädd att mina program inte kommer att fungera med den. För det har varit… Det är risker när det kommer en ny version av den. Men kommer det andra typer av uppdateringar inom systemet då uppdaterar jag oftast direkt.	
115	F	Du har redan nämnt lite, men jag tar ändå frågan ifall det är någonting som du glömt. Hur arbetar du med fysiska säkerhetsåtgärder? Och då nämnde du att du har lås, larm och att vem som helst inte kommer in här utan det är dom som är i denna byggnaden. Och det är här du har all din information, du har den inte…du tar inte med det hem i väskan?	
116	R2	Ibland gör jag. Om jag ska jobba hemma.	
117	F	Så då är det på två ställen kan man säga. Du har skåp här med pärmar och då låser skåpen när du går hem?	
118	R2	Ja	
119	F	Man brukar också prata om så här skydd mot brand och sånt. Är det något specifikt eller det vanliga med brandlarm.	
120	R2	Ja, brandlarm. Här är inget specifikt.	
121	F	Och skåpen är inte brand?	
122	R2	Nej	
123	F	Du har redan nämnt lite grann det här med din tanke med lösenord och att du har en påminnelse om att byta.	

124	R2	Ja, jag har ett system för hantera lösenord.	
125	F	Ja, en lösenordspolicy skulle man kunna kalla det.	
126	R2	Ja	
127	F	Och att du försöker byta lösenord ofta?	
128	R2	Sen kringgår jag min egen policy. Men jag har en.	
129	F	Det är en sak att ha en policy och en annan att följa den.	
130	R2	Ja, men det finns en.	
131	F	Är det också så här hur starkt ditt lösenord ska vara?	
132	R2	Ja där har jag alltid en generatorn. Lösenordsgenerator. Så det är minst 16 eller 18 tecken tror jag. Och specialtecken. Så den väljer alltid.	
133	F	Och du har inte samma på flera ställen?	
134	R2	Nej	
135	F	Toppen, Michelle har du något att tillägga?	
136	F1	Nej, det var nog allt det.	
137	F	Har du någonting som du känner att vi inte riktigt har berört?	
138	R2	Nej, det tror jag inte.	
139	F	Vi har pratat om datorn. Skannar du dokument och så?	
140	R2	Och det har jag ju…För när jag flyttade in här…Man kan ju koppla upp sig på Wifi, men då når alla ens skrivare. Så nu har jag nätverkskabel så att jag… alltså att ingen annan kan få det jag skannar. Jag kan inte skanna det fel utan det går via nätverkskabeln in i datorn direkt.	K
141	F	Är det ditt nätverk? Är någon annan inne på ditt nätverk?	
142	R2	Nej, alltså det vet jag inte. Ingen kan komma… Vi är ju inne på samma internet, men jag kan inte komma åt någon annans information och ingen kan komma åt min. Men det är just skrivare som är boven i dramat. Då kan man. Ja då är det WIFI, men med nätverkskabeln bryter man det ja. Och då är man på sitt eget nätverk ja. Det är så det är	K
143	F	Vad är det för…När behöver du skanna och varför skannar du?	
144	R2	För att jag vill bli mer digital. Men mina kunder är nja lite mer pappersbundna. Så då behöver jag skanna ofta, de de skickar till mig för att få in i mina digitala handlingar. Ofta skannar jag kontoutdrag. Det skannar jag nästan varje dag. För då har man avstämningsfunktion i programmet och då behöver man ofta en kopia.	
145	F	Så det kan ju vara ett sätt att till exempelvis säkerställa integriteten. För att det är kanske lite svårare att ändra i en PDF. Det är lättare om man bara jobbar i word. Då kan någon gå in och ändra i en word fil som man har skickat till någon men just den	

		ett skannat dokument kan ju vara svårt. Så det är ifall det var i det syftet, men då förstår jag att det är för att dina kunder…	
146	R2	Ja och det är en sanning med modifikation. För jag kan ändra alla PDF dokument. Så det är snabbt att ta bort vad jag vill. Det som inte passar sig.	I
147	F	Och hur är det med PDF:er som du laddar ner och att klicka på länkar i mail och så?	
148	R2	Nej länkar klickar jag inte på om jag inte vet vad det är. Men jag laddar hem mycket dokument från nätet mest Skatteverket, så de skannar alltid virusprogrammet av. Och min önskan är att ha en till dator för att ha till andras usb, det är nämligen lite känsligt att säga till kunder att man inte vill sätta i och använda deras usb. Jag har inte gjort det än för jag känner mig lite paranoid men det är möjligt att jag fullföljer det senare. Inte för jag vet om det hade hjälpt för jag hade antagligen upptäckt det för sent ändå… men tänker om man sparar filen på extradatorn och sen lägger den i molnet, pluggar ut usb:et och sen hämtar filen från andra datorn, borde kännas säkrare? Så egentligen i dagsläget har jag inget val så sätter jag ändå i det.	
149	F	Okej, om ingen annan har något att tillägga avslutar jag inspelningen här.	

Appendix 6 – Intervju Respondent 3

22 april 2022 - fysisk intervju
R3 - Respondent, F - Författare, F1 - Författare 2

Rad	Person	Frågor och svar	Kod
1	F	Så då börjar vi lite lätt. Vilken roll har du på detta företag?	
2	R3	Jag är allt i allo	
3	F	Så du har alla roller?	
4	R3	Ja, alltihopa från den högsta till den lägsta.	
5	F	Och hur många personer jobbar då här?	
6	R3	Det är jag och hunden	
7	F	Du och hunden ja	
8	R3	Min bodyguard [skrattar]	
9	F	Vad använder du för IT-stöd? Typ det kan vara datorer, men det kan också vara program på datorerna som du använder.	
10	R3	Ja det är den här lådan här. Det är en vanlig laptop.	
11	F	Mm	
12	R3	Inga speciella program., nej det har jag inte.	
13	F	Vad är det du använder datorn till? Behövs den för att sköta butiken liksom?	
14	R3	Ja, alltså delvis för inköp också. För det är mer och mer inköp via leverantörernas virtuella showroom och så vidare.	
15	F	Jaha ja	
16	R3	Sen är det att sköta betalningar.	
17	F	Är det ett speciellt program du har eller är det bara banken du syftar på?	
18	R3	Ja, det är inga speciella program för det.	
19	F	Har du någon skrivare?	
20	R3	Ja. Och mobil och vanlig telefon. Den ska nog snart bli uppsagd. Jag menar det är en onödig kostnad med fast telefon. Det mesta sköts via mobilen faktiskt.	
21	F	Ja, men precis. Har du gått någon utbildning i informationssäkerhet?	
22	R3	Bara livets hårda skola [skrattar]	
23	F	Ja den ja, men ingen universitet eller högskoleutbildning eller så?	

24	R3	Nej	
25	F	Då kommer en ganska bred fråga så det är okej att ta lite tid att tänka på den. Hur definierar du informationssäkerhet?	
26	R3	Oj oj jaa, man har ju inte funderat på de mer än att man får virus på sin dator.	
27	F	Mycket virus?	
28	R3	Ja så det är ju därför man har sån här...ja vad heter det programmet. Brandvägg? Ska se här, vad heter det? Ja det kvittar, det är sån här jag betalar för. Betaltjänst. Brandvägg	
29	F	Brandvägg och antivirus kanske?	
30	R3	Ja, precis. [borttaget] heter brandväggen och antivirustjänsten. Så det är väl det enda jag har som säkerhet.	
31	F	Så det är för att du inte ska få virus? Eller är det också för att folk inte ska komma in på din dator?	
32	R3	Ja men precis. Så att man kan vara lugn när man går in på internetbank. Plus att andra inte kommer åt min kunddatabas. Det har jag lite grann, men jag använder det inte längre.	K
33	F	Är det något specifikt program du har för din kunddatabas?	
34	R3	Excel	
35	F	Och nu när vi skriver ett arbete är vår definition och liksom vetenskapens definition av informationssäkerhet att man ska bevara informationens konfidentialitet, integritet och…	
36	F2	Tillgänglighet	
37	F	Jag kom bara på det på engelska. Och det innebär inte bara informationen som är på datorn utan det kan även vara ifall du har pärmar och så med lite känsliga uppgift. Och så till exempel att ingen kan komma in och ta din dator eller ta dina pärmar. Och det kan också vara om man pratar i telefon om man då har känsliga uppgifter att man kanske ser till så ingen annan hör det man säger. Det är alla aspekter av att skydda sin information.	
38	R3	Ja, man tänker inte på det andra liksom. Det helt klart att pratar jag om något som ingen annan ska höra då går jag undan. Jag pratar inte om det när kunden står där. Men det gör man automatiskt så när du frågar om det så tänker man inte på det.	K
39	F	Det är därför vi vill berätta det så man inte bara tänker på information i datorn när vi ställer frågorna. Försök att tänka hur gör jag med all slags information, både den jag pratar, har i datorn och den som jag har på papper.	
40	R3	Jadu, det är inte så mycket. Jag antar att ingen går in här på kontoret.	
41	F	Ja, men precis. Då går vi vidare till nästa fråga. Vet du vilken information som är viktig att skydda för ditt företag? Du behöver inte säga vilken information som är viktig, men vet du vad som är viktigt eller du bara skyddar all information lika mycket?	
42	R3	Alltså jag vet inte. Det enda jag har att koncentrera mig på är det här med GDPR eller vad det nu heter. Att man ska skydda information om kunder. Det är det enda jag	

		tänker på. Sen gör jag inte så mycket mer. Klar att jag låser in dagskassan. Men annars inget speciellt så, jag vet inte.	
43	F	Ja, det kan ju vara information om bankuppgifter och sånt som också kan vara känsliga kanske?	
44	R3	Ja sant. Men tänker inte på det mer än de åtgärder jag gör privat, hemma liksom.	
45	F	Det är på samma sätt som du gör hemma alltså?	
46	R3	Ja, precis så.	
47	F	Då går vi vidare. Hur arbetar du för att säkerställa så att obehöriga inte ska få tillgång till företagets information? Då kan det vara företagsinformation så som vi sa om bankuppgifter. Men det kan också vara exempelvis pärmar. Det kan också vara personuppgifter och sånt. Dina egna personuppgifter och sånt.	
48	R3	Alltså jag måste göra er besvikna. Jag arbetar inte på något speciellt sätt utan man går efter sunt förnuft. Så man låser in dator, låser och gör som jag gör hemma.	K
49	F	Så du ser till att dörren är låst?	
50	R3	Ja och det kollar man. Är jag härifrån flera dagar i taget så låser jag in datorn och allt i det här i ett speciellt skåp.	
51	F	Och som du sa att på datorn så var det att du hade det här extra programmet med brandvägg och med antivirus?	
52	R3	Precis och dessa uppdateras hela tiden, kontinuerligt med det nya. Så det känns faktiskt säkert. Jag betalar för det så då släpper jag tanken på det.	
53	F	Ja, precis så du betalar för att slippa tänka på det? Och du sa att du uppdaterar så fort det kommer en ny uppdatering?	
54	R3	Ja, precis ja	
55	F	Hur kommunicerar du känslig information? Skickar du e-mail?	
56	R3	Vad menar ni med känslig information?	
57	F	Det kan vara personuppgifter. Det kan vara kunders mailadresser. Det kan vara företagets bankuppgifter.	
58	R3	Ja, jag vet inte. Det är via e-mail det sker. Den mesta kommunikationen med leverantörer. Så där är inget speciellt så utan det är via e-mail	
59	F	Kommunicerar du med kunder ibland?	
60	R3	Nej, bara vid försäljning i butiken. Jag har gjort utskick innan, men det har jag slutat med för GDPR kom. Det blev så omständligt. Mycket att läsa och gå igenom. Ingen visste hur det skulle fungera. Jag orkade inte hantera det och jag tyckte det skulle ta för mycket tid i jämförelse med vad det ger.	
61	F	Så då valde du att sluta med kundutskick?	
62	R3	Ja, precis	

63	F	Ja, men det är också en konsekvens av det. När man får krav på sig. Denna kan vara lite svår abstrakt, men hur arbetar du för att verksamhetens information alltid rätt? Det kan vara exempelvis att du får en faktura. Hur vet du att det inte är en fejkfaktura? Har du något sätt för, eller någon tanke på hur du med det?	
64	R3	Alltså jag är ju ingen stor firma så jag håller det i huvudet, Jag har koll på vilka leverantörer jag har. Skulle det komma något som jag inte känner igen, något fejk eller något konstigt. Ja då kollar man extra noga eller så reagerar man på det direkt. Det är inte svårare än så för det är så får leverantörer jag har.	
65	F	Har du viss data som du har både i någon pärm och fysiskt? Eller jag menar digitalt.	
66	R3	Ja, det var ju nog så när jag samlade in kunduppgifter för att kunna göra utskick. Då hade jag information på lappar, men också i datorn.	
67	F	För då kan det vara så att om man har information på exempelvis två olika ställen så kan det här också innebära att man ser till att det som står på lapparna är samma som det som står i datorn. Så att man kanske dubbelkollar så att man inte ser in fel nummer eller så	
68	R3	Ja, men mina lappar är lite som en säkerhetskopia då. Eller det var tvärt om från början, men nu är det så.	
69	F	För jag tänkte fråga dig om du jobbar med säkerhetskopiering på något sätt? Men då var det att du hade lappar och gjorde informationen digital?	
70	R3	Ja, precis	
71	F	Men hur är det med fakturor och sånt? Är det digitalt och på papper?	
72	R3	De flesta fakturor är digitala idag. Men sen när man ska lämna till revisorn så har jag liksom fortfarande pappersutskrift som på gamla tider. Det får jag själv köra ut på papper. För jag har ju ett gammalt kassasystem och jag kan inte skicka det direkt digitalt. För att kunna göra det ska man köpa ett nytt kassasystem vilket är stor kostnad för min del. Så jag har valt bort det.	
73	F	Du har inte fakturorna i pappersformat för din egen skull utan det är för revisorns skull?	
74	R3	De flesta fakturor är dock e-fakturor, så jag får skriva ut dom.	
75	F	Hur arbetar du för att säkerställa att all information finns tillgänglig när du behöver den?	
76	R3	Ja hur arbetar jag? Jag letar febrilt bland mina papper på kontoret och i datorn. Allt ligger i datorn. Jag har inget speciellt sätt för att säkerställa att det är tillgängligt.	T
77	F	Har du information som ligger i ett annat system som gör att om deras system ligger nere så kommer inte du åt din information?	
78	R3	Nej det tror jag inte	T
79	F	Så du är inte beroende av internet?	
80	R3	Jo det är jag.	T
81	F	Är det för att kunna göra beställningar?	

82	R3	Ja	
83	F	Så om internet ligger nere skulle det vara svårt för dig att arbeta?	
85	R3	Ja, det funkar inte utan internet.	T
86	F	Har du någon backup eller plan för vad du ska göra om internet skulle gå ner? Har du exempelvis internet på mobil så att du kan använda det?	
87	R3	Ja, jag har internet på mobilen. Det är viktigt med internet.	T
88	F	Hur är det ifall din dator exempelvis skulle gå sönder?	
89	R3	Ja, då är det panik. Då får jag köpa en ny. Jag har dock ingenting på hårddisken. Allting ligger på mail och så vidare. Allt kommer vara tillgängligt även om datorn går sönder. Så inget går förlorat mer än datorn då.	T
90	F	Så det är inte datorn i sig? Alltså att det är lagrade saker på den, utan det är att du ska ha möjlighet att komma ut på internet och göra betalningar och så?	
91	R3	Ja precis. När det gäller foto på mina varor har jag det i mobilen. Jag använder mobilen mer än datorn om man säger så. För då kan man sköta det här med reklam och lägga ut på sociala medier. Det är mest telefonen jag jobbar med.	
92	F	Är det så att du har det både på telefonen och att telefonen sparar det i molnet?	
93	R3	Nja, alltså fotona sparas på den där ja	
94	F	På molnet?	
95	R3	Ja, det är nog det	
96	F	Då finns dina foton på två ställen? Både fysiskt i mobilen och i molnet?	
97	R3	Ja, och även på hårddisken	
98	F	Så på datorn också?	
99	R3	Ja	
100	F	Var det något mer på den frågan, nej det tror jag inte. Hur avgör du vilka säkerhetsåtgärder som du behöver tillämpa för att skydda företagets information?	
101	R3	Hmm, jag vet inte. Det är liksom ingenting som är inplanerat eller så. Det beror på situationen, till exempelvis om det har hänt något. Då kan man utgå ifrån det.	
102	F	Till exempelvis det här med att du köpte det här antivirusprogrammet. Vad fick dig till att göra det?	
104	R3	Jag vet inte. Det är ju för att inte bli angripen. Göra det enklare för mig och slippa tänka på det. Det var nog det?	
105	F	Finns det en informationssäkerhetspolicy i detta företag?	
106	R3	Nej	
107	F	Utbildar du dig i informationssäkerhet? Till exempelvis att du går någon nätutbildning eller så om informationssäkerhet?	

108	R3	Nej, det är slumpmässigt. Det beror på om något dyker upp. Någonting någonstans om ämnet. Då kanske jag undersöker det mer, men inget systematiskt nej. Jag söker inte aktivt efter information om det.	
109	F	Hur arbetar du med fysiska säkerhetsåtgärder? Vi har redan nämnt lite grann. Att du har lås…	
110	R3	Larm. Och sen låser jag in datorn om jag är borta flera dagar. Det gäller även andra känsliga saker som jag inte vill att någon kommer åt om det skulle bli inbrott. Så därför låser jag in saker, men alltså inte bara över en helg utan det gäller längre perioder.	
111	F	Men är ju till exempelvis öppet in till kontoret. Finns det risk att någon kan komma in här utan att du märker det när butiken är öppen?	
112	R3	Därför har jag hunden här. Han släpper inte in någon utan att jag märker det.	
113	F	Ja, så då är det hunden som är din fysiska säkerhetsåtgärd. Ett annat exempel på en fysisk säkerhetsåtgärd är skydd mot brand.	
114	R3	Ja, men brandvarnare har jag ju.	
115	F	Hur är din tanke kring lösenord?	
116	F3	Det ska skiftas och bytas regelbundet. Det gör jag faktiskt då och då. Men någon riktig plan för det har jag inte.	
117	F	Hur ofta byter du lösenord ungefär?	
118	R3	Det kan jag inte riktigt svara på, det är slumpmässigt.	
119	F	Har du någon tanke kring hur starkt ditt lösenord måste vara?	
120	R3	Det kollar jag alltid när jag gör ett nytt. Oftast finns det något som visar hur starkt lösenordet är. Det kan vara exempelvis att fältet blir grönt. Jag väljer alltid lösenord som är starka.	
121	F	Är det så att du använder samma lösenord till alla konton?	
122	R3	Nej olika.	
123	F	Har du någon annan fråga Michelle?	
124	F2	Nej, men jag tror vi har täckt de frågor vi hade.	
125	F	Har du något du vill tillägga som du inte har fått berätta för oss?	
126	R3	Det hade varit annorlunda om jag hade haft anställda. Då hade jag inte velat ha mina papper här helt fritt utan även behövt skydda information från mina anställda. Till exempelvis när jag hade anställda här så fick de inte använda min dator. Sen slänger jag inte mina papper hur som helst heller. Jag river sönder dom så att ingen ska kunna plocka upp de ur soptunnorna, för det har man ju hört om. Men annars nej. Jag hoppas att ni har fått de svaren ni ville ha. Så att jag har bidragit med någonting. Mer än så här vet jag inte.	
127	F	Ja, absolut. Tack så mycket för din medverkan	

Appendix 7 – Intervju Respondent 4

22 april 2022 - fysisk intervju
R4 - Respondent, F - Författare, F1 - Författare 2

Rad	Person	Frågor och svar	
1	F	Så då är min första fråga: Vilken roll har du i detta företag?	
2	R4	Jag är affärsbiträde, chef och allt möjligt. Jag sköter allt så att säga.	
3	F	Då är det bara du som jobbar här?	
4	R4	Ja	
5	F	Vad använder du för IT-stöd? Då är det exempelvis om du har datorer eller något annat digitalt. Det kan också vara program som du använder dig av.	
6	R4	Jag har en dator, men jag änder inga program. Jag gör ju bokföring på papper fortfarande.	
7	F	Men vad använder du datorn till?	
8	R4	Jag använder den till, jag har mitt lager där.	
9	F	Är det i något system som excel exempelvis?	
10	R4	Ja, excel är det.	
11	F	Ja, så då är excel ett program du använder.	
12	R4	Ja, det är där jag lägger in och bokar av. Sen när det är bokslut så kör jag ut listor med lagersaldo så att säga.	
13	F	Och kassa och så, är det kopplat till internet?	
14	R4	Nej	
15	F	Så då har du skrivare också? Har du någon extern hårddisk som du lägger vissa saker på?	
16	R4	Det är bara datorn	
17	F	Har du någon gång gått en utbildning i informationssäkerhet?	
18	R4	Nej	
19	F	Då kommer en ganska bred fråga så det är okej om den tar lite tid att tänka på innan du svarar det. Hur definierar du informationssäkerhet?	
20	R4	Alltså helt ärligt så vet jag inte vad det är egentligen. Vadå informationssäkerhet? Alltså nej, jag kan nog inte svara på det?	
21	F	Hur tänker du när du tänker på att du ska skydda din information? Vad tänker du då? Hur ska du skydda din information?	

22	R4	Alltså på datorn då?	
23	F	Det kan vara all slags information. Det kan vara ifall du har i pappersformat men oftast så tänker man exempel på datorn för att det är så enkelt för där är det liksom samlat.	
24	R4	Ja, alltså jag har ju en sån brandvägg där. Och antivirus. Det är det enda jag har egentligen.	
25	F	Vad är det du tänker att du vill skydda från? Är det att någon ska komma åt filerna eller är det att någon ska förstöra datorn.	
26	R4	Ja, det är väl mest min bank, alltså bankuppgifterna. Att ingen ska komma åt dom för det har jag ju på datorn. Det är där jag sköter företagets finanser så att säga.	K
27	F	Det vi skriver är vetenskaplig så då finns det ju såklart en vetenskaplig definition av informationssäkerhet. Man brukar säga att man ska bevara egenskaperna tillgänglighet, konfidentialitet och integritet på informationen. Uppnår du de tre så har du god informationssäkerhet. Precis som du sa innan om det är på datorn. Så behöver det inte vara. Det kan också vara om du har annan information. Till exempelvis om du pratar i telefonen och ska säga känsliga uppgifter där. Att du då ser till att ingen hör. Det kan också vara i pappersformat. Vissa saker har man kanske skrivit ut. När vi ställer frågor nu så är det bra ifall det finns i dina tankar. Att det inte bara är datorn, utan att det även är att folk ska komma åt…Jag vet inte om du har papper och pärmar och sånt? Det brukar handla om skydd även för den informationen.	
28	R4	Jaha okej.	
29	F	Vet du vilken information som är viktig att skydda för ditt företag? Du nämnde bankuppgifter innan. Du behöver inte uppge i detalj. Har du funderat över vilken information använder jag och vilken information är viktig att skydda?	
30	R4	Ja alltså det är väl i stort sett mina bankuppgifter eller det som har med pengarna och banken att göra. Något annat…Alltså det är inget som någon annan har någon nytta av kan jag tycka.	
31	F	Har du information om kunder?	
32	R4	Nej, inget kundregister eller så. Det har jag inte.	
33	F	Hur arbetar du för att obehöriga inte ska få tillgång till företagets information? Och då är det både papper, i datorn och så.	
34	R4	Ja, alltså det är egentligen lättillgängligt för dom står på kontoret. Men alltså när jag är här i butiken så är det ju ingen som kan gå ut där för då har jag en hund som vaktar och de kommer aldrig förbi henne. Och samma med datorn, den kan dom inte heller komma åt då. Hon skyddar liksom den avdelningen där ute. Det är en levande vakt. Men annars finns det där tillgängligt.	
35	F	Vi pratade om att du har en brandvägg på din dator för att folk inte ska komma åt din information via internet.	
36	R4	Ja, och virusprogram om det skulle hända någonting. Nu är det upplagt en backup på datorn så om det skulle vara någonting så finns det en backup inlagd.	
37	F	Är det på datorn eller ligger det på molnet?	
38	R4	På datorn tror jag han la in det ja. Det var bara i förra veckan igen. Någonting hände med mitt lösenord så jag kom inte in i datorn. Då var det en här och fixade det och då sa han att han även fixade en backup. Det hade jag inte innan.	

39	F	Jag försöker fundera ut på vad det kan vara för backup. Oftast brukar man försöka ha den på ett ställe som exempelvis molnet.	
40	R4	Ja, molnet kanske. Han berättade inte vad det var, bara att han lagt till det för om det skulle hända något så finns uppgifterna kvar.	
41	F	Och då menar du uppgifterna på din dator?	
42	R4	Ja. Det är mest mitt lagersystem. För blir jag av med det så får jag lägga in allt igen och det tar en väldig tid.	
43	F	Sen tänker jag att du kanske också låser när du inte är i butiken? Det är också ett skydd.	
44	R4	Alltså låser när jag är i butiken?	
45	F	Nej, när du inte är här.	
46	R4	Ja, men såklart gör jag det.	
47	F	Hur kommunicerar och delar du känslig information?	
48	R4	Alltså jag vet inte om jag har så mycket känslig information.	
49	F	Du har ju kontakt med din revisor?	
50	R4	Ja, via mail.	
51	F	Skickar du då känsliga uppgifter via mail?	
52	R4	Jag lämnar allt till revisorn.	
53	F	Jaha, så allt sker fysiskt?	
54	R4	Ja.	
55	F	Men ni kommunicerar vi mail?	
56	R4	Ja, men jag skickar inte dokument via mail. Det är en gång om året vi träffas egentligen. Jag sköter allt annat själv.	K
57	F	Du har inte kontakt med kunder eller så via mail?	
58	R4	Nej	
59	F	Den här frågan kan också vara lite svår. Hur arbetar du för att verksamhetens information alltid ska vara rätt? Du har nämnt till exempel det här med säkerhetskopiering att det var någon som kom in. Jag antar att han jobbar inom IT eller något sånt så han har kunskap om det. Om något förstörs eller ändras så har du nu en backup. Men det kan också vara att du får en faktura och du ska säkerställa att den är rätt. Har du något system eller tänker kring det?	
60	R4	Ja, alltså jag vet exakt vilka fakturor jag får och många skickas per mail. Får jag varor så kontrar jag då när varorna kommer och fakturan och det.	
61	F	Så du menar att du dubbelkolla fakturan mot det faktiska?	

62	R4	O ja, absolut. Skulle det då komma en faktura jag inte känner igen, vilket faktiskt har inträffat.	
63	F	Vad gör du då?	
64	R4	Jag polisanmälde och betalde inte den. Sen hände inte mer.	
65	F	Och den här säkerhetskopieringen. Det är inget du behöver göra någonting med, utan han har fixat det? Det är inget du aktivt själv måste göra?	
66	R4	Nej nej. Jag vet inte hur det fungerar ändå så det får han fixa.	
67	F	Så om det är något är det han du ringer?	
68	R4	Ja	
69	F	Hur arbetar du för att säkerställa att informationen alltid finns tillgänglig när den behövs? Och den kan vara lite svår. Det kan vara att man…Behöver du internet?	
70	R4	Ja	
71	F	Om internet då lägger ner, finns det en plan för hur du ska göra?	
72	R4	Nej då är jag helt låst.	
73	F	Finns det att du kanske kan använda internet på en mobil och dela det till datorn?	
74	R4	Nej, det går inte.	
75	F	Så om internet ligger nere påverkas din verksamhet?	
76	R4	Ja, alltså att strömmen går eller att internet ligger nere. Då är man ju helt åt råttorna alltså.	
77	F	Om det är så att din dator går sönder? Har du en annan gammal dator du kan använda?	
78	R4	Det blir att köpa en ny	
79	F	Och då att den här säkerhetskopieringen förhoppningsvis då finns?	
80	R4	Ja, att den funkar. Det är lite kris annars.	
81	F	Ja, det blir lite sårbart.	
82	R4	Det är faktiskt det.	
83	F	Hur avgör du vilka säkerhetsåtgärder som du tillämpar för att skydda företagets information?	
85	R4	Ja, jag vet inte egentligen.	
86	F	Hur bestämde du dig för att du skulle ha det här med antivirus?	
87	R4	Så har jag alltid haft. Det tillhör, jag menar det har man ju på hemma på sina datorer. Då har man det här med naturligtvis. Annars är man nog rätt lättillgänglig.	

88	F	Finns det något annat sådant exempel? Vad tänker jag… Inhämtar du information om hot och hur du kan skydda dig mot de här hoten ?	
89	R4	Det är ju mest om man läser något i tidningen. Till exempelvis att nu är det någon som ringer eller någon som skickar brev om fakturor. Alltså du vet sånt, det läser man naturligtvis om.	
90	F	Ja så det är inget du aktivt söker om? Det kommer till dig eftersom du läser tidningen?	
91	R4	Ja	
92	F	Hur är det med om du till exempelvis får mail som ser konstigt ut?	
93	R4	Jag tar bort det direkt.	
94	F	Ja, okej. Så om du inte vet vem avsändaren är så öppnar du inte mailet?	
95	R4	Det går i skräpen direkt.	
96	F	Du har redan nämnt lite saker. För en fråga är nämligen om det finns någon informationssäkerhetspolicy i företaget. Den behöver inte vara nedskriven, särskilt inte när man bara är en. Men har du vissa saker du tänker att du ska göra och om en ny hade börjat här hade du lärt ut de sakerna till dom också?	
97	R4	Ja om man har kontanter till kassan. De låter jag inte ligga kvar i kassan när jag går härifrån. Det låser jag in så det inte finns pengar och att kassan står öppen. Jag har en övervakningskamera. Om något händer plingar det i min telefon. Så det är dom säkerhetsåtgärderna jag har. Och den är ju riktad mot där. Skulle det hända att jag blir rånad så finns det ju också på film.	
98	F	Och vilka fler fysiska? Du sa att du har kamera, larm?	
99	R4	Nej, inte larm	
100	F	Lås?	
101	R4	Ja	
102	F	Det kan också vara att man behöver skydda mot brand.	
104	R4	Brandvarnare har jag.	
105	F	Har du information i brandskyddade skåp?	
106	R4	Nej, informationen finns på hyllor.	
107	F	Står datorn framme eller låser du in den?	
108	R4	Den står framme.	
109	F	Sen de tekniska säkerhetsåtgärderna så har du nämnt brandvägg och antivirusprogram. Har du lås på datorn?	
110	R4	Nej	
111	F	Vad är din tanke kring lösenord? Måste det vara ett visst antal tecken långt eller har du någon annan fundering kring det.	

112	R4	Nej jag har ett lösenord som jag använder till det mesta där det går.	
113	F	För att det är lätt att komma ihåg? Men byter du lösenord med ett visst intervall?	
114	R4	Nej, det gör jag aldrig	
115	F	Papper som du har med känsliga uppgifter på, hur slänger du dem? Är det vanligt eller du strimlar dem eller du bränner dom?	
116	F4	Jag slänger de i en säck och kör till soptippen.	K
117	F	Har du någonting som du vill tillägga som du känner att vi inte alls har berört? Vi har ställt många frågor, men finns det något du vill ta upp som vi inte frågat om?	
118	R4	Nej, jag tror inte det. Jag kan inte komma på någonting nu.	
119	F	Ja, men så är det. Svårt att bara komma på något på rak arm. Vissa saker gör man ju bara för det är sunt förnuft och så tänker man inte på att det är informationssäkerhet.	
120	R4	Allting går per automatik. Det är som på morgonen när man kommer så kollar man igenom att allt ser okej ut och att inget saknas.	

Appendix 8 – Intervju Respondent 5

27 april 2022 - fysisk intervju
R5 - Respondent, F - Författare, F1 - Författare 2

Rad	Person	Frågor och svar	Kod
1	F	Då börjar vi, vilken roll har du på detta företag?	
2	R5	Jag är ägaren.	
3	F	Och hur många personer arbetar på detta företag?	
4	R5	Fem	
5	F	Och vad använder ni för IT Stöd? Och med det menas datorer, mobiler och även programmen. Vad är det då ni använder?	
6	R5	Vi har ju våra datorer. Bara stationära datorer, inga bärbara. Vi har såklart telefoni, mobiltelefoner. Och program på datorn så är det både lokala program och webbaserade program.	
7	F	Och vad använder ni de programmen till? Är det vissa som hanterar anställda, är det där ni beställer saker? Vad är det för olika funktioner som ni behöver?	
8	R5	Det mesta är ju då… Såklart har vi lön på lokal dator och då är det ett löneprogram och sen har vi administrativa program också lokalt. Men när vi bokar speditörer så är allting uppe i molnet för det mesta. Så då loggar man in på någon webbsida och lägger en bokning. När det är inköp så är det mailkonversation alltid och när det är försäljning så är det också mailkonversation.	
9	F	Då, så har du gått någon utbildning i informationssäkerhet?	
10	R5	Nej	
11	F	Och då kommer en lite bred fråga, hur definierar du informationssäkerhet?	
12	R5	Informationssäkerhet för mig är…Jag ser det som att det är en risk i första hand. Och att man ska skydda sig emot, var man för sin data helt enkelt. Hur säkert är den plattformen, om det är på webben. Vem ansvarar för den? Hur kan vi på bästa sätt säkra vår information? Därför har jag också varit lite försiktig med att lägga upp vårt kundregister uppe på nätbaserad program.	
13	F	Du vill hålla dem lokalt i stället?	
14	R5	Jag har ju velat det fram till nu och även om programmet också har anpassat sig till att det kan ligga i molnet så har jag ändå valt att hålla det kvar det i datorerna för jag anser att det är lite säkrare. Men ja, så. Det största är risken helt enkelt när det gäller säkerheten, att man utsätter sig för en risk på nätet	
15	F	Och det är främst på nätet du tänker på då?	
16	R5	Ja det tänker jag på i första hand.	
17	F	Den definitionen som de som jobbar med informationssäkerhet och dom som forskar har. Det är att all information som vi har vill vi bevara tre olika egenskaper på. Och då är det integriteten, konfidentialiteten och tillgängligheten. Och sen så är det precis	

		som du säger, att det är ju informationen som vi har på vår dator och i molnet, men det kan också vara allt som vi har pappersform och det som vi också pratar och säger så, tex när man pratar i telefon att då kan man ju säga information som andra kanske inte riktigt ska höra och sånt. Så det är den här breda definitionen som vi tänker på.	
18	F	Och då är nästa fråga, vet du vilken information som är viktig att skydda för ditt företag? Och då behöver du inte berätta exakt vad det är för någon men liksom har du en tanke över att den här är viktig, den här är mindre viktig och den här kan alla ta del av.	
19	R5	Vi har ju en uppfattning om det. En sund uppfattning om det, men det är inte så att jag vet enligt lagen vad det vi ska skydda helt och hur länge man ska skydda någonting och hur man ska skydda. Men såklart när du nämner telefonsamtal, att man när det är privat, att man går undan eller när det är, om jag pratar om personalen med Arbetsförmedlingen eller Försäkringskassan så går jag ju undan. Ja, men det är bara naturligt, det är inte att vi har skrivit ner hur man ska göra. Och när det gäller bokföring så har vi också att vi förvarar det i vissa år. Och sen kasserar vi det genom att makulera det. Och att vi inte vill att man ska kunna läsa fakturor eller kunduppgifter, att det ligger på ett papper som att någon kan komma åt. Utan vi har alltid makulerat det helt. Så det är ett stort arbete, men vi har gjort vårt bästa. Och det är inlåst, informationen i pappersform är inlåst. Och det är bara vi som jobbar på kontoret som har tillgång till det. Men även såklart på lagret har de tillgång till följesedlarna ja.	
20	F	Men ligger de på lagret då, eller de är…	
21	R5	De går ju ner dagtid.	
22	F	De transporteras liksom?	
23	R5	Ja	
24	F	Men då förstår jag. Så då känns som att ni behandlar mycket av er information som ganska känslig.	
25	R5	Det tycker jag, för vi har hög integritet. Men samtidigt så vet jag ju inte det här med vad som krävs, utan det är bara en personlig hög integritet.	
26	F	Ja, och du har ju redan varit inne lite på det, till exempel att ni låser in. Men hur arbetar ni för att säkerställa att obehöriga inte ska få tillgång till företagets information? Och det är både då den fysiska och den digitala.	
27	R5	Ja och den fysiska är ju att det bara är vissa som får lov att jobba med det. Och vi har… dels har vi ju separata datorer och oftast är vi också indelade på vilka program vi är inloggade på. Så dels loggar man in på sin dator och sedan loggar man också in separat på programmet och då ser man också vem som har varit inloggad och vem som har gjort vad. Och sen när det gäller det digitala så tänker jag att det ska ju vara en brandvägg och ett program, ett virusprogram till exempel. Men det är inte någonting som jag hanterar utan när vi köper tjänsten, så förmodar jag att det sköts och när det uppdaterar så får vi en länk att vi ska klicka på och så gör vi det	
28	F	Men är det att ni har någon här, alltså en IT person här?	
29	R5	Nej	
30	F	Utan ni köper in en tjänst och sen säger de till, programmen då?	
31	R5	Ja, det är olika. För då är det ju att när man köper ett löneprogram eller ett administrativt program så får vi ju länkar från dom och då uppdaterar de. Och när de	

		uppdaterade så sker det kanske flera gånger om året. Och då gör ju vi uppdateringen här, men vi får initieringen från dem. Vi skulle aldrig själv fråga efter det. Och när det sen är säkerheten på datorerna. När det gäller virusprogram och brandvägg, då är det när vi köper tjänsten. När vi köper produkten, då köper vi också tjänsten av licenserna till det och då ska det ju sköta sig själv och uppdateras.	
32	F	Så ni har inte bara de som kom med i operativsystemet när man köper datorn, utan ni har köpt till andra brandväggar och antivirus också ovanpå det?	
33	R5	Ja ja, så då har vi en extra liten server som vi kallar för server som bara är en separat arbetsstation som står inlåst i ett rum. Och där är ju en brandvägg och virusprogram och en separat backup externt från den datorn.	
34	F	Ja okej	
35	R5	Så även om vi har våra arbetsstationer så skickar vi allting till den. Men det är inte en riktig server i den benämningen.	
36	F	Är den kopplad till internet eller den är bara kopplat till era datorer?	
37	R5	Nej, det ska vara kopplat till internet	
38	F	Hur kommunicerar ni och delar känslig information? Och då säkerställer att den kommer till rätt mottagare. Du sa ju lite om telefonen att då går man undan. Men exempel när ni har mailkontakt hur säkerställer ni att det är rätt person ni mailar med och att inga känsliga uppgifter följer med i mailen och sånt?	
39	R5	Också när det är personalen, så vet jag ju att dem jag har skickat till, det kommer ju alltid till den personen som har hand om ärendet. Men när det gäller kunder, leverantörer så är det ju väldigt allmänt och då skickar man ju till en kundtjänst. Eller inte kundtjänst, men den som beställer och det är oftast en allmän adress med orderadress eller inköpsadress eller sales, försäljningsadress. Och det är inte känslig information vi skickar. Utan vi…De produkterna vi säljer är ju inte känsliga. Så där inte mycket känsligt eller unikt där.	
40	F	Händer det ibland att ni behöver dela uppgifter som är känsliga? Tänker om man har kommunikation med Försäkringskassan och någon är sjukskriven eller så. Eller det sker bara via post och telefon eller är det någon mailkontakt eller så med dem?	
41	R5	Där är ju mailkontakt med Försäkringskassan och då är det ju inte med sjukskrivning utan oftast har det varit med anställningsformen. Och sen gör de uppföljning varje år så där är en tät kontakt med Arbetsförmedlingen och Försäkringskassan och då får inte dem… vi får lov att skriva och dela till dom men dom får inte lov att skicka det till oss. Så dom kommer oftast hit personligen och gör personliga besök, men annars är det ju inte med...det ska ju inte vara en personuppgift eller namn utan det är oftast bara en initial kanske.	
42	F	Okej ja.	
43	R5	Men oftast har de ju sina ärenden med bara en person, så det är oftast lätt att de vet vem man pratar om utan att ange personnummer.	
44	F	Har alla anställda tillgång till all information?	
45	R5	Nej	
46	F	Och det nämnde du lite tidigare att de på lagret har inte tillgång. Men ni på kontoret, har alla ni tillgång till?	

47	R5	Jag har tillgång till allt.	
48	F	Och sen är dom andra utefter deras roller?	
49	R5	Ja	
50	F	Och är det så inne i systemen också?	
51	R5	Ja, ja, jag har alltid tillgång till allt, men det mest personliga eller mest integritets viktiga är bara jag som har koll på	
52	F	Hur arbetar ni för att verksamhetens information alltid är rätt?	
53	R5	Ge mig ett exempel.	
54	F	En delfråga kan vara: Har ni någon information som finns både på pappersform och i datorn? Och är det så att någon sitter för hand och fyller i den så att det kan bli fel för att någon kanske läser fel ordernummer eller så? Eller är det alltid exakta kopior för att man exempel skannar in det eller något sånt?	
55	R5	Den kan förändras. När vi får ett mail så ligger en order på mejlet och då ska det ju föras över in i systemet så är det manuell hantering. När det är... Alla våra data dokument som ligger uppe på hemsidan. De kan man också printa ut i pappersform, men då är det ju samma person som ser till så att de alltid är uppdaterade så när det ändras i någon förteckning eller någonting så ska ju alla dessa dokument ändras och det görs regelbundet av en person.	I
56	F	Så en person som har det ansvaret?	
57	R5	Ja	
58	F	Nu vet jag inte riktigt hur era system ser ut så då är denna fråga kanske helt onödig men. Finns det något sätt att hindra så att informationen som inte ska ändras råkar ändras eller information som inte ska raderas råka raderas.	
59	R5	Det kan ju vara som så om man hade varit uppe i molnet så hade vi ju inte behövt manuellt föra in en order. Då hade kunden kunnat göra det direkt i ett system. Vi brukar alltid ha kontroller. Vi har inte kontrollen på en order in i systemet, men när väl det packas så har vi alltid dubbla kontroller av vad som sker så en får inte lov att göra allt. Det ska alltid bekräftas av någon annan. Och sen har vi också att när vi får tillbaka det att om det blir ett stort fel så ser nästa person det. Då passar ju inte den uppskattade volymen och vikten in...	I
60	F	Nej, precis.	
61	R5	När vi jämför med siffrorna som kommer manuellt skrivna med… så då får vi ju till viss del viss information från systemet, automatiskt uträknad, och viss det räknar vi själv och sen får vi från lagret och sen ska allt detta matchas ihop.	I
62	F	Och då vet man att det är rätt. När allt stämmer?	
63	R5	Ja. Då kan man ana och hoppas att det är rätt. Man vet inte 100 %, men hade det varit i stället att kunden för in det till exempel så hade det varit lättare. Säkrare på så sätt, men osäkert för att då har man den andra risken i stället som jag ser det som.	
64	F	Och du nämnde också någonting om säkerhetskopiering? Är det allting ni gör som blir säkerhetskopierat eller ni har valt ut viss information?	

65	R5	Valt ut. Vi säkerhetskopierar regelbundet våra system, administrativa program. Då läggs det dels till servern och dels lokalt på våra små enheter, de externa.	
66	F	Så ni har externa hårddiskar?	
67	R5	Ja, så vi har, varje dator har sin externa där vi ska kopiera ner det på. Så även om min kollega jobbar i ett program så kan han kopiera ner det till sin externa. Jag kopierar också ner det till min externa när jag går hem så vi har olika datum på kopiorna och samtidigt så ska det skickas till… så ska det vara en signal från servern till den externa, det ska fungera.	
68	F	Och hur ofta sker det?	
69	R5	Det ska ske varje dygn så vid midnatt så ska den kopiera om allt. Men det är inte på Word, Excel, dokument och så utan då måste vi ju själv aktivt gör det.	
70	F	Så det är de här systemen ni säkerhetskopierar?	
71	R5	Ja	
72	F	Men har ni många viktiga dokument som ligger i Excel, word och så? Eller det är sådan information som ni har tänkt att det är inte så viktigt så den behöver inte säkerhetskopieras?	
73	R5	Så tänker jag nu, men när jag hade tappat det kanske det inte hade varit så oviktigt längre. Då kanske det hade varit väldigt viktigt men just nu så ser jag inte det. Det är mer för mina uträkningar som jag har det.	
74	F	Ja, okej. Hur arbetar ni för att säkerställa att information alltid finns tillgänglig när den behövs?	
75	R5	Vi jobbar ju mest bara med program, så den informationen finns alltid där. Men att den ska vara uppdaterad, då ligger det ju på mig till exempel att jag skulle uppdatera priser. Min kollega ska alltid uppdaterad databladen. Så att vi har olika ansvarsområden på hur ofta den ska uppdateras och vem som gör vad.	I
76	F	Ni har ju flera datorer så om din dator skulle gå sönder, skulle du då kunna gå och sätta dig på någon annan dator för att kunna göra ditt jobb?	
77	R5	Jag kan börja jobba där med de administrativa systemen, men min e-mail hade ju inte varit tillgänglig där.	
78	F	Tillgänglighet kan även vara att om internet går ner, har ni någon tanke om backup på det? Att då tar vi mobilt internet eller vi har något annat? Eller om det är nere så kan inte gå in i de systemen?	
79	R5	Vi har inte riktigt pratat om det, men det är klart att alla har vi olika mobilabonnemang, så det finns ju alltid någon form av internet. Men länge har vi sparat papper också så att inte allt är digitalt. Det fanns en tid när vi är in i det sista kunde… Faktiskt när internet gick ner helt och vi var tvungna att boka…Och de hade inte servicen med internet. Och då var vi tvungna till och skriva fraktsedlar manuellt och boka via en fax. Ja, nu är det flera år sedan. Men jag menar, fram till… man var så van vid att internet alltid fungerar. [borttaget]. Och då fick vi nytta av de här papperna som jag aldrig i livet skulle kunna tro att vi skulle ha nytta av.	
80	F	Finns de kvar idag?	

81	R5	Vi har kvar dem. Jag tror fortfarande att vi hade löst det. Nu är alla uppkopplade på speditörssidan så nu hade vi löst med internet. Och även e-mail till kunder. Så nu tror jag det bara är det som gäller.	
82	F	Ja en [borttaget] utan internet. Ja då blir man kanske lite arg	
83	R5	Ja det var det.	
84	F	Och du har nämnt och ni tillämpar ganska många säkerhetsåtgärder och då är min fråga, hur avgör ni vilka säkerhetsåtgärder ni behöver tillämpa?	
85	R5	….	
86	F	Är det du som tar beslut eller du diskuterar med någon eller du får någon rapport från företag som säger så här ska ni göra. Hur går processen till?	
87	R5	En av delarna, när det gäller vår hårdvara och mjukvara så är det ju den som säljer det som rekommenderar och jag bara gör vad han säger. Är det våra egna backup filer så tycker jag det är viktigt att vi alla gör det regelbundet och det tycker jag vi sköter, så det kommer in på en rutin.	
88	F	Och då är det ditt beslut, Det kommer från dig, liksom?	
89	R5	Det kommer från mig från början, men sen är det ju att det är viktigt för oss alla. Men man märker igen inte det för man har råkat ut för någonting som inte fungerar. Så just nu är det fortfarande, kanske på mitt huvud, att jag vet att det sköts.	
90	F	Och det går lite vidare till den här nästa fråga. Om ni har etablerat en informationssäkerhetspolicy? Står den nedskriven någonstans eller du bara säger det muntligt till folk att tänk på detta. Ni måste göra det här, eller?	
91	R5	Det har vi bara muntligt. Vi har ingen direkt policy, men vi… när ni nu skulle komma så läste jag extra på och då tänker jag också att där är vissa saker som jag tycker, jag har tagit till mig, så då har det kommit ner lite på pränt. Men även om det kommer ner på papper så är det inget vi hade tittat på mer än en gång. Och sen hade vi igen bara trillat tillbaka till rutinerna, men då hade, då finns i alla fall ett papper.	
92	F	Om du säga det att ja, men vi ska göra en kopia av det här, att det ska alla göra. Finns det något sätt att se så att dina anställda faktiskt gör det du säger åt dem?	
93	R5	Man kan se vem som har gjort och när det senast har gjorts.	
94	F	Okej, och om det är andra saker, som hur de hanterar… om ni har andra regler för hur man ska göra saker att ja, exempel lämna inte saker framme på bordet eller något sånt…	
95	R5	Är svårare ja. Men den är ju också att jag säger till, förklarar att det inte det ska ligga uppe med text utan det kan komma in folk. Man måste vända upp och ner på det helst så att inte all information…. Vilket fortfarande inte är jätteviktig information. Det är dock bara våra artiklar, men det är ändå viktigt att vända ifall det kommer in besök eller någonting.	
96	F	Ja och…	
97	R5	Igen, eftersom det är ett undantag, det händer så sällan att folk kommer hit. Då blir det också att, till slut förstår ingen varför man ska göra det, för då gör de det som är lättast för dem. Att alltid ha det uppe. Så det är nog den svåraste delen.	
98	F	Att få folk till att göra som man säger?	

99	R5	Ja alltid.	
100	F	Utbildar ni på företaget er inom informationssäkerhet på något vis.	
101	R5	Nej	
102	F	Och finns det någon anledning till varför ni inte gör det? Er det att ni är så pass få så att det inte känns relevant för er, eller det har bara inte funnits ett behov av det?	
103	R5	Jag tror att det, känslan är nog att vi är lite för få, men samtidigt är det väl också att ju mer vi lägger upp. Igen, jag ser första prioritet som att det är internet som är risken. Och ju mer vi litar på det, eller förlitar oss på det så kan det vara nyttigt att alla får information. Vad, hur och när man ska göra saker och vilka risker man utsätter sig för och kunderna. Och hur man hanterar det på bättre sätt, men… Så vi kanske kommer dit där, men just nu så är det inte så att vi har lagt tid på det.	
104	F	Ja och vi har redan varit inne på denna, men det är mer så att du kan få säga ifall ni har fler saker som du inte nämnde och då är frågan. Vad använder ni för tekniska säkerhetsåtgärder? Och då har du nämnt brandvägg och antivirus program? Finns det något mer? Man kan också till exempel lösenordskydda vissa filer eller lösenordskydda mejl som man ska skicka till folk.	
105	R5	Nej det gör vi inte. Vi har bara som sagt i det administrativa programmet så även om tre kan gå in på samma program så där är det personligt. Och då kan man ju också se vem som har gjort vad. Men annars har vi inga lösenordskyddade filer.	
106	F	Hur arbetar ni med fysiska säkerhetsåtgärder? Och det är ju mer lås, om ni har passerkort, har ni något larm och sånt?	
107	R5	Vi har larm, och det kan vi… Det hade vi också i huset innan att man måste vara i huset för att larma på det ändrade vi för något år, ett år sen och då blir det att man kan också larma på via en app. Och då har vi satt upp också en övervakningskamera. Vi har nycklar och lås. Men som sagt här är olika sektioner som larmas av eller larmas på efterhand var vi befinner oss i huset. Är det någon här uppe så kan vi larma på nedervåningen och är det någon där nere kan vi larm övervåningen. Men annars ja, nyckel och lås.	
108	F	Och den här servern som ni hade, är den inlåst?	
109	R5	Ja	
110	F	Hela tiden eller bara…	
111	R5	Ja hela tiden.	
112	F	Och ni låste in papperna också?	
113	R5	Ja	
114	F	Och sen i fysiska säkerhetsåtgärder så ingår också skydd mot brand. För det kan ju förstöra ens information så har ni några specifika skydd mot brand eller så?	
115	R5	Nej, men då har vi ett kassavalv som sägs vara brandsäkert. Vi har viss information där och vi gör det inte längre, men innan när man kunde ha 3,5 tums diskett så hade vi de där inne i det skåpet, men det har vi inte nu. Nu ligger allting på skrivborden med de här externa hårddiskarna. Så det är vi inte så duktiga på, men personuppgifter och löneuppgifter ligger i kassavalvet. Men kunder och leverantörer, de är bara i ett	

		arkivrum så det har vi ingenting… Vi har brandsläckare och varnings med…Rökvarnare på lagret så ska det vara kopplat till [borttaget], ett säkerhetsbolag.	
116	F	Och de här hårddiskarna som ligger vid datorerna. De låses inte in när ni går hem?	
117	R5	Nej	
118	F	Hur är er tanke kring lösenord? Och då kan det vara ska de bytas på ett speciellt sätt eller hur starka de ska vara? Det någonting ni har pratat om eller?	
119	R5	Vi pratar om det. Och min kollega, hon. Hon har någon släkting som jobbar med sånt här, så det är klart att vi diskuterar det. Men människan är lite bekväm av sig och kör på någon vana. Så vi har lösenord på olika program och inloggningar. Men det…Det är inte så att vi uppdaterar dem, de är inte förnyade. Vi kan till och med ha liknande på flera, så vi vet att vi har brister på det, på grund av att också vara kollega trycker lite på att vi måste vara lite mer aktiva. Jag har en [borttaget] som också som tjatar om att vi måste ha några svårare ramsor och att man kan få lätt hjälp i appar. Vi har inte kommit dit ännu, men det tryck lite på.	
120	F	Är det så också att det… som vissa gör när det är så många olika lösenord så sätter man det till och med på post its?	
121	R5	Nej, det gör vi inte.	
122	F	Det försöker ni undvika?	
123	R5	Ja där går gränsen.	
124	F	Precis…	
125	R5	Vi använder A4 ark i stället [skrattar]	
126	F	Ja precis, de ska synas.	
127	F	Sen tänkte jag fråga lite om... För nu kan det komma till exempel mail med länkar som man inte riktigt ska klicka på, och att man kanske inte riktigt ska ladda ner vad som helst från internet. Är det någonting ni tänker på och pratar om, undviker och så?	
128	R5	Det tycker jag att killarna är bra på. De är rätt generation, så de är jätte uppmärksammade på det.	
129	F	Så om någonting ser konstigt ut så…	
130	R5	Klickar de inte alls och de är undersöker först om det är någon annan som har skrivit någonting om någonting som ser suspekt ut. Jag hade telefonsamtal idag. Det var en inspelad röst som sa att, han pratar på engelska och sa att han ringde från svenska polisen. Och, jag var tvungen att klicka.	
131	F	Ja, man får vara observant nu för tiden.	
132	R5	Och slår jag upp telefonnumret, så är det ingen som har skrivit någonting om att det är bedrägeri eller någonting. Jag är den enda som hade sökt på det telefonen. Så de använder kanske tusentals med telefon också så det blir vassare och vassare. Men det pratar vi nog mer ofta om, sådant.	
133	F	Har det hänt att någon har råkat, klicka på någonting eller laddat ner något som har gjort att det har lett till att ni har fått något Virus eller något sånt?	

134	R5	Ja, det kan ha varit så för flera år sedan när det, innan det började bli så vanligt. För att då har vi fått problem med våra datorer. Så det kan också vara att det är därför vi är så försiktiga med det. För att man har upplevt negativa sidan på det.	
135	F	Och hur är det med, vad ska man säga, okända personer som går här? Har ni koll på vem som är här och hur släpper ni in folk?	
136	R5	Det har vi. Vi är ju ett litet företag så vi är inte så många här. Så dagtid är vi bara oss, plus de där nere så 10 personer, kanske max, men sen på kvällstid så har vi… det är aktiviteter här uppe på andra våningen och då har jag informerat att vi har en kamera så här är övervakat. Och sen är det larmat, de är bara inne i rummen som inte är larmade. Och då larmar vi av sektioner och allt annat är låst och de rummen de är tomma.	
137	F	Så där ligger ingen känslig information eller så?	
138	R5	Nej	
139	F	Så, har Michelle något att tillägga?	
140	F1	Nej, jag tyckte du ställde bra följdfrågor också.	
141	F	Toppen. Har du någonting som du vill tillägga som du känner att, det här har ni inte frågat mig om eller det här gör vi jättebra, så det borde ni verkligen veta eller något sånt?	
142	R5	Nej det enda jag tänker på är möjligtvis GDPR, men det är det enda.	
143	F	Och vad tänker du kring det?	
144	R5	Det är också ett område som kanske, det är där är lagkrav på det, men att som företagare så kanske man inte riktigt vet exakt vad som gäller, hur länge? Och ja, men vad som är känsligt och vad som man får lov att spara, hur länge man får spara det, och vad man ska göra när det inte är aktivt längre	
145	F	Är det svårt att ta reda på den informationen? Har man någon att vända sig till, att rådfråga eller hur upplever du det som företagare?	
146	R5	Jag upplever att det är jag själv som måste, ta information, söka. Och även när vi har aktivitet i huset så är det många som bara på grund av aktivitetens karaktär så är det många som filmar in eller spelar in och även det ligger under GDPR. Men det är ingen som tänker på det i de forumen. Och att man alltid ska vara försiktig med vad man lägger ut på internet med ja med ansikte och att folk som kanske inte, alla kanske inte vill vara med på de här klippen.	
147	F	Ja, det är ett stort område, GDPR	
148	R5	Ja, så det är inte bara det här med företag, namn, personuppgifter så utan även alla som lägger ut på de sociala medierna. Så det, det är ju omöjligt att bromsa, men...	
149	F	Ja, det är det. Och har ni pratat om det på jobbet? Att, liksom vad som får läggas ut på sociala medier om ert jobb och vad som inte får läggas ut?	
150	R5	Vi har ju inte heller så mycket. När vi tar våra inspirationsbilder så är det ju också, då nämner vi och pratar om att det är viktigt att det bara kanske är fötter och ben och ryggar som syns. Vi vill inte visa gärna ansikte. Sen kan man ju köpa bilder och där är det ju ansikte.	

151	F	Ja	
152	R5	Men då har de ju kommit överens om att, skrivit ett avtal med de personerna kan jag tänka mig och informerat om, i alla fall att de är i en bildbank som säljs	
153	F	Precis	
154	R5	Men när det gäller de här aktiviteterna och jag säger det, så är det nog ingen som tänker på det eller tar det som allvarligt överhuvudtaget?	
155	F	Nej, precis.	
156	R5	Det var en liten parentes.	
157	F	Ja, men det är bra att lyfta, för det hänger ihop med detta. Det ena är vad ska jag göra för att skydda och det andra är, men vad säger lagen att jag måste göra för att jag inte ska bli straffad liksom.	
158	R5	Och det är till och med en avgift eller en straffavgift. Men det hade jag ingen aning om.	
159	R5	Nej nej det kan bli ganska saftigt. Ja då avslutar jag inspelningen.	

Appendix 9 – Intervju Respondent 6

1 maj 2022 - fysisk intervju
R6 - Respondent, F - Författare, F1 - Författare 2

Rad	Person	Frågor och svar	Kod
1	F	Då börjar vi. Vilken roll har du på detta företag?	
2	R6	Jag är den som driver företaget	
3	F	Är det ett aktiebolag eller enskild firma?	
4	R6	Enskild firma	
5	F	Hur många personer arbetar i detta företag? Ja, en då	
6	R6	Ja, endast en	
7	F	Och vad använder ni för IT stöd? Och då är det både hårdvara, men också mjukvara, det vill säga programmen på exempelvis, datorer och sånt.	
8	R6	Så att jag har ju liksom inget direkt IT stöd, men om jag ska nämna programmen som jag använder så är det [borttaget] som är journalsystem och sen så använder jag [borttaget] när jag registrerar patienter. Jag använder [borttaget] i ekonomi. Det var nog dom som jag använder i företaget.	
9	F	Excel och word. Är det någonting?	
10	R6	Ja Excel och word använder jag ju. Inte så mycket Word, men det händer ju. Jag använder någon sådant scanning program, app, i telefonen.	
11	F	Och vad är det du skannar?	
12	R6	Träningsprogram. Jag kan kolla vad den heter. Lens någonting, det är nog Microsoft. … Ja, det är sådan scanning.	
13	F	Och sen är det en bärbar dator?	
14	R6	Ja, precis. Bärbar dator och mobiltelefonen.	
15	F	Har du någon, fax eller skrivare?	
16	R6	Skrivare har jag ju på arbetsplatserna, så det är ju inte mitt egna. Har ju en skrivare privat också och som enskild firma så kanske det räknas in.	
17	F	Ja, använder du den till liksom…	
18	R6	Ja	
19	F	Toppen har du gått någon utbildning i informationssäkerhet?	
20	R6	Nej	
21	F	Då så, hur definierar du informationssäkerhet?	

22	R6	Så som jag tänker. Så tänker jag hur man skyddar information som inte ska ut till allmänheten. Så som jag tänker en del för mig kan ju vara mobilt bankid som jag använder mycket till och logga in på olika program. Typ så ja, att någon obehörig ska inte få tillgång till. Vad ska man säga? Kritisk information. Typ så.	K
23	F	Det som vetenskapen och dom som jobbar med informationssäkerhet säger, Det är väldigt likt det du säger. Då är det att all information att man vill bevara 3 olika egenskaper hos sin information och då är det konfidentialiteten. Att ingen kommer åt det. Integriteten att den inte ändras när du inte vill att den ska ändras. Och tillgängligheten. Att när du behöver den ska den finnas där så det är dom tre. Det är inte bara digital information utan det gäller all information. Som det som är i pappersform. Det kan vara muntlig information när man pratar i telefon eller då pratar med någon patient. Att andra kanske inte hör det. Så att ja alltså det är den här breda som vi tänker på. Så du har det i åtanke att det inte bara i datorn utan det är liksom allt. Och nästa fråga är, vet du vilken information som är viktig att skydda för ditt företag? Och då behöver du inte säga liksom ja, men det är denna och denna. Utan mer, vet du vad som är viktigt?	
24	R6	Alltså för mig så är det ju viktigt att skydda patienternas personnummer till exempel. Och att den ska komma ut att personen söker vård hos mig, så till exempel att inte prata om patienter. Ja, som vanligt som sjukgymnast att jag får inte sitta på ett café och prata om patientfall och hela den här biten. Så det är väl mycket det och vad gäller mitt företag i och med att de skriver på mig själv och mitt personnummer så är egentligen information om företaget på ett så transparent för andra, så där gäller det ju ja. För mig att inte läcka ut patientinformation via mitt företag, tänker jag.	K
25	F	Och nästa fråga, du varit inne lite på det det. Hur arbetar ni för att säkerställa att obehöriga inte ska få tillgång till företagets information?	
26	R6	Som jag sa innan så har jag mobilt bankid för att logga in i journalsystem och i [borttaget]. Det som är ett problem för mig och som jag ännu inte har löst. Det är att när jag lägger in bokföringsmaterial i mitt bokföringsprogram så kommer vårt patientens personnummer med. Och det är ju en stor brist. Men annars så är det ju ett problem är ju också att jag har 2 arbetsplatser och att jag ibland flyttar material mellan arbetsplatserna, till exempel remisser från ena till andra och då har jag det i min väska när jag åker till jobbet liksom så det är ju också en risk. Likadant med mina kvitton för bokföringar, dom ska ju lagra i x antal år, 7 eller 10, nåt av det något av. Och då måste jag skriva ut kvittona och då har jag personnummer så att jag borde ju egentligen ha ett låst skåp där jag förvarar alla mina bokföringsmaterial.	
27	F	Hur förvaras de idag?	
28	R6	Nu förvaras de hemma hos oss, i pärmar. Vi har larm hemma. [skrattar]	
29	F	Ja nej, men det är sånt som intressant veta. Ja, och hur funkar det exempel, Du sa att du använder din dator, låses den in när du inte använder den eller den är också?	
30	R6	Det är också lite samma risk där att den har jag ju tillgänglig. Det är ju både för mig, min privata dator och min jobbdator så den har jag ju också med mig liksom i en väska till och från jobbet. Och om jag någon gång åker tåg och ska jobba så sitter jag och jobbar liksom på datorn, så det är ju också en stor risk. Där kan man ju skriva journaler så att inte personnumret syns. Men namn kan synas. Ja, och det är ju också ett problem.	

31	F	Och hur kommunicerar och delar du känslig information? Och det kan vara så kanske med din bokföring person, om du nu har någon, eller till exempel om du måste kontakta patienterna. Hur?	
32	R6	Om jag förstår frågan rätt så är det ju så här. Jag har ingen revisor, utan jag sköter allt det själv så att det blir ju rätt så begränsat till att det är jag.	
33	F	Du kommunicerar med dig själv och det går på ett tryggt sätt?	
34	R6	Ja, det är en inre kommunikation. Sen får jag ju hjälp utav min man när vi ska göra bokslut till exempel så mitt företag blir rätt så transparent gentemot honom. Men han är ju aldrig inne och kollar på kvitton på patienter liksom, utan det är ju mer företaget i helhet. Kan du ta frågan en gång till, känns som jag missar svara på någonting.	
35	F	Hur kommunicerar och delar du känslig information?	
36	R6	Mhm.. Skulle det vara så att jag behöver skicka remissen någonstans. Då skickar jag det med post och tänker att det borde vara okej eftersom att typ ja regionen till exempel eller andra privata aktörer gör på samma sätt. Sen har jag kanske inte kollat upp exakt vad som gäller, men jag skickar som material med post.	
37	F	Har du mailkontakt eller så med patienten?	
38	R6	Precis när jag har mailkontakt med patienter så skickar jag inga personnummer via mailen. Och ibland så gör ju patienterna det själva utan att jag har bett om det. Skulle jag behöva personnummer till en patient så ringer jag till patienten. För att få tag på personnummer. För att slippa att det ska synas i mail.	
39	F	Så du försöker…	
40	R6	Försöker värna	
41	F	Men det är din patient då som väljer att…	
42	R6	Patienterna verkar ofta vara väldigt liberala med att skicka sina personnummer, signerar ofta mail med namn och personnummer och då kan jag känna jag att jag kan inte riktigt ta ansvar för det.	
43	F	Nej, precis. Ja vi hoppar frågan om alla anställda har tillgång till all information den känns som…	
44	R6	[skrattar] Ja jag hoppas att jag har tillgång till all information	
45	F	Och då är nästa fråga. Hur arbetar du för att verksamhetens information alltid är rätt?	
46	R6	Rätt, alltså att jag sprider rätt information om mitt företag?	
47	F	Nej, utan det kan vara all information som finns i företaget. Hur säkerställer du att den är rätt? Att personnumret är att det är till rätt person, eller att om du har en excelfil med massa siffror att det inte är fel i dem och sånt exempelvis.	
48	R6	Ja alltså. Så där kan jag väl mer tänka att det är alltså ekonomiskt till exempel att man kollar med balansräkningar och så att allting är rätt och in. Jag fakturerar ju varje månad och att då säkerställa att det jag fakturera stämmer överens med det faktiskt som dragit in och där använder jag ju Excel mycket för att stämma av det… Vad gäller personnummer och så på patienter så är det ju någonting som dom delar till mig. Sen så händer det ju ibland att jag kan skriva in fel telefonnummer till exempel.	I

		Men personnummer dubbelkollar jag alltid en gång extra för att annars får jag inte betalt om jag har fel personnummer.	
49	F	Så personnummer står lite högre upp på listan och telefonnummer är lite mindre känslig information och därför behövs den inte dubbelkollas?	
50	R6	Mm	
51	F	Ja, men då förstår jag det. Och har det hänt att du, att du får fel information? Kanske alltså en faktura eller något sånt?	
52	R6	Det har aldrig hänt.	
53	F	Det har inte hänt utan du vet, vilka du ska få?	
54	R6	Ja, Ofta så handlar det om att jag fakturerar. Det är inte jättemånga som fakturerar mig, det är ju typ mobiltelefon och allt sånt och det går på e-faktura som flera år tillbaka, så det känner jag att det liksom rullar på. Så där har inte fått någon fejk, vad jag vet.	
55	F	Så om försöker lura dig, så…	
56	R6	Då är jag rätt så uppmärksam på vad jag spenderar mina pengar på. Om det är någonting som är rimligt eller inte.	
57	F	Och nästa fråga är då. Hur eller om du arbetar med säkerhetskopiering på något sätt?	
58	R6	Jag säkerhetskopierar via vad heter det, Google drive och sen, så har jag en extern hårddisk som jag lägger över information på.	
59	F	Så har det både i molnet och så har du det på en extern hårddisk också?	
60	R6	Och i pappersform. Inte alla journaler. Journalerna ligger i ett specifikt journalsystem. Där har jag ingen backup.	
61	F	Ja säkerhetskopiering. Du sa att det ligger på system också?	
62	R6	Ja	
63	F	Och hur ofta gör dom här säkerhetskopieringar?	
64	R6	I Google drive går automatiskt, så jag gissar att den gör det. Gissar, jag tror att det gör det liksom en gång om dygnet, alltså ungefär. Borde säkerhetskopiera till min externa hårddisk ofta än vad jag gör. Men det är händer kanske någon gång mellan dag 50 och 100.	
65	F	Ja, men det är bättre än aldrig	
66	R6	Ja, mycket bättre.	
67	F	Ja nästa fråga är då, hur arbetar du för att säkerställa att information alltid finns tillgänglig när den behövs?	
68	R6	Alltså, det är ju att jag har tillgång till exempel mitt journalsystem, bokföringssystem och allting både via datorn och telefonen, så det är ju egentligen där jag hämtar informationen. Och det tycker jag är rätt så tillgängligt, jag har oftast telefonen med mig. Eller ja, oftast datorn med.	T

69	F	Och behöver du internet för att komma åt dem?	
70	R6	Ja, det behöver jag	T
71	F	Så om internet ligger nere…	
72	R6	Så är det ett problem	T
73	F	Men då kanske du har någon annan plats du kan åka till? Du kanske inte har extra internet där du är,	
74	R6	Men om inte hela världens internet ligger nere så bör jag kunna få internet antingen på arbetsplatserna eller någon annanstans.	T
75	F	Ja, och hur avgör du vilka säkerhetsåtgärder du behöver tillämpa för att skydda företagets information?	
76	R6	Där har jag nog mest gått på känsla, vad som känns bra. Jag betalar ju lite extra varje månad, till exempel för att ha det att det skulle gå in med mobilt bankid på Journal programmet till exempel för det känns som ett bra val att göra. Och likadant när jag loggar in i bokföringssystemet så har jag det här med tvåfaktorsautentisering. Så där har jag ju gjort dom valen för att jag tycker att det känns bra att det ska vara bundet till mig. Det är nog det.	
77	F	Så är det vad som känns bra? Det är inte så att du har någonstans där du inhämtar information från som säger att du borde göra så här?	
78	R6	Nej, egentligen inte. Alltså det enda jag hämtat in information om är ju att ja, men jag ska bevara journaler 7 år och sen tror jag att bokföringen står i 7 eller 10 är. Det är dom två jag blandar ihop. Men jag vet ju om att jag ska lagra information så pass länge och det är väl det jag kollat upp. uppenbarligen inte så bra, men jag har koll på att på att det är några år, så jag behåller dom.	
79	F	Jo, jag tänkte fråga dig också när vi pratar om internet ligger ner så kan du hitta någon annanstans. Men om det du har en dator och jobbar på, vad skulle hända ifall den gick sönder eller att någon snor den?	
80	R6	Det är ju såhär att jag har ju inte mitt journalsystem bundet där, utan det är ju jag kan lätt köpa en ny dator. Har jag glömt datorn när jag går till jobbet så kan jag logga in på en annan dator och hämta det där och det samma gäller ju med bokföringen och så där. Det som försvinner för mig om någon snor datorn. Det är mina verifikationer. På patientbetalningar och där är ju ett problem då att där står personnummer på dom, så det är ju en stor brist.	T
81	F	Ja, det är ju alltid tråkigt när någon stjäl ens saker	
82	R6	Ja, jag håller hårt i mina saker.	
83	F	Och då är nästa fråga, har du etablerat en informationssäkerhetspolicy?	
84	R6	Nej	
85	F	Och finns det en anledning till att du inte har gjort det här så har du tänkt att nej det behövs inte för det är bara jag.	
86	R6	Ja, ungefär så har jag tänkt. Det är väldigt liten skala på företaget. Hade jag haft anställda så tror jag att då hade det känts mer viktigt för mig, nu är det bara jag. Och så då. Känns det ja, inte aktuellt helt enkelt.	

87	F	Och nästa fråga. Vi har ju frågat ifall du har gått en utbildning och det kan ju vara utbildning tidigare. Men utbildar ni er någonting på företaget om informationssäkerhet? Om det kommer upp nya…Nu är det nya regler	
88	R6	Nej	
89	F	Ja och sen så är nästa fråga, vad använder ni för tekniska säkerhetsåtgärder? Det kanske vara brandvägg antivirusprogram. Att du krypterar saker för att skydda din information.	
90	R6	Jag har fått för mig det här. Det här har [borttaget] hjälpt mig med. Pinsamt att säga det. Nej, men jag har fått för mig att det finns någon form av kryptering i hur det lagras uppe i Google. Vet inte, men annars krypterar jag ingenting. Så alls.	
91	F	Brandvägg?	
92	R6	Brandvägg och antivirus. Men inte mer än det som är på datorn.	
93	F	Det som kommer med datorn?	
94	R6	Ja, jag har inte köpt till någonting extra eller någonting sånt. Jag kör på det som finns.	
95	F	Är du sån som uppdaterar när det kommer nya uppdateringar till mobiler, datorer direkt eller du som skjuter på det för att du tycker det är jobbigt?	
96	R6	Jag är lite bakåtsträvande, så det tar lite tid innan jag uppdaterar både dator och telefon.	
97	F	Nästa fråga är då, hur arbetar ni med fysiska säkerhetsåtgärder? Och då nämnde du till exempelvis larm.	
98	R6	Ja, vi har hemlarm. Där jag har min dator och telefon. Vi har ju larm på arbetsplatserna också och där är ju låsta dörrar och hela den här biten. Vi har ju till exempel inget säkerhetsskåp, vilket i den bästa utav världar där jag förvarar mitt material skulle vara både brandsäkert och inbrottssäkert. Men det har jag inte. Min säkerhet ingår där också?	
99	F	Alltså dig som person? Nja, det är bara information. [Skrattar]. Och ni har lås på huset då också antar jag?	
100	R6	Ja	
101	F	Mot brand?	
102	R6	Ja, brandlarm som också är kopplat till alltså, jag har ju kombinerat inbrotts och brandlarm så att det går till en central som i så fall också kan skicka hit brandbilar om de ser på våra kameror i huset att det är en utvecklad brand.	
103	F	Ja, okej. Det är ju smidigt	
104	R6	Brandsläckare, och brandfilt	
105	F	Ja, jag tänkte på någonting som du har sagt nu flera gånger att i den bästa av världar så skulle vi haft ett brandsäkert skåp till exempel. Vad är det som gör att det inte är i den bästa världen? Vad är det som hindrar dig från att ta steget att göra det?	

106	R6	Dels, så kan det vara lite ekonomi. Att köpa in de här grejerna. Sen är det väl att så många andra gör på ungefär samma sätt, liksom att det är lite accepterat på något sätt att ja, man gör sitt bästa, men kanske inte hela vägen. Så jag tror att det är det. Plus att jag också har känt att det är så litet.	
107	F	Ja nej, för det är intressant att höra vad det är för hinder. Alltså så, det är en sak att inte vara medveten, men en annan sak att vara medveten och inte göra det. Hur är din tanke kring lösenord?	
108	R6	Ja, jag kan inte så mycket mer om lösenord mer än att man ska använda stora och små tecken och siffror och så där så jag försöker ju att ha så kallade säkra lösenord. Men jag har ju till exempel inte de här säkra lösenorden som datorn slumpar fram för då blir det lite mer beroende utav att jag alltid loggar in på datorn och till exempel inte kan logga in på telefonen. För att jag kommer inte kunna komma ihåg ett sånt starkt lösenord och få rätt på det varje gång jag ska logga in. Så jag har försökt att hitta någon form utav medelväg och då att kombinera det med att jag måste identifiera mig när jag loggar in också, så att jag har inte endast lösenord utan även ja tvåvägs autentisering och mobilt bankid.	
109	F	Hur ofta byter du lösenord? Är det något du har en tanke om eller du kör på dom du har?	
110	R6	Jag kör på dom vi har och nu ska vi se. Nej, jag har inte bytt på journalsystemet. Bokföringsprogrammet har jag bytt på 2 gånger. Men det har varit när jag har bytt mobiltelefon och så här så har det försvunnit lite tvåvägs identifieringen och då jag var tvungen att liksom återställa. Så det har inte varit på eget initiativ.	
111	F	Har du samma lösenord på olika, eller du försöker…?	
112	R6	att hålla olika. Där kanske är en viss grund som liknar varandra, men sen så är det alltid någon skillnad.	
113		Hur tänker du kring att öppna okända mail och klicka på länkar?	
114		Jag skulle vilja säga att jag är ganska medveten om att inte klicka på vilka länkar som helst och bra på att kolla upp. Och jag får inte så ofta konstiga mail.	
115		Hur ser det ut när du är på kontoret, har du då papper och känslig information framme som andar kan komma åt?	
116		Ja, det kan ligga framme så att både kollegor och patienten kan komma åt det.	
117	F	Michelle har du något att tillägga?	
118	F2	Nej	
119	F	Har du något att tillägga som du känner att det här jag är bra? Det här gör jag inte lika bra? Ja, något som du känner att du inte har fått ta upp som du vill nämna?	
120	R6	Jag tycker att jag fått nämna det jag vill nämna.	
121	F	Toppen	

Referenser

Andress, A. (2003). Surviving Security: How to Integrate People, Process, and Technology, 2 uppl, [e-bok] Auerbach Publications, Tillgänglig online: https://doi.org/10.1201/9780203501405 [Hämtad 26 april 2022]

Andress, J. (2014). The basics of information security: Understanding the fundamentals of InfoSec in theory and practice, 2 uppl, [e-bok] Burlington: Elsevier Science, Tillgänglig genom: LUSEM bibliotek hemsida https://www.lusem.lu.se/library [Hämtad 8 april 2022]

Association for Information Systems (AIS). (u.å.). Senior Scholars' Basket of Journals, Tillgänglig online: https://aisnet.org/page/SeniorScholarBasket [Hämtad 13 april 2022]

Baker, W.H., & Wallace, L. (2007). Is Information Security Under Control?: Investigating Quality in Information Security Management, *IEEE Security & Privacy*, vol. 5, nr. 1, s. 36–44, Tillgänglig genom: LUSEM bibliotek hemsida https://www.lusem.lu.se/library [Hämtad 24 mars 2022]

Bhaskar, R., & Kapoor, B. (2013). Information Technology Security Management, i Vacca, J.R. (ed), *Computer and information security handbook*, 3 uppl, [e-bok] Cambridge: Elsevier, Morgan Kaufmann, s.35-44, Tillgänglig genom: LUSEM bibliotek hemsida https://www.lusem.lu.se/library [Hämtad 25 april 2022]

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*,vol. 34, nr. 3, s. 523–548, Tillgänglig genom: LUSEM bibliotek hemsida https://www.lusem.lu.se/library [Hämtad 12 april 2022]

Chen, M.T. (2013). Guarding Against Network Intrusions, i Vacca, J.R. (ed), *Computer and information security handbook*, 3 uppl, [e-bok] Cambridge: Elsevier, Morgan Kaufmann, s. 149–163, Tillgänglig genom: LUSEM bibliotek hemsida https://www.lusem.lu.se/library [Hämtad 22 april 2022]

Dhillon, G., & Backhouse, J. (2000). Information system security management in the new millennium, *Communications of the ACM*, vol. 43, nr. 7, s. 125–128, Tillgänglig genom: LUSEM bibliotek hemsida https://www.lusem.lu.se/library [Hämtad 9 mars 2022]

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives, *Information Systems Journal*, vol. 11, nr. 2, s. 127, Tillgänglig genom: LUSEM bibliotek hemsida https://www.lusem.lu.se/library [Hämtad 29 mars 2022]

European Commission. (u.å.). SME Definition, Tillgänglig online: https://ec.europa.eu/growth/smes/sme-definition_en [Hämtad 9 mars 2022]

Fulp, W.E. (2013). Firewalls, i Vacca, J.R. (ed), *Computer and information security handbook*, 3 uppl, [e-bok] Cambridge: Elsevier, Morgan Kaufmann, s. 219–237,

Tillgänglig genom: LUSEM bibliotek hemsida https://www.lusem.lu.se/library [Hämtad 25 april 2022]

Ghaffari, F., Gharaee, H., & Arabsorkhi, A. (2019). Cloud security issues based on people, process and technology model: a survey, *2019 5th International Conference on web research (ICWR)*, s. 196–202, Tillgänglig genom: LUSEM bibliotek hemsida https://www.lusem.lu.se/library [Hämtad 25 april 2022]

Gupta, A., & Hammond, R. (2005). Information systems security issues and decisions for small business: An empirical examination, *Information Management & Computer Security*, vol. 13, nr. 4, s. 297–310, Tillgänglig genom: LUSEM bibliotek hemsida https://www.lusem.lu.se/library [Hämtad 8 april 2022]

Harley, K., & Cooper, R. (2021). Information Integrity: Are We There Yet?, *ACM Computing Surveys (CSUR)*, vol. 54, nr. 2, s. 1–35, Tillgänglig genom: LUSEM bibliotek hemsida https://www.lusem.lu.se/library [Hämtad 20 april 2022]

Heidenreich, M. (2017). How to design a method for measuring IT security in micro enterprises for IT security level measuring? A literature analysis, *2017 Communication and Information Technologies (KIT)*, s 1–9, Tillgänglig genom: LUSEM bibliotek hemsida https://www.lusem.lu.se/library [Hämtad 24 mars 2022]

Heidenreich, M. (2019). Conceptualization of a Measurement Method Proposal for the Assessment of IT Security in the Status Quo of Micro-Enterprises, *2019 International Conference on Computing, Electronics & Communications Engineering (iCCECE)*, s. 187-192, Tillgänglig genom: LUSEM bibliotek hemsida https://www.lusem.lu.se/library [Hämtad 9 mars 2022]

Heidt, M., Gerlach, J.P., & Buxmann, P. (2019). Investigating the security divide between SME and large companies: How SME characteristics influence organizational IT security investments, *Information Systems Frontiers*, vol. 21 nr. 6, s. 1285–1305, Tillgänglig genom: LUSEM bibliotek hemsida https://www.lusem.lu.se/library [Hämtad 10 april 2022]

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

Jayadevappa, B., & Soh, B. (2009). A new risk analysis method for data backup strategy, *TENCON 2009–2009 IEEE Region 10 Conference*, s. 1–6, Tillgänglig genom: LUSEM bibliotek hemsida https://www.lusem.lu.se/library [Hämtad 21 april 2022]

Kaila, U., & Nyman, L. (2018). Information Security Best Practices: First Steps for Startups and SMEs, *Technology Innovation Management Review*, vol. 8, nr. 11, s. 32–42, Tillgänglig genom: LUSEM bibliotek hemsida https://www.lusem.lu.se/library[Hämtad 10 april 2022]

Katsikas, S.K. (2013). Risk Management, i Vacca, J.R. (ed), *Computer and information security handbook*, 3 uppl, [e-bok] Cambridge: Elsevier, Morgan Kaufmann, s. 507–527, Tillgänglig genom: LUSEM bibliotek hemsida https://www.lusem.lu.se/library [Hämtad 25 april 2022]

Keller, S., Powell, A., Horstmann, B., Predmore, C., & Crawford, M. (2005). Information Security Threats and Practices in Small Businesses, *Information Systems Management,* vol. 22, nr. 2, s. 7–19, Tillgänglig genom: LUSEM bibliotek hemsida https://www.lusem.lu.se/library [Hämtad 9 mars 2022]

Kotkova, B., & Hromada, M. (2021). The Threat of Social Engineering and The Safety of Companies, *2021 25th International Conference on Circuits, Systems, Communications and Computers (CSCC)*, s. 126–133, Tillgänglig genom: LUSEM bibliotek hemsida https://www.lusem.lu.se/library [Hämtad 9 mars 2022]

Kotulic, A.G., & Clark, J.G. (2004). Why there aren't more information security research studies, *Information and Management*, vol. 41, nr. 5, s. 597–607, Tillgänglig genom: LUSEM bibliotek hemsida https://www.lusem.lu.se/library [Hämtad 29 mars 2022]

Kurpjuhn, T. (2015). The SME security challenge, *Computer Fraud & Security*, vol. 2015, nr 3. s. 5–7, Tillgänglig genom: LUSEM bibliotek hemsida http://www.lusem.lu.se/library [Hämtad 15 mars 2022]

Monev, V. (2020). Defining and Applying Information Security Goals for Blockchain Technology, *2020 International Conference on Information Technologies (InfoTech)*, s. 1–4, Tillgänglig genom: LUSEM bibliotek hemsida http://www.lusem.lu.se/library [Hämtad 12 april 2022]

Myndigheten för samhällsberedskap (MSB). (2015). Detta är informationssäkerhet, Tillgänglig online: https://www.informationssakerhet.se/om-informationssakerhet2/vad-ar-informationssakerhet/ [Hämtad 10 mars 2020]

Nagahawatta, R., Lokuge, S., Warren, M., & Salzman, S. (2021). Cybersecurity Issues and Practices in a Cloud Context: A Comparison Amongst Micro, Small and Medium Enterprises, *arXiv preprint arXiv:2111.05993*, Tillgänglig genom: LUSEM bibliotek hemsida http://www.lusem.lu.se/library [Hämtad 9 april 2022]

Nyak, U., & Rao, U.H. (2014). The InfoSec handbook - an introduction to information security, [e-bok] Berkeley: Apress, Tillgänglig genom: LUSEM bibliotek hemsida https://www.lusem.lu.se/library [Hämtad 22 mars 2022]

Oates, B.J. (2006). Researching Information Systems and Computing. London: SAGE

Parker, D.B. (1998). Fighting computer crime: a new framework for protecting information, New York: Wiley

Paulsen, C. (2016). Cybersecuring Small Business, *Computer*, vol. 49, nr. 8, s. 92–97, Tillgänglig genom: LUSEM bibliotek hemsida https://www.lusem.lu.se/library [Hämtad 15 mars 2022]

Renaud, K., & Weir, G.R.S. (2016). Cybersecurity and the Unbearability of Uncertainty, *2016 Cybersecurity and Cyber Forensics Conference (CCC)*, s. 137–143, Tillgänglig genom: LUSEM bibliotek hemsida https://www.lusem.lu.se/library [Hämtad 15 mars 2022]

Rees, J. (2010). Information security for small and medium-sized business, *Computer Fraud & Security*, vol. 2010, nr. 9, s. 18–19, Tillgänglig genom: LUSEM bibliotek hemsida https://www.lusem.lu.se/library [Hämtad 10 april 2022]

Sadok, M., Alter, S., & Bednar, P. (2020). It is not my job : exploring the disconnect between corporate security policies and actual security practices in SMEs, *Information and Computer Security*, vol. 28, nr. 3, s. 467–483, Tillgänglig genom: LUSEM bibliotek hemsida https://www.lusem.lu.se/library [Hämtad 10 april 2022]

Samonas, S., & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security, *Journal of Information Systems Security*, vol. 10, nr. 3, s. 21 - 45, Tillgänglig online: https://www.proso.com/dl/Samonas.pdf [Hämtad 8 mars 2022]

Svenska institutet för standarder (SIS). (2015). Teknisk rapport SIS-TR 50:2015, Terminologi för informationssäkerhet, Tillgänglig online: https://www.sis.se/standarder [Hämtad 15 mars 2022]

Sajal, S.Z., Jahan, I., & Nygard, K.E. (2019). A Survey on Cyber Security Threats and Challenges in Modern Society, *2019 IEEE International Conference on Electro Information Technology (EIT)*, s. 525–526, Tillgänglig genom: LUSEM bibliotek hemsida https://www.lusem.lu.se/library [Hämtad 23 mars 2022]

Siponen, M.T. (2005). An analysis of the traditional IS security approaches: Implication for research and practice, *European Journal of Information Systems*, vol. 14, nr. 3, s. 303–315, Tillgänglig genom: LUSEM bibliotek hemsida https://www.lusem.lu.se/library [Hämtad 29 mars 2022]

Syafitri, W., Shukur, Z., Mokhtar, U.A., Sulaiman, R., & Ibrahim, M.A. (2022). Social Engineering Attacks Prevention: A Systematic Literature Review, *IEEE Access*, vol 10, s. 39325–39343, Tillgänglig genom: LUSEM bibliotek hemsida https://www.lusem.lu.se/library [Hämtad 25 april 2022]

Talu, S. (2020). Strategic Measures in Improving Cybersecurity Management in Micro and Small Enterprises, *2nd International Scientific and Practical Conference on Digital Economy (ISCDE 2020)*, s. 522–528, Tillgänglig online: https://www.atlantis-press.com/article/125947796.pdf [Hämtad 7 februari 2022]

Tsochev, G, Trifonov, R., Nakov, O., Manolov, S., & Pavlova, G. (2020). Cyber security: Threats and Challenges, *2020 International Conference Automatics and Informatics (ICAI)*, s. 1–6, Tillgänglig genom: LUSEM bibliotek hemsida https://www.lusem.lu.se/library [Hämtad 15 mars 2022]

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security, *Computers & Security*, vol. 39, s. 97–102, Tillgänglig genom: LUSEM bibliotek hemsida https://www.lusem.lu.se/library [Hämtad 17 maj 2022]

Watad, M., Washah, S., & Perez, C. (2018). IT security threats and challenges for small firms: Managers' perceptions, *International Journal of the Academic Business World*, vol 12, nr 1, s. 23–30, Tillgänglig genom: LUSEM bibliotek hemsida https://www.lusem.lu.se/library [Hämtad 15 mars 2022]

Wood, C.C. (2004). Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature Computer Fraud and Security, vol. 2004, nr. 1, s. 16–17, Tillgänglig genom: LUSEM bibliotek hemsida https://www.lusem.lu.se/library [Hämtad 12 april 2022]