UPTEC STS 22031
Examensarbete 30 hp
Juni 2022

UPPSALA UNIVERSITET

Informationssäkerhet och den mänskliga faktorn

En tillgång eller ett hot?

Alice Dahlquist

Civilingenjörsprogrammet i system i teknik och samhälle

UPPSALA
UNIVERSITET

Information security and the human factor: An asset or a threat?

Alice Dahlquist

Abstract

As a result of an increasingly digital society, an even higher demand regarding a reliable information security can be seen. In the past, IT-security was something that mostly affected the IT departments of organizations, today it has become an obvious part of the business. A majority of the safety measures that have been implemented in organizations earlier are of technical character. Nowadays, an increasing need to involve the user can be seen.

The impacts of the human factor and human contribution can be seen as two main concepts with reference to theory within the area. In email security, which is in fact the most common attack vector, the human factor is taken advantage of in order to gain access to the organization. As the attacks are getting worse and appearing more frequently, the purpose of this study is to see in what ways organizations should and could work with the human factor and human contribution in order to succeed in their information security work.

A literature study and semi-structured interviews have been conducted in order to gather empirical data. The results show that in order to succeed with the information security work, organizations have to take the cognitive abilities into consideration. This involves creating awareness around the topic, establishing an understanding and making sure the employees realize the consequences and impact an action can result in. A recurring challenge within organizations can also be seen regarding being able to meet the needs of each individual employee.

Teknisk-naturvetenskapliga fakulteten

Uppsala universitet, Utgivningsort Uppsala

Handledare: Magnus Göras Ämnesgranskare: Anders Arweström Jansson

Examinator: Elísabet Andrésdóttir

Populärvetenskaplig sammanfattning

I och med ett alltmer digitaliserat samhälle ställs också högre krav på att en tillförlitlig informationssäkerhet måste finnas. Tidigare var IT-säkerhet något som enkom berörde organisationers IT-avdelning, idag är det en vedertagen del av verksamheten. I takt med att informationen även fått en allt större strategisk och operativ roll inom organisationer har värdet av denna kommit att bli ett konkurrensmedel. Tidigare säkerhetsåtgärder har främst omfattat tekniskt avancerade skydd, idag går det att se ett ökat behov av att även involvera användarens roll i dessa skydd.

I denna uppsats studeras därför den mänskliga faktorn och det mänskliga bidraget i relation till informationssäkerhetsarbetet. Vad som åsyftas är i korta drag det mänskliga beteendet som finns hos alla användare i samtliga system - utifrån ett användarperspektiv. Utan det mänskliga bidraget finns det ingen som varken skapar, utvecklar eller förvaltar systemen samtidigt som kognitiva begränsningar gör att misstag och felaktiga beslut kan komma att utgöra hot och orsaka skada vilket benämns som den mänskliga faktorn.

Inom e-postsäkerhet, som är den vanligaste attackvektorn när det kommer till angrepp mot organisationer idag, är det ofta den mänskliga faktorn som är anledningen till att dessa attacker lyckas. Nätfiske har kommit att bli ett allt vanligare angreppssätt där social manipulation används för att lura användaren att agera på ett skadligt sätt för organisationen. Även om attackerna kommit att bli alltmer frekventa och djupgående än tidigare är det dock en majoritet av attackerna som misslyckas till följd av det mänskliga bidraget.

Syftet med denna studie är att undersöka hur organisationer bör arbeta med den mänskliga faktorn och det mänskliga bidraget, det vill säga de anställda, för att få optimal effekt i sitt informationssäkerhetsarbete och därmed kunna rikta sina resurser där de gör störst skillnad. Initialt studeras därför vilken betydelse och inverkan den mänskliga faktorn har när det kommer till informationssäkerhet för att få en förståelse kring vad som är möjligt att göra. Mer specifikt studeras sedan hur en verksamhet bör arbeta för att dra nytta av det mänskliga bidraget i sitt informationssäkerhetsarbete kopplat till e-post.

För att finna svar på dessa frågeställningar har inledningsvis en litteraturstudie gjorts. Utifrån denna litteraturstudie har sedan en teoretisk referensram skapats i form av en analysmodell i ett försök att visualisera vilka komponenter denna studie har omfattats av. Den empiriska datainsamlingen har sedan genomförts i form av intervjuer som då utgått från denna analysmodell. Slutligen har en tematisk analys genomförts av de resultat som framkommit under intervjuerna.

Studiens resultat visar på att den mänskliga faktorn och det mänskliga bidraget har en betydande roll i organisationers informationssäkerhetsarbete. Som användare i systemen är det alltid människan som tar det avgörande beslutet och således har medarbetaren en central roll. Mer specifikt framkommer det att människans kognitiva förmågor behöver tas i beaktning för att uppnå en optimal effekt av sitt informationssäkerhetsarbete. Detta involverar i sin tur att skapa medvetenhet, etablera en förståelse och få medarbetarna att inse konsekvenserna av vardera individs agerande. En stor utmaning i detta ligger i att kunna bemöta vardera individ utefter dennes individuella behov.

Förord

Denna uppsats markerar slutet på min utbildning vid Civilingenjörsprogrammet System i Teknik och Samhälle vid Uppsala universitet. Jag vill rikta ett varmt tack till alla de som funnits där under min studietid vilket inkluderar såväl vänner som familj. Ni som hejat på, peppat och gratulerat men även stöttat och visat ett ständigt intresse när vägen inte alltid varit spikrak – tack!

Under uppsatsens gång har ett antal personer varit av extra stor betydelse:

Tack till Martin Malm för initial handledning, utan dig hade detta inte påbörjats.

Tack Magnus Göras för fortsatt handledning, tillsammans kunde vi driva detta i mål.

Tack till ämnesgranskare Anders Arweström Jansson som varit ett ständigt stöd under processens gång.

Slutligen, tack till alla de respondenter som tagit sig tid att ställa upp.

Med det vill jag önska trevlig läsning!

Alice Dahlquist

2022-06-15

Innehållsförteckning

1. Inledning

Med målet att bli bäst i världen på att utnyttja digitaliseringens möjligheter finns även ett starkt behov av att öka kunskapsnivån vad gäller informations- och cybersäkerheten i Sverige. Detta framgår tydligt i regeringens nationella säkerhetsstrategi publicerad 2017 där digitala risker, informations- och cybersäkerhet pekas ut som ett av sex fokusområden (Statsrådsberedningen, 2017). Tidigare var IT-säkerhet något som enkom berörde organisationers IT-avdelning, idag är det en vedertagen del av verksamheten. I takt med digitaliseringens framfart suddas gränsen mellan arbete och privatliv ut, samtidigt får informationen en allt större strategisk och operativ roll inom organisationer vilket också ställer högre krav på säkerhetsaspekten. Dagligen görs omfattande investeringar i avancerad teknik i hopp om att kunna skydda sig mot såväl nuvarande som framtida hot, faktum är dock att den tekniska aspekten bara är en del av det totalskydd som krävs (Oscarson, 2019. s.269).

Ett av de områden som kommit att bli alltmer förekommande är vikten av att inkludera den mänskliga faktorn och det mänskliga bidraget i sitt säkerhetsarbete. Detta framgår framför allt i Hallbergs et al. *Informationssäkerhet och organisationskultur* från 2017 som menar på att även om tekniken spelar en viktig roll i den digitala utvecklingen utgör människors beteenden, agerande och attityder en central roll. Här utgör den mänskliga faktorn ett hot genom de kognitiva begränsningar och brister som förekommer hos alla användare. Å andra sidan möjliggör användaren många gånger den digitalisering vi kan se idag vilket i sin tur kan härledas till det mänskliga bidraget (Gonzalez och Sawicka, 2002; Hollnagel, 2014). Traditionellt har informationssäkerhetsarbetet kretsat mestadels kring de tekniska lösningarna, idag kan ett stort behov identifieras när det kommer till att involvera människan i dessa lösningar (Hallbergs et al., 2017. s.11). Även Riksrevisionen, som har till uppdrag att granska statens verksamhet, lyfte redan 2007 behovet av att involvera människans roll (RiR 2007:10). Vid uppföljningen 2016 visade dock den resulterande rapporten att arbetet fortfarande inte håller en tillräcklig nivå för att kunna anses som tillfredsställande (RiR 2016:8).

I takt med att allt fler enheter idag kopplas upp mot internet skapas potentiella ingångar för hackare och hot (Oscarson, 2019. s.26). Alltmer information hanteras, lagras och kommuniceras även digitalt trots att brister kan ses bland informationshanteringens konfidentialitet, tillgänglighet och riktighet (Oscarson, 2019. s.47). Ur en rapport publicerad 2020 av det som idag benämns som det nationella cybersäkerhetscentret framgår att speciellt attacker via e-post är ett framgångsrikt angreppssätt då den utnyttjar den mänskliga faktorn och bristfälliga skyddsbarriärer (SÄPO, 2020. s.15-16).

1.1 Syfte och problemformulering

Till följd av den inledning som presenterats kan ett ökat behov av tillförlitlig informationssäkerhet tydliggöras. Samtidigt framkommer att kunskapsbrist föreligger inom området för att organisationer effektivt ska kunna bemöta de hot och sårbarheter som föreligger. Vad som blir allt tydligare är behovet att utforma informationssäkerhetssystem med den mänskliga faktorn och det mänskliga bidraget i åtanke för att ha optimal verkan. Vidare är det inte självklart hur dessa bör implementeras och involveras i verksamheten för önskad effekt vilket denna uppsats därför syftar till att undersöka med förhoppningen om att kunna bidra till att fylla åtminstone en del av denna kunskapslucka.

Denna uppsats författas i samarbete med Trafikverket som är Sveriges tredje största myndighet och innehar därav en betydande roll i samhället. Genom digitaliseringens framfart ställs allt högre krav, inte minst på säkerhet, inom organisationen för att förhindra och skydda den vitala infrastruktur som finns i Sverige. Syftet med denna studie är därför att undersöka hur kunskap om den mänskliga faktorn och det mänskliga bidraget kan komma att implementeras i verksamhetens säkerhetsarbete för att ytterligare stärka det skydd som finns mot de hot som föreligger. Målet med studien är förbättrad kunskap och i förlängningen en förmåga att hantera de risker och hot som föreligger specifikt vad gäller människans roll inom e-posthantering. Studien ämnar således att undersöka:

- Vilken betydelse och inverkan har den mänskliga faktorn när det kommer till informationssäkerhet?

- Hur bör verksamheten arbeta för att dra nytta av det mänskliga bidraget i sitt informationssäkerhetsarbete kopplat till e-post?

1.2 Avgränsningar

Denna studie är avgränsad till att undersöka svensk hantering och arbete kring informationssäkerhet. Detta då det finns stora skillnader i aspekter såsom lagstiftning och förhållningssätt globalt, vilket inte varit eftersträvat att involvera i ändamålet för denna uppsats. Informationssäkerhet omfattar i regel all typ av information vilket involverar format såsom ljud, bild, film, tal och text vilka i sin tur kan bearbetas, lagras och kommuniceras. I denna studie har begränsningar gjorts genom att främst undersöka hur den digitala informationen behöver skyddas till följd av arbetets inriktning mot e-postsäkerhet. Slutligen har studien avgränsats till att kolla på det intraorganisatoriska informationssäkerhetsarbetet med tanke på den tidsram och omfång som arbetet tilldelats.

1.3 Begreppsdefinition

Den mänskliga faktorn är ett begrepp som har en central roll under denna uppsats vilket syftar till att skildra det mänskliga beteendet. I alla system finns en användare, en människa, som innehar såväl kognitiva begränsningar som möjligheter vilka kan komma att bli sårbarheter. Med den mänskliga faktorn avses därför ofta, men inte alltid, en säkerhetsrisk vilket kan härledas till människans beteende i olika situationer. Begreppet saknar generellt en vetenskaplig definition men vedertaget är ändå ett mänskligt felhandlande som olycksorsak. Oscarson (2019) belyser dock det faktum att människor hela tiden tar beslut och finns på plats för att avvärja hot och undvika misstag och att det endast är en liten del av dessa beslut som resulterar i skada (s.269). Det är här det mänskliga bidraget kommer in som, i motsats till den mänskliga faktorn, belyser människans förmågor och kunskaper som en nödvändig resurs. Begreppet fokuserar i stället på att så mycket som möjligt ska lyckas och på så vis minimera risken för en olycka (Hollnagel, 2014). Forskning visar på att ett fullgott skydd inte kan uppnås med enbart teknik utan ett samspel mellan tekniken och användaren måste finnas, med andra ord behöver hänsyn tas till både den mänskliga faktorn och det mänskliga bidraget vilket kan utgöra såväl begränsningar som möjligheter (Gonzalez och Sawicka, 2002).

1.4 Disposition

Till att börja med inleds denna uppsats med att tydliggöra relevansen för det valda ämnesområdet - informationssäkerhet inom Sverige. Däribland vilka brister som finns samt vilka konsekvenser dessa får i dagens alltmer digitaliserade samhälle. Vidare presenteras den problematik som finns kring e-post för att slutligen landa i betydelsen av den mänskliga faktorn och det mänskliga bidraget inom informationssäkerhetsarbetet, vilka även har centrala roller i uppsatsens frågeställningar.

I efterföljande bakgrund framhävs det ökade behovet av tillförlitlig informationssäkerhet som föreligger i samhället, här tydliggörs även varför informationssäkerhet är så viktigt och vad det är som styr arbetet. Skillnader och likheter vad gäller privat kontra offentlig sektor tas upp och olika typer av säkerhetsåtgärder presenteras. I den slutliga ämnesteoretiska bakgrunden definieras först begreppet informationssäkerhet utefter fyra aspekter för att sedan gå in mer på människans roll, den mänskliga faktorn och det mänskliga bidraget. Slutligen presenteras tidigare forskning inom området e-postsäkerhet i förhållande till den mänskliga faktorn innan den analysmodell som kommer att ligga till grund för denna studie introduceras.

Under metodavsnittet presenteras och redogörs för de metodval som gjorts under studiens gång. I detta fall har en kvalitativ abduktiv metod tillämpats i form av semistrukturerade intervjuer, litteraturstudier samt datainsamling genom sekundära källor. Vid analys av insamlade data har tematisk analys sedan använts där utvalda teman har härletts från den teoretiska referensramen som presenteras under metodens analysmodell.

Vid presentation av studiens resultat grupperas respondenternas svar utefter de utvalda teman som varit grundläggande under denna studies struktur och uppbyggnad. Dessa återanvänds sedan under uppsatsens diskussion och analys för att på ett tydligt sätt knyta an till den forskning som tidigare presenterats under uppsatsens teoriavsnitt. Avslutningsvis presenteras de slutsatser som framkommit samt förslag på vidare och framtida forskning inom området.

2. Bakgrund

I detta avsnitt följer inledningsvis grundläggande information och bakgrund till det växande behovet av informationssäkerhet. Vidare tydliggörs vad det är som styr informationssäkerhetsarbetet och hur detta skiljer sig i privat respektive offentlig sektor. Slutligen presenteras olika typer av säkerhetsåtgärder.

2.1 Behovet av tillförlitlig informationssäkerhet växer

I Per Oscarsons bok *Informationssäkerhet* från 2019 beskrivs ett alltmer digitaliserat samhälle som i sin tur skapar beroenden vilka ställer höga krav på att tillförlitlig cyber- och informationssäkerhet måste finnas. Historiskt har det länge funnits ett behov av informationssäkerhet i någon form. I takt med internets framfart under 1990-talet kom dessutom flertalet branschers sätt att arbeta att ändras samtidigt som förflyttningen från det analoga till det digitala öppnade upp för kriminell verksamhet såsom bedrägeri, sabotage och spionage (Oscarson, 2019. s.20). Bara under senaste åren har allt fler it-attacker fått genomslag och drabbat samhället på flertalet plan. Utöver stora inkomstförluster visar detta även på de hot och sårbarheter som kommer med ett digitaliserat samhälle och inte minst, vikten av informationssäkerhet (KPMG, 2020).

Att det blir allt vanligare att företag utsätts för cyberattacker visar en nyligen publicerad studie från Svenskt Näringsliv (2021) där flertalet av Sveriges största bolag intervjuats. Undersökningen visar på att vidden av attackerna både blivit alltmer frekventa och djupgående än tidigare där nätfiske har kommit att bli ett återkommande bekymmer. Genom e-post skickar avsändaren mail, ofta genom att utge sig för att vara någon annan, så kallad *spoofing,* där mottagaren sedan uppmanas att exempelvis klicka på länkar innehållandes skadlig kod. Attackerna beskrivs av respondenterna i rapporten som ett ständigt brus där riktat nätfiske idag utförs med grundlig research innan angriparen stegvis arbetar sig inåt i organisationen. Med målet att penetrera system hos organisationer har det också framkommit att organisationer i nuläget inte har den beredskap som krävs för att hantera och lösa den situation som råder. Följaktligen blir konsekvenserna allt större i takt med svårare attacker där dagens skydd av IT-systemen inte håller måtten (Svenskt Näringsliv, 2021). Ur en rapport publicerad 2020, författad av de myndigheter som idag ingår i Sveriges cybersäkerhetscenter, kan en ökning vad gäller utnyttjandet av användarens förtroende för molnbaserade tjänster ses i syfte att få användaren att agera utefter angriparens önskemål. När angriparen väl gjort intrång i systemet används sedan offrets identitet för att utnyttja andras förtroende för att komma åt ytterligare information på väg mot det utsatta målet (SÄPO, 2020. s.15-16).

2.2 Vad styr informationssäkerhetsarbetet

Idag styrs informationssäkerhetsarbetet främst av vilka behov och förutsättningar respektive verksamhet har vilket gör att varje enskilt studerat fall kan se olika ut (Ewald, 2018. s.22). Alla organisationer har dock ett grundläggande behov av att implementera informationssäkerhetsmässiga åtgärder. Initialt handlar det ofta om att efterfölja de grundläggande regelverk och lagar som finns för att överhuvudtaget kunna verka i det digitaliserade samhälle som vi lever i idag. På EU-nivå regleras och prioriteras området bland annat genom NIS-direktivet, *The Directive on security of network and information systems,* som syftar till att gemensamt hålla hög standard på säkerhet i nätverk och informationssystem. I Sverige ansvarar Myndigheten för samhällsskydd och beredskap,

MSB, för att detta eftersträvas och finns implementerat i både lagar och förordningar. Under 2021 upprättades även ett nationellt cybersäkerhetscenter på uppdrag av regeringen bestående av flertalet myndigheter som syftar till att tillsammans förstärka Sveriges förmåga att förebygga, upptäcka och hantera cyberhot (Cybersäkerhetscenter, 2021).

Oscarson (2019) ser informationssäkerhet som en nödvändighet och en förutsättning för att kunna uppfylla de förväntningar samhället har på en verksamhet. I och med att allt fler tjänster sköts digitalt tillkommer även ett allt större behov av att erbjuda kunderna säkra lösningar (s.48). Samtidigt som nya tekniker och metoder utvecklas för att motverka digitaliseringens baksida finns även en antagonist redo att hitta svagheter och potentiella ingångar för att i stället skapa skada, ofta med monetära motiv. Emellertid menar Oscarson (2019) på att en god informationssäkerhet inte bara ska ses som ett måste eller ett krav utan med en god informationssäkerhet finns fler argument för att faktiskt satsa tid och resurser på att lyckas. Om inte annat kan ett regelbrott eller annan händelse som påvisar ett misslyckat informationssäkerhetsarbete ha förödande konsekvenser. Utöver straff såsom böter och viten kan verksamhetens förtroende komma att skadas vilket kan leda till att omvärlden väljer att ta avstånd vilket kan bli dyrt att åtgärda, om det överhuvudtaget går, eller i värsta fall leda till konkurs (Oscarson, 2019. s.49). Generellt kan sägas att hela syftet med att inneha en god informationssäkerhetsnivå medför kostnadsbesparingar. Genom att reducera de risker som föreligger genom att implementera de skyddsåtgärder som krävs förebyggs potentiella incidenter vilket skapar bättre och stabilare verksamheter å ena sidan. Å andra sidan förskonas verksamheten från att utöver att gå miste om monetära medel, även slippa förkasta tid och relationer vilka kan komma att försämras såväl externt som internt i organisationen vid en eventuell incident (Oscarson, 2019. s.50). En ytterligare aspekt som kan komma att vara av betydelse när det kommer till att implementera ett fullgott informationssäkerhetsarbete är att det i vissa fall kan krävas en viss nivå eller certifiering för att överhuvudtaget vara aktuell vid en upphandling (Oscarson, 2019. s.52).

2.2.1 Offentlig sektor

När det kommer till myndigheter är det lagstadgat att ett systematiskt och riskbaserat informationssäkerhetsarbete ska bedrivas, likaså för de verksamheter som omfattas av NIS-direktivet och lagen om samhällsviktiga och digitala tjänster (Ewald, 2018. s.46). NIS-direktivet översätts på svenska till "*Åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen*" och omfattar i sin tur både privata och offentliga aktörer inom sju olika sektorer vilka anses vara viktiga för att upprätthålla kritisk samhällelig och ekonomisk verksamhet (MSB, 2022). För statliga myndigheter finns det sedan 2016 även en föreskrift från MSB som innebär att det systematiska och riskbaserade informationssäkerhetsarbetet även ska ske med utgång från ett ledningssystem såsom ISO 27000. Problematiken med ISO 27000 är dock att den inte anger några konkreta lösningar eller tillvägagångssätt till att uppnå certifiering utan standarden talar snarare om *att* och *vad* som behöver införas än *hur* detta skall göras, det är upp till vardera verksamheten och organisation att själva avgöra (Ewald, 2018. s.52). Utöver NIS-direktivet och ISO 27000 omfattas även myndigheter av offentlighets- och sekretesslagen (2009:400) vilken innefattar bestämmelser kring handläggningen av allmänna handlingar (Sveriges riksdag, 2022).

2.2.2 Privat sektor

När det kommer till privat sektor påverkas i många fall mindre företag av vilka ekonomiska resurser som finns tillgängliga. Detta spelar roll utifrån både ett resurs-och kostnadsperspektiv då informationssäkerhetsarbetet i grunden utgår, utformas och begränsas av dessa förutsättningar. Även om privata företag inte omfattas på samma sätt som statliga myndigheter av lagar och regler kring vad som måste finnas implementerat ligger det ändå i vardera verksamhets intresse att skydda sig mot potentiella hot och incidenter som skulle kunna orsaka skada. Däremot handlar det inte enbart om att arbeta med informationssäkerhet för att skydda den egna verksamheten utan också aspekter såsom att bibehålla och stärka förtroendet med omgivande relationer, vilket är minst lika viktigt för att näringen ska kunna fortlöpa, vara motståndskraftig och överleva (Oscarson, 2019. s.20).

2.3 Informationssäkerhetsarbetet i verksamheten

Inom området informationssäkerhet är det viktigt att skilja på *interorganisatoriska* sammanhang som syftar på att beskriva förhållandena *mellan* organisationer likt ett nätverk medan *intraorganisatoriska* sammanhang syftar till att beskriva förhållanden *inom* organisationer (Hallberg et al., 2017. s.61). Enligt Oscarson (2001) utgörs dock grunden för en god interorganisatorisk informationssäkerhet av en god intraorganisatorisk informationssäkerhet och vice versa (s.3). Oscarson (2001) menar på att det i takt med att organisationers information, som kan betraktas som en tillgång, har kommit att bli alltmer värdefull har betydelsen av informationssäkerhet såväl internt som externt kommit att bli ett konkurrensmedel (s.4). Tillgångarna kan i sin tur utsättas för ett eller flera olika slags hot vilka tillsammans bildar en hotbild. Hot inom informationssäkerhet innebär att det finns potentiella händelser som, om de inträffar, förväntas leda till försämring av informationens konfidentialitet, riktighet, tillgänglighet eller spårbarhet. Sammantaget kan hot vara avsiktliga eller oavsiktliga, externa eller interna (Oscarson, 2019. s.77). Om ett hot faktiskt realiseras benämns detta som en incident. Till skillnad mot ett hot, som syftar på en framtida händelse, anger en incident något som händer nu eller något som redan har hänt. Följaktligen kan hoten fortfarande kvarstå trots att en incident redan inträffat och skapat skada vilket syftar på en negativ konsekvens av incidenten (Oscarson, 2007. s.64). Detta visualiseras i Figur 1 vilket är en egen illustration med inspiration tagen från Oscarsons avhandling *"Informationssäkerhet i verksamheter"* från 2001.

Figur 1: Visualisering av ett hot som realiseras till en incident som leder till en skada hos den tillgång som drabbas.

Historiskt har arbetet kring informationssäkerhet främst handlat om att skydda värdefull information genom att applicera tekniskt avancerade lösningar. Idag handlar det snarare om att på en organisatorisk nivå styra sitt informationssäkerhetsarbete utifrån kärnverksamhetens behov. Med andra ord handlar det inte längre om att ha de mest tekniskt avancerade lösningarna utan snarare se vad som är mest relevant i den kontext verksamheten befinner sig inom (Ewald, 2018. s.17). Ewald (2018) påpekar vidare att informationssäkerhetsarbetet inte ska ses som en egen entitet utan utgör en stödfunktion vilken har som mål att fungera även när nya förutsättningar uppkommer och med det nya

hot och risker. Ett riskbaserat arbete där ledningen behöver prioritera och se till att arbetsinsatserna resulterar i både kostnads- och resurseffektiva riskreduceringar (Ewald, 2018. s.24).

Inom organisationer kan variationer fortfarande finnas vad gäller implementering och uppdelning av säkerhetsåtgärder. Svensson (1999) skiljer på IT-säkerhet, fysisk säkerhet och personsäkerhet som alla syftar till att skydda någon typ av information. Ewald (2018) har likt Svensson (1999) också delat upp informationssäkerheten i tre delar, dels den fysiska säkerheten och IT-säkerheten men sedan valt att benämna den tredje delen som organisatorisk säkerhet vilken har kommit att få en allt större roll i dagens digitaliserade samhälle (Ewald, 2018. s.65). Oscarson (2019) har å andra sidan valt att dela upp säkerhetsåtgärderna efter de administrativa, kunskapsbaserade, IT-baserade samt de fysiska. Då den sistnämnda uppdelningen tydliggör vad som ingår under vardera kategori har detta sätt tillämpats vid uppdelning av säkerhetsåtgärder under författandet av denna uppsats.

2.3.1 Administrativa åtgärder

Till att börja med finns de administrativa åtgärderna vilka involverar olika typer av styrmedel och rutiner som enligt Oscarson (2019) nödvändigtvis inte behöver vara explicit uttryckta i text utan kan likväl kommuniceras genom tal eller underförstådda i verksamhetens kontext (s.107). Vidare kan de administrativa åtgärderna vara både beslutade likt lagar och regler eller vedertagna som en del av den kultur som råder. Exempel på administrativa säkerhetsåtgärder är policys, lagar, regler och rutiner (ibid).

2.3.2 Kunskapsbaserade åtgärder

Kunskapsbaserade säkerhetsåtgärder involverar den kunskap och medvetenhet som finns hos individen verksam inom organisationen. En hög grad av kunskap kring ämnet är avgörande för att kunna uppnå en god informationssäkerhetsnivå vilket sker genom bland annat utbildning. I slutändan är det individen, människan, som arbetar med de tekniska och administrativa som tagits fram som hjälpmedel för att uppnå en viss grad av säkerhet. Samtidigt är det även människan som både skapar, använder och förvaltar den innovation som framkommit och implementerats i verksamheten vilket ställer höga krav på både kunskap och medvetenhet inom säkerhetsområdet hos individen i fråga (Oscarson, 2019. s.270).

2.3.3 Tekniska åtgärder

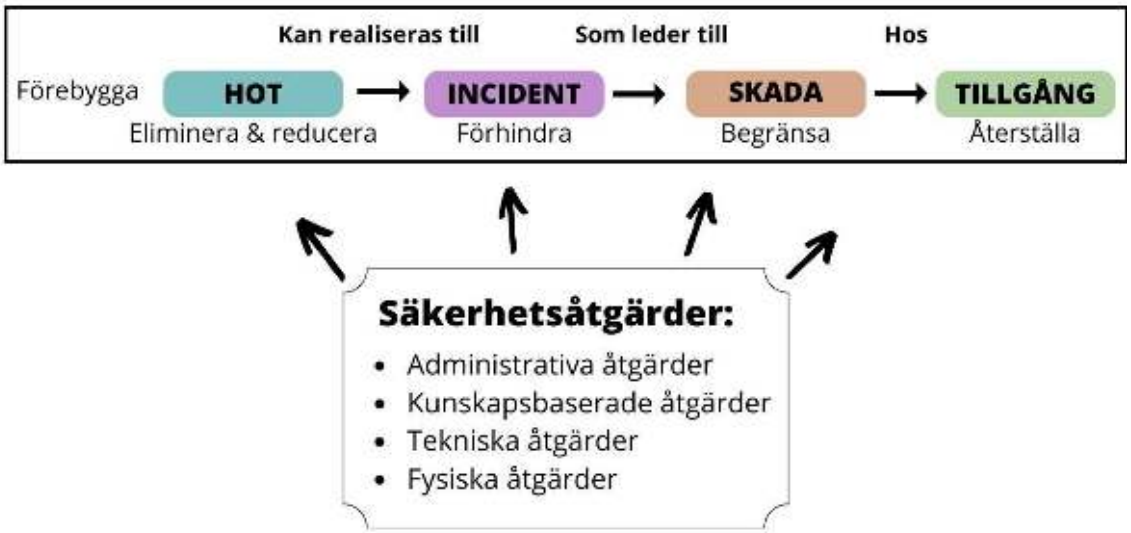
IT-baserade säkerhetsåtgärder kan bestå av mjukvara, hårdvara eller bådadera i IT-system och -produkter vilka har till funktion att skydda. Oscarson (2019) menar på att en majoritet av de IT-baserade säkerhetsåtgärderna syftar till att motverka användarfel genom att exempelvis införa webbfilter samt behörighets- och kontrollsystem. Funktionerna är ofta dolda och till viss del automatiserade genom att arbeta exempelvis med detektering av avvikande användarbeteende (s.109). En växande del av säkerhetsarbetet inom flertalet organisationer har dock kommit att bli utkontrakterat (eng: outsourcing) där hela eller delar av verksamhetens tekniska informationssäkerhetsarbete idag utförs av en extern part. Ewald (2018) understryker dock att detta medför en ökad risk om den egna kompetensen minskar när framtiden i själva verket kräver desto mer kunskap inom området för att helt enkelt kunna förstå, styra och utveckla det framtida säkerhetsarbetet å verksamhetens vägnar (s.67).

2.3.4 Fysiska åtgärder

Slutligen finns de fysiska säkerhetsåtgärderna vilka utgör ett direkt skydd genom exempelvis lås, larm, inpasseringsskydd och dokumentskåp (Oscarson, 2019. s.109). Enligt Ewald (2018) syftar den fysiska säkerheten till att skydda information såväl inom som utanför organisationens lokaler (s.76). När det kommer till att skydda utrustning utanför de egna lokalerna vilket har kommit att bli alltmer förekommande i och med bärbara enheter tillämpas bland annat användarrutiner och tekniska skydd likt kryptering och åtkomstlösningar (Ewald, 2018. s.89).

En viktig aspekt gällande IT-säkerhet är den snabba föränderlighet som finns inom området vilket ställer höga krav på kompetens bland medarbetarna. Då det oftast en kombination av ovan nämnda säkerhetsåtgärder som tillsammans skapar det ultimata skyddet ställs ytterligare krav på bred kompetens även inom verksamheten. Oscarson (2019) betonar vikten av att alltid ha en helhetssyn där fysiska och IT-baserade skydd i princip alltid behöver innefatta en viss grad av administrativt och kunskapsbaserade skydd för att fungera på ämnat och optimalt sätt (s.109).

Oscarson (2001) påpekar även att olika typer av skydd har olika syften beroende på den tidsmässiga relationen till incidentens inträffande. Genom att arbeta proaktivt och förebyggande är målet att reducera de hot som föreligger vilket kan ske genom att exempelvis utbilda sin personal eller upprätta regelverk och policys. Följaktligen gäller det vid ett uppkommet hot som realiseras till en incident att implementera mer direkta åtgärder såsom brandväggar och fysiska lås. Om incidenten ändå inträffar gäller det att försöka begränsa skadan genom att till exempel tillämpa antivirusprogram. Om skadan ändå är gjord gäller det att kunna återställa informationens ursprungliga skick genom att exempelvis ha en säkerhetskopia redo. Detta illustreras i Figur 2 som är en fortsättning till Figur 1 som båda utgår från Oscarsons olika publiceringar inom ämnet informationssäkerhet (Oscarson 2001; Oscarson 2007).



Figur 2: Visualisering av olika steg av skydd som bör tillämpas i relation till säkerhetsbristens utveckling.

3. Ämnesteoretisk bakgrund

I detta avsnitt presenteras en mer vetenskapligt begrundad teoretisk bakgrund till det studerade området. Inledningsvis definieras begreppet informationssäkerhet utifrån fyra aspekter vilka tillämpas i lagar och regler idag. Vidare diskuteras den mänskliga faktorn och det mänskliga bidragets roll i förhållande till informationssäkerhetsarbetet samt informationssäkerhetskulturens roll. Slutligen kopplas dessa delar till informationssäkerhetsarbetet inom e-postsäkerhet innan den analysmodell som används under uppsatsen presenteras.

3.1 Att definiera informationssäkerhet

Att vara medveten om vilka hot som existerar och skydda sig mot dessa har alltid funnits i människans natur. Informationssäkerhet är således ett begrepp applicerbart på flertalet områden i samhället vilket medför att detta är ett komplext och tvärvetenskapligt ämne att studera (Oscarson, 2019. s.53). Att IT-området även är under ständig förändring gör det än mer svåröverskådligt att greppa (Oscarson, 2007. s.2). Sammantaget för de lagar och förordningar som tillämpas i Sverige idag utgår begreppet informationssäkerhet från tre grundläggande aspekter vilka i sin tur härrör från den så kallade CIA-definitionen eller CIA-triaden. CIA är i sin tur en akronym sammansatt från engelskans *confidentiality, integrity* och *availability* vilka på svenska översatts till konfidentialitet, riktighet och tillgänglighet (Ewald, 2018. s.29). Dessa aspekter är bland annat implementerade i den mest etablerade standarden inom informationssäkerhet i Sverige och internationellt, SS-EN ISO/IEC 27000, de används därmed också i MSB:s föreskrifter inom området.

3.1.1 Konfidentialitet

I korthet syftar konfidentialitet till att skydda informationen mot obehörig insyn. Med andra ord eftersträvar denna aspekt att skydda informationen från att tillgängliggöras eller avslöjas för obehöriga individer, enheter eller processer vilket kan ses som en binär egenskap (Oscarson, 2019. s.69). Skyddet kan i sin tur innebära skydd mot både intern och extern obehörig åtkomst. Enligt Ewald (2018) behöver skyddet inte enbart upprättas med tanke på rättsliga eller legala skäl utan kan även grunda sig i andra orsaker. Graden av skydd är också dynamisk över tid och kan i kombination med annan information komma att bli extra känslig, så kallad *aggregerad information* (Ewald, 2018. s.31).

3.1.2 Riktighet

Riktighet handlar om att informationen ska vara fullständig och korrekt, alltså ett skydd mot oönskad förändring. Likt konfidentialitet är även riktighet en binär egenskap vilket innebär att kriteriet för om skyddet är tillgodosett kan besvaras med ett ja eller nej (Oscarson, 2019. s.70). Att bryta skyddet mot riktighet kan ske genom en obehörig, ett misstag eller funktionsstörning vilket främst är applicerbart inom datoriserade processer (Ewald, 2018. s.32).

3.1.3 Tillgänglighet

Tillgänglighet innefattar kravet på att informationen ska vara åtkomlig och användbar på begäran av en behörig inom en viss tid. Likt konfidentialitet är tillgängligheten också en dynamisk faktor vilken beror på sin kontext. Ewald (2018) menar alltså på att behovet av åtkomsten till informationen ofta skiftar över tid vilket innebär att prioriteringar behöver

göras för att uppfylla informationssäkerhetens syfte, att reducera verksamhetens risker på ett kostnadseffektivt sätt (s.32).

3.1.4 Spårbarhet

Utöver konfidentialitet, riktighet och tillgänglighet har en fjärde säkerhetsaspekt kommit att få en allt större betydelse inom informationssäkerheten, nämligen *spårbarheten.* Enligt Ewald (2018) har denna aspekt kommit att bli alltmer aktuell i och med de transaktioner som sker frekvent i samhället idag. Över en längre tid kan det vara av hög betydelse att kunna härleda informationens bakgrund och härstamning för att kunna lokalisera eventuella förändringar eller återskapa en tidigare version. Tidigare har spårbarheten snarare setts som ett komplement till övriga tre säkerhetsaspekter men allt fler involverar denna aspekt i sitt säkerhetsarbete (Ewald, 2018. s.41). Ur rapporten *Informations- och cybersäkerhet i Sverige: Strategi och åtgärder för säker information i staten* (2015) går att läsa att informationssäkerhet utöver riktighet, tillgänglighet och konfidentialitet även innefattar "*att det går att följa hur och när informationen har hanterats och kommunicerats - spårbarhet"* (s.42). Enligt Oscarson (2001) finns även en dialektik mellan aspekterna då det å ena sidan handlar om att skydda informationen men samtidigt göra den tillgänglig (s.2).

Att information i form av data har kommit att bli allt viktigare för företag och organisationer råder det inga tvivel om. Denna snabba förändring har i sin tur gett upphov till uttrycket *"The three V:s"* vilka står för engelskans *volume, velocity* och *variety*. Med andra ord, mängden information som uppstår, samlas in, hanteras, kommuniceras och lagras sker i allt högre takt i en variation av format (Ewald, 2018. s.37). Informationssäkerhet omfattar i regel all typ av information vilken enligt Oscarson (2019) utöver det digitala även involverar såväl ljud, bild, film, text som tal (s.13). I denna uppsats kommer termerna informationssäkerhet, IT-säkerhet och cybersäkerhet att syfta på den information som hanteras digitalt om inget annat anges. Skillnaderna i benämningarna är främst av semantisk karaktär i och med att ämnesområdet fortfarande anses vara omoget och därmed finns ingen standard ännu över hur begreppen skall användas på ett enhetligt sätt internationellt (Ewald, 2018. s.22; Oscarson, 2019. s.48).

Ett mer kritiskt förhållningssätt till huruvida en bör definiera informationssäkerhet utefter termerna konfidentialitet, riktighet och tillgänglighet samt betrakta dessa som skyddsmekanismer bör även diskuteras. Hallberg et al. (2017) menar exempelvis på att de definitioner som presenterats tidigare i denna uppsats inte bör betraktas som just definitioner utan snarare ses som målbilder. Detta grundar sig i att de givna definitionerna inte förhåller sig kritiska till *hur något är* kontra *vad vi vet* samt frågor som *när vi vet* att något är säkert kontra *när det är* säkert (s.202). Hallberg et al. (2017) menar alltså på att begreppen inte duger som en entydig definition då de tillsammans måste vara nödvändiga och tillräckliga i den bemärkelse att uppfyller informationen ett säkert tillstånd uppfylls per automatik alla villkor. På samma sätt, om de ska anses vara tillräckliga, betyder det att om informationen uppfyller alla villkor ska den betraktas som säker vilket inte överensstämmer med verkligheten alla gånger (s.201). Det finns egentligen ingen rangordning mellan aspekterna utan behovet och kraven varierar beroende på kontexten vilka tillsammans skapar det skyddsbehov som i sin tur kräver varierande säkerhetsåtgärder (Oscarson, 2019. s.15). I praktiken löses dock eventuella konflikter mellan säkerhetsaspekterna genom att prioritera men genom att göra det mister en även rätten till att kalla det en definition (Hallberg et al. 2017. s.202). Begreppen har dock ett brett tillämpningsområde och är väl etablerade inom området internationellt vilket även

är anledningen till att dessa aspekter kommer att användas i denna uppsats som en grundläggande syn på begreppet informationssäkerhet.

3.2 Den mänskliga faktorn och det mänskliga bidraget

Att teknologiska framsteg skapat ett förbättrat säkerhetsskydd råder det inga tvivel om men det har också blivit allt tydligare att vi även behöver ta hänsyn till den mänskliga faktorn (Gonzales & Sawicka, 2002). Gehringer (2002) belyser i sin artikel om cybersäkerhet och den mänskliga faktorn den balans som behöver infinna sig genom att kombinera de tekniska lösningarna med hur människor funkar rent kognitivt för att kunna skapa den ultimata skyddsbarriären. Vidare menar han på att säkerheten måste ses som ett helhetssystem vilket involverar såväl det som sker offline som online (Gehringer, 2002). Uttrycket ”den mänskliga faktorn” saknar en vetenskaplig definition men används ofta i negativ bemärkelse då en incident inträffat för att belysa människans roll och inverkan på utfallet. Det kan handla om ett felaktigt beslut, misstag eller svaghet till följd av kognitiva eller mentala hinder som orsakat skada (Oscarson, 2019). Historiskt har människan alltid strävat efter att känna sig trygg, oavsett om det handlar om en enstaka individ eller grupp. Att känna sig trygg kan i sin tur härledas till att känna sig säker vilket enligt Hollnagel (2014) innebär att det som ska ske kommer att ske enligt förväntningarna. När begreppet den mänskliga faktorn används finns ett synsätt att fokusera på att förhindra eller undvika att något går fel snarare än att säkerställa att allt går rätt till (Hollnagel, 2014). Begreppet den mänskliga faktorn användes redan under andra världskriget men då som ett synsätt att effektivisera ett systems användarvänlighet. Användaren sågs i dessa fall som den svaga länken då de kunde agera opålitligt eller arbetade för långsamt och lösningen blev därför att automatisera alternativt begränsa den mänskliga faktorns inverkan (Hollnagel, 2014. s.28).

Oscarson (2019) belyser dock det faktum att människor hela tiden tar beslut och finns på plats för att avvärja hot och undvika misstag och att det endast är en liten del av dessa beslut som resulterar i skada (s.269). Detta är även något som Hollnagel (2014) tar upp i sin bok *Safety-I and Safety-II: The Past and Future of Safety Management* där detta benämns som ”det mänskliga bidraget”. I stället för att fokusera på vad som blev fel och hur vi ska arbeta för att så lite som möjligt ska gå fel och se på människan som en riskfaktor tillämpas ett, på sätt och vis, motsatt synsätt. I stället bör verksamheter fokusera på att så mycket som möjligt ska bli rätt, det behöver finnas en så pass god förståelse för verksamhetens arbete att det proaktivt går att förutse vad som skulle kunna gå fel och i det, se människan som en nödvändig resurs än en risk. Människan har en avgörande roll i verksamhetens arbete i och med den kunskap de anställda besitter. Det behöver därför finnas ett intresse för det mänskliga bidraget och en nyfikenhet kring hur den kunskap som finns ska förvaltas på ett effektivt sätt (Hollnagel, 2014).

Till följd av en alltmer komplex miljö av informations- och IT-användning menar Hallberg et al. (2017) på att det snarare är de anställda som utgör den främsta skyddsbarriären (s.26). Således är det därför av betydelse att kunna koppla och förstå sambandet mellan informationssäkerhetsarbetet, organisationen och de anställda. Kanske är det så att de anställdas beteenden, ageranden och attityder kan ha en avgörande roll i hur lyckat, eller misslyckat, informationssäkerhetsarbetet är och förblir. Medarbetarna bör därför ses som en av de mest väsentliga skyddsåtgärderna då informationssäkerhetsarbetet inte kan fungera utan dem. Utan medarbetare finns ingen som hanterar och efterföljer de administrativa och tekniska skydden. Likaså är det

människan som står bakom de system, teknik och regelverk som upprättats vilka behöver innefatta en helhetssyn med människan i fokus för att det i praktiken ska kunna realiseras på ett tillfredsställande sätt (Oscarson, 2019. s.272).

3.2.1 Informationssäkerhetskultur

Att vara säkerhetsmedveten innefattar att både erhålla den kunskap som krävs samtidigt som beteendet behöver överensstämma med vad kunskapen anger. En person som inte beter sig enligt den kunskap som denne besitter anses därför inte vara säkerhetsmedveten (Oscarson, 2019. s.274). Det kan verka trivialt men kan komma att spela stor roll när det kommer till att utreda huruvida en organisation eller individ kan anses vara säkerhetsmedveten. En enskild individ kan komma att påverka den kontext denna befinner sig i medan kulturen i denna kontext samtidigt påverkar individen. Inom informationssäkerhet benämns det gemensamma säkerhetsmedvetandet som *informationssäkerhetskultur* (Oscarson, 2019. s.275). Törner (2017) definierar begreppet på följande vis:

> *"De gemensamma tanke-, beteende- och värderingsmönster som uppstår och utvecklas i ett socialt kollektiv genom kommunikativa processer, baserade på inre och yttre krav, som traderas till nya medlemmar och som har implikationer för informationssäkerhet"*
> *-Törner, 2017. s.22*

Informationssäkerhetskultur är således något som finns i alla organisationer och kan bedömas vara såväl bra som dålig (Törner, 2017). Hallberg et al. (2017) understryker att en kultur heller inte är statisk utan den utsätts ständigt för nya rön vilka behöver jämkas med redan befintliga värderingar, normer och antaganden. Dessa förändringar kan i sin tur uppstå till följd av nya lagkrav, teknologi eller regelverk (s.22). En människas medvetande formas utefter dennes kunskap och attityd vilket resulterar i ett beteende, detta påverkas i sin tur av flertalet faktorer vilket är av vikt att förstå sig på för att kunna skapa förändring (ibid). Vad som kännetecknar en god informationssäkerhetskultur behöver inte nödvändigtvis innefatta de mest avancerade tekniska systemen eller omfattande administrativa säkerhetsåtgärder utan snarare kan detta förgöra vad det är informationssäkerhetsarbetet syftar till att uppnå (Törner, 2017). Oscarson (2019) tar exempelvis upp graden av tillit hos medarbetare i en verksamhet där majoriteten av de tekniska lösningarna agerar per automatik eller när styrdokument motarbetar den optimala lösningen i en situation till följd av ett för preciserat regelverk (s.278). Nivån av säkerhetsmedvetande behöver därför vara optimal vad gäller avvägningen mellan frihet och ansvar beroende på hur stort handlingsutrymme kontexten innefattar. Även hur en eventuell hierarki ser ut i organisationen kan komma att ha stor betydelse då ledares engagemang i frågan kan anses fungera som förebild. Olika roller kräver olika behov av säkerhetsmedvetenhet men finns ingen förebild finns heller inget större syfte för medarbetaren att prioritera detta (Hallberg et al., 2017). Återigen har olika verksamheter olika behov vilket medför olika höga krav på medarbetarnas prestation. Genom att de anställda innehar en förståelse för det informationssäkerhetsarbete som föreligger i en verksamhet ökar även engagemang och motivation att efterfölja de regelverk och kultur som råder (Oscarson, 2019). Oscarson (2019) understryker även den dynamiska miljö som detta ämne omfattas av vilket innebär att det i princip alltid kommer att finnas ett handlingsutrymme vilket ställer krav på medarbetarnas säkerhetsmedvetande (s.280). Följaktligen kan det finnas olika anledningar till att ett regelverk inte efterlevs, däribland att regeln i fråga helt enkelt är okänd, svår att förstå sig på, av illojalitet eller likgiltighet

där de två sistnämnda leder oss in på en sista aspekt, nämligen motivation och engagemang hos medarbetarna (ibid).

För att medarbetarna ska agera utefter uppsatta mål och rutiner måste det finnas en mening med det som görs. Det innebär att medarbetarna behöver känna sig delaktiga i processen och att det som görs är av betydelse för verksamheten (Oscarson, 2019). Till stor del handlar det om att skapa engagemang och motivation i organisationen och därmed även kunna besvara inte bara *vad* och *hur* utan även *varför* detta är av görs och är av betydelse (Hallberg et al., 2017). Detta samspelar även med den kultur som råder, för att kunna implementera något nytt behöver en viss acceptans finnas för att kunna lyckas. Om det nya inte överensstämmer eller till och med talar emot den kultur som råder kommer det enligt Oscarson (2019) bli svårt att lyckas med implementeringen (s.288).

3.3 Informationssäkerhet inom e-post

Idag handlar informationssäkerhetsarbetet till stor del om att praktiskt hantera de hot som föreligger med hjälp av de olika metoder och verktyg som finns implementerade inom organisationen. Enligt Whitman och Mattord (2016) kan informationssäkerhetens olika skyddsbarriärer delas upp i olika lager vilka behöver tillgodoses för att en god säkerhet skall kunna upprätthållas. Dessa lager består i sin tur av såväl teknologiska lösningar som mänskliga faktorer i form av exempelvis skyddande protokoll, policys, brandväggar och kryptering (Whitman & Mattord, 2016). När det kommer till informationssäkerhet behöver ett holistiskt förhållningssätt innehas för att förstå devisen att systemet inte kommer att vara bättre än sin svagaste länk vilket inom e-postsäkerhet ofta börjar med en mänsklig handling (Oscarson, 2007. s.72).

Likaså handlar informationssäkerhet inte enbart om den faktiska säkerheten utan många gånger är det den upplevda säkerheten som är av betydelse, vilket är en subjektiv uppfattning av det objektiva (Oscarson, 2007. s.5). Detta innebär i sin tur att det inte går att avgöra vad som tillhör den faktiska säkerheten förrän en incident inträffat, följaktligen kan människan heller aldrig anses vara fullärd (ibid). Sammantaget innebär det att människor helt enkelt kan ha skilda uppfattningar om vad som är den faktiska respektive upplevda säkerheten beroende på faktorer såsom kunskap och tidigare erfarenheter (Oscarson, 2007. s.81).

Inom e-posthantering är det enligt Oscarson (2019) vanligt att angriparen använder sig av social manipulation för att få en användare att agera på ett visst sätt och således bryta informationssäkerheten (s.89). Ewald (2018) beskriver den IT-miljö vi lever i idag som en permanent störtskur av skadlig kod, intrångsförsök och andra antagonistiska hot (s.17). Genom e-post, som är den primära attackvektorn, skickas ofta meddelanden innehållande skadlig kod. Skadlig kod är i sin tur ett samlingsnamn för programkod som skapats i syfte att göra skada. Några av de vanligaste undergrupperna av skadlig kod idag är virus, trojaner, maskar, och ransomware som alla har som mål att penetrera organisationers säkerhetssystem (Oscarson, 2019. s.91). Ett av de vanligaste tillvägagångssätten när det kommer till att attackera genom e-post är att använda sig utav nätfiske som är en form av social manipulation där angriparen ofta utger sig för att vara en välkänd myndighet eller organisation för att få användaren, i förtroende, att exempelvis ange sina inloggningsuppgifter på en övervakad sida. Riktat nätfiske har även blivit allt vanligare där målet till en början är att samla in information för att sedan arbeta sig stegvis inåt i organisationen (ibid). Att skydda organisationen mot de hot som föreligger när det

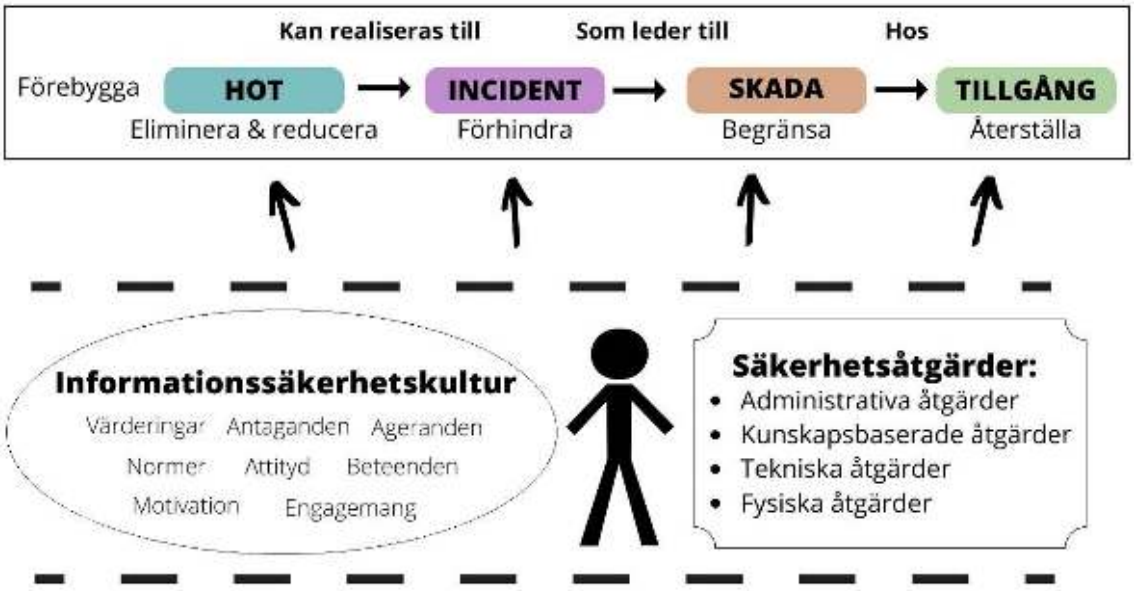
kommer till e-postsäkerhet krävs enligt Ewald (2018) dels ett tekniskt skydd i form av exempelvis programvaror som styr behörighetsåtkomst och uppdatering, men också utbildning och kunskapsspridning bland medarbetare vilket involverar mer administrativa och kunskapsbaserade säkerhetsåtgärder (s.74).

Sammantaget visar detta på vikten av att involvera den mänskliga faktorn för att kunna dra nytta av ett säkerhetssystems fulla potential. Tidigare studier som gjorts inom e-postsäkerhet visar även på att områdets relevans fortsätter att öka. (Dhamija, Tygar & Hearst, 2006). Aleroud och Zhou (2017) beskriver i sin artikel *Phishing environments, techniques, and countermeasures: A survey* hur den mänskliga faktorn har en central roll i hur nätfiske ska kunna motverkas. En variation av faktorer har hittats som ligger till grund för det mänskliga beteendet inom e-postsäkerhet. Exempel på mänskliga aspekter som anses ha en avgörande roll till utfallet är erfarenhet, kunskap, förtroende och medvetenhet. Enligt studien som undersökte varför nätfiske fungerar visade på att det snarare handlar om människors förtroende till ett varumärke som gör att vi klickar på skadliga länkar än hur hemsidan i sig uppfyller vissa säkerhetsaspekter i sin webbadress. Vidare framkommer i denna studie att det effektivaste tillvägagångssättet att motarbeta misstag inom den egna organisationen är utbildning och träning där faktiska nätfiskeattacker ska användas som exemplifiering vid identifiering av misstänkta meddelanden (Aleroud och Zhou, 2017. s.171).

3.4 Analysmodell

Uppsatsens analysmodell i Figur 3 utgår från den bakgrund och teori som presenterats. Modellen syftar till att visualisera hur de teoretiska delarna hänger ihop vilka tillsammans utgör en teoretisk referensram att förhålla sig till. Till följd kan en djupare förståelse fås kring denna studies omfattning och syn på begreppet informationssäkerhet. Analysmodellens struktur har även legat till grund för de intervjufrågor som använts vilka finns bifogade i Bilaga 1.

Uppsatsens första frågeställning handlar om vilken betydelse och inverkan den mänskliga faktorn har inom informationssäkerhetsarbetet. Modellen har därför en utgångspunkt i att initialt försöka förstå och definiera begreppet informationssäkerhet, för att sedan få en bild av hur arbetet ser ut inom de undersökta verksamheterna utifrån de säkerhetsaspekter och åtgärder som presenterats. Vidare skapas en bild av vilken syn det finns på en mer organisatorisk nivå och vilka prioriteringar som görs. Hur ser synen bland de anställda ut för området och om informationssäkerheten har en aktiv och självklar del i den kultur som råder. Slutligen kopplas detta till uppsatsens andra frågeställning som berör det mänskliga bidraget och hur detta kan komma att se ut inom e-postsäkerheten.



Figur 3: Analysmodell över informationssäkerhet som begrepp och dess beståndsdelar i förhållande till vad denna studie ämnar studera.

4. Metod

I detta avsnitt presenteras de metodval som gjorts. Till att börja med presenteras den litteraturstudie som gjorts, följt av den kvalitativa studie som bestått av semistrukturerade intervjuer. Slutligen presenteras de analysmetoder som använts i form av tematisk analys utifrån den teoretiska referensram som presenterats.

Genom att tillämpa en abduktiv forskningsmetod undviks de begränsningar som kan följa av deduktiva och induktiva ställningstaganden. Genom att i stället pendla mellan teori och empiri tillåts ett kontinuerligt lärande där slutsatserna kan dras allteftersom under studiens gång (Bryman och Bell, 2017). Då denna studie ämnat att undersöka vilken roll den mänskliga faktorn och det mänskliga bidraget har inom informationssäkerheten kopplat till e-post samt se hur de arbetssätt och metoder som finns kan användas på ett fördelaktigt sätt har studiens data samlats in på ett flertal sätt. Dels genom semistrukturerade intervjuer, dels litteraturstudier samt granskning av sekundärkällor. Sekundärkällorna har främst bestått av webbaserade artiklar och rapporter inom ämnet. I följande avsnitt presenteras och motiveras vardera del av studiens tillvägagångssätt.

4.1 Litteraturstudie

Vid val av litteratur inom det studerade området gjordes inledningsvis en omfattande litteratureftersökning. Initialt framkom enbart äldre skriftalster inom området vilka inte var av relevans i dagens kontext. En majoritet av de artiklar som publicerats inom området informationssäkerhet fokuserar även till stor del på enbart de tekniska lösningarna. Efter flertalet sökningar inom Uppsala universitets biblioteksdatabas valdes dock tre böcker ut som till stor del har kommit att lägga grunden för den teori som presenterats i kapitel 2 och 3. Genom att sedan följa upp de begrepp och källor som använts i dessa böcker har en starkare teoretisk grund och referensram kunnat bildas. Bryman och Bell (2017) benämner denna typ av litteraturgenomgång för narrativ vilket innefattar att författaren använder litteraturen som vägledning genom att följa upp intressanta spår utan en strukturerad plan allteftersom en djupare förståelse inom det studerade området erhållits.

4.2 Kvalitativ studie

För att kunna finna svar på de frågeställningar som undersökts är det av hög betydelse att få en förståelse för det studerade fenomenet vilket är just vad en kvalitativ metod ämnar göra (Widerberg, 2002). Enligt Harboe (2013) tillåter semistrukturerade intervjuer å ena sidan respondenten möjligheten att fritt uttrycka sig om dennes personliga erfarenheter å andra sidan kan intervjuaren säkerställa att diskussionen håller sig relevant och inom ramarna för vad uppsatsen ämnar studera. Öppna frågor möjliggör även chansen för intervjuaren att följa upp intressanta sidospår, vilka kan ha betydelse för studiens resultat (Dilley, 2000). Under intervjuerna har en passiv kvalitativ metod tillämpats för att undvika att påverka respondentens svar. Widerberg (2002) menar på att observation av respondenterna kan vara av vikt vid tolkning av resultaten. En kvalitativ metod lämpar sig i denna studie på grund av dess flexibilitet i flera avseenden. Exempelvis kunde ljudupptagningar göras, med tillåtelse från respondenten, vilket möjliggör reducering av eventuella missförstånd eller feltolkningar. För att kunna ställa relevanta följdfrågor till respondentens svar gäller det enligt Bryman (2004) att vara ständigt närvarande under intervjun. Till följd av att transkribering är en tidskrävande process kommer endast delar av insamlade data att transkriberades ord för ord. Samtliga intervjuer har även skett

digitalt vilket enligt Bryman och Bell (2017) går att likställas med fysiska intervjuer på plats. I vissa fall kan detta sätt att samla in data till och med vara att föredra då respondenten har möjlighet att själv välja omgivning, tid och plats. För denna uppsats har detta varit avgörande då det i många fall var svårt att få till en fysisk träff med tanke på stora geografiska avstånd till respondenterna samt pandemi.

4.3 Val av respondenter och genomförande

Vid val av respondenter för denna studie har de studerade forskningsfrågorna samt Trafikverkets önskemål legat till grund för urvalet. Då samtliga respondenter som deltagit valts med hänsyn till dennes yrkesroll och förhållande till ämnet informationssäkerhet utgör enligt Bryman och Bell (2017) detta ett målstyrt urval. Följaktligen har totalt 10 djupintervjuer utförts med lika många respondenter från offentlig respektive privat sektor. Målet med studien är att på ett kontrollerat sätt få en viss omvärldssyn på hur organisationer ser på och arbetar med informationssäkerhet med särskild inriktning på den mänskliga rollen inom e-postsäkerhet. Genom det målstyrda urvalet har därför en variation av branscher, roller samt år inom området fått genomsyra detta arbete och på så vis skapat en nyanserad bild av ämnet. Tabell 1 nedan, ger en översikt över de intervjuer som genomförts där vardera respondents befattning, roll, bransch, sektor, år inom området samt intervjuns varaktighet presenteras.

Tabell 1: En översikt över de intervjuer som genomförts.

Nr.	Befattning / roll	Offentlig / privat sektor/ bransch	År inom området	Intervjuns varaktighet
1	Sverigechef - mjukvaruföretag	Privat - IT-säkerhet	15	45 min
2	IT-arkitekt	Offentlig - IT-säkerhet	30	1h 10 min
3	Teknisk specialist	Privat - finansbranschen	10	1h
4	Högstadielärare	Offentlig - kommun	20	30 min
5	Intern kommunikatör	Offentlig - myndighet	8	45 min
6	Specialist risk och cybersäkerhet	Privat - IT-säkerhet	15	45 min
7	Kommunikations-ansvarig	Offentlig - IT-säkerhet	20	1h
8	Gruppchef inom kvalitetskontroll	Privat - läkemedelsbranschen	23	45 min
9	Senior teknisk specialist	Offentlig - IT-säkerhet	30	1,5 h
10	Kommunikationsstrateg ledning	Offentlig - myndighet	20	1 h

4.4 Trovärdighet och äkthet

I motsats till kvantitativa studier där reliabilitet och validitet diskuteras för att påvisa studiens kvalitet tillämpas inom kvalitativa studier i stället begreppen trovärdighet och äkthet. Två sätt att stärka studiens trovärdighet är enligt Bryman och Bell (2017) att använda sig av triangulering och responsvalidering. Triangulering innebär att studien använder sig av fler än en metod vilket i denna studie inneburit att dels en litteraturstudie gjorts, sedan en kvalitativ metod i form av semistrukturerade intervjuer tillämpats och slutligen insamling av sekundära data. Responsvalidering innefattar att respondenterna efter genomförd intervju samt sammanställning av denna ombeds validera de resultat som framkommit. Genom att tillämpa responsvalidering säkerställs att inga missuppfattningar eller feltolkningar gjorts samtidigt som respondenten möjliggörs att fastställa sitt godkännande att vara en del av studien. Enligt Bryman och Bell (2017) är nackdelarna med detta metodval att det dels kan vara en tidskrävande uppgift vid ett stort antal intervjuer samt att respondenterna därmed tillåts få en viss kontroll över den data som framkommit. I denna studie har respondenterna erbjudits responsvalidering då det varit möjligt inom tidsramen för detta arbete.

Beträffande studiens äkthet menar Bryman och Bell (2015) att det är av betydelse att utforma studiens inhämtning av empiriska data på ett strukturerat sätt för att kunna dra relevanta slutsatser. I denna uppsats skulle viss kritik kunna riktas mot urvalet av respondenter. Å ena sidan går det att argumentera för att respondenternas bakgrunder är så pass skilda att de inte går att dra någon generell slutsats, å andra sidan är det en fråga som även begränsas av den tid och omfång som arbetet omfattar. Viktigt att komma ihåg när en läser, inte bara denna studie, är att den bild som ges är just en av många. Bryman och Bell (2015) påtalar även att resultatet skulle kunna ge en missvisande bild i och med att mer än hälften av studiens respondenter innehar en ledande position i verksamheten. De lyfter även att det finns viss kritik som menar på att personliga åsikter kan ha påverkat resultaten och därmed givit en missvisande bild av verksamhetens informationssäkerhetsarbete. Då denna uppsats undersöker den mänskliga rollen utifrån respondenternas egna perspektiv bedöms dock att dessa faktorer inte haft en inverkan på resultaten som varit av betydelse. Eftersom uppsatsen delvis ämnar undersöka ett upplevt fenomen skulle personliga åsikter och uppfattning snarare tillföra substans då detta även är en del av verkligheten då det är de anställda som utgör verksamheten. Respondenterna har även informerats om att anonymitet råder under intervjuerna vilket har varit av vikt för en grundläggande trygghet.

4.5 Analys av genomförande

I denna uppsats utgår intervjufrågorna, som finns att tillgå under Bilaga 1, från den analysmodell som presenterats under avsnitt 3.4. Intervjufrågorna baseras således på den bakgrund och de teorier som presenterats under kapitel 2 samt 3. Vardera intervjufråga fokuserar i sin tur på en del av analysmodellen i taget samtidigt som möjlighet alltid fanns för respondenten att själv prata om vad som kändes relevant i stunden.

Till att börja med ställdes allmänna frågor kring respondentens bakgrund och nuvarande befattning samt tillhörande arbetsuppgifter. Sedan bildades en uppfattning av respondentens kunskaper inom området genom att låta denne definiera och beskriva begreppet informationssäkerhet. Vidare kunde följdfrågor ställas kring informationssäkerhet relaterat till respondentens yrkesroll och arbetsliv. Först fokuserade frågorna på det befintliga säkerhetsarbetet och de olika typer av åtgärder som tillämpas i

verksamheten idag, sedan formulerades frågor som lät respondenten ta ställning till dennes syn på informationssäkerhetsarbetet och dess utmaningar kopplat till e-post. På ett liknande sätt ställdes sedan frågor kring det organisatoriska arbetet kring området. Dessa frågor berörde ämnen som ledning, prioriteringar i verksamheten, medarbetares syn på området samt informationssäkerhetskultur. Slutligen ställdes frågor kring egna erfarenheter och idéer kring området samt dess utmaningar.

4.6 Analys av insamlade data

I denna studie har analys av insamlade data skett med metoden tematisk analys vilket enligt Clarke och Braun (2017) är ett vanligt förekommande analys inom kvalitativa studier. Tematisk analys innebär att gruppera frekvent återkommande ord och begrepp utefter teman som har en direkt koppling till den teoretiska referensramen. I detta fall var ett första tema *informationssäkerhet som begrepp*. Detta involverade svar som berörde hur det omnämns och vilken betydelse det har i respektive verksamhet. Ett andra tema blev *säkerhetsåtgärder och informationssäkerhetsarbetet i verksamheten* vilket grupperade svar som berörde hur respektive verksamhet arbetar med fenomenet och människan samt vilka åtgärder som vidtas. Ett tredje tema blev de svar som handlade om *säkerhetsarbetet i organisationen* vilket kunde handla om hur verksamheten prioriterar i frågan, hur ledningen ser på ämnet samt vilken kultur som rådet. Slutligen grupperades respondenternas svar inom temat *den mänskliga faktorn och det mänskliga bidraget inom e-postsäkerhet* vilket innefattade svar som hade en tydlig koppling till människans roll i e-postsäkerhetsarbetet alternativt en direkt koppling specifikt till antingen den mänskliga faktorn eller det mänskliga bidraget.

5. Resultat

I detta avsnitt presenteras de resultat som framkommit utifrån den analysmodell som beskrivits under avsnitt 3.4. Resultatet har sedan grupperats enligt de teman som beskrivits under avsnitt 4.6. Inledningsvis presenteras de resultat som handlar om vikten av informationssäkerhet och dess definition. Vidare presenteras de resultat som berör den mänskliga rollen i verksamhetens olika åtgärder. Slutligen presenteras de resultat som framkommit som kan knytas till den mänskliga faktorn och det mänskliga bidraget inom e–posthantering.

5.1 Vikten av informationssäkerhet och dess definition

Överlag ges en enad bild från samtliga respondenter att begreppet informationssäkerhet har kommit att få en alltmer prioriterad roll i verksamheten. Historiskt påtalar flertalet av respondenterna att det under de senaste åren har kommit att bli ett alltmer aktuellt ämne i och med den digitalisering som sker i samhället. Respondent 1 påtalar specifikt att det skett ett skifte vad gäller hur angriparna väljer att attackera organisationer. Förr blev det väldigt snabbt tekniskt där fokus för angriparen var att arbeta snabbt där skadan direkt blev tydlig för den utsatta. Det kunde handla om skadlig kod som infekterade nätverk och servrar som gjorde att det inte gick att arbeta vidare. Idag agerar angriparna på motsatt sätt, ofta genom att verka i det dolda. Respondent 2 menar att fokus nuförtiden ligger oftare på att systematiskt och metodiskt angripa en organisation i tystnad för att hela tiden arbeta sig ett steg längre in mot målet. Genom detta angreppssätt får angriparen även åtkomst till värdefull information längs vägen som kan komma att ha ett signifikant värde vid försäljning eller utpressning. Således menar både Respondent 1 och 2 på att just information i form av data har kommit att få ett allt större värde och med det har informationssäkerhet fått en allt viktigare roll i verksamheter.

En återkommande punkt när det kommer till att försöka definiera begreppet informationssäkerhet är även den uppdelning som finns inom området. Begreppet i sig är brett och många respondenter samtycker om att det kan vara svårt att greppa och sätta ord på vad som egentligen menas eller syftas på vilket i sig utgör en risk och utmaning. Specifikt nämns upprepade gånger en uppdelning vad gäller en teknisk del kontra en icke-teknisk del, alternativt en teknisk del respektive den mänskliga rollen. Respondent 8 menar på att det dels handlar om att känna sig säker från ett användarperspektiv men även att med hjälp av tekniken se till att skydda företagsinformationen. Respondent 3, som jobbar i en roll som involverar såväl det tekniska som det affärsmässiga, menar också på att det är viktigt att inse att säkerhet består av dels en teknisk del men även en icke-teknisk del men båda behöver finnas för att det tillsammans ska bli säkert. Respondent 5 tror att de flesta initialt tänker på tekniken som främsta skydd men att det i själva verket är människan som utgör grunden i och med att det är människor som skapar de tekniska säkerhetsskydd som finns. Respondent 9, som även aktivt jobbar inom informationssäkerhet, ser också vikten i att se den tekniska lösningen som ett sista steg i skyddet där människan utgör en slags grund.

"Det spelar ingen roll hur bra tekniskt skydd vi har om ändå ingen förmår sig att använda den. Det går inte att undgå människans roll i att säkerställa ett fullgott skydd."
- *Respondent 9*

En viss skillnad på respondenternas svar kunde ses när det kommer till hur de benämner informationssäkerhetens olika delar. De respondenter som aktivt jobbar med och inom området använde likartade begrepp såsom riktighet, konfidentialitet, tillgänglighet och spårbarhet i sina svar medan respondenter som snarare har rollen som användare i systemen syftar på samma innebörd men uttrycker det på andra sätt. Respondent 4, som arbetar som lärare, pratar exempelvis om den tystnadsplikt och sekretess som råder i yrkesrollen gentemot eleverna snarare än att informationen i sig kan inneha en större betydelse om den sätts i perspektiv till hela organisationen.

"För mig handlar informationssäkerhet om att den information som finns ska vara skyddad mot obehöriga samtidigt som den ska vara tillgänglig för de som har rätt till den." - Respondent 4

Respondent 8 gav ett liknande svar utifrån rollen som gruppchef inom läkemedelsbranschen som har mer av ett användarperspektiv.

"För mig handlar informationssäkerhet, utifrån ett användarperspektiv, om att förstå vad jag får och inte får göra, att känna mig säker i hur jag ska agera för att företagsinformationen ska hållas säker och även kunna förmedla detta till mina anställda." - Respondent 8

Enligt Respondent 6 ligger en stor utmaning i att få människor och anställda att förstå att informationssäkerhet är något som alltid funnits där men som kommit att bli ett alltmer prioriterat område. Förr var det något som ingick under sunt förnuft och inte synliggjordes på samma sätt, vilket enligt respondentens erfarenheter ofta gör att många ryggar tillbaka bara de hör begreppet idag. Respondenten påtalar att det således gäller att anpassa sin kommunikation och göra sig förstådd utifrån målgruppens behov och tidigare kunskaper.

5.2 Säkerhetsåtgärder och informationssäkerhetsarbetet i verksamheten

När det kommer till informationssäkerhetsarbetet i respektive verksamhet kan såväl likheter som olikheter ses. Respondent 10 påtalar dels det skifte som skett från att gå från att information lagras fysiskt på papper till att idag i stor omfattning hanteras digitalt. I och med detta går inte informationen att ”ta på” och konkretisera på samma sätt som det gjorde förr. Detta medför i sin tur utmaningar i att få människan att förstå dels värdet av den information som tillhandahålls men också hur den anställde ska agera för att informationen ska hållas skyddas. Respondent 4 ger som exempel på detta att informationssäkerhetsarbetet tidigare omfattade att se till att personuppgifter på fysiska papper raderades genom dokumentförstörare efter att dess syfte uppnåtts och kopiatorn var en del av vardagen. Idag menar Respondent 4 på att det finns en tveksamhet och okunskap kring hur det säkerställs att känslig data faktiskt är raderad och att följa den exakta spridningen av det som publiceras och delas på nätet känns främmande.

Respondent 9, som arbetar inom en teknisk roll på en myndighet, beskriver verksamhetens informationssäkerhetsarbete dels utifrån ett historiskt perspektiv där de anställdas roll har kommit att få en mer central roll. De tekniska skydd som utvecklas idag ses snarare som hjälpmedel men inte lösningen då det är användaren som slutligen är den som gör valet. Samtidigt som administrativa säkerhetsåtgärder i form av policys och styrande dokument utgör en central utgångspunkt i arbetet är det idag något som

ibland inte beaktas från början vid utvecklingen av ett nytt system. Detta är även något som Respondent 7 understryker under sin intervju som flertalet gånger erfarit att system utvecklas och implementeras men säkerhetsaspekter har kommit in för sent. På grund av detta blir inte systemets säkerhetsåtgärder speciellt användarvänliga utan det behöver finnas med i åtanke redan från början för att på så sätt bli en självklar del av systemet och inte en ytterligare del.

Utifrån utvecklarens perspektiv menar Respondent 2 på att risken blir att det resulterar i en "kaka på kaka" effekt genom att i efterhand behöva komplettera för de bristfälliga beslut som togs från början vid utvecklingen av systemet. Respondent 5 understryker den risk som kommer i de fall säkerhetsåtgärderna uppfattas som efterhandskonstruerade. I värsta fall kan det komma att uppfattas, utifrån användarens perspektiv, som en onödigt omständig process för att utföra sina vardagliga arbetsuppgifter och därmed, vid nästkommande tillfälle, kan detta komma att ignoreras i medarbetarens användarbeteende. För Respondent 3, som jobbar inom finansbranschen, finns ett tydligt säkerhetstänk med från början. Skillnader kan ses över tid i takt med att hoten ständigt förändrats men säkerhetsaspekten har alltid funnits med från början likväl användarens roll vilket respondenten tror är till följd av den typ av verksamhet som bedrivs där det alltid varit prioriterat att skydda såväl verksamhetens som kundernas uppgifter och data.

Respondent 1 säger sig se en tydlig skillnad utifrån egna arbetslivserfarenheter mellan privat respektive offentlig sektor. Offentliga myndigheter omfattas av mer regler och lagar som sätter krav och ramar för vad arbetet bör innefatta men kanske inte alltid hur, vilket skapar en fördröjning då beslutsvägarna ofta är långa. Privata aktörer å andra sidan har snabbare till beslut men kanske inte alltid den kunskap eller resurser som krävs för att implementera ett fullgott skydd och därmed behöver ta in externa leverantörer vilket kan komma att ses som en säkerhetsrisk i sig. Respondent 3 och 8 förklarar att deras respektive verksamheter tillämpar såväl kontinuerlig som sporadiskt säkerhetsarbete. Årligen behöver samtliga medarbetare genomföra en interaktiv utbildning som uppdateras för att vara á jour med vilka utmaningar som finns i dagens samhälle. Respondent 8 berättar även om en erfarenhet där flertalet anställda sattes på prov genom att ett "spoofat" mail skickades ut som test där avsändaren såg ut att vara en kollega och användaren uppmanades att klicka på tillhörande länk i mailet. Då detta var ett test gavs en direkt återkoppling att du blivit utsatt för ett försök till en nätfiskeattack och att detta var en del av ett test från organisationen för att göra medarbetarna uppmärksamma på de hot och risker som föreligger. Respondenten upplevde vid händelsen att det kändes hårt men vid närmre eftertanke ett bra initiativ och att det faktiskt resulterat i ett mer eftertänksamt beteende. Respondenten tror dock att detta behöver ske vid upprepade tillfällen för att det ska få märkbar effekt och inte som en engångsföreteelse.

Respondent 6, som också har erfarenhet både från offentlig och privat sektor, säger sig se en tydlig skillnad i hur offentlig kontra privat sektor jobbar med säkerhetsåtgärder och då med en tydlig utgångspunkt i vart behovet uppkommer. Offentlig sektor styrs till stor del av lagar och regler som gör att det inte är ett alternativ att utesluta dessa frågor medan den privata sektorn styrs mer av vilken efterfrågan och utsatthet företaget i fråga befinner sig i. Respondent 6 understryker att oavsett vilken verksamhet som undersöks har människan en central roll och information är något som alla kommer i kontakt med. Det finns dock alltid en individuell aspekt med vilket gör att olika typer av säkerhetsåtgärder passar bättre och sämre för olika typer av personer och verksamheter men en kombination är oftast att föredra. Respondent 5 talar också om vilket värde olika typer av skydd har

beroende på dess kontext. Administrativa säkerhetsåtgärder i form av policys tänker respondenten är viktiga att ha som grund och vid nyanställning eller anställning av externa konsulter som snabbt behöver veta vad som gäller på arbetsplatsen. Över tid tror dock respondenten att mer kontinuerliga säkerhetsåtgärder är att föredra i form av kunskapshöjande åtgärder såsom interaktiva utbildningar. Respondent 8 har en liknande syn på de administrativa åtgärderna där de utgör en bra grund men det är inget som har en aktiv roll i verksamhetens vardagliga arbete. Mer givande menar respondenten är de mer kreativa informationstillfällena som ges där exempelvis videos, föreläsningar och diskussioner kombineras för att nå så många som möjligt.

Just inom läkemedelsbranschen berättar Respondent 8 att även den fysiska säkerheten är av hög betydelse just för att skydda den informationen som finns stationärt. Till skillnad från andra branscher finns skyddsvärd information på ett helt annat sätt i och med laborationssalar och produktion. Respondent 6 berättar även om en tidigare problematik på arbetsplatsen där anställda höll upp dörren för varandra vid inpassering vilket direkt motarbetade de fysiska åtgärder som tillämpats i form av inpasseringskontroll och användning av passerkort.

Utifrån ett mer organisatoriskt perspektiv kan fler skillnader än likheter ses mellan de olika verksamheter som studerats. Inom myndighet och offentlig sektor tycks det, utifrån den data som framkommit, finnas en tydlig prioritering och helhetssyn på informationssäkerhet som något nödvändigt och som behöver genomsyra hela verksamheten. Dock menar ett fåtal respondenter, verksamma inom offentlig sektor, på att det finns utmaningar som berör hur dessa prioriteringar ska implementeras i verksamheten. Att det finns en prioritering, förståelse och medvetenhet från ledningen är tydlig men när det kommer till det praktiska, vem som ska göra vad, uppstår desto fler frågetecken. Respondent 7 påtalar att ansvaret ligger å ena sidan inte på en del av verksamheten utan behöver genomsyra hela verksamheten, å andra sidan medför detta att det är svårt att avgöra vem som bär det ansvaret.

De respondenter som arbetar inom privat sektor beskriver också synen på informationssäkerhet som något självklart men inte alltid något som genomsyrar samtliga delar av verksamheten. Som exempel berättar Respondent 3 att det som tidigare benämndes som DevOps (eng: developments and operations) idag kallas DevSecOps (eng: developments, security and operations) och har därmed en tydlig säkerhetsaspekt inkluderad. Samtidigt är detta ett beslut som enbart omfattar just denna del av verksamheten, hur andra gör är inget som diskuteras öppet utan det är något som vardera avdelning har eget ansvar över. Respondent 3 understryker även en utmaning i att det å ena sidan ska bli en självklarhet att utveckla säkert samtidigt som utmaningar finns vad gäller synen på vad som är säkert och hur det ska prioriteras inte alltid överensstämmer när det kommer till det tekniska respektive det mer affärsmässiga synsättet, här behöver en enhetlig syn finnas på vad som är viktigt och varför. På liknande sätt berättar Respondent 6 att det utifrån dennes erfarenhet inom privat verksamhet i ledningsgrupper finns en medvetenhet för att det är viktigt men det saknas en förståelse för vad som behöver göras och varför, därför är detta inte något som blir förankrat i verksamheternas arbete.

"Ofta upplever jag det som att det finns en medvetenhet att informationssäkerhet är viktigt men det saknas ofta en förståelse och kunskap för hur detta ska verkställas och

förankras. Det blir lite som en gråzon där man konstaterar men sen inte agerar." - Respondent 6

Respondent 7 tror att det överlag finns en förståelse hos de anställda att informationssäkerhet är något som är viktigt och prioriterat i verksamheten. Samtidigt ligger ett stort ansvar på ledning och styrning att det ska vara lätt att göra rätt. Utifrån respondentens egna erfarenheter upplevs informationssäkerhetsarbetet som nödvändigt men ibland onödigt krångligt. Strävan efter att vilja göra rätt finns där men lösningarna till hur en ska gå tillväga är något som verksamheten behöver bli bättre på. Samtidigt som instruktioner tillhandahålls över vad som inte är tillåtet behöver dessa alltid kompletteras med vad som istället är tillåtet. Risken finns annars att den anställde ställs inför ett val och finns då inte en förståelse för vilka konsekvenser ett agerande kan få är risken stor att den anställde ser detta som ett oviktigt beslut. Med det sagt, menar även Respondent 5 på att en stor del i informationssäkerhetsarbetet innefattar att inte bara utbilda de anställda inom området genom att informera om vilka hot som föreligger utan minst lika viktigt är att sprida kunskap om vilka konsekvenser ett agerande kan få. Både Respondent 9 och 10 understryker även vikten av att förstå aggregerad informations värde och betydelse.

"Information som för dig kanske inte är skyddsvärd kan tillsammans med annan information komma att bli extremt känslig." - Respondent 9

Organisationskultur är något som samtliga respondenter anser har en stor roll i hur informationens innehåll och innebörd värderas. Specifikt påtalar Respondent 2 och 8 vilken risk det ligger i att vanor kan göra att vi ser bortom de säkerhetsåtgärder som finns. Eftersom det inte blev en konsekvens första, andra eller tredje gången någon agerade på detta sätt, varför skulle utfallet bli annorlunda denna gång. Vanor kan även skapa det som Respondent 2 benämner som en "falsk trygghet" där en anställd helt enkelt upplever att dennes beteende och ageranden inte utgör någon risk då detta har kommit att bli en vardaglig rutin. Respondent 8 upplever å ena sidan att kulturen har en stor inverkan på hur de anställda ser på vikten av informationssäkerhet som en väsentlig del att ha i åtanke i sitt arbete, å andra sidan finns en syn på att det är just IT-avdelning som är de som arbetar med detta. Liknande upplevelse har Respondent 4 som berättar att synen på informationssäkerhet inte är en del av det egna arbetet utan det är något som sköts av IT-avdelningen även om det anses vara viktigt. Respondent 8 spekulerar dock om att det antagligen sett annorlunda ut om det varit ett mindre företag där alla är mer involverade i verksamhetens samtliga delar.

"*I och med att organisationen är så pass stor tänker man ofta att det är någon annan som har ansvaret för informationssäkerheten. Vi litar på att de åtgärder som berör oss och som vi behöver vidta, kommer vi att informeras om." - Respondent 8*

Respondent 10 påtalar att en kultur inte är något som går att lära ut, en kultur är det som är en del av vardagen. Med det sagt behöver informationssäkerheten således bli en del av medarbetarnas vardag. En början i detta är policys och regelverk som sätter ramar för, och skapar en grund i det som senare kommer att bli en kultur.

5.3 Den mänskliga faktorn och bidraget inom e-posthantering

När det kommer till den mänskliga aspekten inom informationssäkerhetsarbetet tror samtliga respondenter att människans roll har en avgörande betydelse. Respondent 10 tror att en allt större del har kommit att hamna på individen då det idag är upp till var och en på ett eller annat sätt ta åt sig och skapa sig en förståelse och bild av hur informationssäkerhetsarbetet kan komma att påverka individen i dennes vardag i sin yrkesroll. Med detta menar respondenten att det även kommer stora utmaningar i och med att respektive individ har varierande bakgrund och kunskaper.

"Vi är idag inte vana att se allt som information som behöver omfattas av ett grundläggande säkerhetstänk, att ständigt behöva göra en bedömning är därmed en utmaning." - Respondent 10

Respondenterna 5, 7 och 10, som samtliga har roller inom kommunikation, understryker att en stor utmaning i deras vardag handlar om att få de anställda att mötas och förstå varandra. För någon som jobbar med informationssäkerhet i sin vardag kan det tyckas självklart och grundläggande medan det för den anställde saknas en förståelse för vad, hur eller varför. Detta skapar i sin tur stora utmaningar i att även skapa en tillit till varandra för att få informationssäkerhetsarbetet att fungera optimalt. Respondent 10 påtalar att alla behöver anpassa sitt budskap utefter vardera individs nivå. Det går således inte att anta eller på förhand bestämma en individs nivå av mottaglighet. Det är här kommunikatören har en avgörande roll i hur såväl befintligt som framtida säkerhetsarbete kommer att mottas av de anställda.

En annan utmaning påtalar Respondent 7 ligger i att försöka förutse vilket motstånd ett nytt arbetssätt kan möta utifrån olika individers tidigare kunskaper och erfarenheter. Det är oftast inte informationssäkerheten i sig medarbetare motsätter sig utan det kan handla om att det för den anställde blir ytterligare ett moment att utföra i och med ytterligare säkerhetsåtgärder i ett redan pressat läge. Vidare menar respondenten att medarbetaren kan se att det finns ett behov, verksamheten tar fram ett tillvägagångssätt men själva implementeringen behöver också möta de anställda i deras vardag. Således, genom att även anpassa implementeringen, genom att exemplifiera hur detta arbetssätt kommer att fungera i medarbetarens vardag kan även en större förståelse fås för det behov som föreligger, rätt tillvägagångssätt samt vilka konsekvenser det kan bli om detta tillvägagångssätt inte efterföljs.

Att den mänskliga faktorn har en central roll är en återkommande syn hos flertalet av respondenterna. Inte minst inom e-posthanteringen påtalar majoriteten att den mänskliga faktorn till och med är avgörande. Respondent 2 påtalar att det i takt med att det tekniska skydd som föreligger ständigt förbättras, är det i slutet alltid ett mänskligt beslut som fattas. Även Respondent 8 uttrycker en större osäkerhet när det kommer till hantering av e-post då det i slutändan hänger på individen att inte göra fel. Respondenten berättar, trots denna vetskap, att ämnet vanligtvis inte är något som diskuteras i verksamheten utan det är inte förrän om något hänt som ämnet kommer på tal.

Flertalet av respondenterna tror att den vanligaste orsaken till att anställda drabbas är en kombination av okunskap och att det går för fort. Respondent 8 berättar vidare att det händer att medarbetare kommer och rådfrågar om mail som kan se suspekta ut så att det finns en viss grad av medvetenhet råder det därför inga tvivel om. Respondent 5 och 9 tar båda upp att en förväntan finns på att saker och ting ska gå fort, ofta finns inget intresse i

att lära sig det grundläggande. En återkommande syn är att människor antingen inte tycker sig behöva dölja något alternativt en inställning som tänker att det är oerhört liten sannolikhet att just jag skulle drabbas.

Flertalet, bland annat Respondent 2 och 6, tror att nyckeln till att nå människans roll är att dels få anställda att se till det stora perspektivet och inte enbart utgå från sig själva och sin egen situation utan inse att varje individ är en del av helheten. Samtidigt behöver ämnet och informationen komma som en naturlig del i medarbetarens vardag. Enligt Respondent 6 borde detta vara lika självklart som vilka arbetsvillkor som gäller på en arbetsplats, det ska inte vara en fråga om, utan snarare hur detta ska realiseras.

"Detta ska ingå som en självklar del oavsett vart man jobbar liksom frågor och ansvar som berör arbetsmiljö och arbetsvillkor gör idag." - Respondent 6

Respondent 9 påtalar dels människans centrala roll i hela processen från planeringen, till skapandet, utvecklingen, implementeringen samt förvaltningen av ett systems säkerhetsaspekter. Samtidigt belyser Respondent 1 de utmaningar som kommer med att verksamheter egentligen alltid ligger steget efter. Med det menar respondenten att verksamheter i de flesta fall reagerar aktivt, när en incident inträffat, på så vis lär vi oss av det som redan hänt. En förbättringspunkt menar respondenten därför hade varit att proaktivt försöka förutse framtida attacker och hot och utifrån detta sedan utbilda medarbetarna utifrån ett användarperspektiv.

Idag finns även en utmaning i att kunna dra en tydlig gräns mellan privat och arbetsliv i en alltmer digitaliserad tillvaro. Respondent 9 berättar om flertalet incidenter där användare utnyttjar den arbetsrelaterade e-postadressen för privata ändamål utan att förstå varför detta skulle kunna orsaka problem. Även Respondent 4 tror att mycket av informationssäkerhetsarbetet idag utgår från individens egna bedömningar genom att det antas vara underförstått vad en får eller inte får göra. Respondent 6 påtalar det faktum att information idag ofta handlar om data till skillnad från tidigare då informationen hanterades fysiskt i form av papper, pärmar och mappar. Detta menar respondenten, medför att det idag inte alls är lika påtagligt som tidigare hur informationssäkerheten fortfarande behöver finnas men verka digitalt. Respondenten tar som exempel att hemlig information tidigare hanterades med stor varsamhet genom att inte tilldelas någon obehörig. Dokument med känslig information var ofta stämplade och undertecknade, behövde informationen dessutom fraktas skedde det ofta genom spårbart brev och försegling.

Enligt Respondent 10 behöver informationssäkerheten bli en naturlig del i vår vardag men samtidigt inte en vana som gör att vi bortser från de säkerhetsåtgärder som finns att tillgå, det är en ständig balansgång.

"Det ska bli en naturlig sak som en del av vår vardag, det ska vara självklart att agera informationssäkert, det ska inte krävas en speciell eftertanke. "- Respondent 9

Respondent 3 talar om vikten av ett gränsöverskridande informationssäkerhetsarbete då det idag är något som berör flertalet delar av verksamheten. Samtidigt betonar respondenten även att en ödmjukhet och förståelse behöver finnas för att alla anställda inte har samma bakgrund och följaktligen inte samma förkunskaper. På liknande vis påtalar Respondent 7 på vikten av att synliggöra informationssäkerhetsarbetet på ett

pedagogiskt sätt. Det handlar enligt respondentens egna erfarenheter ofta om att skapa ett intresse snarare än att skrämmas. Återigen, tas vikten av kombinationen kunskap och medvetenhet ihop hos såväl anställda som ledning. Respondenten tror att anledningen till att det inte läggs mer resurser kan vara att det helt enkelt inte hör till kärnverksamheten. Respondent 5 påtalar även de utmaningar som ligger i att en avvägning ständigt behöver göras. Alla åtgärder kostar tid, pengar och kunskap. Respondent 2 tror att fler åtgärder tillämpas först när en incident inträffat, det behöver realiseras och bli kännbart innan någon agerar. Respondent 1 påtalar även att det, trots en initialt stor kostnad, behöver ses i relation till de långsiktiga konsekvenserna ett kortsiktigt agerande kan få.

Samtliga respondenter tror att människans roll, framförallt inom e-postsäkerhet, kommer att öka. Respondent 2 tror dessutom att social manipulation kommer att bli allt vanligare genom att attacker på underleverantörer görs i syfte att nå huvudmålet. Följaktligen kommer även den fysiska säkerheten komma att utgöra det yttersta skalet av säkerheten genom att skydda företagets lokaler och åtkomst till nätverk och dylikt. Samtidigt påtalar Respondent 1 att de tekniska innovationer som finns ligger i framkant men att användarens roll ofta glöms bort under processens gång. En ytterligare utmaning understryker respondenten är det faktum att e-post idag har funnits i över 50 år och därmed innehas ett stort tekniskt arv. Respondent 5 och 9 betonar också den bristfällighet många system uppvisar när det kommer till användarvänligheten, ofta har anställda goda intentioner men väljer en annan väg i brist på alternativa lösningar.

Flertalet av respondenterna påtalar att en del av lösningar inför framtida utmaningar ligger i att konsekvent och kontinuerligt utbilda. Det innefattar att utbilda såväl i unga år under grundskolan som en del av den normala undervisningen till att utbilda gemene man i sin vardag till att organisationer behöver involvera arbetet som en naturlig del i sin verksamhet. Det är inte någon nyhet att sociala medier och det digitala livet har kommit att få ett allt större fotfäste och med det, menar Respondent 7, att människor tids nog kommer att bli alltmer medvetna i och med ett allt större behov.

"Dels kommer kriminaliteten att öka i den digitala världen och därmed kommer människan att bli mer medveten och vidta de åtgärder som behövs." - Respondent 7

För att nå den mänskliga faktorn i informationssäkerhetsarbetet behöver åtgärder vidtas på ett varierande sätt. Flertalet respondenter föreslår att ämnet informationssäkerhet behöver bli en naturlig del av ungas undervisning i skolan. Flertalet respondenter betonar även vikten av att göra informationen till något självklart, som ett beteende som ska sitta i ryggmärgen. Respondent 1 tar som exempel statens beslut om att införa krav på bilbälte, något som tidigare varit långt från självklart. Följaktligen resulterade detta i drastiska beteendeförändringar och idag är bilbälte, för de allra flesta i Sverige, en självklarhet. Respondent 4 talar även, på liknande sätt, om den undervisning som genomförs idag som påtalar effekterna och konsekvenserna av alkohol och droger, informationssäkerhet borde bli lika självklart. Ser en till åtgärder som bör ske på en mer samhällelig nivå föreslår Respondent 7 att informationen kring informationssäkerhet även ska bli en självklar del i individens vardag. Exempelvis genom att dra nytta av de resurser som redan finns, förslagsvis på MSB:s hemsida informatiossäkerhet.se, tydliggörs och synliggörs ämnet. Detta kan i sin tur ske genom reklam, inslag och skyltar runtom i samhället. I verksamheten betonar samtliga respondenter vikten av att ständigt låta informationssäkerhetsarbetet ha en självklar plats. Det kan handla om att informera och utbilda hur användarens roll kan komma att spela in vid en eventuell incident eller vilka

risker som finns vid hanteringen av e-post. Respondent 7 tror att tekniken kring e-post kommer att omfattas av allt fler automatiserade processer där utvecklingspotentialen är stor när det kommer till att säkerställa att detta görs användarvänligt. Respondent 3 menar på att en kombination alltid kommer att vara att föredra för att passa så många olika användare, processer och scenarion som möjligt. Respondent 1 berättar om tidigare forskning som visat på att information i form av fysiska skyltar på arbetsplatsen resulterat i mätbar skillnad i medarbetarnas beteende. Även ledares roll har, enligt respondentens svar, en betydande roll. Inte minst när det kommer till att göra en kulturskillnad då det är av hög vikt för de i ledande positioner att leva som de lär. När det kommer till kulturen tror Respondent 1 att ett effektivt sätt är att se på det som en hälsosam vana, tillsammans skapar medarbetare utrymme för informationssäkerhet som en naturlig del av vardagen och på så vis finns inte en ensam ansvarig utan alla tar ett gemensamt ansvar.

För att i framtiden minska antalet attacker tror Respondent 1 på att hårdare konsekvenser behöver finnas och mindre pengar att tillgå, således ska det vara krångligt, riskfyllt och olönsamt att attackera verksamheter. Respondent 10 lyfter att finns en grundläggande tillit hos alla människor, vilket är bra och något som ska bejakas. Å andra sidan måste det finnas en hälsosam skepsis hos användarna genom att ta det säkra före det osäkra. Inom e-postsäkerheten är det därför en ständig balansgång att bemöta individen utefter dennes behov för att motverka effekten av social manipulation.

6. Analys

I detta avsnitt analyseras de resultat som framkommit i relation till den bakgrund och teori som tidigare presenterats under kapitel 2 samt 3. Analysen är strukturerad utefter de rubriker som tidigare tillämpats under uppsatsens resultatdel i kapitel 5 vilket baserats på den analysmodell som presenterats under avsnitt 3.4 samt framtagna teman under avsnitt 4.6. Till att börja med diskuteras informationssäkerhetens roll i verksamheten och dess definition, vidare diskuteras människans roll och olika tillämpningar av säkerhetsåtgärder inom verksamheten. Därefter analyseras den mänskliga faktorns roll och bidrag kopplat till e-posthantering innan den resulterande modellen presenteras under avsnitt 6.4.

6.1 Informationssäkerhet och dess definition

Till följd av de resultat som framkommit samt den teoretiska bakgrund som presenterats kan en likhet ses mellan hur litteratur definierar begreppet hänvisat till forskning inom området samt hur olika verksamheter ser på och arbetar med det. Respondenternas svar visar på att begreppet informationssäkerhet inom det tekniska området använder sig av just termerna konfidentialitet, riktighet, tillgänglighet och spårbarhet, däremot kan mindre variationer ses vad gäller begreppens prioritering inom enskilda verksamheter. För de respondenter som inte arbetar inom ett direkt tekniskt område beskrivs informationssäkerheten ofta utifrån ett användarperspektiv vilket knyter an till individens roll i informationssäkerhetsarbetet. Sammantaget är det tydligt utifrån respondenternas svar att synen på informationssäkerhet som något viktigt och prioriterat överensstämmer, däremot kan mindre skillnader ses vad gäller exakt definition och tillämpning vilket även knyter av till den teori som presenterats. Både Ewald (2018) och Oscarson (2019) pekar på att informationssäkerhetsarbetet inte handlar om att ha de mest tekniskt avancerade lösningarna utan snarare se vad som är relevant kopplat till den kontext verksamheten befinner sig inom. Således finns ingen strikt rangordning bland aspekterna utan kraven varierar vilka skapar det behov som i sin tur kräver flexibla typer av säkerhetsåtgärder.

Utöver den indelning som görs av begreppet informationssäkerhet framkommer det även att begreppets innebörd består av två delar. Respondenterna benämner dessa som den tekniska kontra den icke-tekniska alternativt den mänskliga rollen. Således tydliggörs hur människans roll är central när det kommer till informationssäkerhetsarbetet. Historiskt berättar ett flertal respondenter att ett skifte skett vad gäller synen på informationssäkerhet. Tidigare låg ansvaret ofta på en enskild IT-avdelning att skydda verksamheten från hot, idag är det snarare en integrerad del av verksamheten. Detta stämmer i sin tur överens med den teori som presenteras där dels ett skifte kan ses samt att det historiskt alltid funnits ett behov, även om det tidigare skett på annorlunda sätt. Även utifrån angriparens synvinkel påtalas att ett skifte skett. Förr agerade angripare på ett sätt där skadan blev direkt tydlig och konsekvenserna påtagliga, idag sker attackerna i det dolda. De respondenter verksamma inom tekniska områden beskriver att attackerna sker på ett alltmer systematiskt och metodiskt arbetssätt för att få ut så mycket data av värde som möjligt vilket också överensstämmer med den teori som presenterats tidigare.

Sammanfattningsvis kan en skillnad ses vad gäller respondenternas individuella utgångspunkt i relation till området informationssäkerhet. Däremot är det tydligt att en enad syn på informationssäkerhetens betydelse finns även om en exakt definition inte tillämpas.

6.2 Säkerhetsåtgärder och människan i verksamheten

Att informationssäkerhet har kommit att få en allt större betydelse i verksamheten är tydlig, både utifrån tidigare forskning samt de empiriska resultat som presenterats. Vidare framgår det även att begreppet har ett brett tillämpningsområde som till viss del kan te sig olika utifrån den kontext som studeras. Samtliga respondenter bekräftar dock att informationssäkerheten överlag har kommit att få en allt större och prioriterad roll i verksamheten, dels till följd av de lagkrav och samhällets utveckling med en alltmer digitaliserad värld som ställer krav på samtliga aktörer. Detta styrks även av den teori som presenterats som visar på att informationssäkerhetens roll har fått en allt större betydelse i och med att det blir vanligare att företag utsätts för cyberattacker. Lagar och regler, som ofta föranleds av tidigare incidenter, implementeras i organisationers policys och regelverk i hopp om att erhålla ett grundläggande skydds - och ramverk. Att följa de regelverk och lagar som finns bildar ofta ett grundläggande behov vilket dock skiljer sig mellan offentlig och privat sektor. Det är utifrån såväl respondenternas svar som den bakgrund som presenterats tydligt att det åligger en distinkt skiljaktighet mellan de två områdena. Inom offentlig sektor har det aldrig varit ett val om ett strukturerat informationssäkerhetsarbete ska involveras i verksamheten, därmed förefaller det sig inte helt obekant hur detta ska komma att implementeras utifrån dagens utvidgade behov. Inom privat sektor härleds informationssäkerhetsarbetet istället utifrån vilka behov som finns och uppkommer. I dagens samhälle är det en nödvändighet att ett grundläggande skydd behöver finnas för att överhuvudtaget kunna verka i det digitala klimat som råder. Informationssäkerhetsarbetet skapar även förutsättningar när det kommer till att uppfylla och leva upp till de förväntningar som finns, och i framtiden kommer att finnas, i samhället. Teorin pekar på att det finns flertalet argument till att lägga tid och resurser på sitt informationssäkerhetsarbete till följd av de långsiktiga konsekvenser en brist på ett sådant kan få. Det handlar således inte enbart om monetära medel utan även relationer kan skadas och sanktioner kan komma att påverka verksamheten. Flertalet av de respondenter som har erfarenhet från både offentlig och privat sektor påtalar även en skillnad i hur verksamhetens storlek kan komma att få en betydande inverkan på informationssäkerhetsarbetet. I och med större organisationer finns i regel mer resurser vilket öppnar upp för mer omfattande åtgärder, däremot påtalas att beslutsvägarna ofta är långa vilket gör att effekterna dröjer, om det ens implementeras. Mindre, privata, aktörer har i motsats ofta kortare beslutsvägar vilket öppnar upp för snabbare åtgärder men de begränsas även av vilka resurser som finns att tillgå i form av kunskap, tid och pengar vilket gör att det oftare görs mer basala och akuta åtgärder.

Att informationssäkerhet involverar människans roll är något som blir alltmer märkbart. Förr var medarbetarens roll inte lika påtaglig som idag, enligt respondenterna var det tidigare sunt förnuft och en outtalad förväntan som låg till grund för informationssäkerhetsarbetet i vardagen. Inom det tekniska menar respondenterna på att ett skifte skett vad gäller perspektiven på de tekniska skydd som skapas vilka idag snarare ses som hjälpmedel än lösningar på informationssäkerhetsproblemen. Användaren utgör således en utgångspunkt vid utvecklandet av tekniska skyddssystem där användarvänligheten behöver finnas i åtanke från första raden kod. Utöver det tekniska skydd som ofta hamnar i fokus om en studerar tidigare forskning, finns även de kunskapsbaserade, administrativa och fysiska säkerhetsåtgärderna. Utifrån respondenternas svar kan slutsatsen dras att samtliga verksamheter innehar flertalet typer av skydd. Däremot har skillnader i vilka sätt dessa tillämpas och kombineras beskrivits av respondenterna. Att en individuell aspekt alltid behöver beaktas är ofrånkomligt liksom det faktum att olika säkerhetsåtgärder har varierande effekt beroende på dess

kontext. Att en kombination av säkerhetsåtgärder ändå utgör det optimala skyddet är något som samtliga respondenter understryker. Administrativa säkerhetsåtgärder i form av regelverk, policys och rutiner verkar ofta som en grundpelare till det övriga säkerhetsarbetet. Respondenterna menar att det är förväntat att detta finns på arbetsplatsen men det är inget som innehar en aktiv roll bortsett från när en nyanställning sker. Således finns en skillnad även vad gäller behov och vilket värde olika typer av skydd har för olika typer av verksamheter under olika tidpunkter, vilket överensstämmer med den teori som lyfts fram. Det är förväntat av medarbetarna att veta vad som gäller vilket medför ett individuellt ansvar men inget som direkt kontrolleras. Över tid tillämpas kontinuerliga kunskapshöjande åtgärder i form av utbildningar, föreläsningar och seminarier. Flertalet av respondenterna påtalar att en kombination av kunskapshöjande aktiviteter är att föredra för att nå så många som möjligt. Samtidigt återkommer det faktum att begränsningar i form av tid och resurser ändå behöver tas i beaktning för att slutligen implementera åtgärderna där de har störst effekt. Att individers kunskap är avgörande benämns även i teorin då det är människan som både skapar, använder och förvaltar de innovationer som framkommer. När det kommer till fysiska säkerhetsåtgärder blir det genast tydligt i verksamheter med essentiell informationsteknisk verksamhet alternativt produktion att det är ett prioriterat område. I somliga fall benämns även en ökad närvaro av social manipulation för att få åtkomst till verksamheters lokaler eller nätverksanslutningar. Följaktligen kan variationer ses vad gäller den mänskliga rollen för respektive skyddsåtgärd.

Utifrån en organisatorisk syn på informationssäkerhetsarbetet kan ett flertal skillnader synliggöras. Dels påtalas att det inom offentlig sektor finns utmaningar när det kommer till implementering av säkerhetsåtgärder som visserligen har en tydlig prioritering från ledningens sida men ändock lyckas det inte implementeras hela vägen till följd av att ingen bär ansvaret eller tar besluten. Samtidigt återfinns ett synsätt på informationssäkerheten som något som ska genomsyra hela verksamheten vilket medför att en implementering som inledningsvis kan verka simpel helt enkelt blir för invecklad och komplicerad. Ett återkommande begrepp från flertalet respondenter är att “det ska vara lätt att göra rätt” vilket är lättare sagt än gjort i stora organisationer. Målbilden finns men vägen dit görs ibland alldeles för krånglig vilket resulterar i ett halvdant resultat med försumbar effekt alternativt slutförs inte projekten överhuvudtaget. Inom privat sektor beskrivs informationssäkerhetsarbetet också som något självklart men inte något som genomsyrar verksamheten på samma sätt. Respondenterna inom privat sektor ser informationssäkerheten snarare utifrån sin yrkesroll än som en del av hela organisationen. Dock finns ändå en medvetenhet att informationssäkerhet är något som berör samtliga delar av organisationen och för att lyckas behöver en strävan finnas åt samma håll. Utan en enhetlig bild är det således lätt hänt att organisationens olika verksamhetsområden drar åt olika håll beroende på vad som anses viktigt för just deras arbete. Här behöver ledningen tydliggöra vad som är prioriterat och hur detta ska genomföras i verksamheten för att optimal effekt ska kunna nås. Respondenterna tycker sig se att en medvetenhet kring ämnet alltid finns men en avsaknad av förståelse resulterar i att det inte blir förankrat i verksamhetens arbete.

Oavsett om en ser till privat eller offentlig sektor finns en enhetlig bild bland respondenterna att organisationens kultur har en betydande inverkan på informationssäkerhetsarbetet. Att vara säkerhetsmedveten innefattar, enligt teorin, att både besitta rätt kunskaper samt agera utefter vad denna kunskap anger. Flertalet respondenter understryker kulturens inverkan på individens synsätt på information som

något skyddsvärt. Vidare påtalas de konsekvenser som kan komma att ha stor inverkan på verksamheten då det räcker med att en enskild individ inte ser allvaret i informationens skyddsbehov. Med andra ord, en enskild individ kan således påverka hela informationssäkerhetsarbetet samtidigt som kulturen inte är något som går att lära ut. Således behöver informationssäkerhetsarbetet bli en naturlig del av medarbetarens vardag.

I takt med att en allt större del av informationssäkerhetsarbetet har kommit att hamna på individen går det inte längre att undgå de utmaningar detta medför vad gäller individers varierande bakgrund och kunskaper. Något som blivit allt tydligare under skrivandet av detta arbete är vikten av en god kommunikation mellan samtliga parter. Det spelar ingen roll hur bra en teknisk lösning är om inte användaren förmår sig att använda den och på liknande sätt spelar det ingen roll hur gärna medarbetaren vill göra rätt om inte en lösning finns att tillgå. Följaktligen åligger det faktum att den utbildning och information som når medarbetarna behöver anpassas efter mottagarens behov. Grundläggande är den tillit och förståelse som behöver finnas medarbetare emellan som i sin tur skapar mening och motivation. Det handlar om att ständigt göra avvägningar mellan individens frihet och ansvar i informationssäkerhetsarbetet. Med varje implementerad säkerhetsåtgärd behöver det finnas en medvetenhet och förståelse för vad och hur detta ska göras men lika viktigt är det att även förmedla varför detta är av betydelse. Ett sätt att arbeta kring denna utmaning är enligt respondenterna att proaktivt försöka förutse vilket motstånd ett nytt arbetssätt skulle kunna innebära och redan innan ha en strategi för hur detta ska bemötas på ett pedagogiskt sätt. I grund och botten vill människan väl, medarbetare vill göra rätt och bidra men insatsen behöver alltid vägas mot priset för att lyckas. Det är här vikten av att se konsekvenserna kommer in, vilket till viss del innefattar att medarbetarna behöver se sin del som en del av helheten. Det mänskliga bidraget skulle här behöva lyftas för att medarbetare själva ska se sig som tillgångar snarare än ett problem.

Sammanfattningsvis står det klart att människan utgör en central roll i verksamhetens informationssäkerhetsarbete. De säkerhetsåtgärder som tillämpas kombineras på olika sätt beroende på verksamhetens kontext då olika säkerhetsåtgärder har varierande effekt beroende på verksamhetens behov. Olika typer av åtgärder innefattar även olika hög grad av mänsklig inblandning. Även organisationers informationssäkerhetskultur har en central roll i informationssäkerhetsarbetet för att skapa en förståelse och medvetenhet kring ämnet som något självklart. Det blir tydligt att individers tidigare kunskaper och erfarenheter behöver has i åtanke vid implementeringen av nya system och tillvägagångssätt för att lyckas. Således har det visat sig att kommunikation har en central roll i informationssäkerhetsarbetet när det kommer till att synliggöra och tydliggöra.

6.3 Den mänskliga faktorn och bidraget inom e-posthantering

E-postsäkerhet är ett område som kommit att bli alltmer komplext och aktuellt, delvis på grund av ett explosionsartat antal användare sedan starten för 50 år sedan. Även till följd av den samhällsutveckling och digitalisering som skett och sker än idag. Tidigare hanterades den fysiska motsvarigheten i form av brev med stor varsamhet i de fall det innehöll skyddsvärd information. Respondenterna beskriver ett tillvägagångssätt som i dagens e-postsäkerhetsarbete direkt skulle kunna kopplas till den definition som tidigare diskuterats. Brev med känslig information var ofta stämplade och undertecknade för att, i informationstekniska termer, säkerställa innehållets riktighet. Vidare fraktades sedan informationen förseglat och spårbart för att således säkerställa konfidentialitet och

spårbarhet. På så vis har informationssäkerhet länge varit en naturlig del i verksamheter men i och med att alltmer sker digitalt idag är det inte lika påtagligt hur detta ska ske. Här gäller det att få det tekniska och mänskliga att mötas, en förståelse måste finnas från båda håll och på så sätt få medarbetarna att se vikten av informationssäkerhet inom e-posthanteringen.

I takt med att social manipulation har kommit att bli ett av de vanligaste tillvägagångssätten när det kommer till att gör intrång i företag skapas en naturlig ingång via e-posten där framförallt den mänskliga rollen behöver tydliggöras. Flertalet respondenter påtalar att den mänskliga rollen inom e-postsäkerhet till och med innehar en avgörande roll då det bortom de tekniska skydd som föreligger till sist handlar om ett mänskligt agerande. Ett beslut som kan ha förödande konsekvenser men även ha en avgörande betydelse i de fall det mänskliga bidraget lyckas att undanröja ett eventuellt hot. Bland de respondenter som intervjuats tror de flesta att en kombination av okunskap och stress är ledande faktorer till varför social manipulation inom e-posthanteringen lyckas trots att en viss grad av medvetenhet kan finnas. Samtidigt lyfts den förväntan som finns att allt idag ska gå fort och således är ett klick i sammanhanget inget som kräver speciellt stor eftertanke. En betydande del av informationssäkerhetsarbetet, inte minst inom e-postsäkerheten, innefattar att öka chanserna att medarbetarna efterföljer vad som beslutats. Detta görs i sin tur genom att först skapa en medvetenhet och etablera en förståelse för såväl behov som konsekvenser. Genom att låta människan vara en del av processen och delaktiga i informationssäkerhetsarbetet ökar chanserna att de metoder och verktyg som finns efterföljs som tänkt. I grund och botten handlar mycket om att individen behöver känna att det är applicerbart och av vikt i dess vardag, annars är de åtgärder som implementeras nästintill försumbara. Samtidigt är det såväl en prioriteringsfråga som en resursfråga där en balans behöver infinna sig och beslut behöver tas för att få resultat och effekt. Somliga respondenter menar på att informationssäkerheten behöver bli en mer integrerad del av verksamhetens dagliga arbete och på så vis komma att bli en naturlig del i medarbetarens vardag. Informationssäkerhetsåtgärder skulle därför gynnas av att levereras som en helhet till medarbetarna där en strategi finns med från start till mål. Med andra ord skulle det vara optimalt om medarbetarna kunde vara med från början i processen för att känna delaktighet och engagemang för att på så sätt värdesätta den metod eller verktyg som sedan ska implementeras. Samtidigt skulle detta innebära ett gränsöverskridande samarbete vilket ett fåtal respondenter benämner som en nyckel till att lyckas.

En annan kunskapshöjande åtgärd som skulle kunna ge effekt även på e-posthanteringen är en mer allmän spridning av information kring ämnet informationssäkerhet. En av de intervjuade respondenterna föreslår att dra nytta av det material som redan existerar. Många är idag inte varse om att exempelvis MSB har publicerad information inom ämnet att tillgå. Detta kan i sin tur involvera reklamkampanjer som får människor att reflektera och agera och således bli mer medvetna. Tidigare forskning visar även på att aspekter som medvetenhet, kunskap, erfarenhet och förtroende har en stor inverkan på det mänskliga beteendet specifikt när det kommer till e-posthantering. Följaktligen ses utbildning och träning i form av fiktiva fall som en av de åtgärder som bör vidtas för störst effekt.

Att den mänskliga faktorn inom e-postsäkerhet är av betydelse är något som samtliga respondenter är överens om. Ett vanligt och växande problem kan ses när det kommer till social manipulation som används alltmer för att komma åt verksamheter genom e-post.

Då anställda ensamma bemöter den e-post som potentiellt skulle kunna innehålla skadlig kod ses även ett allt större behov av att bemöta individen. Istället för att medarbetarna ses som en risk i informationssäkerhetsarbetet behöver här individen ses som nyckeln till lösningen. Det mänskliga bidraget borde, till skillnad från den mänskliga faktorn, vara det organisationer och ledning talar om för att på så vis lyfta de anställdas roll. Genom detta skapas, istället för rädsla, ett engagemang och motivation till att vilja bidra och göra rätt. Förhoppningsvis resulterar detta även i att människor väljer att möta och hjälpa varandra, istället för att se på det som ett misslyckande. Återigen kommer faktorer som att skapa medvetande, etablera förståelse och få medarbetarna att inse vilka konsekvenser ett knapptryck på en okänd länk kan få, men nu med ett helt annat synsätt från grunden.

6.4 Resulterande modell

Till följd av de resultat och den analys som presenterats visualiseras i Figur 4 den modell som framkommit av denna studie. Figuren visar på och vill förmedla den kärna som egentligen all informationssäkerhetsarbete bör utgå från för optimal effekt - det mänskliga bidraget. Kopplat till tidigare analysmodell under 3.4, illustrerar denna modell hur individen bör betraktas i relation till övriga komponenter. Således, oavsett vilken del av informationssäkerhetsarbetet som studeras bör komponenterna i Figur 4 alltid finnas i åtanke för att rätt förutsättningar ska ges för att informationssäkerhetsarbetet ska lyckas.

Figur 4: Visualiserar studiens resultat i form av ett framtida synsätt på hur organisationer bör arbeta med det mänskliga bidraget i sitt informationssäkerhetsarbete.

7. Slutsatser

Syftet med denna studie var att undersöka hur organisationer bör arbeta med den mänskliga faktorn och det mänskliga bidraget i sitt informationssäkerhetsarbete för att ha optimal effekt och därmed kunna nyttja verksamhetens resurser där de har störst effekt. Studien har haft sin utgångspunkt i tidigare forskning där ett ökat behov har identifierats i takt med ett alltmer digitaliserat samhälle.

Studiens resultat visar på att den mänskliga faktorn och det mänskliga bidraget har kommit att få en central och betydande roll i verksamheters informationssäkerhetsarbete. Ett allt större fokus ligger på den enskilde medarbetarens roll att hantera de hot som föreligger, speciellt vad gäller e-posthanteringen som är den största attackvektorn idag.

Vad som framkommit under analysen är vikten av att bemöta varje medarbetare utefter dennes individuella behov. Detta kräver i sin tur att de tekniska behöver förstås av användarna vilket är en utmaning idag. För att lyckas med detta kan ett behov ses vad gäller att skapa medvetenhet hos användaren, etablera en förståelse samt få medarbetarna att förstå vilka konsekvenser som en enskild individs agerande kan få. Sammantaget behöver organisationer idag belysa det mänskliga bidraget snarare än den mänskliga faktorn. Enligt presenterad teori innebär detta att se människan som en tillgång snarare än ett hot.

Den mänskliga faktorn inom informationssäkerheten är således en tillgång och ett hot.

7.1 Förslag till vidare forskning

För framtida studier inom ämnet föreslås att även studera det interorganisatoriska arbetet, vilket denna studie inte omfattat. Det vore även intressant att se hur en större mängd respondenter skulle kunna påverka utfallet av studiens resultat. Alternativt skulle en global studie vara av intresse för att se om det som framkommit i denna studie även kan vara av betydelse för andra nationer.

Referenser

Aleroud, A. & Zhou, L. (2017). *Phishing environments, techniques, and countermeasures: A survey, Computers & security.* vol. 68, pp. 160-196

Bryman, A. (2004). *Quantity and Quality in Social Research*. Routledge, New York. First ed: 1988.

Bryman, A., Bell, E. & Nilsson, B. (2017). *Företagsekonomiska forskningsmetoder.* Upplaga 3 edn, Liber, Stockholm.

Bryman, A., Bell, E. (2015). *Business Research Methods*. Oxford university press. Oxford, United Kingdom. Fourth Edition.

Clarke, V., Braun, V. (2017). *Thematic Analysis*. The journal of Positive psychology. Vol 12, No 3. Routledge.

Cybersäkerhetscenter. (2021). *Nationellt cybersäkerhetcenter – Vårt uppdrag*. Tillgänglig: https://www.cfcs.se/om-centret [Hämtad: 2021-12-16]

Dhamija, R., Tygar, J., & Hearst, M. (2006). *Why phishing works*. Proceedings of the SIGCHI conference on Human Factors in computing systems.

Dilley, P. (2000). *Conducting Successful Interviews: Tips for Intrepid Research*. Theory Into Practice, vol. 39, no. 3, p.131-137.

Ewald, F., Forsgren, L. & Lilius, C. (2018). *Informationssäkerhet: hur gör man?*. Näringslivets arkivråd, Stockholm.

Gehringer, E. (2002). *Choosing Passwords: Security and Human Factors*. Department of Electrical Computer Engineering, Department of Computer Science. North Carolina State University.

Gonzales, J., & Sawicka, A. (2002). *A framework for Human Factors in Information Security*. Grimstad: Agder University College, Department of Information and Communication Technology

Hallberg, J. (2017). *Informationssäkerhet och organisationskultur*, Upplaga 1 edn, Studentlitteratur, Lund.

Harboe, T. (2013). *Grundläggande metod: den samhällsvetenskapliga uppsatsen*. 1. uppl. edn, Gleerup, Malmö.

Hollnagel, E. (2014;2018;). *Safety-I and safety-II: the past and future of safety management*. 1st edn, Ashgate Publishing Company, Farnham, Surrey, UK England;Burlington, VT, USA;.

KPMG. (2020). *KPMG CIO Survey 2020*. KPMG. Stockholm. Tillgänglig: https://assets.kpmg/content/dam/kpmg/xx/pdf/2020/10/harvey-nash-kpmg-cio-survey-2020.pdf [Hämtad: 2022-03-10]

MSB – Myndigheten för samhällsskydd och beredskap. (2022). *NIS-direktivet*. Tillgänglig: https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nis-direktivet/ [Hämtad: 2022-03-12]

Oscarson, P. (2019). *Informationssäkerhet*. Upplaga 1 edn, Studentlitteratur, Lund.

Oscarson, P. (2007). *Actual and Perceived Information Systems Security*. Linköpings universitet.

Oscarson, P. (2001). *Informationssäkerhet i verksamheter*. Linköpings universitet.

Riksrevisionen. (2007). *Regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen.* RiR 2007:10. Stockholm. Tillgänglig: https://www.riksrevisionen.se/download/18.78ae827d1605526e94b2e595/1518435488911/RiR_2007_10.pdf [Hämtad: 2021-10-15]

Riksrevisionen. (2016). *Informationssäkerhetsarbete på nio myndigheter – En andra granskning av informationssäkerhet i staten*. RiR 2016:8. Stockholm. Tillgänglig: https://www.riksrevisionen.se/download/18.78ae827d1605526e94b2dbec/1518435509192/RiR_2016_8_INFOSAK2_WEBB.pdf [Hämtad: 2021-10-15]

Statsrådsberedningen. (2017). *Nationell säkerhetsstrategi*. Regeringskansliet, Statsrådsberedningen. Tillgänglig: https://www.regeringen.se/48e36d/contentassets/a02552ad9de94efcb84154b0f6ed76f9/nationell-sakerhetsstrategi.pdf [Hämtad: 2021-10-08]

Svenskt Näringsliv. (2021). *Företagen och IT-säkerheten – hotbilder, motåtgärder och behov.* Stockholm. Tillgänglig: https://www.svensktnaringsliv.se/sakomraden/sakerhet-och-risk/foretagen-och-it-sakerheten-hotbilder-motatgarder-och-behov_1168797.html [Hämtad: 2022-01-20]

Svensson, T. & Sveriges industriförbund. (1999). F*öretagens skydd och säkerhet: om lagar och praktisk tillämpning*. 2. omarb. utg. edn, Sveriges industriförb, Stockholm.

Sveriges Riksdag. (2022). https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/offentlighets--och-sekretesslag-2009400_sfs-2009-400

Säkerhetspolisen. (2020). *Gemensam kunskap ökar Sveriges motståndskraft mot cyberhot.* Stockholm. Tillgänglig: https://www.sakerhetspolisen.se/ovrigt/pressrum/aktuellt/aktuellt/2020-06-03-gemensam-kunskap-okar-sveriges-motstandskraft-mot-cyberhot.html [Hämtad: 2021-11-24]

Törner, M. (2017). *Inledning och förklaring av några centrala begrepp.* I:Hallberg, J. m.fl. (red.) *Informationssäkerhet och organisationskultur*. Lund. Studentlitteratur, s.15-22.

Whitman, M.E. & Mattord, H.J. (2016). *Principles of information security*. Fifth edn, Cengage Learning, Boston, MA.

Widerberg, K. (2002). *Kvalitativ forskning i praktiken*. Studentlitteratur, Lund.

Bilaga 1 - Intervjuformulär

1. **Kan du berätta lite om dig själv och vad du jobbar med idag och har gjort tidigare?**
    - Offentlig/privat sektor
    - Roll/titel
    - Tid inom verksamheten
    - Tid yrkesverksam inom området totalt

Generellt om informationssäkerhet

2. **Informationssäkerhet är i sig ett väldigt brett begrepp, vad tänker du på initialt när du hör det?** Vad innefattar det för dig?

3. **Hur skulle du säga att informationssäkerhet har kommit att spela in under ditt yrkesliv hittills?**
   Över tid

4. **Vilka utmaningar finns det i finns det i din roll**
    - Att möta den mänskliga faktorn
    - Mänskligt beteende

Faktiska informationssäkerhetsarbetet - inom verksamheten/er

5. **Hur skulle du beskriva inf.säk-arbetet bland verksamheter idag?**
    - Finns rätt förutsättningar?

6. **Kan man se skillnader och likheter när det kommer till aspekter såsom:**
    - Storlek på företaget
    - Privat / offentlig sektor

7. **Vilka säkerhetsåtgärder är vanliga och finns det något som funkar bättre eller mindre bra?**
    - **Administrativa** - policys, regelverk. Manualer
    - **Kunskapsbaserade** - utbildning, skapa medvetenhet, kultur
    - **Tekniska** - antivirusprogram, behörighetsåtkomst, lösenordshantering
    - **Fysiska** - passerkort till dörrar, nyckelhantering, koder

8. **Hur frekvent / aktivt arbetar man med inf.säk?**
    - Proaktivt /aktivt / resilient

9. **Skulle du säga att medarbetare har en aktiv roll i arbetet, på vilket sätt?**

10. **Anser du att de åtgärder som vidtas är tillräckliga /otillräckliga?**

11. **Vad tycker du skulle kunna göras bättre och hur?**

INFORMATIONSSÄKERHETSKULTUR - mer organisatorisk syn

12. **Vilken roll har informationssäkerhetsarbetet inom organisationer?**
    a. Finns en tydlig prioritering/krav uppifrån
    b. Finns en förståelse för vad som behöver göras och varför
    c. Finns en medvetenhet kring ämnet

13. **Hur ser anställda på informationssäkerhetsarbetet?**
    - Är det en enhetlig bild?
    - Diskuteras det öppet?
    - Finns det normer och värderingar som styr?
    - Kan värderingar knytas till inf.säk arbetet?

14. **E-post – retoriska frågor**
    - Vad tror du gör att folk…
    - Vad göra åt det…

SITUATIONSBASERADE FRÅGOR

15. **Har du själv blivit utsatt eller varit med om en incident?**
    - Hur bemötte du detta?
    - Vilka åtgärder vidtog du?
    - Fanns ett tydligt tillvägagångssätt att följa vid en sådan incident?
    - Vilka förbättringar skulle du säga kan göras för att underlätta vid en ev incident?

16. **Hur känner du inför att eventuellt bli drabbad i framtiden?**
    - säker/osäker
    - motiverad/ omotiverad
    - engagerad / förvirrad

17. **Hur medveten är du i ditt dagliga arbete kontra privat om de hot som föreligger?**

AVSLUTANDE FRÅGOR - Tack för din medverkan!

18. **Vilka utmaningar skulle du säga att det finns idag och framöver inom området?**
    - Privat
    - Inom verksamheten
    - I samhället
    - Området i stort

19. **Något jag glömt att fråga som du vill lägga till eller något annat som dykt upp under intervjuns gång?**