LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

Mänsklig Faktor i Cybersäkerhet

En undersökning om hur utbildningen för cybersäkerhet ser ut bland medelstora och stora företag

Kandidatuppsats 15 hp, kurs SYSK16 i Informationssystem

Författare: Milan Bokan

Handledare: Nicklas Holmberg

Rättande lärare: Miranda Kajtazi
Christina Keller

Mänsklig Faktor i Cybersäkerhet: En undersökning om hur utbildningen för cybersäkerhet ser ut bland medelstora och stora företag

ENGELSK TITEL: Human Factor in Cybersecurity: A study of how education for cybersecurity looks like among medium-sized and large companies

FÖRFATTARE: Milan Bokan

UTGIVARE: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

EXAMINATOR: Osama Mansour, Docent

FRAMLAGD: Maj, 2024

DOKUMENTTYP: Kandidatuppsats

ANTAL SIDOR: 46

NYCKELORD: Cybersäkerhet, Mänsklig Faktor i Cybersäkerhet, Serious Games

SAMMANFATTNING (MAX. 200 ORD): Den tekniska utvecklingen tillåter företagen att implementera nya lösningar i sina verksamheter, men den låter även cyberangripare utveckla nya metoder för att angripa företagen. En rad olika metoder bygger på att lura den enskilda anställda i företaget att dela känsliga data med angriparen utan att de själva vet om det. Människan har även beskrivits som den “svaga länken” i cybersäkerhet, eftersom individen fallerar att identifiera försök till attacker och hanterar företagets data på ett "ohygieniskt vis”. Utbildning och träning används idag av företag för att uppmärksamma anställda kring cyberattacker och hur företagets data bör hanteras. Utbildningen är något som kan se olika ut bland olika företag. Vissa företag lägger större tyngd på att informera den anställde om de teoretiska delarna av dessa attacker, medan andra företag lägger större vikt på att inkludera praktiska moment i sin träning. I litteraturen har det noterats att engagemanget bland deltagarna på utbildningstillfällena är något lägre. Som ett lösningsförslag i litteraturen och i arbetet har det diskuterats hur användningen av *serious games*, som är en relativt ny teknologi, samt att ta hänsyn till individens preferenser och kunskapsnivå kan vidare förbättra engagemanget bland deltagarna.

Innehåll

Figurer

Tabeller

1. Introduktion

1.1 Bakgrund

Användningen av olika typer av teknologi är idag en central del av hur företagen bedriver sin verksamhet. Å ena sidan använder företagen teknologi av olika slag till sin fördel för att hitta nya lösningar på problem och för att kontinuerligt sträva efter att vara ett steg framför sina konkurrenter. Detta kan företagen göra genom, som Rohan et al. (2021) skriver, att öka kommunikationshastigheten inom företaget, minska företagets driftskostnader samt förbättra tillgängligheten till företagets system. Å andra sidan, beskriver PR Newswire (2019) att som en direkt konsekvens av den tekniska utvecklingen ökar cyberattacker både i frekvens, men även i hur sofistikerade attackerna som genomförs är mot företagen.

På en nationell nivå skriver Stockholms Handelskammare (2022), att närmare 80 % av alla medelstora och stora företag som är lokaliserade i Sverige har blivit utsatta för minst en cyberattack under året 2020. Fortsättningsvis, diskuterar Stockholms Handelskammare (2022) att cyberkriminalitet skiljer sig från annan typ av kriminalitet i den mån att attackerna som företagen står inför är mer omfattande, i den utsträckning att cyberattacker kan påverka flera delar av företaget samtidigt. Stockholms Handelskammare (2022) skriver att kostnaderna som företagen i Sverige betalade som ett resultat av cyberattacker, uppgick till närmare 30 miljarder kronor under 2021, vilket noterades som en fördubbling i jämförelse med året 2019.

Statistiken som har presenterats av Tech Accord (2021) visar att 95 % av alla cyberattacker som har observerats har varit ett direkt resultat av en *mänsklig faktor*. Ett exempel på en *mänsklig faktor* som Tech Accord (2021) benämner är att människan fallerar att identifiera ett försök till en *nätfiskeattack.*

Rohan et al. (2021) beskriver att den mänskliga faktorn lägger fokus på bland annat hur företagets anställda använder tekniken för att lösa sina arbetsuppgifter samt hur företagets anställda interagerar med företagets system. Rohan et al. (2021) beskriver människan som den “svaga länken” i cybersäkerhet. Corradini (2020) diskuterar att de flesta individerna saknar den förmåga som krävs för att kunna orientera sig på ett säkert vis i den digitala världen, samtidigt som de inte vet vilka risker som de ställs inför. Fortsättningsvis, skriver Corradini (2020), är människans förmåga att lita på andra och deras nyfikenhet också en anledning till att anställda, i hög grad, är benägna att öppna meddelanden och mail från en mottagare som är utanför deras organisation. Den nyfikenheten och tilliten till andra människor är något en tredje part i många fall använder till sin fördel och det är också anledningen till varför simpla metoder, som *nätfiske,* fungerar än idag.

Felhantering av data av företags anställda som bland annat handlar om att de delar data mellan varandra på ett osäkert vis och att de använder svaga lösenord till företagets interna system, men även annan form av felhantering av data beskrivs som att vara den främsta orsaken till att ett dataintrång kan inträffa. Rohan et al. (2021) motiverar, med detta i åtanke, att det inte räcker för företag att implementera tekniska lösningar för att säkerställa att deras data är säker, utan även behöver finna lösningar som inkluderar de anställda som använder företagets system.

För att bringa mer uppmärksamhet till cybersäkerhet och dess risker bland medarbetare i ett företag, har betydelsen av utbildning diskuterats av Microsoft (n.d.). Utbildning är något som kan ske i olika former, Chowdhury et al. (2022) beskriver att utbildningen som används idag bland företagen i många fall är teori-tung, det vill säga att utbildningen lägger mer fokus på *varför* attacken sker istället för *hur* den anställde ska agera för att stoppa attacken, som beskrivet av Aldawood och Skinner (2019). Corradini (2020) och Barletta et al. (2023) har presenterat en något mer innovativ form av utbildning i form av *serious games,* men även att annan typ av praktisk träning, har visat en positiv effekt på utbildningen inom cybersäkerhet. Avslutningsvis har det även en positiv effekt presenterats av Pattinson et al. (2018) och Chowdhury et al. (2022) på utbildningen om individens preferenser och deras kunskapsnivå inkluderas i utformningen av utbildningen.

1.2 Problemformulering

Den tekniska utvecklingen är något som kan påverka företagen på både gott och ont. Som det har presenterats i *bakgrunden* tillåter den tekniska utvecklingen företagen att vidareutveckla sina redan existerande verksamhetsprocesser och implementera nya lösningar för att bedriva sin verksamhet på ett mer effektivt vis. Precis som den tekniska utvecklingen tillåter företagen att komma med nya lösningar, tillåter utvecklingen inom tekniken även cyberangripare att göra samma sak. Som en direkt konsekvens av detta blir metoderna som denna typen av angripare använder sig av bli allt mer sofistikerade och kan påverka företagen på en större skala. Seriositeten av detta har beskrivits i bakgrunden, dels i mängden företag som har drabbats av en cyberattack, dels de monetära konsekvenserna av detta. Vidare har det diskuterats av Tech Accord (2021) och Rohan et al. (2021) att cyberangripare har identifierat den svaga länken i cybersäkerhet, vilket är den mänskliga faktorn. För att adressera den risk som detta utgör för företagen, skriver Corradini (2020) att företagen lägger större investeringar på utvecklingen och implementeringen av tekniska lösningar, när de bör lägga större investeringar på att förbereda sina anställda på risker som de kontinuerligt står inför och hur de bör hantera sin data.

Den vanligaste metoden av upplärning som används inom den privata sektorn, som Chowdhury et al. (2022) beskriver, är utbildning och kampanjer som sker internt i företagen för ökad medvetenhet kring risker inom cybersäkerhet och att förbereda anställda för nödsituationer som kan uppkomma. Problematiken som har presenterats kring denna form av metod som företagen i den privata sektorn har implementerat, som även Flores et al. (2023) presenterar, är att utbildningsmomenten i många fall lider av lågt engagemang bland deltagarna, detta i kombination med att Aldawood och Skinner (2019) har beskrivit att utbildningarna inte ger deltagarna möjligheten att veta *hur* de ska agera vid olika typer av risker, utan endast varför cybersäkerhet är en central del att tänka på.

Vidare har det noterats av Mwangala et al. (2023) att det är ett fåtal som deltar på utbildningsmomenten, Mwangala et al. (2023) skriver 61.4 % av deltagarna i studien som genomfördes inte har deltagit på någon form av cybersäkerhetsträning. Mwangala et al. (2023) har även noterat att de som tidigare har deltagit på någon form av träning, efter träningen har återgått till att använda sig av en osäker hantering av data, Mwangala et al. (2023) har sammanfattat osäker hantering av data som att anställda delar sina lösenord mellan varandra samt att de kontinuerligt öppnar mail från okända personer utanför deras organisationer med okända filer bifogade.

1.3 Frågeställning

Litteraturen för arbetet har påvisat att den mänskliga faktorn är ett större dilemma i cybersäkerhet än vad många företag föreställer sig. För att få en djupare förståelse för hur företagen förbereder sina anställda, kommer följande frågeställning att sätta grund för arbetet:

Hur ser utbildningen för cybersäkerhet ut bland medelstora och stora företag?

1.4 Syfte

För att kunna få en gedigen förståelse för ämnet och det område som undersöks i detta arbete och för att på ett mer konstruerat vis genomföra undersökningen, kommer fokuset främst att delas upp i tre delar. Den första delen handlar om att vidare förstå den *mänskliga faktorn* i cybersäkerhet. Den andra delen handlar om hur det ser ut bland företagen, att undersöka hur utbildningen för cybersäkerhet ser ut bland medelstora och stora företag för att kunna arbeta med de olika cybersäkerhetsrisker som kontinuerligt utvecklas, både i dess komplexitet samt i dess frekvens som de sker i. Baserat på de två tidigare delarna kommer även lösningsförslag att presenteras, som kan användas som en grund för hur företagen kan utveckla utbildningen kring cybersäkerhet. I mån om att tydligare beskriva de olika aspekterna av varför förslagen har inkluderats, kommer förslagen att presenteras i en tabell.

1.5 Avgränsningar

Det har noterats av Corradini (2020) som en del av problemformuleringen att företagen bör se över sina strategier för att “bekämpa” de cybersäkerhetsrisker som företagen står inför, Corradini (2020) skriver att företagen lägger en hög grad av fokus på tekniska lösningar för att kunna behålla sin data säker. I detta arbete, hursomhelst, kommer fokus att läggas på hur företagen utbildar sina anställda och inte vilka tekniska lösningar som företaget har implementerat.

Som det också har noterats i bakgrunden är cybersäkerhet något som företag på en global skala kämpar för. Alla etablerade företag är kontinuerligt i riskzonen för att bli offer för en cyberattack. För att något begränsa den undersökningen som görs kommer fokuset kontinuerligt att placeras på företag av en större omfattning, det vill säga medelstora och stora företag.

2. Litteraturgenomgång

Det primära syftet med detta kapitel är att gå igenom tidigare studier och forskning som har gjorts som är relevant till den mänskliga faktorn i cybersäkerhet, hur utbildningen ser ut bland företagen, problematiken i företagens strategier samt vilka lösningsförslag som har diskuterats i studierna. Resultatet hämtat från de studier som tidigare har genomförts kring de benämnda forskningsområdena kommer sedan att placeras i en tabell tillsammans med källorna som har använts för att identifiera de olika områdena av ämnet som undersöks.

2.1 Vad är cybersäkerhet?

Cybersäkerhet, skriver Microsoft (n.d.), är metoder som används för att skydda bland annat ens digitala information, de enheter som används och ens tillgångar från en skadlig tredje part. Microsoft (n.d.) beskriver att det bland annat kan innefatta personlig information, system som används av ett företag, filer samt konton. Fortsättningsvis, nämner även Microsoft (n.d.) “CIA”, som är ett ramverk som används som kombinerar de tre pelarna av cybersäkerhet.

Konfidentialitet handlar om att sätta upp skydd för att säkerställa att endast de som har tillgång till data kan komma åt datan i ett system, beskriver Cawthra et al. (2020).

Integritet syftar på att sätta upp barriärer för att hindra en tredje part från att modifiera, eller radera, den data som visas i ett system, att den data som visas i ett system är det som ska visas, skriver Microsoft (n.d.).

Åtkomst handlar om att kontinuerligt försäkra att dels, en ska ha åtkomst till det system som används, men även att en ska kunna använda och komma åt system när en behöver det för att, till exempel, kunna utföra sina arbetsuppgifter, skriver Cawthra et al. (2020). Microsoft (n.d.) bygger vidare på detta och beskriver att åtkomstproblem till ett system kan vara en direkt konsekvens av en överbelastningsattack.

För att beskriva konsekvenserna av en cyberattack, skriver IBM (n.d), att cyberattacker kan resultera i störningar i företagets verksamhetsprocesser, orsaka större skador inom företagen samt förstöra företag.

2.1.1 Vad är cybermedvetenhet

Den fundamentala delen av cybermedvetenhet, med hänvisning till Tech Accord (2021), är att anställda bör ha en förståelse för hur en ska identifiera olika typer av hot, bland annat *nätfiske*attacker, men även att de ska ha en förståelse för hur de bör hantera- och dela data internt i företaget på ett säkert vis, inte använda lösenord som är svaga och relativt enkla för en angripare att kunna lista ut samt att de inte ska ansluta sina enheter till opålitliga nätverk och ansluta okända USB-stickor till ens enhet. Tech Accord (2021) skriver att angripare har en tendens att lägga fokus på att hitta svaga länkar i företaget. I många fall handlar detta om anställda som saknar medvetenhet inom cybersäkerhet, det vill säga anställda som har en tendens att operera på ett "ohygieniskt" vis när det kommer till cybersäkerhet.

2.1.2 Den mänskliga faktorn i cybersäkerhet

Rohan et al. (2021) skriver att baserat på den tidigare forskningen, är människor den svagaste länken för företagen att bygga upp en säker miljö för sina system och tillgångar, tillgångar i form av bland annat information som deras verksamhet bygger på. Vidare beskriver Rohan et al. (2021) att dataintrång och andra former av attacker är ett resultat av användarens beteende när de använder företags system och enheter. Detta beteende som Rohan et al. (2021) menar är att användaren i många fall delar lösenord mellan sin medarbetare, kan förse en tredje part med data som de arbetar med genom att de öppna okända länkar som innehåller *inbäddade webbsidor samt* att de i flera fall laddar ner okänd media på sina enheter, bland annat deras datorer och telefoner. Något som vidare bygger på argumentet presenterat av Rohan et al. (2021) som handlar om

slutanvändarens hantering av lösenord, är forskning som har genomförts av Mwangala et al. (2023). Resultatet som presenterades av Mwangala et al. (2023) visar att 63.4 % av medarbetarna som deltog i denna studie delar sina lösenord mellan varandra för enklare hantering. Något som vidare visar på en svagare hantering av lösenord bland anställda är att av de som deltog i studien, menar 66.7 % att de använder samma lösenord för sina arbetsrelaterade plattformar som plattformar som de använder i sitt privatliv, som bland annat sociala medier. Mwangala et al. (2023) beskriver detta som ett tecken på dålig "cyber hygien". Något som sammanfattar vad som har presenterats av Rohan et al. (2021) och Mwangala et al (2023) är att 95 % av de dataintrång som har skett, som har visats av Tech Accord (2023), är ett resultat av misstag som har skett av slutanvändaren, bland annat anställda inom företag.

I spåren av hur data hanteras av anställda inom företag, beskriver Flores et al. (2023) att anställda lägger mer fokus på att avsluta en arbetsuppgift, än att fokusera på de risker som kan uppkomma om de hanterar datan, som de använder för att utföra för sina arbetsuppgifter, på ett felaktigt vis. Detta resultat är något som sammanfattas av Flores et al. (2023) som att högre prioritet bland anställda läggs på att klara en arbetsuppgift, än att fokusera på de risker som kan möjligtvis skapas om datan hanteras på ett felaktigt vis.

2.1.3 Social engineering

För att beskriva vad *social manipulation* handlar om, i enlighet med vad Workman (2007) skriver, handlar detta koncept om olika tekniker som en cyberangipare kan använda sig av för att manipulera en viss person till att göra vad en önskar, vilket kan till exempel vara att en anställd i ett företag utför en viss handling eller delar med sig av sekretessbelagt information. För att bygga vidare på denna definition, beskriver Barber (2001) att *social manipulation* är ett verktyg som attacker kan använda sig av för att komma åt den information som de är ute efter från organisationen som helhet eller från en viss anställd inom ett företag. Detta är något som Barber (2001) likställer med att en cyberangripare kan använda sig av en viss mjukvara eller hårdvara som ett verktyg för att utföra en cyberattack, kan *social manipulation* användas som ett verktyg av en cyberangripare för att nå samma ändamål.

Workman (2007) beskriver vidare att en person som har som ändamål att manipulera en annan kan göra detta på olika vis. Å ena sidan kan denna personen försöka att manipulera en annan person genom att bygga på deras känslor, som till exempel spänning eller rädsla, å andra sidan kan andra inleda försök på att manipulera en annan person genom att bilda en social relation, eller genom att bilda en känsla av tillit med denna personen, med deras *offer.* Workman (2007) skriver att de emotionella faktorer i interaktionerna mellan offret och personen som utför manipulationen, är något som kan distrahera personens förmåga att kunna analysera vad som sägs i interaktionen mellan dessa två parter. Detta är något som sedan kan resultera i att offret delar känslig information som angriparen kan använda sig av för att sedan få åtkomst till personens enheter och för att sedan kunna få åtkomst till data på dessa enheter. Eftersom *social manipulation* är något som bygger på att angriparen använder offrets svagheter till sin fördel, skriver Barber (2001) att *social manipulation* är en av de mest effektiva, men även kraftfulla, *verktygen* som en angripare kan använda sig av för att få tillgång till känslig data.

Nätfiske är ett exempel på en metod som används av angripare som faller under *social manipulation.* MSB (n.d) skriver att nätfiske idag är en av de vanligaste metoderna som används

av angripare. NCSC (2018) skriver att denna typ av attack innebär att en angripare skickar någon form av meddelande, i form av ett sms eller ett mail, direkt till offret, vilket kan vara en anställd inom ett företag. NCSC (2018) fortsätter och skriver att detta meddelande vanligtvis inkluderar en länk som tar personen vidare till en skadlig webbplats. För ett företag, säger MSB (n.d), att detta kan leda till att delar, eller hela, företagets it-system och dess information krypteras och inte är tillgängliga för företagets anställda. Vidare skriver NCSC (2018) att nätfiske kan användas för att lura individen till att, till exempel, dela sina lösenord, genom att leda individen till en hemsida som utger sig vara legitim och ber individen att skriva in sin information för att, till exempel, logga in.

Enligt Hartfield (2017) är *imitation en* typ av cyberattack som bygger på *social manipulation* och används främst av en angripare för att samla information, i form av lösenord och användarnamn, för att kunna logga in och få tillgång till ett system. För att angriparen ska kunna samla den information som är nödvändig, från en anställd i ett företag till exempel, för att de ska kunna logga in på detta system, använder angriparen sig av en rad olika strategier. En av dessa strategier, som Hartfield (2017) beskriver, är *spoofing.* Hartfield (2017) skriver, relaterat till *spoofing,* att en angripare kan ringa en anställd inom ett visst företag och påstå sig själva ringa från en viss avdelning inom företaget som kräver deras *användarnamn* och *lösenord,* genom att använda en viss applikation kan angriparen skriva in vilket nummer som ska presenteras för personen som mottar telefonsamtalet, vilket kommer att resultera i att den anställda kommer att tro att den är någon inom företaget som ringer och är den personen de påstår sig själva vara. Hartfield (2017) skriver att angriparen sedan kan använda den information som de har fått från den anställda inom företaget för att logga in på företagets system som den anställda för att vidare samla in data som kan vara av värde för företaget.

Alotaibi et al (2024) har vidare presenterat problematiken kring *deepfakes* och dess användning som en form av *imitation. Deepfakes,* som Alotaibi et al. (2024) skriver, är något som har använts av en rad olika angripare för både ekonomiskt bedrägeri samt identitetsstöld. *Deepfakes* beskrivs av Barney (2023) som en typ av *artificiell intelligens (AI)* som används för att skapa övertygande videos, bilder och ljud. När en skapar en *deepfake,* skriver Barney (2023), att i de flesta fallen används det redan existerande källinehåll, som ersätts till annat innehåll, men det kan även handla om att det är helt nytt innehåll som skapas där det visas att någon gör, eller säger något, som de inte har gjort, eller sagt. Avslutningsvis, menar Barney (2023), att det främsta hotet som introduceras med användning av sådan teknologi är möjligheten detta skapar att sprida information som är falsk, men ser ut att komma från en pålitlig källa. Genom att använda information om en viss banks direktörer som var tillgänglig för allmänheten, skriver Alotaibi et al. (2024) att cyberkriminella lyckades fabricera ett röstmeddelande från en direktör från denna bank. Detta resulterade sedan i att den finansiella institutionen överförde $35 miljoner till dessa cyberkriminella. Fortsättningsvis, säger Alotaibi et al. (2024) att samma teknologi har använts för att skapa en fiktiv inspelning av en VDs övre chefer, för att godkänna en transaktion på närmare $245,000 till en påhittad leverantör. Dessa två exempel som Alotaibi et al. (2024) presenterade visar på seriositeten som denna teknologi innebär.

2.1.4 Mental hälsa och cybersäkerhet

Corradini (2020) och Puta (2022) beskriver att individens mentala hälsa är något som kan ha en inverkan på hur väl en person hanterar information som presenteras för den. Puta (2022) bygger

vidare på detta resonemang och skriver att av den anledningen är cybersäkerhet och mental hälsa något som är nära kopplat till varandra.

Fortsättningsvis, skriver Puta (2022) att forskning har visat att om en person lider av lindriga mentala besvär, som till exempel stress, kan detta ha en direkt påverkan på människans minne. Puta (2022) ger ett beskrivande exempel och skriver att när någon är stressad, till exempel, kan detta leda till att en glömmer den träning som en har genomgått relaterat till cybersäkerhet och av den anledning kan trycka på en länk som har sänts från en okänd källa.

Psykiska besvär är något som kan visa sig i olika former och är något som kan påverka en på olika vis. Enligt Puta (2022), är detta något som också kan ha en inverkan på en individs förmåga att kunna identifiera ett cyberangrepp, vilket kan leda till att en blir ett offer för en cyberattack. En forskning som Puta (2022) hänvisar till, visar på att under *normala* omständigheter lyckades individerna som deltog i forskning att identifiera 70 % av försöken på cyberangrepp som de ställdes inför. Forskningen visade sedan på att individerna var, i en högre grad, benägna att falla för en cyberattack när de visade tecken på stress, depression eller trötthet.

2.2 Varför utbildning inom cybersäkerhet är viktigt

Det har beskrivits i tidigare litteratur, av bland annat Rohan et al. (2021), att människor och företagets anställda, är något som ses som den svaga länken i cybersäkerhet. Av den anledningen, men även för att anställda ska kunna ha den färdighet som krävs för att kunna identifiera olika typer av cyberattacker, skriver elev8 (n.d.) om betydelsen för företagen att utbilda sina anställda. Som det har presenterats i litteraturgenomgången, men även elev8 (n.d.), drar sig angripare mot anställda som de anser inte kommer kunna identifiera attacken. Angripare ger sig an anställda inom företag genom olika typer av attacker. Elev8 (n.d.) tar upp exempel som bland annat nätfiske, men även andra typer av attacker som bygger på social manipulation. Genom att sedan använda resurser för att lära upp och träna anställda, kan företagets anställda identifiera försök till olika typer av attacker som de ställs inför och minimera risken att de utsätts för en attack. Tyngden i denna typ av träning ligger också i att de olika metoder för cyberattacker som angripare använder sig av, är något som kontinuerligt utvecklas. Elev8 (n.d.) betonar av den anledningen vad utbildning inom cybersäkerhet kan betyda för företagen och för att de ska kunna anpassa sig efter de attacker som kontinuerligt utvecklas.

2.3 Problematiken kring företagens strategier

Intern utbildning och kampanjer, skriver Chowdhury et al. (2022), är en vanlig strategi bland företag vid upplärning av anställda. Vidare tar Chowdhury et al. (2022) upp att det finns en del kritik som presenteras angående effektiviteten av denna strategi för företag inom den privata sektorn. Att denna typ av strategi är något som visats är ineffektiv för företagen, är något som kan visas med hjälp av statistiken presenterad av Tech Accord (2021). Enligt Tech Accord (2021) är 95 % av de cyberintrång som företag utsatts för ett resultat av fel som har begåtts av slutanvändaren, Tech Accord (2021) kommenterar ytterligare att ett exempel på ett sådant fel är att de misslyckas att identifiera ett försök till en *nätfiskeattack.* Något som ytterligare visar på detta är de siffror som har presenterats av Mwangala (2021). Enligt Mwangala (2021) återgår en större andel av dessa anställda till att dela sina lösenord mellan varandra samt att öppna mail och

dess bifogade filer även om dessa mail kom från en person som var utanför deras organisation efter att ha gått på denna typ av träning. Att anställda inom företag fortsätter att dela sina lösenord mellan varandra och öppna okända filer från personer utanför deras organisation, säger Mwangala (2021) är tecken på att deras träning och beredskap inom cybersäkerhet är ineffektiv.

Som diskuterat av Chowdhury et al. (2022), är träningsprogram en av de mer favoriserade och mest använda metoderna för att lära upp deras anställda och samma typ av metod används idag av företag inom den privata sektorn för att lära upp sina anställda i olika roller hur de bör hantera företagets data. Chowdhury et al. (2022) beskriver att en av de mer kritiska faktorerna i ett lyckat träningsprogram är engagemang hos användarna. Enligt Flores et al. (2023), som bygger vidare resonemanget presenterat av Chowdhury et al. (2022), är en av de främsta nackdelarna som företagen står inför vid presenterade träningsprogram relaterat till cybersäkerhet att de löpande lider av lågt engagemang hos deltagarna. Gross (2018) skriver att anledningen till varför engagemanget för dessa typer av träningar är lågt bland deras anställda, är att inte, som Gross (2018) beskriver det, inte “bryr sig” om vad det är som kan hända företaget. Gross (2018) fortsätter och skriver att såvida inte företagen har en förmåga att ändra inställningen att de inte förstår varför företaget gör som de gör och börjar lägga mer fokus på vad som kan hända företaget, kommer attityden hos anställda för dessa typer av träningsprogram inte att ändras. Det Gross (2018) skriver är något som i linje med de resultat som presenteras av Mwangala et al. (2023). Det resultat som presenterades av Mwangala et al. (2023) visar att 61.4 % av deltagarna i studien inte deltog på träning för medvetenhet om cybersäkerhet, medan 32.1 % av de som deltog menade på att träningen som gavs inte var effektiv.

Något som Mwangala et al. (2023) talade för att utbildningen vidare var ineffektiv, var att de som deltog i utbildningen endast deltog en gång. För att utbildningen ska vara effektiv, med hänvisning till Mwangala et al. (2023), bör utbildningen ske minst tre gånger per år.

De träningsprogram som utvecklas inom företagen är något som kan variera baserat på en rad olika faktorer, beskriver Aldawood och Skinner (2019), bland dessa faktorer ingår trycket som uppstår i den marknad som företaget opererar inom samt deras budget. För att företag ska kunna vara profitabla, speciellt inom en kompetitiv marknad, som beskrivet av Aldawood och Skinner (2019), försöker företag att aktivt minska deras utgifter. Som en direkt konsekvens av att företagen försöker minska sina utgifter, fortsätter Aldawood och Skinner (2019) att beskriva att företagen inte prioriterar deras budget som är dedikerade till träningsprogram. För att kunna utveckla ett något mer omfattande träningsprogram, som inkluderar bland annat onlinekurser och andra sorters utbildningssatsningar, som även är uppdaterade, som Aldawood och Skinner (2019) beskriver, krävs en något mer omfattande budget. Fortsättningsvis, menar Aldawood och Skinner (2019), att som en följd av att företagen inte dedikerar en något större budget till träningsprogram som består av olika delar och är uppdaterade, kan cyberkriminella utveckla nya metoder, i form av attacker, som kan kringgå de, nu, föråldrade “barriärer” som företaget satt upp.

Aldawood och Skinner (2019) skriver att traditionella metoder som många företag använder sig av handlar bland annat om att företagen skriver ut affischer som informerar de anställda om cyberattacker samt presenterar den anställde med information på företagets datorer som handlar om konsekvenserna som felhantering av data kan ge. Problematiken med denna typ av metod, som Aldawood och Skinner (2019) vidare diskuterar, är att den fallerar att presentera den anställda med praktisk exponering till de olika formerna av attacker. Genom den *traditionella*

metoden menar Aldawood och Skinner (2019) att företagets anställda introduceras till vad de olika säkerhetsriskerna handlar om och vad de kan innebära för företaget, men inte hur de ska agera för att mitigera risken för en attack och för att kunna identifiera attacken redan i ett tidigt stadium.

2.4 Lösningsförslag diskuterade i litteraturen

Aldawood och Skinner (2019) presenterade att ett problemområde för upplärningen, i dess olika former, för cybersäkerhet är hur företagen allokerar sina resurser. För att företagen ska kunna utveckla ett träningsprogram som adresserar deras behov, skriver Aldawood och Skinner (2019), behöver dedikera en egen budget som kan stödja dessa program. Hursomhelst, detta är något som företagen har fallerat att göra. Detta eftersom, med hänvisning till Aldawood och Skinner (2019), företagen i många fall prioriterar bort den dedikerade budgeten för träningsprogram för att de ska kunna gå med en högre vinst.

För att företagen ska kunna motivera allokationen av resurser, men även för att de ska förstå sitt behov av ett träningsprogram som lägger tyngd på cybersäkerhet, skriver Flores et al. (2023) att företagen bör göra en bedömning för att få en tydligare förståelse av sina behov. För att kunna identifiera specifika behov och typer av träning, diskuterar Wilson och Hash (2003), att en sådan bedömning borde sträcka sig över flera roller i företaget. Bland dessa roller som är involverade i denna process, beskriver Flores et al. (2023) att organisationens ledare genomgående bör vara involverade för att uppmuntra en full överensstämmelse bland deras användare, fortsättningsvis bör även säkerhetspersonal vara involverade i denna process eftersom de har en omfattande förståelse för bästa praxis och regelverk. Avslutningsvis ska även användare som utför rutin arbetsuppgifter i systemet vara med i denna process.

Denna typ av bedömning är något som bör sträcka sig över flera roller, och avdelningar, inom ett företag. Av den anledningen kan denna process komma till att kräva en större del engagemang från flera aktörer inom företaget för att identifiera de olika behoven inom företaget. Flores et al. (2023) nämner att detta är en av de främsta nackdelarna med denna typ av strategi. Vidare diskuterar Floret et al. (2023) att dessa aktörer kan komma att behöva arbeta under specifika roller som eventuellt inte existerar inom vissa företagsstrukturer.

Flores et al. (2023), Pattinson et al. (2018) och Chowdhury et al. (2022), har observerat hur träning som är utformad efter att individens preferenser kan ha en positiv effekt på inlärningsprocessen som helhet. Pattinson et al. (2018) presenterade resultatet att hur ofta, eller hur frekvent, träningen genomfördes inte hade en direkt korrelation till, vad Pattinson et al. (2018) beskriver det som, *Information Security Awareness (ISA)-poäng.* Hursomhelst, visar Pattinson et al. (2018), att träningen hade en mer positiv effekt på *Information Security Awareness (ISA)-poäng* om utformningen som träningen hade matchade med en individs preferenser av olika typer av träning. Pattinson et al. (2018) summerar detta i att den egentliga frekvensen av träningen kan resultera i att budskapet i träningen kan presenteras i olika former, vilket kan leda till att individens preferens i form av träning kan komma att presenteras, men att det är den egentliga matchningen mellan form av träning och individens preferenser som resulterade i, Pattinson et al. (2018) beskriver det, en ökning i *ISA-poäng.*

Problematiken kring detta, som har diskuterats av Pattinson et al. (2018) och Flores et al. (2018) är att det inte är möjligt för ett företag att kunna undersöka allas preferenser inom ett företag och att kunna forma träning som kan inkludera individens preferenser. Detta är något som Pattinson et al. (2018) också har noterat i det presenterade arbetet och skriver att det kan komma till en större fördel för ett företag att istället för att göra en *bedömning på en individnivå* inom företag, istället *undersöka olika grupper och divisioner* inom företag och att sedan forma träningen baserat detta.

Avslutningsvis, skriver Flores et al. (2023) att det kan vara svårare för mindre företag, som saknar en viss grad expertis som krävs för att kunna utföra en sådan bedömning och anpassa olika sorters teknologier för att arbeta mot att matcha formen av träning till de olika preferenser olika individer har. Med detta i åtanke, hänvisar Flores et al (2023) till *Gartner* som erbjuder en rad olika lösningar för företag. Bland dessa hänvisar *Gartner* företagen till en rad olika företag som erbjuder lösningar för datorbaserad träning. Flores et al. (2023) diskuterar även att många av de företag som *Gartner* hänvisar till erbjuder en gratis *kunskapskontroll* samt att många av dessa kan vara tillgängliga för företagen som en *Software as a Service-lösning.*

I spåren av att använda en datorbaserad, och innovativ, lösning som träning, har det diskuterats av bland annat Corradini (2020) och Barletta et al. (2023) hur *Serious Games* kan inkluderas i träningen som en interaktiv och praktisk form av inlärning för att öka medvetenheten vid cybersäkerhet. Vidare skriver Barletta et al. (2023), genom att implementera *Serious Games* som en utbildningsmetod, menar Barletta et al. (2023) att spelaren, till exempel den anställda, kan lära sig olika cybersäkerhetskoncept, men även hur de bör agera i olika scenarion. Detta sker i en icke-hotfull miljö, vilket tillåter en säkrare samt en något mer lekfull form av inlärning, detta i kombination med att det är en kostnadseffektiv form av inlärning för företagen och dess anställda. Att kunna sätta sig in i olika situationer och lösa en uppgift baserat på en *simulation* av en verklig händelse, är även något som erbjuds av Microsoft (n.d.), som en del av deras *Attack simulation training* som låter en att bland annat att arbeta med *nätfiskeattacker.*

Flores et al. (2023) samt Barletta et al. (2023) har presenterat fördelar med hur spel, i form av *serious games,* kan användas som en form av upplärning för cybersäkerhet. Resultatet som presenterades av Flores et al. (2023) visar att spel är något som kan användas som ett användbart verktyg för att vidare förbättra engagemanget från anställda för program för cybersäkerhet. Vidare noterar Flores et al. (2023) att detta är främst något som har visats bland yngre eller har en anställning i företagen på en ingångsnivå. Fortsättningsvis, skriver Barletta et al. (2023) att det för tillfället finns en rad olika spel som fokuserar på olika områden av cybersäkerhet. Bland annat, som Barletta et al. (2023) beskriver, har företag som *Cybersecurity & Infrastructure Security Agency* och *Pacific Northwest National Laboratory* genom ett samarbetet släppt ett flertal spel som lägger fokus på, i en simulerad värld, olika cyberhot, cyberförsvar samt säkerhetsåtgärder. Barletta et al. (2023) refererade till ett förslag på ett spel av Aladawy et al (n.d.), som i artikeln fått namnet “Persuaded”. Spelet handlar om att genom att användaren spelar i en fiktiv värld, ska spelet träna en till att kunna motstå attacker i form av social manipulation, genom att använda sig av psykologiska försvarsmekanismer. Ett annat exempel på ett sådant spel är *CyberHero.* Skaparna av detta spel, Hodhod et al. (2023), menar på att genom att en användare får en möjlighet, genom spelet, att kunna se vilken långvarig konsekvens deras handling kan ha i spelets handling, men även genom att kunna se den direkta konsekvensen av användarens felhantering av information ur ett cyber säkerhetsperspektiv, kan användaren utveckla en djupare förståelse för vilken betydelse cybersäkerhet kan ha i deras vardag.

Hodhod et al. (2023) beskriver att spelet *CyberHero* bygger på *Super Mario Effect* som presenterades av Mark Rober. Mark Rober genomförde ett experiment i form av ett kodnings-spel. Experimentet som Mark Rober genomförde visade att de användare som inte blev straffade när de gjorde ett misstag var mer benägna att börja om från början än de som blev straffade för de misstag de gjorde. Detta koncept bygger på att när en spelar ett spel som *Super Mario*, eller liknande spel, fokuserar en endast på att nå målet genom att försöka flera gånger till en lyckas samtidigt som en lär sig från sina misstag. Slutsatsen som Hodhod et al. (2023) drar från detta, är att *Super Mario Effekten* uppmärksammar betydelsen av att skapa en positiv miljö för inlärning, en positiv miljö där ens misslyckande i ens agerande i en viss situation inte skapar några negativa konsekvenser, utan istället ger en en möjlighet att lära sig från sina misstag. Hodhod et al. (2023) berättar att detta var ett centralt tänkande under utvecklingen av *CyberHero* och menar att genom en fokuserar på målet och är motiverad under spelets gång är sannolikheten större att användaren spelar spelet tills dess slut och lär sig på ett mer effektivt vis.

2.5 Tillämpade teorier

2.5.1 Personalized learning theory

Morin (2020) skriver att *personalized learning theory* är en utbildningsmetod med ändamålet att bygga upp upplärningen baserat på studenternas preferenser, styrkor, behov och färdigheter. Vidare skriver Morin (2020) att det kan ta olika lång tid för individer att lära sig färdigheter, men *personalized learning theory* låter individen nå de krav som är uppställda, i sin egen takt. Morin (2020) beskriver att detta är motsatsen till en, som beskrivs som en, “one size fits all”-metod som idag används i de flesta utbildningstillfällena, *Personalized learning theory* bygger istället på att varje individ tilldelas en inlärningsplan som baseras kring deras färdigheter, styrkor och preferenser.

2.5.2 Optimistisk bias och cybersäkerhet

För att beskriva *optimistisk bias,* skriver Aue och Okon-Singer (2015) att det handlar om individens förmåga att kunna överestimera sannolikheten för att de ska vara med om en positiv händelse, men även deras underestimera att ska vara med om en negativ händelse, i framtiden.

Konsekvensen av *optimistisk bias* som Alnifie och Kim (2023) beskriver är att människor bildar sig en uppfattning som speglar att de är immuna mot cyberattacker. Detta trots att andra har visat att de är sårbara för dessa typer av attacker eftersom de underskattar risken som de ställs inför. Fortsättningsvis, skriver Alnifie och Kim (2023) att denna *optimistiska bias* som har uppstått och faktumet att många människor anser att de är säkra och immuna från cyberangrepp, har resulterat i att många väljer att bortse ifrån och inte använda sig av olika preventiva metoder som idag finns för hot inom cybersäkerhet. De preventiva metoderna som diskuteras av Alnifie och Kim (2023), innebär bland annat *antivirusprogram,* men även andra *programfix*, eftersom de i många fall anser att dessa inte kommer att användas och av den anledningen inte behöver installeras på enheten som de använder.

Vidare nämner Alnifie och Kim (2023) nätfiske och skriver att de som misslyckas att identifiera en sådan attack och blir ett offer för en nätfiskeattack är, till stor del, de som är omedvetna om

denna typ av attack eller de som har ett optimistiskt tänkande. Alnifie och Kim (2023) hänvisar till ett arbete som studerade preventiva metoder kring nätfiskeattacker samt hur ett optimistisk tänkande kan påverka detta. Studien visar att trots att individer har förmågan att kunna identifiera nätfiskeattacker och kunna implementera de nödvändiga preventiva metoder för att stoppa denna typ attack i teorin, hindras de från att göra detta i praktiken på grund av deras optimistiska tänkande.

Alnifie och Kim (2023) hänvisade till en studie som undersökte hur detta kan se ut i praktiken, studien som Alnifie och Kim (2023) hänvisade till visade på att de som, genom ett bias tänkande, ansåg att de kunde vara med om en cyberattack, men att de inte skulle vara en "seriös" attack om det skulle ske, var i en högre grad benägna att öppna hemsidor som var opålitliga. Alnifie och Kim (2023) hänvisade vidare till en annan studie, som visade på en något mer positiv effekt med *optimism bias och cybersäkerhet.* Genom deras optimistiska tänkande kring preventiva metoder för cybersäkerhet. Genom studien att deltagarna menade att om de skulle bli ett offer till en cyberattack, kommer de preventiva metoderna som de har implementerat att rädda dem.

2.5.3 Inlärning med hjälp av praktiska moment

Praktisk träning, eller upplevelsebaserad lärande och *learning by doing* som Main (2023) beskriver det, är ett pedagogiskt tillvägagångssätt som bygger på att, genom praktiska erfarenheter inom ett ämne, kan en individ bygga en djupare förståelse för ämnet eller handlingen som individen genomför. Praktisk erfarenhet, beskriver Main (2023), kan agera som ett "påskyndande medel" för kognitiv utveckling genom aktivt engagemang av deltagaren i lärprocessen. Main (2023) diskuterar att denna metod låter flera sinnen arbeta samtidigt, vilket låter individens hjärna att kontinuerligt engagera sig i aktiviteten, något som sedan resulterar i ökad inlärning om det ämne som behandlas.

Genom att inkludera ett eller flera praktiska moment i inlärningen, beskriver Main (2023), att en kan bilda en djupare förståelse för ämnet, men även att kunna *plocka upp* och bevara kunskap genom ett praktiskt moment. Detta är något som Main (2023) skriver kan ha en betydande inverkan på individens förmåga att kunna utveckla ett kritiskt tänkande samt på hjärnans kognitiva funktioner.

I ett praktiskt moment uppmuntras individen att göra egna beslut och lösa problem som de ställs inför, som en positiv konsekvens av detta, diskuterar Main (2023), att individens kritiska tänkande utvecklas. Genom att vidare arbeta med riktiga problem och andra typer av utmaningar, diskuterar Main (2023), utvecklas individens förmåga att kunna analysera olika situationer, bedöma den information som de ställs framför och komma med kreativa lösningar till problemen.

Att individen uppmuntras att göra egna val när de ställs inför ett problem, är hur Main (2023) presenterar att praktiskt träning skiljer sig från, vad Main (2023) beskriver som, "traditionell upplärning" som lägger mer fokus på att individen ska lyssna på det som sägs och minnas detta.

2.5.4 Teoretisk grund för serious games

För att kunna förklara den teoretiska grunden kring *serious games* och dess användningen i ett syfte för upplärning och för att kunna förklara de psykologiska mekanismer som som låter *serious games* ha den positiva inverkan på inlärningen som det har studerats och visats i

litteraturgenomgången, skriver Krath et al. (2021) att detta är något som bygger på en rad olika teoretiska grunder. Krath et al. (2021) presenterar exempel på teorier som bygger på *motivation and affect*-teorin samt *behavior and learning*-teorin som två primära exempel för att kunna förklara de teoretiska byggstenarna bakom *serious games* och dess positiva inverkan.

Krath et al. (2021) avslutar och skriver att när en användare spelar ett spel, möts användaren av en rad olika mekanismer inom spelets ramar. Krath et al. (2021) presenterar bland annat poäng, levlar, märken samt uppdrag som användaren kan vinna för att vidare bredda sin kunskap och skriver att med hjälp av dessa mekanismerna i spelet, visar spelet olika mål och dess relevans, som användaren kan uppnå, leder spelet användaren till målet, för att uppnå en viss kunskap som är redan uppsatt i spelet.

För att vidare beskriva den teoretiska grunden för *serious games,* hänvisar Hodhod et al. (2023) till ett experiment som genomfördes av Mark Rober. Mark Rober utvecklade, tillsammans med sin kollega, ett enkelt kodnings-spel som han använde och sedan publicerade för sina *youtube-prenumeranter* att spela. Målet med detta spel var att användaren skulle, med hjälp av olika block av kod, kunna transportera en bil från start till mål. När Mark Rober genomförde detta experiment, publicerade han två versioner av spelet. Den enda skillnaden mellan de två versionerna av spelet var att meddelandet som användaren fick när de hade misslyckats. De användare som spelade den ena versionen, “Version A”, förlorade spelaren inga av sina två hundra poäng och presenterades istället endast med meddelandet “That didn’t work, please try again”. Spelarna som fick den andra versionen av spelet, "Version B”, förlorade fem poäng, av sina initiala tvåhundra, vid ett misslyckande av uppgiften och presenterades med meddelandet “That didn’t work. You lost 5 points. You now have 195 points. Please try again”.

Resultatet av detta experiment, med totalt 50,000 deltagare, visade att av de som förlorade fem poäng för varje gång de misslyckades med uppgiften, var det 52 % som klarade av spelet. Av de som inte straffades för deras misslyckade försök, var det 68 % som sedan klarade spelet. De som inte straffades för deras misslyckade försök, "Version A”, klarade av spelet efter tolv försök, vilket kan jämföras med de som spelade “Version B”, som klarade spelet efter fem försök. Rober menar att, baserat på detta resultat, att inlärningsmiljön, som att en straffas för ens misslyckade försök, är något som kan komma att spela en större roll för ens inlärningsprocess. Mark Rober diskuterar sedan att när en spelar ett spel som “Super Mario” och misslyckas, bemöts en inte med ett meddelande om att en har misslyckats, utan spelet börjar om från början. Som resultat av detta, lägger spelaren endast fokus på hur de ska nå målet och inte att de har misslyckats. Rober beskriver att en istället tänker på vad en kan göra annorlunda nästa gång och istället lära sig från sina misstag för att nå målet. Genom att istället fokusera på *vad* en kan göra istället och inte vilka misstag som en har gjort, menar Rober att en kan lära sig något lättare och inom en kortare tidsram.

2.6 Teoretiskt resultat

Grundområde	**Behandlade ämnen**	**Källor**
Cybersäkerhet	- Försäkra tillgänglighet till företagets system	Microsoft (n.d.), Cawthra et al. (2020, IBM (n.d)

	- Skydda informationen - Försäkra företaget från störningar i deras processer - *CIA*	
Cybermevetenhet/Mänsklig faktor i Cybersäkerhet	- Förmågan att kunna identifiera försök på attacker - Behandla data på ett säkert vis - Hur data delas internt inom företaget - Social manipulation - Mental hälsa och cybersäkerhet	Tech Accord (2021), Rohan et al. (2021), Mwangala et al. (2023), Flores et al. (2023), Workman (2007), Barber (2001), MSB (n.d), NCSC (2018), Hartfield (2017), Alotaibi et al (2024), Barney (2023), Puta (2022)
Betydelsen av träning inom cybersäkerhet	- Förmågan att kunna identifiera attacker - Kunna hantera data - Kunna anpassa sig efter att metoder för cyberattacker kontinuerligt utvecklas	Rohan et al. (2021), elev8 (n.d.)
Företagens strategi idag, som identifierat i litteraturen	- Kampanjer - Träning - Utbildning i form av föreläsningar	Chowdhury et al. (2022)
Problematiken kring företagens strategier	- Lågt engagemang bland anställda - Allokeringen av resurser - Ingen praktiskt exponering	Chowdhury et al. (2022), Tech Accord (2021), Mwangala (2021), Flores et al. (2023), Gross (2018), Aldawood och Skinner (2019)
Förslag på lösningar i litteraturen	- Förstå behoven av träning, bedömning - Forma träningen efter preferenser - Serious games, och annan praktisk träning,	Aldawood och Skinner (2019), Flores et al. (2023), Wilson och Hash (2003), Pattinson et al. (2018), Chowdhury et al. (2022), Corradini (2020), Barletta et al. (2023), Hodhod et al. (2023)
Tillämpade teorier	- *Personalized learning theory* - *Optimism bias och cybersäkerhet*	Morin (2020), Aue och Okon-Singer (2020), Alnifie

	- *Praktiskt inlärning* - *Teoretisk grund för serious games*	och Kim (2023), Main (2023), Krath et al. (2021)

Tabell 2.1: Sammanställning av litteratur

3. Metod

Följande avsnitt av arbetet beskriver de tillvägagångssätt som har använts för att samla in data för att undersöka forskningsfrågan. Tillvägagångssättet för att utforma den kvantitativa metoden beskrivs under detta avsnitt samt eventuella hinder som har mötts under insamlingen av data och hur arbetet har genomförts för att arbeta runt dessa hinder.

3.1 Val av metod

För att kunna få någon form av mått samt en djupare förståelse, den utsträckning att det är möjligt att nå ut till fler personer, för hur utbildningen för cybersäkerhet idag ser ut bland medelstora och stora företag, är den valda metoden för denna forskningen kvantitativ, i form av en enkät. För att förtydliga den drivande faktorn för valet av denna metod, är det av värde att klargöra att fokuset kommer främst att ligga den anställdes syn på det hela. För att vidare kunna komplettera de givna svaren av respondenten och bilda en bredare förståelse baserat på de svaren som respondenten ger, kommer även enkäten att ha en viss grad av ett *kvalitativt* instick, i den mån att respondenten kommer kunna ha möjligheten att vidareutveckla sitt svar på några av frågorna som presenteras i enkäten.

Valet av metod för studien går i linje med vad Oates (2006) skriver. Enligt Oates (2006) kan en använda sig av enkät för att kunna samla in samma sorts data från en större grupp av människor. Detta är något som Oates (2006) vidare resonerar kring att eftersom det är en större grupp människor som undersökt när denna metod används, kan en också använda denna data för att presentera en något mer generaliserad slutsats. Fortsättningsvis skriver Oates (2006) att, när en enkät genomförs, kan en leta efter ett mönster baserat på de svaren hämtade från enkäten. Med hänvisning till Oates (2006), är denna typ av metod för att samla data något som är vanligt inom området av *IS* för att kunna undersöka olika synvinklar kring olika områden inom *IS*.

3.2 Enkätutförande

För att adressera en nackdel, diskuterat av DeFranzo (n.d.) med enkäter som handlar om att det inte är möjligt för författaren att beskriva kontexten för de olika frågorna för respondenten, men också för att kunna undersöka forskningsfrågan på ett mer strukturerat vis delades enkäten upp i tre kategorier, i enlighet med de tre delarna som har beskrivits i *syftet* av arbetet. Var fråga i de tre kategorierna som enkäten bygger på, har sin grund i den presenterade litteraturen kring forskningsfrågan, men även forskningsfrågan som helhet.

För att underlätta de olika delar av genomförandet av enkäten, att utforma enkäten och att samla in svar, användes *Google Forms* som plattform. *Google Forms* låter en skicka ut enkäten på ett smidigt vis, men bidrar också till en smidigare insamling av data genom att plattformen låter en att öppna den färdiga enkäten i *Google Sheets,* där en kan skapa diagram för att presentera det slutgiliga resultatet av enkäte.

I mån av att nå ut till respondenter för att besvara frågorna i enkäten, har sociala medier använts. Under författandet av arbetet, för att vidare nå ut till fler personer att svara på enkäten och för att bygga ett bredare resultat i arbetet, kontaktades även personer i författarens egna kontaktnät genomgående med förhoppningen att de hade kunnat svara, men även för att dela vidare enkäten inom deras egna kontaktnät som är en del av urvalsgruppen.

3.3 Sammanställning av data hämtat från enkät

Enkäten som användes för att samla data för denna undersökning genomfördes via *Google Forms.* Google Forms är en gratis plattform som kan användas för att skapa och dela enkäter. Eftersom *Google Drive* inkluderar både *Google Forms* och *Google Sheets,* kan en öppna diagram som innehåller alla svar på enkäten, från *Google Forms,* i *Google Sheets* för att sedan göra justeringar om det önskas och kopiera diagrammet för att placera i arbetet.

Inkluderat i enkäten, fanns det även en möjlighet för respondenten att kunna vidareutveckla och motivera sina svar som de angav på frågor som krävde vidare motivering för att få en djupare förståelse för deras svar. Svaren som angavs i detta format, sammanfattades sedan och placerades i ett cirkeldiagram.

En del av svaren som angavs av respondenterna var något längre, eftersom dessa svar var något längre kunde inte en läsa ut hela svaret när de placerades i ett cirkeldiagram. För att inkludera de längre svaren, trots att de inte kan visas i ett cirkeldiagram, placeras dessa svaren i en tabell och en notering kommer att göras för att, trots att svaren är längre, kunna få en överblick av resultatet i procentsats som resterande av svaren.

3.4 Pilot-enkät

För att adressera den presenterade kritiken av enkäter, att en inte kan vidare förklara frågorna för respondenten vid behov, som presenterat av DeFranzo (n.d.), men även för att säkerställa att enkäten i fråga uppfyller de krav som hade satts upp, i form av resultatet och att det finns tillräckligt med information i enkäten för att respondenten ska kunna förstå kontexten av frågorna som ställdes, genomfördes ett test av enkäten med en person som arbetar inom IT-sektorn. Efter detta test av enkäten gjordes, gjordes en tydlig analys av de givna svaren av respondenten och eventuella problemområden som uppstod när respondenten utförde enkäten korrigerades.

3.4.1 Ändringar i enkäten efter pilot-enkäten

Målet med pilot-enkäten som gjordes innan enkäten skickades ut via de olika sociala medier som användes var att säkerställa att enkäten var tydlig i sitt språk och i dess uppbyggnad och efterhand som pilot-enkäten genomfördes, skulle ändringar göras i enlighet med kommentarer som presenteras av individen som genomförde pilot-enkäten. Hursomhelst, individen som

genomförde pilot-enkäten ansåg att enkäten var tydlig i sitt språk och uppbyggnad och av den anledningen gjordes inga ändringar.

3.5 Insamling av litteratur

En insamling av litteratur har gjorts i samband med detta arbete för att bilda en djupare förståelse, men även för att identifiera vilka luckor det finns för att vidare undersöka, i form av problem kring ämnet baserat på den tidigare forskning som har gjorts. De två primära plattformarna som har använts för att söka efter litteratur kring detta ämne är *Google Scholar* och *LUBSearch.*

Ett antal nyckelord, men även fraser, har använts genomgående i sökningen av litteratur kring ämnet, bland annat;

- *Human factor in cybersecurity*
- *Serious Games and cybersecurity*
- *Training in cybersecurity*
- *Employee Awareness in Cybersecurity*
- *Social Engineering + Cybersecurity*
- *Practical Exposure in Cybersecurity*

Under insamlingen av litteratur har det varit som mål att hitta litteratur som har publicerats under tidsintervallet fem till tio år. Detta är främst för att den genomförda undersökningen ska kunna spegla hur situationen är inom ämnet idag. För att dagens situation i områden ska kunna speglas i arbetet, har det varit av värde att samla in litteratur som även diskuterar den senaste forskningen och de senaste framstegen som har gjorts för att vidare förstå den mänskliga faktorn i cybersäkerhet och hur företagen arbetar mot dessa. Det är, huruvida, av värde att notera att begränsa sig till ett visst tidsintervall är något som inte är möjligt. Av den anledningen har även en rad äldre litteratur använts i arbetet för att vidare bygga upp en förståelse för olika koncept som har varit relevanta till den diskuterade frågeställningen.

För att vidare bygga upp litteraturgenomgången, har det varit av stor betydelse för författaren att under letandet av relevant litteratur för ämnet, har litteraturgenomgången byggts vidare med hjälp av att gå igenom litteraturen som andra relevanta arbeten har refererat till. Denna process är något som har bidragit till en något mer effektiv sökning efter litteratur, men det är också något som har bidragit till att mer relevant litteratur till ämnet har hittats.

3.6 Urval av respondenter

Grunden till undersökningen som gjordes för detta arbete var att vända sig till medelstora och stora företag för att delta i en enkät. Fortsättningsvis, täcker även undersökning ett brett åldersspann, 18-65, för att kunna samla in en bredare spektrum av åsikter kring det ämne som undersöks, men även hur utbildningen kan utvecklas för att inkludera praktisk träning, hur de anser att individens egna preferenser hade påverkat utbildning samt om de anser att de har kunnat tillämpa vad som har presenterats under utbildningstillfällena kring deras egna arbetsuppgifter.

Följande definition följdes vid insamling av respondenter som arbetar på medelstora och stora företag i Sverige:

Presenterat av EUR-Lex (n.d); Ett medelstort företag definieras av ett de har färre än 250 anställda samt att företaget ska ha en årsomsättning som inte överstiger €40 miljoner eller en balansomslutning som inte överskrider €27 miljoner.

Wagman (2022) definierar ett *stort företag* i Sverige som ett företag med över 250 anställda.

3.7 Validitet och reliabilitet

Validitet, å ena sidan, handlar om, som Recker (2013) beskriver det, den insamlade datan undersöker det som är presenterat att arbetet ska undersöka. Oates (2006) skriver att för att kunna säkerställa validitet i enkäten som utförs, ska en säkerställa att enkäten kan generera data om det ämne och koncept som en undersöker. Ämnet som undersöks i detta arbete handlar om hur utbildningen för cybersäkerhet ser ut bland medelstora och stora företag. För att kunna säkerställa, men även för att arbeta mot att förbättra, validiteten i enkäten som gavs ut till respondenterna, läggs fokus i en högre grad på att undersöka frågor som är direkt kopplade till frågeställningen i sig, men även på att lägga fokus på närliggande områden till frågeställningen. Detta är något som går i linje med vad Oates (2006) beskriver, för att kunna säkerställa validiteten i en enkät som, till exempel, undersöker nöjdheten hos kunder, skall enkäten även inkludera områden som är närliggande till detta, för att undersöka ämnet som helhet. För att kunna tillämpa samma princip i denna undersökning, har fokus i enkäten även lagts på att ge respondenten en chans att kunna besvara frågor i stil med om de anser att utbildningen har haft en positiv effekt, i den mån att de har kunna tillämpa det som har presenterats under utbildningen i sina egna arbetsuppgifter, men även om utbildningen har inkluderat någon form av *praktisk* träning samt om de har själva kunna förmedla deras egna preferenser av utformningen av träningen.

Reliabilitet, å andra sidan, som Oates (2006) beskriver det, uppmärksammar om en enkät hade kunnat generera liknande data, i form av svar och åsikter från respondenterna, om det hade utförts igen med samma respondenter. Detta är något som Oates (2006) presenterar problematik kring och skriver att detta är något som är svårare att bedöma, i den mån att respondenten kan ändra sin åsikt kring ett ämne över tid. De kan minnas sina svar som de angav från förra gången de svarade på enkäten i fråga och repetera dessa svar samt att de kan medvetet svara något annat när de utför en enkät en andra gång. För att kontinuerligt arbeta mot, men även för att uppnå, en högre reliabilitet och för att respondenten inte ska behöva fundera efter vad det är som söks i en fråga har fokus lagts på att exemplifiera svårare termer som har använts i enkäten, till exempel “serious games”, men även genom använda ett enkelt språk genomgående i hela enkäten.

3.8 Etiska överväganden

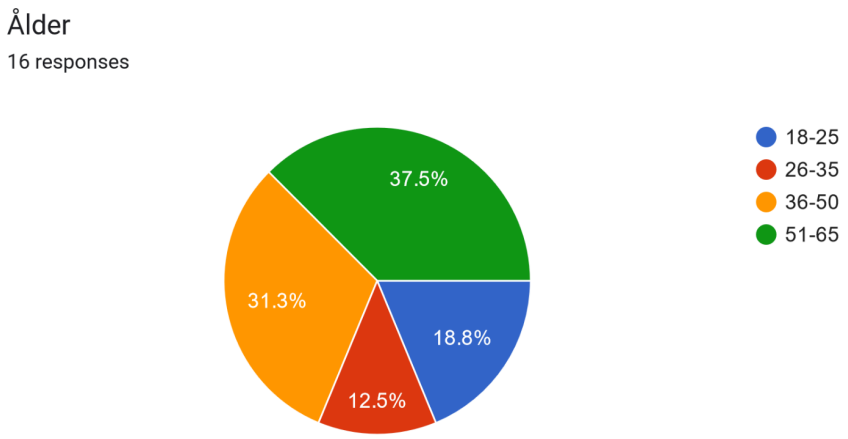
Enkäten som gjordes för detta arbete, följer de etiska överväganden som har presenterats av Fisher (2020). Genom att skriva en kort introduktion i början av enkäten, introduceras respondenten till enkätens syfte, men även hur datan som samlas från enkäten kommer att användas. I linje med vad Williams (2023) har skrivit, informeras även användaren att de är helt anonyma när de gör enkäten samt att de kan välja att avsluta och “dra sig ut” ur enkäten om de känner att de inte vill slutföra den.

4. Resultat

Följande avsnitt av arbetet presenterar de resultat som har hämtats från den kvantitativa undersökningen som genomfördes. För en tydligare representation av resultatet, följs samma logiska struktur som enkäten byggdes på. Det är endast svaren på frågorna som presenteras under detta avsnitt, frågorna som användes för enkäten finns att hitta under appendix.

4.1 Ålder och mänsklig faktor i cybersäkerhet

Den inledande frågan i enkäten handlar om respondentens ålder, detta frågan formar dels en introduktion för personerna som svarar på enkäten, men även en överblick över demografin respondenterna.. I enkäten presenterades respondenten med fyra olika alternativ som täcker fyra åldersintervaller. Det första valet som respondenten kunde välja var 18-25, det andra valet var 26-35, fortsättningsvis täcks åldersintervallet 36-50 och avslutningsvis 51-65. Av de som svarade på enkäten, svarade 37.5 % att de var 51-65, 31.3 % som svarade att de är 36-50 år. Bland de två sista svarsalternativen, svarade 18.8 % att de var mellan 18-25 år och 12.5 % svarade att de är 26-35 år gamla.

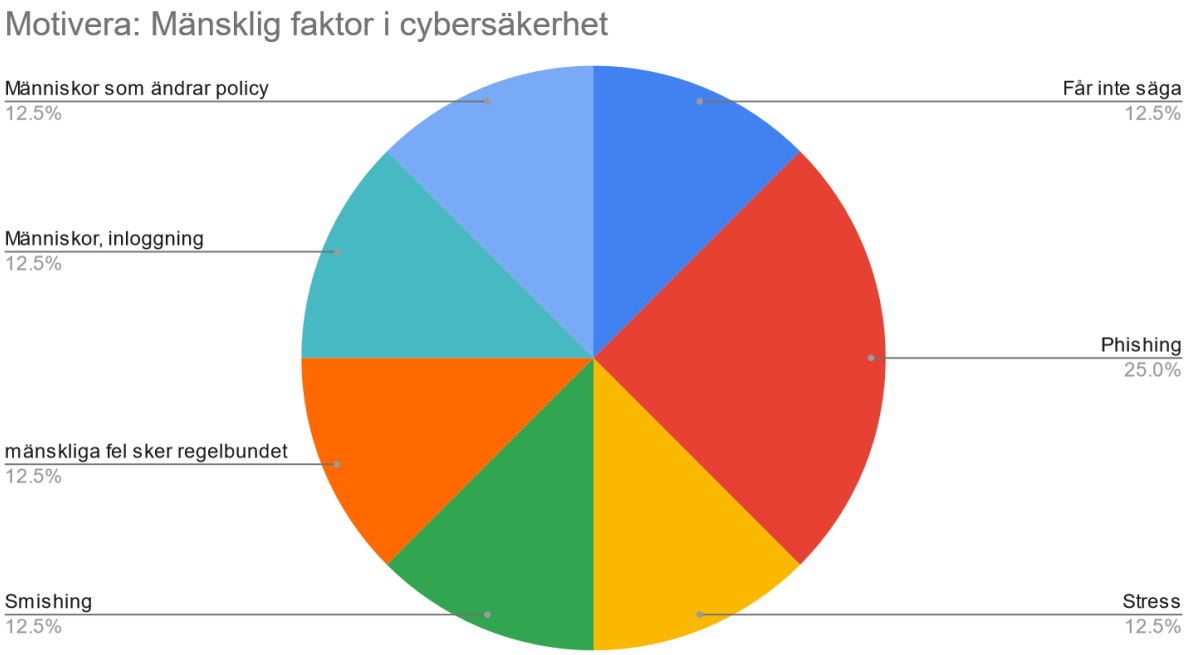


Figur 4.1.1: *Resultat för ålder*

För att bygga vidare på introduktionen för respondenterna till enkäten, men även för att vidare bygga på enkätens syfte i enkäten, handlar den andra frågan som presenterades i enkäten om respondenten själv varit med om en händelse där de har sett att företagets cybersäkerhet har påverkats som en direkt konsekvens av en mänsklig handling. Totalt var det sexton personer som svarade på enkäten, 75 % svarade ja på denna fråga.

***Figur 4.1.2**: Resultat för mänsklig handling i cybersäkerhet*

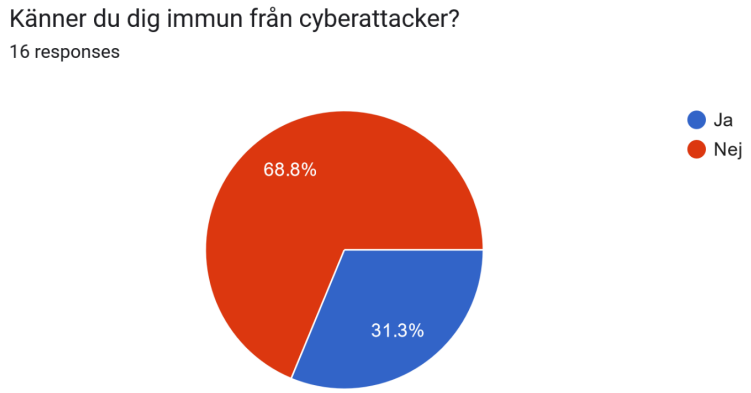
I mån av att vidare bygga vidare på respondentens svar på föregående fråga, hade respondenten möjlighet att, om de svarade ja på frågan, att vidareutveckla deras svar och genom detta förtydliga deras svar och bringa upp kontext till denna händelse.



***Figur 4.1.3**: Resultat på fråga som gav respondenten möjligheten att utveckla sitt svar*

4.2 Optimistisk bias och cybersäkerhet

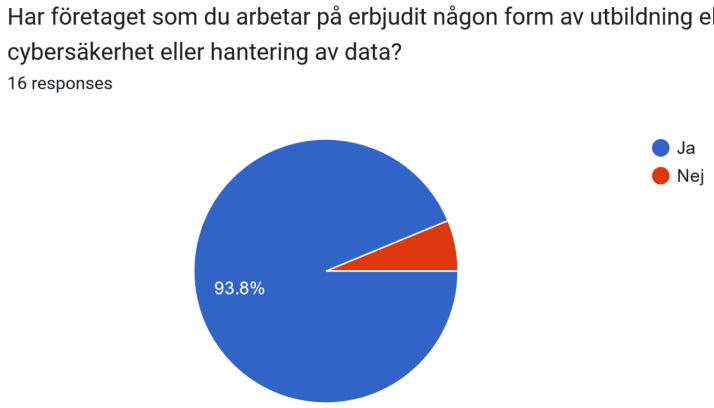
För att vidare bygga upp en förståelse för hur respondenterna tänker kring huruvida de anser att de känner sig immuna från cyberattacker, handlade den tredje frågan just om de känner sig immuna från cyberattacker. På denna fråga kunde respondenten välja bland två alternativ: ja *eller nej*. Av de som svarade på enkäten, svarade 68.8 % att de inte känner sig immuna från cyberattacker (nej) och 31.3 % svarade att de känner sig immuna från cyberattacker (ja).



***Figur 4.2.1**: Resultat för optimistisk bias*

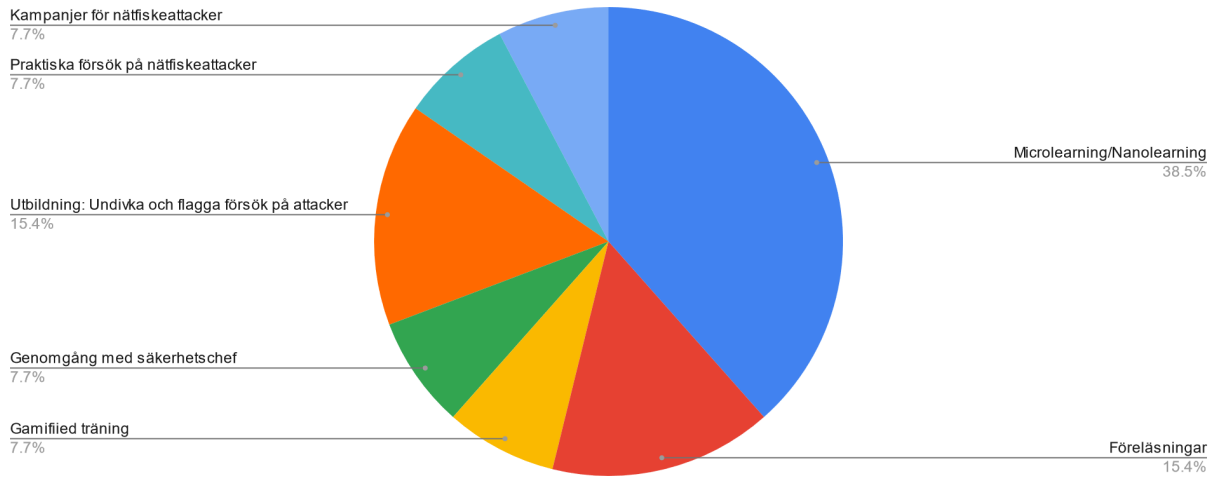
4.3 Träning inom cybersäkerhet

Fortsättningsvis, handlar nästa fråga om respondenten har, genom deras företag, fått någon form av träning som är relaterad till cybersäkerhet. Denna frågan presenteras för respondenten som en *ja* eller *nej*-fråga. På denna fråga, svarade 93.8 % att företaget som de arbetar på har erbjudit någon form av träning, eller utbildning, som är relaterat till cybersäkerhet, medan 6.2 % svarade att deras företag inte hade erbjudit någon form av träning eller utbildning relaterat till cybersäkerhet.



***Figur 4.3.1**: Resultat för utbildning för cybersäkerhet*

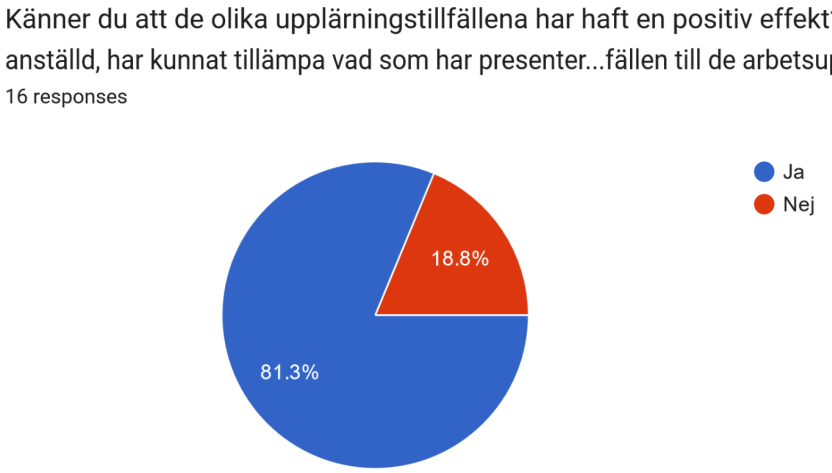
Om respondenten svarade ja på den föregående fråga, gavs respondenten möjligheten att, återigen, vidareutveckla deras svar om de har mottagit någon form av träning relaterat till cybersäkerhet och hur denna sett ut. För att göra resultatet tydligare, sammanfattades svaren och placerades i ett cirkeldiagram.



***Figur 4.3.2**: Sammanställning av respondenternas svar på den motiverande frågan*

För att förtydliga svar som kan verka otydliga i diagrammet ovan. Utbildningen som diskuterades bland respondenterna handlar om *hur* de anställda ska undvika samt hur de ska flagga försök på attacker. Vidare, handlar det praktiska försöket på nätfiskeattacker om att företagen skickade ett eget format försök på attacker som den anställda skulle arbeta utifrån.

För att respondenten ska ha ännu en möjlighet att vidareutveckla sina svar på de två föregående frågorna, handlar den följande frågan om de själva anser att träningen som de har genomgått har haft en positiv effekt, vilket respondenten har möjlighet att svara på genom att välja bland två alternativ, *ja* eller *nej*. En “positiv effekt” exemplifieras i denna frågan som att de anser att de har haft möjligheten att kunna implementera vad som har lärts ut under de olika utbildningstillfällena till de arbetsuppgifter som de arbetar med. 81.3 % svarade att de anser att utbildningen eller träningen som de har genomgått genom deras företag har haft en positiv effekt och 18.8 % svarade att träningen eller utbildningen inte har haft en positiv effekt.



***Figur 4.3.3**: Resultat om respondenten anser att utbildningen gett en positiv effekt*

4.4 *Serious Games* och praktiskt träning

För att bringa fokuset i enkäten mot *serious games*, men även annan typ av praktiskt träning, inkluderas en fråga som handlar om detta och frågar respondenten om *serious games* har varit en del av de utbildningstillfällena som de har deltagit på. På denna fråga svarade 37.5 % att *serious games* har varit en del av den träning som de har genomgått för cybersäkerhet (ja) och 62.5 % svarade att det inte har varit en del av den träning som de har genomgått för cybersäkerhet (nej).

***Figur 4.4.1**: Resultat på frågan som handlar om "serious games"*

För att vidare bringa fokus mot praktisk träning, presenteras respondenten med en ja eller nej fråga som handlar om respondenten har genomgått annan typ av praktisk träning, om de har svaret nej på att träningen har bestått av *serious games* som praktisk träning inom cybersäkerhet. På denna fråga svarade 87.5 % nej och 12.5 % svarade ja, att träningen har bestått av annan praktisk träning istället för *serious games*.

***Figur 4.4.2**: Resultat på frågan som handlar om hands-on-träning*

Om respondenten har deltagit i någon form av praktisk träning som en del av träningen som de har genomgått genom sina företag, hade de möjligheten att på denna fråga motivera huruvida de anser att den praktiska träningen har haft en positiv effekt. I mån om att svaren ska på ett tydligare vis presenteras, har svaren satts in i en tabell.

Respondent (R)	**Svar**
R1	ja absolut, spel har använts… där man får vara med och interagera med det man ska lära sig
R2	Ja, jag känner att jag har fått en ny upplevelse för hur jag kan agera i olika situationer, till exempel hur jag ska agera i nätfiskeattacker.
R3	Ja, man kan få ett bättre förståelse på hur man arbetar mot sånt
R4	Ja, det är roligt och det fastnar lättare.
R5	Kan hända
R6	Gamification av olika slag gör det mer interaktivt och för gemene man bättre förståelse

R7	Ja då vi behöver använda fler sinnen för att det ska fastna.

***Tabell 4.4.3**: Sammanställning av svar som handlar om praktisk träning och dess inverkan (om en har genomgått en sådan träning tidigare*

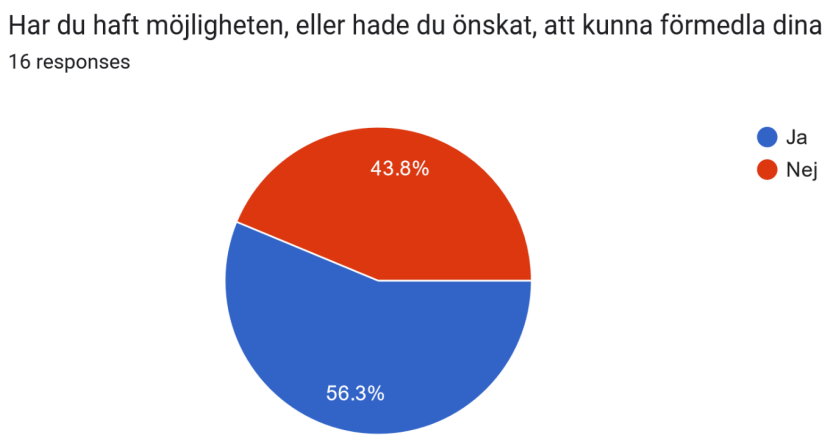
Avslutningsvis, för att ge ett fokus kring praktiskt träning, om deltagaren i enkäten inte har deltagit i någon form av praktisk träning tidigare, hade de möjlighet att motivera deras svar kring om de anser att praktisk träning kan ha en positiv effekt på inlärningsprocessen som helhet. Svaren som gavs av respondenterna på denna fråga var något längre än de svar som gavs på tidigare frågor där respondenten hade möjligheten att motivera sina svar, av den anledningen sattes de angivna svaren av respondenterna i en tabell, för att lättare kunna läsa ut och tolka svaren som gavs.

Respondent (R)	**Svar**
R1	Absolut, slutanvändare behöver i mitt tycke ha korta, informationsrikt innehåll och i kombination med spel lär man sig mer då vi stimuleras av det och inte blir less på en längre tråkig kurs
R2	Ja, som jag nämnde tänker jag att en kan få en ny förståelse för hur man ska agera i olika situationer, eftersom man har en chans att direkt få ett svar på om man har gjort rätt eller fler i en situation och vilka ändringar man kan göra därefter.
R3	Hade säkert varit najs men bolagen verkar inte villiga att betala mer än minsta möjliga till sina anställda men förväntar sig ett digitalt Fort Knox med fullt rationella och felfria arbetare
R4	Förmodligen
R5	Ja, beroende på om det är applicerbart på ens arbetsuppgifter.
R6	Ja, absolut. När en spelar får man reda på direkt vad man har gjort fel och en kan börja om om och om igen tills de klarar situationen som en har satts in i

***Tabell 4.4.4**: Sammanställning av svar som handlar om praktisk träning och dess inverkan (om en inte har genomgått sådan träning tidigare)*

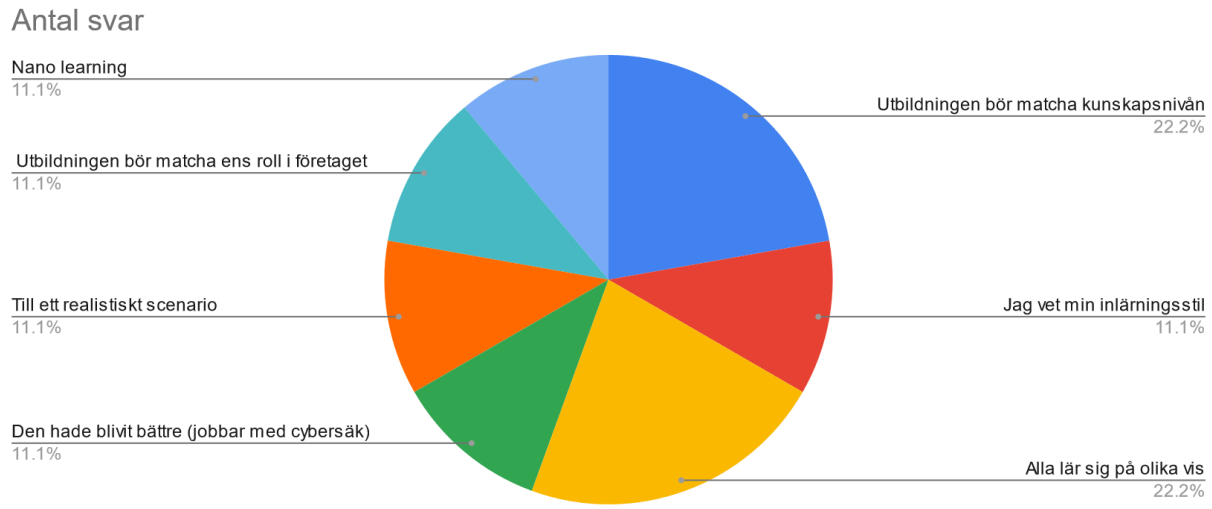
4.5 Användarens preferenser i träningen

Följande del av enkäten som gjordes för detta arbete handlar om *förmedling av preferenser i utbildningen.* Den inledande frågan handlade om huruvida respondenten har haft möjligheten att förmedla sina egna preferenser, eller hade önskat att förmedla sina egna preferenser inför träningen. På denna frågan svarade 56.3 % ja, medan 43.8 % svarade nej.



***Figur 4.5.1**: Resultat som handlar om preferenser i träningen*

För att vidare undersöka frågan, hade respondenten möjligheten att resonera kring hur de anser att kunna förmedla sina egna preferenser som en del av utbildningen hade påverkat utbildningen. Eftersom svaren på denna frågan var något längre och ett antal svar “höll med varandra” varandra, sammanställdes alla svar i ett cirkeldiagram.



***Figur 4.5.2**: Sammanställning av svar som handlar om preferenser i träningen och dess inverkan*

Antal svar;	Svar
1	Gav positiv återkoppling kring Nanolearning och det tillsammans med att de andra på bolaget också såg det som positivt över långa utbildningstillfällen så beslutades det att fortsätta med det formatet. Man får en konstant påminnelse om att tänka på säkerhet.

***Tabell 4.5.1**: Ett längre svar som angavs av en respondent*

Eftersom detta är ett längre svar, är det bättre anpassat att placera detta svaret i en tabell för att kunna läsa ut hela svaret, för att svaret ska kunna inkluderas i diagrammet ovan, kommer detta svar att noteras med "nano learning".

5. Diskussion

I följande avsnitt presenteras och diskuteras eventuella skillnader mellan de svar som har angivits av respondenterna som deltog i enkäten för detta arbete. Dessutom kommer eventuella likheter och skillnader mellan det presenterade resultatet och litteraturgenomgången att redogöras för.

5.1 Mänsklig faktor i cybersäkerhet

Den inledande frågan i enkäten handlade om respondenten har upplevt att företaget som de arbetar på har utsatts för en cybersäkerhetsrisk som en direkt konsekvens av en mänsklig

handling. Av de som deltog i enkäten, svarade 75 % (***Figur 4.1.2)*** att de har upplevt en cybersäkerhetsrisk som en direkt konsekvens av en mänsklig handling i deras företag. Detta är en siffra som kan jämföras med siffran som presenterades av Tech Accord (2021), som visade att 95 % av alla cyberattacker som inkluderades i deras studie var en direkt konsekvens av en mänsklig handling. Trots att den siffran som är hämtad från enkäten visar en fortsatt hög siffra när det kommer till den mänskliga faktorn som en risk i cybersäkerhet, kan en dra slutatsen att resultatet som hämtades som ett resultat från enkäten som genomfördes, visar en något mer positiv siffra i jämförelse med den ursprungliga siffran som presenterades av Tech Accord (2021), en siffra som tyder på att den mänskliga faktorn i cybersäkerhet till viss grad är avtagande. Det är vidare av värde att notera att denna siffran endast visar de cybersäkerhetsrisker som respondenterna själva har observerat. Det är möjligt att siffran hade sett något annorlunda ut om företagen hade studerats individuellt. I mån om att studera individuella fall, kan det också vara så att de som svarade på denna fråga och menade på att det har skett en cybersäkerhetsrisk som en direkt konsekvens av en mänsklig handling arbetar på samma företag eller rapporterar i enkäten om ett gemensamt fall, istället för enskilda fall som diskuterades av Tech Accord (2021).

Följdfrågan till den föregående frågan lade stor vikt vid om individen kunde motivera sitt svar kring hur en mänsklig faktor har resulterat i att företaget har drabbats av en cybersäkerhetsrisk. De främsta anledningarna som togs upp bland respondenterna var att anställda, men även chefer inom ett företag (***Figur 4.1.3)***, tryckte på vad som beskrevs som “uppenbara phishing-länkar”. En av respondenterna beskrev att cyberattacken bestod av en “smishing”-attack (***Figur 4.1.3)***, IBM (n.d.) skriver att *smishing* är likt en nätfiskeattack i den mån att en luras att trycka på en länk, men vad som skiljer “smishing” från en nätfiske är att offret, genom denna länk, luras till att ladda ner en applikation på sin enhet som innehåller skadlig programvara. I litteraturgenomgången, men även under arbetets gång har det hänvisats till statistiken som har presenterats av Tech Accord (2021), som presenterade att 95 % alla cyberattacker är ett direkt resultat av en mänsklig handling, Tech Accord (2021) beskrev en “mänsklig handling” som att individer fallerar att identifiera ett försök på nätfiske, eller dylikt, och det är något som också har visats bland de svar som har getts av respondenterna i enkäten, som speglar resultat på denna statistik, att anställda på olika nivåer misslyckas med att identifiera försök på nätfiske, vilket kan resultera i en cyberattack, vilket diskuteras bland respondenterna på denna fråga. Den mänskliga handlingen i cybersäkerhet är ett brett ämne, men de svar som gavs från respondenterna i enkäten har en direkt korrelation med de exempel som togs upp av Tech Accord (2021), att individer på olika nivåer i ett företag inte har de färdigheter som krävs för att kunna identifiera ett försök på en nätfiskeattack.

I litteraturgenomgången noterades det av Puta (2022) att den mänskliga handlingen i cybersäkerhet inte behöver vara ett direkt resultat av att individen saknar kunskap och färdigheter för att kunna identifiera ett försök på nätfiske, eller liknande attack, utan det kan även handla om stress. Detta är något som även speglas i ett av svaren som gavs av en av respondenterna i enkäten, som menade att stress var den bidragande faktorn till att individen blev ett offer för en cyberattack (***Figur 4.1.3)***. Puta (2022) diskuterade att när någon är stressad, som var ett exempel som togs upp i litteraturen, kan detta ha en inverkan på hur individen hanterar information och kan i flera fall glömma den träning som en har gått igenom för att kunna identifiera olika typer av försök på attacker. Det svar som denna respondenten angav gav även en inblick i hur detta kan se ut i praktiken, och inte bara i teorin som har presenterats i litteraturgenomgången.

I litteraturgenomgången diskuterades främst att den mänskliga faktorn i cybersäkerhet handlar om att människan fallerar att kunna identifiera ett försök på en cyberattack, antingen eftersom de är stressade eller eftersom de saknar kunskapen kring det ämnet, men som ett svar på frågan i enkäten menade en av respondenterna att det också handlar om att människan ändrar eller bryter policys och gör andra val relaterat till företagets cybersäkerhet (***Figur 4.1.3)***. Detta är något som vidare beskrevs av respondenten, att detta öppnar hål i företagets säkerhet, vilket kan resultera i att en tredje part hittar en "väg in" genom de säkerhetshål som har skapats.

5.1.1 Optimism bias och cybersäkerhet

Vidare har det visats i litteraturgenomgången, med hänvisning till Alnifie och Kim (2023) , att *optimistisk bias* kan ha en inverkan på hur datan hanteras av individer och hur individen agerar när de ställs inför, bland annat, ett försök på en cyberattack. *Optimistisk bias* handlar om, i enlighet med Aue och Okon-Singer (2015), att en kan antingen överskatta, eller underskatta, sannolikheten för att individen ska vara med om en viss händelse. Detta har en inverkan på cybersäkerhet i den mån att individer, som ett resultat av *optimistisk bias,* har bildat sig tanken att de är *immuna* mot cyberattacker. Detta fenom som har beskrivits av Alnifie och Kim (2023), är något som vidare diskuterats av Mwangala et al. (2023), Mwangala et al. (2023) visade att 75.8% av deltagarna som var deltog i studien som genomfördes menade att de var säkra från cyberattacker. Enkäten som gjordes för detta arbete visar en något positivare siffra, i jämförelse med siffran Mwangala et al. (2023) presenterade. I enkäten för detta arbete menade 68.8 % (***Figur 4.2.1)*** att de inte känner sig immuna från cyberattacker av olika slag. Detta är en siffra som talar för en något bredare förståelse för cybersäkerhet och dess risker, i den mån att det är fler som känner att de inte är immuna mot en cyberattack, att liksom som att det kan ske för någon annan att de faller offer, eller försök till en attack, kan detta ske för en själv. Den positiva signaler för att de som svarade på enkäten har en bredare förståelse för cybersäkerhet och dess risker, är något som talar positivt för den utbildning, som är den främsta strategin som används av företagen som har identifierats i litteraturgenomgången för att ge mer kunskap kring cybersäkerhet, som de har genomgått genom deras företag för cybersäkerhet i den utsträckning att 81.3 % av de som svarade anser att de har kunnat tillämpa vad som har lärts ut under utbildningstillfällena i de arbetsuppgifter som de utför.

5.2 Utbildning för cybersäkerhet

Utgångspunkten för forskningsfrågan ligger i att undersöka hur medelstora och stora företag designar sina utbildningsprogram för cybersäkerhet, av den anledningen söktes endast personer som arbetar på företag av denna omfattning för denna enkät. Av det totala antalet personer som svarade på enkäten, svarade 93.8 % att de hade genomgått någon form av utbildning inom cybersäkerhet genom det företag som de arbetade på (***Figur 4.3.1)***. Träning och utbildning i dess olika former, har visats i litteraturgenomgången som en av de främsta lösningarna som företagen kan använda sig av för att bringa mer fokus på den mänskliga faktorn i cybersäkerhet och förbättra den anställdes förmåga att kunna identifiera olika typer av försök på cyberattacker samt hur personen skall agera i denna situation.
Vidare finns det en viss kritik som har presenterats i litteraturgenomgången kring utbildningen för cybersäkerhet som lägger fokus på att utbildningen som ges inom företagen inte är effektiv, i den mån att anställda, trots att de har deltagit på utbildningar, återgår till att hantera data på ett "ohygieniskt vis" när de genomför sina arbetsuppgifter, som beskrivet av Mwangala et al (2021).

För att vidare undersöka denna kritik och för att undersöka bland respondenterna om de anser att de har kunnat tillämpa vad som har lärts ut under utbildningstillfällen, lades mer fokus i den nästkommande frågan på den anställdes attityd mot den utbildning som har getts. Frågan som inkluderas i enkäten handlade om de anser att utbildningen som de har gått på har haft en positiv effekt, i den mån att de anser att de har kunnat tillämpa vad som har gåtts igenom på utbildningstillfället i sina egna arbetsuppgifter. Bland de som svarade, menade 81,8 % av respondenterna att utbildningen har gett en positiv effekt på hur de utför sina arbetsuppgifter (***Figur 4.3.3)***. Det resultat på denna enkät är något som sedan kan jämföras med resultatet som hämtades från Mwangala et al (2021), ett resultat som har använts som bas för denna frågan. Mwangala et al (2021) visade att en större andel inte tillämpade det som lärdes ut under utbildningen, medan en större majoritet av respondenterna på denna enkät anser att de har kunnat tillämpa det som har lärts ut under utbildningarna i sina arbetsuppgifter. Hursomhelst, detta är endast en siffra som har visats utan vidare motivering från båda sidorna som kan förklara den övervägande skillnaden mellan de två resultaten. Det är något som bland annat kan ha sin bas i hur utbildningen är formad eller i frekvensen som deltagarna från vadre sidor deltog på utbildningen, Mwangala et al (2021) diskuterade att en större majoritet av deltagarna deltog endast en gång på utbildningsmomenten och motiverade vidare att utbildningen behöver ske flera gånger per år för att utbildningen ska vara effektiv, men en bas för att förstå frekvensen som respondenterna deltog i utbildningen har inte satts i författandet av detta arbete. En av respondenterna på enkäten som genomfördes för detta arbete skrev att företaget som de arbetade på erbjöd *nanolearning* “några gånger per månad”, men detta är inte tillräckligt för att sätta som bas för hela arbetet.

För att vidare kunna få en djupare förståelse för hur utbildningen ser ut i de företagen som respondenterna arbetar för ställdes en fråga i enkäten som bad respondenten att förklara kort hur utbildningen kring cybersäkerhet har sett ut, det noterades i frågan att endast svara på denna fråga om de har genomgått någon form av utbildning. Inledningsvis av arbetet presenterades det av Chowdhury et al. (2022) att företag använder sig främst av kampanjer och intern utbildning för att ge uppmärksamhet kring cybersäkerhet, men även olika typer av träningsprogram för att utbilda sina anställda. Ett flertal svar från respondenterna var i linje med vad Chowdhury et al. (2022) beskrev, i den mån att de svarade att företaget som de arbetade på använde sig av kampanjer och annan relativt teori-tung utbildning, genom att de hade föreläsningar i samlingssal samt webbaserade utbildning med klipp som går igenom hur de ska kunna identifiera försök på cyberattacker och hur de ska hantera data på ett mer säkert vis (***Figur 4.3.2)***.

En del av svaren som gavs skapade en viss skillnad mellan de olika svaren i den utsträckning att en rad av respondenterna menade att företagen som de arbetar på har tillämpat ett något mer praktiskt tillvägagångssätt för utbildningen inom cybersäkerhet. Ett mer praktiskt tillvägagångssätt har visat i företagens tillvägagångssätt för utbildningen till den utsträckning att företagen använder sig av falska försök, som har formats av företagen själva, på nätfiske, som sedan låter individen själv att agera på egen hand (***Figur 4.3.2)***. Något som vidare talar för att företagen har använt sig av ett mer praktiskt tillvägagångssätt som en del av utbildningen, är att 37.5% av de som svarade, svarade att *serious games* har varit en del av utbildningen (***Figur 4.4.1)***.

Något som presenterades av respondenterna, som inte har tidigare diskuterats i litteraturen som har använts under författandet av detta arbete, är att ett flertal respondenter svarade att företagen

har använt *nanolearning* som en strategi för utbildning för cybersäkerhet. *Nanolearning,* eller *microlearning* som är samma sak (***Figur 4.3.2),*** skriver Junglemap (n.d) är en utbildningsstrategi som främst bygger på upprepning, förstärkning och reflektion.

Nanolearning, som beskrevs som en metod som användes bland företagen (***Figur 4.3.2)***, bygger på, bland annat, repetition. Respondenten motiverade vidare att denna utbildning genomfördes några gånger per månad. Hur utbildningen är uppbyggd och hur det genomfördes av företaget, är något som är i enligheten med litteraturen som presenterades av Mwangala et al. (2023) som skriver att för att utbildningen ska vara effektiv, måste detta ske flera gånger per år, och i detta fallet har respondenten beskriver att företaget erbjuder denna typ av utbildning några gånger i månaden.

5.3 Praktiska moment som en del av träningen

I litteraturgenomgången har det diskuterats en viss framgång i användningen av spel, i form av *serious games,* som en del av träningen för cybersäkerhet. *Serious games*, som en del av träningen, placerar användaren i ett förbestämt scenario och låter sedan användaren lösa problem på egen hand för att ta sig ur den situation som de har placerats i. I litteraturgenomgången diskuterades hur detta kan användas som en del av träningen och har visats av Corradini (2020) och Barletta et al. (2023) att denna typ av träning har resulterat i ett förbättrat engagemang, men även inlärning, hos deltagarna. Trots att det beskrivs i litteraturen som en metod som är relativt ny som har visat en viss framgång, svarade 37.5 % av de som deltog i enkäten att *serious games* har varit en del av träningen (***Figur 4.4.1)***. Svaret som gavs av respondenterna i denna enkät, visar en positiv bild av hur en, som det beskrivs i litteraturen, relativt ny teknologi har börjat tillämpas och användas av allt fler företag på en större skala som en del av deras träning för cybersäkerhet.

För att bygga vidare, för att få en förståelse för vilken typ av praktisk träning som har inkluderats som har implementerats bland företaget, handlade följande fråga om att respondenten hade möjligheten att svara ja eller nej huruvida de har genomgått någon annan praktisk träning som en del av undervisningen, vilket endast 12.5 % av de som svarade menade på att de har och 87.5 % menade på att utbildningen inte har byggt på några andra typer av praktiska moment (***Figur 4.4.2)***. Något som denna fråga saknade var en möjlighet för respondenten att vidareutveckla vilka typer av praktiska moment som har använts under utbildningen, men från ett tidigare svar kan informationen hämtas att annan typ av praktisk träning har bland annat handlat om försök till nätfiskeattacker som deltagaren i utbildningen ska arbeta utifrån för att identifiera och flagga. I svaret som respondenten angav motiverades inte vidare om detta är en typ av träning som sker internt i företag eller om företag använder sig av ett externt företag för att erbjuda denna typ av träningen som är baserad på en *simulation,* men i litteraturgenomgången noterades det att *Microsoft* erbjuder en sådan träning som fokuserar på att en ska utgå från ett påhittad försök av nätfiske som en del av deras *Attack simulation training - A phishing risk-reduction tool*-träning.

Som en fortsättning på föregående fråga, om *serious games* har använts som en del av träningen, ställdes frågan om respondenten kunde vidare motivera om de anser att användningen av *serious games* hade en positiv effekt på inlärningsprocessen. Det mönster som kunde skapas genom att följa motiveringarna som respondenterna gav på denna fråga, visar en tydlig positiv attityd bland respondenterna för användningen av *serious games* som en del av upplärningen av cybersäkerhet.

En av respondenterna menar att denna metod är något som kan vara användbart som en del av träningen för cybersäkerhet eftersom en får en chans att uppleva hur en kan, men även bör, agera i olika situationer, till exempel i en nätfiskeattack **(*Tabell 4.4.3)***. Fortsättningsvis, nämndes det av en av respondenterna att genom användningen av *serious games* blir upplevelsen mer interaktiv och därav blir det lättare för individen att plocka upp vad som lärs ut och det blir något som lättare fastnar hos användaren **(*Tabell 4.4.3)***. Motiveringen som respondenterna gav i denna fråga går i linje med den presenterade litteraturen av Main (2023), som skriver att genom att individen sätts i en praktiskt moment, kan personen bilda en djupare förståelse för det ämne, eller den färdighet, som lärs ut. Att sådan typ av träning som gör träningen mer interaktiv, är likt vad Main (2023) beskriver i den mån att individen får göra sina egna beslut för att lösa det problem som de ställs inför, respondenterna är vidare i samförstånd med vad som har presenterats i litteraturen i den mån att de säger att en får en bättre förståelse för ämnet genom denna typ av träning. Avslutningsvis, diskuterades det av en av respondenterna, som en fördel av praktisk träning, att denna metod fungerar eftersom den bygger på att en använder flera sinnen samtidigt. Vad denna respondent diskuterar i denna fråga, är något som visar en direkt korrelation med vad Main (2023) skriver om hur, genom att praktiska moment låter en att använda flera sinnen samtidigt, kan leda till ökad inlärning om det ämne som behandlas i upplärningsmomentet.

Ålder var även en variabel som undersöktes i enkäten. Respondenten hade fyra alternativ: *18-25, 26-35, 36-50* samt 51-65. Genom att följa svaren som gavs på denna fråga, kan en dra slutsatsen att det var en något äldre demografi som deltog i denna enkät, det var 37.5 % som svarade att det var mellan 51-65 år gamla **(*Figur 4.1.1)***. Av de som svarade visades en övervägande positiv attityd kring användningen av *serious games* och annan typ av praktisk träning som en del av utbildningen för cybersäkerhet. I litteraturen diskuterades det av Flores et al. (2023) att det främst var yngre, och individer som arbetar på en ingångsnivå på ett företag, som visade en positiv attityd mot *serious games* som en del av utbildningen. Det resultat som hämtades från enkäten talar något emot vad som har presenterats i litteraturen i den mån att i enkäten har slutsatsen kunnat dras att respondenter i alla åldrar har visat på en positiv attityd mot användningen av *serious games* som en del av träningen. Det är, huruvida, av värde att notera att denna fråga som var i enkäten kan vara något missvisande i den mån att frågan lägger fokus på både *serious games* och annan typ av praktisk träning och av den anledningen kan en inte dra slutsatsen att respondenten svar lägger betoning på spel eller på annan praktiskt träning. Ett antal respondenter, när de har haft möjligheten, har, hursomhelst, noterat att “gamification” låter en att få en bättre förståelse för vad som lärs ut och att det låter en integrera med vad som lärs ut, men trots att detta är två svar som talar direkt för en positiv attityd mot *serious games* är detta inte tillräckligt för att jämföra de två resultaten, från Flores et al. (2023) och denna enkät, direkt med varandra. Fortsättningsvis, inkluderades det inte en fråga i enkäten som handlade om vilken roll respondenten arbeta med på företaget som de arbetar på, av den anledningen går det inte att jämföra attityden för *serious games* i ett utbildningssyfte bland de olika rollerna inom företaget, som det gjordes av Flores et al (2023).

Framgången för *serious games* som metod att använda sig av som träning för cybersäkerhet, men även andra områden, har visats av Mark Rober att ha sin grund i bland annat att när en spelar ett spel, i form av *serious games,* meddelar spelet användaren att de har gjort något fel och låter det att börja om från början. Vad Mark Rober noterade var att en större andel deltagare i experimentet som de genomförde började om från början om de fick ett meddelande som meddelade att börja om igen utan att de förlorade något, i form av poäng eller dylikt, om de började om från början.

Genom att börja om från början ett flertal gånger, beskrev Rober, att fler tillämpade vad de hade gjort fel i deras andra försök tills de till slut klarade "uppdraget" som de genomförde. Något som också var ett positivt tecken för användningen av *serious games* var att detta även var något som noterades av en av respondenterna av enkäten. Respondenten hade en positiv attityd för användningen av *serious games* eftersom "När en spelar [spel] får man reda på direkt vad man har gjort fel och en kan börja om och om igen tills de klarar situationen som en har satts i" **(*Tabell 4.4.4)***.

5.4 Förmedla ens egna preferenser

I litteraturgenomgången för detta arbete, hänvisades det till Pattinson et al. (2018) och Chowdhury et al. (2022) som diskuterade ett resultat som speglade en positiv ökningen i inlärningsprocessen, eller *ISA-score* som Pattinson et al. (2018) beskrev det, om individens preferenser var en inkluderade i den utbildning, eller träningen som ges. Det som diskuterades i litteraturen är vidare något som har sin grund i, vad Morin (2020) menar, att individer lär sig på olika vis och genom att anpassa sig till individens preferenser och inlärningsmetoder, kan detta resultera i att en lär sig ett ämne eller en färdighet snabbare och får en djupare förståelse för ämnet som diskuteras. Detta är något som även har speglats i de resultat som kan hämtas från enkäten som genomfördes, en av respondenterna diskuterade om användningen av *serious games* att "det är roligare och att det fastnar lättare" **(*Tabell 4.4.3)***. Trots att inte följdfrågor har kunnat ställas vad denna individen menar eftersom det är en kvantitativ metod som har använts, har detta svaret en direkt korrelation till litteraturen som har tagits upp, i den mån att *serious games* inte nödvändigtvis behöver vara en "bättre" metod som kan användas för träning, men det är något som kan användas eftersom det är något som en rad tycker gör träningen roligare och mer intressant att en kan sättas i ett fiktivt scenario som en ska arbeta utifrån.

En av respondenterna diskuterade att företaget som de arbetade på använde sig av *Nanolearning* som en träningsmetod för cybersäkerhet och att anställda på företaget hade möjligheten att själva förmedla om de önskade om företaget skulle fortsätta med denna metod **(*Tabell 4.5.1)***. Det tillvägagångssätt som detta företaget valt att använda sig av, visar hur de teoretiska delarna som Pattinson (2018) och Chowdhury et al. (2022) diskuterar hur utbildning bör tillämpas efter individernas preferenser för en ökad inlärning hos deltagarna i utbildningen, kan se ut i praktiken.

Morin (2020) diskuterade vidare, i samband med att alla lär sig på olika vis, att alla besitter olika mycket kunskap om ett visst ämne och att detta även kan vara en grund för att vidare lägga fokus på att anpassa utbildningen efter den färdighet som en redan besitter kring ett ämne, detta är för att den utbildning som ges ska vara givande för alla deltagare. I mån om att inkludera en sådan del i enkäten som gavs ut, var det en fråga som handlade om respondenten själv haft möjligheten att förmedla sina preferenser, eller hade önskat att förmedla sina egna preferenser, på denna fråga svarade 56.3% ja, att de antingen har fått möjligheten, eller hade önskat, att kunna förmedla sina egna preferenser **(*Figur 4.5.1)***. Vidare hade respondenten möjlighet att utveckla sitt svar baserat på den föregående frågan. En respondent menade att de tror att utbildningen hade blivit bättre om "de hade varit bättre anpassat utifrån min kunskapsnivå" **(*Figur 4.5.2)***, medan en annan respondent resonerade att utbildningen bör ske på olika nivåer baserat på kompetensen hos en individ, respondenten menar också att det hade varit "löjligt" att placera en penetrationstestare som har en djupare förståelse för ämnet på en sådan utbildning **(*Figur 4.5.2)***. Vad som har diskuterats bland respondenterna landar i att för att utbildningen ska vara effektiv och att de ska

själva kunna anpassa vad som lärs ut på sina arbetsuppgifter, bör utbildningen anpassa sig för att lära ut något som är relevant för de olika rollerna, om utbildningen inte anpassas på sådant vis introduceras utbildningen till en överhängande risk att den inte är effektiv och vad som lärs ut är inte applicerbart för alla. Detta är något som även Pattinson et al. (2018) och Flores et al. (2021) har resonerat kring i den mån att företagen bör dela upp träningen bland olika divisioner och grupper inom företaget. För att gå tillbaka till svaren på enkäten, kan respondentens kommentar användas till företagens fördel för att dela upp utbildningen i den mån att de avdelningar som har en djupare förståelse för cybersäkerhet, till exempel *penetrationstestare,* får en viss utbildning som är anpassad efter deras expertis och behov, medan utbildningen för en annan avdelning följer de behov som finns bland anställda inom en annan avdelning av företaget.

5.5 Förslag på lösningar

Baserat på litteraturgenomgången som har gjorts för detta arbete och de svar som har angivits av respondenterna i utförandet av den kvantitativa undersökningen, har ett antal problemområden noterats i den träning som ges ut av företagen av en större omfattning för att adressera den mänskliga faktorn i cybersäkerhet. Den bidragande faktorn för att undersöka hur utbildningen för cybersäkerhet ser ut bland större företag och upptäcka lösningar i deras strategi har sin grund i litteraturen som presenterades av Chowdhury et al. (2022), Flores et al. (2023) och Mwangala et al. (2023) att utbildningen, som är företagets främsta strategi för att adressera, samt för att bringa mer uppmärksamhet kring, den mänskliga faktorn lider av lågt engagemang och att deltagarna går tillbaka till att hantera data på ett "ohygieniskt vis” trots att de har deltagit på utbildningsmoment.

I ett tidigare avsnitt av arbetet sades det att förslag på lösningar skulle presenteras, detta är något som vidare diskuterades att det skulle ske som en matris. I följande matris framläggs förslag på lösningar för hur företagen ska kunna utveckla utbildningen för att vidare fokusera på den mänskliga faktorn i cybersäkerhet.

Förslaget delas främst upp i tre delar: *Vad, Hur* och *Varför. Vad* beskriver vad förslaget är, *hur* beskriver hur detta kan se ut i praktiken för att tillämpas och *varför* lägger tyngd på varför det presenterade förslaget har inkluderats.

Vad - Lösningsområde	**Hur - Vidare notering -**	**Varför - Motivering**
- Användning av praktisk träning	- *Serious Games* - Simulationer av attacker, till exempel nätfiskeattacker	- Använder fler sinnen - Kostnadseffektiv - Låter en att börja om från början tills en klarar utmaningen - Låter en att “hitta på” egna lösningar - En positiv miljö som låter en att fokusera på “uppdraget” - Interagerar med det man

		ska lära sig - Ökat engagemang bland deltagarna - Bildar en djupare förståelse för ämnet
- Anpassa träningen efter deltagarnas preferenser - Anpassa träningen efter kunskapsnivåer - Vidare förståelse för företagens behov och "Svaga punkter	- Bedömning som sträcker sig över flera avdelningar i ett företag	- Utbildningen ska vara relevant för de arbetsuppgifter en arbetar med - Utbildningen bör ta hänsyn till att alla lär sig på olika vis - Utbildningen bör ta hänsyn till olika kunskapsnivåer

Tabell 5.5.1 *Förslag på lösningar*

5.6 Metodreflektion

Trots att datan som har hämtats från den kvantitativa undersökningen som har gjorts för att undersöka forskningsfrågan har kunnat används för att få en djupare förståelse hur utbildningen för cybersäkerhet ser ut bland medelstora och stora företag, men även hur praktisk träning har visat en positiv effekt på inlärningen, både i litteraturen och hos de som svarade på enkäten, finns det ett flertal nackdelar med den använda metoden och dess utförande. Den första nackdelen med utförandet av metoden för detta arbete är svarsfrekvensen.

En låg svarsfrekvens när man utför en enkät är något som bland annat har diskuterats av Oates (2006). Som en direkt konsekvens av något som inte kunde kontrolleras under författandet av detta arbete, led detta arbete av tidsbrist i hög grad. Av denna anledningen, var fönstret för utförandet av denna enkät mindre än vad som hade önskats och tiden för att invänta svar från respondenterna var något som endast var cirka en vecka. Hade fönstret varit något större för att samla in data, hade även tidsintervallet för att invänta svar från respondenterna varit något större, hade det varit möjligt att samla in data från en större urvalsgrupp, vilket också hade lett till en djupare förståelse för hur utbildningen för cybersäkerhet ser ut bland medelstora och stora företag. Trots detta, eftersom att enkäten hade en rad kvalitativa instick, i den mån att individen själv hade möjlighet att dela deras tankar och motivera deras svar, har datan som har hämtats från den kvantitativa undersökningen kunnat användas för att dra tydliga slutsatser och jämförelser med den tidigare forskningen som hade gjorts kring forskningsfrågan. .

Vidare har det även noterats av Oates (2006) att ännu en nackdel med den valda metoden är att svaren som ges av respondenten inte kan gå på djupet, detta är främst eftersom den som utför arbetet inte kan ställa följdfrågor till de svar som respondenten ger. I mån av de omständigheter som skedde under författandet av arbetet, var det inte möjligt att utföra intervjuer för detta arbete. För att till viss del, trots detta, uppnå ett visst djup på svaren som gavs av respondenten, användes följdfrågor genomgående i enkäten och respondenten hade möjligheten att vidare motivera deras

svar på ett antal frågor. Detta är något som låter en att vidare kunna studera svaren som gavs på enkäten något mer på djupet.

6. Slutsats

Som det sades i *syftet* för detta arbete, delades forskningsområdet för arbetet i primärt tre delar. Det handlar om den *mänskliga faktorn i cybersäkerhet, hur utbildningen för cybersäkerhet ser ut bland medelstora och stora företag* och *förslag på lösningar för utbildningen.*

Tekniken är här för att stanna och det är något som kontinuerligt kommer att utvecklas. Detta är något som dels företagen i dess olika storlekar använder till sin fördel för att ständigt utveckla sina verksamhetsprocesser, men även deras interna system som de använder sig av. Samtidigt som detta låter företagen utveckla sina verksamhetsprocesser och interna system, är detta något som även låter cyberangripare av olika slag utveckla nya metoder för att angripa företag av olika storlekar, men även olika branscher.

En rad metoder som används av cyberangripare bygger på att komma åt företagens data genom individen som arbetar i företaget, metoder som detta är bland annat *nätfiske* samt *imitation*. Detta är även något som har visats genomgående i arbetet att en större majoritet av cyberattacker, men även andra cybersäkerhetsrisker, som företagen drabbas av är en direkt konsekvens av någon form av mänsklig handling. Ett exempel på en sådan mänsklig handling är att de misslyckas att identifiera olika typer av försök på attacker, främst *nätfiske* och *imitation.* Fortsättningsvis, hanterar anställda i företaget dess data på ett "ohygieniskt vis”, i den mån att de delar lösenord internt mellan varandra i företaget och att de öppnar länkar från okända personer, som kan vara ett försök på nätfiske.

Litteraturgenomgången introducerade att den främsta metoden som används för att bringa mer uppmärksamhet kring cybersäkerhet och olika risker som kan uppkomma relaterat till cybersäkerhet bland anställda, är intern utbildning i form av föreläsningar och andra kampanjer. Detta är även något som har påvisats i resultatet som presenterades för detta arbete. Interna utbildningar och andra kampanjer är en metod som används av en rad företag av större omfattning. Det har också noterats i resultatet av detta arbete att ett antal företag även har implementerat ett något mer praktiskt tillvägagångssätt för hur utbildningen ser ut i den mån att de använder sig av simulationer av försök på nätfiske. Ett antal företag använder sig idag av *serious games* för att bringa mer uppmärksamhet kring hur anställda ska hantera sin data, samt hur de ska hantera försök på olika typer av cyberattacker. Vidare har det även diskuterats bland respondenterna för arbetet, att företagen även har använts sig av *externa lösningar,* i den utsträckning att företagen inkluderar *Nanolearning/Microlearning* som erbjuds av ett externt företag.

I *problemformuleringen* för arbetet noterades det att förslag på lösningar för en ökad utveckling av utbildningen som ges för att fokusera på de mänskliga faktorerna i cybersäkerhet. De två primära problemområden som noterades i arbetet var att utbildningen som ges för cybersäkerhet i många fall lider av *lågt engagemang* bland deltagarna och att anställda går tillbaka till tidigare vanor vid hantering av data efter utbildningen av cybersäkerhet. De primära lösningsförslagen

som angavs i detta arbete var att utbildningen ska inkludera praktiska moment, *serious games* och simulationer av attacker har diskuterats som ett alternativ för praktisk träning. Vidare har det nämnts att användarens kunskapsnivå och preferenser bör inkluderas i utformningen av utbildningen, något som kan göras genom att dela upp deltagarna i olika grupper, baserat på de två kriterierna.

Trots att det har aktualiserats bland respondenterna i resultatet av detta arbete att *serious games* har använts till en viss grad av företagen som en del av utbildningen, har detta diskuterats i litteraturgenomgången som en relativt ny teknologi som har visat bringa en högre grad engagemang bland deltagarna kring utbildningen för cybersäkerhet, engagemanget för utbildningen bland deltagarna var något som tidigare identifierades som ett problemområde i litteraturen. Ett annat lösningsförslag som har identifierats i arbetet, för att introducera en högre grad av engagemang bland deltagarna för utbildningen inom ämnet, är att utbildningen bör ta hänsyn till individens kunskapsnivå och preferenser. Detta är något som företagen kan göra genom att genomföra en bedömning av kunskapsnivån av individerna och dess preferenser för att sedan forma grupper, efter deras kunskapsnivå och preferenser, för att vidare kunna anpassa, men även för att utveckla utbildningen. Både de som har förmedlat att praktisk träning samt att deras kunskapsnivå och preferenser som en del av utbildningen, och de som har resonerat kring detta utan att detta har varit en del av deras träning, har en positiv syn för dessa två lösningsförslagen indikerats.

6.1 Förslag på vidare forskning

Under arbetets gång har en rad områden identifierats som kan användas som grund för vidare forskning inom ämnet. Inledningsvis har *serious games* identifierats i litteraturen som en relativt ny teknologi som kan användas som metod för att träna anställda att kunna identifiera försök till cyberattacker, men även för att vidare förstå risken med cyberattacker. Vidare forskning för *serious games* hade låtit företag att vidare förstå hur det kan användas, men kan även resultera i fler spel som kan användas som en del av träningen. Detta är något som skulle kunna leda till ett bredare utbud av spel som företag kan använda sig av samt för att identifiera nya områden inom cybersäkerhet som spelen kan inkludera.

Vidare diskuterades det, som ett lösningsförslag för de problemområden som har uppstått bland företagen och dess strategier för att implementera utbildningsprogram för att adressera den mänskliga faktorn i cybersäkerhet, att utbildningen bör matcha individens kunskapsnivå och färdigheter. Vidare forskning kan göras för hur detta kan ha en inverkan på hur individen lär sig nya färdigheter och ämnen, men även hur företagen kan implementera en strategi för att kunna identifiera och matcha utbildningen med individens färdigheter och deras kunskapsnivå.

Referenser

Aldawood. H, Skinner, G. (2019). Challenges of Implementing Training and Awareness Programs Targeting Cyber Security Social Engineering. 2019 Cybersecurity and Cyberforensics Conference (CCC), https://ieeexplore-ieee-org.ludwig.lub.lu.se/document/8854548 [Accessed 22 March 2024]

Alnifie. M, K, & Kim, C. (2023). Appraising the Manifestation of Optimism Bias and Its Impact on Human Perception of Cyber Security: A Meta Analysis, *Journal of Information Security*. Vol. 14, no. 2, pp. 93-110. https://doi.org/10.4236/jis.2023.142007

Alotaibi. L, Seher. S, Mohammad. N, (2024), Cyberattacks Using ChatGPT: Exploring Malicious Content Generation Through Prompt Engineering, 2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS), https://ieeexplore-ieee-org.ludwig.lub.lu.se/stamp/stamp.jsp?tp=&arnumber=10459698 [Accessed 16 March 2024]

Aue. T, Okon-Singer. H, (2015), Clinical Psychology Review, *Clinical Psychology Review* vol. 42, pp 85-92, https://doi.org/10.1016/j.cpr.2015.08.005

Barber. R, (2001), Social engineering: A People Problem?, *Network Security*, Volume 2001, Issue 7, pp 9-11, https://doi.org/10.1016/S1353-4858(01)00716-4

Barletta. S, V, Calvano. M, Caruso, F, Curci, A, Piccinno, A. (2023), Serious Games for Cybersecurity: How to Improve Perception and Human Factors, 2023 IEEE International Conference on Metrology for eXtended Reality, Artificial Intelligence and Neural Engineering (MetroXRAINE), https://ieeexplore.ieee.org/document/10405607, [Accessed 27 March 2024]

Barney, N. (2023). Definition: deepfake AI (deep fake) https://www.techtarget.com/whatis/definition/deepfake [Accessed 5 April 2024]

Chowdhury. N, Katsikas. S, Gkioulos. V, (2022), Modeling effective cybersecurity training frameworks: A delphi method-based study, *Network Security,* vol. 113, pp. 1-15 ScienceDirect

Corradini, I, (2020), Building a Cybersecurity Culture in Organizations, Springer

DeFranzo. S, E (n.d.) Advantages and Disadvantages of Surveys, https://www.snapsurveys.com/blog/advantages-disadvantages-surveys/ [Accessed 26 April 2024]

EUR-Lex, (n.d.), Små och medelstora företag, *https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=LEGISSUM:sme* [Accessed 30 April 2024]

Flores, CV, Gonzalez, J, Kajtazi, M, Bugeja, J & Vogel, B (2023), Human Factors for Cybersecurity Awareness in a Remote Work Environment, International Conference on Information Systems Security and Privacy, https://doi.org/10.5220/0011746000003405 [Accessed 13 April 2024]

Elev8, (n.d.), *T*he Importance of Cyber Security Awareness Training for Employees, https://www.elev8me.com/insights/the-importance-of-cyber-security-awareness-training-for-employees [Accessed 5 April 2024]

Gross, A, (2018), Effective Security Training Requires Change in Employee Behavior, https://www.healthitanswers.net/effective-security-training-requires-change-in-employee-behavior/ [Accessed 15 April 2024]

Hartfield. M, J, (2017), Social engineering in cybersecurity: The evolution of a concep*t, Computers & Security*, Volume 73, pp 102-113, https://doi.org/10.1016/j.cose.2017.10.008

Hodhod. R, Hardage. H, Abbas. S, Aldakheel. A, E, (2023), CyberHero: An Adaptive Serious Game to Promote Cybersecurity Awareness. ResearchGate

IBM, (n.d.), What is smishing?, https://www.ibm.com/topics/smishing [Accessed 11 May 2024]

Main, P, (2023), Hands-On Learning, https://www.structural-learning.com/post/hands-on-learning [Accessed 1 May 2024]

Microsoft, (n.d.), Vad är cybersäkerhet?, https://support.microsoft.com/sv-se/topic/vad-%C3%A4r-cybers%C3%A4kerhet-8b6efd59-41ff-4743-87c8-0850a352a390 [Accessed 12 May 2024]

Microsoft, (n.d.), Why is cybersecurity awareness and education critical? https://www.microsoft.com/en-us/security/blog/2023/10/02/celebrate-20-years-of-cybersecurity-awareness-month-with-microsoft-and-lets-secure-our-world-together/ [Accessed 12 May 2024]

Microsoft, (n.d.), Attack simulation training, https://www.microsoft.com/en-us/security/business/threat-protection/attack-simulation-training [Accessed 12 May 2024]

Morin, A, (2020), Personalized learning: What you need to know, *https://www.understood.org/en/articles/personalized-learning-what-you-need-to-know* [Accessed 29 April 2024]

MSB, (n.d), Metoder vid cyberangrepp, https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/risker-och-sarbarheter-inom-cybersakerhet-och-cyberfysiska-system/hot-och-metoder-inom-cybersakerhet/metoder-vid-cyberangrepp/ [Accessed 29 April 2024]

Mwangala. J, Bhunu Shava. F, Chitauro. S, (2023), Human Intelligence an Enabler for Cyber Resilience: A Case for Namibian Public Institutions, IST-Africa Conference, https://ieeexplore.ieee.org/document/10187836 [Accessed 28 March 2024]

NCSC, (2018), Phishing attacks: defending your organisation, https://www.ncsc.gov.uk/guidance/phishing [Accessed 28 March 2024]

Oates, J.B. 2006. Researching Information Systems and Computing. Sage Publications Ltd. London.

Pattinson, M, Butavicius. M, Ciccarello. B, Lillie. M, Parsons. K, Calic. D, McCormac. A, (2018), *Adapting Cyber-Security Training to Your Employees.* Proceedings of the Twelfth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2018), https://www.cscan.org/?page=openaccess&eid=20&id=379

PR Newswire, (2019), Ponemon: Cyberattacker mot små och medelstora företag ökar globalt, blir mer riktade och sofistikerade, https://markets.businessinsider.com/news/stocks/ponemon-cyberattacker-mot-sm%C3%A5-och-medelstora-foeretag-oekar-globalt-blir-mer-riktade-och-sofistikerade-1028586332 [Accessed 1 May 2024]

Puta, D, (2022), Cybersecurity and Mental Health, https://www.infosec.ox.ac.uk/article/cybersecurity-and-mental-health [Accessed 2 May 2024]

Rohan. R, Funilkul. S, Pal. D (2021), Chutimaskul. W, *U*nderstanding of Human Factors in Cybersecurity: A Systematic Literature Review. 2021 International Conference on Computational Performance Evaluation (ComPE), https://doi.org/10.1109/ComPE53109.2021.9752358 [Accessed March 27 2024]

Stockholms Handelskammare, (2022), Cyberbrott mot svenska företag, Stockholms Handelskammare

Tech Accord, (2021), Cybersecurity Awareness in The Commonwealth of Nations, Tech Accord

The Super Mario Effect - Tricking Your Brain into Learning More | Mark Rober | TEDxPenn. (31 May 2018). YouTube video, added by TEDx Talks[Online], The Super Mario Effect - Tricking Your Brain into Learning More | Mark Rober | TEDxPenn [Accessed 29 March 2024]

Trost, J. & Hultåker, O. (2016). Enkätboken. Lund: Studentlitteratur AB. uppl. 5.

Wilson, M. and Hash, J. (2003), Building an Information Technology Security Awareness and Training Program, NIST Special Publication 800-50 https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=151287 [Accessed 13 April 2024]

Workman, M. (2007) Gaining Access with Social Engineering: An Empirical Study of the Threat, Information Systems Security, vol. 16, pp. 315-331.
https://www.tandfonline.com/action/showCitFormats?doi=10.1080/10658980701788165

Bilaga

AI redogörelse

Inga AI-baserade verktyg har använts i författandet av detta arbete.