Uppsala universitet
Inst. för informatik och media

Faktorer som påverkar säkerhetsbeteende: En litteraturstudie utifrån UMISPC-modellen

Herman Båtelsson & Olof Segergren

UPPSALA
UNIVERSITET

Kurs: Examensarbete
Nivå: C
Termin: VT-22
Datum: 2022-09-18
Handledare: Elin Uppström

Sammanfattning:
En av de säkerhetsrisker som företag i dagsläget måste ta hänsyn till är bristande säkerhetsbeteende hos anställda vid användande av informationssystem. Denna brist kan leda till incidenter där produktivitet går förlorad eller känslig data läcks. Detta gör att användarnas beteende och efterlevnad av säkerhetsriktlinjer blir ett viktigt ämne för företag och organisationer. Tidigare studier identifierar flera faktorer som bidrar till bättre eller sämre säkerhetsbeteende hos individer. UMISPC-modellen ("*Unified Model of Information Security Policy Compliance*") skapad av Moody m.fl. (2018) är en ansats till att unifiera faktorer från flera teorier. De inkluderar enbart faktorer som de kunde stödja i ett specifikt kontext men misstänker att effekten av faktorer som de exkluderar kan stödjas i andra kontext. För denna uppsats utfördes en litteraturstudie där faktorer i existerande modeller identifieras och klassificeras in i de faktorer som UMISPC-modellen definierar. Litteraturstudien gjordes via söktjänsten Uppsalas universitetsbibliotek. Resultaten visade att flera av studiernas resultat stöder flera av de faktorer som Moody m.fl. inte fann stöd för. Dessa faktorer kan därför vara aktuella för framtida utökningar av UMISPC-modellen trots att de inte kunde stödjas av Moody m.fl. (2018).

Nyckelord: Säkerhetsbeteende, Säkerhetsmedvetenhet, IT-säkerhet, Riktlinjer, Policy

Abstract:
One of the security risks companies of today have to consider is poor security behavior of employees while using information systems. These behaviors can lead to incidents where productivity is lost or sensitive data is leaked. This causes the users' behavior and compliance with security guidelines to become an important subject for companies and other organizations. Earlier studies identified several factors contributing to better or worse security behavior of individuals. The UMISPC model (*Unified Model of Information Security Policy Compliance*) created by Moody et al. (2018) is an effort to unify factors from multiple theories. They only include factors for which they were able to find support in a specific context but suspect that the effect of factors they exclude can be supported in other contexts. For this essay, a literature study was performed where factors from existing models were classified into factors defined by the UMISPC model. The literature study was performed using the search engine provided by Uppsala's university library. The result showed that several studies support the factors that Moody et al. (2018) did not find support for. These factors can therefore be valid for future extensions of the UMISPC model even though they could not be supported by Moody et al. (2018).

Keywords: Security behavior, Security awareness, IT-security, Guidelines, Policy

Innehållsförteckning

1. Inledning

I detta kapitel presenteras studiens bakgrund, problembeskrivning, syfte, forskningsfråga, avgränsningar samt kunskapsbidrag.

1.1. Bakgrund

Företag hanterar idag ofta stora mängder data. Bristande IT-säkerhetsrutiner kan leda till att känslig data blir tillgänglig för fel personer eller går förlorad. I takt med att digitala säkerhetssystem blir kraftfullare blir användarna en mer attraktiv måltavla för kriminella då det ofta anses vara lättare att lura människor än datorer (Diehl, 2016). I boken *Ten Laws for Security* (Diehl, 2016) beskrivs flera exempel på hur angrepp utförs genom att lura anställda, exempelvis genom att be om bilder på kreditkort eller utge sig för att vara en arbetare från en teleoperatör som behöver kundens uppgifter. Ett annat exempel är genom att skicka en fil som utgör sig innehålla intressant information om aktuella händelser men när den öppnas så exekveras skadlig kod på datorn, detta kan på så sätt äventyra företagets tillgångar.

Bhardwaj m.fl. (2021) nämner den *Mänskliga Brandväggen* i sin artikel. Konceptet involverar vad anställda kan göra för att förhindra säkerhetsincidenter. Om det önskade säkerhetsbeteendet förhindrar eller försenar ordinarie uppgifter kan det leda till försämrat säkerhetsbeteende. Xu och Guo (2019) menar att uppskjutande av säkerhetsuppgifter i koppling till psykologisk likgiltighet är anledningar till brister i anställdas säkerhetsbeteenden. Dessa beror i sin tur på att anställda anser att deras ordinarie uppgifter är viktigare och/eller blir lidande om säkerhetsåtgärder skall utföras (Xu and Guo, 2019). Det förekommer därmed att även anställda som är medvetna om risker och åtgärder har bristande säkerhetsbeteende på grund av flera faktorer. Vilka dessa faktorer är och hur de påverkar varandra är inte självklart, speciellt i olika företag och kulturer.

Det finns ett flertal modeller som är framtagna och testade i olika sammanhang med avsikt att kartlägga dessa faktorer. Några exempel är Xu och Guo (2019) som undersöker anställda på ett företags mentala hanteringsmetoder för att följa eller inte följa ett visst säkerhetsbeteende, Ng m.fl. (2009) som undersöker hur säkerhetsbeteende hos anställda från flera företag kan liknas med patienter som utför handlingar för att undvika hälsorisker, och Hanus och Wu (2016) som undersöker hur säkerhetsmedvetenhet påverkar säkerhetsbeteendet hos datoranvändare bland universitetsstudenter. Den mängd modeller som skapats har enligt Moody m.fl. (2018, s. 2) "*resulterat i en djungel av konkurrerande modeller för säkerhetsbeteende som kanske inte är lätta att jämföra*" (författarnas översättning).

Med detta som bakgrund skapade Moody m.fl. (2018) UMISPC-modellen ("*Unified Model of Information Security Policy Compliance*") en ansats till att kombinera flera teorier för att skapa en unifierad modell för vilka faktorer som påverkar individers efterlevnad av säkerhetsriktlinjer. Deras mål var bland annat att "*syntetisera djungeln av alternativa teorier*" för att underlätta för forskare inom IT-användning.

1.2. Problembeskrivning och problemdiskussion

Moody m.fl. (2018) testade en preliminär version av sin modell i ett kontext med tre hypotetiska scenarion som alumner från ett finskt universitet svarade på. Ett exempel på dessa scenarier var att en anställd tog en kopia på ett USB-minne av känslig data för att kunna arbeta under en tågresa. Dessa tester gjorde att de kunde stödja samband mellan olika faktorer och säkerhetsbeteende. Moody m.fl. (2018) kunde stödja empiriska korrelationer mellan vissa faktorer och anställdas säkerhetsbeteenden, medan andra faktorers påverkan inte kunde påvisas av studiens resultat. De modifierade sin slutgiltiga modell baserat på deras resultat genom att utesluta de faktorer vars korrelation till säkerhetsbeteende inte kunde stödjas. De skriver dock att andra scenarion än de som användes i deras empiriska undersökning kan tänkas leda till andra resultat och att modellen bör "*vidare testas eller till och med revideras för att ta hänsyn till andra säkerhetsåtgärder*" (Moody m.fl. 2018, s. 2) (författarnas översättning). De uppmanar också till vidare forskning genom exempelvis testning av modellen i andra kontext för att avgöra dess begränsningar, utökning av modellen för andra kontext och identifiering av kontext där delar av modellen är irrelevant.

Kajtazi m.fl. (2021) utförde en replikeringsstudie för att testa Moodys m.fl. (2018) modell i ett annat kontext. De använde sig av en onlinepanel med anställda på "*informationsintensiva företag*". Deras resultat kunde inte stödja alla de faktorer Moody m.fl. (2018) presenterar vilket indikerar på att aktuellt kontext påverkar resultaten och att det kontext som Moody m.fl. (2018) använde för att ta fram UMISPC-modellen kan ha lett till att vissa faktorer uteslöts trots att de är relevanta i andra kontext. Dessa faktorer kan därmed uppfylla de kriterier som Moody m.fl. (2018) skapat för inkludering i UMISPC-modellen.

Att dessa faktorer uteslutits från modellen kan leda till att yrkesutövare och akademiker som baserar sitt arbete på den bortser från samma faktorer. Om dessa faktorer ignoreras trots deras påverkan på säkerhetsbeteende kan det leda till ökad risk för säkerhetsincidenter. Exempelvis genom att en säkerhetsansvarig enbart fokuserar på de faktorer Moody m.fl. (2018) finner stöd för, men öppnar upp sin organisation för incidenter genom att inte utbilda sin personal med alla faktorer i åtanke.

1.3. Forskningsfråga

Syftet med denna uppsats är att identifiera faktorer som exkluderas från UMISPC-modellen men som ändå påverkar säkerhetsbeteende i andra kontext med begränsning av att enbart undersöka faktorer som inkluderats eller uteslutits av Moody m.fl. (2018). Forskningsfrågan som besvaras är: *"Vilka faktorer kan vara aktuella för en framtida utökning av UMISPC-modellen?"*.

1.4. Kunskapsbidrag

Studien bidrar med vägledande kunskap (Goldkuhl, 2011) genom att ifrågasätta UMISPC-modellen. Moodys m.fl. (2018) spekulationer om att vissa faktorer påverkar säkerhetsbeteende trots att de uteslöts ur UMISPC-modellen används som argument för och riktning till vidare forskning. De faktorer som Moody m.fl. (2018) utesluter kan ha en påverkan i andra kontext som går att stödja och är i så fall aktuella att undersöka för de framtida revisioner av UMISPC-modellen som Moody m.fl. (2018) rekommenderar.

Denna studie skapar vägledande kunskap för utökning av UMISPC-modellen. Detta genom att föreslå vilka faktorer framtida studier bör testa inför en eventuell revidering av UMISPC-modellen. Förbättring av UMISPC-modellen bidrar på sikt med vägledande kunskap genom att säkerställa att personer som använder UMISPC-modellen i framtiden inte missar viktiga faktorer som inte inkluderas i modellen. Både akademiker och yrkesutövare som på något sätt använder modellen har behov av att modellen beskriver faktorer som påverkar anställdas beteende på ett korrekt sätt. I akademikernas fall genom relevanta förslag till faktorer att undersöka, och i yrkesutövares fall för att kunna ta fram effektiva strategier för förbättring av anställdas säkerhetsbeteende.

1.5. Disposition

Denna studie disponeras på följande sätt:

Kapitel 1: *Inledning*: Bakgrund och problembeskrivning används som grund till forskningsfrågan. Förväntat forskningsbidrag presenteras.
Kapitel 2: *Teori*: Centrala begrepp definieras och studien förankras i tidigare forskning. UMISPC-modellen presenteras i detalj.
Kapitel 3: *Metod och Genomförande*: Studiens forskningsstrategi, datainsamling- och dataanalysmetod, genomförande, kvalitet i genomförande samt forskningsetiska överväganden presenteras.
Kapitel 4: *Resultat och Analys*: Resultaten av datainsamlingen presenteras och analyseras utifrån uppsatta metoder och mål.
Kapitel 5: *Diskussion*: Resultaten av studien samt implementationen av valda metoder diskuteras för att ligga till bas för kvalitetsutvärdering av läsare.
Kapitel 6: *Slutsats*: Vilket bidrag och vilka lärdomar som kan dras från resultaten presenteras, och även hur resultatet potentiellt kan ligga till grund för framtida forskning.

2. Teori

I detta kapitel presenteras centrala begrepp och ämnesmässig förankring följt av tidigare forskning där UMISPC-modellen inkluderas.

2.1. Ämnesmässig förankring

Detta avsnitt beskriver och definierar centrala begrepp och beskriver sedan hur medvetenhet inte alltid är tillräckligt för att uppnå gott säkerhetsbeteende. Avsnittet beskriver även hur en vetenskaplig modell skapas och potentiellt utökas i framtida studier.

2.1.1. Centrala begrepp

Säkerhetsbeteende
Ng m.fl. (2009) definierar ett bra säkerhetsbeteende som "*beteende som minskar risken och/eller effekten av säkerhetsincidenter"* (författarnas översättning, s. 817) och att det krävs "*förebyggande och skyddande beteende för att undvika säkerhetsincidenter"* (författarnas översättning, s. 817). Moody m.fl. (2018) beskriver den närliggande termen "*efterlevnad av policy*" vilket inkluderar "*följande av policyer, procedurer och riktlinjer angående säkerhet*" (författarnas översättning). De två termerna är närliggande då säkerhetsbeteende kan inkludera efterlevnad av policy.

Faktor
I denna uppsats definieras en faktor som "*en sak som bidrar till ett visst resultat eller en viss situation*" (författarnas översättning) (Deming and Morgan 1993, s. 4). När ordet faktor används menas något som påverkar individens säkerhetsbeteende, antingen direkt eller genom att påverka en annan faktor. En faktor kan ha negativ eller positiv påverkan på det slutliga säkerhetsbeteendet på individen. Exempel på faktorer är *Säkerhetsutbildning*, *Träning* och *Medvetenhet* (Nasir et al., 2019).

Teori
Termen teori används i denna uppsats på ett sätt som avser överensstämma med Moody m.fl. (2018). De inhämtar faktorer som kan förklara eller förutsäga olika typer av beteenden från teorier inom andra ämnen. Moody m.fl. (2018) skapar ingen egen definition av termerna *teori* eller *modell* men väljer att separera termerna.

Modell
Det amerikanska försvarsdepartementet (1998, s. 136) definierar termen modell som: "*en fysisk, matematisk eller på annat sätt logisk representation av ett system, entitet, fenomen eller process*" (författarnas översättning). För denna uppsats innebär det att en modell har som avsikt att representera faktorer som påverkar *individens säkerhetsbeteende*. Vanligtvis visualiseras modeller i ett diagram. En modell kan sedan testas empiriskt för att stödja sambanden mellan en viss faktor och ett visst beteende. Ett exempel på en modell är Hanus och Wu (2016) som skapar en modell baserad på teorin *Protection Motivation Theory*. Deras modell använder de faktorer som *Protection Motivation Theory* definierar men anpassade till säkerhetsbeteende hos datoranvändare.

Kontext
Med termen kontext menas ett visst sammanhang där säkerhetsbeteende är aktuellt. Exempelvis en viss typ av arbetsplats i ett visst land. Moody m.fl. (2018) har kontextet finska

alumner, och deras tre exempel på scenarier beskriver ett kontext där en anställd arbetar på ett kontor. Vilka faktorer som påverkar en individs säkerhetsbeteende kan skilja sig beroende på typ av organisation eller kultur, det vill säga olika kontext. Exempelvis en anställd på en skola, ett sjukhus eller en militärbas.

Stödja
I denna uppsats används termen *stödja* för att beskriva ett empiriskt resultat som med statistisk signifikans visar att faktor har en påverkan på beteende, antingen direkt eller indirekt via påverka en annan faktor. Att en artikel eller studie beskrivs stödja en faktor innebär att deras resultat visar ett samband mellan faktorn i fråga och ett visst beteende.

Policy/Riktlinjer
En säkerhetspolicy definieras som en eller flera regler som ett företag avser sina anställda att följa för att minska risken för säkerhetsincidenter. Dessa kan exempelvis inkludera att kryptera e-post eller att inte dela med sig av personliga lösenord. Termerna *policy* och *riktlinjer* används utbytbart i denna uppsats, detta då språknämnden avråder plural-formen av *policy* (sprakbruk.fi, 2004). Ordet *riktlinjer* används där pluralformen krävs.

2.1.2. Förankring

En av de viktigaste faktorerna för effektiv IT-säkerhet är att öka medvetenheten hos de anställda (Layton, 2005) men flera andra faktorer kan leda till bättre eller sämre säkerhetsbeteende. Ng m.fl. (2009) nämner att anställda som är medvetna om *Upplevda sårbarheter och fördelar* (författarnas översättning) kan göra medvetna val för att utföra lämpliga beteenden. Eminağaoğlu m.fl. (2009) skriver att *Medvetenhet* är en bidragande faktor i förbättring av säkerhetsbeteendet hos de anställda på företag. I deras studie undersöktes specifikt anställdas val av lösenord och det noterades att det fanns viss motvillighet till att följa företagets policy för säkerhetsbeteende. Denna motvillighet är ett exempel på att det finns fler bidragande faktorer än anställdas medvetenhet. Tidigare forskning har skapat flera modeller med mål att kartlägga hur dessa faktorer påverkar individers säkerhetsbeteende.

En vetenskaplig modell skapas genom ett deduktivt eller induktivt tillvägagångssätt, alternativt en kombination av båda metoder (DeCarlo, 2018, p. 153). Deduktiva modeller är baserade på en eller flera teorier som studerats och analyserats, exempelvis Hanus och Wu (2016) som utgår från *Protection Motivation Theory*, Ifinedo (2012) som utgår från *Theory of Planned Behavior* och Sohrabi Safa m.fl. (2016) som utgår från *Social Bond Theory*. Genom att utföra en eller flera empiriska studier kan en deduktivt framtagen modell utvärderas och revideras eller bekräftas, beroende på om resultaten stödjer den eller ej (DeCarlo, 2018, p. 155).

En modell som skapats på ett induktivt tillvägagångssätt baseras på empirisk data (DeCarlo, 2018, p. 153). Denna typ av data kan sedan användas för att skapa en modell baserad på generalisering av resultatet, exempelvis Sommestad m.fl. (2014) som använder sig av en litteraturstudie för att hämta data, leta efter faktorer, och sedan generalisera resultatet utifrån data.

Om en ny studies resultat skiljer sig från den ursprungliga studiens resultat kan den ursprungliga studiens resultat ifrågasättas (DeCarlo, 2018). Genom att utföra en konceptuell

replikeringsstudie, vilket denna studie klassas som enligt Hudson (2021) definitioner, kan en modell antingen revideras om nya resultat skiljer sig från orginal studien eller så kan den bekräftas om den nya studien får liknande resultat (DeCarlo, 2018, p. 135; Hudson, 2021).

2.2. Tidigare forskning

Det finns mycket forskning och många modeller inom informationssäkerhet som identifierar faktorer som påverkar säkerhetsbeteende (Moody et al., 2018). Vissa undersöker efterlevnad av företagens riktlinjer, exempelvis Ng m.fl. (2009) och Nasir m.fl. (2019), och vissa undersöker säkerhetsbeteende i situationer där riktlinjer inte finns eller sker i privat miljö, exempelvis Hanus och Wu (2016) och Xu och Guo (2019). Modellerna baseras på faktorer som hämtats från en eller flera teorier, exempelvis från *Protection Motivation Theory* (Rogers, 1975) eller *Health Belief Model* (Becker, 1974) som trots sitt namn är en teori.

Health Belief Model beskriver vilka faktorer som påverkar handlingar individer utför för att undvika hot mot sin hälsa. I den teorin är *Medvetenhet om sårbarhet* och *Upplevda Fördelar* två av faktorerna som påverkar individen. *Protection Motivation Theory* är en teori för att testa hur individers beteende påverkas av rädsla. Teorierna är inte byggda för säkerhetsbeteende men kan anpassas för att användas inom ämnet säkerhetsbeteende på ett liknande sätt. Detta är något som Ng. m.fl. (2009) gör med *Health Belief Model* i sin artikel genom att ställa frågor om anställdas IT-säkerhetsbeteende på ett sätt som gör det möjligt att mäta vad anställda upplever som viktiga faktorer och skapa en modell utifrån det.

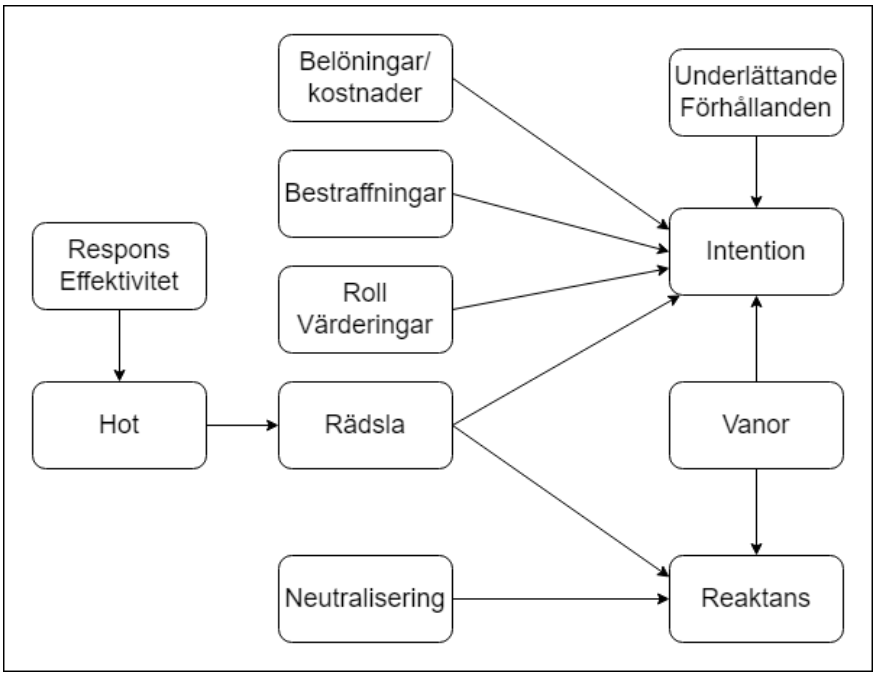
En ansats till att skapa en sammanställning av påverkande faktorer är Sommestad m.fl. (2014) som utförde en systematisk genomgång av resultat från tidigare studier. Artikeln fokuserar på vilka faktorer som är viktiga för efterlevnad av säkerhetsriktlinjer, samt hur viktiga de är. Målet med artikeln var att vägleda beslutsfattare inom företag till vilka faktorer som är viktigast att fokusera på. Deras studie resulterade i 61 identifierade faktorer från 29 artiklar. De kunde inte hitta någon tydlig vinnare bland dessa teorier och faktorer.

En annan ansats är Moody m.fl. (2018) som ansåg att det saknades forskning som unifierade teorier; de skapade därför UMISPC-modellen som en ansats till att skapa en unifierad modell med faktorer som påverkar en individs säkerhetsbeteende. Modellen skapades för att syntetisera "*djungeln av alternativa teorier*", kategorisera faktorer, samt empiriskt testa skillnaderna mellan teorierna och analysera hur de kompletterar varandra.

2.2.1. UMISPC-modellen

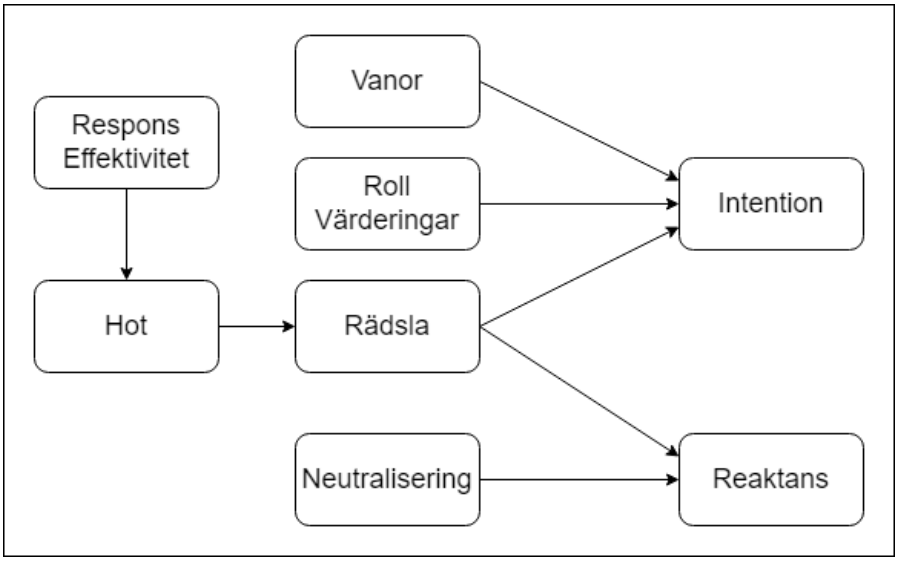
Moody m.fl. (2018) skapade UMISPC-modellen genom att mäta sambanden mellan olika faktorer och dess påverkan på säkerhetsbeteende. De faktorer som stöds med statistisk signifikans inkluderas i den slutgiltiga UMISPC-modellen.

De inledde sin studie med att använda tre scenarion (osäker USB-användning, delning av lösenord, utloggning från arbetsdatorer) hämtade från en tidigare studie och skapade därefter ett frågeformulär med frågor med dessa scenarion som grund. Frågorna var utformade för att mäta de faktorer som extraherats från de teorier som deras artikel baseras på. Sedan utförde de en studie (Studie 1) baserad på dessa frågor där 274 respondenter tillfrågades. Respondenterna hämtades från en lista med alumner från ett finskt universitet. Baserat på denna studie sammanslog forskarna faktorer och skapade en preliminär modell (Figur 2.1.).



Figur 2.1. *Preliminära UMISPC-modellen. Källa: Moody m.fl. (2018)*

Den preliminära modellen testades genom en undersökning (Studie 2) på ett större antal alumner (393 respondenter) från samma universitet. Genom att mäta sambanden mellan olika faktorer i svaren kunde vissa av dem stödjas. Resultatet visar även att ett antal faktorer saknar statistiskt samband med säkerhetsbeteende och kunde därför inte stödjas. Forskarna modifierade därefter modellen genom att behålla de faktorer som stöds av resultaten och exkludera de som inte stöds. Studie 2 fann inget stöd för faktorerna *Underlättande Förhållanden*, *Belöningar/Kostnader*, *Bestraffningar* och inte heller kopplingen mellan *Vanor* och *Reaktans*. Dessa faktorer inkluderades därför inte i den slutgiltiga UMISPC-modellen (Figur 2.2).



Figur 2.2. *UMISPC-modellen. Källa: Moody m.fl.* (2018).

Faktorn *Roll Värderingar* är inte hämtad direkt från en teori. Faktorn togs fram då resultaten från Studie 1 enbart hittade stöd för vissa delar av *Sociala Faktorer*, de delar som kunde

stödjas inkluderade inte sociala inslag vilket gjorde att Moody m.fl. (2018) ansåg att *Roll Värderingar* inte är en social faktor. Istället syftar faktorn på hur individen upplever de åtgärder som riktlinjer förespråkar som lämpliga, berättigade och acceptabla att utföra, i förhållande till den typ av uppgifter som individen utför inom företaget.

Moody m.fl. (2018) spekulerar i sin diskussion att de faktorer som inte kunde stödjas istället kan stödjas i andra sammanhang. *Bestraffningar* samt *Belöningar/Kostnader* misstänks av Moody m.fl. (2018) ha större påverkan i andra scenarier som sker oftare än de som användes i deras undersökning. Deras resultat tyder dock på att det endast finns en svag koppling mellan *allvarlighet på bestraffning* och säkerhetsbeteende. *Sociala Faktorer* undersöktes men användes inte i den slutgiltiga UMISPC-modellen då de inte fann stöd för faktorn i Studie 2. Den spekuleras ha haft en låg påverkan då scenarierna i studien inte anses vara socialt synliga eller socialt accepterade. Faktorn *Underlättande Förhållanden* hittade studien inte stöd för, detta spekuleras vara på grund av att de utvalda scenarierna inte var tekniskt utmanande. Moody m.fl. (2018) rekommenderar att framtida forskning bör undersöka mer tekniskt utmanande scenarier för att se hur det påverkar faktorer. Moody m.fl. (2018) avslutar sin diskussion genom att beskriva hur de olika faktorerna kan tänkas påverka anställda inom ett företag och vilka faktorer säkerhetsansvariga bör lägga vikt på.

3. Metod och genomförande

I detta kapitel beskrivs den metod studien använder sig av. Kapitlet beskriver studiens forskningsstrategi, datainsamling- och dataanalysmetod, genomförande, kvalitet i genomförande och slutligen forskningsetiska överväganden.

3.1. Forskningsstrategi

Det finns mycket forskning och många modeller som avser att kartlägga faktorer som påverkar säkerhetsbeteende. Eftersom dessa artiklar utgör en källa till data angående "*vilka faktorer som påverkar säkerhetsbettende*" valdes litteraturstudie som forskningsstrategi i denna uppsats. Denscombe (2006) nämner att några av fördelarna med litteraturstudier är att artiklar ofta är praktiskt tillgängliga, kostnadseffektiva att samla in och ofta är en permanent källa till data som kan undersökas av andra. För denna uppsats var det relevant då artiklar som inkluderade modeller kunde inhämtas via söktjänster vilket gjorde dem till tillgängliga datakällor.

En litteraturstudie som metod innebär att tidigare forskning används som datakälla. Oates (2006) beskriver hur tidigare utförd forskning kan ligga till grund för framtida studier i form av sekundär datainsamling, detta genom att återanvända resultat från undersökningar. Det är dock viktigt att dokumentets ursprung tas i åtanke för att bekräfta dess pålitlighet, exempelvis genom att ställa krav på att artiklar som används skall ha genomgått kollegial granskning eller publicerats i en etablerad journal (Oates, 2006).

En alternativ forskningsstrategi som studien skulle kunna använda sig av är en fallstudie där en undersökning i så fall skulle utföras på anställda inom ett visst företag. Uppsatsens resultat skulle då kunnat indikera om vissa av faktorerna som UMISPC-modellen utelämnar hade en inverkan på säkerhetsbeteende i det företagets kontext. Att jämföra resultaten från en sådan fallstudie med Moodys m.fl. (2018) resultat skulle dock återge information om enbart ett kontext. Då flera fallstudier utförts på liknande sätt men utan jämförelse med UMISPC-modellen förväntas en litteraturstudie kunna använda resultat från flera studier som är testade i flera olika kontext.

3.2. Datainsamlingsmetod

Moody m.fl. (2018) definierar faktorer som inte kunde stödjas i sin undersökning men som enligt dem möjligtvis kan vara aktuella i andra kontext. Det är möjligt att tidigare forskning som undersökt och skapat modeller för säkerhetsbeteende kan ha empiriskt bevisat att dessa faktorer påverkar individers säkerhetsbeteende. En litteratursökning valdes därför som datainsamlingsmetod.

Sökningens mål var att identifiera artiklar som empiriskt testar faktorer i andra kontext än det Moody m.fl. (2018) utförde sin studie i. Det är möjligt att en artikels definition för en faktor går att klassificera som en av de faktorer Moody m.fl. (2018) undersöker, samt att faktorns samband med säkerhetsbeteende kan stödjas. Målet är att på så vis identifiera faktorer som inte stöds av Moody m.fl. (2018) men som stöds i flera andra empiriska studier. Detta för att stödja Moodys m.fl. (2018) påstående om att faktorer som exkluderas i UMISPC-modellen ändå kan vara aktuella om de kan stödjas i andra kontext.

Då tidigare forskning skapat ett stort antal artiklar som undersöker faktorer i olika kontext finns det ett brett utbud av artiklar att undersöka. Dessa artiklar kan dessutom filtreras för att exkludera de som inte uppfyller akademisk standard, detta för att uppfylla Denscombe (2010) och Oates (2006) rekommendationer. Denscombe (2010) beskriver tillgång som en av de största fördelarna med artiklar som datakälla men att artiklarnas validitet bör övervägas. Även Oates (2006) rekommenderar att försäkra att artikelns journal är riktad till akademiker, har existerat en längre tid och att artikeln inkluderar kollegial granskning. Oates (2006) varnar även för att nya journaler inom informationssystem ofta skapas då ämnet är snabbt omväxlande, men att dessa nya journaler ändå kan vara en acceptabel källa.

En alternativ datainsamlingsmetod är att utföra en undersökning inom en organisation. Genom att fråga respondenter om deras säkerhetsbeteende via intervju eller frågeformulär skulle samband mellan förekomsten av en viss faktor och ett visst beteende kunna mätas. En fallstudie som alternativ datainsamlingsmetod har som fördel att data är ny och mer aktuell. En sådan fallstudie skulle dock enbart framställa relevanta faktorer inom ett visst kontext. För att åstadkomma samma resultat som den planerade litteraturstudien med en fallstudie skulle flera fallstudier i olika kontext behöva utföras, något som redan gjorts i tidigare forskning. Eftersom tidigare artiklar stöder deras faktorer och modeller genom att utföra fallstudier är det möjligt för denna uppsats att behandla faktorer som empiriskt stöds i flera kontext genom att undersöka flera artiklar. Om forskningsfrågan var fokuserad på ett visst kontext som exempelvis hotell, sjukhus eller banker hade en fallstudie kunnat bidra till djupare insyn om vilka faktorer som var relevanta i den typen av organisation.

3.3. Dataanalysmetod

Faktorer i artiklar är ofta lättillgängliga, exempelvis via punktlistor, vilket gör dem enkla att extrahera. Det ansågs därför inte vara nödvändigt att applicera en formell analysmetod för att extrahera dem. Sommestad m.fl. (2014) extraherar faktorer på liknande sätt och använder inte någon speciell analysmetod. Att sedan jämföra och kategorisera faktorer enligt Moodys m.fl. (2018) definitioner ansågs dock kräva en utvald analysmetod.

Då forskningsfrågan var ställd för att söka efter faktorer som ej inkluderas i UMISPC-modellen fanns det behov av att avgöra om en faktor från en artikel redan inkluderas i modellen, samt om en faktor som inkluderas i en artikel kan klassificeras som en av de faktorer Moody m.fl. (2018) inte fann stöd för. Eftersom dessa definitioner inte är kvantitativt jämförbara valdes delar ur den metod för kvalitativ innehållsanalys som Denscombe (2010) beskriver.

Denscombe (2010) skriver att en av fördelarna med innehållsanalys är att metoden utgör ett sätt att kvantifiera en text tydligt och ha en hög repeterbarhet. Dess begränsningar är att den riskerar att separera text från dess kontext och att underförstådda betydelser kan gå förlorade vilket gör att metoden är mest lämpad åt texter som är rättfram, tydlig, enkel och utan subtila meningar (Denscombe, 2010). Metoden ansågs lämplig för de vetenskapliga artiklar som denna studie avsåg undersöka då dessa är skrivna med akademiskt språk.

3.4. Genomförande

En litteraturstudie som metod används vanligtvis för att utvärdera forskningsområdet (Snyder, 2019; Xiao and Watson, 2019) och för att samla information från ett visst område eller ett visst ämne. Det finns olika metoder för att dela upp en litteraturstudies process (Xiao and Watson, 2019), för denna uppsats delades processen in i tre faser: Planering, Utförande och Analys.

- I planeringsfasen planerades studiens utförande baserat på forskningsfrågan och vilka sökalternativ som fanns tillgängliga. I detta steg valdes en lämplig omfattning och vilken typ av litteraturstudie som skulle utföras.
- I utförandefasen utformades och utfördes en sökning enligt de ramar som satts upp i planeringsfasen. Här inkluderades val av sökmetoder och avgränsningar. Detta steg kunde vid behov göras iterativt beroende på typen av studie och möjlighet inkluderades för att gå tillbaka till planeringsstadiet beroende på resultaten av sökningarna. I denna fas utfördes viss analys för att avgöra om en funnen källa var relevant.
- I analysfasen extraherades och analyserades den data som hämtats. Denna data låg till grund för resultatet i denna uppsats, det vill säga de stödda faktorerna och deras definitioner av den data som hämtades från artiklarna.

3.4.1. Planering

För planeringsfasen rekommenderar Okoli (2015) att ett protokoll skapas för att säkerställa att sökning och analys sker på samma sätt mellan gruppmedlemmar. Detta gjordes genom att studiens definition för omfattning och metod valdes baserat på Brockes m.fl. (2015) ramverk (*Process*, *Källor*, *Omfattning* och *Tekniker)*.

- **Process:** En sekventiell process valdes; vilket innebär att sökningen utförs i början av processen. Detta istället för att modifiera sökningen under dess utförande beroende på initiala resultat, då artiklarnas resultat inte förväntades leda till förändrad sökmetod.
- **Källor:** Brocke m.fl. (2015) rekommenderar tre metoder för att söka källor, *citationsindexeringstjänster*, *bibliografiska databaser* och *publikationer*. Den typ av källor som valdes var *bibliografiska databaser*, delvis för att standardisera resultat och delvis för att kunna erhålla resultat från en större mängd journaler. Då kriterierna dessutom var baserade på artiklarnas innehåll snarare än vilken journal den publicerats i eller vilka som citerat källan valdes databaser som metod. Att söka i citationsindexeringstjänster eller specifika publikationer valdes bort av samma anledning, dock inte för att de anses ogiltiga.
- **Omfattning:** Målet för studiens omfattning var att vara representativ och analysera varje källa i sökningen. För att exkludera irrelevanta artiklar användes strikta sökord och kriterier. Att undersöka inflytelserika artiklar var en annan potentiell omfattning (vom Brocke et al., 2015) som övervägdes, en artikels inflytelse ansågs dock inte nödvändigtvis påverka dess relevans i denna sökning. Det ansågs vara mer relevant hur en artikel definierade och mätte faktorer.

- **Tekniker:** Nyckelordssökning användes som sökteknik. Att söka framåt eller bakåt i citeringar utifrån en eller flera relevanta artiklar, så kallad framåt- eller bakåt-sökning (vom Brocke et al., 2015) eller "snowballing" ansågs vara mindre effektiv för att inhämta artiklar från olika kontext. Det var därför mindre relevant att följa vilka artiklar som refererade till varandra.

Litteraturstudien använde sig av systematisk överblick (Kitchenham, 2004) för att identifiera artiklar som empiriskt stödjer faktorer i andra kontext än de Moody m.fl. (2018) använde och på så vis besvara forskningsfrågan: *Vilka faktorer kan vara aktuella för en framtida utökning av UMISPC-modellen?*. Målet med studien var att täcka ett stort antal empiriskt testade modeller inom så många kontext som möjligt som avser att samla faktorer som påverkar säkerhetsbeteende.

En faktor är relevant om den enligt dess definition avser samma faktor som en av de faktorer som Moody m.fl. (2018) definierar. Eftersom Moodys m.fl. (2018) Studie 2 använde en kvantitativ metod för att mäta samband, undersöker denna uppsats enbart studier som mäter samband med liknande kvantitativa metoder. Faktorns samband till säkerhetsbeteende behöver även ha kunnat stödjas på ett liknande kvantitativt sätt som Moodys m.fl. (2018) metod. En faktor som identifierats med en annan metod (kvantitativ eller kvalitativ) kunde potentiellt vara av relevans för tillägg till modellen förutsatt att den har en påverkan på säkerhetsbeteende. Däremot skulle faktorn utifrån det inte kunna påstås uppfylla motsvarande Moodys m.fl. (2018) kriterier för inkludering; vilket var ett krav vi ställde för denna uppsats.

För att motsvara Moody m.fl. (2018) kriterier valdes en begränsning på att enbart inkludera faktorer vars samband kunde stödjas med ett *p-värde* på 0.05 eller lägre. Oates (2006) beskriver att 95% kan användas som acceptansnivå. Ett resultat med *p-värde* lägre än 0.05 betyder att det är statistiskt säkerställt med över 95% sannolikhet att resultatet överensstämmer med verkligheten, snarare än att vara felaktigt på grund av slumpmässig variation. Moody m.fl. (2018) nämner att de hittar stöd med $p < 0.001$ för de faktorer som inkluderas i UMISPC-modellen men definierar inte något gränsvärde i deras studie. Ett *p-värde* lägre än 0.001 innebär en sannolikhet över 99.9%.

3.4.2. Datainsamling

Artiklar som inkluderades i sökresultaten behövde uppfylla följande kriterier för att inkluderas i analysfasen:

- Publicerad i en vetenskaplig journal.
- Skriven på engelska.
- Genomgått kollegial granskning.
- Studerat faktorer i en annan kontext än Moody m.fl.
- Presenterar en modell för faktorer som påverkar en individs säkerhetsbeteende inom informationssäkerhet, inom ett företag, en organisation eller privat.
- Modellen ska vara kvantitativt testad genom en empirisk studie och ha funnit stöd för att någon eller några av sina presenterade faktorer påverkar individers säkerhetsbeteende. Med ett *p-värde* på 0.05 eller lägre.

Sammanfattningsvis så lästes hela innehållet i de artiklar som hade relevanta titlar och sammanfattningar. Om det däremot var tydligt att artikeln inte uppfyllde de kriterier som etablerades ovan så exkluderades den.

Kriterierna skapades för att öka studiens transparens och för att bidra med riktlinjer under urvalsprocessen. Genom att ha objektiva riktlinjer för inkludering förväntades inkludering av artiklar bli mer konsistent oavsett vem som genomförde analysen och därmed förbättra studiens reproducerbarhet.

Då sekventiell metod valdes så utfördes hela sökningen och urval av artiklar samtidigt i början av processen istället för att uppdatera söklistan löpande under studien (vom Brocke et al., 2015). När alla relevanta artiklar valts ut påbörjades analysfasen där faktorer extraherades och analyserades med mål att besvara forskningsfrågan. Detta motsvarar steg tre till fem i Xiao och Watsons (2019) beskrivning av en systematisk process:
Sökning av litteratur och *Filtrera för inkludering,* där titel och sammanfattningar lästes för att ta reda på om artikeln uppfyller datainsamlingens kriterier.
Bedömning av kvalitet, där hela artikelns text övervägs för att försäkra att artikeln är relevant. Snyder (2019) nämner också att läsning av abstrakt och urval kan utföras innan resten av texten läses.

Oavsett om artiklar avser att empiriskt testa modeller i form av *förändrat säkerhetsbeteende* eller i form av *efterlevnad av säkerhetspolicy* finns ofta en liknande struktur av faktorer. Då *efterlevnad av riktlinjer* dessutom kan vara en del av vad som definieras som säkerhetsbeteende (Ng m.fl. 2009; Moody m.fl. 2018; D'Arcy and Lowry. 2019) ansågs det att modeller var jämförbara oavsett om de avser mäta *förändrat säkerhetsbeteende* eller *efterlevnad av riktlinjer*.

En sökprofil utformades för att hitta avgränsad och relevant litteratur till forskningsämnet. Den ursprungliga sökprofilen *"Security" AND ("Behaviour" OR "Compliance") AND "Factors"* resulterade i en för bred sökning. Istället användes en avsmalnad och modifierad version av Sommestad m.fl. (2014) sökprofil.

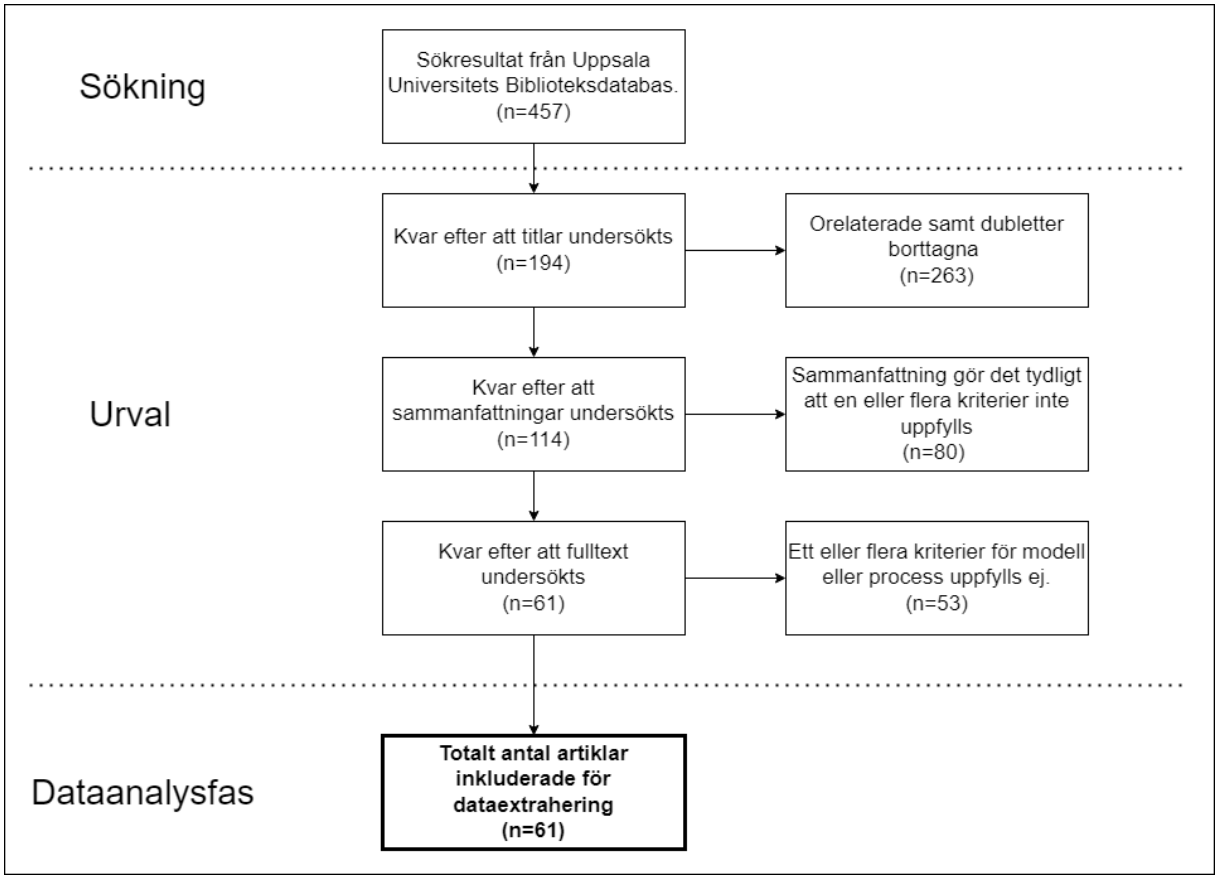
Sökprofilen som användes var: *("employee" OR "employees" OR "user" OR "users" OR "staff") AND ("security behavior" OR "security behaviour" OR "security behavioural" OR "security behavioural") AND ("policy" OR "factor" OR "construct")*. Enbart artiklar på engelska valdes, detta för att få ett så brett urval av olika kontext som möjligt.

Studien använde Uppsala Universitetsbiblioteks söktjänst för att framställa samlingen med artiklar. Söktjänsten har möjlighet att filtrera sökningen enligt önskade egenskaper. Resultat filtrerades med hjälp av dessa inställningar vilket gjorde att antalet resultat som inte uppfyllde vissa kriterier kunde uteslutas automatiskt. Följande inställningar användes i söktjänsten:

- Enbart resultat som genomgått kollegial granskning.
- Enbart tidskriftsartiklar.
- Enbart artiklar skrivna på engelska.
- Enbart artiklar inom "*Computer science*".

Då "*Information systems*" ej var ett alternativ för filtrering i söktjänsten och då Moodys m.fl. (2018) artikel klassificerades som "*Computer science*" valdes denna disciplin som filtrering i söktjänsten då studien är fokuserad på systemanvändare inom olika typer av IT system, samt då den typ av studie som undersöks ofta klassificeras som "*Computer science*" i söktjänsten. Denna avgränsning gav ett rimligt antal artiklar att undersöka. Denna typ av interaktion mellan människor och datorsystem ansågs ingå i disciplinen informationssystem, vilket söktjänsten inkluderar som en del av disciplinen "*Computer science*".

Figur 3.1 visualiserar datainsamlingsprocessen utifrån sökresultaten.



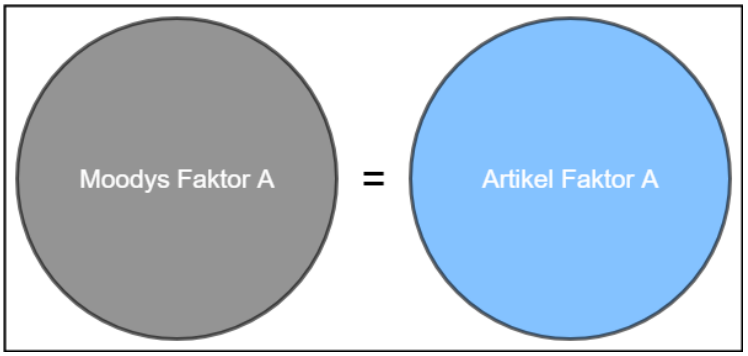
Figur 3.1. *Datainsamlingsprocessen. Baserad på Xiao och Watson* (2019)

3.4.3. Dataanalys

Innehållsanalys kan enligt Denscombe (2010) utföras på alla typer av texter för att dela in dess innehåll i kategorier genom att kategorisera in delar från texten och att sedan räkna enheternas frekvens. Den del av analysprocessen som var mest relevant för denna uppsats är deras Steg 4: "*Koda enheterna i linjer med kategorierna*". Kategorierna är i detta fall de faktorer som påverkar individers säkerhetsbeteende medan enheterna är definitionerna i de olika artiklarna. Genom att jämföra definitionerna kan faktorerna kategoriseras utifrån de definitioner som Moody m.fl. (2018) använder.

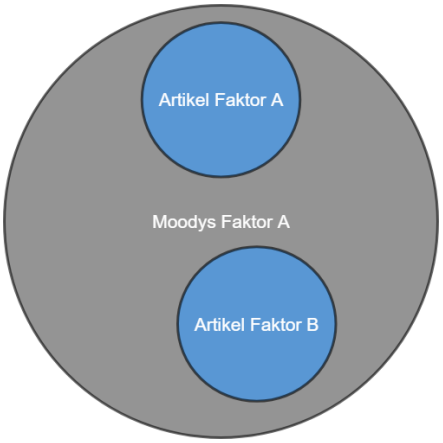
Snyder (2019) skriver att dataanalysfasen bör utföras enligt syfte och forskningsfråga vilket gör att analysmetoden varierar mellan studier. Forskningsfrågan för denna uppsats avser att undersöka vilka faktorers påverkan på säkerhetsbeteende kunde stödjas, inte till vilken grad de påverkar säkerhetsbeteendet. För att uppnå hög reproducerbarhet skapades följande riktlinjer:

- En faktor som undersöks av en artikel noterades och dess definition identifierades för att jämföra faktorn med Moodys m.fl. (2018) definitioner.
- En faktor jämförs alltid med Moodys m.fl. (2018) definitioner, även om de har samma namn.
- En artikels definition av en faktor jämförs med Moodys m.fl. (2018) definition av faktorer. Refererar artikels definition till samma faktor som Moodys m.fl. (2018) definition så klassificeras faktorn därav. (Figur 3.2.)



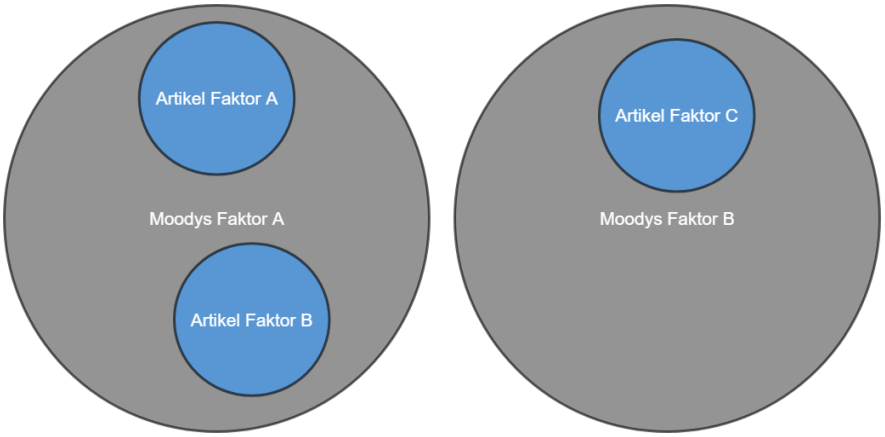
Figur 3.2.

- Om två faktorer från en artikel båda går att klassificera som samma faktor enligt en av Moodys m.fl. definitioner så klassificeras båda faktorer som samma typ. (Figur 3.3.)



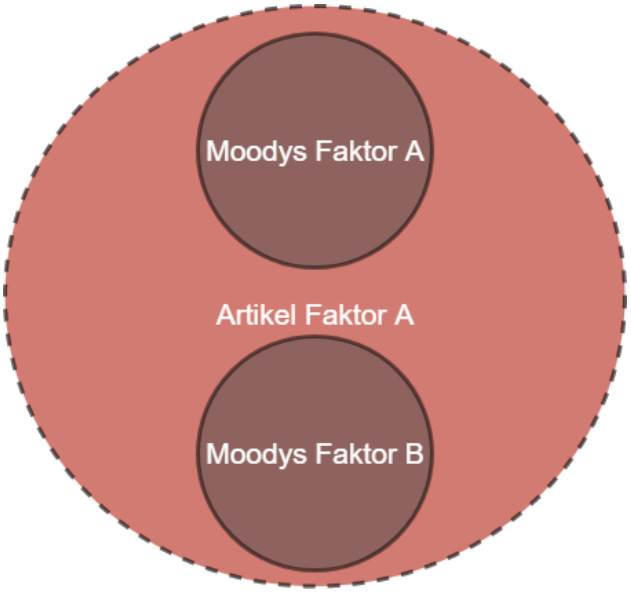
Figur 3.3.

- En faktor som kunde klassificeras som en underkategori av någon av Moodys m.fl. (2018) definierade faktorer klassificeras som den faktorn. (Figur 3.4.)



Figur 3.4.

- I händelse av att en artikel definierar en faktor som täcker mer än en av Moodys m.fl. (2018) definitioner klassificeras faktorn inte som någon av dem, detta på grund av att den faller utanför de två definitionernas avgränsningar. (Figur 3.5.) Det samma gäller om faktorn enbart inkluderar en av Moodys m.fl. faktorer som underfaktor.



Figur 3.5.

Då artiklarna presenterar deras undersökta faktorer som en del av deras resultat och som regel i listform så kunde faktorerna och deras definitioner extraheras. På dessa utfördes en kvalitativ analys för att avgöra om en funnen faktor syftade på samma faktor som någon av de Moody m.fl. (2018) definierar. Till grund för denna analys användes definitioner hämtade från Moodys m.fl. (2018) artikel samt den analysmetod som beskrivs ovan. Tabell 3.1. listar de faktorer som inkluderades i UMISPC-modellen. Tabell 3.2. inkluderar de faktorer som inte kunde stödjas i deras undersökning. Tabellerna är översatta till svenska.

Okoli (2015) rekommenderar även att använda formulär som kan lagra information om artiklarna och som har ett fält för allmänna kommentarer som ett verktyg under extrahering av data. Detta för att i senare steg kunna sammanställa denna information som en del av framställningen av resultatet. För detta syfte användes *Google Sheets* där de olika faktorerna och deras klassificering noterades. Kontextet för varje artikels studie hämtades även ut på detta sätt, detta inkluderar antalet respondenter och vilka typer av individer och/eller företag som tillfrågades.

Tabell 3.1. *Moodys m.fl.* (2018) *lista med definition av faktorer de fann stöd för i sin studie. Källa: Moody m.fl.* (2018).

Faktor	**Definition**
Respons Effektivitet	Den upplevda effektiviteten av beteendet för att minska eller undvika det upplevda hotet.
Hot	Upplevd allvarlighet av och sårbarhet till en upplevd potentiell skada.
Vanor	En vanlig tendens som inte kräver medvetna tankar för att följa informationssäkerhetspolicyn.
Roll Värderingar	Den krävda handlingen för att följa informationssäkerhetspolicyn är lämplig, motiverad och acceptabel, med tanke på den typ av arbete och uppgiften personen utför.
Rädsla	Negativt känslomässigt respons på stimulering.
Neutralisering	Rationaliserat tänkande som tillåter individen att rättfärdiga avvikelser mot avsikt till efterlevnad.
Intention	Benägenheten att ägna sig åt ett visst beteende.
Reaktans	Förnekande om att det finns ett informationssäkerhetsproblem.

Tabell 3.2. *Moodys m.fl.* (2018) *lista med definition av faktorer de föreslog men ej fann stöd för i sin studie. Källa: Moody m.fl.* (2018).

Faktor	**Definition**
Sociala Faktorer	Det summativa inflytandet som upplevs av en individ utifrån sociala normer, roller inom gruppen och individens självuppfattning relevant för gruppen.
Belöningar/Kostnader	Positiv förstärkning som upplevs vid följande av säkerhetsriktlinjer.
Bestraffningar	Negativ förstärkning som upplevs om individen upptäcks bryta mot säkerhetsriktlinjer.

Underlättande Förhållanden	Möjligheten för individens efterlevnad utan hjälp från andra.

3.5. Kvalitet i genomförande

Nackdelarna med litteraturbaserad forskning är primärt källornas trovärdighet (Denscombe, 2010; Oates, 2006) och därför valdes enbart källor som genomgått kollegial granskning. En annan nackdel enligt Denscombe (2010) och Oates (2006) är att sekundärdata ofta är skapad med andra mål. Detta ansågs inte vara ett problem då de tidigare studierna haft som mål att mäta påverkande faktorer till säkerhetsbeteende vilket var vad som gjorde dem relevanta i urvalsprocessen i denna uppsats.

Studien följde den europeiska kodexen för forskningens integritet. Den europeiska kodexen nämner fyra huvudkrav: *Tillförlitlighet*, *Ärlighet*, *Respekt* och *Ansvarighet*. Detta innebär att författarna säkerställer forskningens kvalitet, är öppna och rapporterar om forskning på ett öppet, rättvist, fullständigt och objektivt sätt, samt ansvarar för forskningen under hela arbetsprocessen (ALLEA, 2018). För att uppfylla dessa krav dokumenterades de val som gjordes under forskningsprocessen i stycke 3.4.2. och 3.4.3. samt i Figur 3.1 med mål att öka transparens.

3.6. Forskningsetiska överväganden

Studien följer Vetenskapsrådets (2002) principer. Eftersom litteraturstudien undersökte tidigare studier fanns etiska aspekter. Det var möjligt att den information som samlats in av andra forskare under framtagningen av deras modell var känslig på något sätt, i detta fall var informationen redan tillgänglig genom sökning i akademiska databaser och ansågs därför redan allmänt tillgänglig. Den data som analyserades och presenterades i studien förväntades inte vara av känslig karaktär för någon av de inblandade. I händelse av att sammanställning av data skulle uppdaga något som kunde vara skadligt för påverkade parter som exempelvis respondenter eller forskare i originalstudierna var det möjligt att en viss studie uteslöts från resultatet efter en djupare etisk avvägning där potentiell skada kontra fördelar undersöktes. Ingen sådan situation uppstod dock under projektet.

Den data som presenteras i uppsatsen härstammar endast från källor som är tillgängliga via den använda söktjänsten eller direkt hämtade från dess författare via förfrågan. Alla artiklar i denna uppsats anses därför vara etiskt inhämtade.

Det är viktigt att alla resultat i denna litteraturstudie redovisas och att både resultat som stödjer och inte stödjer författarnas hypotes ingår (Forsberg and Wengström, 2013). Denna studie har inte heller medvetet plagierat, förvrängt eller uteslutit fakta.

4. Resultat och analys

I detta kapitel presenteras och analyseras resultaten av litteratursökningen. Tabellen med resultat sammanfattas i detta avsnitt och de olika typerna av faktorer som artiklarna innehåller beskrivs.

4.1. Sökresultat.

Söktermerna gav totalt 457 träffar varav 61 bedömdes som relevanta efter att kriterierna från Kapitel 3.4. applicerades. Dessa artiklar presenterar någon form av modell för vilka faktorer som påverkar en individs säkerhetsbeteende.

Även om modellerna kan anses vara jämförbara finns en del skillnader, vissa undersöker allmänt säkerhetsbeteende medan andra undersöker efterlevnad av riktlinjer. Vissa använder teorier som Moody m.fl. (2018) utgår ifrån och vissa använder andra teorier, vanligast är *Protection Motivation Theory* skapad av Rogers (1975). Artiklarnas kontext är varierande, de undersöker både privata individer och anställda på företag, individer från olika länder och med olika storlekar på respondentgrupper (som lägst 70, som högst 4153).

Tidigt i sökningen blev det tydligt att faktorn *Självförmåga* var vanligt förekommande i artiklarna. Denna faktor fann Moody m.fl. (2018) inte stöd för i sin inledande studie och den exkluderades ur deras modell. De ger dock en definition baserad på Rogers (1975) vilket gör att faktorn utifrån den definitionen ansågs lämplig att undersöka i denna studie. Denna definition presenteras i Tabell 4.1.

Tabell 4.1. *Definition på faktorn Självförmåga. Källa: Moody m.fl.* (2018).

Faktor	**Definition**
Självförmåga	Individens egna förmåga att genomföra det tänkta beteendet på ett framgångsrikt sätt.

Tre kategorier av faktorer identifierades efter kategoriseringen:

- Faktorer som definieras av Moody m.fl. (2018) men de inte själva finner stöd för. (*Sociala Faktorer*, *Belöningar/Kostnader*, *Bestraffningar*, *Möjliggörande Förhållanden* och *Självförmåga*)
- Faktorer som redan inkluderas i UMISPC-modellen (*Respons Effektivitet*, *Roll Värderingar*, *Neutralisering*, etc.)
- Faktorer som inte definieras av Moody m.fl. (2018). (*Ålder*, *Personlighetstyp*, *Utbildningsnivå*, etc.)

Den förstnämnda kategorin är av intresse för att besvara forskningsfrågan. Den andra kategorin, de faktorer som redan ingår i UMISPC kunde användas för att stödja eller motsäga Moodys m.fl. (2018) resultat. Den tredje kategorin är inte av relevans för tillägg i UMISPC-modellen då Moodys m.fl. (2018) studie inte undersöker dessa. Att identifiera helt nya faktorer för tillägg till UMISPC-modellen ligger utanför denna studies begränsningar.

De första två kategorierna av faktorer och vilka artiklar som innehåller dem presenteras i tabell 4.2. Tabellen representerar enbart faktorer som definieras av Moody men som de inte finner stöd för, samt faktorer som redan inkluderas i UMISPC-modellen. Faktorer som stöds är markerade med "X". Faktorer som testas men ej kunde stödjas är markerade med "—". Om artikeln stödjer en underkategori av en faktor men inte en annan underkategori markeras detta med "X / —".

Tabell 4.2. *Resultat av dataextrahering (innehållsanalys) från relevanta artiklar i sökningen.*
Förkortningar: ***FaCo:*** *Underlättande Förhållanden,* ***SoFc:*** *Sociala Faktorer,* ***Re/Co:*** *Belöningar/Kostnader,* ***Pu:*** *Bestraffningar,* ***Se-ef:*** *Självförmåga,* ***ReEf:*** *Respons Effektivitet,* ***Th:*** *Hot,* ***Ha:*** *Vanor,* ***RoVa:*** *Roll Värderingar,* ***Fe:*** *Rädsla,* ***Ne:*** *Neutralisering,* ***In:*** *Intention,* ***Re:*** *Reaktans.*

Artikel	FaCo	SoFc	Re/Co	Pu	Se-ef	ReEf	Th	Ha	RoVa	Fe	Ne	In	Re
(Ahmad et al., 2019)		X	X		X								
(Aigbefo et al., 2022)		X				X	—					X	
(Arachchilage and Love, 2014)					X								
(Aurigemma and Mattson, 2017)		X		X	X								
(Aurigemma and Mattson, 2019)		X	X		X							X	
(Balozian et al., 2019)				—		X							
(Bax et al., 2021)			X		X	X	X						
(Boehmer et al., 2015)			X / —		X	X	X / —		X		X		
(Chen et al., 2018)	X		—	—	X								
(Chou and Chou, 2016)					X	—	X						
(Claar and Johnson, 2012)			X		X	—	X / —						
(Cox, 2012)	X	X			X		X / —		X			X	
(Crossler and Bélanger, 2014)					X	X	X						
(Cuganesan et al., 2018)	X	X	—	—									
(Davis et al., 2021)	X	X							X				
(Deutrom et al., 2021)													
(Dodel and Mesch, 2019)			X		X	X	X						
(Gillam and Waite, 2021)			X		X	X	X / —					X	
(Guan and Hsu, 2020)				X									
(Hanus and Wu, 2016)					X	X	—		X				
(Hanus et al., 2018)			—		X	X	X		X				
(Herath and Rao, 2009a)		X		X		X							
(Herath and Rao, 2009b)	X	X		—	X	—	—					X / —	
(Hong and Furnell, 2022)	X	X			X								
(Hooper and Blunt, 2020)		—	—	—	X	—	X / —						
(Hwang et al., 2017)	X	X	X							X			
(Hwang et al., 2021)	X	X											
(Ifinedo, 2016)	X			X									
(Johnston and Warkentin, 2010)		X			X	X	X / —						
(Kajtazi et al., 2018)											X		
(Khan and AlShare, 2019)	X	X	—	X					X				
(Kim et al., 2020)	X			X									
(Koohang et al., 2020)	X				X		X					X	
(Koohang et al., 2020)	X								X				
(Lankton et al., 2019)		X							X / —				

(Lee and Kim, 2022)							X						
(Li et al., 2019)													
(Lian, 2021)			X / —		X	X	X						
(Ma, 2022)	—	X	X		X		X			X		X	
(Menard et al., 2014)			X				X						
(Menard et al., 2017)	X				—	X	—		—	—		X	
(Myyry et al., 2009)													
(Nasir et al., 2019)		X			X							X	
(Nasirpouri Shadbad & Biros, 2021)	X												
(Ng et al., 2021)		X	X		X	X	X			X	X		
(Nord et al., 2022)	X								X				
(Ogbanufe et al., 2021)	X								X				
(Posey et al., 2015)	X		X / —		X	X	X			—			
(Solomon and Brown, 2021)	X / —												
(Sommestad et al., 2019)	X		X		X		X		X				
(Tesleem and Tryfonas, 2017)				—		—	X				X / —		
(Torten et al., 2018)	X				X	X	X / —		X				
(Vafaei-Zadeh et al., 2019)		X	X		X								
(Warkentin et al., 2011)	X	X			X								
(White et al., 2017)	X		X		X								
(Wiafe et al., 2020)		X										X	
(Xu and Guo, 2019)							X		X				
(Yang and Lee, 2016)					X	X	X						
(Yazdanmehr and Wang, 2021)	X	X											
(Yoon et al., 2012)		—	X		X	X	—	X		X		X	
(Zhen et al., 2021)			X						X		X		
Stödda total	**23**	**22**	**15**	**6**	**32**	**18**	**16**	**1**	**13**	**4**	**4**	**10**	**0**
Testade, ej stödda total	**1**	**2**	**5**	**6**	**1**	**5**	**5**	**0**	**1**	**2**	**0**	**0**	**0**
Blandade resultat	**1**	**0**	**3**	**0**	**0**	**0**	**7**	**0**	**1**	**0**	**1**	**1**	**0**
Total	**25**	**24**	**23**	**12**	**33**	**23**	**28**	**1**	**15**	**6**	**5**	**11**	**0**

4.2. Faktorer som uteslöts ur UMISPC-modellen

I detta avsnitt presenteras resultatet av litteratursökningen för faktorer som Moody m.fl. (2018) inte fann stöd för. Avsnittet sammanfattar resultatet och presenterar skillnader mellan artiklar och definitioner.

4.2.1. Underlättande Förhållanden

Underlättande Förhållanden hittades stöd för i 23 studier. En studie fann inte stöd för faktorn. En studie kom fram till blandade resultat. Faktorer från artiklarna som klassificerades som *Underlättande Förhållanden* är relaterade till utbildning av individen (Hwang et al., 2021; Posey et al., 2015; White et al., 2017), tekniskt stöd från organisationen/ledning (Cuganesan et al., 2018; Ifinedo, 2016; Ogbanufe et al., 2021). Faktorn inkluderar även tillgängligheten av information om riktlinjer (Herath and Rao, 2009b), detta inkluderar material för utbildning.

Menard m.fl. (2017) påpekar att deras faktor "*Upplevd Kompetens*", vilken klassas som *Underlättande Förhållanden* är konceptuellt lik *Självförmåga*. *Upplevd Kompetens* klassificerades som *Underlättande Förhållanden* trots att det är en egenskap hos individen då faktorn beskriver en bakgrund till utövande av en uppgift, snarare än själva utövandet. De väljer att skilja på faktorerna då *Upplevd Kompetens* täcker individens upplevda förmåga inom en hel domän snarare än individuella uppgifter. De spekulerar dock att de två koncepten är närliggande och kan ha en påverkan mellan varandra, vilket deras resultat även finner stöd för med $p < 0.001$.

Ma (2022) undersökte, men fann inte stöd för *Underlättande Förhållanden*. Deras studie innehöll 804 respondenter från kinesiska IT-organisationer. Deras faktor *Upplevd Beteendekontroll* (författarnas översättning) definieras som hur lätt eller svårt individen upplever utförandet av en uppgift att vara. Notera att denna faktor inte klassificerades som *Självförmåga* då *Upplevd Beteendekontroll* definieras av situationens egenskaper istället för individens. De spekulerar över att detta går emot resultat av tidigare forskning och att det kan bero på att faktorn kan variera beroende på individers upplevelse av en uppgift. Just *Upplevd Beteendekontroll* är en faktor som även Cox (2012) undersöker. I deras studie stödjer de däremot faktorns påverkan, både på avsikt till säkerhetsbeteende och faktiskt utfört säkerhetsbeteende.

Solomon och Brown (2021) kunde både finna stöd för och inte finna stöd för faktorn. Detta beror på att två av deras faktorer klassificerades som *Underlättande Förhållanden*. Deras studie tillfrågade 74 anställda i Sydafrika inom företag som hade en policy för informationssäkerhet. Deras studie undersöker hur organisationens kultur påverkar individen och finner stöd för att *Målinriktning* påverkar individens säkerhetsbeteende, men inte *Regelinriktning*. Baserat på deras definitioner av de två faktorerna är det viktigare att individen upplever att deras arbete gynnar de mål organisationen satt upp än att regler finns lättillgängliga och tydligt nedskrivna. Solomon och Brown (2021) är förvånade av bristen av inflytande av *Regelinriktning* och spekulerar i att den kan ha en indirekt påverkan via andra faktorer.

4.2.2. Sociala Faktorer

Av de 24 artiklar som undersökte en faktor som klassificerades som *Sociala Faktorer* fann 22 artiklar stöd för faktorn medan två inte fann stöd. Bland dessa var faktorn *Subjektiva Normer* vanligt förekommande vilken definieras som individens upplevelse av andra (ofta någon individen ser upp till) personers handlingar och åsikter om ett visst säkerhetsbeteende (Ahmad et al., 2019; Aigbefo et al., 2022). Andra faktorer har liknande definitioner som *Sociala Normer* men med andra namn, såsom *Kamraters Beteende* (Herath and Rao, 2009a), *Socialt Inflytande* (Johnston and Warkentin, 2010). Dessa definitioner faller under Moodys m.fl. (2018) definition av *Sociala Faktorer*, men är enbart en underkategori då Moodys m.fl. (2018) definition är något bredare och inkluderar flera sociala aspekter som individens förhållande till gruppen.

Yoon m.fl. (2012) och Hooper and Blunt (2020) fann inte stöd för *Sociala Faktorer*. Yoon m.fl. (2012) undersökte *Subjektiva Normer* men hittade inte någon signifikant inverkan på studenters avsikter att följa säkerhetsriktlinjer. Deras definition av *Subjektiva Normer* är "*En elevs tro på omfattningen av godkännande från vänner, kamrater eller familj för hans eller hennes beteende inom informationssäkerhet*" och menar på att resultatet antyder att informationssäkerheten inte är lika etablerad hos yngre vuxna. Hooper and Blunt (2020) undersökte faktorn *Sociala Normer* och definierade den som "*Beteendestandard som individer känner sig skyldiga att följa*". De utförde studien på IT-anställda och menar på att resultatet kan bero på att IT-anställda är mer kunniga och säkra på sina egna förmågor och upplever att de inte behöver råd från andra kollegor.

4.2.3. Belöningar/Kostnader

Belöningar/Kostnader hittades stöd för i 15 artiklar, medan fyra inte fann stöd. Tre av artiklarna fick blandade resultat. Av de artiklar som testade men inte fann stöd för *Belöningar/Kostnader* undersökte alla säkerhetsbeteende hos anställda inom olika typer av organisationer. Bland de artiklar vars resultat stöder faktorn undersöks både privat användande och användande inom företag.

Belöningar/Kostnader kan innebära att spara/förlora tid eller pengar (Claar and Johnson, 2012; Vafaei-Zadeh et al., 2019), att en viss uppgift är opraktisk att utföra (Ahmad et al., 2019), eller att andra barrier förhindrar ett visst säkerhetsbeteende (White et al., 2017). Bland studierna så undersöks belöningar och kostnader av säkerhetsbeteende, men även belöningar och kostnader av att *inte* handla på ett säkert sätt, exempelvis finansiella belöningar som utlovas av ett bluffmejl (Bax et al., 2021). Moody m.fl. (2018) specificerar positiv förstärkning i sin artikel, men för denna uppsats syften ansågs negativ förstärkning vara detsamma som brist på positiv förstärkning och vice versa, vilket gjorde att alla faktorer som hanterade dem klassificerade som samma kategori. Denna faktor skiljer sig från faktorn *Bestraffningar* då en kostnad är separat från eventuella sanktioner som individen får på grund av brott mot riktlinjer, även om både en kostnad och en sanktion kan vara av finansiell karaktär. Belöningar skiljer sig från *Respons Effektivitet* då de inkluderar fördelar orelaterade till hur effektiv en viss åtgärd är för att förhindra ett hot.

Faktorn delas in i olika typer av belöningar och kostnader av vissa artiklar. Clay m.fl. (2015) definierar "*Interna-*" och "*Externa Missanpassade Belöningar"* (författarnas översättning). Termen *Interna* definieras av dem som personlig tillfredsställelse som uppkommer utifrån resultat av inte följa riktlinjer. Medan *Externa* kan inkludera finansiella bidrag av att

exempelvis sälja känslig information till utomstående. Att belöningarna anses som missanpassade är ett koncept hämtat från *Protection Motivation Theory* och är den typ av belöningar individen får av bristande säkerhetsbeteende. Clay m.fl. (2015) finner enbart stöd för *Interna Missanpassade Belöningar*. Även Ng m.fl. (2021) har *Missanpassade Belöningar* som en av deras faktorer och finner stöd för dess påverkan på säkerhetsbeteende. Deras definition inkluderar dock även den tid och arbete som sparas av att inte utföra ett visst säkerhetsbeteende. Lian (2021) undersöker specifikt säkerhetsbeteende för medhavda enheter (Även kallat *BYOD* eller "*Bring Your Own Device*") och inkluderar faktorerna *Upplevd Användbarhet, Påverkan på Systemprestanda, Upplevd Kostnad* och *Upplevda Barriärer.* Av dessa faktorer fann de stöd för alla förutom *Upplevda Barriärer*, vilken definieras som aspekter av säkerhetsbeteendet som är opraktiska, tidskrävande och/eller innebär en förändring i vanor. Det vill säga den typ av barriärer som flera andra artiklar finner stöd för. Lian (2021) var den enda av artiklarna som fokuserade på medhavda enheter.

4.2.4. Bestraffningar

Bestraffningar undersöktes av 12 studier. Sex av dessa kunde stödja det som en påverkande faktor. Resterande sex kunde inte hitta signifikant stöd. Denna jämna fördelning överensstämmer med Moodys m.fl. (2018) diskussion om att bestraffningar och belöningar har givit varierande resultat i tidigare studier. Artiklarna studerar framförallt *faktisk allvarlighet* och *upplevd allvarlighetsgrad* av straffet.

Guan och Hsu (2020) och Aurigemma och Mattson (2017) fann stöd för faktorn. Guan och Hsu (2020) skriver att stränga bestraffningar kan påverka anställda med lågt organisatoriskt engagemang. Detta innebär att stränga bestraffningar kan avskräcka anställdas avsikter att inte följa riktlinjerna för personer med lågt engagemang. Aurigemma och Mattson (2017) fann stöd för att strängare bestraffningar har en påverkan på individen, men att anställda med tidigare erfarenheter påverkas helt annorlunda. De menar att personer med tidigare erfarenheter kan förändra styrkan av och till och med invertera effekten av bestraffningarna. Även Khan och AlShare (2019, s. 18) finner stöd för faktorn och rekommenderar att "*Se över korrigerande åtgärder genom att höja straffet*" (författarnas översättning). Herath och Rao (2009a) hittade stöd som motsäger tidigare forskning samt deras egna hypotes. De hittade stöd för att stränga bestraffningar har en negativ inverkan på individens avsikt att följa säkerhetsriktlinjer. Herath och Rao (2009a) skriver att de tror att fram till den tidpunkt då en straffåtgärd som uppsägning införs så tror de att det är osannolikt att användarna tar det på allvar. De diskuterar även om det kanske har att göra med känslan av att påföljden inte gäller dem, vilket liknar Moodys m.fl. (2018) faktor *Neutralisering*.

Sex artiklar hittade inte stöd för faktorn. Hooper och Blunt (2020) menar på att det kan bero på att de undersökte *avsikten att följa informationssäkerheten* snarare än att *inte följa,* där påverkan enligt dem kan vara mer betydande. Chen m.fl. (2018) hittade inte stöd för faktorn och nämner att resultaten från deras studie både matchar och motsäger tidigare forskning samt att ett formellt straff spelar en mindre viktig roll än ett informellt straff.

4.2.5. Självförmåga

Totalt undersökte 33 artiklar *Självförmåga*. 32 av artiklarna fann stöd för att *Självförmåga* var en bidragande faktor för individers säkerhetsbeteende medan en artikel inte fann stöd. Menard

m.fl. (2017) och Hooper och Blunt (2020) nämner också att tidigare studier visat på att *Självförmåga* har stor påverkan på säkerhetsbeteende.

Den artikel som inte fann stöd för faktorn var Menard m.fl. (2017) som undersökte 547 privatpersoners villighet att installera lösenordshanterare. Deras resultat finner inte signifikans för en koppling mellan *Självförmåga* och intention att installera programvaran. I sin diskussion spekulerar de om att deras resultat kan bero på att många anställda är vana att installera och köra programvara på sina datorer vilket gör att *Självförmåga* har mindre påverkan. Deras spekulationer går i enlighet med Moodys m.fl. (2018) diskussion som spekulerar att deras scenarier inkluderade uppgifter som inte krävde en hög nivå av tekniskt kunnande.

De övriga 32 artiklarna som undersökt *Självförmåga* har alla kunnat stödja faktorns påverkan i olika kontext. Nasir m.fl. (2019) studerade universitetsstudenter och nämner att resultatet är i linje med tidigare studier, där *Självförmåga* är en av de påverkande faktorerna. Hooper och Blunt (2020) studerade IT-anställda och nämner också att deras studie stödjer tidigare studiers resultat. Även studier som har studerat flera olika organisationer och olika kontext som exempelvis Koohang m.fl. (2020), Hong och Furnell (2022) och Dodel och Mesch (2019).
Claar och Johnson (2012, s. 23) hittade stöd för faktorn och studerade den som "*privatpersoners förmåga att installera, konfigurera och upprätthålla ett program*" (författarnas översättning) och motsäger Menard m.fl. (2017) resultat.

Den vanligaste källan till faktorn *Självförmåga* var *Protection Motivation Theory* av Rogers (1975), ofta i kombination med en eller flera teorier. *Protection Motivation Theory* är en av de 11 teorier Moody m.fl. (2018) utgår från. Även *Theory of Planned Behavior* av Ajzen (1991) används av flera artiklar, då kallas faktorn *Upplevd Beteendekontroll*. Oavsett om en artikel utgått från *Protection Motivation Theory* och *Theory of Planned Behavior* är deras definitioner av *Självförmåga* likställbara enligt den metod som användes under denna uppsats. Herath och Rao (2009b, s. 111) skriver specifikt att "*Även om självförmåga antas vara en viktig faktor inom Protection Motivation, så har den även varit en viktig faktor inom Theory of Planned Behavior.*" (Författarnas översättning). Vidare delar de upp *Beteendekontroll* i två komponenter: *Tillgänglighet av resurser för att individen skall kunna utföra en uppgift* och *Individens förtroende för sin egen självförmåga att utföra uppgiften*. Detta går i linje med hur metoden för denna uppsats ledde till att faktorn *Upplevd Beteendekontroll* klassificerades som *Underlättande Förhållanden* eller *Självförmåga* beroende på om definitionen i respektive artikel fokuserat på situationens egenskaper eller individens.

4.2.6. Analys

Att faktorerna *Underlättande Förhållanden*, *Sociala Faktorer*, *Belöningar/Kostnader*, *Bestraffningar* och *Självförmåga* stöds i artiklarna kan betyda att dessa faktorer påverkar individers säkerhetsbeteende i andra kontext än de Moody m.fl. (2018) undersöker.

Underlättande Förhållanden och Sociala Faktorer
Moody m.fl. (2018) spekulerar om att *Underlättande Förhållanden* kan ha större inflytande inom mer tekniskt krävande uppgifter och de menar att *Sociala Faktorer* troligen har större inflytande i mer socialt synliga handlingar. *Underlättande Förhållanden* och *Sociala Faktorer* har båda en liknande fördelning av hur många studier som fann stöd eller ej, med en majoritet som finner stöd för ett samband mellan faktorn och individens säkerhetsbeteende. Detta

resultat går emot de resultat Moody m.fl. (2018) tar fram men går i linje med deras diskussion.

Belöningar/Kostnader
Moody m.fl. (2018) skriver att belöningar och avskräckande medel har haft olika resultat i tidigare forskning. Detta kan till viss del ses i resultaten för *Belöningar/Kostnader* då antalet artiklar som stödjer faktorns påverkan är något lägre än motsvarande för *Underlättande Förhållanden* och *Sociala Faktorer.* Dock finns en lutning åt att stödja faktorn bland artiklarna. De artiklar som inte fann stöd för *Belöningar/Kostnader* inkluderade enbart respondenter med anställda på företag, medan de artiklar som stöder faktorn inkluderade både privatpersoner och anställda. Resultaten tyder på att faktorn har påverkan i olika kontext, men kan ej användas för att påstå att faktorn inte har effekt på privatpersoner.

Bestraffningar
Bestraffningar undersöktes i en relativt liten mängd artiklar och resultatet visar på en jämn fördelning av studier som kunde och inte kunde stödja den. Flertalet artiklar nämner att strängheten av straffet påverkar signifikansen och faktorns påverkan på individen. De nämner även att faktorns påverkan på individen är betydligt mindre om det inte finns några exempel på personer som har straffats, detta stödjer Moodys m.fl. (2018) diskussion. Dessa kan vara en orsak till att resultatet i denna studie är varierande, eftersom individer har olika erfarenheter samt straffets stränghet beror på kontext.

Självförmåga
Då *Självförmåga* förekommer och stöds av en stor del av de utvalda studierna talar det emot Moody m.fl. (2018) resultat. Moody m.fl. (2018, s. 18) valde att inte inkludera individens egna uppfattning om sin förmåga i faktorn *Respons Effektivitet*, de menar att "*Eftersom vår datadrivna metod inte identifierade självförmåga, och allvarlighet och sårbarhet subsumeras under hot, inkluderade vi respons effektivitet som en förutsägelse för hot.*" (författarnas översättning). Faktorn *Respons Effektivitet* är istället fokuserad på åtgärdernas effektivitet att motverka hot. Dock var *Självförmåga* förekommande och stöds i flera artiklar, även artiklar som är grundade på olika teorier, vilket tyder på att faktorn faktiskt påverkar individens säkerhetsbeteende i flera olika kontext.

4.3. Inkluderade faktorer

Resultatet från denna studie stödjer resultaten från Moodys m.fl. (2018) studier till viss del. Det finns dock en stor variation i hur många studier som undersöker en viss faktor samt hur stor andel som inte finner stöd för den. Exempelvis *Hot* som undersökts i 34 artiklar, *Vanor* som endast inkluderas i en studie och *Reaktans* som inte inkluderades i någon studie.

Faktorn *Hot* var ofta uppdelat i flera underfaktorer, såsom *sårbarhet* och *allvarlighet* vilket går i linje med Moodys m.fl. (2018) definition. Däremot undersökte vissa artiklar troligheten att bli upptäckt vid brott mot riktlinjer, något som inte Moody m.fl. (2018) inkluderar. För denna uppsats ansågs troligheten att bli upptäckt vara separat från både *Hot* och *Bestraffningar* vilket gjorde att den inte klassificerades som någon av dem. Sex studier fick blandade resultat efter att ha undersökt flera underfaktorer till *Hot* vilket tyder på att det finns underfaktorer med olika påverkan inom faktorn.

Resultaten stödjer även till viss del inkluderingen av *Respons Effektivitet* och *Roll Värderingar* då fördelningen av resultat i artiklarna indikerar på faktorernas relevans. *Rädsla, Neutralisering* och *Intention* inkluderades i relativt få artiklar men var ändå fördelade mot att stödja faktorerna. *Vanor* och *Reaktans* studerades i minst antal artiklar.

5. Diskussion

I detta kapitel diskuteras de resultat som presenterades i Kapitel 4 och hur de uppfyller forskningsfrågan. Metoderna som användes i studien, dess begränsningar och hur de påverkat resultaten diskuteras även i detta kapitel.

5.1. Resultatdiskussion

De artiklar som undersöktes i analysfasen inkluderade faktorer från studier inom flera kontext, exempelvis olika typer av företag, individer och länder. Artiklarna undersökte faktorernas påverkan på ett sätt som ansågs vara jämförbart med den metod Moody m.fl. (2018) använde i sin andra studie. Flera av dessa studier finner stöd för samma faktorer som Moody m.fl. (2018) inkluderar i UMISPC-modellen vilket stödjer modellens val av faktorer. Det viktigaste för denna studie är att faktorer som Moody m.fl. (2018) inte fann stöd för kunde stödjas i andra studier.

Genom att undersöka liknande studier och vilka faktorer deras resultat stödjer har denna uppsats identifierat exempel på studier som finner stöd för de faktorer Moody m.fl. (2018) inte inkluderar i UMISPC-modellen. Detta behöver inte nödvändigtvis motstrida UMISPC-modellen då Moody m.fl. (2018) själva nämner att deras egna val av scenarier kan ha varit anledningen till att de inte fann stöd för vissa av sina faktorer. UMISPC-modellen är inte heller avsedd att vara en universell modell som kan appliceras på varje situation vilket gör att modellen kan vara korrekt även om varje faktor inte har en påverkan i varje kontext. Modellen avser dock att unifiera faktorer vars relevans kan stödjas. Vi anser att förekomsten av dessa faktorer i andra kontext är ett tecken på att de är lämpliga för vidare utvärdering, exempelvis genom framtida fallstudier eller undersökningar.

Resultatet av denna studie säger inte emot Moody m.fl. (2018) resultat. Samtliga faktorer, exklusive *Reaktans*, hittade stöd i minst ett annat kontext än det Moody m.fl. (2018) testade. Detta tyder på att de faktorer som inkluderas i UMISPC-modellen påverkar individer i minst ett annat kontext. Om flera artiklar finner stöd för en faktor än de som inte finner stöd för den tyder det på faktorns relevans för inkludering i UMISPC-modellen. Men att vissa faktorer såsom exempelvis *Bestraffningar* har artiklar vars resultat talar emot dess påverkan vilket indikerar på att andra testmetoder, organisationer, eller kulturer påverkar faktorns påverkningsgrad vilket även är något som Moody m.fl. (2018) nämner i sin diskussion. Det är möjligt att UMISPC-modellen bör anpassas vid praktisk applicering i en viss typ av organisation eller företag, exempelvis genom att inkludera eller exkludera någon av de faktorer som denna studie hittat stöd för. På vilket sätt faktorerna påverkar varandra och direkt påverkar säkerhetsbeteende är även något som eventuellt kan skilja sig mellan kontext men som inte undersökts i denna uppsats.

Att resultaten har så stor variation mellan olika studier talar även för att en universell modell eventuellt inte är lämplig då det finns så pass stor skillnad mellan kontext. Om en sådan modell skulle skapas skulle den behöva vara anpassningsbar nog att faktorer skulle kunna tas bort beroende på aktuellt kontext. Det kan även vara mer lämpligt att skapa en mer "lokal" modell för ett visst kontext där ovidkommande faktorer identifieras och filtreras bort.

Resultatet visar även att vissa studier "delar upp" faktorer, det vill säga att två faktorer i en studie ingår under samma faktor i UMISPC-modellen vilket kan anses som ett argument för

att faktorer i UMISPC-modellen kan separeras då det möjligtvis endast är en del av faktorn i fråga som faktiskt påverkar en individ. Detta kan minimera risken för att onödiga åtgärder utförs i praktiken som inte har någon påverkan på individens säkerhetsbeteende. Ett exempel på en faktor som möjligtvis skulle kunna separeras är *Hot* som både kan innehålla *Upplevd sårbarhet* och *Upplevd allvarlighet*.

5.1.1. UMISPC-modellens uteslutna faktorer

Moody m.fl. (2018) menar att deras val av scenarier kan vara anledningar till att vissa faktorer inte kunde stödjas i deras studie. Deras scenarion är situationer där handlingar är relativt osynliga för andra anställda samt där bestraffningar sällan delas ut. Handlingarna krävde inte heller högt tekniskt kunnande vilket kan ha varit en anledning till att faktorn *Självförmåga* inte upptäcktes i deras undersökning.

Varje faktor hade minst en studie som undersökte dess påverkan utan att finna stöd för dess påverkan, likt Moody m.fl. (2018). Detta anser vi betyda att varje faktor har ett eller flera kontext där den inte påverkar säkerhetsbeteende eller, mindre troligt, att dessa studier fått ett statistiskt ovanligt resultat. Resultaten tyder på att ingen av faktorerna har en universell påverkan på säkerhetsbeteende, även i de fall där faktorn påverkar säkerhetsbeteende i flera eller majoriteten av alla kontext.

Självförmåga
Den faktorn som flest studier kunde stödja bland de faktorer som Moody m.fl. (2018) inte hittade stöd för var *Självförmåga*. Bevis för dess påverkan har tagits fram i flera olika studier och kontext vilket motsäger Moodys m.fl. (2018) resultat. Detta indikerar att individens självförmåga kan påverka dess säkerhetsbeteende i de flesta kontext. Vilket då kan betyda att självförmåga uppfyller de krav som Moody m.fl. (2018) sätter för inkludering i UMISPC-modellen.

Vi anser att faktorn är lämplig att undersöka för att vidare fastslå hur den påverkar individens säkerhetsbeteende. Det är även möjligt att *Självförmåga* kan inkluderas som en underfaktor av andra faktorer då faktorn ofta beskrivs ha en koppling till andra faktorer.

Bestraffningar
Resultatet visar på att *Bestraffningar* kunde stödjas i hälften av studierna som studerade faktorn. Ett relativt lågt antal studier (12 av 61) undersökte denna typ av faktor vilket gör att urvalet är mindre i förhållande till de andra uteslutna faktorerna.

Den jämna fördelningen skiljer sig från de ojämna fördelningarna i övriga faktorer (med undantag av *Hot*). En möjlig anledning till detta är att Moodys m.fl. (2018) definition inkluderar både trolighet och allvarlighet av bestraffning, något som vissa av de funna artiklarna delar upp i separata faktorer (Son, 2011; Wang and Xu, 2021). En ytterligare analys av modellerna i denna uppsats skulle kunna undersöka vilka av dessa som finner att enbart sannolikhet för bestraffning är en faktor i förhållande till hur många som undersöker stränghet av bestraffning. Wang och Xu (2021) påvisar att det finns en skillnad i påverkan mellan troligheten av bestraffning och allvarligheten av bestraffning. Wang och Xu (2021) nämner även att vissa kulturer har en större maktskillnad mellan chefer och arbetare vilket de spekulerar kan påverka vikten av vissa faktorer. Denna typ av skillnader kan vara bidragande

till att Moody m.fl. (2018) inte fann stöd för *Bestraffningar* och att resultaten skiljer sig mellan olika studier.

Vi anser att de varierande resultaten gör att vi inte kan rekommendera *Bestraffningar* för vidare undersökning. Dock kan det faktum att vissa studier funnit stöd för faktorn vara en indikation på att det finns kontext där faktorn är viktig. Det är därmed möjligt att faktorns påverkan beror till stor grad av aktuellt kontext, eller att endast underfaktorer av faktorn är vad som påverkar individens säkerhetsbeteende, exempelvis straffets allvarlighet (Guan and Hsu, 2020). Till sist är det även möjligt att individens upplevda trolighet att bli upptäckt har en påverkan på denna faktor, något som Moody m.fl. (2018) inte undersöker.

Underlättande Förhållanden

Likt *Självförmåga* så fann en stor andel av undersökta artiklar stöd för *Underlättande Förhållanden* i någon form. Moodys m.fl. (2018) diskussion nämner att denna faktor kan ha större påverkan i tekniskt utmanande uppgifter, något som kan vara en anledning till att faktorn stöds av resultaten i flera studier. Eftersom svårigheten av relevant uppgift inte var en del av den dataextrahering som gjordes kan resultaten inte användes för att bekräfta eller förkasta den teorin. Däremot talar den ojämna fördelning för att faktorn har påverkan inom olika kontext.

Underlättande Förhållanden fokuserar på egenskaper hos situationen istället för egenskaper hos individen (vilka då klassas som *Självförmåga*) vilket gör att den inkluderar både utbildning och annat tekniskt stöd. Menards (2017) uppdelning av *Upplevd Kompetens* och *Självförmåga* föreslår en koppling mellan de två vilket kan antyda en koppling mellan *Underlättande Förhållanden* och *Självförmåga*. Trots att Menards (2017) resultat ensamt inte kan anses som avgörande bevis för att *Underlättande Förhållanden* generellt påverkar *Självförmåga* kan det vara ett exempel på hur de faktorer som uteslöts av Moody m.fl. (2018) kan passa in i en utökad version av UMISPC-modellen. Vår åsikt är att dessa resultat tyder på att *Underlättande Förhållanden* bör undersökas vidare i framtida studier.

Sociala Faktorer

Resultatet talar för att *Sociala Faktorer* har en påverkan på individen i de flesta kontext eftersom en stor andel av artiklar fann stöd för detta. Moody m.fl. (2018) föreslår att deras egna resultat berott på att deras scenarion inte är socialt synliga vilket gör att individen i deras fall inte behövde ta hänsyn till medarbetares åsikter. Den sociala synligheten för en uppgift i de olika artiklarnas kontext undersöktes ej i dataanalysen och kan därmed ej avfärdas som påverkande. De studier som inte hittade stöd för faktorn nämner att deras resultat säger emot tidigare forskning och att det troligtvis beror på deras kontext (IT-anställda och elever).

Vi anser att faktorn är lämplig att undersöka för att mäta dess påverkan på säkerhetsbeteende och eventuella samband med andra faktorer i UMISPC-modellen.

Belöningar/Kostnader

Även om resultaten för *Belöningar/Kostnader* inte hade lika ojämn fördelning så lutar resultaten åt att faktorn har påverkan i fler fall än ej. Detta anser vi tyda på att faktorn har påverkan i flera kontext. Moody m.fl. (2018) nämner att *avskräckande medel* undersökts i tidigare forskning med blandade resultat, vilket dessa resultat stödjer. Bland de undersökta artiklarna undersöks belöningar och kostnader med en något bredare definition än Moody m.fl. (2018) vilket kan vara en förklaring till den något jämnare fördelningen än de andra uteslutna faktorerna (med undantag av *Bestraffningar*).

Att alla studier som undersökte faktorn utan att finna stöd för den enbart undersökte anställda gör att resultaten inte kan generaliseras för att påvisa att privatpersoner inte påverkas av faktorn. Men att faktorn påverkar i vissa kontext går att påvisa då de studier vars resultat stöder faktorns påverkan inkluderar respondenter från flera olika kontext. Vi anser att faktorn är relevant för framtida undersökningar trots den mer jämna fördelningen.

5.1.2. Faktorer som inkluderades i UMISPC

Våra resultat är fördelade på ett sätt som stödjer de resultat som Moody m.fl. (2018) tar fram i sin studie. Faktorerna *Respons Effektivitet*, *Hot*, *Roll Värderingar* och *Intention* stöds i flertalet studier medan urvalet för *Vanor*, *Rädsla*, *Neutralisering* och *Reaktans* är relativt litet vilket gör att vi varken stödjer eller motsäger deras relevans, förutom att de har kunnat stödjas i *något* kontext. Däremot går det att se att de uteslutna faktorerna (förutom *Bestraffningar*) har undersökts i lika många eller fler antal artiklar än de inkluderade faktorerna (undantag av *Hot*). De uteslutna faktorerna har alltså undersökts i tidigare forskning och kunnat stödjas i flera studier vilket vi anser talar för deras relevans i flera kontext och potentiell inkludering i UMISPC-modellen.

Hot hade det mest blandade resultatet av faktorerna i UMISPC-modellen. Detta kan bero på att definitionen är relativt bred och inkluderar trolighet och allvarlighet av hotet, samt andra upplevda egenskaper. Dessa är ofta subjektiva och det är möjligt att olika kontext påverkar underfaktorer för *Hot* till varierande grad. Detta kan vara en anledning till att faktorn bör delas upp beroende på situation den används inom.

5.2. Metoddiskussion

Modeller som inkluderas i litteraturstudien uppfyller att de inkluderar faktorer som stöds med en empirisk studie. Uppsalas bibliotekskatalog användes för att försäkra att artiklarna som testar faktorerna uppnådde hög akademisk kvalitet. Målet var att användande av källor med hög kvalitet även skulle öka kvaliteten hos denna uppsats och dess slutsatser.

Denna uppsats studerar säkerhetsbeteende utifrån tidigare empiriskt testade modeller i olika kontext samt undersöker ett stort antal artiklar, detta för att uppnå högre generaliserbarhet. Resultaten är tänkta att vara tillämpbara inom många ämnesområden och inte begränsat till ett fåtal. Däremot hade resultaten kunnat vara användbara även om enbart studier inom ett visst ämnesområde undersökts, dock då enbart i det området. eventuellt i form av en mindre flexibel men mer specialiserad modell än UMISPC.

Uppsatsen begränsades inte till ett specifik fall, detta för att öka vidareförbarheten och även med mål att ha värde, relevans och giltighet utanför de studerade exemplen (Goldkuhl, 2013, p. 13), exempelvis i andra områden, kulturer och företag.

För att öka studiens reproducerbarhet och trovärdighet beskrivs processen och genomförandet i Kapitel 3 samt att alla utvalda artiklar från litteratursökningen inkluderas i Tabell 4.2. En replikeringsstudie med samma syfte och metod förväntas ge liknande resultat, med undantag i fall där en faktors klassificering tolkas på ett annat sätt av andra forskare. Den metod som

användes för klassificering är dock byggd för att minska förekomsten av dessa skillnader i klassificering genom att enbart fokusera på respektive faktorers definitioner.

5.2.1. Begränsningar

Studiens metod inkluderar begränsningar. Vi anser att studiens dataanalysfas är en begränsning då den slutgiltiga klassifikationen av en faktor kan påverkas av forskaren beroende på dess tolkning av liknelsen mellan en studies faktor och Moody m.fl. (2018) faktor. Vi anser att detta påverkar studiens kvalité, trovärdighet, reliabilitet och reproducerbarhet negativt. De riktlinjer för klassificering som etablerades för studien skapades med avsikt att motverka eventuella skillnader i tolkning.

Studien undersöker enbart om det finns ett samband mellan en viss faktor och individers säkerhetsbeteende, inte till vilken grad det påverkas eller om säkerhetsbeteendet påverkas negativt eller positivt. Det är även möjligt att en faktor påverkar säkerhetsbeteende genom att påverka en annan faktor istället för att ha direkt påverkan. Resultaten kan därmed inte direkt användas för att lägga till en faktor i UMISPC-modellen eftersom de inte anger vart eller på vilket sätt faktorn har en påverkan. Däremot kan resultaten påvisa en faktors relevans vilket kan vara en anledning till att mäta vilka samband som finns mellan den och UMISPC-modellens faktorer.

Även om de artiklar som undersöktes under studien var ett urval som ansågs representativt så var de enbart samlade från en söktjänst. Tidigare studier visar på att en söktjänst inte fångar alla relevanta och tillgängliga artiklar, och att två eller flera söktjänster ger en större täckning (Xiao and Watson, 2019; Zhao, 2014). Resultaten från flera söktjänster kan kombineras med en motsvarande sökning från en annan söktjänst för högre täckning av relevanta artiklar och därmed ökad trovärdighet.

6. Slutsats

I detta kapitel sammanfattas vilka slutsatser som kan dras från de resultat som diskuterades i Kapitel 5. Vilka etiska konsekvenser resultaten kan ha och vilka de påverkar diskuteras. Till sist ges förslag till framtida forskning.

För att besvara forskningsfrågan "*Vilka faktorer kan vara aktuella för en framtida utökning av UMISPC-modellen?*" har studier som liknar den som utförs av Moody m.fl. (2018) undersökts. Resultatet visar på att de faktorer som Moody m.fl. (2018) inte finner stöd för har mätts i dessa studier där deras påverkan på individers säkerhetsbeteende kunnat stödjas. Vår slutsats är att dessa faktorer påverkar individer i vissa kontext och därför uppfyller Moodys m.fl. (2018) krav för att inkludera en faktor i UMISPC-modellen. Vidare forskning kan avgöra på vilket sätt faktorerna passar in i UMISPC-modellen.

Studien undersökte 457 artiklar varav 61 stycken var relevanta. De fyra faktorerna (*Sociala Faktorer*, *Belöningar/Kostnader*, *Bestraffningar*, *Underlättande Förhållanden*) samt *Självförmåga* förekommer i artiklar som undersöktes i studien. Dessa artiklar är exempel på empiriskt testade fall där faktorn påverkar individers säkerhetsbeteende på ett sätt som liknar Moody m.fl. (2018) tillvägagångssätt. Eftersom majoriteten av studierna som undersökt faktorerna har kunnat styrka faktorernas påverkan anser vi att alla fem faktorer har bevisats påverka i något kontext och därmed bör inkluderas i UMISPC-modellen. Antingen som en faktor som direkt påverkar säkerhetsbeteende eller som en underfaktor (faktor som påverkar en annan faktor).

Faktorn *Bestraffningar* har i linje med tidigare forskning ett blandat resultat där dess påverkan inte kan stödjas i lika stor andel av studierna som de andra faktorerna. Detta kan betyda att faktorn är mer komplex än de andra fyra faktorerna.

Genom att ge förslag på utökning av UMISPC-modellens faktorer kan resultaten från denna uppsats ligga till grund för eller motivera framtida studier med avsikt att uppdatera modellen. Detta skulle bidra till att UMISPC-modellen på ett mer korrekt sätt representerar vad som påverkar individers säkerhetsbeteende.

6.1. Etiska konsekvenser

Denna studies datainsamling ansågs inte ha några direkta etiska konsekvenser då all data samlades in från publikt tillgängliga källor. Eftersom denna studie enbart var observerande ansågs den inte direkt påverka författarna eller respondenterna i de utvalda artiklarna.

Studiens urval av artiklar har skett objektivt och alla artiklar har inkluderats oavsett deras slutresultat. Detta är enligt Eriksson Barajas m.fl. (2013) ett sätt att agera korrekt ur ett etiskt perspektiv.

Resultaten kan potentiellt tänkas ha vissa konsekvenser för individer inom ett företag om de används som grund för uppdaterade regler och riktlinjer på en arbetsplats. Om resultaten hade varit missvisande eller felaktiga skulle det även kunnat leda till att säkerhetsansvariga

fokuserar på fel faktorer i sitt arbete att förbättra anställdas säkerhetsbeteende. Detta skulle i sin tur kunna leda till försämrat säkerhetsbeteende hos anställda inom företaget. Resultatens slutsatser om vikten av specifika faktorer kan, om de appliceras i en framtida version av UMISPC-modellen, på sikt leda till förändrade arbetsvillkor.

6.2. Vidare forskning

Vi anser att resultaten av denna uppsats bevisar det Moody m.fl. (2018) skriver i sin diskussion angående att deras modell bör testas med modifierade scenarier. De scenarier som skulle användas i en sådan studie bör utformas för att testa om det finns ett samband mellan säkerhetsbeteende och specifika faktorer. Både de fyra som Moody m.fl. (2018) inte finner stöd för i sin andra studie och även *Självförmåga* hos individer. Vid framtida undersökningar kan det vara aktuellt att modifiera frågeställningarna för att även mäta faktorernas underkategorier, exempelvis undersöka *Hot* och identifiera om det är allvarligheten eller troligheten av ett hot som påverkar individen.

Vidare analys kan göras på de artiklar som inkluderas i denna undersökning. Det kan även vara intressant att undersöka om resultaten mellan artiklarna skiljer sig på grund av kontext eller hur de respektive undersökningarna utfördes, detta skulle kunna uppfylla Moodys m.fl. (2018) rekommendation för vidare forskning om i vilka kontext UMISPC-modellen fungerar och om modellen behöver modifieras för att användas i ett specifikt kontext. Detta skulle kunna utföras genom någon form av dataanalys för att ta fram eventuella samband mellan exempelvis land eller typ av respondenter.

En litteratursökning liknande den som gjordes i denna uppsats skulle kunna göras med andra kriterier för att ta fram en viss typ av artiklar. Exempelvis artiklar inom ett visst kontext eller som använder en specifik metod. Alternativt kunde en sökning med samma metod kunna utföras i en annan söktjänst, exempelvis *Google Scholar*. Det skulle då vara möjligt att kombinera resultaten av undersökningarna för att få resultat från ett större urval respondenter. Det är även tänkbart att artiklar som är lika varandra kan väljas ut för att kunna utföra en metaanalys (Snyder, 2019) för att kvantitativt mäta förekomst och påverkan av specifika faktorer.

7. Källförteckning

Ahmad, Z., Ong, T.S., Liew, T.H., Norhashim, M., 2019. Security monitoring and information security assurance behaviour among employees: An empirical analysis. ICS 27, 165–188. https://doi.org/10.1108/ICS-10-2017-0073

Aigbefo, Q.A., Blount, Y., Marrone, M., 2022. The influence of hardiness and habit on security behaviour intention. Behaviour & Information Technology 41, 1151–1170. https://doi.org/10.1080/0144929X.2020.1856928

Ajzen, I., 1991. The theory of planned behavior. Organizational Behavior and Human Decision Processes 50, 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

ALLEA, 2018. Den europeiska kodexen för forskningens integritet. ALLEA.

Arachchilage, N.A.G., Love, S., 2014. Security awareness of computer users: A phishing threat avoidance perspective. Computers in Human Behavior 38, 304–312. https://doi.org/10.1016/j.chb.2014.05.046

Aurigemma, S., Mattson, T., 2019. Effect of long-term orientation on voluntary security actions. ICS 27, 122–142. https://doi.org/10.1108/ICS-07-2018-0086

Aurigemma, S., Mattson, T., 2017. Deterrence and punishment experience impacts on ISP compliance attitudes. ICS 25, 421–436. https://doi.org/10.1108/ICS-11-2016-0089

Balozian, P., Leidner, D., Warkentin, M., 2019. Managers' and Employees' Differing Responses to Security Approaches. Journal of Computer Information Systems 59, 197–210. https://doi.org/10.1080/08874417.2017.1318687

Bax, S., McGill, T., Hobbs, V., 2021. Maladaptive behaviour in response to email phishing threats: The roles of rewards and response costs. Computers & Security 106, 102278. https://doi.org/10.1016/j.cose.2021.102278

Becker, M.H., 1974. The Health Belief Model and Sick Role Behavior. Health Education Monographs 2, 409–419. https://doi.org/10.1177/109019817400200407

Bhardwaj, A., Al-Turjman, F., Sapra, V., Kumar, M., Stephan, T., 2021. Privacy-aware detection framework to mitigate new-age phishing attacks. Computers & Electrical Engineering 96, 107546. https://doi.org/10.1016/j.compeleceng.2021.107546

Boehmer, J., LaRose, R., Rifon, N., Alhabash, S., Cotten, S., 2015. Determinants of online safety behaviour: towards an intervention strategy for college students. Behaviour & Information Technology 34, 1022–1035. https://doi.org/10.1080/0144929X.2015.1028448

Chen, X., Chen, L., Wu, D., 2018. Factors That Influence Employees' Security Policy Compliance: An Awareness-Motivation-Capability Perspective. Journal of Computer Information Systems 58, 312–324. https://doi.org/10.1080/08874417.2016.1258679

Chou, H.-L., Chou, C., 2016. An analysis of multiple factors relating to teachers' problematic information security behavior. Computers in Human Behavior 65, 334–345. https://doi.org/10.1016/j.chb.2016.08.034

Claar, C.L., Johnson, J., 2012. Analyzing Home PC Security Adoption Behavior.

Cox, J., 2012. Information systems user security: A structured model of the knowing–doing gap. Computers in Human Behavior 28, 1849–1858. https://doi.org/10.1016/j.chb.2012.05.003

Crossler, R., Bélanger, F., 2014. An Extended Perspective on Individual Security Behaviors: Protection Motivation Theory and a Unified Security Practices (USP) Instrument. SIGMIS Database 45, 51–71. https://doi.org/10.1145/2691517.2691521

Cuganesan, S., Steele, C., Hart, A., 2018. How senior management and workplace norms influence information security attitudes and self-efficacy. Behaviour & Information Technology 37, 50–65. https://doi.org/10.1080/0144929X.2017.1397193

D'Arcy, J., Lowry, P.B., 2019. Cognitive‐affective drivers of employees' daily compliance

with information security policies: A multilevel, longitudinal study. Info Systems J 29, 43–69. https://doi.org/10.1111/isj.12173
Davis, J., Agrawal, D., Guo, X., 2021. Enhancing users' security engagement through cultivating commitment: the role of psychological needs fulfilment. European Journal of Information Systems 1–12. https://doi.org/10.1080/0960085X.2021.1927866
DeCarlo, M., 2018. Scientific Inquiry in Social Work.
Deming, S.N., Morgan, S.L., 1993. Experimental Design: a Chemometric Approach. Elsevier, Burlington.
Denscombe, M., 2010. The good research guide: for small-scale social research projects. McGraw-Hill/Open University Press, Maidenhead, England.
Deutrom, J., Katos, V., Ali, R., 2021. Loneliness, life satisfaction, problematic internet use and security behaviours: re-examining the relationships when working from home during COVID-19. Behaviour & Information Technology 1–15. https://doi.org/10.1080/0144929X.2021.1973107
Diehl, E., 2016. Ten Laws for Security. Springer International Publishing, Cham. https://doi.org/10.1007/978-3-319-42641-9
DoD, 1998. DoD Modeling and Simulation (M&S) Glossary. Departement of Defence.
Dodel, M., Mesch, G., 2019. An integrated model for assessing cyber-safety behaviors: How cognitive, socioeconomic and digital determinants affect diverse safety practices. Computers & Security 86, 75–91. https://doi.org/10.1016/j.cose.2019.05.023
Eminağaoğlu, M., Uçar, E., Eren, Ş., 2009. The positive outcomes of information security awareness training in companies – A case study. Information Security Technical Report 14, 223–229. https://doi.org/10.1016/j.istr.2010.05.002
Eriksson Barajas, K., Forsberg, C., Wengstr??m, Y., 2013. Systematiska litteraturstudier i utbildningsvetenskap: v??gledning vid examensarbeten och vetenskapliga artiklar. Natur & Kultur, Stockholm.
Forsberg, C., Wengström, Y., 2013. Att göra systematiska litteraturstudier: värdering, analys och presentation av omvärdnadsforskning. Natur & Kultur, Stockholm.
Gillam, A.R., Waite, A.M., 2021. Gender differences in predictors of technology threat avoidance. ICS 29, 393–412. https://doi.org/10.1108/ICS-01-2020-0008
Goldkuhl, G., 2013. Kvalitetskriterier för doktorsavhandlingar: ämnesområdet informationssystemutveckling vid LiU.
Goldkuhl, G., 2011. Kunskapande.
Guan, B., Hsu, C., 2020. The role of abusive supervision and organizational commitment on employees' information security policy noncompliance intention. INTR 30, 1383–1405. https://doi.org/10.1108/INTR-06-2019-0260
Hanus, B., Windsor, J.C., Wu, Y., 2018. Definition and Multidimensionality of Security Awareness: Close Encounters of the Second Order. SIGMIS Database 49, 103–133. https://doi.org/10.1145/3210530.3210538
Hanus, B., Wu, Y. "Andy," 2016. Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. Information Systems Management 33, 2–16. https://doi.org/10.1080/10580530.2015.1117842
Herath, T., Rao, H.R., 2009a. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems 47, 154–165. https://doi.org/10.1016/j.dss.2009.02.005
Herath, T., Rao, H.R., 2009b. Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems 18, 106–125. https://doi.org/10.1057/ejis.2009.6
Hong, Y., Furnell, S., 2022. Motivating Information Security Policy Compliance: Insights from Perceived Organizational Formalization. Journal of Computer Information

Systems 62, 19–28. https://doi.org/10.1080/08874417.2019.1683781
Hooper, V., Blunt, C., 2020. Factors influencing the information security behaviour of IT employees. Behaviour & Information Technology 39, 862–874. https://doi.org/10.1080/0144929X.2019.1623322
Hudson, R., 2021. Explicating Exact versus Conceptual Replication. Erkenn. https://doi.org/10.1007/s10670-021-00464-z
Hwang, I., Kim, D., Kim, T., Kim, S., 2017. Why not comply with information security? An empirical approach for the causes of non-compliance. OIR 41, 2–18. https://doi.org/10.1108/OIR-11-2015-0358
Hwang, I., Wakefield, R., Kim, S., Kim, T., 2021. Security Awareness: The First Step in Information Security Compliance Behavior. Journal of Computer Information Systems 61, 345–356. https://doi.org/10.1080/08874417.2019.1650676
Ifinedo, P., 2016. Critical Times for Organizations: What Should Be Done to Curb Workers' Noncompliance With IS Security Policy Guidelines? Information Systems Management 33, 30–41. https://doi.org/10.1080/10580530.2015.1117868
Ifinedo, P., 2012. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security 31, 83–95. https://doi.org/10.1016/j.cose.2011.10.007
Johnston, Warkentin, 2010. Fear Appeals and Information Security Behaviors: An Empirical Study. MIS Quarterly 34, 549. https://doi.org/10.2307/25750691
Kajtazi, M., Cavusoglu, H., Benbasat, I., Haftor, D., 2018. Escalation of commitment as an antecedent to noncompliance with information security policy. ICS 26, 171–193. https://doi.org/10.1108/ICS-09-2017-0066
Kajtazi, M., Holmberg, N., Sarker, S., Keller, C., Johansson, B., Tona, O., 2021. Toward a unified model of information security policy compliance: A conceptual replication study. AIS Transactions on Replication Research 7, 2.
Khan, H.U., AlShare, K.A., 2019. Violators versus non-violators of information security measures in organizations—A study of distinguishing factors. Journal of Organizational Computing and Electronic Commerce 29, 4–23. https://doi.org/10.1080/10919392.2019.1552743
Kim, Bora, Lee, D.-Y., Kim, Beomsoo, 2020. Deterrent effects of punishment and training on insider security threats: a field experiment on phishing attacks. Behaviour & Information Technology 39, 1156–1175. https://doi.org/10.1080/0144929X.2019.1653992
Kitchenham, B., 2004. Procedures for Performing Systematic Reviews.
Koohang, A., Nowak, A., Paliszkiewicz, J., Nord, J.H., 2020. Information Security Policy Compliance: Leadership, Trust, Role Values, and Awareness. Journal of Computer Information Systems 60, 1–8. https://doi.org/10.1080/08874417.2019.1668738
Lankton, N.K., Stivason, C., Gurung, A., 2019. Information protection behaviors: morality and organizational criticality. ICS 27, 468–488. https://doi.org/10.1108/ICS-07-2018-0092
Layton, T.P., 2005. Information security awareness: the psychology behind the technology, 1. publ. ed. AuthorHouse, Bloomington, Ind.
Lee, C.S., Kim, D., 2022. Pathways to Cybersecurity Awareness and Protection Behaviors in South Korea. Journal of Computer Information Systems 1–13. https://doi.org/10.1080/08874417.2022.2031347
Li, Y., Pan, T., Zhang, N. (Andy), 2019. From hindrance to challenge: How employees understand and respond to information security policies. JEIM 33, 191–213. https://doi.org/10.1108/JEIM-01-2019-0018
Lian, J.-W., 2021. Understanding cloud-based BYOD information security protection

behaviour in smart business: in perspective of perceived value. Enterprise Information Systems 15, 1216–1237. https://doi.org/10.1080/17517575.2020.1791966
Ma, X., 2022. IS professionals' information security behaviors in Chinese IT organizations for information security protection. Information Processing & Management 59, 102744. https://doi.org/10.1016/j.ipm.2021.102744
Menard, P., Bott, G.J., Crossler, R.E., 2017. User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory. Journal of Management Information Systems 34, 1203–1230. https://doi.org/10.1080/07421222.2017.1394083
Menard, P., Gatlin, R., Warkentin, M., 2014. Threat Protection and Convenience: Antecedents of Cloud-Based Data Backup. Journal of Computer Information Systems 55, 83–91. https://doi.org/10.1080/08874417.2014.11645743
Moody, G.D., Siponen, M., University of Jyväskylä, Pahnila, S., University of Oulu, 2018. Toward a Unified Model of Information Security Policy Compliance. MISQ 42, 285–311. https://doi.org/10.25300/MISQ/2018/13853
Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., Vance, A., 2009. What levels of moral reasoning and values explain adherence to information security rules? An empirical study. European Journal of Information Systems 18, 126–139. https://doi.org/10.1057/ejis.2009.10
Nasir, A., Abdullah Arshah, R., Ab Hamid, M.R., 2019. A dimension-based information security culture model and its relationship with employees' security behavior: A case study in Malaysian higher educational institutions. Information Security Journal: A Global Perspective 28, 55–80. https://doi.org/10.1080/19393555.2019.1643956
Nasirpouri Shadbad, F., Biros, D., 2021. Understanding Employee Information Security Policy Compliance from Role Theory Perspective. Journal of Computer Information Systems 61, 571–580. https://doi.org/10.1080/08874417.2020.1845584
Ng, B.-Y., Kankanhalli, A., Xu, Y. (Calvin), 2009. Studying users' computer security behavior: A health belief perspective. Decision Support Systems 46, 815–825. https://doi.org/10.1016/j.dss.2008.11.010
Ng, K.C., Zhang, X., Thong, J.Y.L., Tam, K.Y., 2021. Protecting Against Threats to Information Security: An Attitudinal Ambivalence Perspective. Journal of Management Information Systems 38, 732–764. https://doi.org/10.1080/07421222.2021.1962601
Nord, J., Sargent, C.S., Koohang, A., Marotta, A., 2022. Predictors of Success in Information Security Policy Compliance. Journal of Computer Information Systems 1–11. https://doi.org/10.1080/08874417.2022.2067795
Oates, B.J., 2006. Researching information systems and computing. SAGE Publications, London ; Thousand Oaks, Calif.
Ogbanufe, O., Crossler, R.E., Biros, D., 2021. Exploring stewardship: A precursor to voluntary security behaviors. Computers & Security 109, 102397. https://doi.org/10.1016/j.cose.2021.102397
Okoli, C., 2015. A Guide to Conducting a Standalone Systematic Literature Review. CAIS 37. https://doi.org/10.17705/1CAIS.03743
Posey, C., Roberts, T.L., Lowry, P.B., 2015. The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets. Journal of Management Information Systems 32, 179–214. https://doi.org/10.1080/07421222.2015.1138374
Rogers, R.W., 1975. A Protection Motivation Theory of Fear Appeals and Attitude Change1. The Journal of Psychology 91, 93–114. https://doi.org/10.1080/00223980.1975.9915803

Snyder, H., 2019. Literature review as a research methodology: An overview and guidelines. Journal of Business Research 104, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039
Sohrabi Safa, N., Von Solms, R., Furnell, S., 2016. Information security policy compliance model in organizations. Computers & Security 56, 70–82. https://doi.org/10.1016/j.cose.2015.10.006
Solomon, G., Brown, I., 2021. The influence of organisational culture and information security culture on employee compliance behaviour. JEIM 34, 1203–1228. https://doi.org/10.1108/JEIM-08-2019-0217
Sommestad, T., Hallberg, J., Lundholm, K., Bengtsson, J., 2014. Variables influencing information security policy compliance: A systematic review of quantitative studies. Information Management & Computer Security 22, 42–75. https://doi.org/10.1108/IMCS-08-2012-0045
Sommestad, T., Karlzén, H., Hallberg, J., 2019. The Theory of Planned Behavior and Information Security Policy Compliance. Journal of Computer Information Systems 59, 344–353. https://doi.org/10.1080/08874417.2017.1368421
Son, J.-Y., 2011. Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. Information & Management 48, 296–302. https://doi.org/10.1016/j.im.2011.07.002
Tesleem, F., Tryfonas, T., 2017. Hacking a Bridge: An Exploratory Study of Compliance-Based Information Security Management in Banking Organization. Journal on Systemics, Cybernetics and Informatics Oct 2017, 74–80.
Torten, R., Reaiche, C., Boyle, S., 2018. The impact of security awarness on information technology professionals' behavior. Computers & Security 79, 68–79. https://doi.org/10.1016/j.cose.2018.08.007
Vafaei-Zadeh, A., Thurasamy, R., Hanifah, H., 2019. Modeling anti-malware use intention of university students in a developing country using the theory of planned behavior. K 48, 1565–1585. https://doi.org/10.1108/K-05-2018-0226
Vetenskapsrådet, 2002. Forskningsetiska principer inom humanistisk-samhällsvetenskaplig forskning. Vetenskapsrådet, Stockholm.
vom Brocke, J., Simons, A., Riemer, K., Niehaves, B., Plattfaut, R., Cleven, A., 2015. Standing on the Shoulders of Giants: Challenges and Recommendations of Literature Search in Information Systems Research. CAIS 37. https://doi.org/10.17705/1CAIS.03709
Wang, X., Xu, J., 2021. Deterrence and leadership factors: Which are important for information security policy compliance in the hotel industry. Tourism Management 84, 104282. https://doi.org/10.1016/j.tourman.2021.104282
Warkentin, M., Johnston, A.C., Shropshire, J., 2011. The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. European Journal of Information Systems 20, 267–284. https://doi.org/10.1057/ejis.2010.72
White, G., Ekin, T., Visinescu, L., 2017. Analysis of Protective Behavior and Security Incidents for Home Computers. Journal of Computer Information Systems 57, 353–363. https://doi.org/10.1080/08874417.2016.1232991
Wiafe, I., Koranteng, F.N., Wiafe, A., Obeng, E.N., Yaokumah, W., 2020. The role of norms in information security policy compliance. ICS 28, 743–761. https://doi.org/10.1108/ICS-08-2019-0095
Xiao, Y., Watson, M., 2019. Guidance on Conducting a Systematic Literature Review. Journal of Planning Education and Research 39, 93–112. https://doi.org/10.1177/0739456X17723971

Xu, Z., Guo, K., 2019. It ain't my business: a coping perspective on employee effortful security behavior. JEIM 32, 824–842. https://doi.org/10.1108/JEIM-10-2018-0229
Yang, C.-G., Lee, H.-J., 2016. A study on the antecedents of healthcare information protection intention. Inf Syst Front 18, 253–263. https://doi.org/10.1007/s10796-015-9594-x
Yazdanmehr, A., Wang, J., 2021. Can peers help reduce violations of information security policies? The role of peer monitoring. European Journal of Information Systems 1–21. https://doi.org/10.1080/0960085X.2021.1980444
Yoon, C., Hwang, J.-W., Kim, R., 2012. Exploring Factors That Influence Students' Behaviors in Information Security.
Zhao, J.-G., 2014. Combination of multiple databases is necessary for a valid systematic review. International Orthopaedics (SICOT) 38, 2639–2639. https://doi.org/10.1007/s00264-014-2556-y
Zhen, J., Xie, Z., Dong, K., Chen, L., 2021. Impact of negative emotions on violations of information security policy and possible mitigations. Behaviour & Information Technology 1–13. https://doi.org/10.1080/0144929X.2021.1921029