

Cybersäkerhet och organisatoriskt förtroende:

En kvantitativ studie om kommunanställdas tillit till arbetsgivarens cybersäkerhetsshantering

Cybersecurity and organisational trust:

A quantitative study of municipal employees' trust in employer cybersecurity management

Examensarbete för
kandidatexamen med
huvudområdet socialpsykologi

Grundnivå 15 högskolepoäng

Vårtermin 2026

Student: Robert Eriksson, Lina Samavat &
Christel Tveiten Emanuelsson

Handledare: Sakarias Bank

Examinator: Anette Lundin

Deklarering

Härmed intygar vi, Robert Eriksson, Lina Samavat och Christel Tveiten Emanuelsson, att detta examensarbete har genomförts självständigt och utan otillbörlig hjälp inom ramen för det socialpsykologiska programmet vid Högskolan i Skövde under vårterminen 2026, i syfte att erhålla en kandidatexamen i socialpsykologi. Arbetet har inte tidigare publicerats eller lämnats in för examination. Vi intygar även att samtliga använda källor återfinns i referenslistan.

Datum: 2026-04-30

Resumé

Det digitaliserade arbetslivet har medfört nya möjligheter, men också nya risker, där bristande cybersäkerhet kan få konsekvenser för både organisationer och medarbetare. Särskilt inom offentlig sektor har detta blivit en aktuell fråga, då kommuner hanterar stora mängder känslig information och samtidigt står inför ökade cyberhot. Studien syftar till att undersöka kommunanställdas tillit till arbetsgivarens cybersäkerhetshantering genom att analysera sambanden mellan denna form av tillit och organisatorisk tillit, upplevt organisatoriskt stöd och arbetsrelaterad kontrolluppfattning. En kvantitativ tvärsnittsstudie genomfördes med hjälp av en digital enkät som besvarades av 151 kommunanställda. Data analyserades med faktoranalys, Envägs-ANOVA, korrelationsanalys samt enkla och hierarkiska regressionsanalyser. Resultaten visade att organisatorisk tillit, upplevt organisatoriskt stöd och arbetsrelaterad kontrolluppfattning hade positiva samband med tillit till arbetsgivarens cybersäkerhetshantering. Det framkom även att variablerna tillsammans förklarade 34,4% av variansen i tillit till arbetsgivarens cybersäkerhetshantering. Kontrollvariabeln rapporterad cybersäkerhetsutbildning från arbetsgivaren bidrog dessutom till att förklara ytterligare 9% av variansen i tillit till arbetsgivarens cybersäkerhetshantering. Studien visar att tillit till arbetsgivarens cybersäkerhetshantering inte enbart formas av tekniska lösningar, utan också av hur organisationens agerande tolkas av medarbetare.

Nyckelord: tillit till cybersäkerhetshantering, kommunanställda, organisatorisk tillit, organisatoriskt stöd, arbetsrelaterad kontrolluppfattning

Abstract

Digitalised working life has created new opportunities, but also new risks, where insufficient cybersecurity may have consequences for both organisations and employees. This has become a particularly relevant issue in the public sector, as municipalities handle large amounts of sensitive information while facing increasing cyber threats. The aim of study is to examine municipal employees' trust in their employer's cybersecurity management by analysing the relationships between this form of trust and organizational trust, perceived organisational support and work-related locus of control. A quantitative cross-sectional study was conducted using a digital survey answered by 151 municipal employees. The data were analysed using factor analysis, One Way ANOVA, correlation analyses, and simple and hierarchical regression analyses. The results showed that organisational trust, perceived organisational support, and work locus of control were positively related to trust in the employer's cybersecurity management. It was also found that the variables together explained 34.4% of the variance in trust in the employer's cybersecurity management. The control variable, reported cybersecurity training from the employer, furthermore, contributed to explaining an additional 9% to the variance in trust in the employer's cybersecurity management. The study shows that trust in the employer's cybersecurity management is shaped not only by technical solutions, but also by how the organisation's actions are interpreted by employees.

Keywords: trust in cybersecurity management, municipal employees, organisational trust, perceived organisational support, work locus of control

Förord

Tacksamhet är en dygd. Vi vill därför rikta ett stort tack till alla som bidragit till detta examensarbete. Vår handledare Sakarias Bank för din tid, vägledning och tabelltips. De kontaktpersoner vi haft ute i de medverkande kommunerna som på olika sätt möjliggjorde att vi kunde nå ut till respondenterna. Alla de kommunanställda som tog sig tid att besvara vår enkät. Våra klasskamrater och lärare för feedback och råd. Våra nära och kära som stöttat och haft tålamod när vår tid och energi varit begränsad. Dessutom vill vi tacka varandra för ett fantastiskt samarbete som, trots perioder av motgångar, stress och dålig stämning, resulterade i att vi inte bara slutförde arbetet utan faktiskt överlevde det också.

Begreppsförteckning

Arbetsrelaterad kontrolluppfattning | Eng. *Work Locus of Control* | Medarbetarnas känsla av att kunna påverka och hantera risker som är kopplade till situationer på arbetsplatsen. (Spector 1982)

Kontrolluppfattning | Eng. *Locus of Control* | Individens uppfattning om i vilken grad den själv eller yttre faktorer styr vad som händer i livet. (Rotter 1966)

Organisatorisk tillit | Eng. *Organisational Trust* | En vilja hos en part att göra sig sårbar i förhållande till en annan parts handlingar. Denna vilja bygger på en förväntan om att den andra parten kommer att agera på ett sätt som är viktigt, även utan möjlighet till att övervaka eller kontrollera beteendet. (Mayer, Davis & Schoorman 1995)

Upplevt organisatoriskt stöd | Eng. *Perceived Organisational Support* | De anställdas uppfattning om i vilken utsträckning arbetsgivaren värderar deras insats och bryr sig om deras välmående. (Eisenberger, Huntington, Hutchison & Sowa 1986)

Ordförteckning

Cyberangrepp | En situation där en otillbörlig handling utförs mot ett informationssystem. Handlingen påverkar systemet genom att till exempel information raderas, sparas eller systemet överbelastas. Till följd av detta drabbas systemet eller användarna av negativa konsekvenser. Dessa konsekvenser kan vara att information blir otillgänglig, förvanskad eller röjd. Handlingens avsikt är att medvetet skada eller exploatera systemet. (Myndigheten för samhällsskydd och beredskap [MSB] 2024b).

Cyberhot | Alla typer av hot som kan påverka information, IT-system och digital infrastruktur negativt. Cyberhot kan delas in i tre kategorier:

1. Mänskliga hot. Detta handlar om antagonistiska hot eller icke-antagonistiska hot, alltså om hoten är medvetna eller ej, såsom dataintrång eller felaktig hantering av information.
2. Tekniska hot. Detta är hot som uppstår till följd av tekniska fel som exempelvis systemfel.
3. Naturhot. Hot som skapas av naturfenomen som jordbävningar eller strömvabrott.

Alla dessa hot kan leda till allvarliga konsekvenser och påverka informations- och cybersäkerheten. (MSB 2024a).

Cybersäkerhet | Ett samlingsbegrepp som avser att skydda information och digitala system från hot och risker. Vilket inkluderar informationssäkerhet, tillgänglighet och sekretess. (MSB 2024b).

Incident | En oönskad händelse som har inträffat. När det rör sig om it-incidentrapportering delas det in i de tre huvudkategorierna i cyberhot (se definition av cyberhot). (MSB 2025a).

Personuppgifter | Personuppgifter handlar om all slags information som direkt och indirekt kan knytas till en person som är i livet. Det kan exempelvis röra sig om namn, personnummer och adress. (Integritetsskyddsmyndigheten [IMY] 2021a).

Personuppgiftsincident | En säkerhetsincident som innebär att personuppgifter på något sätt äventyras. Detta kan röra sig om en avsiktlig eller oavsiktlig incident som exempelvis förstöring, ändring, förlust eller obehörig åtkomst av personuppgifter. (IMY 2025c).

Cybersäkerhetshandling | Arbetet med att identifiera, skydda mot och upptäcka cyberhot. (National Institute of Standards and Technology [NIST] 2024)

Innehållsförteckning

<i>Resumé</i>	<i>ii</i>
<i>Abstract</i>	<i>iii</i>
<i>Förord</i>	<i>iv</i>
<i>Begreppsförteckning</i>	<i>v</i>
<i>Ordförteckning</i>	<i>v</i>
<i>Figurförteckning</i>	<i>viii</i>
<i>Tabellförteckning</i>	<i>viii</i>
1. Inledning	1
1.1 Syfte	3
1.2 Hypoteser	3
2. Tidigare forskning	4
2.1 Redogörelse för litteratursökning.....	4
2.2 Tidigare forskning om hantering av cybersäkerhet.....	5
2.3 Tidigare forskning om organisatoriskt stöd och tillit.....	7
2.4 Tidigare forskning om upplevd kontroll och tillit	9
2.5 Sammanfattning och egen positionering till tidigare forskning.....	11
3. Teoretiska utgångspunkter	12
3.1 Organisatorisk tillit.....	12
3.2 Upplevt organisatoriskt stöd	15
3.3 Arbetsrelaterad kontrolluppfattning	16
3.4 Förklarande faktorer för tillit till arbetsgivarens cybersäkerhetshantering	17
4. Metod	18
4.1 Vetenskapsteoretisk utgångspunkt	18
4.2 Metodval.....	18
4.3 Operationalisering.....	19
4.4 Empiriska instrument.....	21
4.5 Urval.....	22
4.6 Tillvägagångssätt	23
4.6.1 Pilotstudie	25
4.7 Analyismetod.....	25
4.8 Kvalitetskriterier	26

4.9 Etiska utmaningar.....	28
5. Resultat.....	30
5.1 Deskriptiv statistik	30
5.1.1 Faktorianalys	32
5.1.2 Envägs-ANOVA.....	32
5.2 Hypotes 1.....	33
5.3 Hypotes 2.....	33
5.4 Hypotes 3.....	34
5.5 Explorativ analys av tillit till arbetsgivarens cybersäkerhetshantering.....	34
6. Diskussion.....	36
6.1 Resultatdiskussion.....	36
6.2 Metoddiskussion	38
6.2.1 Kvalitetskriteriediskussion	39
6.2.2 Etikdiskussion	40
6.2.3 Utmaningar och begränsningar.....	41
6.3 Studiens bidrag till forskningsområdet.....	42
6.4 Framtida studier.....	43
6.4.1 Rekommendationer för praktiker	43
6.5 Slutsats	44
Referenslista.....	- 45 -
Bilaga 1. PRISMA-diagram	- 53 -
Bilaga 2. Sökmatriser	- 54 -
Bilaga 3. Operationaliseringsmatris	- 56 -
Bilaga 4. Enkäten	- 58 -
Bilaga 5. Informationsbrev	- 64 -
Bilaga 6. Kompletterande informationsbrev	- 65 -

Figurförteckning

Figur 1 Illustrering av Integrerad modell för organisatorisk tillit och dess struktur	s.13
Figur 2 Flödesschema över första urvalsprocessen som avslutades den 12 december 2025	s. 53
Figur 3 Flödesschema över andra urvalsprocessen som avslutades den 26 februari 2026	s. 53

Tabellförteckning

Tabell 1 Översikt över urvalskriterier vid litteratursökning	s.5
Tabell 2 Dataextraktion av studier om hantering av cybersäkerhet	s.7
Tabell 3 Dataextraktion av studier om organisatoriskt stöd och tillit	s.8
Tabell 4 Dataextraktion av studier om upplevd kontroll och tillit	s.10
Tabell 5 Deskriptiv statistisk, reliabilitet och korrelation mellan studiens variabler	s.30
Tabell 6 Explorativ faktoranalys (PCA) av skalan tillit till arbetsgivarens cybersäkerhetsshantering.	s.32
Tabell 7 Enkel regression.	s.33
Tabell 8 Enkel regression.	s.33
Tabell 9 Enkel regression.	s.34
Tabell 10 Hierarkisk regressionsanalys.	s.35
Tabell 11.1 Litteratursökning i Libsearch (2025.11.21)	s.54
Tabell 11.2 Litteratursökning i Academic Search Premier (2025.11.25)	s.54
Tabell 11.3 Litteratursökning i PsycINFO (2025.11.25)	s.54
Tabell 11.4 Litteratursökning i Web of Science (2025.12.01)	s.55
Tabell 11.5 Litteratursökning i Libsearch (2026.02.26)	s.55
Tabell 12 Operationaliseringsmatris	s.56

1.Inledning

I ett alltmer digitaliserat samhälle suddas de globala gränserna ut och människor kan enkelt dela kultur, kunskap och upplevelser med varandra. Digitaliseringen skapar en ökad flexibilitet, där samarbete och arbete kan utföras oberoende av plats (Sandblad, Gulliksen, Lantz, Walldius & Åborg 2018, s.15). Samtidigt medför utvecklingen nya hot och utmaningar som kan få allvarliga konsekvenser på alla nivåer, från samhälle till individ. En utmaning är hur cybersäkerheten ska upprätthållas. Enligt Myndigheten för samhällsskydd och beredskap (MSB) (2020) är det svårt att upprätthålla cybersäkerhet med den föränderliga digitala utvecklingen samt att digitaliseringen medför ett beroende av tekniken, från samhällsviktiga funktioner till den enskildes vardagsaktiviteter. Både det digitala beroendet och bristande cybersäkerhet ökar risk över tid, och inget tyder på att detta kommer förändras (Regeringskansliet 2025). I och med detta framträder ett tydligt samhällsproblem, där digitaliseringens sårbarhet kan få allvarliga följder.

Detta gäller även offentliga verksamheter. MSB (2024a) anger att IT-system inte bara stödjer verksamheten utan är avgörande för att den ska fungera. Om verksamheten inte hinner anpassa sig till den föränderliga digitaliseringen ökar risken för cyberhot (MSB 2024a). Rapporter visar att cirka 6 av 10 offentliga verksamheter i Sverige saknar ett tillräckligt systematiskt cybersäkerhetsarbete, och att kommuner är de som hade svagast resultat i mätningarna (MSB 2025b). Detta innebär att stora mängder känslig information riskerar att röjas, däribland personuppgifter. Personuppgiftsincidenter utgör ett betydande cyberhot som kan leda till exponering av känslig information och ska hanteras med varsamhet (Integritetsskyddsmyndigheten [IMY] 2021b; IMY 2025c). Ett tydligt exempel är cyberangreppet som inträffade 2025 mot en extern aktör som hanterar personuppgifter åt svenska kommuner, där minst 164 kommuner drabbades och 1,5 miljoner personers uppgifter röjdes (IMY 2025a; IMY 2025b). För medarbetare kan sådana personuppgiftsincidenter leda till allvarliga konsekvenser såsom ekonomisk skada och identitetsstöld (IMY 2025c). Cybersäkerhet påverkar således inte bara organisationen som helhet, utan har också direkt betydelse för medarbetarnas trygghet, arbetsmiljö och i förlängningen deras hälsa (Regeringskansliet 2021). Medarbetare har begränsad insyn i hur deras personuppgifter behandlas och är beroende av att arbetsgivaren hanterar

cybersäkerhet på ett ansvarsfullt sätt (IMY 2021b). Detta skapar en sårbarhet som gör tilliten till arbetsgivarens cybersäkerhetshandling viktig för medarbetarnas upplevelse av trygghet och kontroll, vilket gör att tilliten till cybersäkerhetshandling bör studeras som ett eget fenomen. Det är därför denna studie fokuserar på den specifika formen av tillit som avser förtroendet för arbetsgivarens förmåga att hantera cybersäkerhet. Samtidigt är det intressant att se om generell organisatorisk tillit hänger ihop med tillit till arbetsgivarens cybersäkerhetshandling, eftersom tillit är domänspecifik (Mayer, Davis & Schoorman 1995).

Ytterligare två faktorer som kan tänkas ha en inverkan på tilliten till arbetsgivarens cybersäkerhetshandling är upplevt organisatoriskt stöd och arbetsrelaterad kontrolluppfattning (Rhoades & Eisenberger 2002; Hadlington, Popovac, Janicke, Yevsejeva & Jones 2019). Organisatoriskt stöd avser i vilken utsträckning medarbetare upplever att organisationen kommunicerar stöd såsom resurser och information om åtgärder (Eisenberger et al. 1986). I en cybersäkerhetkontext kan detta tänkas bidra till att minska osäkerhet kring hur hot hanteras och signalera att organisationen tar frågan på allvar. Arbetsrelaterad kontrolluppfattning handlar om i vilken grad medarbetare upplever att de kan förstå och påverka sin arbetssituation (Spector 1982). I denna studie antas att medarbetare med hög kontrolluppfattning sätter sig in i organisatoriska åtgärder vilket kan bidra till ökad förståelse för dessa åtgärder, inklusive beslut om cybersäkerhetshandling. I föreliggande studie antas att dessa tre faktorer har ett samband med tillit till arbetsgivarens cybersäkerhetshandling.

Att analysera dessa sociala processer är socialpsykologiskt relevant eftersom tillit är en attityd som formas genom subjektiva tolkningar och erfarenheter i samspel med andra (Bergh 2022; Kazemi 2009, s.26). Sociala processer sker dock inte enbart mellan individer, utan även inom och mellan grupper, organisationer samt på samhällsnivå (Giddens & Sutton 2021, s.4, 5). Fokuset i denna studie ligger på samspelet mellan individ och organisation, där tillit förstås som ett resultat av sociala relationer, erfarenheter och upplevda arbetsvillkor. Cybersäkerhet blir i detta perspektiv inte bara en teknisk funktion, utan en del av de villkor som påverkar hur medarbetare upplever trygghet, transparens och ansvar inom organisationen. Tilliten till arbetsgivarens cybersäkerhetshandling ses därför som skapad mellan hur organisationen kommunicerar och agerar och hur

medarbetarna tolkar sina arbetsvillkor och sin egen situation i en digitaliserad arbetsmiljö. Det stora cyberangreppet 2025 som drabbade kommuner påminner oss om att säkerhetsproblem i samband med cyberincidenter ständigt är aktuella (IMY 2025a; IMY 2025b). Detta gör att en studie om medarbetares tillit till cybersäkerhetshanteringen ligger helt rätt i tiden. Vår studie avser att fylla en kunskapslucka genom att flytta fokus från det tekniska till att belysa de socialpsykologiska processerna, där medarbetares upplevelse av generell tillit, kontroll och stöd kan påverka förtroendet till arbetsgivarens cybersäkerhetshantering.

Studiens förhoppning är att resultaten ska ge arbetsgivare en ökad teoretisk förståelse för hur medarbetare uppfattar cybersäkerhetshantering. Genom att synliggöra faktorer som kan påverka tilliten är tanken att arbetsgivare ska kunna få nya insikter och i bästa fall använda detta som teoretiskt underlag i framtida strategier. På så sätt kan studiens resultat inte bara ge arbetsgivare stöd i deras arbete, utan även i förlängningen gagna medarbetarnas hälsa och välbefinnande i vårt digitaliserade samhälle. Detta gör att undersökningen av tillit till arbetsgivarens cybersäkerhetshantering ligger helt i linje med Högskolan i Skövdes profil: Hälsa i vardags- och arbetsliv i ett digitaliserat samhälle. Utifrån detta finns det anledning att närmare undersöka dessa faktorer och deras betydelse för medarbetares tillit till arbetsgivarens cybersäkerhetshantering, vilket mynnar ut i studiens syfte och hypoteser som presenteras nedan.

1.1 Syfte

Syftet med studien är att undersöka kommunanställdas tillit till arbetsgivarens cybersäkerhetshantering genom att analysera samband mellan den här formen av tillit och organisatorisk tillit, organisatoriskt stöd samt arbetsrelaterad kontrolluppfattning.

1.2 Hypoteser

H1: Det finns ett positivt samband mellan organisatorisk tillit och tillit till arbetsgivarens cybersäkerhetshantering.

H2: Det finns ett positivt samband mellan upplevt organisatoriskt stöd och tillit till arbetsgivarens cybersäkerhetshantering.

H3: Det finns ett positivt samband mellan arbetsrelaterad kontrolluppfattning och tillit till arbetsgivarens cybersäkerhetshantering.

2. Tidigare forskning

I detta avsnitt redogörs för litteratursökning, inklusive val av databaser, sökord, inklusions- och exklusionskriterier samt redogörelse för sökprocessen. Sökprocessen beskrivs med stöd av PRISMA-diagram (se bilaga 1) och sökmatriser (se bilaga 2). Därefter presenteras en tematisering av den tidigare forskningen som delats in i teman utifrån relevans för studiens syfte. Inom respektive tema presenteras en dataextraktionstabell som översiktligt redogör för de studier som behandlats, vilket möjliggör en transparent och systematisk redovisning av urvalet (Higgins et al. 2019).

2.1 Redogörelse för litteratursökning

För att säkerställa att artikelurvalet var relevant och representativt för studiens syfte genomfördes en systematisk litteratursökning i flera vetenskapliga databaser. Litteratursökningarna genomfördes i databaserna Web of Science, Libsearch, PsycINFO och Academic Search Premier. Databaserna valdes eftersom de innehåller ett brett urval av tillförlitlig forskning inom socialpsykologi, beteendevetenskap och organisationspsykologi, vilket är relevant för vår studies fokus på medarbetarnas uppfattningar om arbetsgivarens cybersäkerhetshantering. Sökningarna genomfördes gemensamt av studiens författare för att säkerställa överensstämmande bedömningar och minska risken för skillnader i tolkning.

Sökstrategin baserades på kombinationer av termer för anställda, cybersäkerhet, tillit samt organisatoriskt stöd och upplevd kontroll. Exempel på sökord var ”Organisational Trust”, ”Employees”, ”Cyberattack”, ”Cyber Security”, ”Perceived Control” och ”Organisational Support”. För att fånga relevanta studier som inte identifierades i de första sökningarna genomfördes en kompletterande sökning med en ytterligare söksträng den 26 februari 2026. I bilaga 2 redovisas samtliga söksträngar som resulterade i träffar samt vilka databaser som användes, datum, söksträngar i sin helhet och avgränsningar, vilket möjliggör att sökningen kan reproduceras. Sökningen gjordes först med termer för anställda och cybersäkerhet för att samla ett brett urval av artiklar, därefter begränsades resultaten genom att kombinera dem med termer relaterade till tillit. Slutligen inkluderades söktermer för kontroll och upplevt stöd för att ytterligare avgränsa urvalet och säkerställa relevansen för studiens syfte. Detta gjordes på grund av tidsaspekten av

genomförandet av studien, samtidigt bör det noteras att relevanta artiklar som använder andra termer kan ha förbisetts.

Sökmatiserna (se bilaga 2) visar även urvalsstegen med antal träffar och antal efter screening. I det första urvalssteget visas dubblettexkludering som genomfördes med hjälp av rayyan.ai (Rayyan 2026). I det andra urvalssteget visas antalet artiklar som gick vidare efter genomgång av titlar och abstracts. För att minska subjektivitet läste författarna först varje titel och abstract individuellt och diskuterade sedan sina bedömningar gemensamt utifrån studiens inklusions- och exklusionskriterier. Därefter lästes samtliga artiklar i fulltext innan det slutliga urvalet av artiklar fastställdes. Totalt genomfördes fem sökningar som resulterade i träffar och 16 artiklar inkluderades. I tabell 1 presenteras den föreliggande studiens urvalskriterier vid litteratursökningen.

Tabell 1. Översikt över urvalskriterier vid litteratursökning

Inklusionskriterier	Exklusionskriterier
Artiklar publicerade 2015–2025	Artiklar publicerade före 2015
Peer-Review granskade artiklar	Icke Peer-Review granskade artiklar
Tillgängliga i fulltext	Ej tillgängliga i fulltext
Kvantitativa studier (huvudsakligen) samt vissa kvalitativa och konceptuella för att öka förståelsen	Studier som inte bidrar till relevant teoretisk eller empirisk bredd
Studier om cyberincidenter i organisatoriska sammanhang	Studier med enbart tekniskt fokus
Fokus på medarbetarnas perspektiv	Fokus enbart på ledningsperspektiv
Behandlar tillit i relation till cybersäkerhet	Saknar koppling till tillit, cybersäkerhet eller organisation

I bilaga 1 presenteras ett PRISMA-diagram för att visualisera flödet från den första sökningen till det slutgiltiga urvalet (Page et al. 2021) samt ett ytterligare PRISMA-diagram för att visualisera hur det tidigare urvalet kompletterades med den senare sökningen (Haddaway, Page, Prichard & McGuinness 2022). Flödesschemat bidrar till ökad transparens i urvalet av litteratur, men det bygger på en standardiserad mall på engelska. Det sammanlagda sluturvalet säkerställer att studien bygger på aktuella, relevanta och vetenskapligt kvalitetssäkrade artiklar.

2.2 Tidigare forskning om hantering av cybersäkerhet

Medarbetarnas tillit till arbetsgivarens cybersäkerhetshantering påverkas av hur organisationen agerar och hur medarbetarna uppfattar dessa insatser (Svenson, Ballóva

Mikušková & Launer 2023; Searle, Renaud & van der Werff 2024). I takt med att cyberbrottskostnader förväntas öka betonar forskning också vikten av att organisationer arbetar med cybersäkerhet som en helhet (Yarovenko et al. 2025). En god digital beredskap för cyberhot skapas genom styrning, transparens och institutionell kvalitet (Yarovenko et al. 2025). Detta innebär för organisationer att cybersäkerhet inte bara hanteras genom tekniska lösningar, utan även genom organisatoriska och kulturella förändringar som påverkar hur säkerhetsarbete integreras i den dagliga verksamheten (Wang, Asif, Shahzad & Ashfaw 2024). Etablering av säkerhetsramverk och en säkerhetsmedveten organisationskultur har visat sig vara exempel på förändringar som kan stärka tilliten hos anställda (Wang et al. 2024).

Searle, Renaud och van der Werff (2024) belyser att när ett cyberangrepp redan skett kan tilliten till organisationen stärkas genom tidiga insatser, empatiskt ledarskap och transparent kommunikation eller försvagas om fokus läggs på tekniska lösningar och/eller traditionella ledningsmetoder. Andra studier visar att även medarbetarnas copingförmåga påverkas av ledningens empati och resurstöd (Stacey, Taylor, Olowosule & Spanakis 2021). När stöd och resurser upplevs som tillgängliga kan detta bidra till att medarbetare får bättre förutsättningar att hantera situationen, vilket även kan stärka deras tillit till organisationen (Stacey et al. 2021). Dessutom kan tilliten stärkas om medarbetarna uppfattar arbetsgivaren som kompetent och ansvarstagande i sitt agerande i säkerhetsfrågor (Svenson, Ballóva Mikušková & Launer 2023).

Tillit uppstår dock inte enbart av vilka åtgärder som genomförs, utan hur medarbetaren tolkar och värderar dem. Svenson, Ballóva Mikušková och Launer (2023) beskriver tillit i form av trovärdighet som en subjektiv bedömning där medarbetarna väger risker mot fördelar i en värderingsprocess. Ett exempel på risk är upplevelser av förlust av kontroll över information, medan ett exempel på fördelar är upplevelser av organisatorisk trygghet (Svenson, Ballóva Mikušková & Launer 2023). Eftersom cybersäkerhet är ett komplext område sker denna värderingsprocess sällan genom endast en rationell analys, utan påverkas också av subjektiva bedömningar och hur information bearbetas och tolkas av medarbetaren (Svenson, Ballóva Mikušková & Launer 2023). Det blir tydligt att hur arbetsgivaren hanterar cybersäkerhet är viktigt för hur medarbetaren uppfattar och tolkar cybersäkerhetsåtgärder, vilket i sin tur kan påverka tilliten. Stacey et

al. (2021) lyfter även fram organisatoriskt stöds betydelse för att skapa och upprätthålla tillit, därav blir det relevant att undersöka detta vidare.

Nedan presenteras Tabell 2 som sammanfattar studierna som ingår i detta tema. Tabellen utgör en del av studiens dataextraktion (Higgins et al. 2019), och visar författare, år, plats, syfte, metod, typ av data, deltagare och huvudresultat för tidigare forskning som behandlar hantering av cybersäkerhet.

Tabell 2. *Dataextraktion av studier om hantering av cybersäkerhet (Higgins et al. 2019).*

Författare/ År	Plats	Syfte	Metod	Typ av data	Deltagare (N)	Resultat
Svenson, Ballová Mikušková & Launer (2023)	Slovakien	Att undersöka hur rationellt tänkande och intuitivt tänkande påverkar anställdas tillit till personuppgiftsskydd.	Tvårsnitts- design	Enkätdata	N =228	Det fanns ett samband mellan rationellt och intuitivt tänkande och tillit till personuppgiftsskydd. IT-erfarenhet och personlighet hade liten betydelse.
Yarovenko et al. (2025)	Europeiska länder	Att undersöka hur digitalisering påverkar länders beredskap att bekämpa cyberbrott	Longitudinell design (2012–2024)	Paneldata	28 länder	Digitalisering förbättrade inte automatiskt cybersäkerheten; effektiv styrning, transparens och institutionell kvalitet var avgörande
Wang, Asif, Shahzad & Ashfaq (2024)	Pakistan	Att undersöka bankers utmaningar och strategier kring datasekretess och cybersäkerhet	Tvårsnitts- design	Kvalitativ intervjudata	N =15 (IT- specialister)	Säkerhetsåtgärder och regelefterlevnad ökade tilliten, medan intrång, bristande hothantering och externa parter minskade den
Searle, Renaud & van der Werff (2024)	USA	Att undersöka hur tillit inom organisationer påverkas efter cyberattacker eller dataintrång	Konceptuell studie	Dokument- data		Tidigt agerande och öppen kommunikation stärkte tillit, men försvagades av tekniskt fokus och bristande hantering av sårbarhet
Stacey, Taylor, Olowosule & Spanaki (2021)	Stor- britannien	Att undersöka arbetstagares emotionella reaktioner och coping-mekanismer vid cyberangrepp	Tvårsnitts- design	Kvalitativ intervjudata	N=24 (IT-personal och icke- IT-personal)	Copingförmåga stärktes av ledningens empati och resurstöd, vilket ökade tilliten till organisationen

2.3 Tidigare forskning om organisatoriskt stöd och tillit

Organisatoriskt stöd kan förstås som både formella resurser, såsom utbildning och information, och informella faktorer som en inkluderande kultur och social interaktion (Safie, Zulkifili, Sary & Basha 2025; Hawthorne 2025; Dang-Pham, Kautz, Pittayachawan och Bruno 2019). Två viktiga aspekter i organisatoriskt stöd är tillgång till information och hur säkerhetsresurser kommuniceras, och har visat sig påverka hur tillit till cybersäkerhetsarbete formas (Dang-Pham et al. 2019; Hawthorne 2025; Müller, Nohe, Reiners, Becker & Hertel 2025).

Kommunikation och tillgång till säkerhetsrelaterade verktyg underlättar socialiseringen och lärandet i organisationer (Dang-Pham et al. 2019). Tydlig information har dessutom visat sig ha större betydelse för tillit än kollegors individuella egenskaper (Hawthorne 2025), vilket kan tyda på att informationsbrist kan försvaga förtroendet till arbetsgivaren. Även Müller et al. (2025) betonar vikten av organisatoriska resurser och strategier, då dessa kan minska kognitiv belastning för medarbetaren och därigenom stärka förtroendet för organisationens säkerhetsarbete. Safie et al. (2025) framhåller att utbildningsresurser kan vara en sådan insats och har visat sig minska osäkerheten kring digitala hot, eftersom det ses som att organisationen tar riskhantering på allvar.

Organisatoriskt stöd uttrycks genom den kultur som etableras kring cybersäkerhet. När säkerhetsarbete framstår som en belastning för de anställda skapas motstånd och negativa effekter, medan en inkluderande säkerhetskultur kan främja delaktighet och engagemang (Borkovich, Skovira & Kohun 2023). Forskning visar även att cybersäkerhetskultur är mest effektiv när den drivs av ledningen (Borkovich, Skovira & Kohun 2023), vilket indikerar att ledningens engagemang kan signalera organisatoriskt ansvarstagande och påverka hur medarbetare tolkar och följer säkerhetsrutiner. Upplevt stöd har även visat sig öka anställdas vilja att dela säkerhetsrelaterad kunskap och bidra till gemensamma säkerhetsinsatser (Safa & von Solms 2016). Även om organisatoriskt stöd kan skapa organisatoriska förutsättningar för tillit kan individuella faktorer spela roll, som individens egen kontrolluppfattning kring cybersäkerhetsarbete.

I Tabell 3 nedanför presenteras en sammanställning av de studier som ingår i detta tema. Tabellen utgör en del av studiens dataextraktion (Higgins et al. 2019), och visar författare, år, plats, syfte, metod, typ av data, deltagare och huvudresultat för tidigare forskning som behandlar organisatoriskt stöd och tillit.

Tabell 3. *Dataextraktion av studier om organisatoriskt stöd och tillit (Higgins et al. 2019).*

Författare/ År	Plats	Syfte	Metod	Typ av data	Deltagare (N)	Resultat
Safie, Zulkifli, Sapry & Bashah (2025)	Malaysia	Att undersöka hur institutionellt stöd och organisatoriska åtgärder påverkar anställdas förtroende vid digitala hot	Tvärsnitts- design	Enkätdata	N = 157 (myndighets- anställda från tio olika myndigheter)	Implementering påverkades av individuella uppfattningar samt organisatoriska resurser, särskilt träning och stöd

Hawthorne (2025)	Storbritannien & USA	Att undersöka hur tillit till kollegor påverkar tillgång till information i arbetet	Tvärsnittsdesign	Enkätdata	N = 1149 (heltidsanställda)	Tillräcklig information hade större betydelse för tillit än kollegors egenskaper
Dang-Pham, Kautz, Pittayachawan & Bruno (2019)	Vietnam	Att undersöka hur informations säkerhets klimat utvecklas och hur sociala nätverk påverkar informations säkerhet	Longitudinell design	Enkätdata	N = 151 (kontorsanställda)	Sociala nätverk och nyckelpersoner stärkte säkerhetskulturen; tekniska åtgärder behövde kompletteras med sociala insatser
Müller, Nohe, Reiners, Becker & Hertel (2025)	Tyskland	Att undersöka faktorer som bygger förtroende för informationssystem samt hur förtroende påverkar prestation och kognitiva resurser	Longitudinell design	Enkätdata	N = 157 (företagsanställda)	Förtroendet för informationssystem ökade prestation och kognitiva resurser samt minskade ansträngning; långsiktiga strategier krävdes
Borkovich, Skovira & Kohun (2023)	USA	Att undersöka hur cyberkultur påverkar organisationers cybersäkerhet	Konceptuell studie	Dokumentdata		Cyberkultur påverkade cybersäkerhet i hög grad; en positiv kultur stärkte säkerhetsarbetet, medan brister ökade sårbarheten
Safa & von Solms (2016)	Malaysia	Att undersöka faktorer som påverkar anställdas kunskapsdelning inom informations säkerhet	Tvärsnittsdesign	Enkätdata	N = 482 (finansanställda)	Motivation, attityd, sociala normer och upplevd kontroll påverkade viljan att dela kunskap. Organisatoriskt stöd och tillit ökade den faktiska kunskapsdelningen

2.4 Tidigare forskning om upplevd kontroll och tillit

Anställdas upplevda kontroll kan förklara hur tilliten till cybersäkerhetshantering skapas. Detta stöds av Svenson, Ballóva Mikušková & Launer (2023) som visar att även om organisationen sätter in olika typer av stöd kan de anställdas personliga känsla för hur mycket kontroll de har över situationen också påverka tilliten. Upplevd kontroll i samband med cyberincidenter utvecklas genom samspelet mellan organisatoriska resurser och individens förmåga att tolka och agera på säkerhetsinformation (Avrahami & Zwilling 2025). När organisationen erbjuder tydlig kommunikation och stödjande strukturer stärks handlingsförmågan, vilket i sin tur ökar de anställdas upplevda kontroll och förtroendet för organisationens cybersäkerhetsarbete (Avrahami & Zwilling 2025).

Lowry, Posey, Bennetts och Roberts (2015) menar att upplevd kontroll skapas av hur rättvisa och legitima säkerhetsåtgärder uppfattas. Om säkerhetsåtgärderna upplevs som orättvisa eller alltför restriktiva kan anställdas känsla av autonomi minska, vilket kan riskera att tilliten till organisationens cybersäkerhetsarbete försvagas (Lowry et al. 2015). Medarbetarnas uppfattning om i vilken utsträckning de kan påverka och förstå säkerhetsrelaterade beslut är avgörande för hur tillit utvecklas. Detta underbyggs av Ghaleb och Pardeav (2025) som visar att om säkerhetsåtgärder uppfattas som

påverkningsbara och legitima av medarbetarna kan upplevelsen av kontroll öka och i sin tur stärka förtroendet för organisationen.

Tilltro till organisationens tekniska säkerhetslösningar påverkar även hur anställda upplever sitt eget ansvar och sin kontroll (Butavicius et al. 2020). Stark tilltro till tekniska säkerhetslösningar kan ge en falsk känsla av kontroll, där medarbetarnas eget ansvar och vaksamhet minskar (Butavicius et al. 2020). Om den upplevda kontrollen i hög grad baseras på teknikens antagna förmåga snarare än på individens egen bedömning riskerar medarbetare att tolka organisationens kompetens och pålitlighet på ett felaktigt sätt (Butavicius et al. 2020). Boritz, Ge och Patterson (2022) fann att det fanns individuella skillnader som påverkar individers förmåga, uppfattning och hantering av information om cyberhot. Det handlar om hur benägna medarbetare är på att uppmärksamma, tolka och agera på risker (Boritz, Ge & Patterson 2022). Därmed kan resultaten från Boritz, Ge och Patterson (2022) förstås som att upplevd kontroll kan ses som en individuell faktor, eftersom individer skiljer sig åt i hur de bedömer och hanterar risker.

Nedanför presenteras Tabell 4 som sammanfattar studierna som ingår i detta tema. Tabell 4 visar författare, år, plats, syfte, metod, typ av data, deltagare och huvudresultat för tidigare forskning som behandlar upplevd kontroll och tillit (Higgins et al. 2019).

Tabell 4. *Dataextraktion av studier om upplevd kontroll och tillit (Higgins et al. 2019).*

Författare/ År	Plats	Syfte	Metod	Typ av data	Deltagare (N)	Resultat
Svenson, Ballová Mikušková & Launer (2023)	Slovakien	Att undersöka hur rationellt tänkande och intuitivt tänkande påverkar anställdas tillit till personuppgiftsskydd	Tvärsnitts- design	Enkätdata	N = 228	Det fanns ett samband mellan rationellt och intuitivt tänkande och tillit till personuppgiftsskydd. IT- erfarenhet och personlighet hade liten betydelse
Avrahami & Zwilling (2025)	Israel	Att undersöka hur tekniska lösningar och männliga faktorer samverkar för att stärka cyberresiliens	Tvärsnitts- design	Enkätdata	N = 208 (cybersäkerhets- experter)	Insamling och analys av cyberhot stärkte medarbetarnas färdigheter och organisationens resiliens; effektiva strategier krävde en kombination av tekniska lösningar och kunskap
Lowry, Posey, Bennett & Roberts (2015)	USA	Att undersöka faktorer bakom anställdas negativa reaktioner på skärpta informationssäkerhets- policyer	Tvärsnitts- design	Enkätdata	N = 533 (anställda inom finans)	Skärpta policyer skapade negativa reaktioner när de upplevdes som orättvisa medan tydlighet och rättvisa ökade tilliten och minskade regelbrott.
Ghaleb & Pardaev (2025)	Saudi- arabien	Att undersöka faktorer som påverkar informationssäkerhets- beteende	Tvärsnitts- design	Enkätdata	N = 261 (anställda på produktions- företag)	Organisationskultur och medvetenhet ökade säkerhetsbeteende; engagemang och tillit till ledningen förstärkte effekterna

Butavicius et al. (2020)	Australien	Att undersöka tillit till tekniska säkerhetslösningar och dess påverkan på säkerhetsbeteenden	Experiment- & tvärsnittsdesign	Enkät- & experimentdata	N = 607 (användare av digitala enheter på jobbet)	Övertro till tekniska säkerhetslösningar var kopplad till lägre medvetenhet och sämre phishingidentifiering, men ej lösenordsstyrka
Boritz, Ge & Patterson (2022)	Kanada	Att undersöka individuella faktorer som påverkar anställdas mottaglighet för phishingattacker	Tvärsnittsdesign	Enkäter & observation	N = 208 (bank- & företag-anställda)	Skepticism, impuls kontroll och yrkescertifiering minskade mottagligheten för phishing, medan vissa kognitiva faktorer och ökade sårbarheten

2.5 Sammanfattning och egen positionering till tidigare forskning

Sammantaget visar den tidigare forskningen som har presenterats ovan att tillit till arbetsgivarens hantering av cybersäkerhet skapas både av hur organisationer agerar och hanterar cyberhot samt hur medarbetare uppfattar och värderar de åtgärder som vidtagits (Searle et al. 2024; Svenson, Ballóva Mikušková & Launer 2023). Arbetsgivarens hantering av säkerhetsåtgärder påverkar därmed inte bara teknikens säkerhet utan den kommunicerar även signaler om organisationens ansvarstagande och kompetens till sina anställda (Searle et al. 2024; Wang et al. 2024; Svenson, Ballóva Mikušková & Launer 2023). Den tidigare forskningen visar även att organisatoriska resurser, som informationstillgång och stödjande strukturer, är avgörande faktorer för att skapa och upprätthålla tillit i kontexten av informationssäkerhet (Dang-Pham et al. 2019; Müller et al. 2025; Safie et al. 2025; Hawthorne 2025). Ännu en faktor som spelar roll för hur anställda tolkar informationssäkerhet är upplevd kontroll. Den upplevda kontrollen skapas i samspelet mellan organisatoriska strukturer, hur information tolkas och individuella förutsättningar som därigenom påverkar hur tillit utvecklas vid cyberincidenter (Avrahami & Zwilling 2025; Butavicius et al. 2020; Boritz, Ge & Patterson 2022; Ghaleb & Pardaev 2025; Svenson, Ballóva Mikušková & Launer 2023).

Samtidigt har tidigare forskning som används i vår studie ofta analyserat organisatoriska och individuella faktorer separat, och sällan kopplat dem till just tilliten till arbetsgivarens cybersäkerhetshantering. Vid den systematiska litteratursökningen framkom dessutom att kombinationer av begrepp som organisatorisk tillit, upplevd kontroll, stöd och tillit till organisations cybersäkerhet genererade i få eller inga träffar på de utvalda databaserna. Detta kan tyda på att forskningsfältet behandlat dessa faktorer var för sig eller sett på andra omständigheter. För att hantera denna observerade kunskapslucka fokuserar föreliggande studie på sambandet mellan tillit till arbetsgivarens

cybersäkerhetshantering och individuella samt organisatoriska faktorer. För att möjliggöra en hanterbar forskningsdesign avgränsas studien till en individuell faktor som i denna studie är arbetsrelaterad kontrolluppfattning, medan andra faktorer såsom personlighetstyper och teknisk kompetens har uteslutits. Studien avgränsar organisatoriska faktorer till generell organisatorisk tillit och organisatoriskt stöd. Organisatoriskt stöd har avgränsats till hur säkerhetsrelaterad information och resurser kommuniceras till medarbetarna, snarare än utbildningsinsatser och organisationskultur. Utöver ovanstående avgränsningar är många studier genomförda utanför svensk kontext, vilket begränsar deras överförbarhet. Förhoppningen med föreliggande studie är att öka förståelsen för ämnet i en svensk kontext med teoretiska insikter om de sociala processerna runt upplevelsen av tillit kring cybersäkerhet, snarare än att fokusera på de tekniska aspekterna. Ur ett socialpsykologiskt perspektiv kan studien ge insikt i hur medarbetare tolkar organisatoriska signaler och hur dessa tolkningar påverkar deras upplevelse av kontroll och därigenom deras tillit till arbetsgivarens cybersäkerhetshantering. Detta kan bidra till ökad förståelse för samspelet mellan individ och organisation.

3. Teoretiska utgångspunkter

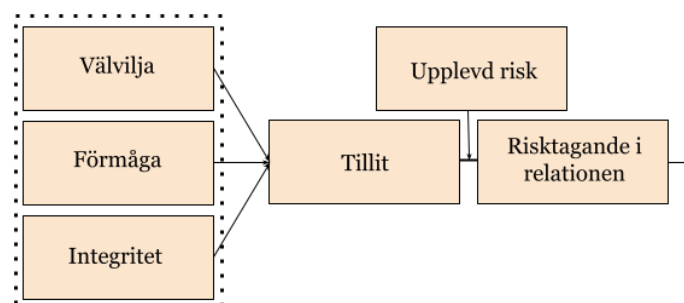
I detta avsnitt presenteras studiens teoretiska ramverk. Studien fokuserar på tillit till arbetsgivarens cybersäkerhetshantering, alltså hur medarbetarna uppfattar ledningens förmåga och vilja att skydda information och digitala system. Ramverket består av tre teoretiska begrepp. *Organisatorisk tillit* fångar medarbetarnas bedömning av ledningens pålitlighet och kompetens. *Upplevt organisatoriskt stöd* visar hur stöd och omsorg från ledningen påverkar förtroendet, medan *arbetsrelaterad kontrolluppfattning* belyser individuella skillnader i hur medarbetare tolkar och reagerar på säkerhetsåtgärder. Tillsammans utgör dessa teorier ett ramverk för att förstå tilliten till arbetsgivarens cybersäkerhetsarbete inom kommunal verksamhet.

3.1 Organisatorisk tillit

Tillit innebär en vilja att göra sig sårbar inför någon annans handlingar och bygger på en förväntan om att den andra parten agerar på ett sätt som är viktigt för individen, även när kontroll saknas (Mayer, Davis & Schoorman 1995). I en organisationskontext betyder

tilliten att medarbetare är villiga att ta risker och agera, eftersom deras arbetsituation ofta påverkas av organisationens beslut och kompetens (Mayer, Davis & Schoorman 1995; Schoorman, Mayer & Davis 2007). Detta innebär att tilliten blir en avgörande faktor för att skapa ett välfungerande och effektivt arbete inom organisationen (Mayer, Davis & Schoorman 1995; Schoorman, Mayer & Davis 2007). I samband med cybersäkerhet kan detta betyda att medarbetare uppfattar att organisationen har en god förmåga att hantera hot och incidenter, vilket gör det möjligt för medarbetarna att fokusera på sitt dagliga arbete trots förekomsten av cybersäkerhetsrisker.

Mayer, Davis och Schoorman (1995) har utvecklat en integrerad modell för organisatorisk tillit, där de menar att tillit uppstår genom samspelet mellan individens benägenhet att lita på andra och bedömningen av motpartens upplevda pålitlighet. Denna pålitlighet bedöms utifrån tre faktorer: förmåga, välvilja och integritet (Mayer, Davis & Schoorman 1995). Samspelet mellan dessa faktorer bidrar till en viss nivå av tillit. Det är dock viktigt att skilja mellan tillit, som avser viljan att göra sig sårbar, och det faktiska beteendet att ta en risk i relationen (Mayer, Davis & Schoorman 1995). Även om modellen ursprungligen utvecklades för att förklara tilliten mellan individer har efterföljande studier visat att den kan tillämpas på organisationsnivå, där uppfattningar om förmåga, välvilja och integritet påverkar i vilken grad organisationen uppfattas som pålitlig (Schoorman, Mayer & Davis 2007). I Figur 1 presenteras modellen och efter figuren följer en vidare beskrivning av modellen. Det är viktigt att poängtera att modellen används i denna studie för att förstå hur generell organisatorisk tillit utvecklas, snarare än att dessa komponenter kommer empiriskt prövas var för sig.



Figur 1 Illustrering av Integrerad modell för organisatorisk tillit översatt till svenska av denna studies författare (Mayer, Davis & Schoorman 1995).

Förmåga avser den upplevda kompetensen inom ett specifikt område och kan förklaras som domänspecifikt (Mayer, Davis & Schoorman 1995). Domänspecifikt innebär att organisationen kan uppfattas som mer kompetent inom ett område, men mindre kompetent i ett annat (Schoorman, Mayer & Davis 2007). Detta leder till att organisatorisk tillit till arbetsgivaren kan samexistera med låg tillit till organisationens förmåga att hantera frågor som cybersäkerhet. Tillit i relation till cybersäkerhetsfrågor kan därför ses som en domänspecifik form av tillit.

Utöver förmåga påverkas upplevelsen av tillit även av välvilja som avser i vilken grad organisationen uppfattas agera i medarbetarnas intresse (Mayer, Davis & Schoorman 1995). Välvilja innebär att organisationen upplevs ha en genuin vilja att främja medarbetarnas bästa, och inte endast handla utifrån egen vinning (Mayer, Davis & Schoorman 1995; Schoorman, Mayer & Davis 2007). Detta kan kopplas till organisationens strukturer, där organisationen använder olika system för exempelvis rapportering, säkerhet och efterlevnad av policyer (Schoorman, Mayer & Davis 2007). I ett cybersäkerhetssammanhang kan det handla om hur säkerhetsåtgärder upplevs. Ett exempel är om system används främst för övervakning, snarare än för att skydda medarbetarnas trygghet eller säkerhet. Detta kan minska upplevelsen av välvilja och därigenom delar av den organisatoriska tilliten (Schoorman, Mayer & Davis 2007).

Den sista faktorn är integritet som avser upplevelsen att organisationen agerar konsekvent och i enlighet med de principer som medarbetarna anser acceptabla (Mayer, Davis & Schoorman 1995; Schoorman, Mayer & Davis 2007). Bedömningen av integritet påverkas av faktorer som tidigare erfarenheter, känsla av rättvishet samt i vilken grad organisationens handlingar överensstämmer med dess uttalade intentioner (Mayer, Davis & Schoorman 1995). Det råder en maktobalans och informationsasymmetri mellan organisationen och medarbetarna där organisationen har större möjligheter att styra relationen (Schoorman, Mayer & Davis 2007). Detta blir särskilt tydligt i relation till cybersäkerhet, där arbetsgivaren styr informationen om säkerhetsåtgärder och hantering av personuppgifter (IMY 2021b). Medarbetare blir därmed beroende av att organisationen agerar konsekvent och ansvarsfullt. Om organisationens hantering upplevs som otydlig eller bristfällig kan detta påverka tilliten till arbetsgivarens cybersäkerhetshantering negativt.

I denna studie förstås organisatorisk tillit som en generell tillitsform till organisationen som kan relateras till den mer specifika tilliten till arbetsgivarens cybersäkerhetshantering. Tillitens domänspecifika natur innebär att dessa kan särskiljas, men samtidigt vara kopplade till varandra. Detta gör det rimligt att anta att medarbetare som uppvisar hög organisatorisk tillit också tenderar att ha högre tillit till arbetsgivarens hantering av cybersäkerhet, vilket motiverar följande hypotes:

H1: Det finns ett positivt samband mellan organisatorisk tillit och tillit till arbetsgivarens cybersäkerhetshantering.

3.2 Upplevt organisatoriskt stöd

För att förstå vad som kan inverka på medarbetares tillit till arbetsgivarens cybersäkerhetsarbete appliceras teorin upplevt organisatoriskt stöd. *Upplevt organisatoriskt stöd* avser medarbetares uppfattningar om hur organisationen värdesätter deras arbetsinsatser och bryr sig om deras välbefinnande (Eisenberger et al. 1986). Enligt Eisenberger et al. (1986) tenderar medarbetare att tolka organisationens handlingar, beslut och kommunikation som uttryck för organisationens avsikter. Detta innebär att organisationen personifieras som en aktör som bär ansvaret och har avsiktliga intentioner (Eisenberger et al. 1986). Upplevelsen av organisatoriskt stöd skapas därmed både genom organisationens agerande samt det dagliga samspelet mellan chefer och kollegor, där chefer uppfattas som representanter för organisationen (Eisenberger et al. 1986).

Stödjande åtgärder kan uppfattas av medarbetarna som tecken på omsorg och ansvarstagande, medan bristande stöd kan tolkas som likgiltighet eller brist på engagemang (Eisenberger et al. 1986). Hur stödet upplevs kan bero på tidigare händelser som exempelvis hur organisationen har reagerat på tidigare misstag (Eisenberger et al. 1986). Upplevelsen av stöd bidrar till att skapa ett positivt känslomässigt band mellan medarbetaren och organisationen, som i sin tur kan stärka medarbetarens prestation för att nå organisationens mål (Eisenberger et al. 1986).

Eisenberger, Fasolo och Davis-LaMastro (1990) betonar att den starkaste indikationen på att organisationen bryr sig är när handlingarna uppfattas som frivilliga. Detta innebär att när organisationen erbjuder stöd utöver vad som formellt krävs, signalerar det till medarbetare att de genuint bryr sig (Eisenberger, Fasolo & Davis-LaMastro 1990). Kommunikation spelar en avgörande roll, inte bara för beröm och

erkännande, utan även för hur viktig information når medarbetarna. För att medarbetarna ska känna sig sedda och värderade behöver kommunikationen upplevas som äkta, både när det gäller erkännande av insatser och i delning av information (Eisenberger et al. 1986; Eisenberger, Fasolo & Davis-LaMastro 1990).

När organisationen kommunicerar omsorg, erbjuder hjälp och tar ansvar i svåra situationer kan detta stärka uppfattningen om att arbetsgivaren vill medarbetarnas bästa, vilket i sin tur kan öka viljan att förlita sig på organisationen (Mayer, Davis & Schoorman 1995; Eisenberger et al. 1986). Vid cyberincidenter finns det en risk för ökad osäkerhet och sårbarhet hos medarbetarna. Detta innebär att hur organisationen kommunicerar stöd och hanterar konsekvenserna spelar en viktig roll för hur medarbetarna uppfattar cyberincidenten och därigenom utvecklar tillit. Mot bakgrund av detta antas att upplevt organisatoriskt stöd kan bidra till att upprätthålla eller reparera tilliten till arbetsgivarens cybersäkerhetshantering, och därför formuleras följande hypotes:

H2: Det finns ett positivt samband mellan upplevt organisatoriskt stöd och tillit till arbetsgivarens cybersäkerhetshantering.

3.3 Arbetsrelaterad kontrolluppfattning

Utöver upplevt organisatoriskt stöd kan medarbetares upplevelse av kontroll över cybersäkerhetsåtgärder påverka hur de tolkar risker. *Kontrolluppfattning* beskriver individens grundläggande uppfattning om var kontrollen över livshändelser placeras (Rotter 1966). I denna studie tillämpas arbetsrelaterad kontrolluppfattning som är en vidareutveckling på kontrolluppfattning fast i en organisationskontext (Spector 1982). *Arbetsrelaterad kontrolluppfattning* handlar om att förstå hur känsla av kontroll påverkar hur medarbetare tänker, känner och agerar i arbetssituationer (Spector 1982). Spector (1982) beskriver att personer med hög kontrolluppfattning tenderar att se utfall som påverkbara genom sina egna handlingar, medan personer med låg kontrolluppfattning upplever att händelser styrs av yttre faktorer, såsom tur eller oförutsägbara omständigheter.

Skillnader i arbetsrelaterad kontrolluppfattning blir särskilt relevant i relation till risk. Situationer som upplevs som okontrollerbara tenderar att framstå som mer hotfulla, medan om de upplevs som hanterbara kan de tolkas som mindre riskfyllda (Spector 1982). Graden av kontrolluppfattning kan därför påverka hur sårbar en individ känner sig.

Medarbetare med högre kontrolluppfattning är generellt sett mer benägna att ha en positiv inställning till sitt arbete och till organisationen som helhet (Spector 1982). De brukar känna större engagemang, arbetstillfredsställelse och en högre benägenhet att aktivt påverka sin arbetssituation genom att söka information inom organisationen (Spector 1982). I en organisatorisk cybersäkerhetskontext kan arbetsrelaterad kontrolluppfattning kopplas till i vilken utsträckning medarbetare sätter sig in i och försöker förstå organisationens rutiner och åtgärder kring cybersäkerhet. En högre upplevd kontroll kan innebära att medarbetare i större utsträckning engagerar sig i att förstå hur arbetsgivaren arbetar med cybersäkerhet och cyberrisker, vilket kan bidra till en mer nyanserad uppfattning om säkerhetsarbetet och dess hantering. Detta kan vara kopplat till en minskad upplevelse av komplexitet och hot, och därför kan det finnas ett samband mellan hög arbetsrelaterad kontroll och tillit till arbetsgivarens cybersäkerhetshantering. Mot bakgrund av detta formuleras följande hypotes:

H3: Det finns ett positivt samband mellan arbetsrelaterad kontrolluppfattning och tillit till arbetsgivarens cybersäkerhetshantering.

3.4 Förklarande faktorer för tillit till arbetsgivarens cybersäkerhetshantering

Sammanfattningsvis utgör teorierna studiens teoretiska ramverk för att förstå hur medarbetarna uppfattar tillit till arbetsgivarens cybersäkerhetshantering. Organisatorisk tillit avser medarbetarnas uppfattning om arbetsgivarens förmåga, välvilja och integritet (Mayer, Davis & Schoorman 1995) och antas utgöra den generella tilliten till arbetsgivaren, medan upplevt organisatoriskt stöd speglar i vilken grad organisationen uppfattas bry sig om och stödjer sina medarbetare (Eisenberger et al. 1986). Arbetsrelaterad kontrolluppfattning avser i vilken utsträckning medarbetare upplever att de kan förstå och påverka sin arbetssituation (Spector 1982).

I en cybersäkerhetskontext som ofta präglas av komplexa situationer, osäkerhet och begränsad insyn (Regeringen 2025) kan dessa faktorer samverka i hur medarbetare tolkar arbetsgivarens åtgärder och förmåga att hantera cyberrisker. Den generella organisatoriska tilliten kan påverka hur medarbetarna tolkar organisationens agerande i säkerhetsfrågor, upplevt organisatoriskt stöd kan bidra till att säkerhetsåtgärder uppfattas som genuina, medan arbetsrelaterad kontrolluppfattning kan förklara i vilken utsträckning medarbetare sätter sig in i och försöker förstå hur dessa åtgärder fungerar för att hantera

cyberincidenter. I denna studie antas teorierna kunna förklara hur medarbetarna tolkar tilliten till arbetsgivarens cybersäkerhetshandling. Sambanden analyseras med hjälp av en explorativ regressionsanalys som inte är hypotesdriven.

4. Metod

I detta avsnitt presenteras den vetenskapsteoretiska utgångspunkten, metodval, operationalisering, empiriska instrument, urval, tillvägagångssätt, analysmetod, kvalitetskriterier och etik.

4.1 Vetenskapsteoretisk utgångspunkt

Studiens vetenskapliga utgångspunkt följer en positivistisk tradition men med nyrealistisk syn på kunskap. Den positivistiska utgångspunkten innebär att mänskligt beteende kan studeras empiriskt, även om full objektivitet inte är möjligt (McGhee 1998, s.7). Det nyrealistiska synsättet utgår från förståelsen att världen är socialt skapad, samtidigt som det finns en verklighet som existerar oberoende av människan (Wetherell & Still 1998, s.111). Denna ontologiska blick ansågs passa denna studie eftersom vi utgick från att kommunanställdas tillit till arbetsgivarens cybersäkerhetshandling utgör en verklighet som kan studeras empiriskt, även om denna verklighet förstås och uttrycks olika beroende på kontext och individ.

4.2 Metodval

Studien har en kvantitativ ansats med ett hypotetiskt-deduktivt förhållningssätt. Detta innebär att vi formulerade tre hypoteser baserade på teori, samlade in data och analyserade resultatet för att avgöra om hypoteserna kunde stödjas eller förkastas (Clark-Carter 2024, s.10). Detta tillvägagångssätt valdes för att kvantifiera medarbetarnas upplevda tillit till arbetsgivarens cybersäkerhetshandling. Studien använde sig av en tvärsnittsdesign som betyder att variabler mäts vid ett tillfälle utan uppföljning över tid (Clark-Carter 2024, s.50). Datainsamlingen genomfördes via en digital enkät i programmet Qualtrics som distribuerades till medarbetarna vid ett tillfälle. Enkät valdes som datainsamlingsmetod då den är lämplig för att nå ett större antal respondenter på ett tidseffektivt och kostnadseffektivt sätt (Clark-Carter 2024, s.71). Metoden möjliggjorde även standardiserad datainsamling, där samtliga respondenter fick samma frågor, vilket stärker studiens pålitlighet (Clark-Carter 2020, s.7, 25). Trots att tvärsnittsdesign är

tidseffektiv medför den också begränsningar, då den endast kan visa skillnader och samband mellan variablerna men inte förklara deras orsaker (Clark-Carter 2024, s.50). Studien kan därför bara bidra med en del av förståelsen av ämnet.

Den digitala enkätformen innebar flexibilitet för respondenterna att själva välja när och var de ville besvara den, samtidigt gav den möjlighet att använda obligatoriska frågor för att minska internt bortfall. Dock finns det begränsningar med metoden. Enkätformen kan både öka risken för avbrutna svar samt exkludera vissa grupper, exempelvis personer med funktionsvariationer eller bristande språkkunskaper (Clark-Carter 2024, s.70). Detta kan påverka studiens representativitet (Clark-Carter 2024, s.70–72). Vidare kan medarbetarnas tidigare erfarenheter av exempelvis cyberincidenter och/eller relationer till arbetsgivaren ha påverkat svaren, vilket innebär att bakomliggande faktorer som inte undersökts kan ha inverkat på resultatet (Clark-Carter 2024, s.50). Slutligen kan enkätlängden påverka deltagandet, då längre enkäter kan leda till bortfall (Clark-Carter 2024, s.71). För att minimera denna risk avgränsades enkäten till 29 items och det genomfördes en pilotstudie med deltagare som liknar urvalsgruppen.

4.3 Operationalisering

I denna studie är den beroende variabeln tillit till arbetsgivarens cybersäkerhetshantering, medan de oberoende variablerna är organisatorisk tillit, upplevt organisatoriskt stöd och arbetsrelaterad kontrolluppfattning. De teoretiska begreppen operationaliseras till fyra mätbara variabler för att möjliggöra kvantitativ analys. Detta innebär att abstrakta begrepp bryts ner i underliggande begrepp och indikatorer, vilket i sin tur mäts genom specifika påståenden (Clark-Carter 2024, s.29; Hoyle & Duvall 2004, s.314). En fullständig operationaliseringsmatris återfinns i Bilaga 3. Alla variabler förutom tillit till arbetsgivarens cybersäkerhetshantering använde sig av befintliga och validerade mätskalor. Reliabiliteten för alla indexerade skalorna testades med Cronbach's alfa för att bedöma om påståendena mäter samma fenomen, där ett värde över 0.7 räknas som godtagbart och över 0.8 är önskvärda (Pallant 2016, s.101, 104). Nedanför följer en sammanfattning av huvudvariablernas utformning och Cronbach's alfa värden:

Tillit till arbetsgivarens cybersäkerhetshantering (beroende variabel) bygger på kombination av Nationalencyklopedins (u.å.) definition av tillit som *“övertygelsen om att någon är pålitlig och har goda avsikter mot en själv”* och cybersäkerhetshantering som

kan beskrivas som arbetet med att identifiera, skydda mot och upptäcka cyberhot (National Institute of Standards and Technology [NIST] 2024). Variabeln mättes med indikatorerna förtroende för förebyggande insatser, upptäckt, informationshantering och ledningens cybersäkerhetsarbete. Skalan består av fem items exempelvis *“Jag har förtroende för att organisationen kan upptäcka cyberincidenter i tid”*. Ett medelvärdeindex skapades och visade god intern reliabilitet ($\alpha = 0.86$). Eftersom skalan är egenutvecklad genomfördes en explorativ faktoranalys för att undersöka den underliggande faktorstrukturen och säkerställa att alla items mäter ett gemensamt bakomliggande fenomen och stärka begreppsvaliditeten (Clark-Carter 2024, s.360). Resultaten bör dock tolkas med viss försiktighet, då den saknar tidigare validering.

Organisatorisk tillit (oberoende variabel) mättes med en etablerad skala (Mayer & Davis 1999) och omfattar underbegreppen kompetens, välvilja och integritet. Indikatorerna inkluderar upplevd kompetens, upplevd omsorg från ledningen och upplevd principfasthet. Organisatorisk tillit mättes med sex items och exempel på påstående var *“Mina behov och önskemål är mycket viktiga för högsta ledningen”*. Ett medelvärdeindex skapades och även denna visade god intern reliabilitet ($\alpha = 0.84$). Skalan mättes med en femgradig Likertskala från “instämmer inte alls” till “instämmer helt”.

Upplevt organisatoriskt stöd (oberoende variabel) mättes med en etablerad skala (Eisenberger et al. 1986) och operationaliserades genom indikatorerna upplevd uppskattning från ledningen och upplevd villighet från ledningen. Organisatoriskt stöd mättes med sex items och ett exempel är *“Hjälp finns tillgänglig från organisationen när jag har ett problem.”* och mättes på en femgradig Likertskala från “instämmer inte alls” till “instämmer helt”. Ett medelvärdeindex skapades och uppvisade god intern reliabilitet ($\alpha = 0,93$).

Arbetsrelaterad kontrolluppfattning (oberoende variabel) mättes med en etablerad skala (Spector 1988). Som operationaliserades genom underbegreppen intern och extern kontrolluppfattning som ledde till indikatorerna hög och låg kontrolluppfattning för att fånga respondenternas upplevelse av kontroll över sin arbetssituation. Arbetsrelaterad kontrolluppfattning mättes med sex items exempel på påstående var *“Befordringar ges till anställda som presterar bra på jobbet”* och mättes

på en sexgradig skala från "instämmer verkligen inte" till "instämmer helt". Ett medelvärdeindex skapades och uppvisade ett godtagbart värde ($\alpha = 0.7$).

Studien inkluderade kontrollvariabler i form av kön, utbildningsnivå, anställningsform samt daglig digital arbetstid. Dessa mättes med kategoriska svarsalternativ. Ytterligare två kontrollvariabler inkluderades, upplevd risk för cyberhot och rapporterad cybersäkerhetsutbildning från arbetsgivaren. Dessa variabler mättes på Likertskala från "instämmer inte alls" till "instämmer helt" och behandlades som kontinuerliga variabler i analysen. Kontrollvariablerna inkluderades för att reducera risken för snedvridna samband mellan huvudvariablerna.

4.4 Empiriska instrument

Datainsamlingen genomfördes med en digital enkät konstruerad i Qualtrics och distribuerades online. Enkäten bestod sammanlagt av 29 items, detta inkluderar både bakgrundsfrågor och påståenden som respondenterna fick ta ställning till. Syftet med instrumentet var att operationalisera de teoretiska variablerna för att möjliggöra prövning av studiens hypoteser (Borg & Westerlund 2012, s.29). Enkäten var strukturerad i separata block baserade på respektive variabel. Respondenterna besvarade huvudsakligen påståenden på en femgradig Likertskala, förutom arbetsrelaterad kontrolluppfattning som mättes på en sexgradig skala i enlighet med ursprungsskalan (Spector 1998). Valet av Likertskala möjliggjorde nyanserade svar och inkluderade en neutral mittpunkt, utan att ställa för höga krav på precision hos respondenterna (Clark-Carter 2024, s.83, 85). Men samtidigt innebär det en risk att skalstegen kan tolkas olika av respondenterna, vilket kan påverka jämförbarheten och därmed studiens resultat (Clark-Carter 2024, s.85). För ökad tydlighet av enkäten inleddes varje avsnitt med en kort instruktion och begreppsdefinition. Enkäten finns i sin helhet i bilaga 4.

För att säkerställa att den svenska enkätversionen motsvarade originalskalorna genomfördes först en översättning av frågorna till svenska och därefter en back-translation tillbaka till engelska av en oberoende engelsktalande person (Clark-Carter 2024, s.29). Detta gjordes för att kontrollera att innebörden i frågorna inte förändrades. Slutligen gjordes mindre språkliga justeringar för att anpassa formuleringar till studiens kontext och för att göra enkäten enklare att besvara. Ett antal påståenden var negativt formulerade och omkodades inför analysen för att säkerställa en enhetlig riktning i

samtliga skalor. Detta gällde items i organisatorisk tillit "*Högsta ledningens handlingar och beteenden är inte särskilt konsekventa*" samt tre items inom arbetsrelaterad kontrolluppfattning "*Befordringar beror oftast på tur*", "*På de flesta arbeten krävs mycket tur för att bli en framstående medarbetare*" och "*Skillnaden mellan personer som tjänar mycket respektive lite pengar beror till stor del på tur*". Omkodningen genomfördes för att säkerställa att samtliga påståenden tolkas i samma riktning vid indexerings av skalorna. Anpassningarna kan påverka skalornas validitet och reliabilitet. Intern reliabilitet kontrollerades genom Cronbach's alfa-test på samtliga skalor.

4.5 Urval

Studien använde sig av icke-slumpmässigt urval, vilket innebär att inte alla enheter av målpopulationen hade möjlighet att delta (Daniel 2011, s.258). Ett slumpmässigt urval hade kunnat ge mer representativa resultat, men detta ansågs inte vara genomförbart inom studiens tidsramar och med de praktiska begränsningarna i tillgång till kommunanställda. Urvalet genomfördes i flera steg. Först skickades en förfrågan om deltagande till HR-chefer i 30 kommuner i Västra Götaland, men endast tre kommuner valde att delta. Kontaktpersonerna i dessa kommuner fungerade som grindvakter, det vill säga personer som kontrollerar åtkomsten till den miljö forskningen avser att nå (Clark-Carter 2024, s.91). De avgjorde själva om kommunens medarbetare skulle bjudas in till studien och därefter fick medarbetarna ta ställning till om de ville delta, vilket innebar självselektion i två steg (Clark-Carter 2024, s.72, 99). Detta kan göra att vissa grupper deltar oftare än andra. I vår studie kan de tänkas att medarbetare som arbetar med eller har intresse för IT i högre grad kan ha valt att delta då de uppfattar ämnet som relevant. Därför kan vi i studien inte utesluta urvalsbias och som en följd av detta ett skevt urval, där deltagarna inte fullt ut representerar den population som studien avser (Clark-Carter 2024, s.72).

Första steget av urvalet kan beskrivas som ett målinriktat urval där syftet var att inkludera kommunanställda. Målinriktat urval innebär att forskaren medvetet väljer deltagare som uppfyller specifika kriterier, som att de tillhör en specifik grupp (Clark-Carter 2024, s.143). Urvalskriterierna baserades på anställning i kommunal verksamhet i Sverige utan uppdelning efter yrkesroll. Informationsbrev och enkäter skickades via kontaktpersoner på kommunerna till arbetsmejl och publicerades på interna digitala forum för att nå ut till urvalsgruppen. Trots hjälp från grindvakter nådde inte studien

önskat antal respondenter och studiens författare fick sprida enkäten via sina privata Facebooksidor. Detta innebär att andra steget utgjorde ett bekvämlighetsurval, vilket betyder att deltagare rekryteras utifrån tillgänglighet (Clark-Carter 2024, s.143). Bekvämlighetsurvalet möjliggjorde en effektiv spridning av enkäten, men kan samtidigt ha påverkat urvalet då det främst når personer inom författarnas egna nätverk. Detta innebär att vissa grupper inkluderas i högre utsträckning än andra. Trots dessa begränsningar ansågs ett bekvämlighetsurval lämpligt, eftersom studiens tidsramar och praktiska förutsättningar gjorde det svårt att genomföra ett slumpmässigt urval. Eftersom urvalet är icke-slumpmässigt och inkluderar två olika urvalstrategier med flera självsektioner går det inte att avgöra hur väl resultaten speglar situationen i samtliga kommuner i regionen. Resultatet kan därför vara skevt och representerar inte nödvändigtvis hela populationen (Clark-Carter 2024, s.144).

Totalt deltog 151 kommunanställda i studien. Av dessa var 78,8% kvinnor ($n=119$), 19,2% män ($n=29$), 0,7% icke-binär ($n=1$) och 1,3% ville inte uppge ($n=2$). Urvalets anställningsform var 80,1% tillsvidareanställda ($n=121$), 11,3% visstidsanställda ($n=17$), 7,3% timanställda ($n=11$) och 1,3% annan typ av anställning. Gällande högsta utbildning uppgav 51% högskola/universitet ($n=77$), 32,5% gymnasium ($n=49$), 12,6% eftergymnasial utbildning/yrkeshögskola ($n=19$), 2,6% grundskola ($n=4$), 0,7% annan utbildning ($n=1$) och 0,7% ville inte uppge ($n=1$). Den dagliga digitala arbetstiden var 31,1% 1-2h ($n=47$), 24,5% 7-8h ($n=37$), 19,2% 5-6h ($n=29$), 17,9% 3-4h ($n=27$) och 7,3% 9h eller mer ($n=11$). Av de 151 deltagande hade 134 fullständiga enkätsvar. På grund av internt bortfall (11,2%, $n=17$), där några deltagare saknade svar på vissa frågor varierade antalet inkluderade deltagare mellan analyserna.

4.6 Tillvägagångssätt

Datainsamlingen genomfördes med hjälp av en digital enkät via Qualtrics riktad till anställda inom kommunala verksamheter i tre kommuner i Västra Götaland. Enkäten distribuerades via kontaktpersoner i deltagande kommuner, antingen genom totalt mejlutskick eller via interna forum. Att gå igenom kontaktpersoner bedömdes vara lämpligt, då ingen av studiens författare hade en naturlig tillgång till urvalsgruppen för studien samt att respondenterna hade möjligheten att genomföra enkäten under arbetstid. Tillvägagångssättet möjliggjorde även att deltagarna kunde besvara enkäten individuellt,

när det passade dem och utan påverkan från studiens författare, då ingen av dem var närvarande vid genomförandet.

Inledningsvis kontaktades 30 kommuner via mejl med en förfrågan om deltagande. I samband med detta presenterades studiens syfte samt kontaktuppgifter till författarna. De tre kommuner som valde att delta erhöll ett informationsbrev med länk till enkäten samt information om datainsamlingsperioden. Genom informationsbrevet fick respondenterna ta del av information om studiens syfte, frivillighet, anonymitet, konfidentialitet och kontaktuppgifter innan de besvarade enkäten. Informationsbladet återfinns i Bilaga 5. Informationen upprepades när respondenterna startade enkäten och i första frågan i enkäten fick respondenterna aktivt ge sitt samtycke. I början och slutet av enkäten påmindes respondenterna att deltagandet var frivilligt och de erhöll en identifikationskod som de kunde mejla till studiens författare vid önskan om att avbryta och hade en svarsfrist på två veckor. Enkäten som helhet återfinns i Bilaga 4.

Enligt pilotstudien och Qualtrics analys tog enkäten cirka sju minuter att besvara och datainsamlingen pågick mellan 16 mars och 5 april. För att öka deltagandet skickades en påminnelse ut via kommunerna under datainsamlingsperioden. Bortfall förekom för att alla kommunanställda som nåddes av enkäten inte valde att delta och det initiala deltagandet var lägre än förväntat trots påminnelser. På grund av detta distribuerades enkäten även via studiens författare via deras privata Facebook den 30 mars som ett komplement till ursprungsinsamlingen. Vi är medvetna om att denna spridningsmetod kan medföra en risk för att personer utanför den avsedda urvalsgruppen besvarar enkäten. För att begränsa denna risk angavs det vid två tillfällen i informationsbladet att respondenterna skulle vara kommunanställda. Trots att det finns en möjlighet till partiska svar (Clark-Carter 2024, s.72) bedömdes detta lämpligt för att snabbt nå ut till urvalsgruppen. Informationsbrev till den kompletterande datainsamlingen återfinns i Bilaga 6. Inga tekniska problem rapporterades under datainsamlingen och ingen ersättning utgick till respondenterna. Eftersom distributionen av enkäten skedde via kommunerna uppstod variationer i hur den spreds, vilket kan ha påverkat svarsfrekvensen. Kontaktpersonerna inom kommunerna var grindvakter och därmed kunde påverka vilka som nåddes av enkäten (Clark-Carter 2024, s.91). Detta begränsade studieförfattarnas möjlighet att styra spridningen och kan ha påverkat urvalet.

4.6.1 Pilotstudie

Innan den slutgiltiga datainsamlingen genomfördes en pilotstudie med 15 personer som arbetar som kommunanställda. Deltagarna varierade i ålder, kön och bakgrund, och valdes för att spegla studiens målgrupp. Syftet var att testa enkätens utformning, identifiera eventuella oklarheter i frågor och instruktioner samt uppskatta tidsåtgången (Clark-Carter 2024, s.30, 77). Pilotstudien visade att enkätens frågor i stort sett var tydliga, men vissa formuleringar och instruktioner behövde förtydligas. Efter återkoppling från deltagarna i pilotstudien omarbetades den inledande texten för att öka tydligheten. Det fanns svårigheter att förstå syftet med vissa påståenden som indikerade att det fanns risk för feltolkningar. Texten som lades in lød *“Frågorna i enkäten berör områden som cybersäkerhet, tillit, organisatoriskt stöd och kontroll. Alla frågor handlar därför inte direkt om cybersäkerhet utan vissa frågor rör faktorer som kan ha en inverkan på hur medarbetare upplever arbetsgivarens cybersäkerhetsarbete”*. Även några mindre justeringar gjordes, såsom korrigerings av stavfel och språkliga missar. Genomförandetiden uppmättes till cirka sju minuter, vilket bekräftade att enkäten hölls inom en rimlig tidsplan (Clark-Carter 2024, s.30). Pilotstudien bidrog därmed till att säkerställa enkätens funktion, minska risken för bortfall och stärka studiens ansiktsvaliditet (Clark-Carter 2024, s.417).

4.7 Analyismetod

För att testa hypoteserna användes parametriska tester som bestod av regressionsanalyser. Parametriska tester förutsätter kontinuerliga variabler och vissa antaganden om datans fördelning (Clark-Carter s.172, 173). Normalfördelning bedömdes genom granskning av histogram, q-plots samt skewness- och kurtosisvärden. Bedömningen visade en godtagbar normalitet. Linjäritet bedömdes med scatterplots (spridningsdiagram) som visade linjära residualspridning mellan kontinuerliga variabler (Pallant 2016, s.130). Homoskedasticitet kontrollerades genom residualplottar, som visade en godtagbar spridning av residualerna. Multikollinearitet kontrollerades med VIF-värden, där värden under 10 anses indikera låg risk (Borg & Westerlund 2012, s.410). Data kontrollerades även för extremvärden (outliers). Då samtliga antaganden uppfylldes och variablerna var kontinuerliga bedömdes förutsättningar för regressionsanalys vara tillgodosedda (Nishisato 2004, s.3). Regressionsanalysen möjliggör analys av både samband och prediktion av den beroende

variabel utifrån oberoende variabeln (Clark-Carter 2024, s.294). Valet av analys motiveras av studiens fokus på prediktiva samband, vilket är mer lämpligt än korrelations- eller Chi-2-tester. Innan de huvudsakliga analyserna gjordes en explorativ faktoranalys av den egenutvecklade skalan för att säkerställa begreppsvaliditeten.

Inledningsvis genomfördes univariata analyser i form av deskriptiv analys, därefter bivariata analyser med Envägs-ANOVA och Pearson korrelationskoefficient för att undersöka skillnader mellan grupper och grundläggande samband mellan den beroende variabel och oberoende variablerna samt bakgrundsvariablerna. För hypoteserna användes enkla linjära regressioner, eftersom varje analys undersökte effekten av en enskild oberoende variabel, organisatorisk tillit (H1), upplevt organisatoriskt stöd (H2), och arbetsrelaterad kontrolluppfattning (H3) på den beroende variabeln "tillit till arbetsgivarens cybersäkerhetshantering". För att ytterligare analysera beroende variabeln användes en multipel regression, eftersom analysen inkluderar flera oberoende variabler, och är lämplig när flera variabler antas bidra till samma utfall och deras förklaringskraft delvis kan överlappa (Clark-Carter 2024, s.294, 299). Den multipla regressionen gjordes hierarkiskt, där varje variabel lades till stegvis och bildade separata modeller (Ho 2013, s.319). Det hierarkiska tillvägagångssättet valdes för att förklara hur variabelernas förklaringsgrad utvecklades stegvis och i sista modellen inkluderas även en kontrollvariabel. Samtliga analyser genomfördes i SPSS Version 29.

4.8 Kvalitetskriterier

Validitet och reliabilitet är grundläggande kvalitetskriterier som stärker studiens objektivitet. Reliabilitet innebär hur tillförlitliga de använda mätinstrumenten är i att få konsekventa resultat (Clark-Carter 2024, s.25). Reliabilitet kan delas upp i intern och extern. För att säkerställa den interna reliabiliteten använde studien etablerade och empiriskt prövade skalor. Dessa skalor har i tidigare studier rapporterat Cronbach's alfa-värden på över 0.7 (Eisenberger et al. 1986; Mayer & Davis 1999; Schoorman, Mayer & Davis 2016; Spector 1988) som indikerar en acceptabel intern konsistens i skalorna (Pallant 2016, s.104). Det är dock viktigt att beakta att dessa studier använde fullskaliga skalor. Skalan i Eisenberger et al. (1986) bestod av 36 påståenden, medan Spector (1988) använde 16 påståenden och Mayer och Davis (1999) skala hade 40 påståenden utav dessa 92 valdes endast 18 påstående ut till enkäten, därav genomfördes nya Cronbach's alfa-

test. För varje variabel beräknades index baserat på respektive skala för att testa att det mäter samma fenomen. Detta möjliggjorde en mer robust mätning av de underliggande begreppen (Zumbo & Rupp 2004, s.73). Samtliga index visade värden över 0.8 förutom indexet för arbetsrelaterad kontrolluppfattning som visade värdet ($\alpha = 0.7$). Detta något lägre värde accepteras dock ofta vid skalor på mindre än tio frågor (Pallant 2016, s.101). Den egenutformade skalan för "Tillit till arbetsgivarens cybersäkerhetshantering" reliabilitetstestades, eftersom den inte tidigare prövats empiriskt. Den externa reliabiliteten är däremot begränsad, eftersom studien bygger på en tvärsnittsdesign och datainsamling skedde vid ett tillfälle, vilket gör att resultatens stabilitet över tid inte kan bedömas (Clark-Carter 2024, s.25). Samtidigt stärker användningen av etablerade mätinstrument studiens reproducerbarhet och ger möjlighet att upprepa.

Validitet avser hur väl studien mäter det den ska mäta (Clark-Carter 2024, s.25). Validitet kan delas upp i två delar, intern och extern. Extern validitet rör möjligheten att generalisera resultatet, medan intern validitet handlar om att påvisa orsak-och-verkan (Clark-Carter 2024, s.35, 36). Den interna validiteten var svår att uppnå eftersom studien baseras på enkäter, vilket begränsade möjligheten att kontrollera de testade omständigheterna (Clark-Carter 2024, s.37). Studiens användning av tvärsnittsdesign och självrapporterad data kan därför inte ge kausala slutsatser, vilket begränsar den interna validiteten. De statistiska analyserna som valdes i studien möjliggör endast undersökning av samband mellan variablerna (Clark-Carter 2024, s.270). Den interna validiteten kan också begränsas av bakomliggande faktorer såsom exempelvis tidigare erfarenhet av cyberincidenter, ledningsstrukturer eller medierapportering (Clark-Carter 2024, s.37). Alla faktorer går inte att kontrollera, men i denna studie inkluderades bland annat bakgrundsvariablerna kön, utbildning, digital arbetstid, upplevd cyberhotrisk och rapporterad cybersäkerhetsutbildning från arbetsgivaren i analysen för att till viss del kontrollera alternativa faktorer. Extern validitet kan stärkas genom att enkäten möjliggjorde datainsamling från ett större antal respondenter, även om självselektion och bortfall kan påverka generaliserbarheten (Clark-Carter 2024, s.35).

Begreppsvaliditet säkerställs i hög grad genom att använda empiriskt prövade mätinstrument för att mäta begrepp (Zumbo & Rupp 2004, s.84) samt genom explorativ faktoranalys på den egenutvecklade skalan. Faktoranalysen kan bidra till studiens

replikerbarhet, då mätinstrumentet kan användas till framtida studier för att pröva resultatens stabilitet. Samtidigt påpekar Clark-Carter (2024, s.26) att begrepp bör förklaras utifrån sin specifika kontext, snarare än en generell begreppsförklaring. Därför är enkäten utformad med beprövade och organisationsanpassade mätinstrument förutom den egenutvecklade skalan som mäter en specifik form av tillit. Den egenutvecklade skalan har försökt att anpassas till sin kontext och beskrivs ytterligare i avsnitt 4.3 operationalisering. Clark-Carter (2024, s.26) beskriver att innehållsvaliditet handlar om att täcka relevanta aspekter av begreppet. Eftersom den egenutvecklade skalan baseras på författarnas egen övergripande bedömning av hur tillit till arbetsgivarens cybersäkerhetshantering kan mätas och kan därmed ha missat viktiga delar av begreppet finns en risk för en begränsning i innehållsvaliditeten. Ansiktsvaliditet innebär att säkerställa att både forskaren och respondenterna förstår vad mätinstrument avser att mäta (Clark-Carter 2024, s.18, 26). Studien ämnade att säkerställa ansiktsvaliditeten genom informationsbrev, dialog med extern aktör, instruktioner i enkäten samt pilotstudien.

4.9 Etiska utmaningar

God forskningsetik är avgörande i studier som involverar människor och de fyra etiska kraven och ska följas genom hela processen (Vetenskapsrådet 2017, s.2). Studien genomfördes i enlighet med såväl Vetenskapsrådets riktlinjer som de etiska principerna i Högskolan i Skövdes riktlinjer för examensarbeten (dnr HS 2025/572). Informationskravet innebär att deltagarna informeras om studiens syfte, transparens och anonymitet (Vetenskapsrådet 2002, s.7) samt att denna information måste vara tillräcklig och korrekt (Brown & Hedges 2008, s.391). Detta uppfylldes genom informationsbrev och med neutralt formulerade enkätfrågor (Se bilaga 4, 5 och 6).

Eftersom deltagarna var anställda och studien rörde tillit till arbetsgivarens cybersäkerhetshantering fanns en potentiell beroendeställning, vilket enligt Vetenskapsrådet (2002, s.10, 11) kräver särskild försiktighet. Med tanke på att enkäten bland annat distribuerades via kommunerna kunde det finnas en upplevd förväntan att delta och risk för socialt önskvärda svar (Steenkamp, De Jong & Baumgartner 2010). För att motverka detta tydliggjordes i informationsbrevet att deltagandet var frivilligt, anonymt och att arbetsgivaren inte hade tillgång till rådatan. För att stärka frivilligheten informerades deltagarna om att de när som helst kunde avbryta sitt deltagande. De

informerades även om att en identifikationskod fanns i slutet av enkäten, vilken kunde användas om de ville dra tillbaka sina redan inskickade svar. Att deltagarna fick denna information och bekräftade sitt samtycke innan datainsamlingen startade innebar att samtyckeskrauet uppfylldes, som kräver att deltagandet ska vara informerat, frivilligt och möjligt att återta (Vetenskapsrådet 2024, s.63).

Konfidentialitetskravet avser att deltagarnas uppgifter skyddas och att ingen kan identifieras (Vetenskapsrådet 2002, s.11, 12). I denna studie var detta särskilt viktigt eftersom frågorna rörde arbetssituationer och tillit till arbetsgivarens hantering av cybersäkerhet, vilket kan upplevas som känsligt. För att säkerställa konfidentialitet samlades inga personuppgifter in, kommunerna anonymiserades och resultaten redovisades utan möjlighet till identifiering samt att kommunerna inte fick ta del av enskilda resultat. Detta i syfte att minska risken för negativa konsekvenser för både deltagare och berörda verksamheter. Enkäten innehöll endast relevanta frågor och deltagarna informerades om att deras svar inte påverkade deras arbetssituation. Vid datainsamlingen beaktades även att digitala system automatiskt kan samla in metadata (Burbules 2008, s.553, 554). Detta framgick tydligt i informationsbrevet, där deltagarna informerades om vilken data som samlades in och hur den lagrades.

Nyttjandekravet innebär att insamlad data endast används för forskningsändamålet (Vetenskapsrådet 2002, s.14). I vår studie var detta särskilt viktigt eftersom enkäten distribuerades via kontaktpersoner i kommuner. För att deltagarnas svar inte skulle påverkas av externa intressen, ansvarade vi självständigt för design, analys och rapportering. Varken kommunerna eller obehöriga hade tillgång till rådata eller möjlighet att påverka tolkningen av resultaten. Endast data som var nödvändig för studiens syfte samlades in, och all insamlad data raderas när författarna uppnår ett godkänt resultat. Målet var att inte belasta deltagarna i onödan, därav är enkäten utformad i enlighet med studiens syfte, som kan minska risken för snedvridna resultat (Brown & Hedges 2008, s.391, 392). Genom att studien är tydlig, transparent och objektiv skapades förutsättningar för att deltagarna skulle kunna besvara enkäten utan upplevt tryck, vilket stärker både deltagarnas trygghet och studiens trovärdighet i enlighet med ALLEA-kodexen för god forskningssed (Vetenskapsrådet 2024, s.11).

5. Resultat

I detta avsnitt presenteras studiens deskriptiva statistik samt förberedande analyser för att pröva statistiska antaganden inför de huvudsakliga analyserna. Detta inkluderade faktoranalys för att undersöka den egenutvecklade skalans konstruktion, Envägs-ANOVA för att identifiera eventuella gruppkillnader samt korrelationsanalyser för att undersöka potentiell överlappning mellan variabler som kompletterades med VIF-värde för att bedöma multikollinearitet. Därefter redovisas resultaten för de tre hypoteserna som analyserades med enkla regressionsanalyser, följt av en kompletterande explorativ hierarkisk multipel regressionsanalys.

5.1 Deskriptiv statistik

Första delen i analysen avser deskriptiv data om studiens indexering av variablerna samt de två kontinuerliga bakgrundsvariablerna "upplevd risk för cyberhot" och "rapporterad cybersäkerhetsutbildning från arbetsgivaren". Deskriptiv statistik för studiens huvudvariabler som har indexerats, inklusive antalet (n), medelvärdet (M), standardavvikelsen (SD), Cronbach's alpha (α) och korrelation (Pearson r) redovisas i Tabell 5. Syftet med detta är att ge en översikt på variablernas fördelning och centrala tendensmått, spridningsmått samt sambandsmönster mellan studiens variabler. Samtliga indexerade variabler mättes på en femgradig skala, med undantag för arbetsrelaterad kontrolluppfattning som mättes på en sexgradig skala.

Tabell 5. Deskriptiv statistisk, reliabilitet och korrelation mellan studiens variabler ($N=134-151$)

Variabel	M	SD	α	1	2	3	4	5	6
1. Tillit till arbetsgivarens cybersäkerhetshantering	3.53	.81	0.86	-					
2. Organisatorisk tillit	3.01	.81	0.84	.543**	-				
3. Organisatoriskt stöd	3.10	.96	0.93	.537**	.772**	-			
4. Arbetsrelaterad kontrolluppfattning	3.85	.76	0.7	.413**	.365**	.476**	-		
5. Upplevd risk för cyberhot	3.49	1.11		.111	.115	.265**	.089	-	
6. Rapporterad cybersäkerhetsutbildning från arbetsgivaren	2.77	1.31		.525**	.391**	.313**	.355**	.137	-

Not. M = medelvärde, SD = standardavvikelse, α = Cronbach's alpha. Korrelationer (Pearson r) presenteras under diagonalen och är markerad i fetstil. Variablerna 5 och 6 utgör studiens bakgrundsvariabler. N varierar mellan 134 och 151 beroende på internt bortfall. * = $p < .05$, ** = $p < .01$ (2-tailed)

Resultaten visar att tillit till arbetsgivarens cybersäkerhetshantering hade ett medelvärde på 3,53 ($SD = 0.81$, $n = 141$), vilket indikerar att respondenterna i genomsnitt upplevde en relativt hög nivå av tillit till arbetsgivarens cybersäkerhetshantering. Organisatorisk tillit uppvisade ett medelvärde på 3.01 ($SD = 0.81$, $n = 143$), medan organisatoriskt stöd hade ett medelvärde på 3.1 ($SD = 0.96$, $n = 134$), vilket indikerar att respondenterna upplever en måttlig nivå av tillit respektive stöd från organisationen. Slutligen visade arbetsrelaterad kontrolluppfattning det högsta medelvärdet ($M = 3.85$, $SD = 0.76$, $n = 134$) som kan indikera att respondenterna upplevde en relativt hög grad av arbetsrelaterad kontroll. Standardavvikelse varierade mellan 0,76 och 0,96 för studiens huvudvariabler, vilket visar en normal spridning i respondenternas svar. Upplevt organisatoriskt stöd uppvisade den högsta spridningen ($SD = 0.96$), vilket indikerar större variation i respondenternas upplevelser. Arbetsrelaterad kontrolluppfattning visade den lägsta spridningen ($SD = 0.76$) som indikerar en mer samlad bedömning bland respondenterna.

Resultatet visar att respondenterna i genomsnitt uppfattade cyberhot som en relativt allvarlig risk för organisationen ($M = 3.49$, $SD = 1.11$, $n = 150$). När det gäller rapporterad cybersäkerhetsutbildning från arbetsgivaren visade resultatet från respondenterna att de inte hade fått tillräcklig utbildning inom området ($M = 2.77$, $SD = 1.31$, $n = 150$).

Pearsons korrelationsanalys visar att variablerna generellt samvarierar i samma riktning. Ett särskilt starkt samband framkommer mellan organisatorisk tillit och organisatoriskt stöd ($r = .77$, $p < .01$), vilket tyder på att dessa konstruktioner är nära relaterade men ändå distinkta. Bland bakgrundsvariablerna framkommer att upplevd allvarlighetsgrad av cyberhot inte har något signifikant samband med tillit till arbetsgivarens cybersäkerhetshantering ($r = .11$, $p = 0.191$). Däremot finns ett statistiskt signifikant samband mellan rapporterad cybersäkerhetsutbildning från arbetsgivaren och tillit till arbetsgivarens cybersäkerhetshantering ($r = .53$, $p < .01$), vilket indikerar att högre rapporterad utbildning är associerad med högre tillit till arbetsgivarens cybersäkerhetshantering. Baserat på detta inkluderas kontrollvariabeln rapporterad cybersäkerhetsutbildning i den efterföljande hierarkiska regressionsanalysen.

5.1.1 Faktoranalys

För att undersöka att den egenutvecklade skalan "tillit till arbetsgivarens cybersäkerhetshantering" mäter det den avser att mäta genomfördes en explorativ faktoranalys (Principal Component Analysis). I Tabell 6 redovisas resultaten från analysen. Analysen visade KMO index på 0.83 och Bartlett's test var signifikant ($p < .001$), vilket visade att data var lämplig för vidare analys, då KMO värden över 0.8 anses vara goda (Clark-Carter 2024, s.363). Analysen visade att en faktor hade egenvärde > 1 och förklarade 64% av variansen. Samtliga variabler uppvisade mycket goda faktorladdningar från 0.738 till 0.847, vilket tyder på att de mäter samma bakomliggande konstruktion.

Tabell 6. *Explorativ faktoranalys (PCA) av skalan tillit till arbetsgivarens cybersäkerhetshantering.*

	Faktor 1
Jag har förtroende för att organisationen arbetar aktivt för att förebygga cyberincidenter	0.847
Jag har förtroende för att organisationen kan upptäcka cyberincidenter i tid	0.817
Jag litar på att organisationen ger mig snabb och korrekt information om en cyberincident inträffar	0.838
Jag litar på att organisationen skyddar min personliga information vid en cyberincident	0.738
Jag har förtroende för att ledningen tar cybersäkerhet på allvar	0.760

Not. Tabellen visar faktorladdningar för samtliga items i beroende variabeln. Endast en faktor extraherades (egenvärde > 1), vilket förklarade 64% av den totala variansen. Samtliga faktorladdningar överstiger .70, vilket indikerar god intern konsistens, KMO = 0.83, Bartlett's test var signifikant ($p < .001$)

5.1.2 Envägs-ANOVA

En serie envägs-ANOVA-analyser genomfördes för att undersöka om tillit till arbetsgivarens cybersäkerhetshantering skiljde sig mellan olika grupper. Levene's test visade att variansantagandet om homogenitet var uppfyllt i samtliga analyser.

Resultaten påvisade inga statistiskt signifikanta skillnader i tillit till arbetsgivarens cybersäkerhetshantering mellan kön ($F(2, 138) = 0.337, p = 0.715$), utbildningsnivå ($F(4.136) = 2.036, p = 0.093$), anställning ($F(3, 137) = 0.841, p = 0.473$) eller antal digitala arbetstimmar per dag ($F(4.136) = 0.898, p = 0.467$). Sammantaget tyder resultaten på att tillit till arbetsgivarens cybersäkerhetshantering inte skiljer sig signifikant mellan de undersökta grupperna.

5.2 Hypotes 1

En enkel regressionsanalys genomfördes för att undersöka sambandet mellan organisatorisk tillit och tillit till arbetsgivarens cybersäkerhetshantering. Resultatet redovisas i Tabell 7 och visade att organisatorisk tillit har en positiv och signifikant påverkan på tilliten till arbetsgivarens cybersäkerhetshantering ($\beta=0.540$, $t = 7.631$, $p<.001$). Modellen förklarade 29 % av variansen i beroende variabeln (Adjusted $R^2=.290$), vilket innebär att Hypotes 1 stöds.

Tabell 7: Enkel regression. Beroende variabel: tillit till arbetsgivarens cybersäkerhetshantering. Standardiserad beta-koefficient, t-värde och Adjusted R^2

	β	t	Adjusted R^2
Organisatorisk tillit	0.540***	7.631	0.290

*** = $p < .001$ ** = $p < .01$ * = $p < .05$

Resultatet indikerar att högre organisatorisk tillit är associerad med högre tillit till arbetsgivarens cybersäkerhetshantering. Detta kan stödjas av teoretiska utgångspunkten om att generell organisatorisk tillit baseras på uppfattningar om organisationens förmåga, välvilja och integritet (Mayer, Davis & Schoorman 1995). Utifrån detta kan resultatet förstås som att medarbetare i högre grad utgår ifrån sin generella tillit till organisationen när de bedömer cybersäkerhet som är ett område där de själva har begränsad insyn och kunskap.

5.3 Hypotes 2

En enkel regressionsanalys genomfördes för att undersöka sambandet mellan upplevt organisatoriskt stöd och tillit till arbetsgivarens cybersäkerhetshantering. Resultatet redovisas i Tabell 8 och visade att upplevt organisatoriskt stöd har en positiv och signifikant påverkan på tilliten till arbetsgivarens cybersäkerhetshantering ($\beta=0.537$, $t=7.402$, $p < .001$). Modellen förklarade 28,3 % av variansen i tillit (Adjusted $R^2 = .283$), vilket betyder att Hypotes 2 bekräftas.

Tabell 8. Enkel regression. Beroende variabel: tillit till arbetsgivarens cybersäkerhetshantering. Standardiserad beta-koefficient, t-värde och Adjusted R^2

	β	t	Adjusted R^2
Organisatoriskt stöd	0.454***	7.402	0.283

*** = $p < .001$ ** = $p < .01$ * = $p < .05$

Resultatet indikerar att högre upplevt organisatoriskt stöd är associerat med högre tillit till arbetsgivarens cybersäkerhetshantering. Resultatet är i enlighet med teorin om upplevt organisatoriskt stöd (Eisenberger et al. 1986). Där medarbetarna tolkar organisationens agerande som signaler om hur väl organisationen värdesätter dem och bryr sig om deras välbefinnande, alltså att om medarbetarna upplever ett genuint stöd ökar tilliten.

5.4 Hypotes 3

En enkel regressionsanalys genomfördes för att undersöka sambandet mellan arbetsrelaterad kontrolluppfattning och tillit till arbetsgivarens cybersäkerhetshantering. Resultatet redovisades i Tabell 9 och visade att arbetsrelaterad kontrolluppfattning har en positiv och signifikant påverkan på tilliten till arbetsgivarens cybersäkerhetshantering ($\beta=0.413$, $t=5.204$, $p <.001$). Modellen förklarade 16,4 % av variationen i tillit (Adjusted $R^2 = .164$), detta innebär att Hypotes 3 bekräftas.

Tabell 9. Enkel regression. Beroende variabel: tillit till arbetsgivarens cybersäkerhetshantering.

	β	t	Adjusted R^2
Arbetsrelaterad kontrolluppfattning	0.413***	5.204	0.164

*** = $p <.001$ ** = $p <.01$ * = $p <.05$

Resultatet indikerar att högre arbetsrelaterad kontrolluppfattning är associerad med högre tillit till arbetsgivarens cybersäkerhetshantering. Detta överensstämmer med Spectors (1982) teori som betonar att individers upplevelse av kontroll påverkar hur situationer tolkas. I en cybersäkerhetskontext där kunskapen ofta är begränsad, kan därför en hög kontrolluppfattning bidra till att situationen upplevs som mer hanterbar, vilket i sin tur kan öka tilliten till organisationen.

5.5 Explorativ analys av tillit till arbetsgivarens cybersäkerhetshantering

För att ytterligare undersöka tillit till arbetsgivarens cybersäkerhetshantering genomfördes en hierarkisk multipel regressionsanalys i syfte att få mer en djupgående och heltäckande analys av de tre signifikanta resultaten från H1-H3 samt kontrollvariabeln rapporterad cybersäkerhetsutbildning från arbetsgivaren. Resultaten från den hierarkiska multipla regressionsanalysen redovisas i tre modeller i Tabell 10 och

visar hur förklaringsvärde och variabelernas effekter förändras när ytterligare variabler inkluderas. Samtliga tre modeller är statistiskt signifikant ($p < .001$).

Tabell 10. Hierarkisk regressionsanalys. Beroende variabel: tillit till cybersäkerhetshantering. Standardiserade beta-koefficienter, VIF-värden i fetmarkerad text.

	Modell 1	Modell 2	Modell 3
	Organisatorisk tillit och organisatoriskt stöd	Organisatorisk tillit, organisatoriskt stöd och arbetsrelaterad kontroll	Organisatorisk tillit, organisatoriskt stöd, arbetsrelaterad kontroll och upplevd säkerhetsutbildning från arbetsgivaren
Organisatorisk tillit	β 0.318 ** 2.4	β 0.318** 2.4	β 0.196 2.6
Organisatoriskt stöd	β 0.289* 2.4	β 0.192 2.7	β 0.184* 2.7
Arbetsrelaterad kontrolluppfattning		β 0.205* 1.3	β 0.116 1.4
Rapporterad cybersäkerhetsutbildning från arbetsgivaren			β 0.342*** 1.3
n	134	134	134
Adjusted R²	31,6 %	34,4 %	43,4 %

Not: *** = $p < .001$ ** = $p < .01$ * = $p < .05$. Rapporterad cybersäkerhetsutbildning från arbetsgivaren är en kontrollvariabel.

I modell 1 är både organisatorisk tillit ($\beta=0.318$, $p<.05$) och organisatoriskt stöd ($\beta=0.289$, $p<.05$) positiva och signifikanta prediktorer av tillit till arbetsgivarens cybersäkerhetshantering. Modellen förklarar 31,6% av variansen (Adjusted $R^2= 0.316$). Detta resultat stämmer överens med Mayer, Davis & Schoorman (1995) där tillit baseras på individens uppfattningar om organisationens förmåga och pålitlighet. Organisatoriskt stöd kan i detta sammanhang förstås som en indikator på hur väl organisationen uppfattas värdesätta sina medarbetare (Eisenberger et al. 1986), vilket i sin tur kan ha en inverkan på hur tilliten skapas.

I modell 2 inkluderas arbetsrelaterad kontrolluppfattning, vilket ökar variansen till 34,4% (Adjusted $R^2= 0,344$). I denna modell kvarstår organisatorisk tillit som signifikant, medan organisatoriskt stöd inte längre är signifikant. Arbetsrelaterad kontrolluppfattning uppvisar samtidigt ett positivt och signifikant samband med tillit till arbetsgivarens cybersäkerhetshantering. Detta tyder på att effekten av organisatoriskt stöd minskar när kontrolluppfattning inkluderas i modellen, vilket kan tyda på att delar av sambandet mellan stöd och tillit till arbetsgivarens cybersäkerhetshantering förklaras av individens

upplevda kontroll. Detta kan kopplas till teorin om arbetsrelaterad kontrolluppfattning där upplevd kontroll påverkar individens tolkning och hantering vid osäkra situationer och hot (Spector 1982). Resultatet indikerar att högre kontrolluppfattning kan bidra till ökad tillit för arbetsgivaren genom att medarbetaren aktivt letar information, exempelvis vid cyberangrepp.

I modell 3 inkluderas kontrollvariabeln rapporterad cybersäkerhetsutbildning från arbetsgivaren, vilket ytterligare ökar förklaringsgraden till 43,4% (Adjusted $R^2 = 0.434$). I modell 3 framstår rapporterad cybersäkerhetsutbildning som en signifikant prediktor, medan övriga variabler får reducerad eller icke-signifikant effekt. Resultaten från modell 3 visar att utbildning har en stark positiv effekt, som kan tyda på att specifik ökad kunskap kan fungera som en förklarande faktor för både upplevd kontroll och tillit. Sammantaget indikerar resultaten i modellerna att organisatorisk tillit och kontrollvariabeln cybersäkerhetsutbildning har effekt på tillit till arbetsgivarens cybersäkerhetshantering, medan effekten av organisatoriskt stöd och arbetsrelaterad kontrolluppfattning varierar beroende på vilken ordning variablerna läggs in.

6. Diskussion

I detta avsnitt presenteras diskussioner om studiens olika delar som inkluderar resultat, metod, kvalitetskriterierna, etik, utmaningar och begränsningar, bidrag till forskningsområdet, framtida studier, rekommendationer till praktiker och slutsats.

6.1 Resultatdiskussion

Syftet med studien var att undersöka om det finns ett samband mellan organisatorisk tillit, organisatoriskt stöd, arbetsrelaterad kontrolluppfattning och kommunanställdas tillit till arbetsgivarens cybersäkerhetshantering. Resultatet visar att samtliga tre faktorer har en inverkan på tillit samt att cybersäkerhetsutbildning framträder som en viktig faktor. Nedan diskuteras hypoteserna i relation till studiens tidigare forskning.

Den första hypotesen avsåg sambandet mellan organisatorisk tillit och tillit till arbetsgivarens cybersäkerhetshantering. Resultatet bekräftade ett tydligt positivt samband som stöds av tidigare forskning i området. Enligt Svenson, Ballóva Mikušková och Launer (2023) skapas tillit till säkerhetsrelaterade frågor genom subjektiva bedömningar, där upplevda risker och fördelar vägs mot varandra. I detta

fall fungerar organisatorisk tillit som en bedömning om hur cybersäkerhetsåtgärder uppfattas. Detta stöds av Searle, Renaud och van der Werff (2024) som menar att tillit vid osäkra situationer som cyberhot främst bygger på hur organisationens agerande uppfattas, inte på deras tekniska kunskap. Det betonas även av Wang et al. (2024) att cybersäkerhet inte endast är en teknisk fråga, utan också är en social process. Resultatet kan förstås som att organisatorisk tillit fungerar som en indikator på hur organisationens agerande tolkas, vilket i sin tur påverkar det mer specifika tillitsområdet cybersäkerhetshantering.

Den andra hypotesen visade att organisatoriskt stöd hade ett positivt samband med tillit till arbetsgivarens cybersäkerhetshantering. Resultatet överensstämmer med tidigare forskning som belyser vikten av tydlig information, resurser och stödjande strukturer (Dang-Pham et al. 2019; Müller et al. 2025; Safie et al. 2025). På samma gång visar studiens resultat att effekten försvagas när andra variabler inkluderades, vilket antyder att organisatoriskt stöd inte utgör en helt oberoende faktor. Att effekterna försvagas kan stämma överens med Dang-Pham et al. (2019) studie som fann att organisatoriskt stöd inte räcker i sig utan kan behöva kompletteras med andra faktorer, såsom nyckelpersoner i verksamheten. Effekterna kan också förklaras med hjälp av Hawthornes (2025) forskning som visade att tillgång till tydlig information inte direkt skapar tillit utan fungerar som en grund för att bygga den. Detta kan tyda på att organisatoriskt stöd kan förstås som en bidragandefaktor som kan lägga en grund för att skapa tillit, i stället för att vara en direkt förklarande faktor.

Den tredje hypotesen avsåg sambandet mellan arbetsrelaterad kontrolluppfattning och tillit till arbetsgivarens cybersäkerhetshantering. Resultatet visade att hög arbetsrelaterad kontrolluppfattning är kopplad till hög tillit till arbetsgivarens cybersäkerhetshantering, vilket bekräftas av tidigare forskning. Avrahami och Zwilling (2025) menar att upplevd kontroll utvecklas genom samspelet mellan organisatoriska resurser och individens förmåga att tolka information, medan Svenson, Ballóva Mikušková och Launer (2023) framhåller att subjektiva tolkningar spelar en avgörande roll i tillitsbedömningar. Samtidigt visar Butavicius et al. (2020) att hög tilltro till tekniska system kan skapa en falsk känsla av kontroll och medarbetarnas egen varsamhet minskar. Trots detta kan resultatet förstås som att en hög arbetsrelaterad

kontrolluppfattning minskar osäkerheten runt komplexa situationer och stärker tilliten till organisationen. Men att tilliten kan bygga på en förenklad bild av organisationens kompetens. Slutsatsen är att tillit till cybersäkerhet skapas av både organisatoriska åtgärder och hur individen upplever sin och organisationens handlingsförmåga.

Den kompletterande explorativa hierarkiska regressionsanalysen undersökte hur stor del av variansen i beroende variabeln som förklaras av de tre oberoende variablerna samt den signifikanta kontrollvariabeln rapporterad cybersäkerhetsutbildning från arbetsgivaren. Resultatet visade att de hade ett relativt högt förklaringsvärde (Cohen 1988, s.414). Detta sammanfaller med studiens egen positionering till forskningsfältet om att tillit konstrueras genom samspelet mellan organisatoriska och individuella faktorer. Ett särskilt intressant resultat är att rapporterad cybersäkerhetsutbildning framträder som en stark prediktor när den inkluderades i modellen. Vilket bekräftas av Safie et al. (2025) och Stacey et al. (2021) som beskriver att utbildning minskar osäkerhet och kan stärka tilliten. Även Avrahami och Zwilling (2025) belyser att kombinationen av organisatoriska insatser och kunskap stärker både kontroll och tillit. Resultatet visar att cybersäkerhetsutbildning, trots att den användes som kontrollvariabel är en signifikant faktor för tilliten till arbetsgivarens cybersäkerhetshantering. Detta tyder på att specifik utbildning kan öka tillit till specifika tillitsområden.

Trots att cybersäkerhetsutbildning är en väsentlig förklaringsfaktor var modellen i sin helhet fortfarande signifikant. Det signifikanta resultatet antyder att de andra variablerna är med och bidrar till att förklara variansen i denna tillit. Resultatet understryker vikten av samspelet mellan organisationens åtgärder och hur medarbetare tolkar dessa, där tillit till arbetsgivarens cybersäkerhetshantering snarare kan förstås som ett resultat av detta samspel än som en effekt av en enskild faktor.

6.2 Metoddiskussion

Alla studier påverkas av de metodologiska och designmässiga val som görs under forskningsprocessen, och denna studie utgör inget undantag. Att mäta subjektiva upplevelser med kvantitativa metoder är utmanande, särskilt i en tvärsnittsdesign, där all data samlas in vid ett tillfälle och består av självrapporterad data. Detta betyder att den aktuella studien inte kan dra kausala slutsatser och resultaten visar endast

statistiska samband mellan variablerna. Vi har försökt vidta åtgärder för att underlätta en sådan mätning genom att använda etablerade skalor, kontrollera skalornas reliabilitet, undersöka initiala samband mellan variablerna samt genomföra en faktoranalys av vår egen skala. Samtidigt hade en poweranalys kunnat användas för att uppskatta ett mer exakt deltagarantal för våra analyser och därigenom säkerställa tillräcklig statistisk power. Detta hade lett till att vi ökat sannolikheten ytterligare för att upptäcka verkliga effekter och då minskat risken för typ II-fel (Pallant 2016, s.209). Eftersom studien använde sig av flera oberoende variabler var det viktigt att kontrollera att de inte överlappade varandra. I den multipla regressionen var alla VIF-värden godtagbara, vilket indikerar att modellen inte uppvisade statistiskt problematisk multikollinearitet. Den förberedande korrelationsanalysen visade dock att organisatorisk tillit och upplevt organisatoriskt stöd hade ett starkt samband ($r=.77$), vilket gör att deras unika effekter kan vara svåra att särskilja.

6.2.1 Kvalitetskriteriediskussion

Att använda etablerade skalor är ofta en styrka, men reliabilitet och validitet kan variera beroende på urval och kontext. I vår studie har begrepps- och innehållsvaliditeten påverkats av att de etablerade skalorna är äldre och delvis svårtolkade. Men för att stärka innehållsvaliditeten inleddes varje enkätavsnitt med en begreppsdefinition, samtidigt som skalorna behölls nära originalen för att bevara begreppsvaliditeten. Vidare visade reliabilitetstesterna godtagbara värden vilket tyder på att skalorna fungerade på ett tillförlitligt sätt. Skalan för upplevt organisatoriskt stöd hade ett Cronbach's alfa över 9 ($\alpha=.93$) vilket i efterhand kunde ses som att någon fråga eventuellt var överflödig. Motsatt hade skalan för arbetsrelaterad kontrolluppfattning relativt låga men godtagbara värden ($\alpha=.7$), vilket indikerar att vi möjligen tog bort någon fråga för mycket. Om en utförligare pilotstudie hade utförts hade reliabiliteten kunnat testas och i det skedet eventuellt justera antalet. När det gäller vår egenutvecklade skala fanns en viss osäkerhet för om vår bedömning om variabelns frågor var tillräcklig, därför genomfördes både reliabilitetstest och faktoranalys som visade goda resultat avseende reliabilitet och begreppsvaliditet. Detta var positivt samtidigt som skalan rekommenderas fortsätta utvärderas om den ska användas i framtida studier. Det gjordes förändringar i skalan för arbetsrelaterad

kontrolluppfattning. Skalan justerades genom att vissa påståenden omvändes poängmässigt så att alla items mätte kontrolluppfattning i samma riktning. I ursprungsskalan görs en liknande justering, men i denna studie valde vi att vända skalan i motsatt riktning för att tydligare fokusera på hög kontrolluppfattning. Denna anpassning bedömdes som metodologiskt likvärdig, då poängvändning inte förändrar innehållet i variabeln utan endast riktningen på skalan samt att det genomfördes ett Cronbach's alfa-test som visade acceptabel intern konsistens.

I syfte att fånga alternativa förklaringar inkluderade studien flera potentiella kontrollvariabler. De flesta visade sig vara icke-signifikanta, med undantag för rapporterad cybersäkerhetsutbildning som därför inkluderades i slutet av den hierarkiska multipla modellen. När denna lades till ökade modellens förklaringsgrad tydligt, samtidigt som flera oberoende variabler minskade. Detta tyder på att cybersäkerhetsutbildning fångar en del av den varians som tidigare förklarades av exempelvis arbetsrelaterad kontrolluppfattning och organisatorisk tillit. Detta kan tolkas som att utbildning utgör en närliggande förklaringsfaktor till tillit till arbetsgivarens cybersäkerhetshantering, i stället för bara en kontrollvariabel. Samtidigt bör resultaten tolkas med försiktighet eftersom variabeln mättes med endast en fråga, till viss del överlappar begreppsligt med organisatoriskt stöd och dessutom placerades sist i den hierarkiska modellen, vilket kan ha förstärkt dess effekt.

6.2.2 Etikdiskussion

För studiens författare var det en fördel att få möjlighet att skicka ut enkäten via kontaktpersoner inom några kommuner. Detta eftersom anställda förmodligen är mer benägna att svara på kommunikation som kommer från arbetsgivaren än från studenter. Samtidigt innebar detta upplägg att en del av kontrollen över datainsamlingen försvann. När enkäten skickades ut via arbetsgivaren fanns en risk att anställda upplevde tvång att svara. Det kan dessutom uppstå en oro för att arbetsgivaren på något sätt skulle kunna ta del av svaren vilket i sin tur kan leda till att respondenterna anpassar sina svar i en mer socialt önskvärd riktning.

All säkerställande information om anonymitet, frivillighet och databehandling skickades med i ett informationsbrev som vi förutsätter har nått respondenterna. En kort information fanns också i början av enkäten och respondenterna behövde

dessutom aktivt ge samtycke. De tilldelades även en identifikationskod som möjliggjorde återkallande av deras svar, men ingen respondent valde att göra detta. Utöver etiska överväganden gentemot respondenterna var det också viktigt att tydliggöra för de deltagande kommunerna att ingen data kunde kopplas till en specifik arbetsplats eller kommun. Studien syftade inte till att jämföra kommuner eller presentera resultat på organisationsnivå. Därför namnges inga kommuner varken i resultatet eller i studien som helhet.

6.2.3 Utmaningar och begränsningar

Studien utgick från tre skilda teorier i syftet att fånga både individuella och organisatoriska faktorer. En utmaning var att studien inkluderade två närliggande former av tillit, den generella organisatoriska tilliten och den specifika tilliten till arbetsgivarens cybersäkerhetshanteringen. Detta innebär en risk för begreppslig överlappning, vilket kan kopplas till svårigheter att helt skilja närliggande konstruktioner (Clark-Carter 2024, s.26). Trots att reliabilitet och korrelationer visar att måtten i huvudsak mäter olika saker, kan överlappning inte uteslutas. Detta kan påverka tolkningen av resultaten, eftersom det kan vara svårt att avgöra varje variabls unika bidrag i regressionsanalyserna. Faktoranalys av samtliga variabler hade kunnat förbättra resultatets tillförlitlighet. En tydligare avgränsning till färre teorier hade kunnat stärka den röda tråden i studien, men samtidigt behöver man vara medveten om att komplexa fenomen ofta kräver att flera faktorer beaktas (Clark-Carter 2024, s.10).

Datinsamlingen präglades av utmaningar att nå respondenter. Trots att många kommuner kontaktades deltog endast tre, vilket resulterade i ett mindre urval än planerat. I vissa fall uttryckte kommunerna ett intresse, men endast under förutsättning att de fick ta del av sina egna resultat som inte var möjligt inom ramen för studiens upplägg. Dessutom missförstod vissa kommuner studiens syfte och uppfattade den som enbart inriktad på cybersäkerhet. Detta bidrog till svårigheter att nå respondenter och på grund av detta spreds enkäten via författarnas privata Facebooksidor. Trots en ökad risk för snedvridet urval där personer inom författarnas egna nätverk är överrepresenterade valdes detta på grund av tidsramen för studien. Studien baserades alltså på två icke-sannolikhetsurval i form av målinriktat urval och bekvämlighetsurval samt självselektion. Det vill säga att respondenterna inte valdes ut slumpmässigt, vilket

kan medföra urvalsbias och begränsad representativitet (Clark-Carter 2024, s.144). Det förekom även ett internt bortfall på 11,7 %. Detta innebär att vissa variabler baseras på ett reducerat antal observationer, vilket kan påverka resultaten. Endast fullständiga svar inkluderades i respektive analys. Könsfördelningen i urvalet är ojämn, där kvinnor utgör 78,8 % av respondenterna. Detta kan påverka resultatet, eftersom upplevelser och erfarenheter kan skilja sig mellan grupper. Samtidigt motsvarar fördelningen i stor utsträckning den faktiska könshöjningen inom kommunal sektor, där 76,1% av de anställda är kvinnor (Sveriges kommuner och regioner 2025). Studiens externa validitet stärks i viss mån genom att urvalet speglar den faktiska könshöjningen inom kommunal sektor, men den mindre överrepresentationen av kvinnor kan ha påverkat generaliserbarheten. Däremot eftersom urvalet består av icke-sannolikhetsurval i två former är den externa validiteten fortfarande begränsad.

6.3 Studiens bidrag till forskningsområdet

Den aktuella studien bidrar med en djupare förståelse för socialpsykologisk kunskap. Det som framkommer i studien är att tillit till arbetsgivarens cybersäkerhetshantering inte skapas i ett vakuum utan att de skapas i det sociala samspelet mellan individer och organisationer. Där tillit inte uppstår av sig själv och som en ensam reaktion på tekniska åtgärder, utan de skapas genom hur medarbetaren tolkar, förstår och upplever organisationens agerande i arbetslivet. I detta samspel blir organisationens signaler, såsom kommunikation om stöd, viktiga eftersom de har en inverkan på hur medarbetare uppfattar organisationens intentioner och kompetens inom cybersäkerhet. Samtidigt spelar individens egna upplevelser av kontroll en roll i hur dessa signaler tolkas. Tillit kan alltså förstås som något som kontinuerligt formas och förhandlas i relationen mellan organisationens handlingar och medarbetarnas tolkningar, snarare än som en statisk uppfattning speciellt i en föränderlig digital miljö.

Kunskapsluckan som identifieras är att visa hur organisatorisk tillit, upplevt organisatoriskt stöd och arbetsrelaterad kontrolluppfattning skapar tillit till arbetsgivarens cybersäkerhetshantering. I den tidigare forskningen som studien använder sig av behandlades faktorer var för sig eller hade ett större fokus på medarbetarnas misstag. Det är därför denna studie synliggör hur tillit till cybersäkerhetshantering utvecklas i samspelet mellan organisationens agerande och

medarbetarnas tolkningar. Samtidigt är detta inte helt nytt, utan studiens främsta bidrag ligger därför i att belysa dessa samband i en svensk kommunal kontext. Vår studie kan bidra med ett teoretiskt underlag för kommuner, där forskning om cybersäkerhet och tillit fortfarande är begränsad. Den praktiska nyttan med studien är därmed att den kan ge arbetsgivare en ökad förståelse för vilka faktorer som kan stärka medarbetarnas tillit till cybersäkerhetshandlingen.

6.4 Framtida studier

Variablerna kan behöva mätas mer noggrant i framtiden. De oberoende variablerna har mätts med få frågor, vilket kan göra resultaten mindre exakta. Med fler frågor och mer utvecklade skalor skulle man kunna få en tydligare och mer tillförlitlig bild av sambanden. Det kan också diskuteras om dessa variabler är de mest lämpliga för att förklara tillit till arbetsgivarens cybersäkerhetshandling, eftersom andra faktorer också kan vara viktiga.

Cybersäkerhetsutbildning borde i framtida studier behandlas som en oberoende variabel. För att möjliggöra mätningen av cybersäkerhetsutbildning bör det utformas en egen skala med flera items i stället för en enskild fråga, vilket hade öppnat upp för en omfattande mätning som hade kunnat fånga olika aspekter därigenom ökat mätningens tillförlitlighet. Ännu intressantare hade det varit med experimentell longitudinell design där cybersäkerhetsutbildning hade varit en central variabel. En sådan design hade kunnat mäta tilliten till cybersäkerhet innan och efter en cybersäkerhetsutbildningsinsats samt jämföra en interventiongrupp mot en kontrollgrupp, vilket hade kunnat ge mer kausala samband. Eftersom studiens urval var begränsat och gjorde det svårt att generalisera till populationen behöver framtida studier öka och variera urvalet genom att inkludera fler kommuner. Det hade varit intressant att få tillgång till kommunanställda i varje kommun i Sverige för att göra urvalet mer representativt, det hade även minskat risken för snedvridet urval.

6.4.1 Rekommendationer för praktiker

Organisationer bör satsa på cybersäkerhetsutbildning för anställda, eftersom resultaten visar ett tydligt samband mellan denna utbildning och tillit till hur cybersäkerhet hanteras. Utbildningen behöver vara anpassad till den specifika verksamhetens kontext

och kommunerna bör ge tydlig information om hur de hanterar cybersäkerhet. Detta kan göra att medarbetarna känner sig tryggare och gör cybersäkerhet till en integrerad del av arbetslivet, vilket stärker deras upplevda kontroll.

6.5 Slutsats

Studien undersökte tillit till arbetsgivarens cybersäkerhetshantering och om det finns ett samband mellan denna tillit och organisatoriska faktorer och individens egen kontroll. Organisatorisk tillit, upplevd organisatoriskt stöd och arbetsrelaterad kontrolluppfattning var alla statistiskt signifikanta för denna tillit, men deras effekter förändras när de analyseras tillsammans. Resultatet visar även att cybersäkerhetsutbildning har ett signifikant samband och kan stärka tilliten till arbetsgivarens cybersäkerhetshantering. Detta bör dock vidare undersökas då det endast var en kontrollvariabel med en enskild fråga. Sammanfattningsvis visar studien att tillit till cybersäkerhetshantering inte bara konstrueras genom organisatoriska åtgärder, utan också genom hur medarbetare tolkar och upplever organisationens agerande i det digitala arbetslivet.

Referenslista

- Avrahami, Z. & Zwilling, M. (2025). The Impact of Cyber Threat Intelligence (CTI) on Employee Behavior and Skills and the Implications for Organizational Cyber Resilience. *International Journal of Information Security*, 24, Artikel 184. doi:10.1007/s10207-025-01096-y
- Bergh, A. (2022). *Social tillit - varför är den viktig och hur främjas den*. Institutet för Näringslivsforskning. <https://www.ifn.se/media/do1pyc4f/2022-bergh-social-tillit-varfor-ar-den-viktig-och-hur-framjas-den.pdf> [2025-11-05]
- Brown, B.L. & Hedges, D. (2008). Use and Misuse of Quantitative Methods: Data Collection, Calculation, and Presentation. I Mertens, D. & Ginsberg, P. (red.) *The Handbook of Social Research Ethics*. SAGE Publications, Inc, s. 389–402. Tillgänglig på: <https://www.perlego.com/book/4791888> [2025.12.11].
- Borg, E. & Westerlund, J. (2012). *Statistik för beteendevetare: faktabok*. 3 uppl. Liber.
- Boritz, J. E., Ge, C., & Patterson, K. (2022). Factors Affecting Employees' Susceptibility to Cyber-Attacks. *Journal of Information Systems*, 36(3), s. 27–60. doi:10.2308/ISYS-19-053
- Borkovich, D. J., Skovira, R. J., & Kohun, F. (2023). Foundation of Cybersecurity Infoscapes: It's All About the Culture. *Issues in Information Systems*, 24(3), s. 1–14. doi:10.48009/3_iis_2023_101
- Burbules, N.C. (2008). Privacy and New Technologies: The Limits of Traditional Research Ethics. I Mertens, D. & Ginsberg, P. (red.) *The Handbook of Social Research Ethics*. SAGE Publications, Inc., s. 553–565. Tillgänglig på: <https://www.perlego.com/book/4791888> [2025.12.11].
- Butavicius, M., Parsons, K., Lillie, M., McCormac, A., Pattinson, M., & Calic, D. (2020). When Believing in Technology Leads to Poor Cyber Security: Development of a Trust in Technical Controls Scale. *Computers & Security*, 98, Artikel 102020. doi:10.1016/j.cose.2020.102020
- Clark-Carter, D. (2024). *Quantitative Psychological Research*. 5 uppl., Routledge. doi:10.4324/9781003208419
- Cohen, J. (1988). *Statistical Power Analysis for the Behavioral Sciences*. 2 uppl., Lawrence Erlbaum associates.

- Dang-Pham, D., Kautz, K., Pittayachawan, S. & Bruno, V. (2019). Explaining the Development of Information Security Climate and an Information Security Support Network: A Longitudinal Social Network Analysis. *Australasian Journal of Information Systems*, 23. doi:10.3127/ajis.v23i0.1822
- Daniel, J. (2011). *Sampling Essentials: Practical Guidelines for Making Sampling Choice*. SAGE Publications, Inc. Tillgänglig på:
<https://www.perlego.com/book/2800569> [2026.03.24]
- Eisenberger, R., Huntington, R., Hutchison, S. & Sowa, D. (1986). Perceived Organizational Support. *Journal of Applied Psychology*, 71, s, 500-507. doi:10.1037/0021-9010.71.3.500
- Eisenberger, R., Fasolo, P., & Davis-LaMastro, V. (1990). Perceived Organizational Support and Employee Diligence, Commitment, and Innovation. *Journal of Applied Psychology*, 75(1), s, 51–59. doi:10.1037/0021-9010.75.1.51
- Ghaleb, M.M. S. & Pardaev, J. (2025). Controlling Cyber Crime Through Security Compliance Behavior: Role of Cybersecurity Awareness, Organizational Culture and Trust in Management. *International Journal of Cyber Criminology*, 19(1), s. 1-26. Tillgänglig på:
<https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/437/123>
- Giddens, A. & Sutton, P.W. (2021). *Sociology*. 9 uppl. Polity. Tillgänglig på
<https://www.perlego.com/book/2359514> [2026-04-06]
- Haddaway, N.R., Page, M. J., Pritchard, C. C. & McGuinness, L. A. (2022). PRISMA 2020: An R Package and Shiny App for Producing PRISMA 2020-Compliant Flow Diagrams, with Interactivity for Optimised Digital Transparency and Open Synthesis. *Campbell Systematic Reviews*, 18(2). doi:10.1002/cl2.1230
- Hadlington, L., Popovac, M., Janicke, H., Yevseyeva, I. & Jones, K. (2019). Exploring the Role of Work Identity and Work Locus of Control in Information Security Awareness. *Computer & Security*, 81, s. 41-48. doi:10.1016/j.cose.2018.10.006
- Hawthorne, B.N. (2025). Understanding What Really Drives Trust in the Workplace and the Importance of Trustor Characteristics as Predictors of Co-Worker Trust. *Scientific Reports*, 15, Artikel 34411. doi: 10.1038/s41598-025-17397-0

- Higgins, J.P.T., Thomas, J., Chandler, J., Cumpston, M., Li, T., Page, M.J. & Welch, V.A. (2019). *Cochrane Handbook for Systematic Reviews of Interventions*. 2 uppl., Wiley-Blackwell. Tillgänglig på: <https://www.perlego.com/book/1148893> [2026.01.05]
- Ho, R. (2013). *Handbook of Univariate and Multivariate Data Analysis with IBM SPSS*. 2 uppl., Chapman and Hall/CRC. Tillgängligt på: <https://www.perlego.com/book/1605407> [2026.04.10]
- Hoyle, R.H., & Duvall, J.L. (2004). Determining the Number of Factors in Exploratory and Confirmatory Factor Analysis. I Kaplan, D. (red.) *The SAGE Handbook of Quantitative Methodology for the Social Sciences*. SAGE Publications, Inc., s. 301–316. Tillgänglig på: <https://www.perlego.com/book/1004190> [2026.03.24]
- Högskolan i Skövde (2025). *Riktlinjer för examensarbeten*. Dnr. HS 2025/572. <https://www.his.se/globalassets/styrdokument/utbildning-grundniva-och-avancerad-niva/riktlinjer-for-examensarbeten.pdf> [2026-04-05]
- Integritetsskyddsmyndigheten (IMY) (2021a). *Vad är personuppgifter?* <https://www.imy.se/privatperson/dataskydd/introduktion-till-gdpr/vad-ar-personuppgifter/> [2025-11-05]
- Integritetsskyddsmyndigheten (IMY) (2021b). *Behandling av personuppgifter i arbetslivet*. <https://www.imy.se/verksamhet/dataskydd/dataskydd-pa-olika-omraden/aretsliv/> [2025-11-05]
- Integritetsskyddsmyndigheten (IMY) (2025a). *IMY inleder granskningar utifrån Miljödata-läckan*. [pressmeddelande], 3 november. <https://www.imy.se/nyheter/imy-inleder-granskningar-utifran-miljodata-lackan/>
- Integritetsskyddsmyndigheten (IMY) (2025b). *Omfattande personuppgiftsincident hos Miljödata*. [pressmeddelande], 27 augusti. <https://www.imy.se/nyheter/omfattande-personuppgiftsincident-hos-miljodata/>
- Integritetsskyddsmyndigheten (IMY) (2025c). *Personuppgiftsincidenter*. <https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/personuppgiftsincidenter/> [2025-11-05]
- Integritetsskyddsmyndigheten (IMY) (2025d). *Personuppgiftsansvariga och personuppgiftbiträde*. <https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/personuppgiftsansvariga-och-personuppgiftsbitraden/> [2025-12-11]

- Kazemi, A. (2009). Välbefinnande. I Kazemi, A. (red.) *Välbefinnande i arbetslivet: socialpsykologiska perspektiv*. Studentlitteratur, s. 23–33.
- Lowry, P.B., Posey, C., Bennett, R. & Roberts, T.L. (2015). Leveraging Fairness and Reactance Theories to Deter Reactive Computer Abuse Following Enhanced Organisational Information Security Policies: An Empirical Study of the Influence of Counterfactual Reasoning and Organisational Trust. *Information Systems Journal*, 25(3), s. 193–230. doi: 10.1111/isj.12063
- Mayer, R.C., Davis, J.H. & Schoorman, F.D. (1995). An Integrative Model of Organizational Trust. *The Academy of Management Review*, 20(3) s. 709–734. doi:10.2307/258792
- Mayer, R.C. & Davis, J.H. (1999). The Effect of the Performance Appraisal System on Trust for Management: A Field Quasi-Experiment. *Journal of Applied Psychology*, 84(1), s. 123–136. doi:10.1037/0021-9010.84.1.123
- McGhee, P. (1998). Experimental Social Psychology. Defining Social Psychology. I Sapsford, R., Still, A., Wetherell, M., Miell, D & Stevens, R. (red.). *Theory and Social Psychology*. Sage, s.7, 8.
- Müller, L.S., Nohe, C., Reiners, S., Becker, J. & Hertel, G. (2025). Building Trust in Workplace Information Systems: A Four-Company Study. *Behaviour & Information Technology*. [förhandspublicerad online] doi:10.1080/0144929X.2025.2518236
- Myndigheten för samhällsskydd och beredskap (MSB) (2020). *Cybersäkerhet i Sverige: Hot, metoder, brister och beroenden*.
<https://www.msb.se/siteassets/dokument/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nationellt-center-for-cybersakerhet/rapport-cybersakerhet-i-sverige-2020--hot-metoder-brister-och-beroenden.pdf>
- Myndigheten för samhällsskydd och beredskap (MSB) (2024a). *Cyberhot*. <https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/risker-och-sarbarheter-inom-cybersakerhet-och-cyberfysiska-system/hot-och-metoder-inom-cybersakerhet/cyberhot/> [2025-11-05]

- Myndigheten för samhällsskydd och beredskap (MSB) (2024b). *Verktyg för ökad motståndskraft och stärkt civilt försvar: Årsrapport it- incidentrapportering 2024* <https://rib.msb.se/filer/pdf/31004.pdf>
- Myndigheten för samhällsskydd och beredskap (MSB) (2025a). *It- incidentens påverkan: Ramverk för bedömning av påverkan på it- miljö, verksamhet och samhälle*. <https://rib.msb.se/filer/pdf/31096.pdf> [2025-11-05]
- Myndigheten för samhällsskydd och beredskap (MSB) (2025b). *Resultatredovisning av Cybersäkerhetskollen 2024: Det systematiska cybersäkerhetsarbetet i den offentliga förvaltningen*. <https://rib.msb.se/filer/pdf/30971.pdf>
- Nationalencyklopedin (u.å). *Svensk ordbok*. https://www.ne.se/ordb%C3%B6cker/search?d=ne_sv_ordbok&s=tillit [2026-04-02]
- National Institute of Standards and Technology (NIST) (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. doi:10.6028/NIST.CSWP.29
- Nishisato, S. (2004). Dual scaling. I Kaplan, D. (red.). *The SAGE Handbook of Quantitative Methodology for the Social Sciences*. SAGE Publications, Inc., s. 3–24. Tillgänglig på: <https://www.perlego.com/book/1004190> [2026.03.27]
- Page, M.J. et al. (2021). The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews. *Bmj*, 372(7) doi:10.1136/bmj.n71
- Pallant, J. (2016). *SPSS Survival Manual: A Step by Step Guide to Data Analysis Using IBM SPSS*. 6 uppl., Open University Press.
- Rayyan.ai. (2026). *Faster Systematic Literature Reviews*. <https://www.rayyan.ai/> [2026-03-25]
- Regeringskansliet (2021). *Ett hälsosamt arbetsliv*. <https://www.regeringen.se/regeringens-politik/arbetsmiljostrategin-2021-2025/ett-halsosamt-arbetsliv/> [2026-04-05]
- Regeringskansliet (2025). *Cybersäkerhet*. <https://www.regeringen.se/regeringens-politik/cybersakerhet/> [2025-11-05]
- Regeringen (2025). *Nationell strategi för cybersäkerhet 2025–2029*. Skr.2024/25:121. <https://www.regeringen.se/contentassets/a35c523611834fa1997d1ff5b2297338/nationell-strategi-for-cybersakerhet-20252029-skr.-202425121.pdf> [2025-11-05]

- Rhoades, L. & Eisenberger, R. (2002). Perceived Organizational Support: A Review of the Literature. *Journal of Applied Psychology*, 87(4), s. 698-714.
doi:10.1037/0021-9010.87.4.698
- Rotter, J.B. (1966). Generalized Expectancies for Internal Versus External Control of Reinforcement. *Psychological Monographs: General and Applied*, 80 (1), s. 1-28. doi: 10.1037/h0092976
- Safa, N. S., & von Solms, R. (2016). An Information Security Knowledge Sharing Model in Organizations. *Computers in Human Behavior*. 57, s. 442-451. doi: 10.1016/j.chb.2015.12.037
- Safie, S.I., Zulkifli, M., Sapry, H.R. & Bashah, S.R.M. (2025). Integrating Individual and Organizational Perspectives: A TAM-TOE Framework for ISO 27037 Adoption in Malaysian Government Digital Forensics Agencies. *Journal of open innovation: Technology, Market, and Complexity*, 11(3), Artikel 100595.
doi:10.1016/j.joitmc.2025.100595
- Sandblad, B., Gulliksen, J., Lantz, A., Walldius, Å. & Åborg, C. (2018). *Digitaliseringen och arbetsmiljön*. Studentlitteratur.
- Schoorman, F.D., Mayer, R.C. & Davis, J.H. (2007). An Integrative Model of Organizational Trust: Past, Present, and Future. *Academy of Management Review*, 32(2), s. 344-354. doi:10.5465/AMR.2007.24348410
- Schoorman, F.D., Mayer, R.C. & Davis, J.H. (2016). Empowerment in Veterinary Clinics: The Role of Trust in Delegation. *Journal of Trust Research*, 6(1), s. 76-90. doi:10.1080/21515581.2016.1153479
- Searle, R., Renaud, K.V. & van der Werff, L. (2024). Shaken to the Core: Trust Trajectories in the Aftermaths of Adverse Cyber Events. *Journal of Intellectual Capital*, 25(5-6), s. 1154–1183. doi:10.1108/JIC-02-2024-0038
- Stacey, P., Taylor, R., Olowosule, O. & Spanaki, K. (2021). Emotional Reactions and Coping Responses of Employees to a Cyber-Attack: A Case Study. *International Journal of Information Management*, 58, Artikel 102298.
doi:10.1016/j.ijinfomgt.2020.102298
- Steenkamp, J.B.E.M., De Jong, M.G. & Baumgartner, H. (2010). Socially Desirable Response Tendencies in Survey Research. *Journal of Marketing Research*, 47(2), s. 199-214. doi:10.1509/jmkr.47.2.199

- Spector, P.E. (1982). Behavior in Organizations as a Function of Employee's Locus of Control. *Psychological Bulletin*, 91(3), s. 482-497. doi:10.1037/0033-2909.91.3.482
- Spector, P.E. (1988). Development of the Work Locus of Control Scale. *Journal of Occupational Psychology*, 61, s. 335–340. doi:10.1111/j.2044-8325.1988.tb00470.x
- Sveriges kommuner och Regioner (2025). *Tabeller Kommunal personal 2025*.
<https://skr.se/personalochkompetensforsorjning/statistikompersonalochkompetensforsorjning/personalstatistik/tabellerkommunalpersonal2025.9188.htm>
- Svenson, F., Ballová Mikušková, E., & Launer, M. A. (2023). Credibility and Trust of Information Privacy at the Workplace in Slovakia. The Use of Intuition. *Journal of Information, Communication and Ethics in Society*, 21(3), s. 302–321. doi:10.1108/JICES-02-2022-0011
- Vetenskapsrådet (2002). *Forskningsetiska principer 2002*.
https://www.vr.se/download/18.68c009f71769c7698a41df/1610103120390/Forskningsetiska_principer_VR_2002.pdf
- Vetenskapsrådet (2017). *God forskningssed 2017*.
<https://www.vr.se/analys/rapporter/vara-rapporter/2017-08-29-god-forsknings-sed-2017.html>
- Vetenskapsrådet (2024). *God forskningssed 2024*.
<https://www.vr.se/analys/rapporter/vara-rapporter/2024-10-02-god-forsknings-sed-2024.html>
- Wang, S., Asif, M., Shahzad, M.F. & Ashfaw, M. (2024). Data Privacy and Cybersecurity Challenges in the Digital Transformation of The Banking Sector. *Computers & Science*, 147, Artikel 104051. doi:10.1016/j.cose.2024.104051
- Wetherell, M. & Still, A. (1998). Realism and Relativism. I Sapsford, R., Still, A., Wetherell, M., Miell, D & Stevens, R. (red.) *Theory and Social psychology*. Sage, s. 99–114.
- Yarovenko, H., Bilovodska, V., Bylbas, R., Pankiv, O., Baghizade, M., Niemi, O. & Djakons, D. (2025). Digital Readiness of European Countries to Combat Corruption and Cyber Threats: Panel Analysis. *Business Ethics & Leadership*,

9(2), s. 238–265. Tillgänglig på:

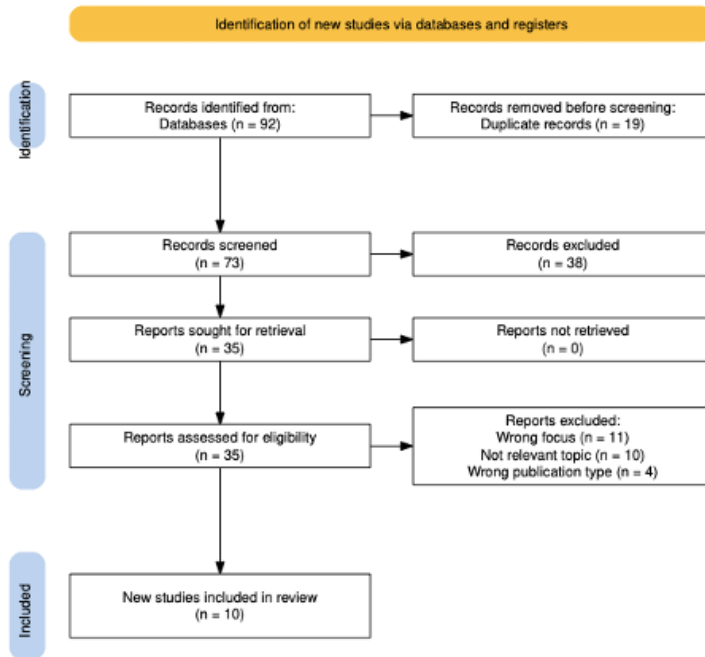
<https://armgpublishing.com/journals/bel/volume-9-issue-2/article-18/>

Zumbo, B.D. & Rupp, A.A. (2004). Responsible Modeling of Measurement Data for Appropriate Inferences: Important Advances in Reliability and Validity Theory. I

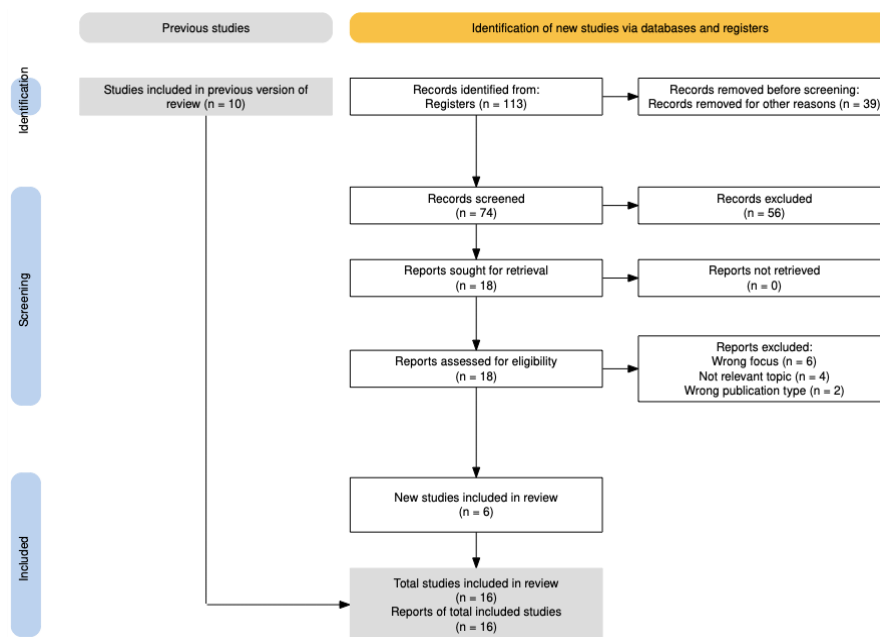
Kaplan, D. (red). *The SAGE Handbook of Quantitative Methodology for the Social Sciences*. SAGE Publications, Inc., s. 73–92. Tillgänglig på:

<https://www.perlego.com/book/1004190> [2026.01.08]

Bilaga 1. PRISMA-diagram



Figur 2. Flödesschema över första urvalsprocessen som avslutades den 12 december 2025 (Page et al. 2021)



Figur 3. Flödesschema över andra urvalsprocessen som avslutades den 26 februari 2026 (Haddaway et al. 2022).

Bilaga 2. Sökmatriser

Tabell 11.1 *Litteratursökning i Libsearch (2025.11.21)*

Databas	Sökord	Avgränsningar	Antal träffar	Urval 1	Urval 2
Libsearch					
Datum	21/11-25				
1	((Employee* OR "Co-worker*" OR worker* OR leader* OR employer* OR "employee satisfaction") AND ("cyber attack" OR cybersecurity OR "information security" OR "insider threat" OR "phishing susceptibility" OR "security awareness" OR "security compliance"))	Filter: Peer Reviewed, akademiska tidskrifter	5112		
2	AND (trust OR "interpersonal trust" OR "organizational trust" OR "trust dynamics" OR "trust repair" OR "psychological factors" OR "social psychology" OR "organizational behavior")	Filter: Peer Reviewed, akademiska tidskrifter	466		
3	AND ("Social support" OR "workplace support" OR "Support group" OR "Support system" OR "Colleag* support" OR "Lead* Support" OR "social relationships" OR "social networks"))	Filter: Peer Reviewed, akademiska tidskrifter	8	4	3

Tabell 11.2 *Litteratursökning i Academic Search Premier (2025.11.25)*

Databas	Sökord	Avgränsningar	Antal träffar	Urval 1	Urval 2
Academic Search Premier					
Datum	25/11-25				
1	((Employee* OR "Co-worker*" OR worker* OR leader* OR employer* OR "employee satisfaction") AND ("cyber attack" OR cybersecurity OR "information security" OR "insider threat" OR "phishing susceptibility" OR "security awareness" OR "security compliance"))	Filter: Peer-review, Akademiska tidskrifter	2183		
2	AND (trust OR "interpersonal trust" OR "organizational trust" OR "trust dynamics" OR "trust repair" OR "psychological factors" OR "social psychology" OR "organizational behavior")	Filter: Peer-review, Akademiska tidskrifter	194		
3	AND (control or "perceived control"))	Filter: Peer- review, akademiska tidskrifter, senare 10 år3n	30	28	9

Tabell 11.3 *Litteratursökning i PsycINFO (2025.11.25)*

Databaser	Sökord	Avgränsningar	Antal träffar	Urval 1	Urval 2
Psycinfo					
Datum	25/11-25				
1	((Employee* OR "Co-worker*" OR worker* OR leader* OR employer* OR "employee satisfaction") AND ("cyber attack" OR cybersecurity OR "information security" OR "insider threat" OR "phishing susceptibility" OR "security awareness" OR "security compliance"))	Filter: Peer reviewed och engelska	174		
2	AND (trust OR "interpersonal trust" OR "organizational trust" OR "trust dynamics" OR "trust repair" OR "psychological factors" OR "social psychology" OR "organizational behavior")	Filter: Peer reviewed och engelska	27		
3	AND (control or "perceived control"))	Filter: Peer reviewed och engelska	7	7	1

Tabell 11.4 Litteratursökning i Web of Science (2025.12.01)

Databas	Sökord	Avgränsningar	Antal träffar	Urval 1	Urval 2
Web of Science					
Datum	01/12- 25				
1	((Employee* OR "Co-worker*" OR worker* OR leader* OR employer* OR "employee satisfaction") AND ("cyber attack" OR "security awareness" OR "data leak" OR datalek)	Filter: Vetenskapliga artiklar	1574		
2	AND ("employee trust" OR "trust in employer" OR Confidence OR reliance OR "trust in company" OR "Trust in organization" OR "Trust in organisation" OR intrest OR "Rely on the company"	Filter: Vetenskapliga artiklar	212		
3	AND ("Social support" OR "workplace support" OR "Support group" OR "Support system" OR "Colleag* support" OR "social relationships" OR "social networks"))	Filter: Vetenskapliga artiklar. De senaste fem åren.	27	25	17

Tabell 11.5 Litteratursökning i Libsearch (2026.02.26)

Databas	Sökord	Avgränsning	Antal träffar	Urval 1	Urval 2
Libsearch					
Datum	26.02.26				
1	((Employee* OR "Co-worker*" OR worker* OR leader* OR employer* OR "employee satisfaction") AND ("cyber attack*" OR "cyber incident*" OR "cyber security" OR "data leak" OR cyber*))	Filter: Akademiska tidskrifter Peer-review Senast 10 år	12150		
2	AND (Trust OR "employee trust" OR "trust in employer" OR "trust in company" OR "Trust in organization" OR "Trust in organisation" OR "Rely on the company" OR "Organizational trust" OR "Organisational trust" OR "Company trust" OR "trust in organisational cybersecurity" OR "trust in organizational cybersecurity" OR "organisational cybersecurity management*" OR "trust in organizational cybersecurity management*")	Filter: Akademiska tidskrifter Peer-review Senast 10 år	552		
3	AND (Control* OR "work locus of control" OR "Perceived work locus of control" OR "locus of control in work*" OR "Control in work*" OR "Perceived control"))	Filter: Akademiska tidskrifter Peer-review Senast 10 år	113	74	18

Bilaga 3. Operationaliseringsmatris

Tabell 12 som visar vår operationalisering

Huvudbegrepp	Underbegrepp	Indikatorer	Enkätfrågor
Bakgrundsfrågor	Sociodemografiska frågor	Självidentifierat kön	Vilket kön identifierar du dig som? Kvinna/Man/Icke-binär/annat/vill inte uppge
		Högsta avslutad utbildning	Vilken är din högsta avslutade utbildning? Grundskola/Gymnasium/Eftergymnasial utbildning t.ex. Yrkeshögskola/Universitet-Högskola/Annat/vill inte uppge
		Anställningsform	Vad är din nuvarande anställningsform? Tillsvidareanställd/Visstidsanställd/Timanställd/Annat/Vill inte uppge
		Daglig digital arbetstid	Ungefär hur många timmar per dag använder du digitala enheter (dator/mobil) i ditt arbete? 0 1-2, 3-4, 5-6, 7-8, 9-mer
		Riskuppfattning av cyberhot i organisationen	Jag uppfattar cyberhot som en allvarlig risk för min organisation Instämmer inte alls -Instämmer helt, 1-5
Cybersäkerhetsrelaterade bakgrundsvariabler	Cybersäkerhetsrelaterade bakgrundsvariabler	Grad av exponering för cybersutbildning	Jag har fått tillräckligt med utbildning i information eller cybersäkerhet genom min arbetsgivare Instämmer inte alls -Instämmer helt, 1-5
		Förtroende för förebyggande insatser	Jag har förtroende för att organisationen arbetar aktivt för att förebygga cyberincidenter Instämmer inte alls - Instämmer helt 1-5
		Förtroende för upptäckt	Jag har förtroende för att organisationen kan upptäcka cyberincidenter i tid Instämmer inte alls - Instämmer helt 1-5
		Förtroende för informationshantering	Jag litar på att organisationen ger mig snabb och korrekt information om en cyberincident inträffar Instämmer inte alls - Instämmer helt, 1-5
		Förtroende för informationshantering	Jag litar på att organisationen skyddar min personliga information vid en cyberincident Instämmer inte alls - Instämmer helt, 1-5
Tillit till arbetsgivarens cybersäkerhetshantering	Tillit "Övertygelsen att någon är pålitlig och har goda avsikter mot en själv" (NE u.å.) Cybersäkerhetshantering Arbetet med att identifiera, skydda mot och upptäcka cyberhot (NIST 2024)	Förtroende för ledningens cybersäkerhetsarbete	Jag har förtroende för att ledningen tar cybersäkerhet på allvar Instämmer inte alls - Instämmer helt, 1-5
		Upplevd kompetens	Högsta ledningen har stor kunskap om det arbete som behöver göras Instämmer inte alls - Instämmer helt, 1-5
		Upplevd kompetens	Högsta ledningen är väl kvalificerad. Instämmer inte alls - Instämmer helt, 1-5
		Upplevd omsorg från ledningen	Högsta ledningen är mycket mån om mitt välbefinnande Instämmer inte alls - Instämmer helt, 1-5
		Upplevd omsorg från ledning	Mina behov och önskemål är mycket viktiga för högsta ledningen Instämmer inte alls - Instämmer helt, 1-5
Organisatorisk tillit	Förmåga/ Kompetens "Den grupp av färdigheter, kompetenser och egenskaper som gör det möjligt för en part att ha inflytande inom ett område" (Mayer & Davis 1999). Välvilja "I vilken utsträckning en betrodd part anses vilja göra gott för den som ger förtroendet bortom ett egocentriskt vinstmotiv." (Mayer & Davis 1999).	Upplevd kompetens	Högsta ledningen har stor kunskap om det arbete som behöver göras Instämmer inte alls - Instämmer helt, 1-5
		Upplevd kompetens	Högsta ledningen är väl kvalificerad. Instämmer inte alls - Instämmer helt, 1-5
		Upplevd omsorg från ledningen	Högsta ledningen är mycket mån om mitt välbefinnande Instämmer inte alls - Instämmer helt, 1-5
Organisatorisk tillit	Organisatorisk tillit "Viljan att vara sårbar inför en annan parts handlingar." (Mayer, Davis & Schoorman 1995).	Organisatorisk tillit	Organisatorisk tillit "Viljan att vara sårbar inför en annan parts handlingar." (Mayer, Davis & Schoorman 1995).

	Integritet ”Den som ger förtroendets uppfattning att den betrodda följer en uppsättning principer som den som ger förtroendet finner acceptabla.” (Mayer & Davis 1999).	Upplevd principfasthet	Jag behöver aldrig undra om högsta ledningen kommer att hålla sitt ord. Instämmer inte alls - Instämmer helt, 1-5
		Upplevd principfasthet*	Högsta ledningens handlingar och beteenden är inte särskilt konsekventa.* Instämmer inte alls - Instämmer helt, 1-5
Upplevt organisatoriskt stöd <i>De övergripande uppfattningar som anställda skapar kring hur mycket arbetsgivaren värdesätter deras bidrag och bryr sig om deras hälsa och välmående</i> (Eisenberger et al 1986).		Upplevd uppskattning från ledning	Organisationen värdesätter mitt bidrag till dess välbefinnande. Instämmer inte alls - Instämmer helt 1-5
		Upplevd uppskattning från ledning	Organisationen tar i hög grad hänsyn till mina mål och värderingar. Instämmer inte alls - Instämmer helt 1-5
		Upplevd villighet från ledningen	Hjälp finns tillgänglig från organisationen när jag har ett problem. Instämmer inte alls - Instämmer helt 1-5
		Upplevd uppskattning från ledning	Organisationen bryr sig verkligen om mitt välbefinnande. Instämmer inte alls - Instämmer helt 1-5
		Upplevd villighet från ledningen	Organisationen är villig att anstränga sig för att hjälpa mig utföra mitt arbete på bästa möjliga sätt. Instämmer inte alls - Instämmer helt 1-5
		Upplevd uppskattning från ledning	Organisationen bryr sig om mina åsikter Instämmer inte alls - Instämmer helt 1-5
Arbetsrelaterad kontrolluppfattning (Work Locus of Control) <i>”En individs grundläggande inställning till var makten över livshändelser är placerad”</i> (Spector 1982).	Intern kontrolluppfattning <i>”En generell förväntan om huruvida belöningar, förstärkningar eller livshändelser bestäms av individens egna handlingar”</i> (Spector 1988).	Upplevd hög påverkan	På det flesta jobb kan människor i princip uppnå vad de än bestämmer sig för Instämmer verkligen inte - Instämmer verkligen 1-6
		Upplevd hög påverkan	Befordringar ges till anställda som presterar bra på jobbet Instämmer verkligen inte - Instämmer verkligen 1-6
		Upplevd hög påverkan	Människor som presterar bra på jobbet belönas vanligtvis Instämmer verkligen inte - Instämmer verkligen 1-6
	Extern kontrolluppfattning <i>”En generell förväntan om huruvida belöningar, förstärkningar eller livshändelser bestäms av yttre omständigheter.”</i> (Spector 1988).	Upplevd låg påverkan*	Befordringar beror oftast på tur* Instämmer verkligen inte - Instämmer verkligen 1-6
		Upplevd låg påverkan*	På det flesta arbeten krävs mycket tur för att bli en framstående medarbetare * Instämmer verkligen inte - Instämmer verkligen 1-6
		Upplevd låg påverkan*	Skillnaden mellan personer som tjänar mycket respektive lite pengar beror till stor del på tur* Instämmer verkligen inte - Instämmer verkligen 1-6

Bilaga 4. Enkäten

Hej och tack på förhand för ditt deltagande!

Enkäten innehåller 29 frågor och tar cirka 5-10 minuter att besvara.

Deltagandet är frivilligt och du är anonym. Dina svar kommer endast att delas med de personer som anges i mailet och ingen annan.

Frågorna i enkäten berör områden som cybersäkerhet, tillit, organisatoriskt stöd och kontroll. Alla frågor handlar därför inte direkt om cybersäkerhet utan vissa frågor rör faktorer som kan ha en inverkan på hur medarbetare upplever arbetsgivarens cybersäkerhetsarbete. För att undersökningen ska hålla hög kvalitet uppskattar vi att du svarar på så många frågor och påståenden som möjligt.

Om det dyker upp frågor kring ditt deltagande eller studien är det bara att kontakta oss på mejladresserna nedan.

Vi uppskattar dina svar och din tid!

Med vänliga hälsningar,

Robert Eriksson, a23rober@student.his.se

Lina Samavat, d23linsd@student.his.se

Christel Tveiten Emanuelsson, a23chrem@student.his.se

Jag samtycker till att mina svar används för studiens syfte.

- Ja
- Nej

I slutet av enkäten får du en identifikationskod. Spara den om du vill kunna dra tillbaka ditt deltagande.

Om du vill avbryta ditt deltagande skickar du mejl till någon av kontaktpersonerna i informationsbladet med din identifikationskod och texten "Jag önskar att avbryta mitt deltagande". Dina svar kommer då att raderas.

Demografiska frågor:

1. Vilket kön identifierar du dig som?

- Kvinna
- Man
- Icke-binär
- Vill inte uppge
- Annat

2. Vilken är din högsta avslutade utbildning?

- Grundskola
- Gymnasium
- Eftergymnasial (t.ex. yrkeshögskola)
- Universitet/Högskola
- Annan utbildning
- Vill inte uppge

3. Vad är din nuvarande arbetsform?

- Tillsvidareanställd
- Visstidsanställd
- Timanställd
- Annat
- Vill inte uppge

4. Ungefär hur många timmar per dag använder du digitala enheter (dator eller mobil) i ditt arbete? Detta inkluderar journalsystem, e-post, verksamhetssystem och intranät.

- 0h
- 1-2h
- 3-4h
- 5-6h
- 7-8h
- 9h och mer

I följande påståenden anger du i vilken grad som du instämmer.

Med *cyberhot* menas digitala angrepp eller försök att komma åt, störa eller skada organisationens information eller IT-system.

Med *cybersäkerhet* menas skydd av information och digitala system, inklusive informationssäkerhet, tillgänglighet och sekretess

5. Jag uppfattar cyberhot som en allvarlig risk för min organisation

1. Instämmer inte alls
2. Instämmer i liten grad
3. Varken eller
4. Instämmer i hög grad
5. Instämmer helt

6. Jag har fått tillräckligt med utbildning i information eller cybersäkerhet genom min arbetsgivare

1. Instämmer inte alls
2. Instämmer i liten grad
3. Varken eller
4. Instämmer i hög grad
5. Instämmer helt

Tillit till arbetsplatsen

I följande påståenden anger du i vilken grad som du instämmer.

Med *högsta ledningen* menas kommunen i sin roll som arbetsgivare.

Förmåga och kompetens

7. Högsta ledningen har stor kunskap om det arbete som behöver göras

1. Instämmer inte alls
2. Instämmer i liten grad
3. Varken eller
4. Instämmer i hög grad

5. Instämmer helt

8. Högsta ledningen är väl kvalificerad.

1. Instämmer inte alls
2. Instämmer i liten grad
3. Varken eller
4. Instämmer i hög grad
5. Instämmer helt

Välvilja

9. Högsta ledningen är mycket mån om mitt välbefinnande

1. Instämmer inte alls
2. Instämmer i liten grad
3. Varken eller
4. Instämmer i hög grad
5. Instämmer helt

10. Mina behov och önskemål är mycket viktiga för högsta ledningen

1. Instämmer inte alls
2. Instämmer i liten grad
3. Varken eller
4. Instämmer i hög grad
5. Instämmer helt

Integritet

11. Jag behöver aldrig undra om högsta ledningen kommer att hålla sitt ord.

1. Instämmer inte alls
2. Instämmer i liten grad
3. Varken eller
4. Instämmer i hög grad
5. Instämmer helt

12. Högsta ledningens handlingar och beteenden är inte särskilt konsekventa. *

1. Instämmer inte alls
2. Instämmer i liten grad
3. Varken eller
4. Instämmer i hög grad
5. Instämmer helt

Cybersäkerhetshantering

I följande påståenden anger du i vilken grad som du instämmer om digital säkerhet

Med *organisationen* menas kommunen i sin roll som arbetsgivare.

Med *cyberincidenter* menas händelser som påverkar organisationens information eller digitala system, till exempel intrång eller skadlig kod.

Förebyggande och beredskap

13. Jag har förtroende för att organisationen arbetar aktivt för att förebygga cyberincidenter

1. Instämmer inte alls
2. Instämmer i liten grad
3. Varken eller
4. Instämmer i hög grad
5. Instämmer helt

14. Jag har förtroende för att organisationen kan upptäcka cyberincidenter i tid

1. Instämmer inte alls
2. Instämmer i liten grad
3. Varken eller
4. Instämmer i hög grad
5. Instämmer helt

15. Jag litar på att organisationen ger mig snabb och korrekt information om en cyberincident inträffar

1. Instämmer inte alls
2. Instämmer i liten grad
3. Varken eller
4. Instämmer i hög grad
5. Instämmer helt

16. Jag litar på att organisationen skyddar min personliga information vid en cyberincident

1. Instämmer inte alls
2. Instämmer i liten grad
3. Varken eller
4. Instämmer i hög grad
5. Instämmer helt

17. Jag har förtroende för att ledningen tar cybersäkerhet på allvar

1. Instämmer inte alls
2. Instämmer i liten grad
3. Varken eller
4. Instämmer i hög grad
5. Instämmer helt

Upplevt organisatoriskt stöd

I följande påståenden ska du ange i vilken grad du instämmer i hur din organisation visar stöd

Med *organisationen* menas kommunen i sin roll som arbetsgivare.

18. Organisationen värdesätter mitt bidrag till dess välbefinnande

1. Instämmer inte alls
2. Instämmer i liten grad
3. Varken eller
4. Instämmer i hög grad
5. Instämmer helt

19. Organisationen tar i hög grad hänsyn till mina mål och värderingar

1. Instämmer inte alls
2. Instämmer i liten grad
3. Varken eller
4. Instämmer i hög grad
5. Instämmer helt

20. Hjälp finns tillgänglig från organisationen när jag har ett problem

1. Instämmer inte alls
2. Instämmer i liten grad
3. Varken eller
4. Instämmer i hög grad
5. Instämmer helt

21. Organisationen bryr sig verkligen om mitt välbefinnande

1. Instämmer inte alls
2. Instämmer i liten grad
3. Varken eller
4. Instämmer i hög grad
5. Instämmer helt

22. Organisationen är villig att anstränga sig för att hjälpa mig utföra mitt arbete på bästa möjliga sätt

1. Instämmer inte alls
2. Instämmer i liten grad
3. Varken eller
4. Instämmer i hög grad
5. Instämmer helt

23. Organisationen bryr sig om mina åsikter

1. Instämmer inte alls
2. Instämmer i liten grad
3. Varken eller
4. Instämmer i hög grad
5. Instämmer helt

Arbetsrelaterad kontrolluppfattning

I följande påståenden anger du hur mycket du instämmer i vad som kan påverka framgång i arbetslivet

Intern kontrolluppfattning

24. På de flesta jobb kan människor i princip uppnå vad de än bestämmer sig för

1. Instämmer verkligen inte
2. Instämmer inte
3. Instämmer delvis inte
4. Instämmer delvis
5. Instämmer
6. Instämmer verkligen

25. Befordringar ges till anställda som presterar bra på jobbet

1. Instämmer verkligen inte
2. Instämmer inte
3. Instämmer delvis inte
4. Instämmer delvis
5. Instämmer
6. Instämmer verkligen

26. Människor som presterar bra på jobbet belönas vanligtvis

1. Instämmer verkligen inte
2. Instämmer inte
3. Instämmer delvis inte
4. Instämmer delvis
5. Instämmer
6. Instämmer verkligen

Extern kontrolluppfattning

27. Befordringar beror oftast på tur. *

1. Instämmer verkligen inte
2. Instämmer inte
3. Instämmer delvis inte
4. Instämmer delvis
5. Instämmer
6. Instämmer verkligen

28. På de flesta arbeten krävs mycket tur för att bli en framstående medarbetare. *

1. Instämmer verkligen inte
2. Instämmer delvis inte
3. Instämmer delvis
4. Instämmer
5. Instämmer verkligen

29. Skillnaden mellan personer som tjänar mycket respektive lite pengar beror till stor del på tur. *

1. Instämmer verkligen inte
2. Instämmer inte
3. Instämmer delvis inte
4. Instämmer delvis
5. Instämmer
6. Instämmer verkligen

Bilaga 5. Informationsbrev

Hej,

Vi är tre studenter som studerar på det Socialpsykologiska programmet på Högskolan i Skövde. Vi håller just nu på med vårt examensarbete och skulle uppskatta din hjälp genom att du besvarar vår enkät.

Enkäten handlar om medarbetarnas upplevelse av arbetsgivarens cybersäkerhetsarbete. Syftet med vår studie är att bidra med kunskap som kan hjälpa kommuner att utveckla arbetssätt som bättre stödjer och underlättar för medarbetarna.

Enkäten innehåller 29 frågor och tar cirka 5-10 minuter att besvara.

Deltagandet är frivilligt och du är anonym. Du kan när som helst avbryta utan att ange anledning. Studien är godkänd i enlighet med etiska riktlinjer för uppsatser vid Högskolan i Skövde.

LÄNK TILL ENKÄTEN

https://qualtricsxmgp63lqvxl.qualtrics.com/jfe/form/SV_5iGr4nIsnBBOhyS

Personuppgifter

Enligt dataskyddsförordningen (2016/679) är Högskolan i Skövde personuppgiftsansvarig för personuppgiftsbehandlingar i studentarbeten. Det personuppgifter som samlas in i enkäten är anställningsform, kön, utbildningsnivå, IT-erfarenhet samt svar på frågor om arbetsrelaterade och organisatoriska faktorer. Uppgifterna används endast för detta examensarbete, lagras digitalt på Högskolan i Skövdes och kan inte kopplas till dig som person eller påverka din arbetssituation. Alla uppgifter raderas efter att arbete är godkänt.

Den rättsliga grunden för behandlingen är ditt samtycke.

Om det dyker upp frågor kring ditt deltagande eller studien är det bara att kontakta oss på mejladresserna nedan.

Tack på förhand för ditt deltagande!

Kontakt

Robert Eriksson, a23rober@student.his.se

Lina Samavat, d23linsd@student.his.se

Christel Tveiten Emanuelsson, a23chrem@student.his.se

Handledare

Sakarias Bank, sakarias.bank@his.se och telefonnummer: 0500-448220

Vid eventuella klagomål

Om du har några funderingar eller klagomål avseende hur dina personuppgifter behandlas kan du kontakta högskolans dataskyddsombud via dataskyddsombud@his.se

Bilaga 6. Kompletterande informationsbrev

ÄR DU KOMMUNANSTÄLLD?

Delta i vår enkät om cybersäkerhet i kommuner!

Hej, vi är tre studenter på Socialpsykologiska programmet vid Högskolan i Skövde som just nu genomför vårt examensarbete.

Vi söker dig som arbetar inom en kommun, oavsett roll eller arbetsområde, och som vill bidra genom att svara på vår enkät om hur medarbetare upplever arbetsgivarens cybersäkerhetsarbete.

LÄNK TILL ENKÄTEN:

https://qualtricsxmgp63lqvxl.qualtrics.com/jfe/form/SV_5iGr4nIsnBBOhyS

- Enkäten tar ca 5-10 minuter och innehåller 29 frågor.
- Deltagandet är helt frivilligt och anonymt.
- Du kan avbryta när som helst utan att ange anledning

Enkäten handlar om medarbetarnas upplevelse av arbetsgivarens cybersäkerhetsarbete. Syftet är att bidra med kunskap som kan hjälpa kommuner att utveckla bättre stöd och arbetssätt kring cybersäkerhet för sina medarbetare.

Stort tack för att du tar dig tid att hjälpa oss!

Har du frågor är du välkommen att kontakta oss via mejl:

Robert Eriksson, a23rober@student.his.se

Lina Samavat, d23linsd@student.his.se

Christel Tveiten Emanuelsson, a23chrem@student.his.se