JÖNKÖPING UNIVERSITY
School of Engineering

Cybersäkerhets-medvetenheten bland produktionsnära personal hos små och medelstora företag i tillverkningsindustrin

HUVUDOMRÅDE: *Informatik*
FÖRFATTARE: *Carl Lundin, Erik Ruotanen och Oliver Zaar*
HANDLEDARE: *Sonny Johansson*
JÖNKÖPING 2026 juni

Detta examensarbete är utfört vid Tekniska Högskolan i Jönköping inom informatik. Författarna svarar själva för framförda åsikter, slutsatser och resultat.

Examinator: Anders Adlemo

Handledare: Sonny Johansson

Omfattning: 15 hp (grundnivå)

Datum: 2026-06-06

Sammanfattning

Den ökade digitaliseringen av tillverkningsindustrin har gjort små och medelstora företag mer beroende av uppkopplade system, automatiserade processer och integrerade IT- och operationsteknologiska system (OT-miljöer). Detta skapar nya möjligheter för effektivitet och utveckling, men innebär samtidigt ökade cybersäkerhetsrisker. I detta sammanhang spelar cybersäkerhetsmedvetenhet en viktig roll, särskilt hos produktionsnära personal som arbetar nära digitala system men ofta saknar anpassad utbildning och tydliga säkerhetsrutiner. Syftet med denna studie är att skapa en fördjupad förståelse för cybersäkerhetsmedvetenhet inom små och medelstora tillverkningsföretag, med särskilt fokus på produktionsnära personal. Studien undersöker vilken nivå av cybersäkerhetsmedvetenhet som beskrivs i tidigare forskning samt vilka metoder, strategier och organisatoriska faktorer som kan bidra till att stärka denna medvetenhet.

För att besvara studiens syfte har en scoping review genomförts. Vetenskaplig litteratur har identifierats genom sökningar i databaser såsom Scopus, Primo, Google Scholar och IEEE Xplore. Det insamlade materialet har därefter analyserats genom tematisk analys. Analysen resulterade i fyra centrala teman: nivån av cybersäkerhetsmedvetenhet hos produktionsnära personal, organisatoriska faktorer som påverkar cybersäkerhetsmedvetenhet, metoder och strategier för att stärka cybersäkerhetsmedvetenhet samt utmaningar och begränsningar vid implementering. Resultatet visar att cybersäkerhetsmedvetenheten hos produktionsnära personal ofta är begränsad och ojämnt fördelad. Studien visar även att utbildning, policyer och tekniska lösningar kan bidra till ökad medvetenhet, men att sådana insatser behöver vara kontinuerliga, praktiskt relevanta och anpassade till produktionsmiljön. Vidare framkommer att ledningens engagemang, resurser, ansvarsfördelning, organisationskultur och samordning mellan IT och OT har stor betydelse för hur cybersäkerhetsmedvetenhet utvecklas i praktiken. Studien är begränsad till tidigare publicerad forskning och innehåller ingen egen empirisk datainsamling från företag. Trots detta bidrar studien med en samlad bild av forskningsläget och visar att cybersäkerhetsmedvetenhet bör förstås som en del av organisationens samlade säkerhetsarbete, snarare än som enbart en individuell kunskapsfråga.

Nyckelord

Cyberhot, cybersäkerhetsmedvetenhet, IT/OT, produktionsnära personal, scoping review, små och medelstora företag, tematisk analys, tillverkningsindustri.

Innehåll

Innehåll I

1 Introduktion 3

1.1 Problemformulering 4

1.1.1 Digitalisering och ökad riskbild 4

1.1.2 SMF och resursbegränsningar 5

1.1.3 Produktionsnära personal och mänskliga faktorer 6

1.1.4 Forskningslucka och behov 6

1.2 Syfte 7

1.3 Frågeställningar 8

1.4 Avgränsningar 8

1.5 Disposition 9

2 Metod och genomförande 10

2.1 Scoping review 14

2.2 Databaser 16

2.3 Sökkriterier 17

2.4 Söktermer 18

2.5 Inkluderade studier 20

2.6 Dataanalys 20

2.7 Trovärdighet 23

2.8 Överväganden 25

2.9 AI användning 26

3 Tidigare Forskning 27

4 Resultat 32

4.1 Nivån av cybersäkerhetsmedvetenhet hos produktionsnära personal 34

4.2 ORGANISATORISKA FAKTORER SOM PÅVERKAR CYBERSÄKERHETSMEDVETENHET 36

4.3 METODER OCH STRATEGIER FÖR ATT STÄRKA CYBERSÄKERHETSMEDVETENHET 38

4.4 UTMANINGAR OCH BEGRÄNSNINGAR I IMPLEMENTERING AV CYBERSÄKERHETSMEDVETENHET 41

4.5 SAMMANFATTNING AV RESULTAT 43

5 Diskussion 46

5.1 DISKUSSION KOPPLAT TILL FORSKNINGSFRÅGA 1 46

5.2 DISKUSSION KOPPLAT TILL FORSKNINGSFRÅGA 2 46

5.3 METODDISKUSSION 48

6 Slutsatser och rekommendationer 51

6.1 PRAKTISKA IMPLIKATIONER 52

6.2 VETENSKAPLIGA IMPLIKATIONER 54

6.3 VIDARE FORSKNING 55

7 Referenser 57

1 Introduktion

Digitaliseringen av tillverkningsindustrin har förändrat hur små och medelstora företag (SMF) bedriver sin verksamhet. Införandet av uppkopplade maskiner, sensorer, molntjänster och Industrial Internet of Things (IIoT), alltså uppkopplade industriella enheter samt automatiserade produktionsprocesser skapar nya möjligheter men ökar samtidigt exponeringen för cyberhot och systemrelaterade sårbarheter (Corallo et al., 2022). Corallo et al. (2022) beskriver vidare att integrationen mellan traditionell IT och OT, alltså styrsystem och utrustning som driver själva produktionen förstärker riskbilden, eftersom många industriföretag saknar anpassade rutiner för att hantera den tekniska komplexitet som uppstår vid denna sammanvävning. I takt med att produktionen digitaliseras ökar även attackytan genom fler uppkopplade enheter och system, vilket gör att säkerhetsrisker sprids över både tekniska och organisatoriska nivåer.

Utmaningarna handlar dock inte enbart om teknik. Forskning inom cybersäkerhetsområdet framhåller att mänskliga faktorer såsom attityder, beteenden och kunskapsnivåer ofta utgör en betydande orsak till säkerhetsincidenter (Khando et al., 2021). Johansson et al. (2022) betonar att produktionsnära personal ofta är den mest utsatta gruppen eftersom de arbetar nära uppkopplad utrustning men samtidigt sällan får kontinuerlig och anpassad utbildning. Detta stöds även av Brunken et al. (2025), som visar att produktionspersonal i tillverkningsmiljöer ofta har begränsad kontakt med traditionella IT-system och därför inte alltid uppfattar cybersäkerhet som en del av sitt eget ansvar. Samtidigt understryker Akter et al. (2025) att cybersäkerhetsmedvetenhet inte bör betraktas enbart på individnivå utan snarare som något som formas av organisationens samt ledningens kultur, strategi och prioriteringar. Forskning visar även att organisatoriska arbetssätt har stor betydelse för hur väl informationssäkerhet fungerar i praktiken. Alzahrani och Seth (2021) visar att faktorer som säkerhetsutbildning, kunskapsdelning, säkerhetsrelaterad utbildning och synliggörande av säkerhetsarbete inom organisationen har en tydlig positiv påverkan på hur väl informationssäkerheten fungerar i små och medelstora tillverkningsföretag. Studien visar även att säkerhetsutbildning och kunskapsdelning bidrar till ökat förtroende inom organisationen, vilket i sin tur kan stärka det övergripande säkerhetsarbetet. Detta understryker att cybersäkerhetsmedvetenhet inte enbart formas

av individuella kunskaper, utan också av hur organisationen arbetar med att sprida kunskap, skapa engagemang och gör säkerhetsfrågor synliga i det dagliga arbetet.

Sammantaget visar forskningen att tekniska säkerhetslösningar i sig inte är tillräckliga utan behöver kompletteras med satsningar på mänsklig och organisatorisk kompetensutveckling. Små och medelstora företag har ofta begränsade resurser och organisatoriska strukturer, vilket gör dem mer sårbara för cyberhot. En viktig men ofta förbisedd målgrupp är den produktionsnära personalen som spelar en viktig roll i det operativa säkerhetsarbetet. Trots att flera studier presenterar olika metoder för att stärka cybersäkerhetsmedvetenheten saknas fortfarande en tydlig samlad bild av vilka metoder som är mest effektiva i just tillverkningsindustrin, särskilt i små och medelstora företag.

1.1 Problemformulering

I detta kapitel presenteras bakgrunden och problemområdet som arbetet utgår från.

1.1.1 Digitalisering och ökad riskbild

Digitalisering och automatisering har under det senaste decenniet förändrat förutsättningarna för tillverkningsindustrin i grunden. Genom införandet av teknologier som IIoT, molnplattformar och integrerade styrsystem har produktionsmiljöer blivit alltmer uppkopplade och datadrivna (Corallo et al., 2022). IIoT-system är särskilt relevanta eftersom de kopplar samman fysiska maskiner med digitala nätverk och därmed öppnar upp produktionsprocesser för externa hot som tidigare inte var möjliga. Till skillnad från traditionella IT-system styr IIoT-system enheter som robotar, sensorer, produktionslinjer och kvalitetsövervakning i realtid. Detta innebär att ett cyberangrepp eller ett mänskligt misstag kan påverka fysiska processer; exempelvis stoppa produktionen, ändra maskinparametrar eller orsaka kvalitetsbrister. Denna utveckling har skapat nya möjligheter för effektivitet, spårbarhet och flexibilitet, men samtidigt har attackytan för cyberhot ökat kraftigt. När IT- och OT-system smälter samman och där produktionskedjan i allt högre grad är beroende av digital infrastruktur blir tillverkningsföretag särskilt sårbara för cyberattacker, inte minst de SMF som ofta har mer begränsade resurser och utveckling inom cybersäkerhetsområdet (Erdogan et al., 2023).

1.1.2 SMF och resursbegränsningar

Till skillnad från större företag som ofta har specialiserad personal som jobbar med säkerhet, incidenthanteringsplaner och kontinuerlig utbildning, visar forskning att många SMF saknar både interna riktlinjer och strategisk kapacitet för cybersäkerhetsarbete (Johansson et al., 2022; Rawindaran et al., 2025). De organisatoriska förutsättningarna inom SMF kännetecknas ofta av små IT-avdelningar, bristfällig tydlighet i säkerhetspolicyer och brist på strukturerad utbildning. Dessa förhållanden gör att inte bara tekniken utan även personalens beteende och kompetensnivå får en avgörande betydelse för den digitala säkerheten.

Cybersäkerhetsmedvetenhet har i detta sammanhang identifierats som en viktig del av organisationen (Akter et al., 2025). Cybersäkerhetsmedvetenhet handlar alltså inte enbart om kunskap om hot och risker, utan även om individens förmåga att agera säkert, följa policyer och tolka säkerhetsrelaterad information korrekt. Khando et al. (2021) visar att majoriteten av cybersäkerhetsincidenter i industrin beror på mänskliga misstag eller omedvetet riskbeteende snarare än tekniska brister. Det innebär att även om tekniska säkerhetslösningar finns på plats, är dessa ofta verkningslösa om personalen saknar förståelse eller följer bristfälliga rutiner. Cybersäkerhetsarbetet blir därmed en fråga om ledarskap, utbildning, kultur och kommunikation. Detta är faktorer som ofta förbises när SMF digitaliserar sin verksamhet.

Detta perspektiv stärks även av Ani et al. (2019), som visar att många industriella cyberattacker lyckas kringgå tekniska säkerhetslösningar genom att utnyttja mänskliga sårbarheter kopplade till kunskap, färdigheter och beteenden. Studien betonar att det därför inte räcker att enbart fokusera på tekniska skyddsåtgärder, utan att organisationer även behöver utvärdera personalens faktiska cybersäkerhetsmedvetenhet. Författarna presenterar en strategi för att bedöma personalens säkerhetskunskap och praktiska säkerhetsfärdigheter i industriella miljöer, med syftet att identifiera de svagaste länkarna i organisationen och rikta säkerhetsinsatser mer träffsäkert. Detta är särskilt relevant för små och medelstora tillverkningsföretag, där begränsade resurser gör det extra viktigt att kunna prioritera utbildning och åtgärder utifrån var sårbarheten är som störst.

1.1.3 Produktionsnära personal och mänskliga faktorer

En grupp som riskerar att vara extra utsatt i detta sammanhang är produktionspersonalen: maskinoperatörer, underhållstekniker, montörer och andra yrkesgrupper som befinner sig nära produktionen. Flera studier pekar på att denna grupp sällan inkluderas i systematiska cybersäkerhetsinsatser trots att de i praktiken hanterar digitala verktyg, interagerar med nätverksuppkopplad utrustning och kan fungera som första ingångspunkter för cyberangrepp (Alqudhaibi et al., 2024a; Erdogan et al., 2023). Brist på regelbunden utbildning kombinerat med stark tidspress och bristfälliga IT-förkunskaper gör att produktionsmedarbetare riskerar att omedvetet bidra till ökad sårbarhet i verksamheten.

1.1.4 Forskningslucka och behov

Chaudhary et al. (2023b) lyfter samtidigt att det idag saknas sammanhållen forskning om hur cybersäkerhetsmedvetenhet bäst kan implementeras, mätas och underhållas inom just små och medelstora tillverkningsföretag. Trots att dessa företag utgör en betydande del av industrisektorn i Europa och globalt brukar forskningen fokusera på stora företag, offentliga aktörer eller generella IT-miljöer. Det finns alltså ett tydligt kunskapsgap i att förstå vilka träningsstrategier, kommunikationsmodeller och tekniska verktyg som lämpar sig bäst för att stärka cybersäkerhetsmedvetenheten hos produktionsnära personal i små och medelstora tillverkningsföretag.

Flera metoder har föreslagits, exempelvis ”spelbaserat” lärande (s.k. serious gaming), simulerade övningar (Schuh et al., 2020), analys av säkerhetspolicies (Wong et al., 2022) och branschspecifika ramverk (Alqudhaibi et al., 2024b). Men det råder fortfarande osäkerhet kring hur effektiva dessa metoder är i praktiken särskilt för målgrupper med låg IT-kompetens och begränsad tillgång till utbildningsresurser. Även faktorer som företagskultur, stöd från ledning och hur utbildningsinsatserna kopplas till företagets affärsmål är avgörande. (Mmango & Gundu, 2023).

Vidare spelar kommunikationens utformning en avgörande roll. Studier visar att hur säkerhetsinformation presenteras exempelvis beroende på om budskapet är känslomässigt formulerat eller fokuserar på vilka konsekvenser ett visst beteende kan få påverkan på hur väl det förstås och följs av personalen (Button et al., 2024). Detta ställer krav på anpassad kommunikation som tar hänsyn till utbildningsnivå, språkbruk, arbetssituation samt även kulturella faktorer. Även detta område är

bristfälligt utforskat i relation till SMF där förutsättningarna kan variera stort mellan olika typer av verksamheter. Utifrån detta blir det uppenbart att cybersäkerhetsmedvetenhet inte kan ses som ett individuellt ansvar utan som en ett ansvar för hela organisationen.

Akter et al. (2025) menar att cybersäkerhetsmedvetenhet kan ses som en kombination av tre saker: hur personalen tänker och agerar kring säkerhet, hur ledningen prioriterar säkerhetsfrågor och hur väl infrastrukturen stödjer ett säkert arbetssätt. Om något av dessa tre saknas riskerar insatserna att misslyckas.

Trots den teoretiska modell som beskrivs av Akter et al. (2025) saknas det fortfarande praktisk kunskap om hur dessa dimensioner integreras i mindre industriföretag, vilket kan göra det svårt att skapa hållbara och effektiva strategier.

Sammantaget finns ett tydligt behov av att kartlägga, analysera och syntetisera befintlig forskning om hur cybersäkerhetsmedvetenhet konkret kan stärkas inom SMF:s produktionsmiljöer. Genom att fokusera på just produktionspersonalen, en grupp som ofta hamnar i bakgrunden i cybersäkerhetsdiskussioner, kan detta arbete bidra till att minska risker, stärka affärsprestanda och förbättra hela leverantörskedjans motståndskraft mot cyberhot (Oroni & Xianping, 2023; Wong et al., 2022)

Med anledning av ovanstående finns ett tydligt behov av att sammanställa och analysera aktuell forskning kring cybersäkerhetsmedvetenhet i tillverkningsindustrins SMF. Studien bygger på detta behov och syftar till att skapa en kunskapsgrund för hur medvetenhet, utbildning och beteendeförändring effektivt kan stärkas i praktiken.

1.2 Syfte

Syftet med denna studie är att, utgående från befintlig forskning inom cybersäkerhetshantering av produktionsnära personal i små och medelstora tillverkningsföretag, analysera vilka faktorer och aktiviteter som kan bidra till att öka personalens cybersäkerhetsmedvetenhet. Studien fokuserar på hur cybersäkerhetsmedvetenhet hos produktionsnära personal beskrivs i tidigare forskning samt vilka organisatoriska, utbildningsrelaterade och praktiska insatser som lyfts fram som betydelsefulla för att stärka denna medvetenhet i små och medelstora tillverkningsföretag.

I linje med detta bygger arbetet vidare på tidigare forskning som visar att företag behöver satsa på utbildning, förändrade arbetssätt, förståelse för säkerhetspolicys och stärkt organisationsförmåga (Akter et al., 2025; Khando et al., 2021; Wong et al., 2022). Särskilt relevant är den samlade bilden av att personalens kunskap, attityder och beteenden är avgörande faktorer för organisationens säkerhet (Alqudhaibi et al., 2024b; Ponsard & Grandclaudon, 2020).

1.3 Frågeställningar

Forskningsfrågorna utgår från problemformuleringen och studiens syfte.

Forskningsfråga 1:

Hur beskrivs nivån av cybersäkerhetsmedvetenhet hos produktionsnära personal i små och medelstora tillverkningsföretag i tidigare forskning?

Forskningsfråga 2:

Vilka metoder, modeller eller utbildningsstrategier lyfts i tidigare forskning som effektiva för att höja cybersäkerhetsmedvetenhet hos produktionsnära personal i tillverkningsindustrins SMF?

1.4 Avgränsningar

Studien avgränsas till cybersäkerhetsmedvetenhet hos produktionsnära personal i små och medelstora tillverkningsföretag. Studien fokuserar därmed inte på samtliga anställda i organisationen, utan på personal som arbetar nära produktion, produktionssystem och industriella miljöer där människa och teknik samverkar. Arbetet avgränsas även till befintlig forskning och bygger därför inte på egen empirisk datainsamling, exempelvis intervjuer, enkäter eller observationer. Studien undersöker heller inte specifika tekniska säkerhetslösningar, såsom brandväggar, intrångsdetektering eller nätverkssegmentering, annat än när dessa berörs i relation till personalens medvetenhet, beteenden eller utbildningsbehov. Vidare fokuserar studien på faktorer och aktiviteter som kan bidra till att stärka cybersäkerhetsmedvetenhet, exempelvis utbildning, organisatoriska arbetssätt, kommunikation och säkerhetskultur. Studien gör därför inte någon praktisk utvärdering av enskilda utbildningsprogram eller modeller i en specifik organisation.

1.5 Disposition

Rapporten är indelad i sju kapitel. Kapitel 1 introducerar studiens problemområde och presenterar problemformulering, syfte, forskningsfrågor, avgränsningar och disposition. I kapitlet behandlas även digitaliseringens påverkan på tillverkningsindustrin, små och medelstora företags resursbegränsningar, produktionsnära personals roll samt den forskningslucka som studien utgår från.

Kapitel 2 redogör för studiens metod och genomförande. Här beskrivs scoping review som metod, vilka databaser som använts, vilka sökkriterier och söktermer som tillämpats samt hur urvalet av inkluderade studier genomförts. Kapitlet behandlar även dataanalys, trovärdighet, överväganden och användning av AI.

Kapitel 3 presenterar tidigare forskning som är relevant för studiens område. Kapitlet ger en forskningsmässig bakgrund till cybersäkerhetsmedvetenhet, små och medelstora tillverkningsföretag samt produktionsnära personal.

Kapitel 4 redovisar studiens resultat. Resultatet presenteras utifrån identifierade teman: nivån av cybersäkerhetsmedvetenhet hos produktionsnära personal, organisatoriska faktorer som påverkar cybersäkerhetsmedvetenhet, metoder och strategier för att stärka cybersäkerhetsmedvetenhet samt utmaningar och begränsningar vid implementering. Kapitlet avslutas med en sammanfattning av resultatet.

Kapitel 5 innehåller studiens diskussion. Här diskuteras resultatet i relation till studiens forskningsfrågor och tidigare forskning. Kapitlet innehåller även en metoddiskussion där studiens genomförande, styrkor och begränsningar diskuteras.

Kapitel 6 presenterar studiens slutsatser och rekommendationer. Här sammanfattas studiens huvudsakliga resultat och dess praktiska och vetenskapliga implikationer. Kapitlet avslutas med förslag till vidare forskning.

Kapitel 7 innehåller de referenser som använts i studien.

2 Metod och genomförande

Detta kapitel beskriver i detalj hur studien har genomförts, från de första metodvalen till hur materialet analyseras och hur studiens trovärdighet har säkerställts. Målet är att på ett tydligt och strukturerat sätt visa hur arbetet är uppbyggt och varför valen var rimliga i relation till studiens syfte. Eftersom studien handlar om cybersäkerhetsmedvetenhet i små och medelstora tillverkningsföretag, där både teknik, organisation och mänskliga beteenden samverkar, har metodvalen anpassats efter denna komplexa verklighet. Det innebär att metoden inkluderade tekniska aspekter och hur människor arbetar, tänker och agerar i produktionsmiljöer. Flera forskare inom cybersäkerhetsområdet framhåller att säkerhetsproblem sällan enbart kan förstås genom tekniska analyser, utan kräver ett bredare perspektiv där organisatoriska och mänskliga faktorer inkluderas (Akter et al., 2025; Khando et al., 2021; Rawindaran et al., 2025). Liknande resonemang förs även av Mmango & Gundu (2023), som visar att motståndskraft mot cyberattacker i små och medelstora företag utvecklas genom en kombination av tekniska skydd, organisatoriskt ledarskap och medvetenhet hos anställda. Även Akter et al. (2025) beskriver cybersäkerhetsmedvetenhet som en som en del av organisationens arbetssätt, där faktorer som kunskap, utbildning, ledningsstöd och teknisk infrastruktur samverkar.

Utgångspunkten för metoden är att studien ska ge en tydlig och övergripande bild av hur forskningen ser ut kring cybersäkerhetsmedvetenhet hos personal som arbetar nära produktionen i små och medelstora tillverkningsföretag. Tidigare forskning visar att ämnet är utspritt över flera olika områden som till exempel informationssäkerhet, industriell IT, organisationsstudier och beteendeforskning. Chaudhary et al. (2023b) menar att forskningen ofta är splittrad och att SMF inte får tillräckligt stort utrymme eller behandlas ytligt. Liknande slutsatser presenteras även av Panko et al. (2025) som i en litteraturbaserad analys visar att forskning om cybersäkerhet i små och medelstora företag är splittrad och spridd över flera forskningsfält. Även Cremer et al. (2022) visar att cybersäkerhetsrelaterad forskning ofta lider av brist på samlade data och struktur, vilket gör det svårare att skapa en tydlig överblick över forskningsläget. Därför är det motiverat att göra en studie som samlar ihop, strukturerar och skapar en överblick över detta område. Forskning om digitalisering i industrin visar också att cybersäkerhetsfrågor i ökande grad kopplas till utvecklingen av Industry 4.0 och Industrial Internet of Things (IIoT), där uppkopplade system och digitalt styrda

processer skapar nya typer av säkerhetsrisker och organisatoriska utmaningar (Alqudhaibi et al., 2024a; Amirova et al., 2025).

Mot denna bakgrund valdes en s.k. scoping review som metod. Det innebär att studien inte försöker bevisa en specifik hypotes, utan i stället kartlägger vad som redan finns publicerat inom området. Syftet är att identifiera återkommande mönster, begrepp, arbetssätt och kunskapsluckor. En scoping review passar således bra när forskningen är bred, splittrad och inte fullt sammanhållen, vilket flera forskare inom cybersäkerhetsmedvetenhet har påpekat, bland annat Akter et al. (2025), Chaudhary et al. (2023b) och Khando et al. (2021). Flera studier inom cybersäkerhetsområdet har dessutom använt liknande metoder för att kartlägga forskningsfält och identifiera viktiga teman, exempelvis Panko et al. (2025) som analyserar forskningsutvecklingen inom cybersäkerhet i SMF samt Rawindaran et al. (2025) som identifierar viktiga faktorer för motståndskraft mot cyberattacker i mindre organisationer. Även Mmango & Gundu (2023) använder en liknande metod, där litteraturanalys kombineras med praktiska insikter för att identifiera faktorer som påverkar motståndskraften för cybersäkerhet i små och medelstora företag. Genom att använda en scoping review blir det möjligt att skapa en bred översikt över forskningsfältet och samtidigt identifiera mönster, återkommande teman och potentiella kunskapsluckor.

I den här studien är ”data” alltså de vetenskapliga artiklar som identifieras i sökningen, väljs ut i urvalet och sedan analyseras tematiskt. Ingen egen empiri samlas in från företag utan bygger analysen på publicerad forskning.

Studien bygger främst på kvalitativa metoder. Det innebär att innehållet i tidigare forskning tolkas och analyseras snarare än att mäta eller räkna nya data. Samtidigt ingår det även att läsa studier som bygger på kvantitativa undersökningar såsom enkäter och statistiska analyser. Dessa används dock inte för att göra egna beräkningar utan för att bidra till förståelsen av hur cybersäkerhetsmedvetenhet mäts och beskrivs i olika sammanhang. Detta är viktigt eftersom flera forskare till exempel Akter et al. (2025) och Oroni & Xianping (2023), visar att cybersäkerhetsmedvetenhet är något som inte enbart kan mätas i siffror utan även måste förstås som en del av hur organisationen fungerar, vilket påverkas av kultur, ledning, struktur och arbetsmiljö. Även García Arellano et al. (2024) betonar att cybersäkerhetsmedvetenhet påverkas av interna förhållanden, såsom utbildning, säkerhetskultur och rutiner, vilket gör att kvalitativa tolkningar ofta behövs för att förstå hur säkerhetsarbete fungerar i

praktiken. Ibrahim et al. (2025) har föreslagit metoder för att mäta cybersäkerhetsmedvetenhet och säkerhetsrutiner i små och medelstora företag med hjälp av olika mått och modeller, vilket visar att både kvalitativa och kvantitativa perspektiv behövs för att analysera cybersäkerhetsmedvetenhet på ett mer heltäckande sätt.

Forskningen genomförs steg för steg där varje del av processen bygger vidare på den föregående. Först preciserades forskningsproblemet och studiens syfte. Därefter utformades en plan för hur litteraturen skulle sökas fram. Efter detta följde ett urval där relevanta studier valdes ut och slutligen genomförs analys av materialet. Detta arbetssätt gör att processen blir systematisk och inte bygger på slumpmässiga val. Enligt Chaudhary et al. (2023b) och Rawindaran et al. (2025) är en strukturerad litteraturprocess särskilt viktig i studier som behandlar komplexa forskningsområden där många olika discipliner möts. Panko et al. (2025) beskriver också att liknande systematiska arbetssätt har använts i flera tidigare studier inom cybersäkerhetsforskning, där forskare analyserar stora mängder publikationer för att identifiera betydande forskningsmönster och teman.

Genom att arbeta systematiskt med litteratursökning, urval och analys kan studien säkerställa att forskningen som inkluderas är relevant för studiens syfte och forskningsfrågor.

I denna studie genomförs litteratursökningen i flera steg, där vetenskapliga databaser används för att identifiera relevanta artiklar. Databaser såsom Primo och Scopus används eftersom de innehåller ett stort antal peer-review-granskade vetenskapliga publikationer inom områden som informationssäkerhet och industriell IT. Enligt Panko et al. (2025) och Chaudhary et al. (2023b) används liknande databaser ofta i tidigare studier inom cybersäkerhetsområdet, eftersom de ger tillgång till internationellt publicerad forskning från flera områden. Genom att använda etablerade databaser ökar sannolikheten att relevanta och vetenskapligt granskade studier inkluderas i analysen. Amirova et al. (2025) betonar dessutom att bredare forskningsdatabaser är särskilt viktiga i forskning om cybersäkerhet i industriella system, eftersom ämnet omfattar både tekniska och organisatoriska perspektiv.

När litteraturen identifierats genomförs ett urval där studier bedöms utifrån deras relevans för studiens forskningsfrågor. Urvalet baseras på studier som behandlar

cybersäkerhetsmedvetenhet, små och medelstora företag eller tillverkningsindustri samt deras vetenskapliga kvalitet. Enligt Akter et al. (2025) och Rawindaran et al. (2025) används denna typ av urvalsprocess ofta i litteraturstudier för att säkerställa att endast relevanta studier inkluderas i analysen. Genom att använda tydliga urvalskriterier minskar risken för subjektiva bedömningar och studiens transparens ökar. García Arellano et al. (2024) beskriver att liknande urvalsprocesser även används i studier som analyserar cybersäkerhetskultur och cybersäkerhetsmedvetenhet i organisationer.

Efter urvalsprocessen analyseras materialet genom en tematisk analys där återkommande teman och mönster identifieras i forskningen. Den tematiska analysen syftar till att strukturera forskningsfältet genom att identifiera viktiga begrepp, metoder och forskningsresultat som återkommer i flera studier. Liknande analysmetoder används ofta i litteraturstudier inom cybersäkerhetsområdet för att skapa en mer sammanhållen bild av forskningsfältet (Chaudhary et al., 2023b; Panko et al., 2025). Tematisk analys används även i forskning om motståndskraft mot cyberattacker i små och medelstora företag för att identifiera återkommande faktorer som påverkar organisationers säkerhetsarbete (Mmango & Gundu, 2023). Genom att analysera studiernas resultat och jämföra deras slutsatser kan studien bidra till en mer samlad förståelse av hur cybersäkerhetsmedvetenhet utvecklas och påverkar organisationer.

Det är också viktigt att säkerställa studiens trovärdighet. Detta görs bland annat genom att använda vetenskapligt granskade artiklar, tydliga urvalskriterier och en systematisk analysprocess. Genom att basera studien på redan etablerad forskning och tydligt redovisa hur materialet samlats in och analyserats ökar studiens transparens och tillförlitlighet. Inom cybersäkerhetsområdet framhåller exempelvis Khando et al. (2021), Chaudhary et al. (2023b) och Rawindaran et al. (2025) vikten av transparens och tydliga metoder i litteraturstudier, eftersom forskningsfältet ofta är komplext och omfattar flera områden. Även García Arellano et al. (2024) samt Mmango & Gundu (2023) betonar att i studier om cybersäkerhetskultur och motståndskraft mot cyberattacker i organisationer, vikten av tydlig metod och öppenhet i forskningsprocessen för att säkerställa trovärdiga resultat.

Ett ytterligare skäl till att studera området utifrån ett brett och systematiskt sätt är att cybersäkerhetsmedvetenhet i små och medelstora tillverkningsföretag inte enbart har

betydelse internt i organisationen, utan även i relation till leverantörskedjan och företagets resultat. Stentoft et al. (2025) visar att cybersäkerhetsmedvetenhet i sig inte hade någon betydande total effekt på företagets ekonomiska resultat, men att det fanns en positiv indirekt effekt genom cybersäkerhetsrelaterad riskhantering i leverantörskedjan. Resultaten tyder därmed på att cybersäkerhetsmedvetenhet behöver förstås tillsammans med de organisatoriska arbetssätt och riskhanteringsprocesser som omsätter medvetenheten i praktiken. Detta stärker valet av en scoping review, eftersom forskningsfältet omfattar flera aspekter som hänger ihop såsom medvetenhet, organisatoriska processer, risker i leverantörskedjan samt verksamhetsmässiga konsekvenser.

2.1 Scoping review

En scoping review är en metod för att sammanställa forskning och används för att kartlägga hur mycket forskning som finns och vilken typ av forskning som gjorts inom ett visst område. Metoden syftar till att identifiera vilka typer av studier som finns, vilka viktiga begrepp som används samt vilka kunskapsluckor som finns i litteraturen. Till skillnad från mer ingående litteraturstudier som försöker besvara en specifik forskningsfråga genom att väga samman resultat från tidigare studier, fokuserar en scoping review i stället på att skapa en bred översikt över forskningsfältet och dess utveckling (Hadie, 2024; Rubinstein & Parrott, 2021). Denna metod används ofta när ett forskningsområde är komplext eller splittrat och där tidigare forskning är spridd över flera områden.

Enligt Hadie (2024) har scoping reviews blivit allt vanligare inom forskning eftersom metoden möjliggör en omfattande genomgång av befintlig litteratur, samtidigt som den kan tydliggöra begrepp, identifiera forskningsluckor och analysera vilka metoder som tidigare studier har använt. Genom att kartlägga forskningen på detta sätt kan en scoping review även fungera som ett första steg inför mer djupgående litteraturstudier, exempelvis systematiska litteraturöversikter. Rubinstein & Parrott (2021) framhåller också att scoping reviews är särskilt användbara när forskare vill få en övergripande bild av ett forskningsområde utan att begränsa sig till en mycket specifik forskningsfråga.

Processen för att genomföra en scoping review kan delas in i flera steg. Först definieras studiens forskningsområde och forskningsfrågor. I detta steg fastställs

syftet med studien och vilka aspekter av forskningsområdet som ska undersökas. Ett tydligt formulerat syfte är viktigt eftersom det styr hur litteratursökningen utformas och vilka studier som senare inkluderas i analysen. Enligt Hadie (2024) är detta en viktig del av metodprocessen eftersom forskningsfrågorna fungerar som en vägledning genom hela studien.

Nästa steg är att identifiera relevant litteratur. Detta sker genom systematiska sökningar i vetenskapliga databaser, där sökord och sökstrategier utvecklas för att hitta studier som är relevanta för forskningsområdet. Sökprocessen genomförs ofta iterativt, vilket innebär att sökorden kan justeras och utvecklas under arbetets gång i takt med att forskaren får en bättre förståelse för hur forskningsfältet är uppbyggt. Rubinstein & Parrott (2021) beskriver att denna typ av sökstrategi gör det möjligt att identifiera ett brett urval av studier och därmed skapa en mer heltäckande bild av den tillgängliga forskningen.

Efter att relevanta studier har identifierats genomförs ett urval där studier granskas utifrån deras relevans för forskningsfrågorna. I detta steg analyseras exempelvis studiernas ämnesområde, metod och kontext för att avgöra om de bör inkluderas i analysen. En scoping review handlar i detta skede om att inkludera studier som tillsammans kan bidra till att visa bredden och variationen i forskningsområdet, i stället för att bara välja vissa typer av studier (Cuellar et al., 2015).

När urvalet av studier är genomfört analyseras materialet genom att återkommande teman, begrepp och forskningsresultat identifieras. Analysen syftar till att beskriva hur forskningsområdet ser ut, vilka typer av studier som dominerar samt vilka frågor som fortfarande saknar tillräcklig forskning. Cuellar et al. (2015) beskriver att en scoping review därför kan användas för att kartlägga omfattningen, variationen och karaktären av forskning inom ett område samt för att identifiera områden där ytterligare studier behövs.

Slutligen sammanställs resultaten i en rapport där forskningsfältets struktur och identifierade teman presenteras. Hadie (2024) samt Rubinstein & Parrott (2021) beskriver att resultatet av en scoping review därmed blir en översikt över befintlig forskning som kan bidra till en bättre förståelse av forskningsområdet och samtidigt ge vägledning för framtida forskning. På detta sätt fungerar scoping reviews som ett

viktigt verktyg för att skapa struktur och överblick i forskningsområden där litteraturen är omfattande och spridd över flera olika forskningsfält.

2.2 Databaser

Identifieringen av relevanta vetenskapliga studier genomförs genom sökningar i forskningsdatabaser. Databaser är viktiga i en scoping review. eftersom de innehåller ett stort antal vetenskapligt granskade publikationer och ger tillgång till forskning från flera olika områden. Eftersom en scoping review syftar till att kartlägga omfattningen av forskning inom ett område, krävs en bred och systematisk sökstrategi där flera databaser används för att identifiera relevanta studier (Hadie, 2024; Rubinstein & Parrott, 2021).

I denna studie används databaserna Scopus och Primo som huvudsakliga källor för litteratursökningen. Scopus är en av de största vetenskapliga databaserna och innehåller ett omfattande urval av peer-review-granskade artiklar inom bland annat informationssäkerhet, industriell IT, organisationsforskning och teknik. Databasen används därför ofta i forskningsstudier där syftet är att skapa en bred översikt över ett forskningsområde.

Primo används som kompletterande söktjänst eftersom den ger tillgång till universitetets bibliotekssystem och därmed till ytterligare vetenskapliga publikationer från flera olika databaser samtidigt. Att söka i flera databaser gör det lättare att hitta många relevanta studier inom området.

Utöver dessa databaser används även Google Scholar och IEEE Xplore för att bredda sökningen ytterligare. Google Scholar möjliggör identifiering av vetenskapliga publikationer som ibland inte återfinns i traditionella databaser, medan IEEE Xplore innehåller ett stort antal tekniskt inriktade publikationer inom områden som cybersäkerhet, industriella system och digital infrastruktur.

Valet av dessa databaser motiveras dels av deras breda täckning av internationell forskning, dels av deras tillgänglighet genom högskolans bibliotekstjänster. Genom att använda etablerade databaser ökar sannolikheten att studien inkluderar relevant och vetenskapligt granskad forskning. Detta bidrar till ökad transparens och tillförlitlighet.

Eftersom olika databaser använder olika sökfunktioner, kan sökningar inte alltid genomföras identiskt i varje databas. I praktiken innebär detta att söktermer appliceras

på olika delar av artiklarna, beroende på databasens funktionalitet. Vanliga fält som används vid litteratursökningar är titel, abstrakt och nyckelord, eftersom dessa delar av artiklar vanligtvis innehåller de mest viktiga begreppen kopplade till studiens ämne. Genom att kombinera sökningar i dessa fält kan relevanta studier identifieras, samtidigt som antalet ej relevanta träffar minimeras.

2.3 Sökkriterier

För att avgränsa litteraturen och säkerställa att endast relevanta studier inkluderas i analysen används ett antal sök- och urvalskriterier. Sådana kriterier är viktiga i en scoping review, eftersom de hjälper forskaren att systematiskt filtrera bort studier som inte är relevanta för forskningsområdet, samtidigt som de skapar en tydlig struktur i urvalsprocessen (Hadie, 2024).

Urvalsprocessen genomförs i flera steg. Först görs en inledande granskning av studiernas titlar och abstrakt, för att identifiera artiklar som verkar relevanta för forskningsområdet. Detta steg syftar till att skapa en första översikt över den tillgängliga litteraturen och att samla in ett större antal potentiellt relevanta studier. Därefter granskas studierna mer ingående för att avgöra om de uppfyller de kriterier som fastställts för studien.

I denna studie används både inkluderingskriterier och exkluderingskriterier. Inkluderingskriterierna används för att säkerställa att de studier som inkluderas är relevanta för forskningsområdet och håller tillräcklig vetenskaplig kvalitet. Exempel på inkluderingskriterier är att studien ska behandla cybersäkerhet, informationssäkerhetsmedvetenhet eller relaterade säkerhetsaspekter i organisationer. Studierna ska också vara publicerade i vetenskapliga tidskrifter eller konferenser för att säkerställa att materialet är vetenskapligt granskat.

Vidare inkluderas studier som är skrivna på engelska, eftersom majoriteten av internationell forskning inom cybersäkerhet publiceras på detta språk. Detta gör det möjligt att inkludera ett brett urval av internationella studier samtidigt som litteraturen förblir hanterbar inom ramen för studien.

Exkluderingskriterier används för att filtrera bort studier som inte är relevanta eller som inte uppfyller studiens kvalitetskrav. Exempel på sådana kriterier är studier som saknar koppling till cybersäkerhetsmedvetenhet eller som enbart behandlar tekniska säkerhetslösningar, utan att inkludera organisatoriska eller mänskliga aspekter.

Studier som identifieras flera gånger i olika databaser tas också bort från urvalet för att undvika dubbletter i analysen.

Genom att använda tydliga sök- och urvalskriterier blir litteraturprocessen mer systematisk och reproducerbar. Detta är särskilt viktigt i en scoping review, eftersom metoden syftar till att kartlägga ett forskningsfält på ett strukturerat sätt och därmed skapa en tydlig översikt över den befintliga forskningen (Rubinstein & Parrott, 2021). Samtidigt gör kriterierna det möjligt att säkerställa att de studier som inkluderas i analysen är relevanta för studiens syfte och forskningsfrågor.

2.4 Söktermer

Söktermer är en viktig del av studien, eftersom de direkt påverkar vilken litteratur som inkluderas i analysen. Valet av söktermer avgör vilka studier som identifieras i databassökningarna och har därför stor betydelse för studiens resultat. För att studien ska kunna uppnå sitt syfte att kartlägga forskning om cybersäkerhetsmedvetenhet i små och medelstora tillverkningsföretag, behöver sökorden vara tillräckligt inkluderande för att fånga relevanta studier, samtidigt som de bör begränsa mängden irrelevanta resultat till en hanterbar nivå.

Vid databassökningar kan resultatet variera beroende på var sökorden appliceras, exempelvis i artikelns titel, abstrakt, nyckelord eller i hela texten. Dessutom kan användandet av s.k. boolean operators påverka resultatet av sökningen. Genom att kombinera söktermer med operators som AND, OR och NOT kan sökningen anpassas för att både bredda och avgränsa resultaten. Samtidigt finns en risk att alltför strikta sökningar exkluderar relevanta studier.

Under arbetets gång genomfördes flera test av olika kombinationer av sökord. Inledningsvis prövades mer specifika söktermer kopplade till cybersäkerhet och industriella miljöer, exempelvis industrial cybersecurity, cybersecurity training, SME security och manufacturing security. Dessa mer avgränsade sökningar resulterade dock ofta i ett relativt begränsat antal träffar och riskerade att exkludera studier som behandlade ämnet ur ett bredare organisatoriskt eller beteendemässigt perspektiv.

För att säkerställa att relevanta studier inte missades utökades därför sökningen med mer övergripande begrepp kopplade till cybersäkerhetsmedvetenhet och organisatoriska säkerhetsaspekter. Särskilt fokus lades på begrepp som ofta förekommer i forskning om cybersäkerhet i organisationer och industriella miljöer.

Söktermerna togs fram utifrån studiens syfte och identifierades löpande under arbetets gång baserat på vad som bedömdes vara relevant. De söktermer som slutligen användes i studien inkluderar bland annat:

- “Cybersecurity awareness”
- “Cyber resilience”
- “SME” OR “small and medium enterprises”
- “Manufacturing” OR “industrial sectors”
- “Industrial workers” OR “factory workers”
- “Human factors”
- “Industrial Internet of Things” OR “IIoT”
- “Organizational security”

Söktermerna kombinerades med hjälp av boolean operators (AND, OR) för att skapa strukturerade söksträngar. Exempelvis användes följande kombinationer:

- “cybersecurity awareness” AND “manufacturing” AND “SME”
- (“cyber resilience” OR “organizational security”) AND “industrial internet of things” AND “manufacturing”
- (“human factors” AND “cybersecurity awareness”) AND (“industrial workers” OR “factory workers”)

Genom att kombinera dessa begrepp kunde sökningar genomföras som inkluderar både tekniska, organisatoriska och mänskliga aspekter av cybersäkerhet. Kombinationen av begrepp gör det möjligt att identifiera forskning som behandlar cybersäkerhetsmedvetenhet i industriella miljöer, samtidigt som studier som saknar koppling till organisationer eller arbetsmiljöer i högre grad exkluderas.

Söktermerna bidrar därmed till att skapa en bred grund för insamlingen av litteratur i studien. En bredare sökstrategi innebär att fler potentiellt relevanta artiklar identifieras, vilket minskar risken att viktiga studier missas. Samtidigt leder detta till att ett större antal artiklar behöver granskas och filtreras genom de inkluderings- och exkluderingskriterier som används i studien. Detta ses dock som en nödvändig del av processen för att säkerställa att studien ger en så heltäckande bild som möjligt av forskningen inom området cybersäkerhetsmedvetenhet i små och medelstora tillverkningsföretag.

Databassökningarna kompletterades med manuell sökning genom att följa relevanta referenser i redan identifierade studier. På så sätt kunde artiklar fångas in som annars riskerar att missas av enbart databassökningar.

2.5 Inkluderade studier

Urvalsprocessen resulterade i totalt 21 inkluderade studier som ligger till grund för den tematiska analysen. Studierna identifierades främst via databassökningar och kompletterades med manuell granskning av referenslistan. Tabell 2 visar vilka studier som ingick i den tematiska analysen.

Tabell 1: Inkluderade studier i analysen

Akter et al.	2025	Giriraj et al.	2022
Alzahrani & Seth	2021	Johansson et al.	2022
Amirova et al.	2025	Khando et al.	2021
Ani et al.	2019	Mani et al.	2017
Arellano et al.	2024	Mmango & Gundu	2023
Arroyabe et al.	2024	Oroni & Xianping	2023
Brunken et al.	2025	Panko et al.	2025
Button et al.	2024	Rawindaran et al.	2025
Chidukwani et al.	2024	Schuh et al.	2020
Corallo et al.	2022	Wong et al.	2022
Erdogan et al.	2023		

2.6 Dataanalys

När allt material väl samlats in, studerats och valts ut, genomfördes analysen med hjälp av så kallad tematisk analys. Det innebär att de inkluderade studier analyseras noggrant utifrån vilka huvudteman som återkommer i materialet (Braun & Clarke, 2006). Exempel på teman som förväntas identifieras är utbildningsmetoder, organisationens roll, ledarskap, mänskligt beteende, säkerhetskultur samt tekniska förutsättningar. Analysen görs både utifrån befintlig teori och tidigare forskning, samt

även utifrån mönster som växer fram under arbetets gång. Detta gör det möjligt att genomföra en analys som är både flexibel och tydligt anpassad efter hur komplext materialet är.

Arbetet har hämtat inspiration från tidigare forskning som behandlar cybersäkerhetsmedvetenhet som en helhetsfråga, snarare än enbart en utbildningsfråga. Studier som Akter et al. (2025), Khando et al. (2021) och Mmango & Gundu (2023) visar att säkerhetsmedvetenhet i SMF är nära kopplat till organisationens kultur, ledarskap och sätt att sprida kunskap. Därför har analysen inte begränsats till genomförda utbildningar och kurser, utan även tagit hänsyn till hur företag arbetar strategiskt med cybersäkerhet, samt hur ledningen påverkar medarbetarnas beteenden.

Det teoretiska ramverket i studien bygger på tidigare forskning som beskriver cybersäkerhetsmedvetenhet som ett samspel mellan mänskliga, organisatoriska och tekniska faktorer. Perspektivet utgår bland annat från Akter et al. (2025), där cybersäkerhetsmedvetenhet förstås som en organisatorisk förmåga som påverkas av exempelvis ledarskap, organisationskultur och kunskapsspridning. Ramverket har använts som ett analytiskt stöd vid tolkningen och kategoriseringen av studiens teman och resultat.

För att säkerställa studiens trovärdighet har hela arbetsprocessen dokumenterats noggrant. Sökord, databaser, urvalskriterier och analysmetoder redovisas tydligt för att andra ska kunna följa hur studien gått till. Genom att förankra arbetet i tidigare etablerad forskning, som Chaudhary et al. (2023b), Corallo et al. (2022), Johansson et al. (2022) och Khando et al. (2021), stärks dessutom studiens vetenskapliga grund.

Särskild hänsyn tas också till studiens sammanhang. Eftersom huvudfokus ligger på tillverkningsindustrin och produktionsnära personal, är analysen hela tiden kopplad till hur verkligheten ser ut i fabriker och produktionsmiljöer där digitalisering, IIoT, automation och högt tempo präglar vardagen. Detta är något som lyfts fram i studier av bland annat Alqudhaibi et al. (2024a), Corallo et al. (2022) och Johansson et al. (2022). Resultaten som presenteras i detta arbete är därför inte enbart teoretiska, utan relateras kontinuerligt till hur cybersäkerhetsmedvetenhet fungerar i vardagen och i praktiken inom industrin.

Under analysprocessen jämfördes resultaten från olika studier, detta för att identifiera likheter och skillnader i hur cybersäkerhetsmedvetenhet beskrivs och analyseras. Genom att studera flera studier samtidigt, kan gemensamma mönster identifieras, men även olika perspektiv och tillvägagångssätt som forskare använder när de studerar cybersäkerhet i organisationer.

Analysen syftar också till att tydliggöra vilka områden som är väl undersökta inom forskningen, och vilka områden där det fortfarande finns begränsad kunskap. Genom att strukturera materialet i återkommande teman, kan forskningen organiseras på ett mer överskådligt sätt, vilket gör det möjligt att skapa en mer tydlig bild av forskningsfältet.

Ett ytterligare syfte med analysen är att koppla forskningsresultaten till den praktiska verkligheten i industriella organisationer. Många studier behandlar cybersäkerhet på en övergripande nivå, men i denna studie analyseras resultaten särskilt utifrån hur de kan relateras till produktionsmiljöer, där personal arbetar nära tekniska system. På så sätt blir analysen inte enbart teoretisk, utan även relevant för hur cybersäkerhetsmedvetenhet fungerar i praktiken i tillverkningsföretag.

För att strukturera analysprocessen ytterligare, kan den tematiska analysen beskrivas i ett antal faser. Enligt Nowell et al. (2017) kan tematisk analys delas upp i sex steg som tillsammans bidrar till en systematisk och transparent analysprocess.

Fas 1: Bekanta sig med data: Det första steget innebär att forskaren bekantar sig med materialet genom att läsa igenom de insamlade studierna flera gånger. Detta gör det möjligt att skapa en övergripande förståelse för innehållet i litteraturen och identifiera viktiga begrepp, perspektiv och forskningsresultat som återkommer i materialet.

Fas 2: Skapa koder: I den andra fasen identifieras relevanta delar av materialet och märks med korta beskrivande koder. Kodningen genomförs genom att textavsnitt i studierna som är relevanta för forskningsfrågorna markeras och kategoriseras. Koderna fungerar sedan som byggstenar för den fortsatta analysen.

Fas 3: Identifiering av teman: Efter att de initiala koderna har skapats, analyseras dessa för att identifiera möjliga teman. Teman bildas genom att relaterade koder grupperas tillsammans i mer övergripande kategorier som representerar återkommande mönster i materialet.

Fas 4: Granskning av identifierade teman: I detta steg granskas alla identifierade teman, för att säkerställa att de representerar materialet på ett meningsfullt sätt. Teman kan i denna fas justeras, slås samman eller delas upp för att bättre spegla innehållet i insamlade data.

Fas 5: Definiering och namngivning av teman: När samtliga teman har fastställts, analyseras varje tema mer ingående för att tydliggöra dess innebörd och betydelse i relation till studiens syfte. Alla teman ges därefter tydliga namn som beskriver deras innehåll och gör dem lättare att förstå för läsaren.

Fas 6: Producering av rapport: Den sista fasen innebär att resultaten av analysen sammanställs och presenteras i studiens resultat- och diskussionskapitel. Samtliga identifierade teman används då som en struktur för att beskriva hur cybersäkerhetsmedvetenhet behandlas i forskningen, samt vilka faktorer som påverkar organisationers säkerhetsarbete.

2.7 Trovärdighet

I forskningsstudier är trovärdighet en mycket viktig aspekt, eftersom den avgör hur tillförlitliga studiens resultat kan anses vara. Enligt Wohlin et al. (2012) påverkas trovärdigheten av flera faktorer, bland annat val av metod, hur studien genomförs samt i vilken utsträckning forskarnas egna tolkningar eller tidigare kunskap kan påverka resultatet. Författarna betonar även att frågor som rör validitet bör beaktas redan i planeringsstadiet av studien och inte enbart under datainsamling eller analys.

När litteraturstudier genomförs är det särskilt viktigt att säkerställa att sökprocessen och urvalet av artiklar sker på ett systematiskt sätt. Kitchenham (2004) framhåller att kvaliteten i en litteraturstudie i stor utsträckning beror på hur väl sökstrategin är planerad och dokumenterad. Att arbeta med ett tydligt protokoll för hur artiklar söks, väljs ut och analyseras gör att studiens trovärdighet kan stärkas.

För att analysera trovärdighet i forskning används ofta olika typer av validitetsbegrepp. Wohlin et al. (2012) beskriver fyra viktiga dimensioner som är särskilt relevanta i litteraturstudier: internvaliditet, externvaliditet, begreppsvaliditet och reliabilitet.

Internvaliditet handlar om i vilken grad studiens slutsatser verkligen speglar de relationer som undersöks. I forskningsstudier är det viktigt att säkerställa att

observerade samband inte beror på andra okända faktorer. I denna studie innebär det exempelvis att analysen av cybersäkerhetsmedvetenhet måste ta hänsyn till flera organisatoriska faktorer såsom utbildning, ledarskap och säkerhetskultur.

Externvaliditet avser i vilken utsträckning resultaten kan överföras till andra sammanhang. Eftersom denna studie analyserar forskning om cybersäkerhetsmedvetenhet inom tillverkningsindustrin är det viktigt att studierna som analyseras är relevanta för liknande organisationer.

Begreppsvaliditet handlar om hur väl de metoder och begrepp som används i studien faktiskt mäter det fenomen som ska studeras. I denna studie innebär det att de analyserade artiklarna måste behandla cybersäkerhetsmedvetenhet på ett sätt som är relevant för studiens forskningsfrågor.

Reliabilitet beskriver hur reproducerbara resultaten är. Om en annan forskare skulle genomföra samma studie och följa samma metod bör resultaten i stora drag bli liknande. För att öka reliabiliteten i denna studie dokumenteras därför hela forskningsprocessen, inklusive databaser, söktermer, urvalskriterier och analysmetoder.

Ett ytterligare metodologiskt problem som ofta diskuteras i litteraturstudier är publikationsbias. Kitchenham (2004) framhåller att studier med tydliga eller positiva resultat oftare publiceras än studier som visar mer begränsade eller negativa resultat. Detta kan påverka vilka studier som finns tillgängliga i databaser och därmed även vilka resultat som inkluderas i en litteraturstudie. Flera databaser har använts för att få bredare täckning, men publikationsbias kan fortfarande finnas eftersom studien bygger på publicerad litteratur.

Zhou et al. (2016) beskriver även olika typer av hot mot validiteten i litteraturstudier. Dessa hot kan uppstå i olika delar av forskningsprocessen, exempelvis under planering, datainsamling, analys eller rapportering. I denna studie har flera potentiella risker identifierats och åtgärder har vidtagits för att minska deras påverkan.

En viktig del i arbetet har varit att analysera materialet systematiskt och att använda en tydlig kodningsprocess. Kodningen har genomförts induktivt för att göra det möjligt att identifiera mönster och teman direkt från materialet. Genom att analysera studierna separat och därefter jämföra resultaten kan tolkningar diskuteras och analyseras mer kritiskt.

Valet av söktermer är också en faktor som påverkar studiens validitet. I denna studie har sökningar genomförts med relativt breda söktermer för att säkerställa att så många relevanta studier som möjligt identifieras. Detta innebär att även irrelevanta artiklar kan förekomma i den initiala sökningen, vilket kräver en mer omfattande urvalsprocess. Samtidigt minskar det risken att viktiga studier förbises.

Tabell 1 sammanfattar de viktigaste hoten mot studiens validitet samt de åtgärder som vidtas för att minska dessa risker.

Tabell 2: Hot mot studiens validitet

Hot	Påverkad validitet	Åtgärd	Fas
Otydliga definitioner av söktermer eller urvalskriterier	Internvaliditet, begreppsvaliditet	Tydliga definitioner och beskrivningar i metodkapitlet	Planeringsfas
Relevanta studier missas i sökningen	Internvaliditet, begreppsvaliditet	Användning av etablerade sökmetoder från tidigare forskning	Planeringsfas
För få analyserade studier	Internvaliditet	Snöbollsmetod samt användning av flera databaser och söktermer	Datainsamlingsfas
Subjektiva bedömningar vid urval av studier	Internvaliditet, reliabilitet	Fördefinierade urvalskriterier följs under hela urvalsprocessen	Genomförandefas
Studier med begränsad generaliserbarhet	Externvaliditet	Tydliga exkluderingskriterier	Rapporteringsfas

2.8 Överväganden

För att säkerställa att studien genomförs på ett etiskt korrekt sätt har arbetet utgått från de riktlinjer som presenteras i Vetenskapsrådets publikation. (Vetenskapsrådet, 2024) Dessa riktlinjer betonar bland annat vikten av transparens, noggrann dokumentation samt ett ansvarsfullt förhållningssätt till tidigare forskning.

I praktiken innebär detta att studien redovisar sina metoder, analysprocesser och resultat på ett öppet och transparent sätt. Alla källor som används i studien refereras tydligt för att säkerställa att tidigare forskning erkänns och inte används utan korrekt hänvisning.

Eftersom sökningarna genomfördes i flera databaser med olika sökfunktioner har exakta antal träffar inte redovisats i varje steg. I stället beskrivs urvalsprocessen tydligt med inkluderings och exkluderingskriterier samt hur granskningen gjordes.

Eftersom studien baseras på analys av tidigare publicerad forskning innebär den heller inte någon direkt datainsamling från individer. Däremot behandlar studien frågor som rör cybersäkerhet i organisationer vilket innebär att forskningsresultat ibland kan beröra känsliga aspekter av organisationers säkerhetsarbete. I analysen har därför särskild hänsyn tagits till hur resultat presenteras, detta för att undvika att enskilda organisationer kan identifieras eller framställas på ett sätt som kan uppfattas som negativt.

Studien strävar också efter att ge en rättvis och balanserad bild av forskningsfältet. Detta innebär att olika perspektiv i litteraturen beaktas och att forskningsresultat inte selekteras på ett sätt som skulle kunna snedvrida analysen.

2.9 AI användning

Under vissa delar av skrivprocessen har ChatGPT använts som stöd. Detta främst för att förbättra akademiska formuleringar. Vidare har verktyget använts för att få feedback på arbetets struktur, och även få förslag på förbättringar. Exempel på promptar är:

- Läs igenom stycket och ge förslag på hur språket kan bli mer akademiskt och formellt.
- Kontrollera grammatiken och meningsbyggnaden i detta stycke.

3 Tidigare Forskning

Arroyabe et al. (2024) visar att IT-säkerhetsfrågor har en tydlig koppling till implementeringen av Industry 4.0 i små och medelstora tillverkningsföretag. Studien visar att säkerhetsrelaterade utmaningar inte enbart fungerar som hinder, utan i vissa fall även som drivkrafter för digitalisering av verksamheten. Samtidigt framkommer att graden av digitalisering varierar kraftigt mellan olika företag, från verksamheter som har integrerat avancerade teknologier såsom robotik, molntjänster och smarta enheter till företag som fortfarande befinner sig i ett tidigt skede. Detta belyser det nära sambandet mellan cybersäkerhetsfrågor och digital mognad i tillverkningsindustrins SMF.

Chidukwani et al. (2024) visar att små och medelstora företag ofta hindras i sitt cybersäkerhetsarbete av brist på ekonomiska resurser, låg kännedom om var säkerhetsarbete bör påbörjas samt begränsad kunskap om relevanta ramverk och regelverk. Studien pekar också på brister i bland annat åtkomstkontroll, individuella användarkonton, tydliga riktlinjer och resurser avsatta för säkerhet, vilket ytterligare belyser de praktiska svårigheter som många SMF står inför.

SMF har dessutom särskilda strukturella utmaningar. Erdogan et al. (2023) visar att resurser, tid och kompetens ofta är begränsade vilket leder till låg Cybersecurity Awareness (cybersäkerhetsmedvetenhet) och avsaknad av etablerade processer för att hantera säkerhetsrelaterade incidenter. Detta bekräftas även av Rawindaran et al. (2025), som visar att många SMF saknar både grundläggande säkerhetspolicyer och tillräcklig riskmedvetenhet bland personalen. Flera studier pekar på att mindre företag ofta saknar både ekonomiska och organisatoriska förutsättningar att implementera avancerade säkerhetsramverk, vilket ytterligare ökar deras sårbarhet i en digitaliserad industriell miljö (Panko et al., 2025).

Branschspecifika studier visar att konsekvenserna av cyberattacker kan bli särskilt allvarliga i tillverkningssektorn. Alqudhaibi et al. (2024b) beskriver exempelvis hur cyberattacker mot livsmedelsindustrin kan störa produktionen, påverka försörjningskedjor och försvaga konsumenters förtroende för verksamheten. Oroni och Xianping (2023) visar även att cybersäkerhetsmedvetenhet kan ha en direkt påverkan på företags prestationsförmåga, vilket innebär att området inte enbart är en teknisk säkerhetsfråga utan även en strategisk affärsfråga för många organisationer.

Forskning visar även att cybersäkerhet i tillverkningsindustrin inte bara är en intern fråga inom organisationen, utan påverkar även hur leverantörskedjan fungerar och håller över tid. Mani et al. (2017) visar att användningen av s.k. big data analytics kan bidra till att identifiera och förutse risker i leverantörskedjan, inklusive arbetsmiljöproblem, säkerhetsrisker, oetiskt beteende och andra operativa störningar. Genom att analysera stora datamängder kan företag upptäcka avvikelser och potentiella hot i ett tidigt skede, vilket möjliggör proaktiva åtgärder. Studien visar även att ett datadrivet arbetssätt kan bidra till att stärka både ekonomisk, social och miljömässig hållbarhet i verksamheten. Detta är särskilt relevant i en digitaliserad tillverkningsindustri där cybersäkerhetsrisker ofta sprider sig genom komplexa och sammankopplade leverantörsnätverk, vilket ytterligare understryker behovet av att integrera cybersäkerhetsmedvetenhet i hela organisationen.

Flera forskare har också analyserat varför SMF har svårt att utveckla sin säkerhetsförmåga. Wong et al. (2022) pekar på bristande policyefterlevnad och lågt engagemang bland anställda som betydande hinder. Button et al. (2024) visar att utformningen av cybersäkerhetsrelaterat tränings- och kommunikationsmaterial har stor betydelse för hur väl budskap accepteras och omsätts i praktiken. Skräddarsydda, psykologiskt anpassade och ibland även mer känslomässigt engagerande budskap kan i vissa fall vara mer effektiva än traditionella informationskampanjer. Mmango & Gundu (2023) lyfter fram ledarskapets viktiga roll i att skapa en organisationskultur där cybersäkerhet integreras i det dagliga arbetet. Samtidigt visar Chaudhary et al. (2023a) att forskningen om cybersäkerhetsmedvetenhet specifikt riktad mot SMF fortfarande är begränsad, vilket innebär att många företag saknar tillgång till anpassade och kostnadseffektiva lösningar för att stärka sin säkerhetskompetens.

Den nyare forskningen betonar även behovet av verktyg som hjälper SMF att förstå sitt nuvarande säkerhetsläge. Schuh et al. (2020) visar att många företag inte upptäcker cyberangrepp förrän skadan redan har inträffat, vilket ofta beror på bristande medvetenhet, begränsade resurser och avsaknad av stödverktyg för riskbedömning. För att adressera detta föreslår de ett angreppssätt baserat på så kallad serious gaming, där företag genom simulerade scenarier kan identifiera sina svagheter och samtidigt få en bättre förståelse för vilka säkerhetsåtgärder som bör prioriteras utifrån både risk och kostnad.

Forskning om cybersäkerhet i små och medelstora företag (SMF) har under de senaste åren ökat, detta i takt med att digitaliseringen av verksamheter och införandet av Industry 4.0-teknologier blivit alltmer omfattande. En litteraturbaserad studie av Panko et al. (2025) analyserade 245 vetenskapliga publikationer om cybersäkerhet i SMF publicerade mellan 2005 och 2025. Studien visar att forskningen inom området växer snabbt och att viktiga teman i litteraturen inkluderar cybersäkerhetsmedvetenhet, riskhantering och digitalisering. Samtidigt konstaterar författarna att små och medelstora företag ofta är mer sårbara för cyberhot än större organisationer, detta på grund av begränsade resurser, bristande teknisk kompetens och låg cybersäkerhetsmedvetenhet bland anställda.

I takt med att industriella system blir alltmer uppkopplade, har även cybersäkerhetsriskerna inom industrin ökat. Amirova et al. (2025) beskriver hur utvecklingen av Industrial Internet of Things (IIoT) har gjort det möjligt att integrera uppkopplade tekniska system, realtidsdata och automatisering i industrimiljöer. Samtidigt innebär denna ökade uppkoppling nya säkerhetsutmaningar, eftersom komplexa och sammankopplade system skapar fler potentiella attackytor. Studien framhåller därför vikten av att organisationer utvecklar både tekniska säkerhetsåtgärder och organisatoriska strategier för att hantera dessa risker, där cybersäkerhetsmedvetenhet bland anställda utgör en viktig komponent.

Flera studier har också undersökt betydelsen av cybersäkerhetskultur och medvetenhet i organisationer. García Arellano et al. (2024) genomförde en studie där cybersäkerhetskulturen i organisationer i León i Mexiko analyserades. Resultaten visar att många säkerhetsincidenter kan kopplas till bristande cybersäkerhetsmedvetenhet bland anställda och att organisationer ofta saknar strukturerade program för att utveckla en stark säkerhetskultur. Studien betonar att cybersäkerhetskultur bör betraktas som en kombination av organisatoriska rutiner, utbildning och individuella attityder till säkerhet.

Forskning har även visat att cybersäkerhetsmedvetenhet kan påverka organisationers prestation och verksamhetsresultat. Oroni och Xianping (2023) undersökte sambandet mellan ledningsförmåga, cybersäkerhetsmedvetenhet och organisationsprestation i tillverkningsföretag. Resultaten visar att cybersäkerhetsmedvetenhet är en viktig länk mellan ledningens kapacitet och hur bra organisationen presterar, vilket innebär att organisationer med högre säkerhetsmedvetenhet ofta uppvisar bättre operativa

resultat. Studien visar också att ledningens engagemang i cybersäkerhetsfrågor är avgörande för att etablera en organisationskultur där säkerhet integreras i det dagliga arbetet.

Šafár et al. (2025) visar att cybersäkerhetsmedvetenhet och cybersäkerhetsnivå i SMF påverkas av företagsspecifika egenskaper, särskilt ägarstruktur och företagsstorlek. Studien visar samband mellan större företag och företag utan familjeägd struktur uppvisar högre nivåer av cybersäkerhet. Resultaten visar också ett positivt samband mellan cybersäkerhet och företagens ekonomiska situation. Detta bidrar med ytterligare förståelse för att cybersäkerhetsmedvetenhet i SMF inte enbart formas av tekniska eller utbildningsrelaterade faktorer, utan även av organisatoriska och strukturella förutsättningar.

Akter et al. (2025) diskuterar vidare cybersäkerhetsmedvetenhet i relation till den datadrivna digitala ekonomin, och beskriver hur bristande medvetenhet kan utsätta organisationer för betydande cyberhot. Studien identifierar flera dimensioner av cybersäkerhetsmedvetenhet, inklusive kunskap om hot, förståelse för säkerhetsrutiner och individers förmåga att agera säkert i digitala miljöer. Författarna framhåller att cybersäkerhetsmedvetenhet bör ses som något organisationen behöver arbeta med och utveckla kontinuerligt genom utbildning, policyer och organisatoriskt stöd.

Vidare har forskning även fokuserat på hur cybersäkerhetsmedvetenhet kan stärka organisationers motståndskraft mot cyberattacker. Mmango och Gundu (2023) presenterar ett ramverk för hur små och medelstora organisationer kan stå emot och hantera cyberattacker. Ramverket bygger på litteraturstudier och intervjuer med företagare och cybersäkerhetsexperter, och visar att cybersäkerhetsmedvetenhet är en viktig komponent i organisationers förmåga att hantera cyberhot. Studien framhåller att utbildning, tydliga säkerhetspolicyer och organisatoriskt stöd är viktiga faktorer för att stärka motståndskraften mot cyberattacker i SMF.

Ett ytterligare perspektiv inom forskningen rör den mänskliga faktorns betydelse för informationssäkerhet. Giriraj et al. (2022) framhåller att en stor andel av säkerhetsincidenter kan kopplas till mänskliga misstag och att många organisationers utbildningsinsatser brister eftersom de främst fokuserar på tekniska aspekter. Studien betonar vikten av att inkludera mänskliga faktorer i cybersäkerhetsarbete och föreslår ett lämpligt ramverk för att anpassa utbildningsmaterial efter användarens

kunskapsnivå. Detta är särskilt relevant för små och medelstora tillverkningsföretag där cybersäkerhetsmedvetenhet behöver utvecklas utifrån både organisatoriska förutsättningar och personalens varierande kunskapsnivåer.

Sammanfattningsvis visar tidigare forskning att cybersäkerhetsmedvetenhet spelar en avgörande roll i organisationers cybersäkerhetsarbete, särskilt i små och medelstora företag där resurser och säkerhetskompetens ofta är begränsade. Samtidigt pekar forskningen på att cybersäkerhetsutmaningar ökar i takt med att digitaliseringen och uppkopplingen av industriella system fortsätter att utvecklas. Trots detta finns fortfarande begränsad forskning om hur cybersäkerhetsmedvetenhet kan utvecklas och implementeras i praktiken i små och medelstora tillverkningsföretag, vilket motiverar behovet av ytterligare studier inom området.

4 Resultat

Resultaten bygger på 21 vetenskapliga studier som inkluderats i scoping reviewn och analyserats tematiskt. Den tematiska analysen av det inkluderade forskningsmaterialet resulterade i identifieringen av flera återkommande mönster som tillsammans ger en samlad bild av hur cybersäkerhetsmedvetenhet (CSA) beskrivs i kontexten små och medelstora tillverkningsföretag. Genom en iterativ kodningsprocess där initiala koder successivt grupperades och omstrukturerades, framträdde fyra övergripande teman som bedöms vara viktiga för att förstå sig på området.

Dessa teman ska inte ses som isolerade kategorier, utan snarare som ömsesidigt beroende dimensioner av cybersäkerhetsmedvetenhet. Forskningen visar tydligt att CSA inte kan reduceras till en enskild faktor, utan uppstår i samspelet mellan individ, organisation och teknik. Dessa fyra teman representerar därför olika analytiska perspektiv på samma underliggande fenomen.

För att göra kopplingen till studiens forskningsfrågor tydlig kan resultatet sammanfattas på följande sätt: Tema 1 svarar främst på forskningsfråga 1 om hur nivån av cybersäkerhetsmedvetenhet beskrivs i tidigare forskning. Tema 3 och tema 4 svarar främst på forskningsfråga 2 om vilka metoder och strategier som lyfts samt vilka hinder som påverkar genomförandet. Tema 2 fungerar som en viktig bakgrund eftersom organisatoriska faktorer påverkar både nuläget och vilka insatser som blir möjliga i praktiken.

Ett första framträdande resultat i analysen är att forskningen konsekvent skiljer mellan individnivå och organisationsnivå, där cybersäkerhetsmedvetenhet på individnivå handlar om kunskap, attityder och beteenden, medan organisationsnivån fokuserar på strukturer, resurser och styrning. Denna uppdelning återkommer i flera studier och ligger till grund för hur samtliga identifierade teman strukturerats.

Det första temat behandlar den faktiska nivån av cybersäkerhetsmedvetenhet hos produktionsnära personal. Här framkommer att forskningen i stor utsträckning fokuserar på brister i kunskap och riskförståelse, men också på skillnaden mellan vad produktionsnära personal vet och hur de faktiskt agerar i praktiken. Detta tema fungerar som en nulägesbeskrivning och utgör därmed en grund för samtliga efterföljande teman.

Det andra temat rör organisatoriska faktorer som påverkar cybersäkerhetsmedvetenhet. Analysen visar att CSA i hög grad formas av ledningens prioriteringar, tillgång till resurser samt hur ansvar för cybersäkerhet är fördelat inom organisationen. Forskningen indikerar att brist på tydlig styrning och avsaknad av formella strukturer ofta leder till låg och inkonsekvent medvetenhet.

Det tredje temat fokuserar på metoder och strategier för att stärka cybersäkerhetsmedvetenhet. Här lyfter litteraturen fram olika typer av insatser, såsom utbildningsprogram, policyimplementering och tekniska stöd. Samtidigt visar resultaten att traditionella utbildningsinsatser ofta har begränsad effekt om de inte anpassas till den specifika kontexten i tillverkningsmiljöer.

Det fjärde temat behandlar de utmaningar och begränsningar som organisationer möter vid implementering av cybersäkerhetsmedvetenhet. Här framträder särskilt små och medelstora företags begränsade resurser, brist på specialistkompetens samt konflikter mellan säkerhet och produktion som vanligt förekommande hinder.

En viktig observation i analysen är att dessa teman inte följer en tydlig ordning, utan snarare påverkar och förstärker varandra. Exempelvis kan låg prioritering leda till bristande utbildning, vilket i sin tur resulterar i låg individuell medvetenhet. På samma sätt kan begränsade resurser påverka möjligheten att implementera effektiva strategier, vilket förstärker befintliga svagheter.

Vidare visar analysen att forskningen ofta behandlar cybersäkerhetsmedvetenhet som en del av ett bredare säkerhetsarbete, snarare än som ett isolerat fenomen. Detta innebär att CSA ofta kopplas till begrepp som riskhantering, säkerhetskultur och organisatorisk motståndskraft. Detta stärker bilden av att cybersäkerhetsmedvetenhet bör förstås som en integrerad del av organisationens övergripande förmåga att hantera cyberhot.

Ett ytterligare mönster som framträder i analysen är att forskningen i hög grad fokuserar på generella aspekter av cybersäkerhetsmedvetenhet, medan mer specifika faktorer kopplade till tillverkningsmiljöer ofta behandlas mer begränsat. Detta gäller särskilt produktionsnära miljöer där IT och operativa system samverkar. Denna observation är särskilt relevant i relation till studiens syfte, då den indikerar att det finns ett behov av att bättre förstå hur cybersäkerhetsmedvetenhet tar sig uttryck i just tillverkande verksamhet.

Analysen visar även att flera studier implicit utgår från en IT-centrerad syn på cybersäkerhet, vilket kan innebära att viktiga aspekter kopplade till produktion och operativa processer inte fullt ut beaktas. Detta förstärker behovet av att analysera cybersäkerhetsmedvetenhet i en bredare organisatorisk kontext, där både tekniska och verksamhetsnära perspektiv inkluderas.

Sammanfattningsvis visar den tematiska analysen att cybersäkerhetsmedvetenhet i små och medelstora tillverkningsföretag är ett komplext och mångdimensionellt fenomen. De teman som identifierats ger en strukturerad förståelse av detta fenomen och fungerar som en analytisk grund för de mer detaljerade resultat som presenteras i de följande avsnitten.

4.1 Nivån av cybersäkerhetsmedvetenhet hos produktionsnära personal

Detta tema kopplar främst till forskningsfråga 1 och sammanfattar hur tidigare forskning beskriver nivån av cybersäkerhetsmedvetenhet hos produktionsnära personal.

Analysen av det insamlade, vetenskapliga materialet visar att cybersäkerhetsmedvetenheten hos produktionsnära personal i små och medelstora tillverkningsföretag generellt beskrivs som begränsad och ojämnt fördelad. Detta framträder som ett återkommande resultat i litteraturen och utgör en viktig utgångspunkt för att förstå de risker som dessa organisationer står inför (Akter et al., 2025; Chaudhary et al., 2023b; Ibrahim et al., 2025)

Ett återkommande mönster är att produktionsnära personal ofta saknar en tydlig förståelse för hur deras dagliga arbetsuppgifter är kopplade till cybersäkerhet. Arbetet i produktionsmiljöer präglas i hög grad av fokus på effektivitet, kontinuitet och drift, vilket innebär att säkerhetsaspekter tenderar att prioriteras ned eller uppfattas som sekundära. Cybersäkerhet ses därmed inte alltid som en integrerad del av arbetsrollen, utan snarare som något som hanteras av IT-specialister eller externa aktörer (Brunken et al., 2025).

Vidare visar resultaten att kunskapsnivån kring cyberhot kan variera. Detta är relevant eftersom tidigare forskning visar att mänskliga faktorer ofta bidrar till informationssäkerhetsincidenter och att anställdas informationssäkerhetsmedvetenhet därför är central för organisationers säkerhetsarbete (Khando et al., 2021).

Analysen indikerar även att beteenden i många fall påverkas av informella normer snarare än formella riktlinjer. I produktionsmiljöer där arbetsmoment ofta är standardiserade och tidspressade kan informella arbetssätt få större genomslag än dokumenterade policyer. Detta innebär att även väl utformade säkerhetsriktlinjer riskerar att åsidosättas om de inte är anpassade till hur arbetet faktiskt utförs i praktiken (Wong et al., 2022).

Vidare framträder att upplevd konsekvens spelar en viktig roll för beteendeförändring. När risker upplevs som abstrakta eller osannolika minskar drivkraften att agera säkert. Detta bidrar till att cybersäkerhet ofta prioriteras ned i vardagliga situationer, särskilt i miljöer där fokus ligger på att upprätthålla drift och produktivitet (Button et al., 2024).

En viktig aspekt som framkommer i analysen är skillnaden mellan medvetenhet och beteende. Flera studier visar att även när personal har viss kunskap om cybersäkerhetsrisker omsätts denna kunskap inte nödvändigtvis i praktiken. Exempel på detta kan vara fortsatt användning av svaga lösenord, delning av inloggningsuppgifter eller åsidosättande av säkerhetsrutiner. Detta tyder på att cybersäkerhetsmedvetenhet inte enbart är en fråga om informationsnivå, utan även om motivation, attityder och organisatoriska normer (Ani et al., 2019).

Resultaten indikerar också att erfarenhet av tidigare incidenter kan påverka medvetenheten. Organisationer som har varit utsatta för cyberattacker eller säkerhetsproblem tenderar att bli mer uppmärksamma på risker och behovet av rutiner. På individnivå kan direkt eller indirekt exponering för incidenter bidra till ökad vaksamhet och större benägenhet att följa säkerhetsrutiner. Detta tyder på att erfarenhetsbaserat lärande kan spela en roll i utvecklingen av cybersäkerhetsmedvetenhet (Rawindaran et al., 2025).

Samtidigt visar analysen att denna typ av lärande ofta är reaktiv snarare än proaktiv. Medvetenheten ökar först efter att en incident har inträffat, snarare än genom förebyggande arbete. Detta pekar på en brist i organisationernas förmåga att arbeta systematiskt och långsiktigt med cybersäkerhetsmedvetenhet (Panko et al., 2025).

En annan viktig observation är att det finns variationer inom gruppen produktionsnära personal. Medvetenheten påverkas av faktorer såsom tidigare erfarenhet, utbildningsbakgrund och exponering för IT-system. Personer som i större utsträckning interagerar med digitala system tenderar att ha bättre förutsättningar att förstå

cybersäkerhetsrisker, medan personal som arbetar mer praktiskt eller manuellt kan ha lägre förståelse för cybersäkerhetsfrågor. Detta skapar en ojämn fördelning av medvetenhet inom organisationen, vilket i sig kan utgöra en sårbarhet (Giriraj et al., 2022).

Forskningen pekar även på att kommunikationen kring cybersäkerhet inom organisationer ofta är bristfällig. Säkerhetsinformation når inte alltid ut till produktionsnära personal på ett sätt som är anpassat till deras arbetskontext. Detta innebär att även när organisationer har policyer och riktlinjer är det inte säkert att dessa förstås eller efterlevs i praktiken (Alzahrani & Seth, 2021).

Sammanfattningsvis kan det konstateras att cybersäkerhetsmedvetenheten hos produktionsnära personal i små och medelstora tillverkningsföretag präglas av flera utmaningar. Den är generellt låg, varierar mellan individer och påverkas av både organisatoriska och individuella faktorer. Framför allt framträder en tydlig skillnad mellan kunskap och beteende, samt en tendens att medvetenhet utvecklas reaktivt snarare än genom strukturerade och förebyggande insatser (Akter et al., 2025).

4.2 Organisatoriska faktorer som påverkar cybersäkerhetsmedvetenhet

Detta tema påverkar båda forskningsfrågorna. Organisatoriska förutsättningar förklarar både nuläget hos personalen och vilka insatser som faktiskt blir möjliga att genomföra.

Den tematiska analysen visar att cybersäkerhetsmedvetenhet i små och medelstora tillverkningsföretag i hög grad formas av organisatoriska faktorer, snarare än enbart individuella egenskaper. Forskningen pekar på att CSA bör förstås som en organisatorisk förmåga, där ledning, struktur, resurser och kultur tillsammans påverkar hur säkerhetsmedvetenhet utvecklas och upprätthålls inom verksamheten (Akter et al., 2025).

En av de mest framträdande faktorerna är ledningens engagemang och prioritering av cybersäkerhet. Resultaten visar att organisationer där ledningen aktivt arbetar med och kommunicerar vikten av cybersäkerhet generellt har bättre förutsättningar att skapa medvetenhet bland anställda. När cybersäkerhet integreras i strategiska beslut och ses som en del av verksamhetens övergripande mål tenderar det att få större genomslag i organisationen (Oroni & Xianping, 2023).

I kontrast visar resultaten att när cybersäkerhet betraktas som en sekundär fråga eller enbart ett tekniskt ansvar för IT-avdelningen, leder detta ofta till låg prioritet i organisationen. Detta resulterar i bristande riktlinjer, otydliga ansvarsförhållanden och en generell avsaknad av säkerhetsfokus i det dagliga arbetet (Rawindaran et al., 2025).

En annan viktig aspekt är tillgången till resurser, vilket inkluderar både ekonomiska resurser och kompetens. Små och medelstora företag kännetecknas ofta av begränsade säkerhetsbudgetar och avsaknad av dedikerade säkerhetsfunktioner. Detta innebär att cybersäkerhetsarbete ofta får konkurrera med andra affärskritiska prioriteringar, såsom produktion och leverans (Erdogan et al., 2023).

Flera studier visar att denna resursbrist påverkar möjligheten att implementera strukturerade säkerhetsinitiativ, såsom utbildningsprogram eller policyarbete. Analysen visar även att kortsiktiga prioriteringar ofta dominerar i små och medelstora företag, vilket påverkar cybersäkerhetsarbetets långsiktighet. Investeringar i säkerhet kan uppfattas som kostnader snarare än långsiktiga investeringar, särskilt i organisationer med begränsade marginaler. Detta bidrar till att säkerhetsinitiativ ofta genomförs reaktivt snarare än som en del av en övergripande strategi (Chidukwani et al., 2024).

Vidare framkommer att graden av ledningens förståelse för cybersäkerhetsrisker påverkar hur resurser fördelas. I organisationer där ledningen har begränsad insikt i cyberhotens potentiella konsekvenser tenderar säkerhetsarbete att få en lägre prioritet, vilket i sin tur påverkar hela organisationens medvetenhet. Resultatet av detta blir att cybersäkerhetsmedvetenhet utvecklas sporadiskt och utan en tydlig långsiktig strategi (Mmango & Gundu, 2023).

Vidare framträder ansvarsfördelning och organisatorisk struktur som en avgörande faktor. I många SMF saknas tydligt definierade roller kopplade till cybersäkerhet, vilket leder till osäkerhet kring vem som ansvarar för vad. Detta skapar en situation där säkerhetsfrågor faller mellan olika funktioner eller avdelningar och där ingen har ett uttalat helhetsansvar (Alzahrani & Seth, 2021).

Forskningen visar att organisationer med tydliga roller och ansvarsfördelning, exempelvis genom utpekade säkerhetsansvariga eller formaliserade processer, har bättre förutsättningar att arbeta systematiskt med cybersäkerhetsmedvetenhet (Ponsard & Grandclaudon, 2020).

En ytterligare viktig dimension är organisationskultur, där normer, värderingar och beteenden påverkar hur cybersäkerhet uppfattas och prioriteras. Resultaten visar att i organisationer där säkerhet ses som en naturlig del av arbetet tenderar anställda att i större utsträckning följa riktlinjer och agera säkert. I miljöer där effektivitet och produktion prioriteras framför säkerhet kan cybersäkerhetsåtgärder däremot uppfattas som hinder, vilket kan leda till att rutiner kringgås eller ignoreras, särskilt om de upplevs som tidskrävande eller komplicerade (García Arellano et al., 2024).

Kommunikation framträder också som en viktig organisatorisk faktor. Forskningen visar att hur cybersäkerhet kommuniceras inom organisationen har stor betydelse för medvetenheten. Generella policyer och riktlinjer är ofta otillräckliga om de inte anpassas till den specifika arbetskontexten. I tillverkningsmiljöer, där arbetet ofta är praktiskt och tidspressat, krävs tydlig, konkret och situationsanpassad kommunikation för att säkerhetsbudskap ska få genomslag. Bristande kommunikation leder annars till att säkerhetsarbetet uppfattas som irrelevant eller svårt att tillämpa i praktiken. (Button et al., 2024).

Slutligen visar analysen att integration mellan IT och produktion, alltså IT/OT, är en viktig organisatorisk utmaning. I många tillverkningsföretag är dessa två områden organisatoriskt separerade, vilket kan leda till bristande samordning i säkerhetsarbetet. Detta skapar sårbarheter, särskilt i miljöer där digitala system är direkt kopplade till produktionen (Corallo et al., 2022).

Sammanfattningsvis visar detta tema att cybersäkerhetsmedvetenhet i små och medelstora tillverkningsföretag i stor utsträckning formas av organisatoriska förutsättningar. Ledningens prioriteringar, tillgång till resurser, tydlighet i ansvarsfördelning, organisationskultur samt kommunikation och samordning mellan funktioner framträder som avgörande faktorer. Detta innebär att arbetet med att stärka cybersäkerhetsmedvetenhet inte enbart bör fokusera på individen, utan i hög grad måste adressera organisatoriska strukturer och processer (Akter et al., 2025).

4.3 Metoder och strategier för att stärka cybersäkerhetsmedvetenhet

Detta tema kopplar främst till forskningsfråga 2 och sammanfattar vilka metoder, modeller och utbildningsupplägg som lyfts i tidigare forskning för att stärka cybersäkerhetsmedvetenhet.

Analysen av det vetenskapliga materialet visar att ett brett spektrum av metoder och strategier används för att stärka cybersäkerhetsmedvetenhet i små och medelstora tillverkningsföretag. Samtidigt framgår det tydligt att effektiviteten av dessa insatser varierar, och att framgångsrika initiativ ofta kännetecknas av att de är anpassade till organisationens specifika kontext (Johansson et al., 2022).

En av de mest vanligt förekommande strategierna i litteraturen är utbildnings- och träningsinsatser. Dessa kan inkludera allt från grundläggande informationsmöten till mer avancerade och kontinuerliga utbildningsprogram. Resultaten visar att utbildning är en viktig del i arbetet med cybersäkerhetsmedvetenhet, men att traditionella, engångsbaserade utbildningar ofta har begränsad långsiktig effekt. Forskningen betonar i stället vikten av kontinuerligt lärande, där utbildning sker återkommande och integreras i det dagliga arbetet (Khando et al., 2021).

Interaktiva metoder, såsom simuleringar, scenariobaserade övningar och spelbaserat lärande, lyfts fram som särskilt relevanta eftersom de kan skapa en mer konkret förståelse för hot och risker. Sådana metoder kan hjälpa organisationer att identifiera svagheter och samtidigt öka personalens förståelse för vilka säkerhetsåtgärder som bör prioriteras (Schuh et al., 2020).

Vidare framträder policyer och riktlinjer som en viktig strategi. Organisationer som implementerar tydliga säkerhetspolicyer har bättre förutsättningar att skapa en gemensam förståelse för vad som förväntas av anställda. Samtidigt visar analysen att policyer i sig inte är tillräckliga. Om de uppfattas som för generella, komplexa eller irrelevanta för den dagliga verksamheten finns en risk att de inte efterlevs i praktiken (Wong et al., 2022).

En tredje strategi som lyfts fram i litteraturen är användningen av tekniska lösningar. Dessa inkluderar exempelvis system för autentisering, automatiserade säkerhetskontroller och användarvänliga säkerhetslösningar. Resultaten visar att tekniska lösningar kan fungera som ett komplement till utbildning genom att minska beroendet av individuellt beteende. Samtidigt betonas att tekniska åtgärder inte kan ersätta medvetenhet, utan snarare bör ses som en del av ett helhetsgrepp där både mänskliga och tekniska faktorer beaktas (Ani et al., 2019).

Analysen visar även att ledningsstyrda initiativ spelar en avgörande roll. Organisationer där ledningen aktivt driver cybersäkerhetsarbete, exempelvis genom

att prioritera resurser, sätta tydliga mål och följa upp säkerhetsarbete, har större möjligheter att implementera effektiva strategier för att öka medvetenheten. Ledningens engagemang bidrar inte bara till att möjliggöra insatser, utan fungerar också som en signal till organisationen om att cybersäkerhet är en prioriterad fråga (Oroni & Xianping, 2023).

En ytterligare strategi som identifieras är utvecklingen av en säkerhetskultur. Forskningen visar att långsiktigt hållbar cybersäkerhetsmedvetenhet uppstår när säkerhet blir en naturlig del av organisationens värderingar och arbetssätt. Detta innebär att anställda inte enbart följer regler, utan också förstår vikten av säkerhet och agerar därefter. Att skapa en sådan kultur kräver dock tid och kontinuitet, samt att säkerhetsarbete integreras i organisationens dagliga processer (García Arellano et al., 2024).

Samtidigt framkommer det att standardiserade ramverk och modeller ofta används som stöd i arbetet med att strukturera och implementera säkerhetsåtgärder. Dessa ramverk kan fungera som vägledning för organisationer som saknar egen kompetens eller erfarenhet inom området. Dock visar resultaten att sådana ramverk ibland kan upplevas som komplexa eller svåra att anpassa till mindre organisationers förutsättningar, vilket kan begränsa deras praktiska användbarhet (Alqudhaibi et al., 2024b).

En viktig övergripande observation i analysen är att enskilda åtgärder sällan är tillräckliga. Effektiva strategier kännetecknas i stället av en kombination av flera insatser, där utbildning, policyer, tekniska lösningar och organisatoriskt stöd samverkar. Detta pekar på behovet av ett samlat angreppssätt, där cybersäkerhetsmedvetenhet integreras i organisationens övergripande verksamhet (Akter et al., 2025).

Analysen indikerar även att implementeringen av strategier ofta påverkas av organisationens mognadsnivå inom cybersäkerhet. Företag med låg mognadsgrad tenderar att fokusera på grundläggande åtgärder, medan mer mogna organisationer arbetar mer systematiskt och integrerat med säkerhetsfrågor. Detta innebär att samma strategi kan ha olika effekt beroende på organisationens förutsättningar (Panko et al., 2025).

Vidare framträder att flexibilitet i implementeringen är en viktig framgångsfaktor. Strategier som tillåter anpassning till lokala arbetsförhållanden och individuella behov har större sannolikhet att accepteras och få genomslag i praktiken. Detta är särskilt relevant i produktionsnära miljöer där personalens arbetsuppgifter, tekniska exponering och kunskapsnivå kan variera (Giriraj et al., 2022).

Sammanfattningsvis visar detta tema att det finns ett flertal metoder och strategier för att stärka cybersäkerhetsmedvetenhet, men att deras effektivitet är beroende av hur väl de anpassas till organisationens kontext. Framgångsrika insatser kännetecknas av kontinuitet, praktisk relevans och stöd från ledningen, samt av att de kombinerar flera olika typer av åtgärder snarare än att förlita sig på en enskild metod (Ponsard & Grandclaudon, 2020).

4.4 Utmaningar och begränsningar i implementering av cybersäkerhetsmedvetenhet

Analysen visar att små och medelstora tillverkningsföretag står inför ett flertal återkommande utmaningar i arbetet med att implementera och upprätthålla cybersäkerhetsmedvetenhet. Dessa utmaningar är både strukturella och operativa, och påverkar i hög grad organisationernas förmåga att omsätta strategier och åtgärder i praktiken (Panko et al., 2025).

En av de mest framträdande utmaningarna är begränsade resurser, både i form av ekonomi och kompetens. Små och medelstora företag saknar ofta dedikerade säkerhetsbudgetar och specialiserad personal inom cybersäkerhet. Detta innebär att säkerhetsarbete i många fall blir reaktivt och prioriteras ned till förmån för mer direkt affärskritiska aktiviteter, såsom produktion och leverans. Resursbristen påverkar även möjligheten att genomföra kontinuerliga utbildningsinsatser och implementera mer avancerade säkerhetslösningar, vilket i sin tur begränsar utvecklingen av cybersäkerhetsmedvetenhet (Erdogan et al., 2023).

En annan återkommande utmaning är konflikten mellan säkerhet och operativ effektivitet. I tillverkningsmiljöer är fokus ofta riktat mot att upprätthålla en stabil och effektiv produktion. Säkerhetsåtgärder som upplevs som tidskrävande eller störande kan därför möta motstånd från personalen. Detta leder till att säkerhetsrutiner ibland kringgås eller inte efterlevs fullt ut, särskilt i situationer där de uppfattas som hinder

för arbetsflödet. Analysen visar att denna konflikt är särskilt tydlig i produktionsnära miljöer där tidspress och kontinuitet är avgörande (Brunken et al., 2025).

Vidare framträder brist på anpassning till kontext som en betydande begränsning. Många av de metoder och ramverk som föreslås i forskningen är utvecklade för större organisationer eller mer IT-fokuserade miljöer. När dessa tillämpas i små tillverkningsföretag kan de upplevas som komplexa, resurskrävande eller svåra att integrera i den dagliga verksamheten. Detta resulterar i att organisationer antingen avstår från att implementera dem fullt ut eller gör förenklade anpassningar som minskar deras effektivitet (Chaudhary et al., 2023b).

En ytterligare utmaning som identifieras är bristande kontinuitet i säkerhetsarbetet. Cybersäkerhetsmedvetenhet hanteras ofta som en engångsinsats, exempelvis genom enstaka utbildningar eller tillfälliga initiativ. Avsaknaden av ett långsiktigt och systematiskt arbetssätt leder till att effekterna av dessa insatser avtar över tid. Detta förstärker den tidigare identifierade problematiken kring att medvetenhet tenderar att utvecklas reaktivt snarare än proaktivt (Khando et al., 2021).

Analysen pekar även på svårigheter i att förändra beteenden som en viktig begränsning. Även när kunskap och riktlinjer finns på plats, är det inte självklart att dessa leder till förändrade arbetssätt. Beteendeförändring kräver inte bara information, utan även motivation, uppföljning och stöd från organisationen. Utan tydliga incitament och konsekvenser riskerar säkerhetsarbete att få låg prioritet i praktiken (Ani et al., 2019).

En annan viktig aspekt är bristande integration mellan IT och produktion, alltså IT/OT. I många tillverkningsföretag hanteras dessa områden separat, vilket kan leda till bristande helhetssyn i säkerhetsarbetet. Detta skapar särskilda utmaningar i miljöer där digitala system är direkt kopplade till fysiska processer. Bristen på samordning innebär att cybersäkerhetsåtgärder inte alltid är anpassade till produktionsmiljön, vilket kan leda till både ineffektivitet och ökade risker (Corallo et al., 2022).

Slutligen visar analysen att mätning och uppföljning av cybersäkerhetsmedvetenhet är ett område med tydliga begränsningar. Det saknas ofta etablerade metoder för att utvärdera effekten av genomförda åtgärder, vilket gör det svårt för organisationer att avgöra vad som fungerar och vad som behöver förbättras. Denna brist på uppföljning försvårar ett systematiskt förbättringsarbete och bidrar till att

cybersäkerhetsmedvetenhet inte utvecklas på ett strukturerat sätt (Ibrahim et al., 2025).

Sammanfattningsvis visar detta tema att implementeringen av cybersäkerhetsmedvetenhet i små och medelstora tillverkningsföretag präglas av flera samverkande utmaningar. Begränsade resurser, organisatoriska prioriteringar, bristande anpassning av metoder samt svårigheter att förändra beteenden framträder som väsentliga hinder. Dessa utmaningar bidrar till att cybersäkerhetsmedvetenhet ofta utvecklas ojämnt och utan långsiktig stabilitet, vilket i sin tur påverkar organisationernas generella förmåga att hantera cyberhot (Rawindaran et al., 2025).

4.5 Sammanfattning av resultat

Den tematiska analysen av det insamlade forskningsmaterialet visar att cybersäkerhetsmedvetenhet i små och medelstora tillverkningsföretag är ett komplext och varierat fenomen som påverkas av en kombination av individuella, organisatoriska och tekniska faktorer. Resultaten från fyra identifierade teman ger tillsammans en samlad bild av både nuläge, påverkande faktorer, möjliga åtgärder samt de utmaningar som organisationer står inför.

Analysen visar att cybersäkerhetsmedvetenheten hos produktionsnära personal generellt är begränsad och ojämnt fördelad inom organisationer. Det framkommer tydligt att det finns en skillnad mellan kunskap och faktisk beteendeförändring, där personalen i många fall är medvetna om risker men ändå inte agerar i enlighet med säkerhetsrutiner. Detta indikerar att cybersäkerhetsmedvetenhet inte enbart handlar om att tillföra kunskap, utan även om att påverka personalens attityder och beteenden.

Vidare framträder organisatoriska faktorer som avgörande för hur cybersäkerhetsmedvetenhet utvecklas och upprätthålls. Ledningens engagemang, tillgång till resurser, tydlig ansvarsfördelning och organisationskultur identifieras som viktiga komponenter i detta. Resultaten visar att organisationer som saknar struktur och tydlig styrning har svårare att etablera en stabil nivå av cybersäkerhetsmedvetenhet.

Vad gäller metoder och strategier visar analysen att det finns flera tillvägagångssätt för att stärka cybersäkerhetsmedvetenhet, där utbildning, policyer och tekniska lösningar är de mest framträdande. Samtidigt framgår det att enskilda insatser sällan är tillräckliga, utan att ett kombinerat och kontinuerligt arbetssätt krävs för att uppnå

långsiktig effekt. Anpassning till organisationens specifika kontext framstår som en viktig faktor för framgång.

Resultaten visar även att implementeringen av cybersäkerhetsmedvetenhet präglas av flera utmaningar. Begränsade resurser, konflikter mellan säkerhet och produktion, bristande anpassning av metoder samt svårigheter att förändra personalens beteenden utgör betydande hinder. Dessa faktorer bidrar till att cybersäkerhetsarbete ofta blir reaktivt och fragmenterat, snarare än proaktivt och systematiskt.

Tabell 3: Inkluderade studier kopplade till teman

Tema 1: Nivån av cybersäkerhetsmedvetenhet

Tema 2: Organisatoriska faktorer

Tema 3: Metoder och strategier

Tema 4: Utmaningar och begränsningar

Artikel	Tema 1	Tema 2	Tema 3	Tema 4
Akter et al. (2025)	X	X	X	
Alzahrani & Seth (2021)		X	X	
Amirova et al. (2025)		X		X
Ani et al. (2019)	X		X	X
Arellano et al. (2024)		X	X	
Arroyabe et al. (2024)		X		X
Brunken et al. (2025)	X		X	X
Button et al. (2024)	X	X	X	
Chidukwani et al. (2024)		X		X
Corallo et al. (2022)		X		X
Erdogan et al. (2023)	X	X		X
Giriraj et al. (2022)	X		X	
Johansson et al. (2022)	X		X	X
Khando et al. (2021)	X		X	X
Mani et al. (2017)		X		X
Mmango & Gundu (2023)		X	X	X
Oroni & Xianping (2023)		X	X	
Panko et al. (2025)	X	X		X
Ponsard & Grandclaudon (2020)			X	X
Rawindaran et al. (2025)	X	X		X
Wong et al. (2022)	X	X	X	X

5 Diskussion

I diskussionen kopplas resultaten tillbaka till studiens två forskningsfrågor. Först diskuteras hur nivån av cybersäkerhetsmedvetenhet hos produktionsnära personal beskrivs i tidigare forskning. Därefter diskuteras vilka metoder och förutsättningar som lyfts som viktiga för att kunna stärka medvetenheten i små och medelstora tillverkningsföretag.

5.1 Diskussion kopplat till forskningsfråga 1

Analysen av forskningsfråga 1 visar resultaten att nivån av cybersäkerhetsmedvetenhet hos produktionsnära personal ofta beskrivs som begränsad och ojämn (Johansson et al., 2022). Forskningen pekar också på att det kan finnas ett glapp mellan att känna till risker och att faktiskt agera säkert i vardagen, särskilt i miljöer där tidspress och produktionstakt påverkar arbetssättet (Ani et al., 2019).

En rimlig tolkning utifrån litteraturen är därför att medvetenhet i praktiken inte bara beror på individers kunskap, utan också på vilka rutiner och förutsättningar som finns runt dem (Brunken et al., 2025). Det blir en naturlig övergång till forskningsfråga 2 som handlar om vilka insatser och arbetssätt som kan stärka medvetenheten.

5.2 Diskussion kopplat till forskningsfråga 2

För forskningsfråga 2 visar resultaten att utbildning och träning ofta lyfts fram som en viktig del för att stärka cybersäkerhetsmedvetenhet, men att enstaka insatser sällan räcker. Litteraturen pekar i stället på behovet av återkommande och praktiskt relevanta upplägg som passar produktionsmiljön och vardagens arbetsflöden (Khando et al., 2021).

Resultatet visar också att organisatoriska faktorer har stor betydelse för om sådana insatser faktiskt blir av och om de får effekt. Ledningens prioriteringar, resursfördelning och tydligt ansvar påverkar om säkerhetsarbete blir långsiktigt eller om det blir reaktivt (Akter et al., 2025).

Ett annat framträdande resultat är betydelsen av organisatorisk kultur och kommunikation. Cybersäkerhetsmedvetenhet påverkas inte enbart av formella policys och riktlinjer, utan också av hur dessa uppfattas och efterlevs i praktiken.

Om säkerhetsrutiner upplevs som krångliga eller hindrande, finns en risk att de kringgås av medarbetare, särskilt i produktionsnära miljöer där effektivitet och drift ofta prioriteras. Detta pekar på vikten av att utforma säkerhetsåtgärder som är både användarvänliga och anpassade till verksamhetens behov, snarare än att enbart fokusera på teknisk säkerhet (Wong et al., 2022).

Resultatet belyser även utmaningar kopplade till integrationen mellan IT och OT (Operational Technology), vilket är särskilt relevant i tillverkningsindustrin. Studien visar att dessa två områden ofta är organisatoriskt och tekniskt separerade, vilket kan skapa säkerhetsluckor. Medan IT-miljöer ofta är relativt väl skyddade och standardiserade, kan OT-miljöer vara äldre, mer komplexa och svårare att uppdatera. Denna separation innebär att cybersäkerhetsarbete riskerar att bli fragmenterat, där olika delar av organisationen har olika säkerhetsnivåer och arbetssätt. Detta kan i sin tur utnyttjas av angripare som riktar in sig på den svagaste länken i systemet (Corallo et al., 2022).

En ytterligare viktig aspekt som framkommer i resultatet är resursbegränsningar inom små och medelstora företag. Till skillnad från större organisationer har dessa företag ofta begränsade ekonomiska och personalmässiga resurser att avsätta för cybersäkerhet. Detta påverkar möjligheten att implementera avancerade säkerhetslösningar, genomföra regelbundna utbildningar och arbeta proaktivt med säkerhetsfrågor. I stället tenderar arbetet att bli mer reaktivt, där åtgärder vidtas först efter att en incident inträffat. Detta understryker behovet av kostnadseffektiva och skalbara lösningar som är anpassade till mindre organisationers förutsättningar (Erdogan et al., 2023).

Resultatet visar även att externa faktorer, såsom regelverk och standarder, kan fungera både som drivkrafter och utmaningar i cybersäkerhetsarbetet. Å ena sidan kan ramverk och lagkrav bidra till att strukturera och prioritera säkerhetsarbetet, men å andra sidan kan de upplevas som komplexa och svåra att implementera, särskilt för organisationer med begränsad erfarenhet inom området. Detta kan leda till att implementeringen blir ytlig eller att organisationer fokuserar på att uppfylla formella krav snarare än att faktiskt förbättra säkerheten i praktiken (Alqudhaibi et al., 2024b).

Sammanfattningsvis visar resultatet att cybersäkerhetsmedvetenhet i tillverkningsföretag är beroende av en balans mellan flera faktorer. Individuell

kunskap är viktig, men måste stödjas av organisatoriska strukturer, tydligt ledarskap, anpassade tekniska lösningar och en kultur som främjar säkerhetsmedvetet beteende. Utan denna helhetssyn riskerar insatser att bli fragmenterade och ineffektiva. Studien bidrar därmed till en djupare förståelse av hur cybersäkerhetsmedvetenhet kan utvecklas i praktiken och belyser behovet av integrerade och långsiktiga strategier snarare än enskilda åtgärder (Mmango & Gundu, 2023).

5.3 Metoddiskussion

Eftersom studien bygger på publicerad litteratur kan urvalet påverkas av att vissa typer av studier publiceras oftare än andra. Ingen formell kvalitetsgranskning har gjorts av varje enskild studie, vilket innebär att resultaten ska förstås som en kartläggning av forskningsläget snarare än en värdering av evidensstyrka. Det betyder också att resultaten främst visar vilka mönster som återkommer i litteraturen och inte hur situationen ser ut i ett specifikt företag.

Valet av metod i denna studie har varit avgörande för möjligheten att uppnå studiens syfte, som är att skapa en fördjupad förståelse för cybersäkerhetsmedvetenhet inom små och medelstora tillverkningsföretag. Genom att använda en litteraturbaserad ansats har det varit möjligt att samla in och analysera ett brett spektrum av tidigare forskning inom området, vilket ger en övergripande och teoretiskt förankrad bild av fenomenet. Detta är särskilt relevant i en kontext där området är relativt nytt och där empiriska studier fortfarande är begränsade.

En av de främsta styrkorna med den valda metoden är möjligheten att identifiera återkommande mönster, teman och forskningsluckor genom att jämföra flera studier. Genom att analysera olika forskningsbidrag har det varit möjligt att skapa en mer nyanserad förståelse av cybersäkerhetsmedvetenhet, där både tekniska, organisatoriska och mänskliga aspekter beaktas. Detta bidrar till att resultatet inte baseras på en enskild studie eller kontext, utan i stället speglar ett bredare forskningsläge.

Samtidigt innebär valet av en litteraturstudie vissa begränsningar som är viktiga att beakta. Eftersom studien bygger på sekundärdata är resultatet beroende av kvaliteten på de artiklar som inkluderats. Eftersom de inkluderade studierna har olika metodval, avgränsningar och undersökningskontexter kan detta indirekt påverka hur resultaten tolkas i denna studie. Vidare kan urvalet av artiklar ha påverkat vilka perspektiv som

framkommer. Även om en systematisk ansats har eftersträvats finns alltid en risk att relevant forskning exkluderas, exempelvis på grund av val av databaser, sökord eller inklusions- och exklusionskriterier.

En annan aspekt att reflektera över är användningen av tematisk analys som metod för dataanalys. Tematisk analys möjliggör en flexibel och strukturerad bearbetning av kvalitativ data, vilket är en styrka i en studie av detta slag. Genom att identifiera och kategorisera teman har det varit möjligt att strukturera komplex information och lyfta fram viktiga aspekter av cybersäkerhetsmedvetenhet. Samtidigt innebär denna metod att analysen till viss del bygger på forskarnas egna tolkningar. Detta kan introducera en grad av subjektivitet, särskilt vid identifiering och tolkning av teman.

För att hantera denna utmaning har analysen genomförts med fokus på tydliga och återkommande mönster i litteraturen, snarare än enstaka observationer. Trots detta kan det inte uteslutas att andra forskare skulle kunna tolka materialet på ett delvis annorlunda sätt. Detta är en generell utmaning inom kvalitativ forskning och påverkar studiens reliabilitet, det vill säga möjligheten att uppnå samma resultat vid en upprepning av studien.

När det gäller studiens validitet, det vill säga i vilken utsträckning studien faktiskt undersöker det som avses, kan det argumenteras att den teoretiska ansatsen är väl anpassad till syftet. Studien fokuserar på att förstå cybersäkerhetsmedvetenhet som fenomen snarare än att mäta det empiriskt, vilket gör en litteraturstudie till ett rimligt val. Samtidigt innebär avsaknaden av empirisk datainsamling, såsom intervjuer eller fallstudier, att studien inte kan ge en direkt inblick i hur cybersäkerhetsarbete bedrivs i praktiken inom specifika organisationer. Detta kan begränsa möjligheten att dra konkreta slutsatser om implementering i verkliga miljöer.

En ytterligare begränsning är att cybersäkerhetsområdet utvecklas snabbt, vilket innebär att forskning snabbt kan bli inaktuell. De studier som analyserats speglar därför kunskapsläget vid tidpunkten för datainsamlingen, men det är möjligt att nya hot, tekniker och arbetssätt har utvecklats efter detta. Detta påverkar studiens aktualitet och understryker behovet av kontinuerlig forskning inom området.

Trots dessa begränsningar bedöms den valda metoden vara lämplig i relation till studiens syfte. Genom att kombinera flera forskningskällor och analysera dessa systematiskt har studien kunnat bidra till en ökad förståelse av

cybersäkerhetsmedvetenhet inom tillverkningsindustrin. För framtida forskning skulle det vara värdefullt att komplettera denna typ av studie med empiriska undersökningar, exempelvis genom intervjuer eller fallstudier, för att undersöka hur de identifierade faktorerna faktiskt tar sig uttryck i praktiken.

Sammanfattningsvis har metodvalet möjliggjort en bred och teoretiskt förankrad analys av cybersäkerhetsmedvetenhet, men med vissa begränsningar kopplade till urval, subjektivitet och avsaknad av empirisk data. Dessa aspekter är viktiga att beakta vid tolkning av studiens resultat och slutsatser.

6 Slutsatser och rekommendationer

Utifrån studiens syfte och genomförda analys kan det konstateras att cybersäkerhetsmedvetenhet inom små och medelstora tillverkningsföretag är ett komplext och mångdimensionellt fenomen som inte kan reduceras till enbart individers kunskap eller tekniska lösningar. Resultatet visar att cybersäkerhetsmedvetenhet snarare bör förstås som en organisatorisk förmåga, där flera faktorer samverkar och tillsammans formar hur effektivt säkerhetsarbetet bedrivs i praktiken.

En viktig slutsats är att utbildning och träning, trots sin betydelse, inte är tillräckliga i sig för att skapa ett hållbart cybersäkerhetsarbete. Studien visar att sådana insatser ofta riskerar att bli ineffektiva om de genomförs som enstaka aktiviteter utan koppling till organisationens dagliga verksamhet. För att uppnå en varaktig effekt krävs att utbildning integreras i arbetsprocesser, kompletteras med praktiska moment och kontinuerligt följs upp.

Vidare framkommer att ledarskap och organisatorisk prioritering har en avgörande påverkan på cybersäkerhetsmedvetenheten. Organisationer där cybersäkerhet ses som en strategisk fråga och där ledningen aktivt engagerar sig i säkerhetsarbetet har bättre förutsättningar att skapa en stark säkerhetskultur. I motsats till detta tenderar organisationer med bristande ledningsfokus att jobba mer reaktivt, vilket ökar risken för sårbarheter och incidenter.

En ytterligare viktig slutsats är att den organisatoriska och tekniska separationen mellan IT och OT utgör en betydande utmaning inom tillverkningsindustrin. Denna uppdelning leder ofta till att säkerhetsåtgärder implementeras ojämnt, vilket skapar svaga punkter i organisationens totala säkerhetsstruktur. För att hantera detta krävs en mer integrerad syn på cybersäkerhet, där IT- och OT-miljöer betraktas som delar av ett enda sammanhängande system.

Studien visar även att små och medelstora företag står inför särskilda utmaningar relaterade till begränsade resurser. Brist på tid, kompetens och ekonomiska medel påverkar möjligheten att arbeta proaktivt med cybersäkerhet, vilket i många fall leder till att åtgärder vidtas först efter att en incident inträffat. Detta understryker behovet

av anpassade och kostnadseffektiva lösningar som är realistiska att implementera i denna typ av organisationer.

Sammanfattningsvis visar studien att cybersäkerhetsmedvetenhet i tillverkningsföretag kräver ett helhetsperspektiv där tekniska, organisatoriska och mänskliga faktorer integreras. Utan en sådan samordning riskerar säkerhetsarbetet att bli fragmenterat och ineffektivt. Studien bidrar därmed till en fördjupad förståelse av cybersäkerhetsmedvetenhet och belyser vikten av långsiktiga och integrerade strategier för att möta den ökande och föränderliga hotbilden.

6.1 Praktiska implikationer

Utifrån studiens resultat framträder flera viktiga praktiska implikationer för små och medelstora tillverkningsföretag som strävar efter att stärka sin cybersäkerhetsmedvetenhet. En viktig implikation är att cybersäkerhet inte bör betraktas som enbart en teknisk fråga, utan som en integrerad del av organisationens övergripande verksamhet. Detta innebär att säkerhetsarbetet behöver förankras på ledningsnivå och inkluderas i strategiska beslut, snarare än att hanteras isolerat inom IT-avdelningen.

Vidare visar studien att organisationer bör gå bort från att enbart genomföra enstaka utbildningsinsatser och i stället arbeta med kontinuerlig och kontextanpassad träning. För att skapa en verklig förändring i personalens beteende krävs att utbildning kopplas till medarbetarnas dagliga arbetsuppgifter och att den kompletteras med praktiska moment, såsom simuleringar av phishing-attacker eller scenariobaserade övningar. Genom att regelbundet följa upp och förstärka kunskap ökar sannolikheten att säkerhetsmedvetna beteenden faktiskt etableras i organisationen.

En annan viktig implikation är behovet av att utveckla en stark säkerhetskultur. Organisationer bör arbeta aktivt med att skapa en miljö där cybersäkerhet ses som ett gemensamt ansvar snarare än en individuell uppgift. Detta kan uppnås genom tydlig kommunikation, enkla och användarvänliga säkerhetsrutiner samt genom att uppmuntra rapportering av misstänkta incidenter utan rädsla för negativa konsekvenser. När medarbetare känner sig delaktiga och trygga i säkerhetsarbetet ökar organisationens totala motståndskraft mot cyberhot.

Resultatet pekar även på vikten av att förbättra samarbetet mellan IT och OT. För att minska säkerhetsrisker bör organisationer sträva efter att integrera dessa områden både organisatoriskt och tekniskt. Detta kan innebära att införa gemensamma säkerhetsprocesser, tydliggöra ansvarsfördelning och säkerställa att säkerhetskrav tillämpas konsekvent i hela verksamheten. En mer sammanhållen struktur bidrar till att eliminera säkerhetsluckor som annars kan uppstå mellan olika delar av organisationen.

För små och medelstora företag är det särskilt viktigt att prioritera åtgärder som ger stor effekt i förhållande till kostnad. Studien indikerar att grundläggande säkerhetsåtgärder, såsom tydliga policys, regelbunden utbildning och ökad medvetenhet, ofta kan ha större praktisk betydelse än avancerade tekniska lösningar. Genom att fokusera på dessa områden kan organisationer skapa en stabil grund för sitt cybersäkerhetsarbete, även med begränsade resurser.

Sammanfattningsvis innebär studiens resultat att SMF behöver arbeta mer systematiskt och långsiktigt med cybersäkerhetsmedvetenhet. Genom att integrera säkerhetsarbete i verksamheten, stärka säkerhetskulturen och anpassa åtgärder efter organisatoriska förutsättningar, kan företag förbättra sin förmåga att förebygga och hantera cyberhot.

Utifrån studiens resultat kan följande rekommendationer riktas till små och medelstora tillverkningsföretag som vill stärka cybersäkerhetsmedvetenheten hos produktionsnära personal:

1. **Förankra cybersäkerhet i ledningen**
   Cybersäkerhet bör behandlas som en strategisk verksamhetsfråga och inte enbart som ett tekniskt ansvar för IT-avdelningen. Ledningen behöver tydligt prioritera säkerhetsarbetet, avsätta resurser och kommunicera varför cybersäkerhet är viktigt för hela verksamheten.
2. **Inför återkommande och praktiskt anpassad utbildning**
   Utbildning bör inte genomföras som enstaka informationsinsatser, utan återkomma regelbundet och kopplas till produktionspersonalens faktiska arbetsuppgifter. Exempel kan vara korta utbildningspass, scenariobaserade övningar eller simuleringar av vanliga hot som phishing.

3. **Gör säkerhetsrutiner enkla och relevanta för produktionen**
   Policyer och riktlinjer behöver vara konkreta, tydliga och anpassade till den produktionsnära arbetsmiljön. Om rutiner upplevs som för krångliga eller tidskrävande finns en risk att de kringgås i praktiken.
4. **Stärk samarbetet mellan IT och OT**
   Små och medelstora tillverkningsföretag bör arbeta för bättre samordning mellan IT-funktioner och produktionsnära verksamhet. Gemensamma rutiner, tydlig ansvarsfördelning och regelbunden kommunikation kan minska risken för säkerhetsluckor mellan olika delar av organisationen.
5. **Börja med grundläggande och kostnadseffektiva åtgärder**
   Företag med begränsade resurser bör prioritera åtgärder som ger stor praktisk effekt, exempelvis tydliga lösenordsrutiner, grundläggande säkerhetsutbildning, enkel incidentrapportering och regelbunden uppföljning av säkerhetsbeteenden.

6.2 Vetenskapliga implikationer

Denna studie bidrar till forskningsfältet genom att belysa cybersäkerhetsmedvetenhet inom små och medelstora tillverkningsföretag ur ett helhetsperspektiv, där tekniska, organisatoriska och mänskliga faktorer integreras i analysen. Till skillnad från tidigare forskning, som ofta fokuserar på enskilda aspekter såsom utbildning eller tekniska lösningar, visar denna studie att cybersäkerhetsmedvetenhet bör förstås som något som beror på organisationens behov, kultur och arbetssätt. Detta innebär att framtida forskning kan behöva fokusera mer på hur olika delar hänger ihop, i stället för att undersöka dem var för sig.

En viktig vetenskaplig implikation är att begreppet cybersäkerhetsmedvetenhet behöver vidareutvecklas och tydliggöras. Studien visar att begreppet ofta används brett och ibland otydligt i tidigare forskning, vilket kan skapa svårigheter vid jämförelser mellan studier. Genom att lyfta samspelet mellan individ, organisation och teknik bidrar studien till en mer nyanserad förståelse av cybersäkerhetsmedvetenhet, vilket kan vara användbart i framtida forskning.

Vidare lyfter studien fram betydelsen av kontext, särskilt inom tillverkningsindustrin där integrationen mellan IT och OT skapar unika utmaningar. Detta pekar på behovet av mer kontextspecifik forskning inom cybersäkerhet, där olika branscher och

organisatoriska förutsättningar beaktas. Generella modeller och ramverk kan vara användbara, men riskerar att bli otillräckliga om de inte anpassas till specifika verksamhetsmiljöer.

Studien bidrar även genom att synliggöra små och medelstora företags perspektiv, en grupp som ofta är underrepresenterad i cybersäkerhetsforskning. Eftersom dessa företag utgör en stor del av industrin och samtidigt har andra förutsättningar än större organisationer, är det viktigt att forskning i högre grad inkluderar denna kontext. Detta gäller särskilt frågor relaterade till resursbegränsningar, kompetensbrist och praktisk implementering av säkerhetsåtgärder.

Studien visar också att cybersäkerhetsmedvetenhet behöver förstås ur flera olika perspektiv. Det handlar inte bara om teknik utan även om hur organisationen fungerar och hur människor tänker och agerar i sitt dagliga arbete. Därför behöver forskning om cybersäkerhet använda kunskap från flera områden, till exempel informationssystem, organisationsforskning, beteendevetenskap och säkerhetsstudier.

Sammanfattningsvis bidrar denna studie till en fördjupad och mer integrerad förståelse av cybersäkerhetsmedvetenhet. Genom att lyfta fram komplexiteten i fenomenet och betona vikten av kontext och samspel mellan olika faktorer skapas en grund för vidare teoretisk utveckling inom området.

6.3 Vidare forskning

Denna studie har bidragit till en ökad förståelse av cybersäkerhetsmedvetenhet inom små och medelstora tillverkningsföretag, men identifierar samtidigt flera områden där ytterligare forskning är nödvändig. Ett av dessa behov är att komplettera litteraturbaserade studier med empiriska undersökningar. Genom att exempelvis genomföra intervjuer, fallstudier eller observationer i organisationer kan framtida forskning få en djupare inblick i hur cybersäkerhetsmedvetenhet faktiskt tar sig uttryck i praktiken. Detta skulle möjliggöra en bättre förståelse för skillnaden mellan teoretiska modeller och verkliga arbetssätt.

Vidare finns ett behov av att utveckla och testa konkreta metoder för att stärka cybersäkerhetsmedvetenhet. Även om studien identifierar viktiga faktorer, såsom utbildning, ledarskap och organisatorisk kultur, saknas det i stor utsträckning forskning som empiriskt utvärderar vilka åtgärder som är mest effektiva i olika kontexter. Framtida studier skulle därför kunna fokusera på att designa och utvärdera

specifika insatser, exempelvis utbildningsprogram, simuleringar eller tekniska stödverktyg, för att undersöka deras faktiska påverkan.

Ett annat relevant forskningsområde är hur produktionsnära personal påverkas av kopplingen mellan IT och OT. I denna studie har IT/OT identifierats som en viktig del av produktionsmiljön, eftersom produktionsnära personal ofta arbetar i miljöer där digitala system, uppkopplad utrustning och fysiska produktionsprocesser samverkar. Framtida forskning skulle därför kunna undersöka hur cybersäkerhetsmedvetenhet hos produktionsnära personal påverkas av denna tekniska och organisatoriska miljö, samt hur utbildning, rutiner och kommunikation kan anpassas för att stödja säkra arbetssätt i sådana produktionsmiljöer.

Det finns även behov av forskning som specifikt fokuserar på små och medelstora företags förutsättningar. Dessa organisationer skiljer sig från större företag när det gäller resurser, kompetens och organisatorisk struktur, vilket påverkar deras möjligheter att implementera cybersäkerhetsåtgärder. Framtida forskning skulle därför kunna utveckla anpassade ramverk och riktlinjer som tar hänsyn till dessa begränsningar och samtidigt är praktiskt genomförbara.

Slutligen är det relevant att undersöka hur den ökande digitaliseringen och utvecklingen inom Industry 4.0 påverkar cybersäkerhetsmedvetenhet. Nya teknologier, såsom uppkopplade produktionssystem och IoT-enheter, skapar både möjligheter och nya säkerhetsrisker. Detta innebär att cybersäkerhetsarbete behöver anpassas till en snabbt föränderlig teknisk miljö, vilket i sin tur ställer nya krav på både organisationer och forskning.

Sammanfattningsvis visar denna studie att cybersäkerhetsmedvetenhet är ett dynamiskt och komplext område där det fortfarande finns betydande kunskapsluckor. Genom fler praktiska studier, utveckling av bättre arbetsmetoder och större fokus på olika typer av verksamheter kan framtida forskning bidra till både ökad förståelse och bättre arbetssätt inom cybersäkerhet.

7 Referenser

Akter, S., Uddin, M. R., Sajib, S., Lee, W. J. T., Michael, K., & Hossain, M. A. (2025). Reconceptualizing cybersecurity awareness capability in the data-driven digital economy. Annals of Operations Research, 350(2), 673–698. https://doi.org/10.1007/s10479-022-04844-8

Alqudhaibi, A., Albarrak, M., Jagtap, S., Williams, N., & Salonitis, K. (2024a). Securing Industry 4.0: Assessing cybersecurity challenges and proposing strategies for manufacturing management. Cyber Security and Applications, 3, Article 100067. https://doi.org/10.1016/j.csa.2024.100067

Alqudhaibi, A., Krishna, A., Jagtap, S., Williams, N., Afy-Shararah, M., & Salonitis, K. (2024b). Cybersecurity 4.0: Safeguarding trust and production in the digital food industry era. Discover Food, 4(1). https://doi.org/10.1007/s44187-023-00071-7

Alzahrani, L., & Seth, K. P. (2021). The impact of organizational practices on information security management performance. Information, 12(10), 398. https://doi.org/10.3390/info12100398

Amirova, A., Aldasheva, L., & Abdiraman, A. (2025). Securing the Industrial Internet of Things: Threats, Vulnerabilities, and Recommendations. Procedia Computer Science, 272, 625–630. https://doi.org/10.1016/j.procs.2025.10.258

Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: Evaluating the cybersecurity capacity of the industrial workforce. Journal of Systems and Information Technology, 21(1), 2–35. https://doi.org/10.1108/JSIT-02-2018-0028

Arroyabe, M. F., Arranz, C. F. A., Arroyabe, I. F. de, & Arroyabe, J. C. F. de. (2024). The effect of IT security issues on the implementation of Industry 4.0 in SMEs: Barriers and challenges. Technological Forecasting and Social Change, 199, 123051. https://doi.org/10.1016/j.techfore.2023.123051

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brunken, L., Schöps, M., Buckmann, A., Meißner, F., & Sasse, M. A. (2025). Noise and Stress Don't Help With Learning: A Qualitative Study to Inform Design of Effective Cybersecurity Awareness in Manufacturing Environments. Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security, 633–647. https://doi.org/10.1145/3719027.3744880

Button, D., Ophoff, J., Irons, A., & McDonald, S. (2024). "Probably put some sort of fear in": Investigating the role of heuristics in cyber awareness messaging for small to medium sized enterprises. In IFIP Advances in Information and Communication Technology. https://doi.org/10.1007/978-3-031-72563-0_8

Chaudhary, S., & Gkioulos, V., & Goodman, D. (2023a). Cybersecurity awareness for small and medium-sized enterprises (SMEs): Availability and scope of free and inexpensive awareness resources. In Lecture Notes in Computer Science. https://doi.org/10.1007/978-3-031-25460-4_6

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2023b). A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises. Computer Science Review, 50, 100592. https://doi.org/10.1016/j.cosrev.2023.100592

Chidukwani, A., Zander, S., & Koutsakis, P. (2024). Cybersecurity preparedness of small-to-medium businesses: A Western Australia study with broader implications. Computers & Security, 145, 104026. https://doi.org/10.1016/j.cose.2024.104026

Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. Computers in Industry, 137, Article 103614. https://doi.org/10.1016/j.compind.2022.103614

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. The Geneva Papers on Risk and Insurance - Issues and Practice, 47(3), 698–735. https://doi.org/10.1057/s41288-022-00266-6

Cuellar, N. G., Whisenant, D., & Stanton, M. P. (2015). Hypnic jerks: A scoping literature review. Sleep Medicine Clinics, 10(3), 393–401. https://doi.org/10.1016/j.jsmc.2015.05.010

Erdogan, G., Halvorsrud, R., Boletsis, C., Tverdal, S., & Pickering, J. B. (2023). Cybersecurity awareness and capacities of SMEs. In International Conference on Information Systems Security and Privacy. https://doi.org/10.5220/0011609600003405

García Arellano, F. J., Donoso Barraza, ítalo, Flores Bustos, A., Pon Soto, C., Flores Fonseca, V., & Martínez-Peláez, R. (2024). Examining cybersecurity culture in Leon city organizations: Insights from 2022. Ingeniare : Revista Chilena de Ingenieria, 32, 1–16. https://doi.org/10.4067/S0718-33052024000100211

Giriraj, A., Haggag, S., & Haggag, H. (2022). Human centric framework for customising and producing effective cybersecurity training materials. In Proceedings of the IWESQ 2022 & APSEDEI 2022 (pp. 69–77). CEUR-WS. https://ceur-ws.org/Vol-3356/paper-11.pdf

Hadie, S. N. H. (2024). ABC of a scoping review: a simplified JBI scoping review guideline. Education in Medicine Journal, 16(2), 185–197. https://doi.org/10.21315/eimj2024.16.2.14

Ibrahim, A., Rehman, S. U., Williams, P. A. H., & Jolfaei, A. (2025). Introducing CHARM: a Practical Cyber Hygiene Awareness Rating Metric for MSMEs. IEEE Transactions on Consumer Electronics, 1–1. https://doi.org/10.1109/TCE.2025.3642985

Johansson, K., Paulsson, T., Bergström, E., & Seigerroth, U. (2022). Improving cybersecurity awareness among SMEs in the manufacturing industry. Advances in Transdisciplinary Engineering. https://doi.org/10.3233/ATDE220140

Khando, K., Gao, S., Islam, M. S., & Salman, A. (2021). Enhancing employees' information security awareness in private and public organisations: A systematic literature review. Computers & Security, 106, 102267. https://doi.org/10.1016/j.cose.2021.102267

Kitchenham, B. (2004). Procedures for Performing Systematic Reviews. Keele, UK, Keele University, 33(2004), 1-26. https://www.researchgate.net/publication/228756057_Procedures_for_Performing_Systematic_Reviews

Mani, V., Delgado, C., Hazen, B., & Patel, P. (2017). Mitigating supply chain risk via sustainability using big data analytics: Evidence from the manufacturing supply chain. Sustainability, 9(4), 608. https://doi.org/10.3390/su9040608

Mmango, N., & Gundu, T. (2023). Cyber resilience in the entrepreneurial environment: A framework for enhancing cybersecurity awareness in SMEs. In ICECET 2023. https://doi.org/10.1109/ICECET58911.2023.10389226

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. International Journal of Qualitative Methods, 16(1), 1–13. https://doi.org/10.1177/1609406917733847

Oroni, C. Z., & Xianping, F. (2023). Structural evaluation of management capability and the mediation role of cybersecurity awareness towards enterprise performance. Journal of Data, Information and Management, 5, 223–240. https://doi.org/10.1007/s42488-023-00108-7

Panko, M., Šafár, L., & Mešťan, M. (2025). Small Firms, Big Threats: Cybersecurity Research and the Role of Public Policy in the SME Sector. Central European Journal of Public Policy, 19(2), 87–110. https://doi.org/10.2478/cejpp-2025-0010

Ponsard, C., & Grandclaudon, J. (2020). Guidelines and tool support for building a cybersecurity awareness program for SMEs. In Communications in Computer and Information Science. https://doi.org/10.1007/978-3-030-49443-8_16

Rawindaran, N., Jayal, A., & Prakash, E. (2025). Cybersecurity framework: Addressing resiliency in Welsh SMEs for digital transformation and Industry 5.0. Journal of Cybersecurity and Privacy, 5(2), 17. https://doi.org/10.3390/jcp5020017

Rubinstein, M. L., & Parrott, J. S. (2021). Scoping reviews of the microbiology literature: Methods and payoffs. Clinical Microbiology Newsletter, 43(15), 127–133. https://doi.org/10.1016/j.clinmicnews.2021.07.001

Šafár, L., Pekarčik, M., Morawiec, P., Rutecka, P., & Wieczorek-Kosmala, M. (2025). Mapping Cybersecurity in SMEs: The role of ownership and firm characteristics in the Silesian Region of Poland. Information, 16(7), 590. https://doi.org/10.3390/info16070590

Schuh, G., Hicking, J., Engländer, J., Zeller, V., & Perau, M. (2020). Helping companies to evaluate their status quo in information security with a serious gaming-based economical quantification approach. Procedia CIRP, 93, 150–155. https://doi.org/10.1016/j.procir.2020.05.196

Stentoft, J., Peressotti, M., Mayer, P., Wickstrøm, K. A., Schmitt, O., Keating, V. C., Theussen, A., Tumchewics, L. A., & Kankam-Boateng, J. (2025). The relationship between cybersecurity awareness, cybersecurity supply chain risk management and firm performance. Supply Chain Management, 30(5), 497–517. https://doi.org/10.1108/SCM-11-2024-0765

Vetenskapsrådet. (2024). God forskningssed (Reviderad utg.). https://www.vr.se/analys/rapporter/vara-rapporter/2024-10-02-god-forskningssed-2024.html

Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., & Wesslén, A. (2012). Experimentation in Software Engineering. Berlin/Heidelberg: Springer. https://doi.org/10.1007/978-3-642-29044-2

Wong, L.-W., Lee, V.-H., Tan, G. W.-H., Ooi, K.-B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. International Journal of Information Management, 66, 102520. https://doi.org/10.1016/j.ijinfomgt.2022.102520

Zhou, X., Jin, Y., Zhang, H., Li, S., & Huang, X. (2016). A Map of Threats to Validity of Systematic Literature Reviews in Software Engineering. Proceedings of the 23rd Asia-Pacific Software Engineering Conference (APSEC). https://doi.org/10.1109/APSEC.2016.031