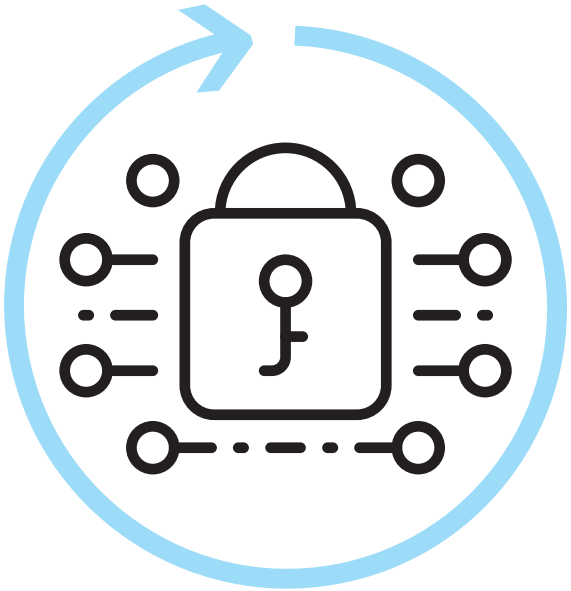
CYBERSIKKERHED OG FORRETNINGSKONTINUITET



Cybersikkerhed i praksis: Indsigter fra danske produktionsvirksomheder

Jan Stentoft, Ole Stegmann Mikkelsen, Kent Adsbøll Wickstrøm, Vincent Keating, Louise Tumchewics, Amelie Theussen, Marco Peressotti, Peter Mayer og Judith Kankam-Boateng

April 2026

INDUSTRIENS FOND

SDU Syddansk Universitet

FORSVARSAKADEMIET

Cybersikkerhed i praksis:
Indsigter fra danske produktionsvirksomheder

ISBN: 97887-85464-11-8

Korrektur og opsætning:
Tina Højrup Kjær, Tekst og Web

Rapporten er et delresultat i projektet
”Cybersikkerhed og Forretningskontinuitet”,
der gennemføres med økonomiske midler fra Industriens Fond.

Projektets hjemmeside er:
www.cyber-smv.dk

Forskningsprojektet gennemføres af forskere fra Institut for
Erhverv og Bæredygtighed, SDU, Center for War Studies, SDU,
Institut for Matematik og Datalogi, SDU samt Forsvarsakademiet.

INDHOLDSFORTEGNELSE


Survey
New Tab
http://www.
Survey
Customer Statisfaction Survey
1. Please tick a box on each line to indicate how much you rate level of service
Excellent
Good
Average
Poor
a. Location
b. Comfort
c. Facilities
d. Staff
e. Value for money
What can we do to improve service?
Submit
Terms of Use
Privacy Policy
Copyright
Contact
Page Loaded

Resumé

Denne rapport behandler resultaterne af en landsdækkende spørgeskemaundersøgelse, der har fokus på danske små og mellemstore produktionsvirksomheders praksis med cybersikkerhed. I alt har 155 virksomheder deltaget i undersøgelsen. Specifikt søger rapporten svar på 11 overordnede spørgsmål:

1. I hvilket omfang opfattes cybersikkerhed som teknisk komplekst?
2. Hvad er den konkrete praksis med IT-/OT-integration?
3. I hvilket omfang har virksomhederne oplevet cyberangreb?
4. I hvilket omfang møder SMV'erne krav til cybersikkerhed fra forskellige interessenter?
5. I hvilket omfang er virksomhederne underlagt NIS 2 compliancekrav?
6. I hvilket omfang stiller man krav til cybersikkerhed mod kunder og leverandører?
7. I hvilket omfang har virksomhederne fokus på cybersikker supply chain risk management?
8. I hvilket omfang opfanger SMV'erne muligheder med cybersikkerhed, hvordan udnyttes mulighederne, og hvordan ændrer og tilpasser SMV'erne sig (cybersikre dynamiske kapabiliteter)?
9. I hvilket omfang er SMV'erne påvirket af geopolitiske markedskræfter?
10. I hvilket omfang opfanger SMV'erne muligheder med geopolitiske markedspåvirkninger, hvordan udnyttes mulighederne, og hvordan ændrer og tilpasser SMV'erne sig (dynamiske kapabiliteter for geopolitiske markedspåvirkninger)?
11. I hvilket omfang arbejder SMV'erne med geopolitisk risikostyring?

Opfattelser af cybersikkerhed som teknisk komplekst

Respondenterne oplever ikke høj intern teknisk kompleksitet i opfattelsen af cybersikkerhed. Alle udsagn scorer omkring 2 på en 5-punkts Likert-skala (1,62 - 2,12) svarende til 'i mindre grad', om end der kan være variationer bag gennemsnittene. Samlet set indikerer tallene et relativt tilfredsstillende niveau, både hvad angår rettidig installation af sikkerhedsopdateringer (et gennemsnit på 1,62), overblik over tilsluttede enheder (et gennemsnit på 2,03) samt tilpasning af cybersikkerhed til OT-systemer (et gennemsnit på 2,12).

Praksis med IT-/OT-integration

Respondenterne angiver, at de i nogen til høj grad har styr på integrationen mellem IT og OT, særligt når det gælder overblik over aktiver, sikre kommunikationsprotokoller og netværkssegmentering, som alle fremstår som tydelige styrker.

Cyberangreb

25 % af respondenterne svarer, at de har været udsat for cyberangreb indenfor de seneste par år.

Krav til cybersikkerhed fra interessenter

Krav til cybersikkerhed fra virksomhedens interessenter drives primært af ledelsen og i mindre grad af bestyrelsen, hvor sidstnævnte kun har øget sit fokus marginalt siden 2024. Dette tyder på et fortsat begrænset pres fra bestyrelsesniveau trods stigende opmærksomhed i omverdenen.

NIS 2 compliancekrav

22 % af respondenterne er omfattet af NIS 2-direktivet, 67 % er ikke, mens 11 % angiver, at de ikke ved det.

Krav til cybersikkerhed mod kunder og leverandører

Virksomhederne stiller kun i begrænset omfang cybersikkerhedskrav i deres aftaler, både over for leverandører og kunder, hvilket peger på en lav modenhed i håndteringen af cybersikkerhed i værdikæden.

Cybersikker supply chain risk management

Respondenterne opnår overraskende lave gennemsnitsværdier for deres vurdering af SMV'ernes brug af ti praksisser indenfor cybersikker supply chain risk management med gennemsnitsværdier fra 2,86 som det højeste til 1,82. Det samlede resultat peger på et lavt fokus på cybersikker supply chain risk management og dermed et stort udviklingsbehov i virksomhederne.

Cybersikre dynamiske kapabiliteter

Resultaterne viser et bekymrende lavt niveau af cybersikre dynamiske kapabiliteter blandt SMV'er, med gennemsnit på 2,0 for sensing, 1,94 for seizing

og 2,4 for transforming. Dette indikerer en begrænset evne til at identificere, udnytte og tilpasse sig cyberrelaterede muligheder og trusler, hvilket øger risikoen for forsinkede reaktioner og svækker virksomhedernes langsigtede robusthed.

Geopolitiske markedskræfter

Respondenterne oplever generelt en påvirkning fra geopolitiske markedskræfter i nogen til lav grad. Den største påvirkning ses i øget bekymring for IT-sikkerhed som følge af statssponsorerede cyberangreb (med et gennemsnit på 2,98) samt krige og uligheder (med et gennemsnit på 2,90), mens nye EU-sanktioner vurderes at have den laveste påvirkning på usikkerhed omkring kontrakter og betalingsstrømme (med et gennemsnit på 2,25).

Dynamiske kapabiliteter for geopolitiske markedspåvirkninger

Resultaterne viser, at produktions-SMV'er generelt har lave niveauer af dynamiske kapabiliteter i forhold til geopolitiske markedspåvirkninger med gennemsnitsværdier på 2,04 for sensing, 2,36 for seizing og 2,15 for transforming. Dette indikerer et begrænset fokus på både at identificere, udnytte og tilpasse sig geopolitiske muligheder.

Praksis med geopolitisk risikostyring

Arbejdet med geopolitisk risikostyring er relativt svagt med gennemsnitlige vurderinger mellem 1,67 og 2,81. Samlet peger resultaterne på et behov for, at SMV'er styrker deres strategiske og organisatoriske håndtering af geopolitik.

Forord

Denne rapport kortlægger, hvordan danske små og mellemstore produktionsvirksomheder arbejder med cybersikkerhed i praksis, og sammenholder resultaterne med en tilsvarende undersøgelse gennemført i 2023/2024 (Stentoft et al., 2024). Formålet er at give et aktuelt billede af virksomhedernes modenhed, udfordringer og udvikling over tid – samt at identificere områder, hvor der er behov for en styrket indsats.

Cybersikkerhed er ikke kun et IT-anliggende. For produktionsvirksomheder er det tæt forbundet med drift, leveringssikkerhed og konkurrenceevne.

Mange produktionsvirksomheder er i dag afhængige af ERP-systemer, produktionsstyring (MES), automatiserede maskiner og digitale leverandørportaler. Et ransomware-angreb kan lamme adgangen til disse systemer. Konkrete konsekvenser kan være:

- Produktionslinjer, der står stille i flere dage
- Manglende adgang til styklister, tegninger og produktionsdata
- Forsinkede leverancer og bodskrav fra kunder

Produktions-SMV'er indgår ofte i komplekse forsyningskæder. Hvis en hacker får adgang til en mindre virksomheds systemer, kan det potentielt bruges som springbræt til større industrivirksomheder. Derfor stiller flere større kunder i dag krav om dokumenteret cybersikkerhed f.eks. i forbindelse med:

- Leverandøraudits
- Kontraktfornyelser
- Adgang til fælles digitale platforme

Produktionsvirksomheder håndterer ofte:

- Konstruktionsfiler og tekniske tegninger
- Prototypedata
- Kundespecifikke løsninger
- Prisstrukturer og tilbud

Hvis disse oplysninger kompromitteres, kan det føre til tab af konkurrencefordel, kopiering af produkter eller brud på fortrolighedsaftaler. Det kan i værste fald underminere virksomhedens markedsposition.

Kravene til datasikkerhed og dokumentation er skærpet markant de seneste år. Overtrædelse af regler om databeskyttelse (f.eks. GDPR) kan medføre betydelige bøder og omdømmemæssige konsekvenser. Samtidig bevæger reguleringen sig i retning af øgede krav til cybersikkerhed i forsyningskæder og kritiske sektorer. For mange produktions-SMV'er betyder det, at cybersikkerhed i stigende grad bliver et compliancekrav – ikke et frivilligt tilvalg.

Digitalisering af produktion, fjernadgang til maskiner, cloud-baserede systemer og online samarbejdsplatforme har skabt effektivitet – men også flere potentielle indgange for cyberangreb. En kompromitteret medarbejderkonto eller utilstrækkeligt sikret fjernadgang kan give uvedkommende adgang til produktionsmiljøet. Derfor skal cybersikkerhed tænkes ind som en integreret del af virksomhedens operationelle strategi og risikostyring.

Investering i cybersikkerhed handler i sidste ende om at sikre stabil drift. En robust sikkerhedsindsats øger virksomhedens modstandsdygtighed og evne til hurtigt at genoptage produktionen efter et angreb. Det reducerer risikoen for langvarige driftsforstyrrelser og styrker tilliden hos kunder, samarbejdspartnere og finansielle aktører. Der er derfor stærke argumenter for, at produktions-SMV'er arbejder systematisk med cybersikkerhed – ikke mindst i et forsyningskædeperspektiv, hvor én virksomheds sårbarhed kan få konsekvenser for mange andre.

Stor tak til alle respondenter, som har bidraget med tid og indsigter. Jeres deltagelse er afgørende for at skabe et solidt vidensgrundlag om cybersikkerhed i danske produktions-SMV'er. Tak til Industriens Fond for den økonomiske støtte til projektet Cybersikkerhed og Forretningskontinuitet (www.cyber-smv.dk), som denne spørgeskemaundersøgelse indgår i.

Endelig tak til kommunikationskonsulent Tina Højrup Kjær, Tekst og Web, for korrekturlæsning, redigering og opsætning.

April 2026

Jan Stentoft, Ole Stegmann Mikkelsen, Kent Adsbøll Wickstrøm, Vincent Keating, Louise Tumchewics, Amelie Theussen, Marco Peressotti, Peter Mayer og Judith Kankam-Boateng.

1. Introduktion

1.1 Baggrund

Rammevilkårene for danske produktions-SMV'er har ændret sig markant de seneste år. Hvor virksomheder tidligere opererede i en relativt stabil international kontekst, er de i dag en del af en mere usikker og geopolitisk kompleks virkelighed. Øgede stormagtskonflikter, strategisk fokus på kritisk infrastruktur og en mere fragmenteret verdenshandel påvirker direkte de danske produktionsvirksomheders risikobillede. Samtidig har den digitale økonomi fundamentalt ændret måden, produktionsvirksomheder driver forretning på. Digitalisering, automatisering og globalt integrerede forsyningskæder har skabt nye muligheder for effektivitet og vækst – men også nye sårbarheder.

Allianz Risk Barometer 2026 (Allianz, 2026) viser, at cyberhændelser fortsat er den største globale forretningsrisiko for virksomheder. Ifølge rapporten har cyberrisici – herunder ransomware, databrud og IT-nedbrud – været den vigtigste bekymring for virksomheder i fem år i træk og blev i 2026 valgt af 42 % af respondenterne som den største trussel. Samtidig er kunstig intelligens (AI) den hurtigst stigende risiko. Den er rykket fra en 10. plads i 2025 til 2. pladsen i 2026, hvilket afspejler både de muligheder og de nye operationelle, juridiske og omdømmemæssige risici, som AI skaber for organisationer.

Geopolitik, eksport og forsyningskæder

Mange danske produktions-SMV'er er afhængige af eksport og internationale leverandørrelationer. Geopolitiske spændinger, handelsrestriktioner og sanktioner kan derfor have direkte konsekvenser for deres markedsadgang og leverancesikkerhed. I denne kontekst er cybersikkerhed blevet et strategisk anliggende. Cyberangreb anvendes i stigende grad som redskab i både statslige og kriminelle konflikter. Produktionsvirksomheder kan blive ramt direkte – eller indirekte via deres position i forsyningskæden. Et cyberangreb mod én virksomhed kan hurtigt sprede sig til samarbejdspartnere og kunder. Dermed bliver cybersikkerhed ikke blot et internt anliggende, men et fælles ansvar i supply chain-netværket.

Øget digital afhængighed – øget eksponering

Danske produktions-SMV'er er i dag dybt afhængige af IT-systemer til:

- Produktionsstyring og automatisering
- Ordrebehandling og ERP-systemer
- Udveksling af data med kunder og leverandører

- Fjernadgang til maskiner og service
- Cloud-baserede samarbejdsplatforme

Digitaliseringen har gjort processer hurtigere, billigere og mere integrerede. Men den har samtidig øget virksomhedernes angrebsflade betydeligt (Colicchia et al., 2019). Ransomware, industrispionage, tyveri af immaterielle rettigheder og sabotage er ikke længere hypotetiske risici. Flere danske virksomheder – både store koncerner og SMV'er – har oplevet angreb, der har lammet produktionen og forhindret levering af varer og ydelser i dage eller uger.

Konsekvenserne rækker ud over den enkelte virksomhed:

- Kunder kan ikke opretholde deres egen produktion.
- Leverancer forsinkes gennem hele værdikæden.
- Tillid og omdømme svækkes.

For en mindre produktionsvirksomhed kan tab af troværdighed over for nøglekunder være mere skadeligt end det direkte økonomiske tab.

Regulering og skærpede krav

Den regulatoriske udvikling går i retning af strengere krav til cybersikkerhed. EU's NIS 2-direktiv udvider kredsen af virksomheder, der omfattes af krav om risikostyring, dokumentation og ledelsesansvar. For mange danske produktions-SMV'er betyder det, at cybersikkerhed i stigende grad bliver et compliance- og ledelsesanliggende. Manglende overholdelse kan medføre sanktioner, men endnu vigtigere kan det føre til tab af forretningsmuligheder, hvis virksomheden ikke kan dokumentere et tilstrækkeligt sikkerhedsniveau over for kunder og samarbejdspartnere.

Cybersikkerhed som konkurrenceparameter

Cybersikkerhed bør derfor ikke betragtes som en ren omkostning, men som en strategisk investering. På linje med kvalitet, miljøhensyn og social ansvarlighed er et dokumenteret højt sikkerhedsniveau i stigende grad en forudsætning for at være en attraktiv og troværdig samarbejdspartner. Et styrket fokus på cybersikkerhed indebærer blandt andet:

- Klar adgangsstyring og stærk autentificering
- Systematisk data-backup og beredskabsplaner
- Opdatering og certificering af hard- og software
- Firewall- og netværkssikring
- Overholdelse af relevante standarder og reguleringer
- Leverandøraudits og risikovurderinger i forsyningskæden
- Overvågning af systemer og håndtering af hændelser i realtid

Nyere forskning peger på, at der fortsat er behov for øget viden og modenhed inden for cybersikkerhed blandt danske produktions-SMV'er – særligt

i et forsyningskædeperspektiv (Stentoft et al., 2025). Der er derfor et klart behov for at styrke virksomhedernes indsigt, praksis og strategiske tilgang til cybersikkerhed. Cybersikkerhed og konkurrenceevne hænger tæt sammen. I en mere usikker og digitaliseret verden er robusthed ikke blot et spørgsmål om risikominimering – men om langsigtet markedsposition. Chadge et al. (2020) fremhæver, at eksisterende forskning i høj grad har fokuseret på teknologiske aspekter af cybersikkerhed, mens menneskelige og organisatoriske faktorer i forsyningskæder er mindre undersøgt. Derudover efterlyser de også behov for forskning i samarbejde og informationsdeling mellem virksomheder i forsyningskæder, da cyberrisici ofte opstår på tværs af virksomheder. Endelig understreges vigtigheden af at udvikle integrerede modeller og governance-mekanismer, der kombinerer teknologiske, organisatoriske og supply chain-perspektiver for bedre at kunne styrke cyberresiliens i globale forsyningsnetværk (Chadge et al., 2020).

1.2 Formål med undersøgelsen

Formålet med undersøgelsen er *at afdække danske små og mellemstore produktionsvirksomheders praksis med cybersikkerhed* med henblik på at analysere, om virksomhedernes praksis er blevet styrket sammenholdt med 2024-undersøgelsen (Stentoft et al., 2024).

2. Teoretisk referenceramme

Dette afsnit giver en kortfattet beskrivelse af de centrale teoriområder, der ligger til grund for undersøgelsen. Afsnittet er delt op i fem underafsnit: 1) supply chain management, 2) karakteristika ved SMV'er, 3) cybersikkerhed, 4) geopolitik og 5) dynamiske kapabiliteter.

2.1 Supply chain management

Supply chain management (SCM) handler i praksis om at få hverdagen til at fungere på tværs af leverandører, produktion og kunder. Det drejer sig om at sikre, at materialer leveres til tiden, at information flyder korrekt mellem parterne, og at betalinger og fakturering håndteres effektivt. For en dansk produktions-SMV kan SCM eksempelvis omfatte:

- Indkøb af råvarer og komponenter fra internationale leverandører
- Planlægning af produktion via ERP- og produktionsstyringssystemer
- Udveksling af forecasts og ordrebekræftelser med kunder
- Koordinering med logistikpartnere om levering
- Elektronisk fakturering og betalingsstyring

En definition af SCM er:

> "*... transformation af efterspørgselsinformation til fysisk levering af varer og serviceydelser. Forsyningskædeledelse starter med kunders behov for varer og serviceydelser, som skaber efterspørgsel for varer og serviceydelser bagud i forsyningskæder og netværk. Nøglefokus er rettet mod materiale-, informations-, og finansielle flows, som udfolder sig i forretningsprocesser. Ledelsesidealet er at skabe differentieret ledelse af intra- og interorganisatoriske aktiviteter og processer med det formål at opfylde kundernes behov ved at levere varer og serviceydelser fra udvindelsestidspunktet til forbrugstidspunktet til de laveste samlede omkostninger, til den rette tid og til det højeste påkrævede kvalitetsniveau.*" (Stentoft et al., 2018).

SCM tager udgangspunkt i kundens behov. Hvis en større kunde eksempelvis ændrer sit forecast eller afgiver en hasteordre, påvirker det produktionsplanlægning, indkøb og leverancer bagud i kæden. Det betyder, at produktions-SMV'er er afhængige af præcise og rettidige data. Hvis ordresystemet kompromitteres, eller hvis data manipuleres, kan det føre til fejlleverancer, overproduktion eller produktionsstop.

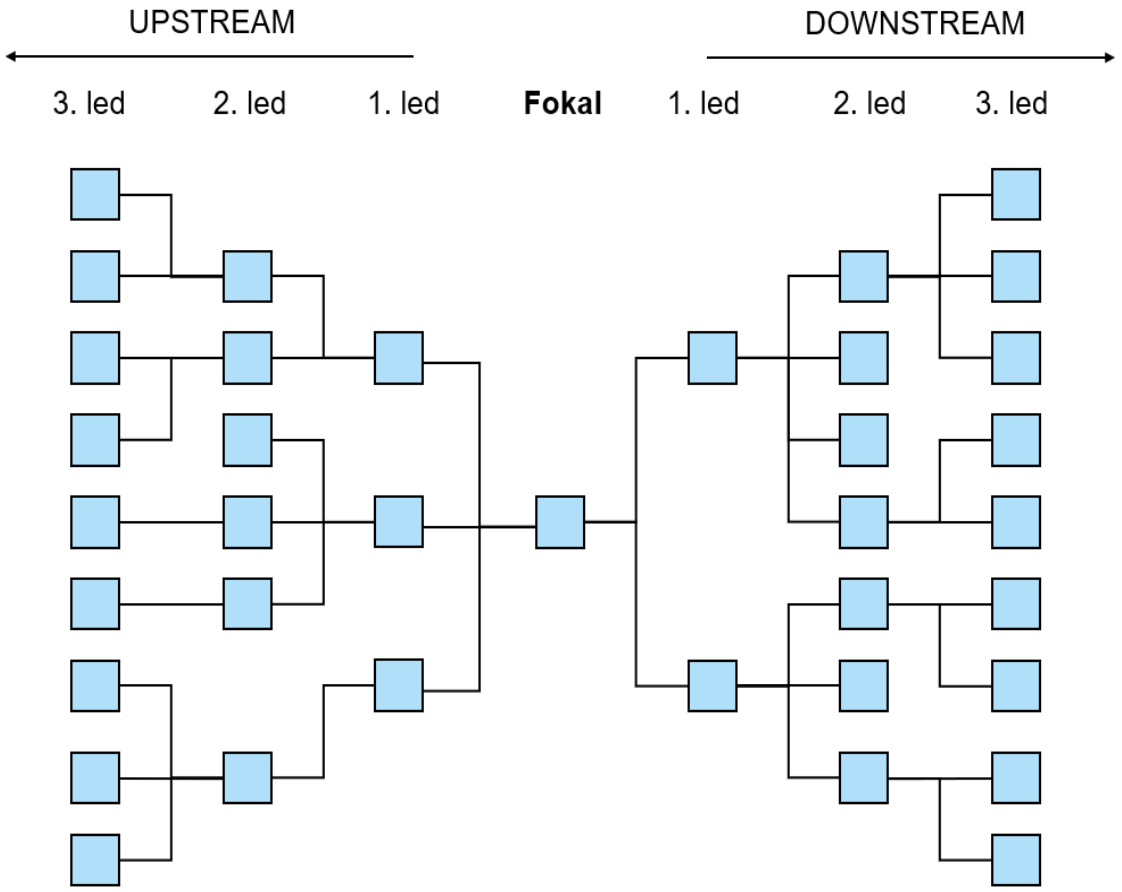
Virksomheder samarbejder ikke ens med alle leverandører og kunder. En kritisk leverandør af specialkomponenter kræver typisk tættere koordinering og større gennemsigtighed end en standardleverandør. Det samme gælder cybersikkerhed. En SMV bør stille højere sikkerhedskrav til:

- Leverandører med adgang til virksomhedens systemer
- IT-servicepartnere med fjernadgang til produktionsudstyr
- Kunder, der integrerer direkte i virksomhedens ERP-system

Hvis en ekstern serviceleverandør får kompromitteret sine loginoplysninger, kan det give adgang direkte ind i produktionsmiljøet. Derfor er leverandørstyring også en del af cybersikkerheden.

Produktions-SMV'er fungerer ofte som knudepunkt mellem upstream-leverandører og downstream-kunder (se figur 2.1).

Figur 2.1: Forsyningskædernes netværksstruktur



Kilde: Stentoft et al. (2018, p. 39).

Upstream-risici kan f.eks. være:

- En leverandør sender inficerede filer (f.eks. tegninger eller softwareopdateringer)
- En kompromitteret leverandørkonto bruges til svindel med betalingsoplysninger

Downstream-risici kan f.eks. være:

- En kundeportal kompromitteres, så ordredata lækkes
- Produktionsdata eller kundespecifikke tegninger stjæles og misbruges

Et ransomware-angreb i én virksomhed kan forplante sig gennem fælles systemintegrationer og påvirke hele værdikæden. Hvis en produktions-SMV ikke kan levere, kan kundens produktion også gå i stå. I praksis betyder det, at cybersikkerhed bør integreres i SCM-arbejdet på linje med kvalitet, leveringstid og omkostningsstyring. Det kan eksempelvis indebære:

- Krav om to-faktor-autentifikation for eksterne samarbejdspartnere
- Gennemførelse af leverandøraudits med fokus på IT-sikkerhed
- Segmentering af netværk mellem kontor-IT og produktions-IT
- Regelmæssig backup af produktionsdata og test af gendannelsesprocedurer
- Klare beredskabsplaner for håndtering af cyberhændelser

For en produktions-SMV handler det i sidste ende om at sikre stabil drift og bevare kundernes tillid. En stærk position i forsyningskæden forudsætter ikke alene høj kvalitet og leveringssikkerhed – men også dokumenteret cybersikkerhed. Cybersikkerhed er derfor ikke blot et teknisk spørgsmål. Det er en forudsætning for at være en robust og attraktiv samarbejdspartner i moderne forsyningsnetværk.

2.2 Karakteristika ved SMV'er

SMV'er (små og mellemstore virksomheder) spiller en central rolle i den samfundsøkonomiske udvikling. I OECD-landene udgør de 99 % af alle virksomheder (OECD, 2023, p. 9). Ifølge Europa-Kommissionen beskæftiger SMV'er mellem 10 og 250 medarbejdere, har en årlig omsætning på op til 50 mio. EUR og/eller en balancesum på op til 43 mio. EUR (European Commission, 2020). SMV'ernes betydning er ikke kun numerisk.

Sammenlignet med store virksomheder opererer SMV'er under andre strukturelle vilkår. De har typisk færre menneskelige, finansielle og teknologiske ressourcer (Forsman, 2008; Zach et al., 2014) og er ofte mere eksponeret for ekstern usikkerhed (Storey, 1994, p. 74). De mangler i mange tilfælde be-

slutningsrelevant information, har begrænsede ledelsesressourcer og arbejder med strammere likviditet (Pal et al., 2014).

I praksis betyder det, at ledelsen – ofte ejeren eller direktøren – er dybt involveret i den daglige drift. Strategiske initiativer må ofte vige for akutte driftsopgaver, og en hverdag præget af "brandslukning" kan begrænse fokus på langsigtet udvikling (Kull et al., 2018). Flere studier peger desuden på, at SMV'er ofte har en reaktiv tilgang til strategi og begrænset erfaring med implementering af nye teknologier (Ghobakhloo, 2018; Löfving et al., 2014; Zach et al., 2014). Karakteristiske træk ved SMV'er omfatter, jf. Zach et al. (2014), blandt andet:

- Begrænsede finansielle og menneskelige ressourcer
- Synlig og aktiv topledelse
- Få ledelseslag og centraliseret beslutningstagning
- Kortsigtede beslutningshorisonter
- Intuitive beslutningsprocesser
- Flade og mindre komplekse organisationsstrukturer
- Lavere grad af specialisering
- Uformelle regler og procedurer
- Lav grad af standardisering og formalisering
- Begrænset IT-viden og begrænset strategisk IT-planlægning

Disse strukturelle vilkår har direkte betydning for arbejdet med cybersikkerhed.

Begrænsede ressourcer betyder, at mange produktions-SMV'er ikke har dedikerede IT-sikkerhedsmedarbejdere. Cybersikkerhed håndteres ofte som en delt funktion – eksempelvis af økonomichefen, en ekstern IT-leverandør eller direktøren selv. Dette kan øge sårbarheden over for trusler som ransomware, phishing og industrispionage. Den lave grad af formalisering og standardisering kan desuden betyde, at:

- Adgangsrettigheder ikke systematisk revideres
- Backup-procedurer ikke testes regelmæssigt
- Leverandørers IT-sikkerhed ikke vurderes struktureret
- Der mangler dokumenterede beredskabsplaner

Samtidig kan SMV'ernes karakteristika også være en styrke. Den synlige topledelse og korte beslutningsveje kan muliggøre hurtig implementering af sikkerhedstiltag, hvis ledelsen prioriterer området. Den organisatoriske fleksibilitet og evne til at tilpasse sig ændrede markedsforhold (Pal et al., 2014; Vossen, 1998) kan også understøtte en agil tilgang til risikohåndtering.

Produktions-SMV'er spiller også en central rolle i integrationen af forsyningskæder gennem anvendelsen af Industri 4.0-teknologier (Müller et al., 2018). Digital integration med kunder og leverandører – via ERP-systemer,

produktionsdata, IoT-enheder og cloud-løsninger – øger effektiviteten, men også den digitale afhængighed. Når en produktions-SMV integrerer systemer med større kunder eller internationale leverandører, bliver den samtidig en del af et fælles risikobillede. En sårbarhed hos én aktør kan få konsekvenser for hele netværket. I denne sammenhæng bliver cybersikkerhed ikke alene et internt anliggende, men et konkurrenceparameter. Evnen til at dokumentere robuste sikkerhedsforanstaltninger kan være afgørende for at indgå i strategiske leverandørrelationer.

2.3 Cybersikkerhed

2.3.1 Beskyttelsesmål

I en digital økonomi er beskyttelsen af data og systemer blevet en grundlæggende forudsætning for både forretningsdrift og privatliv. Cybersikkerhed handler i sin kerne om de teknologier, processer og organisatoriske tiltag, der beskytter netværk, systemer og information mod uautoriseret adgang, manipulation eller nedbrud. Ligesom fysisk sikkerhed er det i sidste ende et spørgsmål om risikostyring: Hvilke trusler er mest sandsynlige? Hvad er den potentielle skade? Og hvad koster det at reducere risikoen til et acceptabelt niveau?

Virksomheder med lav modenhed på området håndterer ofte cybersikkerhed reaktivt. Først når et angreb rammer, reagerer man – typisk under tidspres og med høje omkostninger. De seneste år har vist, hvor dyr denne tilgang kan være. Ransomware-angreb mod hospitaler og kommuner i Europa har medført aflyste operationer og nedlukning af digitale systemer i dagevis. I 2024–2025 har flere store detail- og logistikvirksomheder i Europa oplevet driftsstop som følge af leverandørkompromitteringer, hvor ét svagt led i forsyningskæden gav adgang til centrale systemer. Konsekvenserne er ikke kun tekniske, men også økonomiske og omdømmemæssige.

En proaktiv tilgang begynder med at identificere virksomhedens kritiske aktiver. Det kan være produktionsudstyr, cloud-baserede platforme, kundedata, algoritmer, kontrakter eller adgang til digitale betalingssystemer. Når aktiverne er identificeret, bør de vurderes ud fra de tre klassiske beskyttelsesmål: Fortrolighed, integritet og tilgængelighed (på engelsk benævnt CIA, Confidentiality, Integrity og Availability).

Fortrolighed handler om at sikre, at kun autoriserede personer har adgang til information. Hvis eksempelvis kundedata eller forretningshemmeligheder lækkes via en kompromitteret cloud-konto, kan det føre til bøder, tab af konkurrencefordel og mistillid hos kunder. I flere nyere tilfælde har hackere kunnet overtage virksomheders mailkonti og fælles systemer, simpelthen fordi der ikke var ekstra login-sikring ud over adgangskoden. Når de først var logget ind, kunne de læse med i mails, hente fortrolige dokumenter og sende beskeder ud i virksomhedens navn.

Integritet vedrører beskyttelse mod uautoriserede ændringer. I supply chain-angreb har angribere indsat ondsindet kode i legitime softwareopdateringer eller manipuleret data i finansielle systemer. Selv mindre ændringer i produktionsdata eller betalingsinstruktioner kan få store konsekvenser, hvis de ikke opdages rettidigt. Angreb mod open source-komponenter og tredjepartsbiblioteker har i de senere år illustreret, hvor sårbar den digitale værdikæde kan være.

Tilgængelighed betyder, at systemer og data er operative, når de skal bruges. Distribuerede denial-of-service-angreb (DDoS), ransomware eller fejlkonfigurationer i cloud-miljøer kan lamme booking-, betalings- eller produktionssystemer. For en e-handelsvirksomhed kan blot få timers nedetid under en kampagneperiode resultere i betydelige tab, mens nedbrud i energisektoren eller sundhedssektoren kan have samfundskritiske konsekvenser.

En moden cybersikkerhedstilgang kræver derfor løbende risikovurderinger, ledelsesforankring og systematisk implementering af basale kontroller som multifaktorgodkendelse, segmentering af netværk, sikker backup og testet beredskab. Det er sjældent de mest avancerede teknikker, der forhindrer angreb, men derimod konsekvent gennemførelse af grundlæggende sikkerhedsprincipper.

Cybersikkerhed skaber ikke direkte indtjening, men det beskytter virksomhedens evne til at skabe værdi. I en tid med øget geopolitisk spænding, regulatoriske krav (f.eks. NIS 2) og stigende digital afhængighed er en proaktiv og struktureret tilgang ikke længere et valg, men et ledelsesansvar.

2.3.2 Opmærksomhedsområder

Mange virksomheder – og især SMV'er – oplever, at cybersikkerhed virker komplekst og ressourcekrævende. Men en række helt konkrete indsatser kan reducere risikoen markant, hvis de håndteres systematisk.

Forberedelse på hændelser og genopretning

Det er ikke et spørgsmål om hvis, men hvornår en organisation bliver ramt. Derfor bør der være en klar beredskabsplan, før en hændelse opstår. Det indebærer, at det er tydeligt, hvem der kontakter IT-leverandør, hvem der håndterer kommunikation til kunder, og hvem der vurderer eventuel anmeldelsespligt efter GDPR. Et konkret eksempel er ransomware-angreb, hvor virksomhedens filer krypteres. Hvis virksomheden har offline-backups, der løbende testes (f.eks. kvartalsvis gendannelsestest), kan driften ofte genetableres uden at betale løsesum. Flere danske virksomheder har erfaret, at backups eksisterede – men ikke kunne gendannes i praksis, fordi de ikke var testet.

Beskyttelse mod social engineering

Phishing, CEO-fraud og kompromitterede leverandørmails er blandt de mest udbredte angrebsformer. Et typisk scenarie er en mail, der tilsyneladende

kommer fra direktøren med besked om en hastende betaling til en "ny samarbejdspartner". Uden klare interne procedurer kan økonomiafdelingen overføre betydelige beløb. Forebyggelse handler ikke kun om awareness-kurser, men om konkrete kontrolmekanismer:

- Krav om telefonisk verificering ved ændring af kontonumre
- To-faktorgodkendelse på mailkonti
- Simulerede phishing-tests med opfølgende læring

Tiltagene skal dog tilpasses arbejdsgangene. Hvis sikkerhed opleves som en barriere for effektivitet, vil medarbejdere ofte finde uformelle genveje – f.eks. dele loginoplysninger eller gemme følsomme filer lokalt.

Grundlæggende teknisk hygiejne

En stor andel af succesfulde angreb udnytter kendte sårbarheder, hvor sikkerhedsopdateringer allerede findes. Derfor er systematisk patch management afgørende. Et konkret eksempel er udnyttelse af ældre VPN- eller firewall-løsninger, hvor manglende opdateringer har givet angribere adgang til interne netværk. Derudover bør følgende være standard:

- Unikke og stærke adgangskoder administreret via password manager
- To-faktorgodkendelse på alle kritiske systemer (mail, økonomisystem, cloud-platforme)
- Begrænsning af administrative rettigheder efter 'least privilegie'-princippet

I mange kompromitteringer har angribere fået fuld kontrol, fordi én kompromitteret konto havde unødigt brede rettigheder.

Udfordring af egne antagelser

En væsentlig risikofaktor er organisatoriske blinde vinkler. Antagelser som "vi er for små til at være interessante" eller "vores IT-leverandør tager sig af sikkerheden" kan skabe falsk tryghed. I praksis rammes SMV'er ofte, netop fordi de har lavere modenhedsniveau og kan fungere som indgang til større samarbejdspartnere via leverandørkæden. En struktureret risikovurdering bør derfor dokumentere centrale antagelser, f.eks.:

- Hvilke systemer er forretningskritiske?
- Hvor længe kan vi undvære dem?
- Hvad sker der, hvis en leverandør kompromitteres?

Ved at gøre antagelser eksplicitte bliver det muligt at teste deres holdbarhed og prioritere investeringer mere rationelt. Samlet set handler cybersikkerhed for de fleste virksomheder ikke om avancerede teknologiske løsninger, men om ledelsesmæssig prioritering, klare procedurer og konsekvent gennemførelse af grundlæggende foranstaltninger.
Se mindset-værktøjerne på www.cyber-smv.dk.

2.3.3 Cybersikkerhedsstandarder

Cybersikkerhedsstandarder spiller en stadig større rolle for danske produktionsvirksomheder. Digitaliseringen af produktion, integrationen mellem ERP-systemer og produktionsudstyr samt øgede krav fra kunder og myndigheder betyder, at informations- og driftssikkerhed ikke længere kan håndteres ad hoc. Standarder og rammeværktøjer giver virksomhederne et struktureret grundlag for at arbejde systematisk, risikobaseret og dokumenterbart med cybersikkerhed. De mest udbredte og relevante rammer for danske produktions-SMV'er er ISO/IEC 27001 (Informationssikkerhed), IEC 62443, NIST Cybersecurity Framework (CSF) (NIST, 2024), D-mærket, samt CIS Controls. EU's NIS 2-direktiv medfører, at flere virksomheder møder skærpede krav til risikostyring og cybersikkerhed.

ISO/IEC 27001 – den ledelsesmæssige tilgang. ISO/IEC 27001 er udviklet af International Organization for Standardization (ISO) og International Electrotechnical Commission (IEC) og er en anerkendt international standard for ledelse af informationssikkerhed (Culot et al., 2021). Standarden etablerer et ledelsessystem for informationssikkerhed (ISMS), hvor sikkerhed forankres på ledelsesniveau og integreres i virksomhedens styringsprocesser. Kernen i ISO 27001 er den risikobaserede tilgang: Virksomheden skal identificere sine informationsaktiver, vurdere trusler og sårbarheder og implementere passende kontroller.

For en produktions-SMV betyder det eksempelvis at analysere, hvad der vil ske, hvis ERP-systemet kompromitteres, hvis produktionsudstyr bliver utilgængeligt, eller hvis kundetegninger lækkes. Standarden kræver ikke bestemte teknologier, men dokumentation for at risici håndteres systematisk. ISO 27001 er certificerbar, hvilket giver ekstern validering. For SMV'er, der leverer til større koncerner eller indgår i internationale leverandørkæder, kan certificering være en konkurrencefordel og i nogle tilfælde et adgangskrav (license to operate). Udfordringen for mindre virksomheder er, at standarden kræver moden processtyring, valide stamdata og løbende dokumentation. Implementeringen er derfor ikke kun et IT-projekt, men et organisatorisk forandringsprojekt.

IEC 62443 – sikkerhed i industrielle miljøer. IEC 62443-serien er udviklet af International Electrotechnical Commission (IEC) og fokuserer specifikt på cybersikkerhed i industrielle kontrolsystemer. Hvor ISO 27001 primært adresserer informationssikkerhed generelt, går IEC 62443 i dybden med produktionsmiljøer og OT-systemer. Den introducerer blandt andet zone- og conduit-modellen, hvor netværk opdeles i sikkerhedszoner med kontrollerede forbindelser imellem dem. For danske produktions-SMV'er med automatiserede anlæg, PLC'er og SCADA-systemer er dette særligt relevant. Produktionsudstyr er ofte designet med fokus på drift og oppetid – ikke cybersikkerhed. IEC 62443 hjælper med at strukturere krav til både interne systemer og eksterne leverandører, herunder fjernadgang og patch management. Im-

plementering kræver teknisk indsigt i OT-miljøer og tæt samarbejde mellem produktion, IT og eksterne leverandører. Til gengæld adresserer standarden netop de risici, der kan føre til produktionsstop.

NIST Cybersecurity Framework – struktur og modenhed. NIST Cybersecurity Framework er udviklet af det amerikanske National Institute of Standards and Technology (NIST, 2024). I modsætning til ISO 27001 er det ikke en certificeringsstandard, men et fleksibelt rammeværktøj. Frameworket strukturerer cybersikkerhed i seks overordnede funktioner: 1) Govern, 2) Identify, 3) Protect, 4) Detect, 5) Respond og 6) Recover. Denne struktur gør det muligt at vurdere virksomhedens modenhed og identificere huller i sikkerhedsarbejdet.

For en produktionsvirksomhed kan NIST CSF fungere som et styringsværktøj:

- "Identify" kan afdække afhængigheder mellem IT og OT
- "Protect" kan omfatte netværkssegmentering og adgangsstyring
- "Detect" kan handle om overvågning af både kontor- og produktionsnetværk
- "Recover" kan fokusere på beredskabsplaner og test af backup

Den store styrke ved NIST CSF er fleksibiliteten. Den kan anvendes som overordnet ramme og kombineres med mere konkrete kontrolkataloger som CIS Controls eller ISO 27001. For mange SMV'er vil NIST CSF være et pragmatisk sted at starte, fordi den ikke kræver certificering og kan skaleres efter behov.

D-mærket – det danske kvalitetsstempel. D-mærket er en dansk certificeringsordning for IT-sikkerhed og ansvarlig dataanvendelse, der hjælper virksomheder og organisationer med at dokumentere, at de arbejder systematisk med digital sikkerhed og beskyttelse af data. Certificeringen fungerer som et kvalitetsstempel, der signalerer til kunder, samarbejdspartnere og myndigheder, at virksomheden tager cybersikkerhed og dataansvar alvorligt. Formålet er at øge tilliden til danske virksomheders digitale løsninger ved at gøre det synligt, at de lever op til bestemte standarder for cybersikkerhed, databeskyttelse og ansvarlig digital praksis. Ordningen er særligt rettet mod SMV'er, som ofte mangler ressourcer til selv at udvikle omfattende sikkerhedsprogrammer. For at opnå D-mærket skal en virksomhed arbejde struktureret med bl.a.:

- IT-sikkerhed og risikostyring
- Beskyttelse af persondata og GDPR-overholdelse
- Ansvarlig brug af data
- Sikker digital drift og beredskab
- Awareness og træning af medarbejdere i cybersikkerhed

Certificeringen indebærer både en selvevaluering og ekstern verificering, hvor virksomheden dokumenterer, at den lever op til kravene.

CIS Controls – den operationelle tilgang. CIS Controls er udviklet af Center for Internet Security (CIS), en amerikansk non-profit-organisation (Edwards, 2024). CIS 18 er en del af CIS Critical Security Controls v8, som er udviklet af Center for Internet Security (CIS). Rammeværket består af 18 prioriterede sikkerhedskontroller, der skal hjælpe virksomheder med at reducere deres cyberrisici på en praktisk og operationel måde (Darktrace, 2023). De 18 kontroller er:

- Inventar og kontrol over virksomhedens aktiver
- Inventar og kontrol over softwareaktiver
- Databeskyttelse
- Sikker konfiguration af virksomhedens aktiver og software
- Kontostyring
- Styring af adgangskontrol
- Kontinuerlig sårbarhedsstyring
- Håndtering af logning og revisionslogs
- Beskyttelse af e-mail og webbrowsere
- Beskyttelse mod malware
- Datagendannelse
- Styring af netværksinfrastruktur
- Netværksovervågning og forsvar
- Sikkerhedsbevidsthed og kompetencetræning
- Styring af leverandører og tjenesteudbydere
- Sikkerhed i applikationssoftware
- Håndtering af sikkerhedshændelser (Incident Response)
- Penetrationstest

Placeringen af penetrationstestning som den sidste kontrol i version 8 understreger, at det fungerer som en samlet validering af organisationens sikkerhedsniveau. Den bruges typisk i virksomheder, der allerede har implementeret grundlæggende sikkerhedsforanstaltninger og ønsker at teste deres modenhed og robusthed mod reelle angreb. I takt med øget brug af cloud-løsninger og stigende cybertrusler er CIS 18 blevet et centralt værktøj til at dokumentere og styrke cybersikkerheden. For produktions-SMV'er kan CIS Controls fungere som en praktisk handleplan. Tiltag som aktivstyring, multifaktorgodkendelse, sårbarhedsscanning og sikker backup kan implementeres relativt hurtigt og reducere risikoen markant. CIS Controls er særligt velegnet i opstartsfasen eller som supplement til en overordnet ramme som NIST CSF.

NIS 2 (Network and Information Security) – sikkerhed på tværs i EU
NIS-direktivet (Network and Information Security Directive) var EU's første fælles lovgivning om cybersikkerhed, som havde til formål at sikre et højt niveau af sikkerhed for netværks- og informationssystemer i medlemsstaterne. Direktivet blev oprindeligt vedtaget i 2016 og opdateret i 2022 gennem NIS 2-direktivet, som udvider kravene til flere sektorer og organisationer. Formålet er at beskytte kritisk infrastruktur og digitale tjenester mod stigende cybertrusler samt at forbedre samarbejdet mellem EU-landene om cybersik-

kerhed. NIS stiller krav til organisationer om at implementere passende tekniske og organisatoriske sikkerhedsforanstaltninger samt at rapportere alvorlige cybersikkerhedshændelser til nationale myndigheder.

Derudover skal medlemsstaterne etablere nationale cybersikkerhedsstrategier, kompetente myndigheder og Computer Security Incident Response Teams (CSIRT). Direktivet gælder primært for organisationer, der leverer essentielle tjenester, såsom energi, transport, sundhed og digitale tjenester. NIS 2 udvider desuden reguleringen til flere sektorer og stiller strengere krav til risikostyring, rapportering og ledelsesansvar. Samlet set skal direktivet styrke EU's modstandsdygtighed over for cyberangreb og skabe et mere ensartet cybersikkerhedsniveau i hele Unionen (European Commission, 2026; Ruohonen, 2024).

2.3.4 Cybersikker supply chain risk management

Cybersikker supply chain risk management (C-SCRM) kan forstås som en systematisk tilgang til at identificere, vurdere og reducere cyberrisici, der opstår gennem leverandører, IT-/OT-produkter, serviceydelser og øvrige tredjepartsrelationer i hele livscyklussen (f.eks. design, indkøb, implementering, drift, vedligehold og udfasning) (Melnyk et al., 2022). I en produktionsvirksomhed er C-SCRM særligt relevant, fordi 'forsyningskæden' ikke kun er fysiske materialer, men også digitale afhængigheder: ERP-systemer, cloud-services, EDI/kundeportaler, fjernservice til maskiner, softwareopdateringer til OT-udstyr og dataudveksling med kunder og leverandører. Når disse forbindelser kompromitteres, kan konsekvensen være driftsstop, datalæk, fejl i planlægning/produktion eller sabotage – og effekten kan hurtigt sprede sig i netværket (upstream/downstream).

Stentoft et al. (2025) undersøger sammenhængen mellem cybersecurity awareness, C-SCRM og performance i danske produktions-SMV'er. Studiet bygger på surveydata og interviews og peger på, at C-SCRM fungerer som en vigtig mekanisme mellem bevidsthed og (især) finansiel performance. Dvs., at bevidsthed skal 'oversættes' til konkrete C-SCRM-praksisser for at skabe målbar effekt. Det er et vigtigt erhvervsrettet budskab: Awareness er nødvendigt, men ikke tilstrækkeligt. Effekten kommer, når awareness kobles til leverandørstyring, krav, kontroller og løbende opfølgning i forsyningskæden.

I praksis opstår cyber-supply-chain-risici typisk indenfor tre områder (Boyens et al., 2022):

1. Leverandøradgang: Eksterne IT-leverandører, automations-partnere eller maskinleverandører har ofte fjernadgang. Hvis deres legitimationsoplysninger kompromitteres, kan angriberen få direkte adgang til miljøer, der påvirker drift.
2. Produkt- og softwareafhængigheder (IT/OT-produkter & services): Sårbarheder kan følge med ind via software, firmware, opdateringer, biblioteker, cloud-komponenter og integrerede platforme. C-SCRM handler derfor også om at håndtere risici indbygget i det, man køber.

3. Forretningsprocesser og dataflow: Ordredata, forecasts, tekniske tegninger, kvalitetsdata og betalingsoplysninger flyder på tværs af virksomheder. Manipulation eller læk kan give økonomiske tab og tab af konkurrenceevne (f.eks. hvis IP/tegninger kompromitteres).

2.4 Cybersikkerhed og geopolitik

Cybersikkerhed er i stigende grad uløseligt forbundet med geopolitik. Digitale infrastrukturer understøtter i dag centrale samfundsfunktioner som energiforsyning, finansielle transaktioner, sundhedsvæsen, logistik og offentlig administration. Denne gennemgribende digitalisering betyder, at staters økonomiske og politiske handlekraft i høj grad afhænger af stabile og sikre netværk. Samtidig er afhængigheden gensidig og global, hvilket skaber nye former for sårbarheder i et internationalt system præget af strategisk rivalisering (Farrell & Newman, 2019).

Internettets udbredelse i 1990'erne og 2000'erne blev båret af forestillingen om et åbent og grænseoverskridende cyberspace. I dag er denne forestilling udfordret af tendenser til digital suverænitet, teknologisk blokdannelse og øget statslig kontrol. Stormagtskonkurrence mellem blandt andre USA og Kina udspiller sig ikke kun gennem handel og militær oprustning, men også gennem kontrol over halvledere, 5G-infrastruktur, kunstig intelligens og standarder for datastyring (Farrell & Newman, 2019; Segal, 2016). Cyberspace er dermed blevet et centralt domæne for magtprojektion.

Cyberoperationer giver stater og ikke-statslige aktører mulighed for at påvirke modstandere under tærsklen for konventionel krig. Angreb kan rette sig mod kritisk infrastruktur, demokratiske processer eller forsyningskæder og udføres med relativt lave omkostninger sammenlignet med kinetiske operationer (Valeriano et al., 2018). Eksempler fra de senere år omfatter omfattende ransomware-kampagner mod sundhedssektoren, statsligt støttede angreb mod satellitkommunikation i forbindelse med krigen i Ukraine samt cyberoperationer rettet mod energisektoren i Europa. Disse hændelser illustrerer, hvordan cyberangreb kan indgå som et supplement til diplomatiske, økonomiske og militære virkemidler.

Det kan samtidig være meget svært at finde ud af, hvem der faktisk står bag et cyberangreb. Det kan både være teknisk og politisk vanskeligt entydigt at fastslå, hvem der står bag et angreb, hvilket komplicerer afskrækkelse og respons (Rid, 2020). Der eksisterer internationale normprocesser, herunder FN's grupper af statslige eksperter, men udviklingen af bindende regler for statsadfærd i cyberspace har været præget af uenighed mellem stormagter om suverænitet, ansvar og proportionalitet (Ruhl et al., 2020). Den teknologiske udviklingshastighed overstiger ofte tempoet i international regulering.

Samlet set peger forskningen på, at cyberspace er blevet en integreret del af

det geopolitiske magtspil. Digital infrastruktur fungerer både som strategisk ressource og som angrebsoverflade. I en tid med øget geopolitisk spænding må stater og virksomheder derfor betragte cybersikkerhed som en central komponent i national og økonomisk sikkerhed – ikke blot som et teknisk anliggende, men som et strukturelt vilkår i det internationale system.

2.5 Dynamiske kapabiliteter

I en verden præget af teknologiske skift, geopolitisk usikkerhed og stigende cybertrusler er det ikke tilstrækkeligt, at virksomheder blot er effektive i deres daglige drift. De skal også kunne tilpasse sig, omstille sig og forny sig løbende. Det er kernen i teorien om dynamiske kapabiliteter. Begrebet blev introduceret af Teece et al. (1997) og videreudviklet af bl.a. Teece (2007). Dynamiske kapabiliteter kan defineres som virksomhedens evne til at integrere, opbygge og omstrukturere interne og eksterne kompetencer for at imødegå hurtigt foranderlige omgivelser (Teece et al., 1997). Hvor almindelige kapabiliteter handler om at 'gøre tingene rigtigt' i den daglige drift (f.eks. at producere effektivt og levere til tiden), handler dynamiske kapabiliteter om at 'gøre de rigtige ting', når omgivelserne ændrer sig.

Ifølge Teece (2007) består dynamiske kapabiliteter af tre overordnede ledelsesaktiviteter:

1. *Sensing* – at opdage og forstå nye muligheder og trusler
2. *Seizing* – at handle på mulighederne gennem investeringer og beslutninger
3. *Transforming* – at omstille organisationen og dens ressourcer i takt med ændringerne

For praktikere kan det oversættes til følgende:

1. *Sensing*: Har vi systemer og ledelsesmæssig opmærksomhed, der gør os i stand til at opdage nye risici – f.eks. nye cybertrusler, regulatoriske krav eller ændrede kundekrav?
2. *Seizing*: Er vi i stand til at træffe beslutninger og afsætte ressourcer til at handle – f.eks. at investere i nye sikkerhedsløsninger eller ændre leverandørstrategi?
3. *Transforming*: Kan vi ændre strukturer, processer og kompetencer, så ændringen faktisk bliver implementeret i praksis?

Forskning viser, at SMV'er både har udfordringer og fordele i relation til dynamiske kapabiliteter. De har ofte færre ressourcer og mindre formaliserede processer (Zach et al., 2014), hvilket kan begrænse deres strategiske analysekapacitet. Samtidig har de korte beslutningsveje, tæt topledelse og organisatorisk fleksibilitet (Vossen, 1998), hvilket kan understøtte hurtig omstilling.

I praksis kan dynamiske kapabiliteter i en produktions-SMV komme til udtryk ved, at ledelsen:

- Løbende overvåger ændringer i kundekrav, teknologi og regulering
- Aktivt udvikler medarbejderkompetencer inden for nye områder (f.eks. digitalisering og cybersikkerhed)
- Reviderer samarbejdet med leverandører, når risikobilledet ændrer sig
- Integrerer nye teknologier som f.eks. Industri 4.0-løsninger i forretningsmodellen

Cybersikkerhed er et område, hvor dynamiske kapabiliteter er særligt relevante. Trusselsbilledet ændrer sig konstant, og nye sårbarheder opstår i takt med digital integration i forsyningskæder. En virksomhed med stærke dynamiske kapabiliteter vil ikke alene implementere en firewall og betragte opgaven som løst. Den vil formentlig:

- Overvåge nye trusler og regulatoriske krav (*sensing*)
- Investere i relevante sikkerhedsforanstaltninger og leverandørkrav (*seizing*)
- Justere organisation, processer og samarbejder løbende (*transforming*)

Det handler således om at opbygge en organisatorisk læringsevne, hvor sikkerhed bliver en integreret del af strategisk ledelse. For ledere i produktions-SMV'er kan dynamiske kapabiliteter omsættes til tre konkrete spørgsmål:

1. Har vi strukturer til systematisk at identificere nye risici og muligheder?
2. Har vi beslutningskraft og ressourcer til at handle hurtigt?
3. Kan vi ændre vores organisation og samarbejdsrelationer, når det er nødvendigt?

Dynamiske kapabiliteter er ikke et enkelt projekt, men en vedvarende ledelsesdisciplin. I en tid med digitalisering, geopolitiske spændinger og stigende cyberrisici kan netop denne evne til løbende omstilling være afgørende for langsigtet konkurrenceevne.

3. Metode

Undersøgelsen er gennemført som en landsdækkende spørgeskemaundersøgelse i perioden december 2025 til februar 2026. Målgruppen var danske produktionsvirksomheder med 20-250 ansatte inden for NACE-branchekoder 10-33. Virksomhederne blev identificeret via databasen Navne og Numre Erhverv, som omfatter alle momsregistrerede virksomheder i Danmark.

Den indledende bruttoliste omfattede 1.434 virksomheder. Listen blev efterfølgende kvalitetssikret og renset for bagerier samt virksomheder, der ikke længere var aktive. Dette resulterede i en nettoliste på 1.341 virksomheder. Spørgeskemaet blev sendt direkte til administrerende direktører, IT-ansvarlige, CFO'er eller Supply Chain Managers. I tilfælde, hvor specifikke kontaktoplysninger ikke var tilgængelige, blev invitationen sendt til virksomhedens hovedmailadresse adresseret "Til hvem det måtte vedrøre".

I alt accepterede 245 virksomheder at deltage i undersøgelsen, hvoraf 155 afgav fuldt udfyldte besvarelser. Det svarer til en svarprocent på 11,6 blandt de kontaktede virksomheder og 63,3% blandt de virksomheder, der accepterede at deltage. Respondenternes og virksomhedernes karakteristika fremgår af tabel 3.1 og 3.2.

Tabel 3.1: Karakteristik af respondenterne

Respondenternes jobtitler	Antal
Ejer	4
Ejer og adm. direktør	28
Adm. direktør	22
Andet	101
I alt	**155**

Tabel 3.1 viser fordelingen af jobtitler blandt de 155 respondenter. Gruppen bestående af "Ejer", "Ejer og adm. direktør" og "Adm. direktør" udgør samlet set 34,8 % af respondenterne. De resterende 65,2 % er kategoriseret som "Andet". Denne fordeling indikerer, at ansvaret for cybersikkerhed organisatorisk er placeret forskelligt på tværs af virksomhederne – forudsat at respondenterne også repræsenterer det faktiske ansvar for området. I 12,3 % tilfælde har mere end én person medvirket til besvarelsen. I introduktionsbrevet blev det tydeliggjort, hvilke temaer spørgeskemaet omfattede, så respondenten kunne

forberede sig og – om nødvendigt – inddrage relevante kolleger.

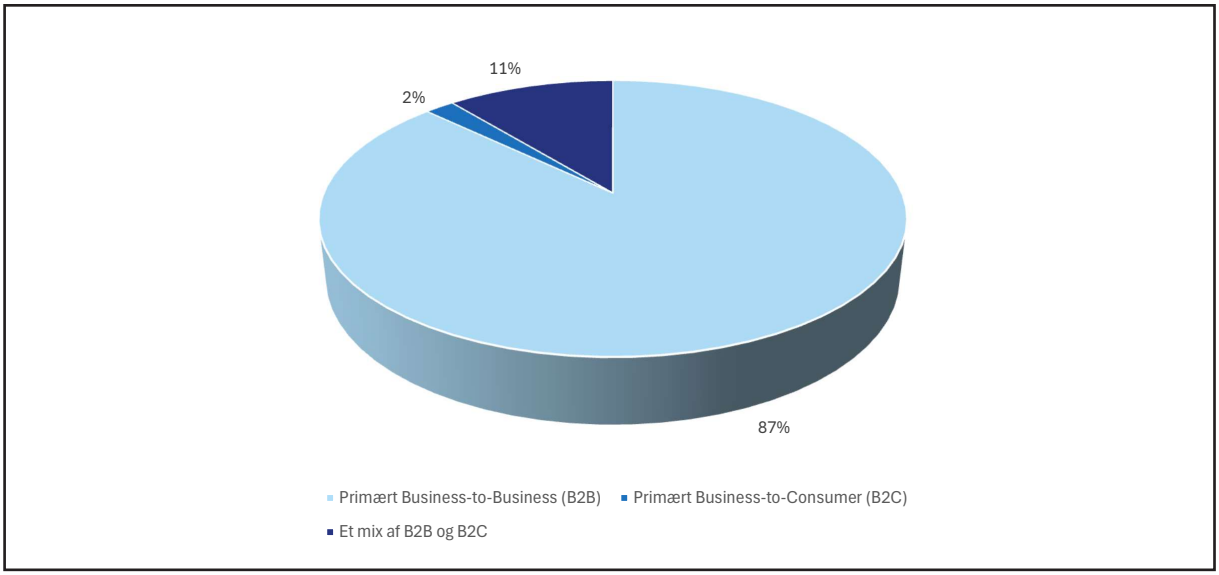
De 65,2 % af respondenterne, der svarer til 101 jf. tabel 3.1, fordeler sig i følgende kategorier, som vist i tabel 3.2.

Tabel 3.2: Uddybning af jobområder for kategorien "Andet" jf. tabel 3.1

Jobområder	Antal
CIO/IT-chef/CTO	33
Supply Chain Manager/Supply Chain Director	3
CFO/Controller	8
Fabrikschef/produktionschef	4
Indkøber/Sourcing Manager/Category Manager	4
Senior Manager (Compliance, Sales, Marketing)	1
COO	9
Partner/bestyrelsesmedlem	1
Andet	38
I alt	**101**

Som det fremgår af figur 3.1 er 87 % af respondenterne B2B virksomheder, 2 % B2C virksomheder og 11 % et mix mellem B2B og B2C.

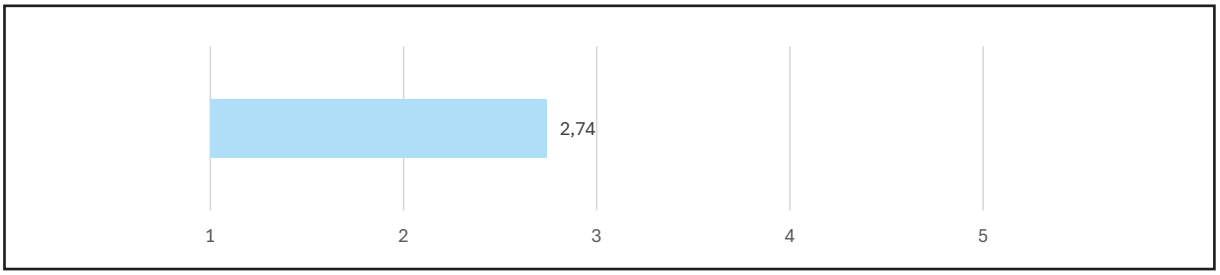
Figur 3.1: Respondenternes fordelig efter type virksomhed



Respondenterne er blevet spurgt ind til, i hvilken grad de er bevidste om 2. leds leverandører, dvs. deres leverandørers leverandører. Det er vigtigt ikke kun at fokusere på 1. leds leverandører i en cybersikkerhedskontekst, fordi trusler ofte opstår længere nede i leverandørkæden, hvor sikkerhedsniveauet

typisk er lavere. Angribere udnytter ofte disse svagere led til at få indirekte adgang til organisationers systemer og data, hvilket ses i stigende grad af supply chain-angreb som f.eks. SolarWinds-hændelsen. SolarWinds-hændelsen var et omfattende cyberangreb, der blev opdaget i 2020, hvor hackere indsatte skadelig kode i en officiel softwareopdatering fra IT-firmaet SolarWinds. Da tusindvis af kunder installerede opdateringen, fik angriberne adgang til deres systemer, herunder flere amerikanske myndigheder og store virksomheder. Angrebet er et eksempel på et såkaldt supply chain-angreb og tilskrives bredt en russisk statsstøttet hackergruppe. Da virksomheder ofte mangler overblik over deres leverandørers underleverandører, kan der opstå blinde vinkler i risikostyringen. Derfor er det nødvendigt at have fokus på hele leverandørkæden for at opnå et retvisende risikobillede og leve op til krav i reguleringer som NIS 2. Som det fremgår af figur 3.2., svarer respondenterne med et gennemsnit på 2,74 (under 'i nogen grad') på en 5-punkts Likert-skala, at de har fokus på 2. leds leverandører. En forklaring til dette lave gennemsnit kan skyldes manglende ressourcer eller viden om denne vigtighed. Det kan anbefales, at cybersikkerhed kommer med på agendaen i kontakter med leverandørerne, samt at deres spørges ind til leverandørernes leverandører. På denne måde kan man skridt for skrift oparbejde et bedre vidensgrundlag.

Figur 3.2: Bevidsthed om 2. leds leverandører



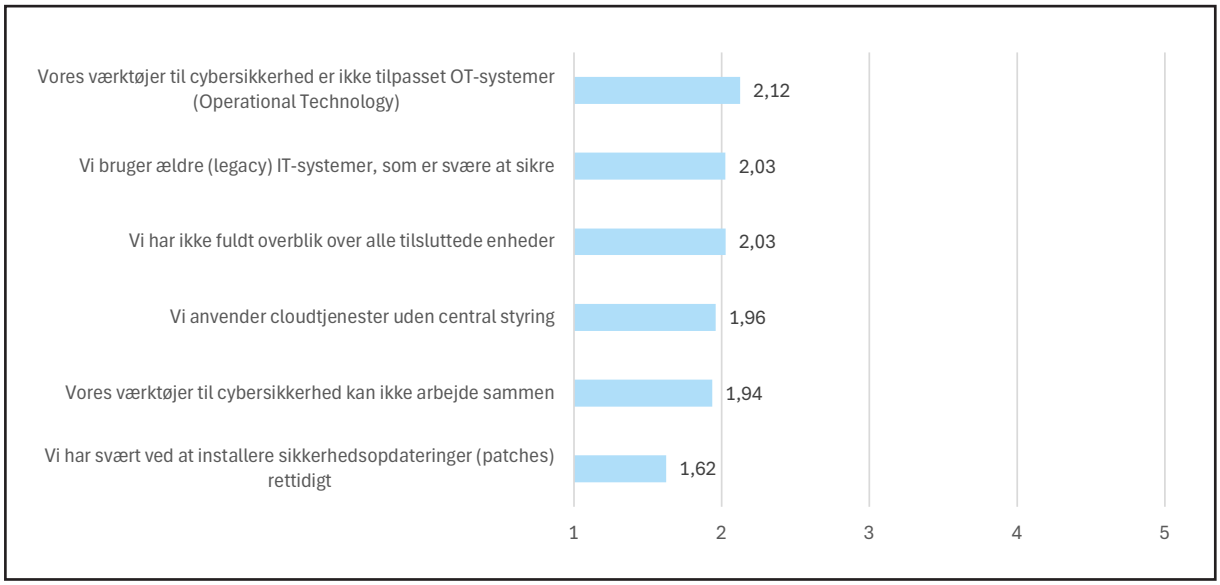
4. Analyse

Dette afsnit præsenterer resultaterne af analyserne af de forskellige temaer relateret til cybersikkerhed.

4.1 IT-teknisk kompleksitet

Som det fremgår af figur 4.1, viser data, at der ikke er en opfattelse af en særlig høj teknisk kompleksitet internt i virksomhederne. Således viser gennemsnittene på en 5-punkts Likert-skala, at alle udsagn i gennemsnit besvares med omkring 2 (fra 1,62 til 2,12), hvilket svarer til 'i mindre grad'. Der kan dog i tallene være skjult større variationer indenfor de enkelte udsagn. Så ud fra tallene ser virksomhederne ud til at være godt med, både hvad angår, hvorvidt man har svært ved at installere sikkerhedsopdateringer rettidigt, hvor respondenterne svarer så lavt som et gennemsnit på 1,62 (mindre end i lav grad) over ikke at have fuldt overblik over alle tilsluttede enheder (et gennemsnit på 2,03) til, at cybersikkerhed ikke er tilpasset OT-systemerne (med et gennemsnit på 2,12).

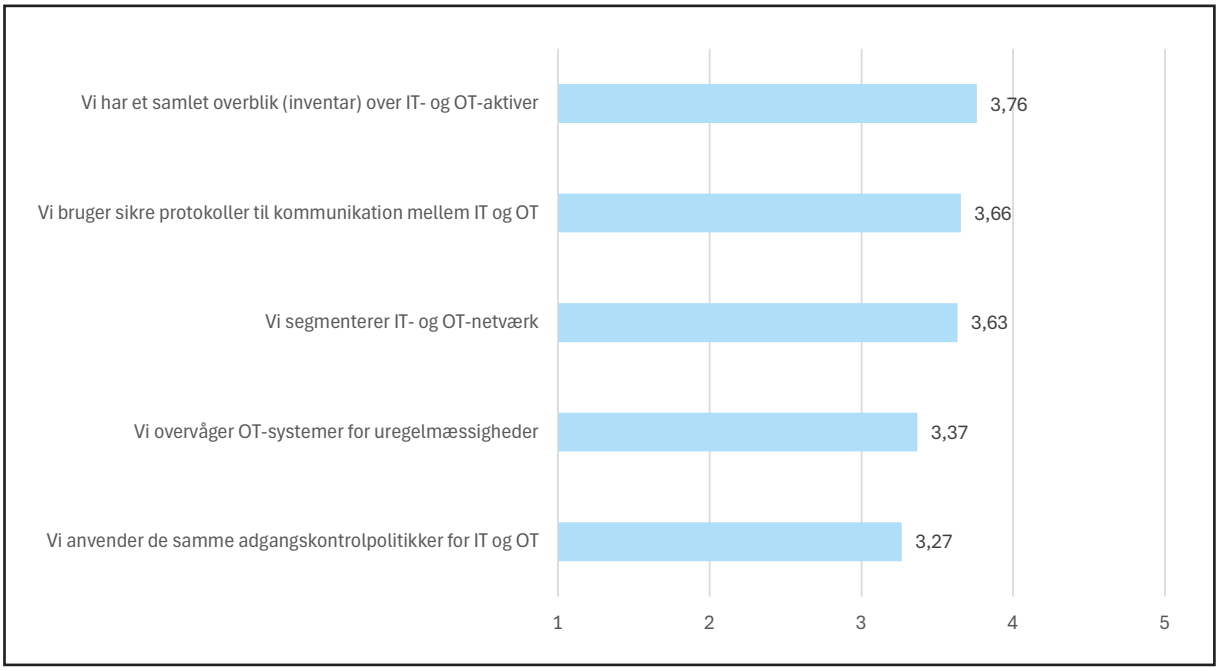
Figur 4.1: Opfattelser af IT-teknisk kompleksitet



4.2 IT-/OT-integration

Ser vi nu på tallene for IT-/OT-integration, fremgår disse af figur 4.2 herunder. Her ligger gennemsnitsværdierne mellem 3,27 og 3,76, hvilket på Likert-skalaen svarer til lige godt og vel fra 'i nogen grad' til knap i 'høj grad'. Da tallene er angivet som gennemsnit af populationen, kan der være spredning i angivelsen af tallene internt for de enkelte udsagn for de bagvedliggende virksomheder. Især synes virksomhederne at have et nogenlunde til godt "overblik over sine IT- og OT-aktiver", som angives med et gennemsnitstal på 3,76. De to næste udsagn "sikre protokoller til kommunikation mellem IT og OT", samt "segmentering af IT- og OT-netværk" angives med hhv. 3,66 og 3,63. I denne type af undersøgelser anses gennemsnitsværdier på 3,50 og derover, for at være signifikante og betydningsbærende. De tre udsagn her ovenfor kan således anses for værende signifikante.

Figur 4.2: IT-/OT-integration



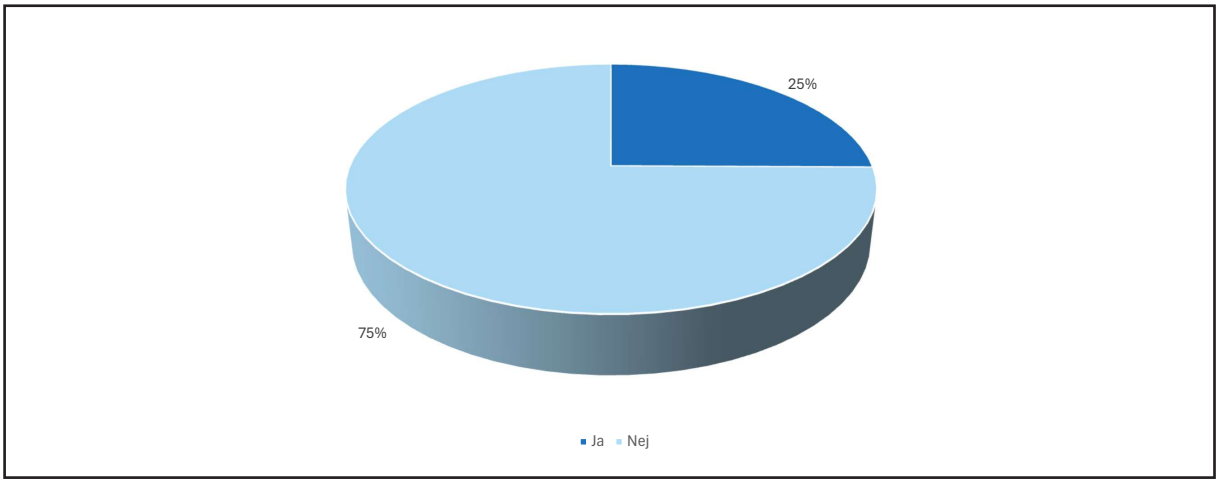
De sidste to udsagn 'overvågning af OT-systemer for uregelmæssigheder' og især 'anvendelsen af samme adgangskontrollerpolitikker for hhv. IT og OT', ligger derimod en del lavere med hhv. 3,37 og 3,27 i gennemsnit svarende til godt og vel i nogen grad. Der er med andre ord plads til forbedringer på især disse specifikke områder.

4.3. Ramt af cyberangreb indenfor de seneste par år

Cybersikkerhed handler om at beskytte organisationers systemer, netværk, data og digitale enheder mod uønsket adgang, misbrug og angreb. Medierne

flyder i denne tid over med, hvordan enkeltindivider rammes af internetsvindel via phishing, smishing og lignende. Det samme gør sig gældende for virksomheder. I takt med, at de bliver mere digitaliserede, er de også blevet mere sårbare over for cyberangreb. Cyberangreb kan blandt andet bestå af phishing, ransomware, datatyveri eller nedbrud på IT-systemer samt distribuerede denial of service-angreb (DDoS), og konsekvenserne kan være alvorlige i form af økonomiske tab, driftsforstyrrelser, tab af fortrolige oplysninger og skade på omdømme. I lighed med undersøgelsen af Stentoft et al. (2024), er det derfor fundet interessant at spørge ind til, hvorvidt virksomhederne er blevet ramt af et cyberangreb indenfor de seneste par år. Som det fremgår af figur 4.3, angiver 25 %, at de har været udsat for et cyberangreb indenfor de seneste par år, mens 75 % angiver, at de ikke har været udsat for et cyberangreb de seneste par år. Dette kan skyldes, at de reelt ikke har været ramt, men det kan også hænge sammen med, at nogle virksomheder kan være tilbageholdende med at oplyse om cyberhændelser, da det kan have betydning for virksomhedens omdømme. Cybersikkerhed er derfor ikke kun et teknisk spørgsmål, men også et strategisk og ledelsesmæssigt anliggende.

Figur 4.3: Har I været ramt af cyberangreb indenfor de seneste par år?



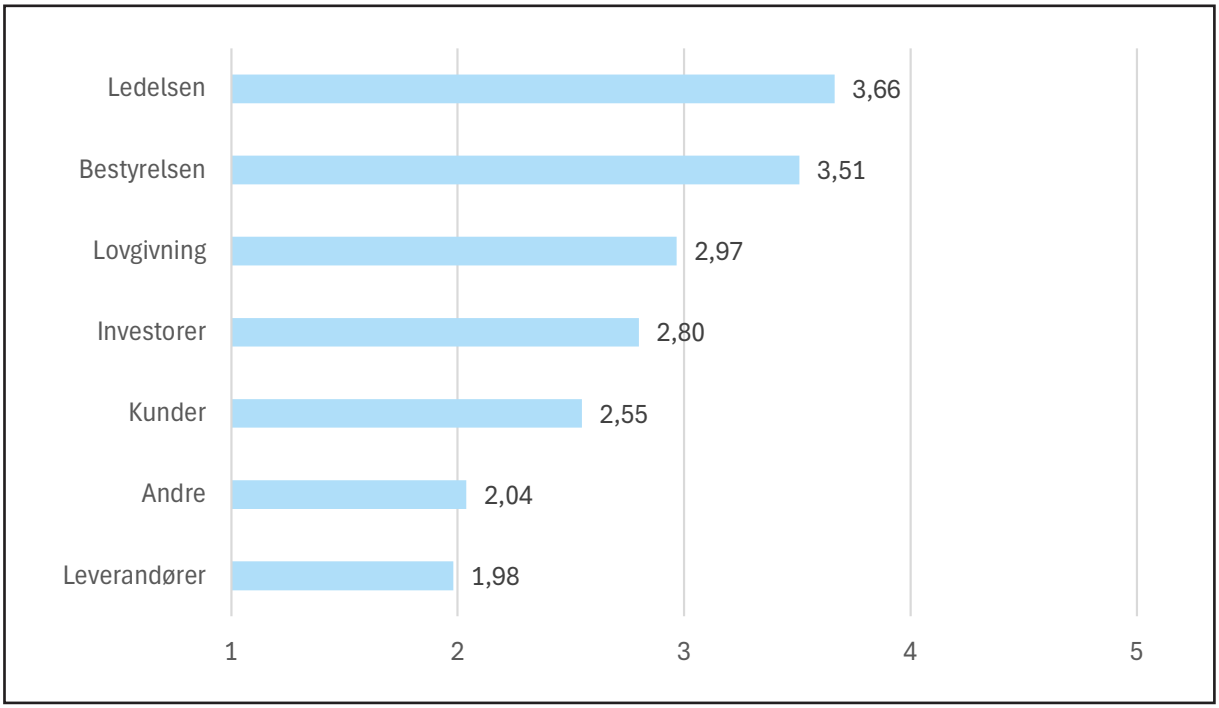
I forhold til 2024-undersøgelsen af Stentoft et al. (2024) viser det en stigning på 25 % (fem procentpoint), fra 20 % i 2024 til nu 25 % i nærværende undersøgelse. Altså ser vi en markant forøgelse af virksomheder, som har været udsat for et cyberangreb indenfor de seneste par år. Og vi må forvente, at dette tal vil stige over de kommende år.

4.4 Krav til cybersikkerhed fra interessenter

Vender vi os nu mod, hvorfra virksomhederne møder kravet om cybersikkerhed, ses disse data i figur 4.4. Her er det især ledelsen og bestyrelsen, som stiller krav om cybersikkerhed med hhv. 3,66 og 3,51 i gennemsnit. Dette er kun en mindre ændring på +0,08 i forhold til 2024-undersøgelsen (Stentoft et al., 2024), hvor bestyrelsen stillede krav om cybersikkerhed med et gennemsnit på 3,43. Så der synes stadigt ikke at være et specielt stort pres fra

bestyrelsens side på trods af en stigende opmærksomhed fra mediernes side. I 2024-undersøgelsen blev der ikke spurgt ind til ledelsens krav om cybersikkerhed. Men, omvendt må det antages, at ledelsen er underlagt krav fra bestyrelsen omkring cybersikkerhed, som herefter lander på ledelsens skrivebord, Men selvom et gennemsnit på 3,66 er signifikant, er det ikke voldsomt. Det kan skyldes, at det er udtryk for et gennemsnitstal, hvor nogle virksomheder rammes direkte af cybersikkerhedskrav, medens andre SMV'er endnu ikke har erkendt (eller er ramt), at når de større virksomheder bliver berørt af krav, siver disse krav nedad i forsyningskæden og rammer SMV'erne. Nøjagtigt som kravene til kvalitet og miljø tidligere har gjort.

Figur 4.4: Krav til cybersikkerhed fra virksomhedens interessenter

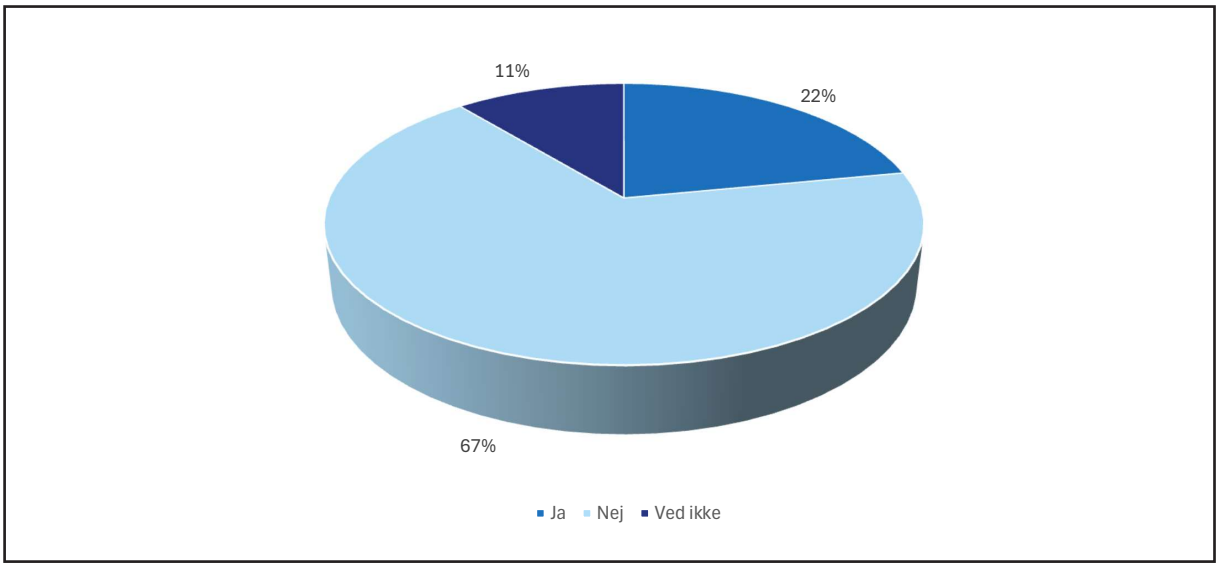


Endnu lavere, efter krav fra ledelsen og bestyrelsen, følger krav fra lovgivning med 'i nogen grad' (med et gennemsnit på 2,97) samt investorer med et gennemsnit på 2,80. Især tallet for krav fra lovgivning kan synes lavt, selvom det er steget lidt siden 2024-undersøgelsen, hvor krav fra myndigheder lå på et gennemsnit på 2,74 (Stentoft et al., 2024). Men det kan skyldes undersøgelsens fokus på SMV'er, hvor lovgivningskrav endnu ikke er slået igennem. Interessant nok er krav fra investorerne faldet fra et gennemsnit på 2,91 i 2024-undersøgelsen til nu 2,80. Kunders krav om cybersikkerhed ligger endnu lavere med kun 2,55 i gennemsnit, hvilket er nøjagtigt det samme som for 2024. De virksomheder, der er spurgt, er typisk underleverandører til større virksomheder. Man kunne derfor forvente, at disse større virksomheder ville stille sådanne krav, men tallene viser det ikke endnu. Så noget kunne tyde på, i forlængelse af ovenstående, at kravene fra kunder ikke er begyndt at manifestere sig endnu og sive ned i kæden. Krav fra leverandørerne opleves ifølge respondenterne kun 'i mindre grad' med et gennemsnit på kun 1,98. Andre ligger en anelse højere med 2,04 i gennemsnit.

4.5 Er virksomheden omfattet af NIS 2?

NIS 2 (Network and Information Security 2) er et nyere EU-direktiv, der stiller strengere krav i forhold til cybersikkerhed for virksomheder og organisationer, som driver kritisk infrastruktur eller leverer vigtige digitale tjenester. Direktivet omfatter også danske produktions-SMV'er. Derfor er det fundet interessant at spørge ind til, hvorvidt virksomhederne ser sig omfattet af dette direktiv. Respondenternes svar fremgår af figur 4.5.

Figur 4.5: Er virksomhederne omfattet af NIS 2?



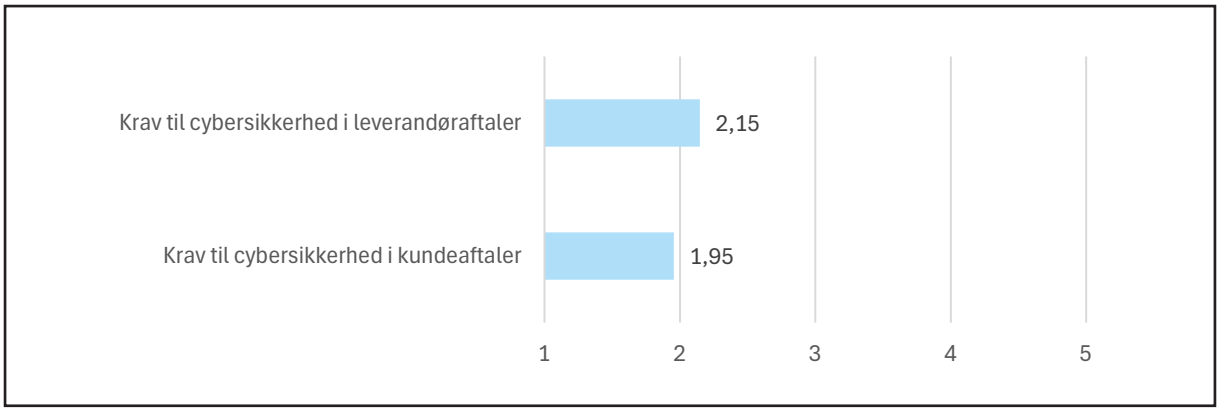
Som det ses af figur 4.5, angiver 22 %, at de er omfattet af NIS 2-direktivet, medens 67 % angiver, at de ikke er. Relateres tallene til figur 4.4, omkring hvordan krav til cybersikkerhed fra interessenterne opleves, stemmer det godt overens med tallet for krav fra lovgivning, som ligger på 'i nogen grad' (2,97). Den relativt større andel, som ikke er omfattet af NIS 2-direktivet, vil alt andet lige trække gennemsnittet ned (67 % mod 22 %). Det er dog også interessant, at hele 11 % ikke ved, om de er omfattet af NIS 2. Disse virksomheder bør få afklaret, om de er omfattet eller ej.

4.6 Krav til cybersikkerhed mod kunder og leverandører

På samme måde, som der ikke i større grad opleves cybersikkerhedskrav fra kunder (2,55 i figur 4.4), stiller virksomhederne i endnu mindre grad cybersikkerhedskrav i aftalerne mod egne leverandører. Her anfører respondenterne, jf. figur 4.6, en score på kun 2,15 i gennemsnit, hvilket svarer til 'i mindre grad', lidt højere end i undersøgelsen fra 2024 på 2.01 (Stentoft et al, 2024). En gammel sandhed siger, at en kæde ikke er stærkere, end det svageste led. Der ligger m.a.o. et markant uindfriet potentiale ved at styrke virksomheder-

nes aftalegrundlag overfor leverandørerne. Endnu lavere, end krav til leverandørerne, ligger krav til cybersikkerhed i forhold til egne kundeaftaler med kun 1,95 i gennemsnit.

Figur 4.6: Krav til cybersikkerhed mod egne kunder og leverandører



Hvor klar er din virksomhed til at håndtere nutidens cybertrusler?

	Niveau 1 Reaktiv	Niveau 2 Proaktiv	Niveau 3 Resilient
AI som angrebsflade	• En grundlæggende 'brug ikke' eller 'vær forsigtig'-politik vedrørende brug af AI. • Interne AI-værktøjer mangler sikkerhedskontroller. • AI-drevne trusler (deepfakes, phishing) overvåges ikke.	• Et AI-governance-udvalg er etableret; tilknyttede risici er dokumenteret og anerkendt. • AI-risici håndteres ved at begrænse adgang til data; der findes visse prompt-kontroller til at fjerne åbenlyst skadelig hensigt. • AI-drevne trusler overvåges lejlighedsvis.	• AI-sikkerhed er fuldt integreret i udviklings- og vedligeholdelses-livscyklussen. • Strenge adgangskontroller til data samt overvågning af output og løbende overvågning af AI-trusler. • AI-specifik medarbejdertræning og risikovurderinger.
Multikanalangreb	• Sikkerheden fokuserer primært på e-mail. • SMS-, telefon- og sociale medieangreb håndteres kun gennem politikker og awareness-uddannelse. • Ingen beredskabsplan for multikanalangreb.	• Der foregår en vis overvågning af SMS, samarbejdsværktøjer og sociale medier. • Der findes detektion, men responsen varierer på tværs af kanaler • Medarbejdere modtager begrænset træning i multikanal-phishing.	• En samlet forsvarsstrategi, der dækker alle angrebskanaler • Proaktiv overvågning på tværs af e-mail, SMS og sociale platforme. • Regelmæssige, personligt tilpassede medarbejdersimulationer vedrørende multikanaltrusler.

	Niveau 1 Reaktiv	Niveau 2 Proaktiv	Niveau 3 Resilient
Risici i forsyningskæden og hos tredjeparter	• Manglende sikkerhed for 100% dækning af tredjeparter. • Leverandørsikkerhed begrænset til compliance-tjeklister. • Ingen overvågning af fjerdepartsrisici. • Ingen struktureret håndtering af leverandørbrud.	• Leverandører vurderes, men tredjepartsrisici er fortsat uklare. • Der stilles sikkerhedskrav til leverandører, men håndhævelse og opfølgning er svag. • Hændelseshåndtering omfatter leverandørbrud, men mangler formaliserede processer.	• Regelmæssige tredjepartsrisikovurderinger med test og audit, der står mål med den tilknyttede risiko og afhængighed. • Sikkerhedskrav indarbejdet i leverandørkontrakter, herunder 'cascade-down'-krav, hvor det er nødvendigt. • Fjerdepartsrisici inddrages, vurderes og håndteres. • Klare beredskabsplaner for angreb på forsyningskæden. • Leverandører inddrages i øvelser vedrørende forretningskontinuitet.
Trusler mod personlige identiteter	• Grundlæggende træning i social engineering-taktikker. • Ingen sikkerhedsforanstaltninger for medarbejderes personlige konti. • Identitetsbaserede trusler uden for arbejdet prioriteres ikke.	• Awareness-træning på arbejdspladsen, men ingen strukturerede beskyttelsesforanstaltninger for personlige identiteter. • Medarbejdere opfordres, men pålægges ikke at sikre deres personlige konti. • Fokus på beskyttelse af ikke-arbejdsrelaterede identiteter gælder kun direktion og bestyrelsesmedlemmer.	• Et målrettet awareness-program omfatter også beskyttelse af personlige identiteter og enheder. • Stærk beskyttelse af ledelsens og medarbejdernes identiteter. • Regelmæssig overvågning for kompromitterede legitimations-oplysninger.

	Niveau 1 Reaktiv	Niveau 2 Proaktiv	Niveau 3 Resilient
Ulighed i cyber-robusthed	• Minimal investering i cybersikkerhed. • Compliance opfattes som et irriterende mål. • Sikkerhedsbeslutninger er reaktive.	• Der findes sikkerhedsforanstalt-ninger, men finansiering og ledelsesmæssig opbakning er begrænset. • Regelmæssig overholdelse af nødvendige standarder. • ISO 27000-serien anvendes som mål for driftsmodellen eller er implementeret i begrænset omfang. • Trusler håndteres reaktivt. • Viden om trusler og cyberkriminalitetstendenser hentes fra almindelige medier. • Ingen langsigtet tilpasningsstrategi.	• Cybersikkerhed er en strategisk prioritet med dedikerede ressourcer. • Certificeret efter ISO 27000-serien for hovedparten af de væsentlige systemer. • Aktivt engagement med branchemyndigheder for at udforme og videreudvikle regulatoriske krav. • Ledelsen støtter aktivt cybersikkerheds-initiativer. • Robusthedsstrategier er tilpasset virksomhedens behov.
Fremgangen i cyber-kriminalitet	• Trusler håndteres reaktivt. • Viden om trusler og cyberkriminalitetstendenser hentes fra almindelige medier. • Ingen langsigtet tilpasningsstrategi.	• Cyberkriminalitets-tendenser overvåges, men reaktionerne fokuserer på umiddelbare trusler. • Der foregår en vis indsamling og deling af trussels-information, men tilpasningen til nye taktikker er begrænset. • Medarbejdere informeres om tendenser, men modtager ikke regelmæssig træning.	• Personaliserede trusselsinformationsydelser informerer aktivt sikkerhedsstrategien. • Løbende tilpasning til nye cyberkriminelle taktikker, teknikker og procedurer (TTP). • Kendskab til kriminelles TTP'er er en integreret del af virksomhedens kultur.

Kilde: Sosafe (2025).

4.7 Cybersikker supply chain risk management

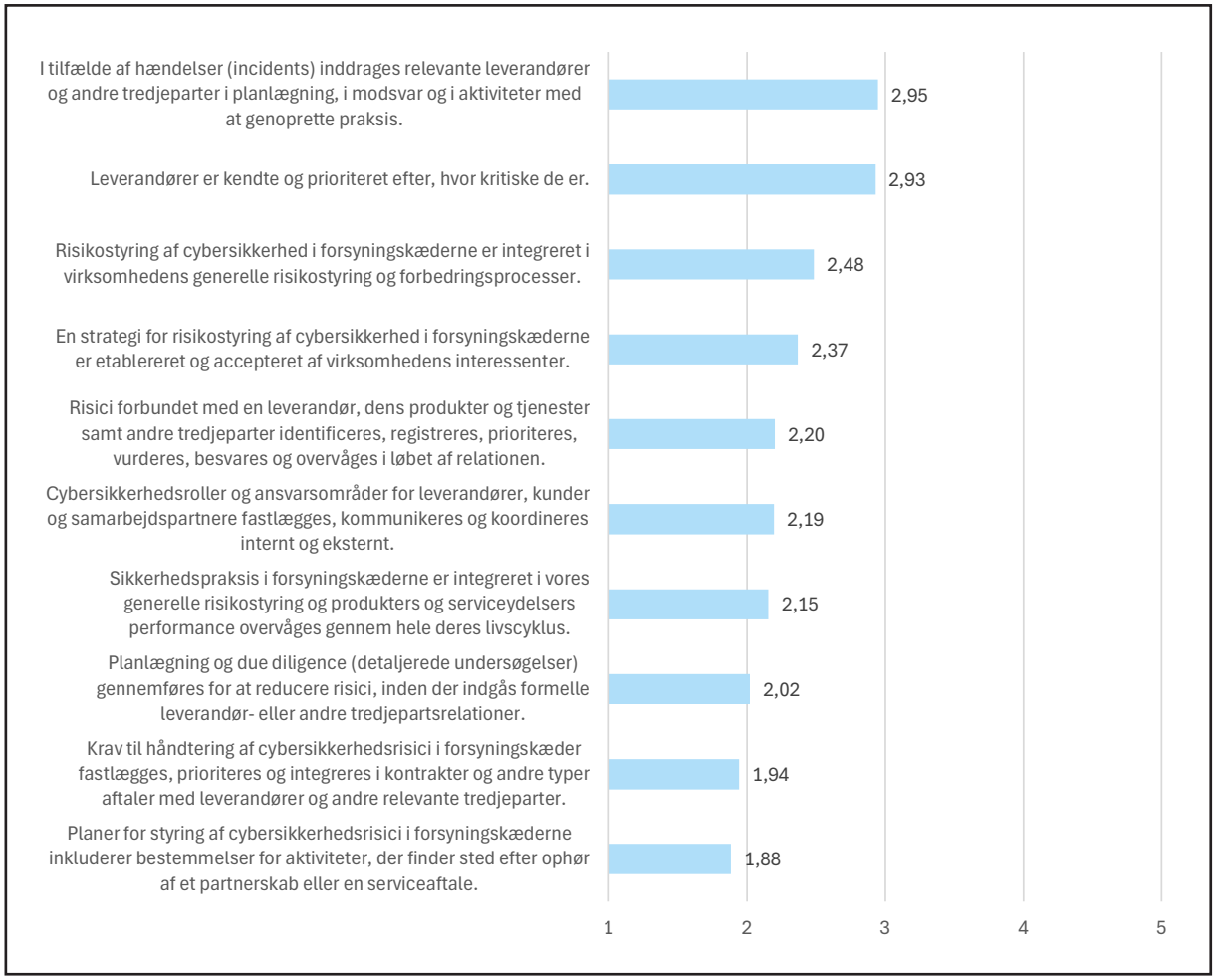
Respondenterne er blevet bedt om at vurdere deres virksomheders praksis indenfor cybersikkerhed supply chain risk management som vist i figur 4.7. Det er overraskende så lave gennemsnitsværdier (fra 2,95 til 1,88 på en 5-punkts Likert-skala), der opnås på de 10 praksisser fra NIST (2024) omkring at sikre cybersikkerhed i et forsyningskædeperspektiv. Resultaterne i figur 4.7 er faktisk lavere end resultaterne fra 2024-undersøgelsen af de samme praksisser (Stentoft et al., 2024). Det højeste gennemsnit på 2,95 opnås af praksissen med at inddrage relevante interessenter i tilfælde af cyberhændelser. Dernæst følger, at leverandører er kendte og prioriteret efter, hvor kritiske de er. Det er et overraskende lavt gennemsnit, at man ikke engang i nogen grad har fokus på basale forhold i en forsyningskæde omkring ens leverandører. I 2024-undersøgelsen var dette gennemsnit på 3,08 (Stentoft et al., 2024). Der er ingen tvivl om, at de 10 praksisser vist i figur 4.7 er ressourcekrævende for produktions-SMV'erne. Dernæst kan det også være en udfordring, at man nok kan læse om de 10 praksisser, men, at man samtidig mangler viden om, hvordan man konkret operationalisere dem. I projektet **Cybersikkerhed og Forretningskontinuitet** er der udviklet 10 konkrete værktøjer – ét værktøj pr. praksis i figur 4.7. Værktøjerne kan findes på projektets hjemmeside www.cyber-smv.dk.

Risikostyring af cybersikkerhed som et led i virksomhedens øvrige risikostyring opnår et gennemsnit på 2,48, hvilket også indikerer et behov for udvikling. Det relativt lave gennemsnit kan skyldes, at den mere generelle risikostyring måske også er mangelfuld. Det kan også ses i relation til praksissen med at have en strategi for risikostyring af cybersikkerhed i forsyningskæderne, hvor gennemsnittet er på 2,37. Risici forbundet med leverandører og andre tredjepartnere overvåges kun løbende med et gennemsnit på 2,20. Ligeledes opnår praksis med definering af roller og ansvarsområder for cybersikkerhed også kun et gennemsnit på 2,19. Produkter og serviceydelsers performance overvåges i lav grad gennem deres livscyklus med et gennemsnit på 2,15. Også praksis med detaljerede undersøgelser af cyberrisici (gennemsnit på 2,02) sker i lav grad, inden der indgås formelle aftaler med leverandører med et gennemsnit på 1,94. Dette indikerer et klart forbedringsområde til at inkludere informationssikkerhed i nye og eksisterende aftaler med samarbejdspartnere. Det laveste gennemsnit på 1,88 vedrører praksissen med, at der er klarhed over, hvad der sker med data, når en aftale med en ekstern partner ophører.

Sammenfattende kan resultaterne i figur 4.7 forklares ved en kombination af begrænsede ressourcer, organisatorisk umodenhed og kompleksitet i SMV'ernes forsyningskæder. SMV'er har ofte færre økonomiske og kompetencemæssige ressourcer til at arbejde systematisk med cybersikkerhed, og sikkerhed prioriteres typisk lavere end den daglige drift. Samtidig mangler mange formaliserede processer for leverandørstyring, herunder krav til leverandørers cybersikkerhed og løbende risikovurderinger, hvilket er centralt i cybersikker supply chain risk management. Produktions-SMV'er er desuden karakteriseret ved komplekse og ofte internationale forsyningskæder samt brug af ældre produk-

tionssystemer, hvilket gør det vanskeligt at skabe overblik over risici. Historisk har der også været begrænset reguleringspres på SMV'er, hvilket har reduceret incitamentet til at arbejde strategisk med området, og cybersikkerhed opfattes ofte som et rent IT-anliggende frem for et tværorganisatorisk ansvar. Samlet set peger de lave scorer derfor på en lav modenhed i håndteringen af cybersikkerhed i forsyningskæden snarere end nødvendigvis lav teknisk sikkerhed.

Figur 4.7: Cybersikker supply chain risk management



4.8 Cybersikre dynamiske kapabiliteter

I en stadig mere digitaliseret og usikker verden, hvor cybertrusler fylder mere, er traditionelle markedskapabiliteter ikke længere tilstrækkelige. Virksomheder må derfor udvikle cybersikre dynamiske kapabiliteter for effektivt at kunne forebygge, håndtere og tilpasse sig cyberrisici. Analysen viser dog et generelt lavt modenhedsniveau, hvilket understøtter rapportens overordnede billede af SMV'ernes overvejende reaktive tilgang til cybersikkerhed og strategi.

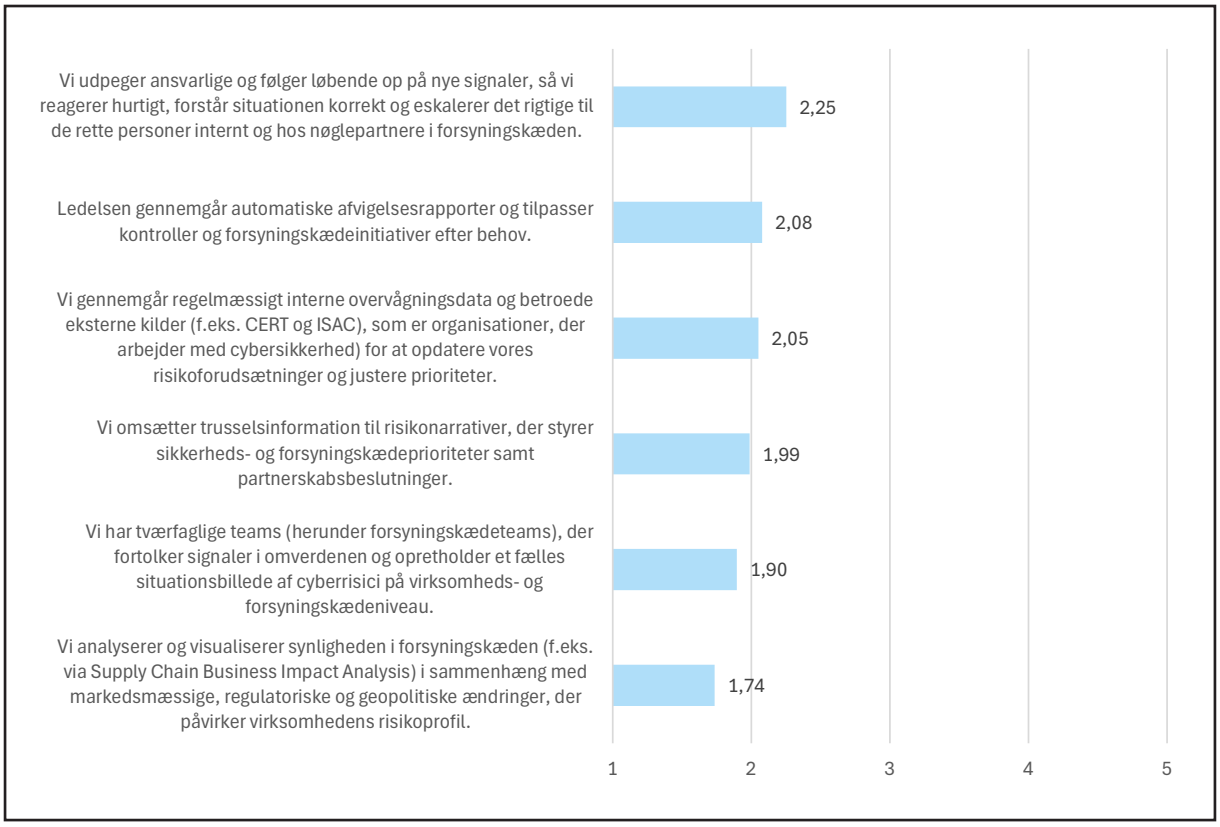
4.8.1 Sensing

Resultaterne viser, at danske SMV'er stadig er i gang med at udvikle deres dynamiske kapabiliteter inden for cybersikkerhed og har en tendens til at være reaktive. Dette er bekymrende i lyset af den stigende kompleksitet i cybertrusler, de voksende regulatoriske krav i forbindelse med NIS 2 samt den tætte sammenkobling i moderne forsyningskæder.

Figur 4.8 viser resultaterne for sensing, som afspejler virksomhedernes evne til aktivt at scanne, opdage, identificere og overvåge nye cybertrusler og muligheder i forsyningskæden. Den gennemsnitlige score er 2,00, hvilket indikerer, at virksomhederne i begrænset omfang overvåger og fortolker signaler om cybertrusler i deres eksterne miljø. Dette tyder på, at meget få virksomheder har etableret tværfunktionelle teams eller processer til systematisk at indsamle og analysere trusselsinformation fra forsyningskæden. Derudover antyder det, at de fleste virksomheder mangler systemer eller værktøjer til at scanne deres omgivelser for nye cybertrusler, overvåge cybersikkerhedsniveauet hos samarbejdspartnere i forsyningskæden eller integrere ekstern trusselsinformation i deres risikovurderinger.

Dette resultat stemmer overens med nyere forskning, der fremhæver 'sensing' som en grundlæggende, men underudviklet kapabilitet i opbygningen af cyberrobusthed i forsyningskæder. Herburger et al. (2024) identificerer tre specifikke mikrofundamenter for sensing, der kan styrke cyberrobustheden: 1) udvikling af viden om risici i forsyningskæden, 2) forbedring af synligheden af cyberrisici i forsyningskæden og 3) opbygning af trusselsintelligens i forsyningskæden. Uden tilstrækkelige sensing-kapabiliteter er virksomheder ikke i stand til at identificere, hvilke partnere i forsyningskæden, der udgør forhøjede risici, hvilke digitale afhængigheder der skaber kædereaktioner af sårbarheder, eller hvilke eksterne kilder til trusselsinformation der kan styrke deres cybersikkerhed. Resultaterne peger derfor på et væsentligt strategisk gap. Derudover identificerer Afshari-Mofrad et al. (2024) netværk for cybertrusselsintelligens som en central sensing-kapabilitet for cybersikkerhedsagilitet. De argumenterer for, at virksomheder både skal udvikle forståelse for nuværende og fremtidige trusler og samtidig deltage i videndelingsnetværk og fællesskaber for at lære af andre. Den lave sensing-score blandt danske SMV'er tyder på, at proaktiv indsamling af trusselsinformation og samarbejdsbaseret læring stadig er begrænset, hvilket efterlader virksomhederne mere sårbare over for trusler, som mere modne organisationer ville opdage og håndtere tidligere. Den lave score viser dermed, at SMV'er har behov for at styrke deres strategiske overvågning af cybertrusler, herunder anvendelse af eksterne kilder (f.eks. CERT'er og ISACs) samt løbende analyse af forsyningskædens synlighed og sårbarheder.

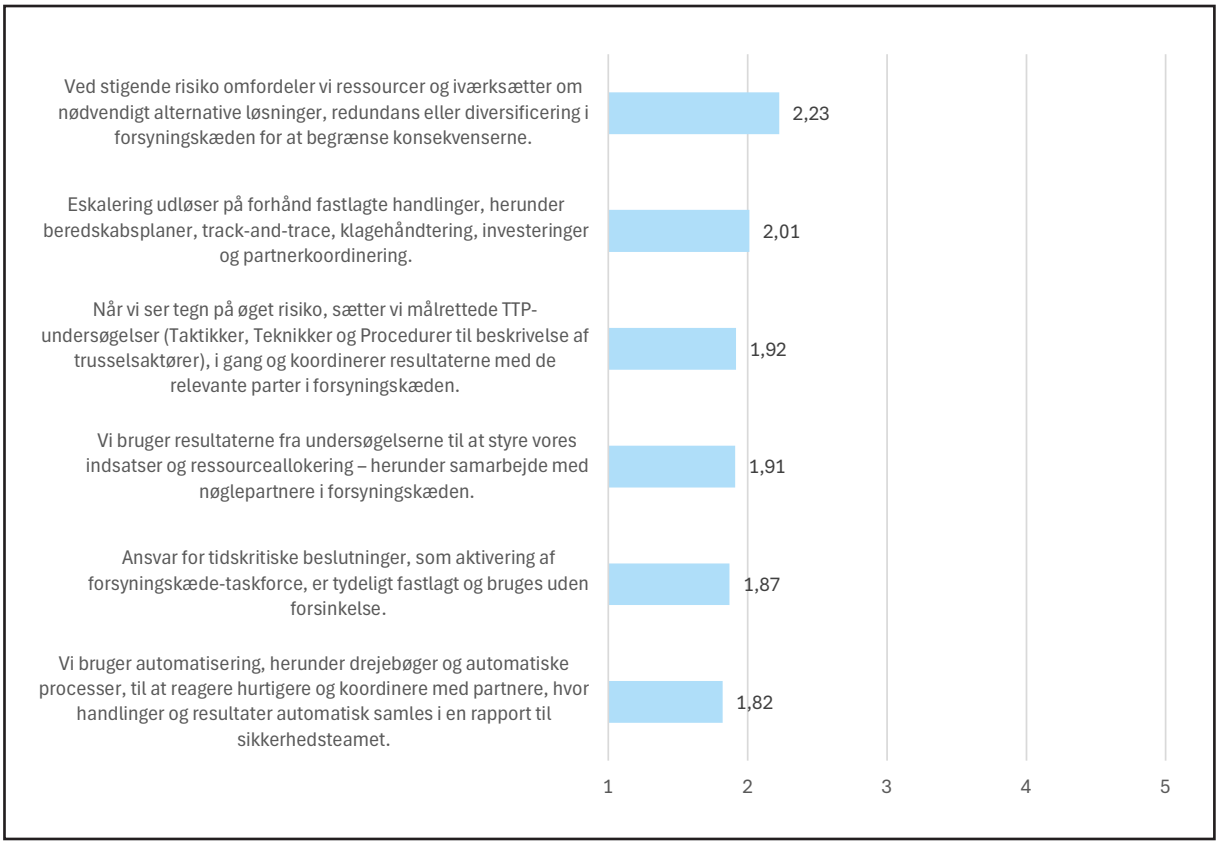
Figur 4.8: Sensing - Cybersikre dynamiske kapabiliteter



4.8.2 Seizing

Seizing-kapabiliteterne fremstår lige så lave som sensing-kapabiliteterne. Selvom det kan virke logisk, at lave sensing-scorer afspejles i lave seizing-scorer, viser det også, at SMV'erne ikke kompenserer for manglende sensing gennem øget seizing. Alle seizing-relaterede målepunkter scorer i gennemsnit under 3 (jf. figur 4.9). Faktisk er den samlede gennemsnitsscore på 1,96 endnu lavere end de 2,00, der ses for sensing. Især beslutninger om at etablere taskforces og automatisere processer, som muliggør hurtig reaktion på hændelser, scorer meget lavt. Dette indikerer, at seizing-kapabiliteterne i danske SMV'er er meget begrænsede og i høj grad trænger til forbedring. Selvom de lavest scorende områder naturligt har størst behov for forbedring, viser de generelt lave scorer på tværs af alle målepunkter, at enhver indsats for at styrke kapabiliteterne vil være gavnlig for SMV'erne. Set i lyset af de lave sensing-scorer kan en SMV, der ønsker at opbygge sine egne kapabiliteter, med fordel først styrke sine sensing-kapabiliteter, så de efterfølgende udviklede seizing-kapabiliteter kan baseres på et solidt og velunderbygget beslutningsgrundlag.

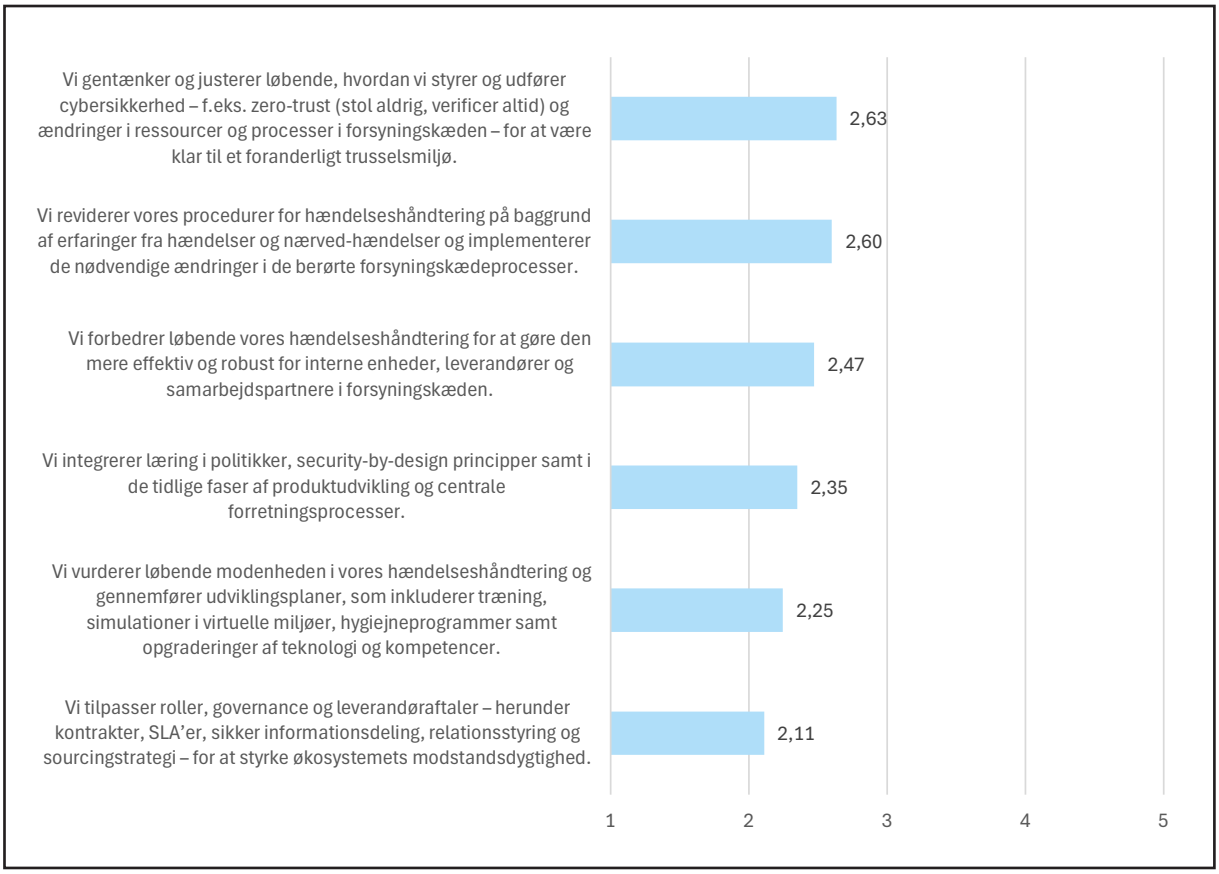
Figur 4.9: Seizing - Cybersikre dynamiske kapabiliteter



4.8.3 Transforming

Det er interessant, at deltagende SMV'er vurderer deres transforming-kapabiliteter højere end både sensing- og seizing-kapabiliteterne, men med en gennemsnitlig score på 2,40 – og tilsvarende lave scorer på de enkelte aspekter – ligger niveauet stadig klart under skalaens midtpunkt på 3 (jf. figur 4.10), hvilket indikerer et fortsat betydeligt forbedringsbehov. Transformation inden for cybersikre dynamiske kapabiliteter handler om virksomheders evne til løbende at tilpasse organisation, processer og teknologier i takt med et foranderligt trusselsbillede, herunder gennem strukturelle ændringer, kompetenceudvikling og integration af cybersikkerhed i forretningsstrategien for at opbygge langsigtet robusthed. Respondenterne har vurderet deres praksis på seks kapabiliteter inden for dette område, hvor løbende gentænkning og justering af cybersikkerhed opnår et gennemsnit på 2,63, mens tilpasning af roller, governance og leverandøraftaler scorer lavest med 2,11. Særligt bekymrende er det, at cybersikkerhedsstyring i forhold til leverandører (f.eks. Service Level Agreements) er blandt de lavest scorende områder, hvilket afspejler de lave sensing- og seizing-niveauer og peger på væsentlige svagheder i håndteringen af forsyningskæderisici. Samtidig fremstår automatisering af cybersikkerhedsrespons som et centralt forbedringsområde. Samlet set indikerer resultaterne, at SMV'er kun i begrænset omfang formår at omstille sig strategisk og organisatorisk i forhold til cybertrusler, og at de især halter på de mere strukturelle og langsigtede tilpasninger, hvilket kan begrænse deres evne til effektivt at håndtere og tilpasse sig et stadig mere komplekst trusselsbillede.

Figur 4.10: Transforming - Cybersikre dynamiske kapabiliteter



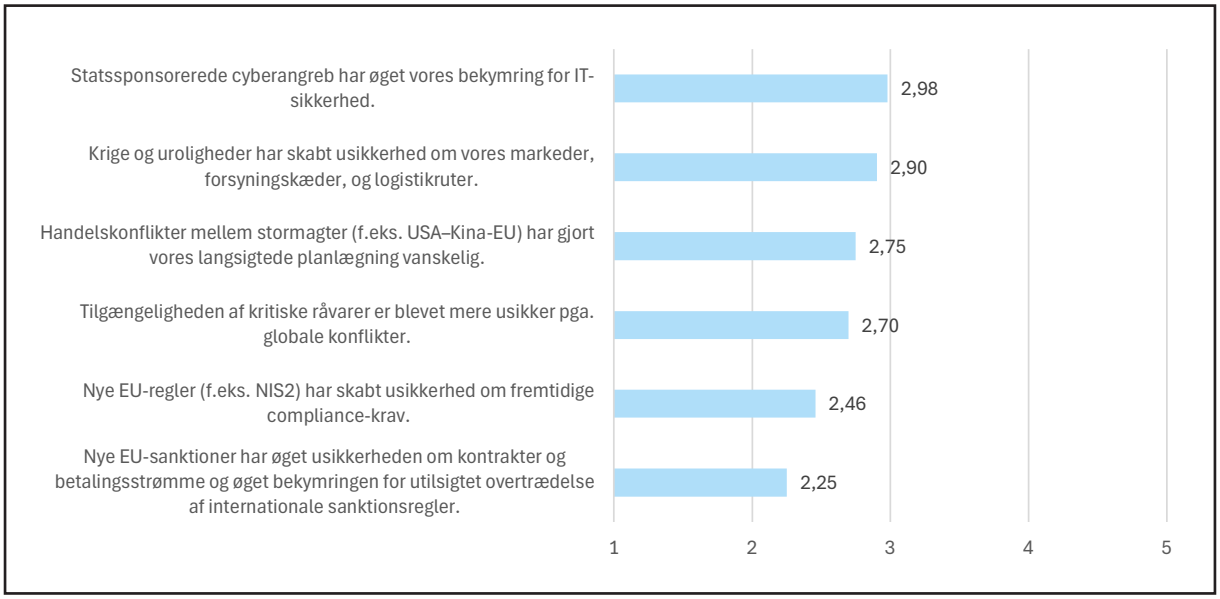
4.9 Geopolitiske markedskræfter

Som beskrevet i rapportens indledning er rammevilkårene for danske produktions-SMV'er under kraftig forandring på grund af øgede stormagtskonflikter og en mere fragmenteret verdenshandel. Denne overgang fra en liberal til en geoøkonomisk verdensorden betyder, at økonomi og sikkerhedspolitik nu er tæt sammenkoblet.

Resultaterne i figur 4.11 sår imidlertid tvivl om, hvorvidt denne nye virkelighed reelt er sunket ind hos virksomhederne. Selvom respondenterne udtrykker størst bekymring for statssponsorerede cyberangreb (med et gennemsnit på 2,98) tæt efterfulgt af usikkerheder skabt af krige og uroligheder (med et gennemsnit på 2,90), er det bemærkelsesværdigt, at ingen af gennemsnitsværdierne overstiger 3 på en 5-punkts Likert-skala. Dette tyder på, at mens der er en vis spirende erkendelse af problemerne, er forståelsen slet ikke på det niveau, man må forvente i betragtning af de geopolitiske forandringer, vi aktuelt er vidne til. At bekymringen, for f.eks. utilsigtede overtrædelser af nye EU-sanktioner kun scorer 2,25, peger på en underestimering af, hvor hurtigt storpolitisk *Weaponized Interdependence* kan ramme den enkelte SMV's markedsadgang. *Weaponized Interdependence* beskriver, hvordan stater kan udnytte gensidige økonomiske og teknologiske afhængigheder som et magtmiddel i international

politik. I en globaliseret verden er lande forbundet gennem netværk som handel, finans og teknologi, og hvis et land har kontrol over centrale knudepunkter i disse netværk, kan det bruge denne position til at lægge pres på andre lande. Det kan f.eks. ske ved at begrænse adgang til markeder, betalingssystemer eller kritiske ressourcer. På den måde bliver afhængighed ikke kun et tegn på samarbejde, men også et potentielt redskab til politisk kontrol og sanktioner. Samlet set viser dataene, at der er markant plads til forbedring, og at produktions-SMV'erne i høj grad fortsat mangler at internalisere alvoren af disse makroøkonomiske trusler som et grundlæggende forretningskritisk vilkår.

Figur 4.11: Geopolitiske markedskræfter



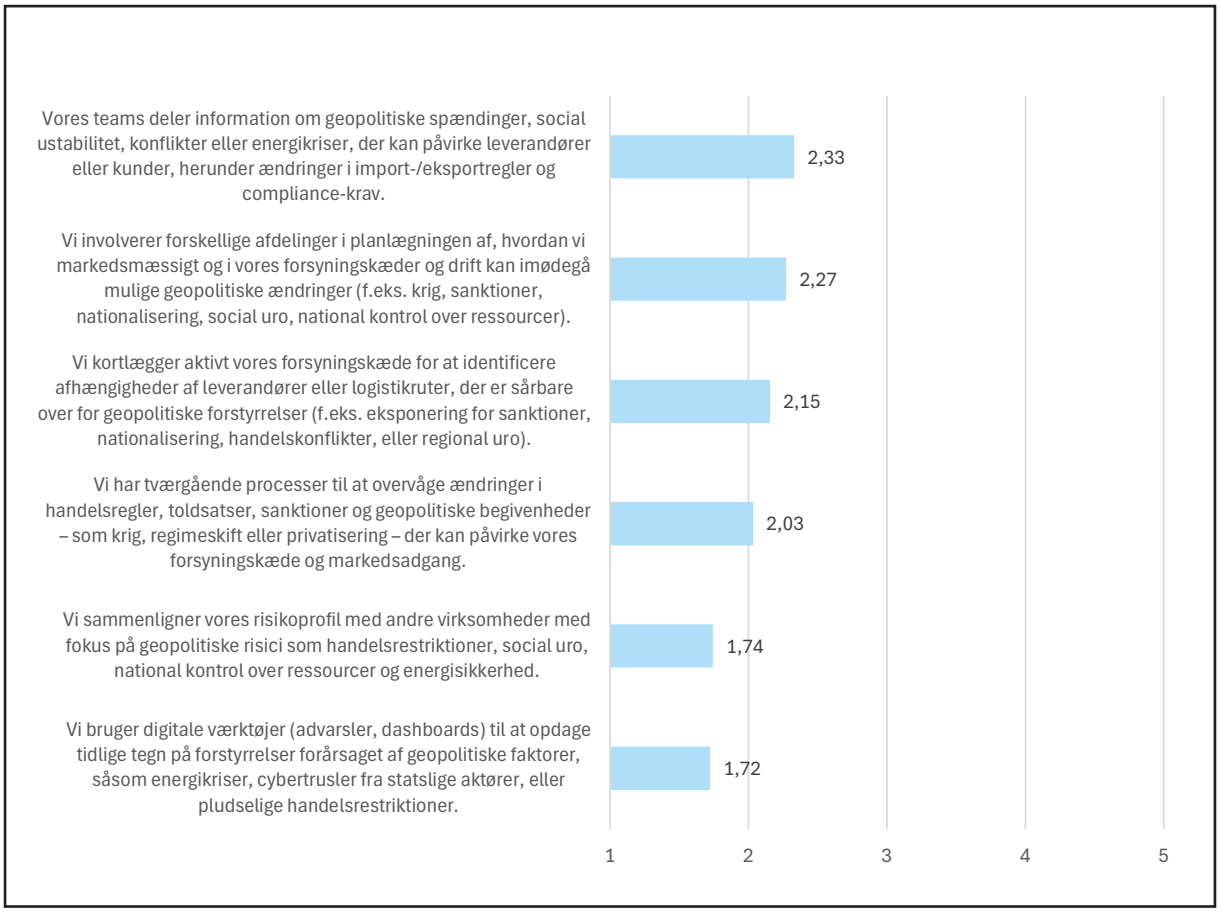
4.10 Dynamiske kapabiliteter for geopolitiske markedspåvirkninger

For at navigere i et omskifteligt og globalt marked, der bliver gjort til et spørgsmål om sikkerhed, er traditionelle markeds-kapabiliteter utilstrækkelige. Virksomhederne skal i stedet udvikle geopolitiske dynamiske kapabiliteter (GDC). Analysen viser imidlertid en generel lav modenhed, hvilket harmonerer med rapportens overordnede fund vedrørende SMV'ernes reaktive tilgang til sikkerhed og strategi.

4.10.1 Sensing

Evnen til at opfange geopolitiske trusler er desværre lav. Selvom virksomhederne i nogen grad deler information om spændinger (med et gennemsnit på 2,33) jf. figur 4.12, mangler de systematiske processer. De anvender stort set ikke digitale værktøjer til at opdage tidlige tegn på forstyrrelser (med et gennemsnit på 1,72), ligesom de sjældent benchmarker deres geopolitiske risikoprofil mod andre (med et gennemsnit på 1,74). Dette afspejler en fundamental blind vinkel: Uden datadrevet sensing risikerer SMV'erne at blive overrumplet af ideologiske friktioner, før de konkret rammer driften.

Figur 4.12: Sensing - Kapabiliteter for geopolitiske markedspåvirkninger

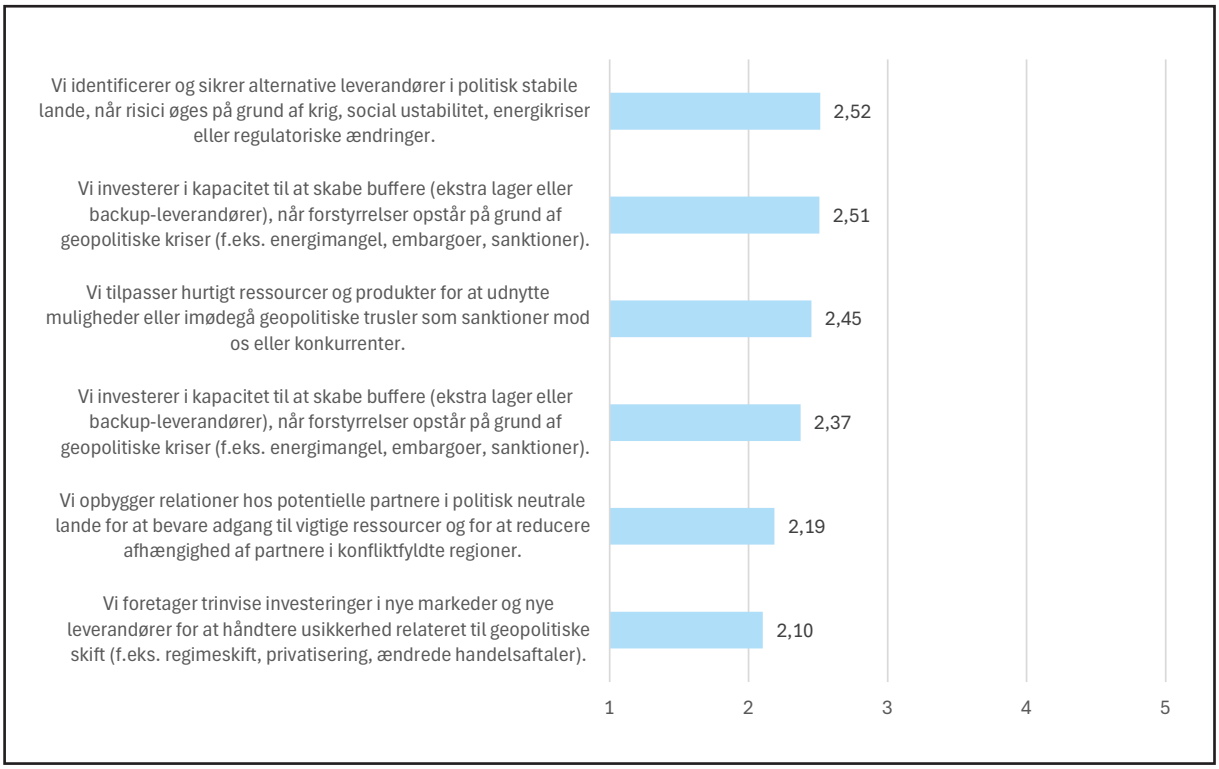


Samlet opnås der et gennemsnit på 2,04 for de seks sensing-kapabiliteter.

4.10.2 Seizing

Den samlede score for seizing er marginalt højere (med et gennemsnit på 2,36), måske primært drevet af velkendte, reaktive brandsluknings-tiltag. Men alle seks kapabiliteter opnår gennemsnitsværdier under 3 (’i nogen grad’). SMV’erne er relativt dygtige til at sikre alternative leverandører i stabile lande (med et gennemsnit på 2,52) jf. figur 4.13 og investere i ekstra lagerkapacitet (med et gennemsnit på 2,51) under kriser. Til gengæld er den strategiske, langsigtede investering i nye markeder og leverandører markant lavere (med et gennemsnit på 2,10). Dette indikerer, at virksomhedernes respons oftere er præget af akut krisestyring frem for en bevidst strukturel opbygning af modstandsdygtighed.

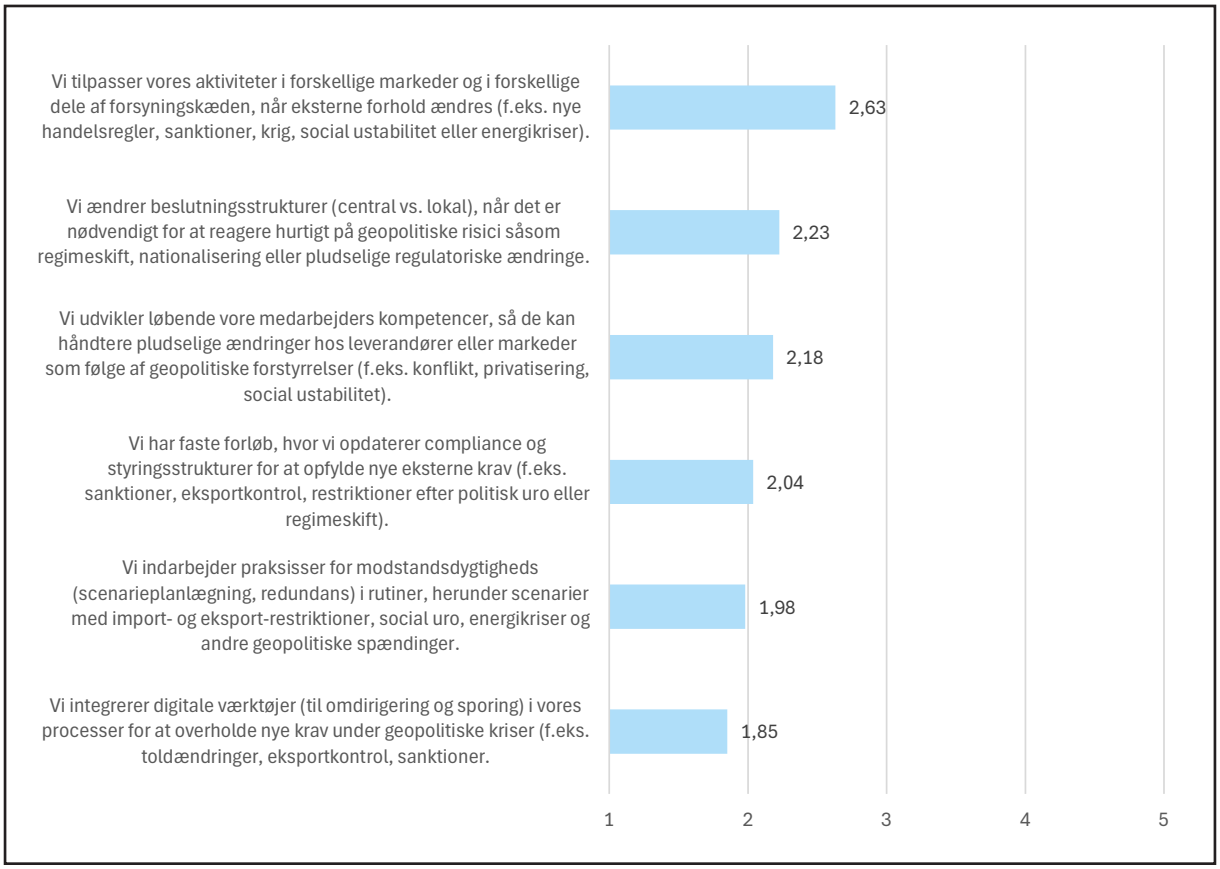
Figur 4.13: Seizing - Kapabiliteter for geopolitiske markedspåvirkninger



4.10.3 Transforming

Evnen til operativ omstilling er ligeledes svag. Mens SMV'erne tilpasser aktiviteterne, når eksterne forhold ændres (et gennemsnit på 2,63) jf, figur 4.14, mangler de faste procedurer for det. Implementeringen af resiliens-praksisser som scenarieplanlægning i de daglige rutiner halter (med et gennemsnit på 1,98) jf. figur 4.14, og der mangler integration af digitale sporingsværktøjer til at overholde nye eksportkontrolkrav (et gennemsnit på 1,85). Den manglende transformationsevne understreger, at mange SMV'er fortsat arbejder ud fra uformelle strukturer frem for formaliseret risikostyring.

Figur 4.14: Transfoming - Kapabiliteter for geopolitiske markedspåvirkninger



Det samlede gennemsnit for transformationskapabiliteterne er på 2,15.

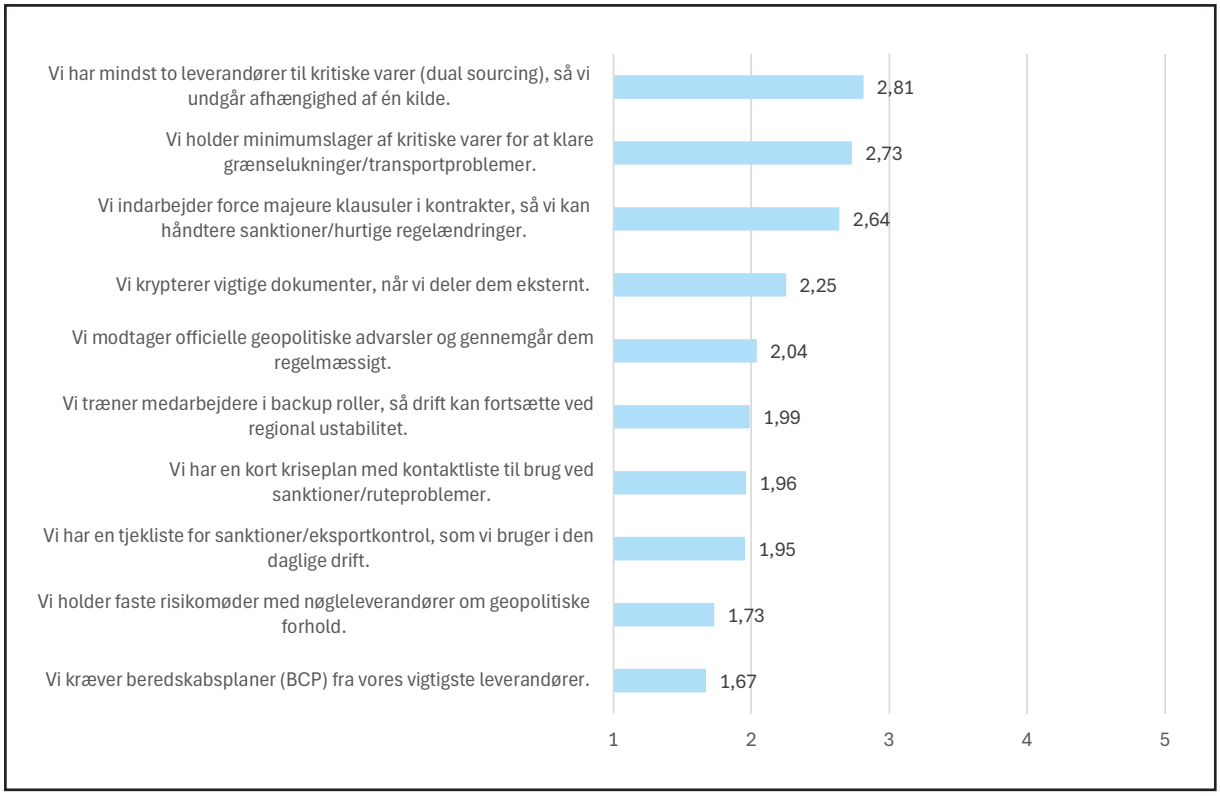
4.11 Geopolitisk risikostyring

Rapportens formål er at afdække konkret praksis og resultaterne for geopolitisk risikostyring. Figur 4.15 viser tydeligt afstanden mellem trusselsbilledet og handlingen.

Virksomhederne forlader sig primært på traditionelle, isolerede forsyningskædeværktøjer: De etablerer dual sourcing (et gennemsnit på 2,81), opretholder minimumslagre (et gennemsnit på 2,73) og indarbejder force majeure-klausuler (et gennemsnit på 2,64). Derimod fejler de eklatant, når det kommer til integration og samarbejde i forsyningskæden, hvilket netop er et af rapportens hovedfokuspunkter.

Fokusset på tværorganisatorisk sikkerhed er alarmerende lavt. Yderst få SMV'er afholder faste risikomøder med nøgleleverandører (et gennemsnit på 1,73), og endnu færre kræver deciderede beredskabsplaner (BCP) fra deres vigtigste partnere (et gennemsnit på 1,67). Ligesom rapporten fastslår, at cybersikkerhed ikke længere er et internt IT-anliggende, beviser disse tal, at geopolitiske risici ikke kan løses ved blot at købe mere og lagerføre det. Det kræver fælles governancemekanismer i værdikæden.

Figur 4.15: Geopolitisk risikostyring



Resultaterne tydeliggør et kritisk behov for den procesmodel og de trænings-forløb, projektet tilbyder, for at flytte SMV'erne fra en passiv tilstand til et niveau, hvor resiliens integreres aktivt på tværs af forsyningskæden.

5. Konklusion

Denne rapport har haft til formål at undersøge praksis med cybersikkerhed i danske produktions-SMV'er. Dette er sket gennem en landsdækkende spørgeskemaundersøgelse, hvor 1.434 SMV'er er kontaktet med henblik på deltagelse i undersøgelsen. 245 virksomheder ønskede at deltage i undersøgelsen, og ud af disse har 155 levereret fulde svar, hvilket fører til en svarprocent på 10,7 ud af de samlede kontaktede virksomheder og 62,9 % ud af de virksomheder, der accepterede at deltage i undersøgelsen. Undersøgelsen søger at give svar på følgende spørgsmål:

1. I hvilket omfang opfattes cybersikkerhed som teknisk komplekst?
2. Hvad er den konkrete praksis med IT-/OT-integration?
3. I hvilket omfang har virksomhederne oplevet cyberangreb?
4. I hvilket omfang møder SMV'er krav til cybersikkerhed fra forskellige interessenter?
5. I hvilket omfang er virksomheder underlagt NIS 2 compliancekrav?
6. I hvilket omfang stiller man krav til cybersikkerhed mod kunder og leverandører?
7. I hvilket omfang har virksomheder fokus på cybersikker supply chain risk management?
8. I hvilket omfang opfanger SMV'er muligheder med cybersikkerhed, hvordan udnyttes mulighederne, og hvordan ændrer og tilpasser SMV'erne sig (cybersikre dynamiske kapabiliteter)?
9. I hvilket omfang er SMV'er påvirket af geopolitiske markedskræfter?
10. I hvilket omfang opfanger SMV'er muligheder med geopolitiske markedspåvirkninger, hvordan udnyttes mulighederne, og hvordan ændrer og tilpasser SMV'er sig (dynamiske kapabiliteter for geopoli tiske markedspåvirkninger)?
11. I hvilket omfang arbejder SMV'er med geopolitisk risikostyring?

På spørgsmålet om, *i hvilket omfang cybersikkerhed opfattes som teknisk komplekst* oplever virksomhederne ikke høj intern teknisk kompleksitet. Alle udsagn scorer omkring 2 på en 5-punkts Likert-skala (gennemsnit fra 1,62 til 2,12), svarende til 'i mindre grad', om end der kan være variationer bag gennemsnittene. Samlet tyder tallene på et relativt godt niveau både ift. rettidig installation af sikkerhedsopdateringer (med et gennemsnit på 1,62), overblik over tilsluttede enheder (med et gennemsnit på 2,03) og tilpasning af cybersikkerhed til OT-systemer (med et gennemsnit på 2,12). Respondenterne svarer på spørgsmålet om *deres konkrete erfaringer med OT-/IT-integration*, at de i nogen til høj grad har styr på integrationen mellem IT og OT, særligt hvad angår overblik over aktiver, sikre kommunikationsprotokoller og netværkssegmentering, som alle fremstår som signifikante styrker. 25 % af respondenterne svarer, at de indenfor de seneste par år *har været ramt af et cyberangreb*. På spørgsmålet om de virksomheder, respondenterne repræsenter, er *omfattet af NIS 2*, angiver 22 %, at de er omfattet af NIS 2-direktivet, mens 67 % angiver, at de ikke er. 11 % svarer 'ved ikke'. Hvad angår *krav til cybersikkerhed fra virksomhedens interessenter*, drives dette primært af ledelsen og i mindre grad af bestyrelsen, hvor sidstnævnte kun har øget sit fokus marginalt siden 2024, hvilket tyder på et fortsat begrænset pres fra bestyrelsesniveau trods stigende opmærksomhed i omverdenen. På spørgsmålet om *i hvilket omfang der stilles krav til cybersikkerhed mod kunder og leverandører*, viser resultaterne, at virksomhederne kun i begrænset omfang stiller cybersikkerhedskrav i deres aftaler både over for leverandører og kunder, hvilket peger på en lav modenhed i håndteringen af cybersikkerhed i værdikæden.

Respondenterne er blevet bedt om at tage stilling til deres brug af 10 praksisser indenfor *cybersikker supply chain risk management*, og resultatet viser gennemsnitsværdier fra 2,86 som det højeste til 1,82 som det laveste på de 10 praksisser. Det samlede resultat peger på et lavt fokus på cybersikker supply chain risk management og dermed et stort udviklingsbehov i virksomhederne. I fht. hvilket omfang SMV'erne *opfanger muligheder med cybersikkerhed, hvordan mulighederne udnyttes, og hvordan SMV'erne ændrer og tilpasser sig* (cybersikre dynamiske kapabiliteter) svarer respondenterne med et bekymrende lavt fokus på sensing, seizing og transforming kapabiliteter med gennemsnitsværdier, på 2,0, 1,94 og 2,4. De lave niveauer viser, at SMV'er i begrænset omfang både opdager, udnytter og tilpasser sig cybersikkerhedsrelaterede muligheder og trusler. Det øger risikoen for sene eller utilstrækkelige reaktioner på cyberangreb og svækker virksomhedernes evne til at opbygge langsigtet robusthed i et stadig mere komplekst trusselsbillede. Respondenterne svarer, at de i nogen grad til lav grad er *påvirket af geopolitiske markedskræfter*. Det højeste gennemsnit opnås ved statssponsorerede cyberangreb, der har øget SMV'erne bekymring for IT-sikkerhed med et gennemsnit på 2,98. Krige og uligheder opnår et gennemsnit på 2,90. I den anden ende ligger nye EU-sanktioner som har øget usikkerheden om kontrakter og betalingsstrømme med et gennemsnit på 2,25.

På spørgsmålet, om i hvilket omfang SMV'erne *opfanger muligheder med geopolitiske markedspåvirkninger, hvordan mulighederne udnyttes, og hvordan SMV'erne ændrer og tilpasser sig (dynamiske kapabiliteter for geopolitiske markedspåvirkninger)*, opnås der generelt lave gennemsnitsværdier for de tre grupper af kapabiliteter. *Sensing*-kapabiliteter for geopolitiske markedspåvirkninger opnår et gennemsnit på 2,04, *seizing*-kapabiliteter opnår et gennemsnit på 2,36 og *transforming*-kapabiliteter et gennemsnit på 2,15. Produktions-SMV'er bør systematisk styrke deres dynamiske kapabiliteter i forhold til geopolitiske markedspåvirkninger – særligt deres evne til at identificere (sensing), udnytte (seizing) og organisatorisk implementere forandringer (transforming). Svar på det sidste spørgsmål angående *i hvilket omfang SMV'erne arbejder med geopolitisk risikostyring* er ikke ligefrem opmuntrende. På de 10 udsagn om risikostyringspraksisser opnås der et gennemsnit fra 2,81 (lidt under i nogen grad) til 1,67 (lidt under i lav grad).

En undersøgelse som denne indebærer en række metodiske begrænsninger. For det første er der tale om en kvantitativ tilgang, som primært belyser omfanget af de undersøgte tiltag, men ikke forklarer de bagvedliggende årsager; dette kan med fordel uddybes gennem kvalitative studier som casestudier. For det andet baserer undersøgelsen sig på én besvarelse pr. virksomhed, hvilket kan begrænse validiteten, og fremtidige studier bør derfor inddrage flere respondenter. Endelig afhænger det samlede billede af cybersikkerhed af de specifikke spørgsmål, der er stillet, og da cybersikkerhed i et supply chain-perspektiv fortsat er et relativt nyt område, er der behov for en yderligere begrebsmæssig udvikling.

6. Referencer

Afshari-Mofrad, M., Abedin, B. & Amrollahi, A. (2024), ”Developing dynamic capabilities to increase cybersecurity policymaking agility and resilience”, *PACIS 2024 Proceedings*, Pacific Asia Conference on Information Systems.

Allianz (2026), *Allianz Risk Barometer 2026: Cyber Remains Top Business Risk but AI Fastest Riser* at #2, Allianz, https://commercial.allianz.com/news-and-insights/news/allianz-risk-barometer-2026.html (tilgået 3. marts 2026).

Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A. & Fallon, M. (2022), *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, National Institute of Standards and Technology, U.S. Department of Commerce.

Chadge, A., Weiβ, M., Caldwell, N.D. & Wilding, R. (2020), “Managing cyber risk in supply chains: a review and research agenda”, *Supply Chain Management: An International Journal*, Vol. 25 No. 2, pp. 223-240.

Colicchia, C., Creazza, A. & Menachof, D.A. (2019), “Managing cyber and information risks in supply chains: insights from an exploratory analysis”, *Supply Chain Management: An International Journal*, Vol. 24 No. 2, pp. 215-240.

Culot, G., Nassimbeni, G., Podrecca, M. & Sartor, M. (2021), “The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda”, *The TQM Journal*, Vol. 33 No. 7, pp. 76-105.

Darktrace (2023), *Center for Internet Security: The 18 Critical Security Controls*, Darktrace Holdings Limited, Cambridge, UK, tilgå materialet her.

Edwards, J. (2024), *Critical Security Controls for Effective Cyber Defense: A Comprehensive Guide to CIS 18 Controls*, Apress, New York.

European Commission (2026), https://digital-strategy.ec.europa.eu/en/policies/nis2-directive, tilgået 3. april, 2026.

European Commission (2020), *User Guide of the SME Definition*, The European Union, Luxembourg.

Farrell, H. & Newman, A.L. (2019), “Weaponized interdependence: How global economic networks shape state coercion open access”, *International Security*, Vol. 44 No. 1, pp. 42-79.

Forsman, H. (2008), “Business development success in SMEs: A case study approach”, *Journal of Small Business and Enterprise Development*, Vol. 15 No. 3, pp. 606-622.

Ghobakhloo, M. (2018), “The future of manufacturing industry: a strategic roadmap toward Industry 4.0”, *Journal of Manufacturing Technology Management*, Vol. 29 No. 6, pp. 910-936.

Herburger, M., Wieland, A. & Hochstrasser, C. (2024), “Building supply chain resilience to cyber risks: a dynamic capabilities perspective”, *Supply Chain Management: An International Journal*, Vol. 29 No. 7, pp. 28–50.

Kull, T.J., Kotlar, J. & Spring, M. (2018), “Small and medium enterprise research in supply chain management: The case for single-respondent research designs”, *Journal of Supply Chain Management*, Vol. 54 No. 1, pp. 23-34.

Löfving, M., Säfsten, K. & Winroth, M. (2014), “Manufacturing strategy frameworks suitable for SMEs”, *Journal of Manufacturing Technology Management*, Vol. 25 No. 1, pp. 7-26.

Melnyk, S.A., Schoenherr, T., Speier-Perob, C., Peters, C., Chang, J.F. & Friday, D. (2022), “New challenges in supply chain management: cybersecurity across the supply chain”, *International Journal of Production Research*, Vol. 60 No.1, pp.162-183.

Müller, J.M., Buliga, O. & Voigt, K.-I. (2018), “Fortune favors the prepared: How SMEs approach business model innovations in Industry 4.0”, *Technological Forecasting & Social Change*, Vol. 132, pp. 2-17.

NIST (National Institute of Standards and Technology) (2024), *The NIST Cybersecurity Framework (CSF)* 2.0., National Institute of Standards and Technology, Gaithersburg, MD.

OECD (2023), *OECD SME and Entrepreneurship Outlook 2023*, OECD Publishing, Paris.

Pal, R., Torstensson, H. & Mattila, H. (2014), “Antecedents of organizational resilience in economic crises - an empirical study of Swedish textile and clothing SMEs”, *International Journal of Production Economics*, Vol. 147 (PART B), pp. 410–428.

Rid, T. (2020), *Active Measures: The Secret History of Disinformation and Political Warfare*, Picador, London.

Ruhl, C., Hollis, D., Hoffman, W. & Maurer, T. (2020), *Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads*, Carnegie Endowment for International Peace, Washington, DC.

Ruohonen, J. (2024), “A systematic literature review on the NIS2 Directive”, https://arxiv.org/abs/2412.08084.

Segal, A. (2016), *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*, PublicAffairs, New York.

Sosafe (2025), *Cybercrime Trends 2025: The Latest Threats and Security Best Practices*, Sosafe, Cologne.

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: An International Journal*, Vol. 30 No. 5 pp. 497–517.

Stentoft, S., Mikkelsen, O.S., Schmitt, O., Keating, V., Theussen, A., Peressotti, M., Mayer, P., Kankam-Boateng, J. & Tumchewics, L. (2024), *Cybersikkerhed i små og mellemstore danske produktionsvirksomheder*, Institut for Erhverv og Bæredygtighed, SDU, Center for War Studies, SDU, Institut for Matematik og Datalogi, SDU samt Forsvarsakademiet.

Stentoft, J., Mikkelsen, O.S. & Rajkumar, C. (2018), *Supply Chain Management: Sources for Competitive Advantages*, Hans Reitzels Forlag, Copenhagen.

Storey, D. (1994), *Understanding the Small Business*, Thomson, London.

Teece, D.J., Pisano, G. & Shuen, A. (1997), "Dynamic capabilities and strategic management", *Strategic Management Journal*, Vol. 18 No. 7, pp. 509-533.

Teece, D.J. (2007), "Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance", *Strategic Management Journal*, Vol. 28 No. 13, pp. 1319-1350.

Valeriano, B., Jensen, B. & Maness, R. (2018), *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford University Press, Oxford.

Vossen, E.W. (1998), "Relative strength and weaknesses of small firms in innovation", *International Small Business Journal: Researching Entrepreneurship*, Vol. 16 No. 3, pp. 88-94.

Zach, O., Munkvold, B.E. & Olsen, D.D. (2014), "ERP system implementation in SMEs: Exploring the influences of the SME context", *Enterprise Information Systems*, Vol. 8 No. 2, pp. 309-335.

Om forfatterne

Jan Stentoft, ph.d., er professor i supply chain management ved Institut for Erhverv og Bæredygtighed på Syddansk Universitet. Hans forskning er anvendelsesorienteret, og hans forskningsinteresser og undervisning er relateret til supply chain management, supply chain resilience, cybersikkerhed, geopolitik, supply chain innovation, lean filosofi, sales & operations planning og lokalisering af produktion fra et globalt perspektiv med vægt på brugen af nye digitale teknologier. Jan har praktisk industrierfaring fra stillinger hos Dandy, Gumlink og LEGO og fra løbende opgaver som ledelseskonsulent.

Ole Stegmann Mikkelsen, ph.d., er lektor i supply chain management ved Institut for Erhverv og Bæredygtighed på Syddansk Universitet. Hans forskningsmæssige interesser og undervisning ligger indenfor supply chain management, supply chain resilience og risk management, strategisk og global sourcing, supply chain innovation, sales & operations planning og lokalisering af produktion fra et globalt perspektiv. Ole har praktisk industrierfaring fra stillinger hos Milliken Denmark A/S og Danfoss A/S.

Kent Adsbøll Wickstrøm, ph.d., er lektor ved Institut for Erhverv og Bæredygtighed inden for organisationsteori på Syddansk Universitet. Hans forskningsmæssige interesser og undervisning ligger indenfor organisationsdesign, organisationsadfærd, digital transformation, digital strategi, teknologiledelse, videnledelse, og supply chain resilience. Kent er forskningsgruppeleder for Supply Chain og Technology Management og ansvarlig for cand.merc.-linjen Data Driven Business Development på SDU.

Vincent Keating, ph.d., er lektor ved Center for War Studies på Syddansk Universitet. Hans forskning falder indenfor sikkerhedsstudier fra politisk sociologi og politisk teoris perspektiv. Vincents tidligere forskning har undersøgt, hvordan stater og ikke-statslige organisationer opretholder tillid og legitimitet, hvordan den ideologiske tiltrækning af russiske værdier får vestlige populistiske grupper til at støtte russisk udenrigspolitik, og hvordan stater træffer valg mellem menneskerettigheder og sikkerhed.

Louise Tumchewics er ph.d, og post.doc. hos Center for War Studies på Syddansk Universitet. Louise har opnået sin ph.d. i krigsstudier ved King's College London. Hendes forskning fokuserer på krig og teknologi, økonomisk krigsførelse og civil-militære relationer. Før hun kom til SDU, var Louise seniorforsker ved den britiske hærs Center for Konfliktforskning (CHACR), adjunkt ved Rabdan Academy i De Forenede Arabiske Emirater og Visiting

Research Fellow ved King's College London. Louise er redaktør af Small Armies, Big Cities – en undersøgelse af moderne bykrigsførelse, og så er hun forfatter til to kommende bøger.

Amelie Theussen, ph.d., er lektor ved Forsvarsakademiet og faglig leder for Center for Arktisk Sikkerhedsstudier. Hun forsker i sikkerhedssituationen i Arktis og Østersøregionen, dansk og tysk sikkerheds- og forsvarspolitik og spørgsmålet om, hvordan krig forandrer sig, og hvilke konsekvenser det har for politiske og juridiske normer omhandlende magtanvendelse. Desuden designer og gennemfører hun prisvindende simulationsøvelser for universiteter og militære uddannelser.

Marco Peressotti, ph.d., er lektor ved Institut for Matematik og Datalogi, Syddansk Universitet. Marcos forskningsmæssige mission er at gøre det mere effektivt at programmere, analysere og sikre digitale systemer. Han udvikler nye metoder og værktøjer til at støtte udvikling og vedligeholdelse af korrekt og sikkert software specielt til sammenkoblede systemer, der udgør kernen i den digitale omstilling. Et overordnet tema i hans forskningsmetode er brugen af teknikker fra cybersikkerhed, kunstig intelligens og programmeringssprog samt målet om et sammenfattende matematisk perspektiv.

Peter Mayer, ph.d., er lektor ved Institut for Matematik og Datalogi, Syddansk Universitet. Peter forsker i "End-user Viable Information Security & Privacy Solutions". Derved, uafhængigt af, om slutbrugeren af en sikkerhedsløsning er en lægmand, en administrator eller en udvikler, ligger fokus på at gøre sikkerheds- og privatlivsløsninger levedygtige for målgruppen ved at tage hensyn til deres specifikke behov og kompetencer. En vigtig rolle i denne forskning spiller på forståelse af slutbrugeres mentale modeller, dvs., på hvilke måder de tror, cybersikkerhed påvirker dem, samt hvor effektive modforanstaltninger er.

Judith Kankam-Boateng er ph.d.-studerende ved Institut for Matematik og Datalogi, Syddansk Universitet. Judith er bachelor i informationsteknologi og har en mastergrad i jura, digital innovation og bæredygtighed med fokus på digitalisering. Hun har en stor forskningsmæssig interesse i databaser, programmering og softwareudvikling. Judith har bl.a. arbejdet som undervisningsassistent for et kursus i nye teknologier i AI, ML og Blockchain Technologies. Hun har ekspertise indenfor ERP Microsoft Dynamics NAV 2018, og så har hun erfaring som Business Analyst, Product Owner og Scrum Master.

Projektet Cybersikkerhed og Forretningskontinuitet er gennemført som ét projekt i en samlet portefølje af fem projekter i en temaindkaldelse hos Industriens Fond om cybersikkerhed i værdikæderne. De fem projekter er:

1. Cybersikkerhed og Forretningskontinuitet (læs mere her).
2. Cyber Safe Robotics (læs mere her).
3. Styrket cybersikkerhed for SMV'er. (læs mere her).
4. Cybersikre fødevareværdikæder (læs mere her).
5. Cybersikre værdikæder (læs mere her).

INDUSTRIENS FOND
SDU Syddansk Universitet
FORSVARSAKADEMIET