SMV'ers cybersikkerhed og forretningskontinuitet: Resultater og perspektiver

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

April 2026

CYBERSIKKERHED OG FORRETNINGSKONTINUITET

SMV'ers cybersikkerhed og forretningskontinuitet: Resultater og perspektiver

ISBN: 97887-85464-22-4

Korrektur:
Tekst og Web, Kolding

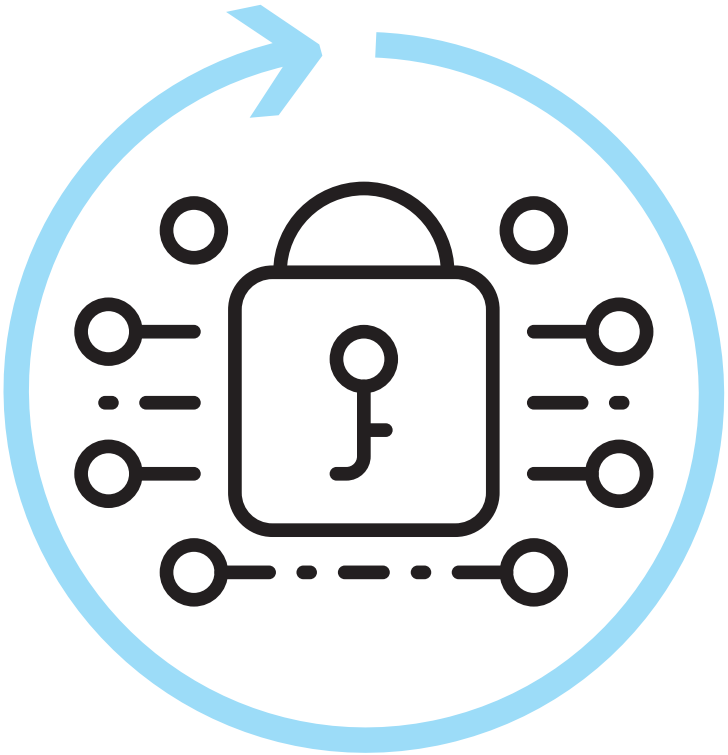
Opsætning/layout:
TadaahGrafisk Design og Web, Kolding

Print:
Inprint, Kolding

Oplag:
1000 eksemplarer

Dette er den afsluttende rapport i projektet
"Cybersikkerhed og Forretningskontinuitet",
der er gennemført med økonomiske midler fra Industriens Fond.
Projektets hjemmeside er: **www.cyber-smv.dk**

Forskningsprojektet er gennemført af forskere fra Institut for
Erhverv og Bæredygtighed, Syddansk Universitet, Center for War Studies, Syddansk Universitet,
Institut for Matematik og Datalogi, Syddansk Universitet samt Forsvarsakademiet.



Indholdsfortegnelse

Forord ved Industriens Fond

I takt med, at digitaliseringen accelererer på tværs af brancher og aktiviteter, er cybersikkerhed et anliggende, der rækker langt ud over virksomhedernes IT-afdelinger. Cybersikkerhed er i dag blevet et forretningskritisk emne, som har direkte betydning for virksomheders drift, værdiskabelse og overlevelse – og som derfor vedrører alle ansatte i virksomhederne.

Udfordringen med cybersikkerhed er også stor hos små og mellemstore danske produktionsvirksomheder. Her er kompleksiteten i forsyningskæderne høj og afhængigheden af digitale systemer, leverandører og samarbejdspartnere kolossal.

Det er i det lys, at Industriens Fond gennem en dedikeret indsats stiller skarpt på cybersikkerhed i værdikæderne på tværs af dansk erhvervsliv. Virksomhedernes værdikæder er altafgørende for forretningen, og derfor skal de sikres systematisk. Det skal ske ved at styrke modstandskraften, så virksomhederne kan stå imod, når hackere angriber, og det skal ske ved at gøre virksomhederne velforberedte, så de kan fortsætte driften og leve op til deres aftaler og rolle i værdikæden både under og efter et hackerangreb.

Vigtigt for alle

Der findes desværre et forkert verdensbillede flere steder i dansk erhvervsliv. Alt for mange ledere i mindre virksomheder har fortsat den fejlopfattelse, at deres virksomheder ikke er attraktive mål for cyberkriminelle.

Både organiserede kriminelle og statslige aktører målretter hver dag angreb mod danske virksomheder – ofte via det svageste led i værdikæden. Dermed bliver også mindre virksomheder angrebet. Ikke nødvendigvis som det primære mål, men som adgangsveje til større aktører.

Derfor er cybersikkerhed og cybersikre værdikæder en aktuel tematik for alle.

Med det udgangspunkt har projektet Cybersikkerhed og Forretningskontinuitet gennem en årrække arbejdet med at cybersikre værdikæder i dansk er-

hvervsliv ud fra en tværdisciplinær tilgang med bred appel og med relevans for de fleste. En tilgang, der kan gøre cybersikkerhedsarbejdet mere komplekst, fordi mange i organisationen skal involveres, men også en tilgang, der er nødvendig grundet værdikædens mange indgange i virksomheden.

Virksomhedsrettede værktøjer

Projektet kombinerer forskning, teori og kompetenceudvikling inden for supply chain management og cybersikkerhed med scenarieudvikling og praksisnære aktiviteter hos danske virksomheder. Den kombination af viden og handling har været afgørende for at udvikle virksomhedsrettede værktøjer til at styrke forretning og værdikæder.

Værktøjerne spænder bredt og adresserer især cybersikkerhed i et forsyningskædeperspektiv, hvor fokus rækker langt ud over den enkelte virksomheds egne fire vægge. Et af de mest centrale værktøjer er en digital løsning, som understøtter arbejdet med en supply chain resilience procesmodel, der hjælper virksomheder med at arbejde systematisk og tværorganisatorisk for at identificere og håndtere sårbarheder i - og angreb på værdikæden.

For at illustrere og konkretisere angreb har projektet også udviklet en række fremtidsscenarier, der beskriver forskellige kritiske situationer. Scenarierne understøtter virksomheders arbejde med beredskab gennem simulationer, og de tvinger virksomhederne – og de ledelsesmæssige nøglepersoner – til at besvare en række væsentlige spørgsmål: hvad gør vi i sådan et scenarie, hvem gør hvad, hvornår og hvordan gør vi det, og hvor er vores svagheder?

En sikker investering

Med værktøjer og scenarier ved hånden kan danske produktionsvirksomheder arbejde mere systematisk og strategisk med cybersikre værdikæder. Og det er nødvendigt. Både for den enkelte virksomhed og for erhvervslivet generelt.

Et øget fokus på cybersikkerhed skaber en mere sikker virksomhed og minimerer en række risici. Men derudover er det en investering, der gør virksomheden mere attraktiv for kunder og samarbejdspartnere. Derfor håber vi, at mange virksomheder tager denne rapport og de nye værktøjer til sig og omsætter dem til konkurrencekraft og vækst.

God læse- og arbejdslyst!

Malene Stidsen
Programchef
Industriens Fond

Projektgruppens forord

Denne afsluttende rapport om projektet Cybersikkerhed og Forretningskontinuitet er resultatet af et treårigt forskningsprojekt, der er gennemført for **Industriens Fond** af medarbejdere fra Institut for Erhverv og Bæredygtighed, Syddansk Universitet, Center for War Studies, Syddansk Universitet, Institut for Matematik og Datalogi, Syddansk Universitet og Forsvarsakademiet i perioden september 2023 til juni 2026. Projektet har haft til formål at styrke danske produktions-SMV'ers cybersikkerhed i en stadig mere urolig verden. Målet er således, at målgruppen styrker og udvikler sin forståelse og praksis med cybersikkerhed, så det kan bidrage til konkurrencemæssige fordele.

Den nuværende geopolitiske uro, præget af konflikter, handelskonflikter og øget rivalisering blandt stormagter, har skabt et mere uforudsigeligt trusselsbillede - også i cyberspace. For danske produktions-SMV'er betyder det en markant forhøjet risiko for cyberangreb, da de ofte indgår i internationale forsyningskæder og dermed kan blive indirekte mål i større strategiske konflikter. Samtidig har mange mindre virksomheder begrænsede ressourcer til IT-sikkerhed, hvilket gør dem særligt sårbare over for f.eks. ransomware, industrispionage og leverandørkædeangreb. Kombinationen af global ustabilitet og digital afhængighed øger derfor behovet for, at SMV'er prioriterer cybersikkerhed som en central del af deres risikostyring.

Rapporten præsenterer 30 værktøjer, der kan hjælpe danske produktions-SMV'er med at blive bedre rustet mod cyberangreb. Projektet bygger videre på et tidligere initiativ støttet af **Industriens Fond**, hvor der blev udviklet en procesmodel til at styrke modstandsdygtigheden i forsyningskæder (Stentoft, Mikkelsen & Kjær, 2023). En central erfaring fra dette arbejde – som er blevet yderligere bekræftet i nærværende cyberprojekt – er, at intern dialog og tværgående samarbejde på tværs af funktioner som salg, produktion, indkøb, økonomi, IT og produktudvikling er afgørende. Det er netop denne involvering, der sikrer, at virksomhederne arbejder med de mest relevante indsatser for at styrke både supply chain resilience og cybersikkerhed (Stentoft & Mikkelsen, 2024).

Rapporten anbefaler derfor, at virksomheder starter med procesmodellen for supply chain resilience, som består af fire faser. I nærværende projekt er fase 2 og 3 blevet videreudviklet og kodet til et open source-software. Procesmodellen har fokus på først at identificere sårbarheder, risici og nødvendige kapabiliteter i forsyningskæden, hvilket hænger sammen med, at projektet er

finansieret under et call fra **Industriens Fond** om cybersikre forsyningskæder. Erfaringerne fra det tidligere projekt viste, at mange virksomheder havde begrænset praksis for tværorganisatorisk samarbejde om at forstå konkrete udfordringer i deres forsyningskæder. Arbejdet med procesmodellen skabte nye dialoger og en bedre forståelse af sårbarheder, hvilket gjorde det lettere at prioritere de begrænsede ressourcer.

I det 'nye' projekt arbejdede virksomhederne derfor med alle fire faser i procesmodellen for at etablere et fælles udgangspunkt på tværs af virksomheden. En vigtig pointe er, at cybersikkerhed ikke kan placeres isoleret i IT-afdelingen – det er et fælles ansvar for hele virksomheden, hvorfor det er vigtigt, at arbejdet er forankret i ledelsen.

Der er en række personer og organisationer, som har bidraget til projektet, og som vi gerne vil takke. Vi vil først og fremmest rette en stor tak til **Industriens Fond** for at have prioriteret projektet og dermed gjort det muligt at gennemføre det. Dernæst vil vi gerne sige tak til projektets styregruppe, dekan **Marianne Holmer**, Syddansk Universitet, branchedirektør **Andreas Holbak Espersen**, DI, direktør **Pernille Kræmmergård**, DI2X, ejer **Kristian Fischer**, KFISCH og direktør **Søren Vammen**, Zoriac, for jeres engagement og konstruktive input. Vi vil også gerne takke den tilknyttede referencegruppe, der har bestået af vicedirektør **Henrik Findahl Brodersen**, Styrelsen for Samfundssikkerhed, underdirektør **Joachim Finkielman**, DI, adm. direktør **Morten Bjørn Hansen**, Business Kolding, Manager **Zaynab Al-Hussaini**, Capgemini Invent, chefkonsulent **Berit Aadal**, Dansk Standard og projektleder **Tina Højrup Kjær**, Odense Robotics. Vi har arbejdet med 30 forskellige virksomheder i to forløb. Vi siger tak til de medarbejdere, der har deltaget og dermed bidraget til at realisere projektet.

I projektets andet forløb med virksomheder har studerende bidraget til at facilitere arbejdet med supply chain resilience procesmodellen i virksomhederne. Vi vil gerne rette en stor tak til **Sarah Elvira Johansen**, **Sander Guldbrandsen**, **Matilde Damgaard Magnussen**, **Pirjo Adele Elisabeth Brændeholm**, **Jonas Skovdam Jørgensen**, **Julie Nyhuus Gill** og **Anne Cecilie Karlsen**, som alle er cand.merc.-studerende ved Syddansk Universitet i Kolding.

April 2026

Jan Stentoft, professor, Syddansk Universitet
Ole Stegmann Mikkelsen, lektor, Syddansk Universitet
Kent Adsbøll Wickstrøm, lektor, Syddansk Universitet
Vincent Keating, lektor, Syddansk Universitet
Louise Tumchewics, post.doc., Syddansk Universitet
Olivier Schmitt, professor, Forsvarsakademiet
Amelie Theussen, lektor, Forsvarsakademiet
Marco Peressotti, lektor, Syddansk Universitet
Peter Mayer, lektor, Syddansk Universitet
Judith Kankam-Boateng, ph.d.-studerende, Syddansk Universitet

1.
Indledning

Den digitale transformation har de seneste årtier fundamentalt ændret vilkårene for danske produktions-SMV'er. Produktionsapparatet er i dag tæt integreret med digitale styringssystemer, cloud-baserede platforme, automatiserede logistikløsninger og globale leverandørnetværk. Samtidig er forsyningskæderne blevet mere komplekse og internationalt forbundne. Denne udvikling har skabt betydelige effektivitetsgevinster og nye forretningsmuligheder, men den har også øget virksomhedernes sårbarhed over for cybertrusler markant. I takt med, at produktion, lagerstyring, indkøb, kvalitetssikring og distribution er blevet digitalt sammenkoblet, er cybersikkerhed ikke længere alene et IT-anliggende, men et strategisk og forretningskritisk spørgsmål.

Dette treårige projekt har haft til formål at styrke danske små og mellemstore produktionsvirksomheders (produktions-SMV'ers) cybersikkerhed med særligt fokus på forsyningskæden. Udgangspunktet har været erkendelsen af, at trusselsbilledet i stigende grad retter sig mod hele økosystemer frem for enkeltstående virksomheder. Angreb rammer ikke nødvendigvis den største eller mest modne aktør direkte, men kan ske via mindre leverandører, servicepartnere eller underleverandører med svagere sikkerhedsforanstaltninger. Dermed bliver cybersikkerhed et fælles ansvar i forsyningskæden og en forudsætning for robusthed, konkurrenceevne og tillid.

1.1 Forstyrrelser i forsyningskæderne

Forsyningskæder påvirkes i stigende grad af en bred vifte af forstyrrelser, der både kan være fysiske, organisatoriske og digitale. Traditionelt har virksomheder fokuseret på risici som f.eks. naturkatastrofer, brand, strejker, pandemier, geopolitiske spændinger, handelsrestriktioner og transportmæssige flaskehalse. Disse hændelser kan medføre leveranceforsinkelser, mangel på kritiske komponenter og markante prisudsving. I de senere år er cyberrelaterede forstyrrelser imidlertid blevet en lige så væsentlig risikofaktor. Når forsyningskæder er digitalt integrerede gennem fælles ERP-systemer, lagerstyring, produktionsplanlægning, EDI-løsninger og cloud-platforme, kan et cyberangreb ét sted i kæden hurtigt få konsekvenser for alle øvrige aktører. Et ransomware-angreb mod en logistikleverandør kan f.eks. lamme booking- og trackingsystemer, hvilket forsinker transport og skaber usikkerhed om vareflows. Kompromitterede leverandørkonti kan føre til svindel via falske fakturaer eller ændrede betalingsoplysninger. Manipulation af produktionsdata eller tekniske specifikationer kan resultere i fejlproduktion og kvalitetsproblemer, som først opdages sent i processen. Dermed fungerer cybersikkerhed både som en selvstændig risikofaktor og som en forstærker af eksisterende forstyrrelser. Digitale sårbarheder kan udløse driftsstop, skabe informationsasymmetri og forringe beslutningsgrundlaget i hele værdikæden. Jo mere kompleks og global forsyningskæden er, desto større er afhængigheden af stabile og sikre digitale forbindelser og desto mere kritisk bliver en systematisk og koordineret indsats for cybersikkerhed på tværs af aktørerne.

1.2 Cybersikkerhed som forretnings-kritisk faktor

Cybersikkerhed i produktions-SMV'er handler ikke kun om at beskytte data, men i lige så høj grad om at beskytte drift, leveringssikkerhed, kvalitet og omdømme. Produktionsmiljøer er i stigende grad baseret på industrielle kontrolsystemer (ICS), SCADA-løsninger og IoT-enheder, som kobler den fysiske produktion sammen med digitale styrings- og overvågningssystemer. Dette kaldes også Operational Technology (OT). Disse systemer har traditionelt været designet med fokus på driftssikkerhed og effektivitet og ikke nødvendigvis med cybersikkerhed som primær prioritet. Når de i dag forbindes til virksomhedens øvrige IT-systemer og eksterne netværk, opstår nye angrebsflader.

Et vellykket cyberangreb kan få direkte og umiddelbare konsekvenser for produktionen. Ransomware-angreb, hvor virksomhedens systemer krypteres og først frigives mod betaling, har i flere tilfælde medført fuldstændig nedlukning af produktionslinjer i dage eller uger. For en produktions-SMV kan selv kortvarige driftsstop medføre betydelige økonomiske tab i form af mistet omsætning, kontraktbrud, forsinkede leverancer og øgede omkostninger til genopretning.

Et konkret eksempel er globale angreb, hvor produktions-SMV'er har måttet standse driften midlertidigt, fordi centrale systemer til planlægning og styring ikke var tilgængelige. I sådanne situationer påvirkes ikke blot den enkelte virksomhed, men hele forsyningskæden. Leverandører kan ikke levere som planlagt, og kunder modtager ikke deres varer rettidigt. For virksomheder med just-in-time-produktion kan selv mindre forstyrrelser få kædereaktioner med omfattende konsekvenser.

Cyberkriminalitet har i de senere år udviklet sig fra isolerede hackeraktiviteter til en mere organiseret og professionaliseret praksis med klare industrielle træk. Som beskrevet i *Usynlig fjende – Hackerangreb og hemmelige netværk* af Espersen, Sjøberg & Kaastrup (2026) opererer moderne cyberkriminelle i netværk, hvor opgaver er specialiserede, og hvor både værktøjer, adgang og data handles på skjulte markedspladser. Data er i stigende grad blevet en handelsvare, og angreb som ransomware illustrerer, hvordan digitale trusler er blevet kommercialiserede og skalerbare. Samtidig udviskes grænsen mellem traditionel kriminalitet og statssponsorerede aktiviteter, hvilket øger kompleksiteten i trusselsbilledet. Bogen peger også på, hvordan sociale manipulationsteknikker og teknologiske værktøjer kombineres, hvilket gør cyberkriminalitet både teknisk og menneskeligt forankret. Samlet set understøtter dette en forståelse af cyberkriminalitet som en struktureret og markedsdrevet aktivitet med karakteristika, der minder om en industri.

1.3 Forsyningskæden som angrebsvej

Et centralt fokus i dette projekt har været forsyningskædeperspektivet. Digitaliseringen har medført en tæt integration mellem virksomheder og deres leverandører. Deling af produktionsdata, tegninger, forecasts, ordresystemer og kvalitetsdokumentation sker ofte via digitale platforme med direkte adgang mellem organisationer. Hver integration repræsenterer en potentiel sårbarhed.

Angribere udnytter i stigende grad det svageste led i kæden. Et mindre IT-modent underleverandørfirma kan blive kompromitteret og herefter fungere som indgang til en større virksomhed. Dette kan f.eks. ske gennem kompromitterede loginoplysninger, inficerede softwareopdateringer eller manipulerede filer. I sådanne tilfælde bliver den ramte virksomhed offer for et indirekte angreb, hvor tilliden i samarbejdet misbruges.

Konsekvenserne kan være omfattende. Hvis en leverandørs systemer kompromitteres, kan det føre til manipulation af produktionsdata, ændringer i tekniske tegninger eller indsættelse af skadelig kode i software, der anvendes i produktionen. I værste fald kan dette medføre fejlproduktion, sikkerhedsrisici for slutbrugere eller tilbagekaldelser af produkter. Derudover kan følsomme oplysninger om kunder, priser, kontrakter og produktudvikling lækkes, hvilket kan svække virksomhedens konkurrenceposition.

Et særligt alvorligt scenarie er kompromittering af softwareleverancer. Hvis en leverandør leverer opdateringer eller styringssoftware til produktionsudstyr, og denne leverance er kompromitteret, kan angrebet spredes til alle kunder, der installerer opdateringen. Dermed bliver ét kompromitteret led i forsyningskæden en multiplikator for risiko.

Kronik: Et svagt led kan lamme os alle – derfor kræver forsyningskæder stærk cybersikkerhed (sammendrag)

Forestil dig, at en enkelt leverandør i en global forsyningskæde rammes af et cyberangreb. Produktionen går i stå, logistikken bryder sammen, og samfundskritiske funktioner påvirkes. Det skyldes ikke nødvendigvis virksomhedens størrelse, men dens rolle som et afgørende led i en kæde, vi alle er afhængige af. Fra energi og fødevarer til sundhedsvæsen og transport er vores samfund i stigende grad baseret på digitale forbindelser, der gør os mere effektive – men også mere sårbare. Cyberangreb kan ramme både IT-systemer, netværk og servere samt OT-systemer, hvor fysiske processer styres digitalt. Derfor er cybersikkerhed ikke kun et anliggende for store virksomheder, men også for SMV'er.

Informationssikkerhed bygger ofte på CIA-principperne: Confidentiality (fortrolighed), Integrity (integritet) og Availability (tilgængelighed). Fortrolighed handler om at beskytte data mod uautoriseret adgang, integritet om at sikre, at information ikke ændres, og tilgængelighed om, at systemer og data er tilgængelige, når de skal bruges. Disse principper kan styrkes gennem bl.a. awareness-træning, adgangskontrol, backup, logning og beredskabsplaner.

Forsyningskæder er komplekse netværk af kunder, leverandører, transportører og producenter, som ofte anvender forskellige systemer og sikkerhedsniveauer. Data deles på tværs af organisationer og landegrænser, og sammenkoblingen af IT, OT (Operational Technology) og IoT (Internet of Things) øger risikoen for, at et enkelt angreb kan forplante sig gennem hele kæden.

Cybersikkerhed er derfor blevet en *license to operate*. Reguleringer som NIS 2 og DORA stiller krav til sikkerhed, og virksomheder møder i stigende grad cybersikkerhedskrav fra kunder, investorer og samarbejdspartnere. Organisationer uden tilstrækkelig cybersikkerhed risikerer både økonomiske tab, omdømmeskader og tab af kontrakter.

Arbejdet med cybersikkerhed bør begynde med øget bevidsthed, klare retningslinjer og prioritering af de mest kritiske systemer og data. Mindre, men kontinuerlige tiltag som backup, multifaktorgodkendelse og træning kan reducere risikoen markant. Cybertrusler er en permanent realitet, og styrket cybersikkerhed i hele forsyningskæden er afgørende for både virksomheder og samfund.

Kilde: Stentoft, Mikkelsen & Wickstrøm (2025a) *Læs kronikken her*

1.4 Konsekvenser af cyberangreb for virksomheder

Skaderne ved cyberangreb kan opdeles i direkte og indirekte konsekvenser. De direkte omfatter omkostninger til genopretning af systemer, ekstern rådgivning, juridisk bistand, bøder, eventuel løsesumsbetaling samt tabt produktion. De indirekte konsekvenser kan være endnu mere vidtrækkende. Det kan være tab af kundetillid, svækket brand, forringede markedsandele og vanskeligere adgang til nye markeder.

For danske produktions-SMV'er, som ofte indgår i internationale forsyningskæder, kan mangelfuld cybersikkerhed få betydning for adgang til samarbejde med større globale aktører. Flere internationale kunder stiller i dag eksplicitte krav til dokumenteret cybersikkerhedsniveau hos deres leverandører. Manglende modenhed kan derfor medføre eksklusion fra udbud eller partnerskaber.

Desuden er reguleringen på området under hastig udvikling. Nationale og europæiske krav til informationssikkerhed, herunder skærpede krav til kritisk infrastruktur og væsentlige sektorer, betyder, at virksomheder i stigende grad skal kunne dokumentere deres sikkerhedsforanstaltninger. Manglende efterlevelse kan føre til sanktioner og bøder samt øget tilsyn.

Et andet væsentligt aspekt er virksomhedens interne ressourcer og arbejdsmiljø. Håndtering af et større cyberangreb lægger et massivt pres på organisationen. Medarbejdere skal arbejde intensivt med genopretning, kommunikation og krisestyring. Ledelsen skal træffe hurtige beslutninger under usikkerhed, og virksomhedens fokus flyttes fra kerneforretning til krisehåndtering. Dette kan påvirke både produktivitet og trivsel.

1.5 Produktionsvirksomheders særlige udfordringer

Produktions-SMV'er adskiller sig fra mange andre typer af virksomheder ved at have en tæt kobling mellem digitale systemer og fysiske processer. Når IT og OT (Operational Technology) smelter sammen, opstår komplekse afhængigheder. En kompromittering af et IT-system kan få direkte indvirkning på maskiner, robotter og produktionsudstyr. Omvendt kan manglende opdatering eller segmentering i OT-miljøer skabe vedvarende sårbarheder.

Mange SMV'er opererer desuden med ældre udstyr, hvor opdateringer og sikkerhedsforanstaltninger er begrænsede. Udskiftning af produktionsanlæg er ofte kapitalkrævende og langsigtet, hvilket kan betyde, at sårbare systemer forbliver i drift i mange år. Samtidig kan nedlukning for opdatering eller test være forbundet med betydelige produktionsomkostninger.

I forsyningskædeperspektivet forstærkes kompleksiteten yderligere. En moderne produktions-SMV kan have hundredvis af leverandører og samarbejdspartnere på tværs af landegrænser. Overblik over sikkerhedsniveau, processer og afhængigheder kræver systematisk kortlægning og løbende dialog. Det stiller krav til governance, risikovurdering og kontraktuelle mekanismer.

1.6 Projektets relevans og formål

Med afsæt i de forrige afsnit er behovet for en målrettet indsats for at styrke cybersikkerheden i danske produktions-SMV'er tydelig. Nærværende projekt har haft til formål at udvikle, afprøve og implementere metoder og værktøjer, der kan understøtte SMV'ernes arbejde med at identificere, vurdere og håndtere cyberrisici i et forsyningskædeperspektiv.

Relevansen ligger ikke alene i at reducere risikoen for konkrete hændelser, men i at styrke SMV'ernes samlede robusthed og konkurrenceevne. En systematisk tilgang til cybersikkerhed kan bidrage til bedre risikostyring, øget transparens i værdikæden og styrket tillid mellem samarbejdspartnere. Dermed bliver cybersikkerhed et strategisk element i virksomhedens forretningsudvikling - ikke blot en omkostning.

Projektets resultater, som denne rapport præsenterer, skal ses i lyset af et dynamisk og stadigt skiftende trusselsbillede. Cybertrusler udvikler sig løbende, og nye teknologier skaber både muligheder og risici. Derfor er formålet ikke at levere en endelig løsning, men at bidrage med viden, erfaringer og anbefalinger, som kan danne grundlag for fortsat udvikling i virksomhederne.

1.7 Bestyrelsens rolle i at sikre virksomheders cybersikkerhed

Cybersikkerhed er i dag et strategisk anliggende, som bestyrelsen må forholde sig aktivt til. Digitale trusler kan påvirke drift, økonomi og omdømme, og derfor bør cyberrisici indgå som en fast del af virksomhedens samlede risikostyring. Bestyrelsen har ansvar for at fastlægge risikovillighed, sikre klare ansvarsforhold i ledelsen og modtage løbende rapportering om trusselsbillede og hændelser. Det er ikke bestyrelsens opgave at være tekniske specialister, men de skal kunne stille kvalificerede spørgsmål og sikre, at der er de rette kompetencer og ressourcer til stede. Samtidig bør der være et testet beredskab for håndtering af sikkerhedsbrud, da ingen organisation kan eliminere risikoen fuldstændigt. Endelig har bestyrelsen et ansvar for, at virksomheden overholder gældende regulering. I EU omfatter det bl.a. databeskyttelsesforordningen (GDPR).

Et søsterprojekt i cyberporteføljen: Styrket cybersikkerhed for SMV'er

Projektet "Styrket cybersikkerhed for SMV'er" er forankret hos **Erhvervshus Midtjylland** og hjælper danske SMV'er med at opbygge et stærkere og mere modstandsdygtigt digitalt beredskab. Projektet udspringer af et stigende trusselsniveau, nye regulatoriske krav som NIS 2 og virksomhedernes behov for at kunne dokumentere cybersikkerhed over for kunder og samarbejdspartnere.

Gennem projektet tilbydes virksomhederne en række målrettede aktiviteter: Gratis og uvildig 1:1-vejledning, workshops, webinarer, konferencer og adgang til konkrete værktøjer – bl.a. CyberSurvey, som hjælper virksomhederne med at afdække risici og få anbefalinger til næste skridt. Projektet styrker både virksomhedens interne sikkerhedspraksis og samarbejdet i værdikæden, hvor alle i værdikæden har et ansvar for digital robusthed/sikkerhed.

Indsatsen bygger på et landsdækkende samarbejde mellem erhvervshusene og er støttet af Industriens Fond. Målet er at gøre cybersikkerhed håndterbart og operationelt – og skabe varig værdi ved at løfte modenhedsniveauet, øge eksekveringskraften og støtte virksomhederne i at gøre cybersikkerhed til en integreret del af driften og derved sikre deres eksistens i værdikæden.

Læs mere om projektet her
Link til CyberSurvey her

2.

Teoretisk ramme

Dette afsnit giver et overblik over den teoretiske ramme, som det samlede projekt har arbejdet ud fra. Afsnittet er inddelt i otte delafsnit: 1) SMV-karakteristika, 2) forsyningskæder og risikostyring, 3) geopolitik, 4) cybersikkerhed, 5) forretningskontinuitet, 6) supply chain resilience procesmodel, 7) cybersikker supply chain risk management og 8) dynamiske kapabiliteter.

2.1 SMV'ers karakteristika

Et grundlæggende kendetegn ved produktions-SMV'er er deres begrænsede størrelse målt på antal medarbejdere og omsætning. Ifølge EU's definition har en SMV færre end 250 ansatte og en årlig omsætning på højst 50 mio. euro eller en samlet balance på højst 43 mio. euro (Europa-Kommissionen, 2003). I en dansk kontekst er langt størstedelen af produktionsvirksomhederne små eller mellemstore (SMVdanmark, 2026). Størrelsen betyder typisk kortere beslutningsveje, tæt kontakt mellem ledelse og medarbejdere samt en relativt uformel organisationsstruktur.

En anden central karakteristik er ejerledelse. Mange produktions-SMV'er er familieejede eller ledet af grundlæggeren. Det medfører ofte en stærk kobling mellem ejerskab og daglig drift, hvilket kan skabe høj beslutningshastighed og stærk værdiforankring. Omvendt kan det også betyde, at strategiske beslutninger i høj grad afhænger af én eller få nøglepersoner, hvilket kan udgøre en sårbarhed ved generationsskifte eller sygdom. Produktions-SMV'er er ofte specialiserede og nicheorienterede. I stedet for at konkurrere på volumen og stordriftsfordele fokuserer de typisk på specialproduktion, kundetilpasning og teknisk ekspertise. De indgår ofte som underleverandører i større værdikæder, som f.eks. inden for metal-, plast-, fødevare- eller maskinindustri. Denne position gør dem fleksible og i stand til hurtigt at tilpasse produktionen, men også afhængige af større kunder og konjunkturudsving. Ressourcemæssigt er produktions-SMV'er kendetegnet ved begrænsede administrative og finansielle ressourcer (Zach, Munkvold & Olsen, 2014). De har sjældent store stabsfunktioner inden for HR, IT eller strategi, og ledelsen varetager ofte flere funktioner samtidigt. Det kan fremme en praksisnær og handlingsorienteret kultur, men det kan også begrænse kapaciteten til langsigtet udvikling, digitalisering og systematisk innovation.

Mange produktions-SMV'er står teknologisk mellem det traditionelle håndværk og mere moderne automatisering. Nogle har investeret i avanceret produktionsteknologi, robotter og digitale systemer, mens andre stadig er præget af manuelle processer. Digitalisering og grøn omstilling udgør derfor både en udfordring og en mulighed. Kulturelt er produktions-SMV'er ofte præget af stærk lokal forankring. Relationer til medarbejdere, kunder og leverandører er ofte langvarige og baseret på tillid. Organisationskulturen kan være præget af høj faglighed, loyalitet og praktisk orientering.

Samlet set er produktions-SMV'er karakteriseret ved begrænset størrelse, ejerledelse, specialisering, fleksibilitet, ressourceknaphed og stærk lokal forankring. Disse karakteristika giver både styrker – såsom hurtig beslutningstagning og kundetilpasning – og udfordringer i forhold til skalering, kapitaladgang

og strategisk udvikling. Deres betydning for dansk økonomi er væsentlig, særligt som underleverandører og som drivkraft for beskæftigelse og specialiseret produktion.

Et søsterprojekt i cyberporteføljen: Cyber Safe Robotics

Cyber Safe Robotics, der er forankret hos **Odense Robotics**, har til formål at styrke cybersikkerheden og dermed konkurrenceevnen i den danske robot-, drone- og automationsindustri.

Programmet består af seks forskellige temadage om cybersikkerhed i forsyningskæden. Dagene gennemføres som workshops med en blanding af faglige indlæg fra eksperter samt deltagernes aktive arbejde med konkrete værktøjer tilknyttet de individuelle temaer som forankring af opnået viden.

Temaerne er: 1) Det regulatoriske landskab, 2) Det konkurrencemæssige potentiale, 3) Det ledelsesmæssige ansvar, 4) Samarbejde i forsyningskæden, 5) Sikkerhed i softwareudviklingen og 6) Når det går galt (beredskabsplaner).

Deltagerne får et overblik over lovgivning og standarder i forsyningskæden, så de kan gennemføre nødvendige tiltag for at sikre compliance og opnå en konkurrencemæssig fordel. Som ledelse får man indblik i og overblik over virksomhedens strategiske handlerum i forhold til cybersikkerhed gennem et forskningsbaseret værktøj, der kan understøtte arbejdet med design og implementering af cybersikkerhedsstrategier. Deltagerne får desuden viden om sikkerhed i deres supply chain samt kompetencer og konkrete værktøjer til at styrke og understøtte samarbejdet på tværs af værdikæden. Herudover bliver de introduceret til værktøjer, der understøtter sikkert design og softwareudvikling som f.eks. en sårbarhedsscanner. Endelig lærer de at lave og teste beredskabsplaner for deres egen forretning og deres relationer med kunder og leverandører.

Læs mere om projektet her

2.2 Forsyningskæder og risikostyring

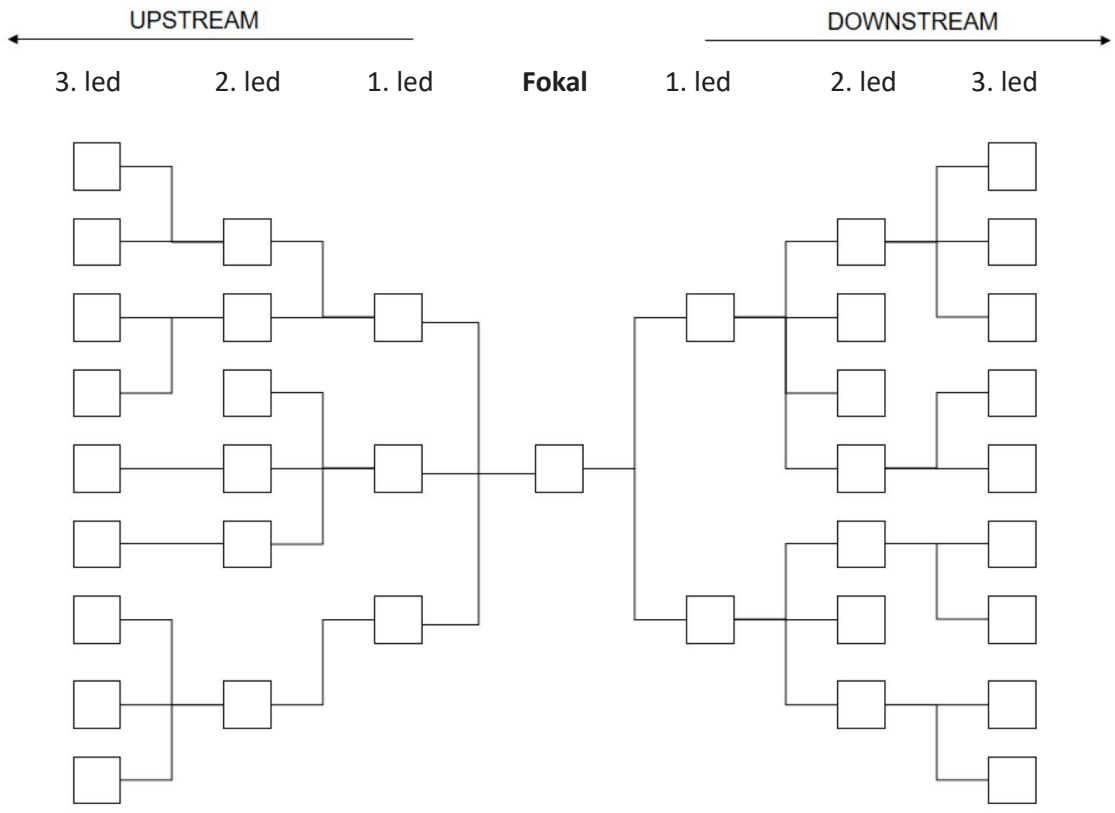
Forsyningskæden i en produktionsvirksomhed omfatter alle de aktiviteter, aktører og strømme, der er nødvendige for at bringe et produkt fra råvare til slutkunde. Den består typisk af leverandører af råvarer og komponenter, transport- og logistikaktører, virksomhedens egne produktions- og lagerfunktioner samt distributionskanaler og kunder. I en dansk produktionsvirksomhed – særligt en SMV – vil forsyningskæden ofte være international på indkøbssiden og mere regional eller europæisk på kundesiden, afhængigt af branche og specialisering.

En klassisk forståelse af supply chain management beskriver styringen af materialer, information og finansielle strømme på tværs af organisationer med henblik på at skabe værdi for slutkunden (Stentoft, Mikkelsen & Rajkumar, 2018). Formålet er at sikre høj leveringssikkerhed, konkurrencedygtige omkostninger, passende lagerniveauer og fleksibilitet. For produktionsvirksomheder betyder det konkret koordinering mellem indkøb, produktion, lager og distribution.

Strukturen i forsyningskæden varierer. Nogle produktionsvirksomheder opererer i simple kæder med få, stabile leverandører og standardiserede produkter. Andre indgår i komplekse, globale netværk med mange underleverandører og kundespecifik produktion. Særligt underleverandører til større industrikoncerner oplever høje krav til kvalitet, sporbarhed og leveringstid. Her er integration via ERP-systemer og digitale planlægningsværktøjer ofte central.

Virksomheder indgår i forsyningsnetværk som illustreret i figur 2.1, hvor den enkelte SMV i fokus kaldes for den fokale virksomhed. Cybersikkerhed i forsyningskæderne har således fokus på, hvordan virksomhederne kan forbedre deres cybersikkerhed i de forskellige led af leverandører frem mod virksomheden (upstream) og fra virksomheden mod forskellige led af kunder (*downstream*).

Figur 2.1 Forsyningskædernes netværksstruktur



Kilde: Stentoft, Mikkelsen & Rajkumar (2018, p. 39)

Forsyningskæder er imidlertid sårbare over for forstyrrelser. Globalisering, just-in-time-principper og lave lagre har øget effektiviteten, men samtidig reduceret robustheden. COVID-19-pandemien, geopolitiske spændinger og energikriser har tydeliggjort, hvor hurtigt forstyrrelser kan sprede sig gennem værdikæder (Stentoft, Mikkelsen & Wickstrøm, 2025b). Her kommer supply chain risk management ind i billedet. Ifølge ISO 31000: 2018 defineres risikostyring til sæt af koordinerede aktiviteter, der anvendes til at lede og styre en organisation med hensyn til risiko, hvor risiko forstås som effekten af usikkerhed på mål (Woods, 2022, p. 26). Overført til forsyningskæder handler det om at identificere potentielle hændelser, der kan forstyrre materiale- og informationsflow eller relationer i kæden.

Risici i forsyningskæder kan opdeles i flere kategorier (Christopher & Peck, 2004). Forsyningsrisici omfatter leverandørsvigt, kvalitetsproblemer og kapacitetsmangel. Det kan også være afhængighed af bestemte leverandører, som man er låste til, fordi der ikke er andre at skifte til (Narasimhan et al., 2009). Efterspørgselsrisici relaterer sig til udsving i kundebehov eller prognosefejl. Operationelle risici kan være maskinnedbrud eller IT-nedbrud, mens eksterne risici omfatter naturkatastrofer, politisk ustabilitet eller handelsbarrierer. For danske produktions-SMV'er er også cyberrisici og afhængighed af enkelte leverandører centrale problemstillinger.

Supply chain risk management følger typisk en proces med fire hovedtrin: (1) kortlægning af forsyningskæden og kritiske afhængigheder, (2) identifikation og vurdering af risici ud fra sandsynlighed og konsekvens, (3) udvikling af afbødende tiltag (mitigering) og (4) løbende monitorering og opdatering (Fan & Stevenson, 2018). Tiltag kan omfatte dual sourcing, strategiske lagerbuffere, tættere leverandørsamarbejde, kontraktuelle sikringer eller øget transparens via digitale systemer (Stentoft & Mikkelsen, 2024).

I en produktionsvirksomhed er balancen mellem effektivitet og robusthed central. For store lagre og redundans øger omkostningerne, mens for slanke systemer øger sårbarheden. Strategisk risikostyring handler derfor om at finde et niveau af robusthed, der matcher virksomhedens risikoprofil og kundekrav. Samlet set er forsyningskæden rygraden i en produktions-SMV's værdiskabelse, og supply chain risk management er et centralt ledelsesværktøj til at sikre stabil drift, konkurrenceevne og langsigtet bæredygtighed i en stadig mere usikker og kompleks global økonomi.

Et søsterprojekt i cyberporteføljen: Cybersikre Fødevareværdikæder

Projektet Cybersikre Fødevareværdikæder, der ledes af **Food & Bio Cluster Denmark**, tager afsæt i en erkendelse, som i stigende grad præger fødevare- og bioressourcebranchen: Cybersikkerhed er ikke længere et isoleret IT-anliggende - det er en forretningskritisk disciplin, der rækker på tværs af hele værdikæden. Når råvarer, produktion, logistik og distribution er digitalt forbundet, kan sårbarheder ét sted få konsekvenser langt ud over den enkelte virksomhed. Projektet arbejder derfor målrettet med at styrke cybersikkerheden gennem samarbejde på tværs af aktører i værdikæden, så virksomheder ikke blot beskytter sig selv, men også hinanden.

En central udfordring, som projektet adresserer, er, at mange virksomheder oplever cybersikkerhed som komplekst og svært at omsætte til konkrete handlinger. Her introducerer projektet en mere praksisnær tilgang: Risikovurderinger skal være konkrete, handlingsorienterede og lette at forstå – også for ledelsen. I stedet for lange, tekniske rapporter handler det om at skabe et klart overblik over de mest kritiske systemer og de væsentligste trusler, der kan påvirke dem. Når dette overblik kobles med virksomhedens aktuelle sikkerhedsniveau, opstår der et reelt beslutningsgrundlag.

I projektet er der udviklet et Risk Assessment Tool, der understøtter en struktureret og operationel tilgang til risikostyring – med særlig fokus på OT (Operational Technology). Det guider virksomhederne gennem en systematisk vurdering af trusler, sårbarheder og konsekvenser – og omsætter det til et overskueligt billede af, hvor risikoen er størst, og hvor indsatsen bør prioriteres.

Samlet set bidrager Cybersikre Fødevareværdikæder til et nødvendigt skifte: Fra komplekse, tekniske øvelser til enkel, handlingsorienteret risikostyring, der skaber reel værdi – både for den enkelte virksomhed og for værdikæden som helhed.

Læs mere om projektet her

2.3 Geopolitik

Projektets teoretiske ramme for geopolitik tager afsæt i en fundamental transformation af den globale orden. Vi bevæger os væk fra en post-koldkrigsæra domineret af liberal kapitalisme og markedsintegration, hvor økonomisk aktivitet og sikkerhedspolitik i høj grad var afkoblet. I denne tidligere liberale orden kunne virksomheder operere ud fra en *markedslogik*, hvor profitmaksimering og effektivitet var de primære styringsparametre, og hvor stater primært agerede som neutrale regulatorer, der håndhævede regler for fri konkurrence. Den underliggende præmis var gensidig afhængighed – tanken om, at øget økonomisk integration og velstand i sig selv ville reducere risikoen for konflikter mellem stater.

I dag er denne adskillelse mellem økonomi og sikkerhed brudt sammen i takt med en fornyet stormagtsrivalisering og overgangen til et post-amerikansk hegemonisk system – et system hvor USA mister relativ magt og indflydelse. Den nye geopolitiske virkelighed er kendetegnet ved, at stater systematisk genkobler velstand og sikkerhed. Denne fremvoksende geoøkonomiske orden bygger på en *geopolitisk logik*, hvor relationer ofte antager en nulsums-karakter, og hvor modparters økonomiske gevinster opfattes som potentielle sikkerhedstrusler.

2.3.1 Våbenbaseret indbyrdes afhængighed (weaponized interdependence)

Et vigtigt teoretisk begreb for at forstå denne udvikling er weaponized interdependence (Farrell & Newman, 2019). Konceptet beskriver, hvordan asymmetriske globale økonomiske netværk – såsom forsyningskæder, teknologiske infrastrukturer og finansielle systemer – i stigende grad udnyttes strategisk af stater til at opnå politisk indflydelse, overvåge eller udøve tvang over for andre aktører. Dette manifesterer sig særligt gennem to teoretiske mekanismer:

Panoptikon-effekten: Stater overvåger informations- og kapitalstrømme gennem de centrale netværksknudepunkter, de kontrollerer rent fysisk eller juridisk.

Chokepoint-effekten: Stater begrænser eller blokerer tredjeparters adgang til kritiske netværk for at udøve massivt politisk eller økonomisk pres, da disse netværk er yderst vanskelige at omgå.

2.3.2 Økonomisk sikkerhed og statecraft

Som en direkte konsekvens af denne netværksudnyttelse opererer vi nu i en æra defineret af økonomisk sikkerhed (*economic statecraft*), hvor stater proaktivt og kontinuerligt anvender økonomiske instrumenter til at beskytte nationale interesser. Hvor virksomheder tidligere udelukkende navigerede efter markedsøkonomiske incitamenter, må de i dag forholde sig til statslig indgriben gennem en række specifikke værktøjer:

Handelspolitik og sanktioner: Brug af importforbud, eksportkontrol og finansielle sanktioner til at afskære modstandere, signalere politiske grænser og svække rivaler økonomisk.

Investeringspolitik: Øget statslig kontrol og screening af udenlandske direkte investeringer samt strategiske opkøb af aktiver gennem statslige investeringsfonde for at opnå politisk indflydelse

Monetær politik og direkte støtte: Finansiel manipulation og statsstøtte designet til at forvride markeder, skabe afhængighedsforhold og fremme national industri på bekostning af globale konkurrenter.

Kontrol over ressourcer og juridiske instrumenter: Strategisk tilbageholdelse af energi eller kritiske råstoffer samt den voksende ekstraterritoriale anvendelse af national lovgivning.

2.3.3 Sammenstødet mellem to logikker

For produktions-SMV'er skaber denne konflikt mellem den traditionelle markedslogik og den nye geopolitiske logik et fundamentalt strategisk dilemma. Markedsorienterede kapabiliteter, der tidligere skabte global effektivitet - så-

Podcast: Geopolitiske spændinger og cybersikkerhed (uddrag)

Ny geopolitisk virkelighed

"Globaliseringen, som vi har kendt til den, er nu under pres. For det første har USA de sidste 30 år været den eneste dominerende magt, som også har indsat militær for at sikre den globale handel. For det andet var globaliseringen afhængig af, at næsten alle var enige om en neoliberal globalisering og at fremme demokrati. Disse to elementer gjorde globaliseringen mulig, men de er nu på retur", siger Olivier Schmitt. "USA er ikke mere den eneste supermagt, og der findes nu også konkurrerende modeller for økonomisk udvikling, som går imod den frie handel og det frie flow af varer og serviceydelser, som vi har haft de sidste 30 år", supplerer Vincent Keating.

Påvirkninger i forsyningskæderne

Danske virksomheder er ofte afhængige af eksport og globale forsyningskæder. Råvarer og halvfabrikata indkøbes i forsyningskæderne, som forarbejdes på op til flere geografiske lokationer og afsættes på indenlandske markeder såvel som på eksportmarkederne. Nye geopolitiske spændinger vil i stigende grad påvirke forsyningskæderne. "Man kan sige, at der kan opstå tre typer af 'chok'. Der kan komme forsyningschok, hvor virksomheder kan få udfordringer med at skaffe råvarer og halvfabrikata. Der kan komme efterspørgselschok, hvor markeder kan lukkes. Og der kan komme *connecticity* chok, som handler om det, der forbinder virksomhederne i form af produktion og transport", fortæller Olivier Schmitt.

Nye risici

Der er behov for nye tilgange til at håndtere nye risici, som vil opstå i takt med stigende geopolitiske spændinger. Der kan ske ændringer i den måde, forsyningskæder udvikles og struktureres på – f.eks. et større fokus på regionalisering i stedet for globalisering. "Det kan være mere omkostningstungt med regionalisering, men en sådan beslutning kan bidrage til at mitigere risici, hvor alternativet kan være at miste en nøgleleverandør. I den nye kommende æra er der behov for at tænke på efterspørgsel, forsyning og connectivity på helt nye måder, og hvordan de vil blive påvirket af geopolitiske hændelser", siger Vincent Keating.

Kilde: Schmitt et al. (2024) Hør podcasten her

som lean-principper, just-in-time leverancer og outsourcing til lavtlønslande - udgør nu kritiske sårbarheder i et system præget af weaponized interdependence. Dette nødvendiggør en radikal rekonfigurering af virksomhedernes dynamiske kapabiliteter og tilgang til risikostyring, hvor geopolitik indlejres som en endogen, uundgåelig faktor frem for noget udefrakommende og ekstraordinært.

Kronik: Hvordan sikrer vi, at cybersikkerhed bliver taget alvorligt? (sammendrag)

Manglende vedligeholdelse af cybersikkerhed i både private og offentlige organisationer er en voksende udfordring i takt med samfundets stigende digitalisering. Center for Cybersikkerhed vurderer i dag trusselsniveauet mod Danmark som meget højt. Baggrunden er bl.a. øgede geopolitiske spændinger og risikoen for, at statslige aktører udnytter cybersårbarheder til at påvirke danske virksomheder og institutioner. Angrebene bliver stadig mere målrettede og omfatter bl.a. ransomware og datatyveri rettet mod kritisk infrastruktur som energi, sundhed og transport. Samtidig er organisationer sårbare over for såkaldte supply chain-angreb, hvor angreb sker indirekte gennem leverandører og samarbejdspartnere.

Et vigtigt skridt i håndteringen af truslen er EU's NIS 2-direktiv. Direktivet udvider kravene til cybersikkerhed i flere sektorer og stiller strengere krav til risikostyring, hændelsesrapportering og samarbejde mellem EU-landene. Formålet er at styrke robustheden i kritiske samfundssektorer. Men selv om regulering spiller en central rolle, rejser det også spørgsmålet om, hvorvidt cybersikkerhed bør være et lovkrav for langt flere virksomheder. Et alvorligt cyberangreb kan lamme en virksomhed i uger eller måneder og i værste fald true dens eksistens.

Derfor kan etableringen af en Styrelse for Cybersikkerhed være et vigtigt næste skridt. En sådan styrelse kunne samle kompetencer inden for forebyggelse, regulering og respons på cybertrusler. Den kunne udvikle sikkerhedsstandarder, styrke uddannelse og rådgivning samt sikre hurtigere reaktioner på cyberhændelser. Samtidig kunne styrelsen fungere som et nationalt videnscenter og støtte især SMV'er, som ofte mangler ressourcer og ekspertise til at håndtere cyberrisici.

En central myndighed vil også kunne bidrage til at styrke tilliden til digitale systemer i samfundet. I et digitaliseret samfund er tillid til datasikkerhed afgørende. Investering i cybersikkerhed er derfor ikke blot en teknisk opgave, men en strategisk investering i Danmarks økonomiske stabilitet og samfundets modstandsdygtighed over for fremtidige cybertrusler.

Kilde: Stentoft, Keating, Peressotti & Mayer (2025) Læs kronikken her

2.4 Cybersikkerhed

Cybersikkerhed refererer til ”forebyggelse af skade på, beskyttelse af og genopretning af computere, elektroniske kommunikationssystemer, elektroniske kommunikationstjenester, trådbåren kommunikation og elektronisk kommunikation, herunder information indeholdt heri, for at sikre deres tilgængelighed, integritet, autentifikation, fortrolighed og uafviselighed” (NIST, 2026). Begrebet dækker både tekniske løsninger (f.eks. firewalls og kryptering) og organisatoriske tiltag såsom politikker, træning og risikostyring. I takt med den stigende digitalisering af samfundet er cybersikkerhed blevet en central del af virksomheders drift, da kritiske forretningsprocesser i stigende grad er afhængige af IT-systemer. Typer af cyberangreb kan være:

- Ransomware (online afpresning)
- Phishing (forsøg på at opnå adgang til adgangskoder og kortoplysninger)
- CEO-fraud (direktørsvindel, hvor man udgiver sig for at være chefen for at få overført penge eller følsomme data)
- Fakturabedrageri (betaling af en falsk eller ændret faktura)
- DDoS-angreb (overbelastning af hjemmesider eller tjenester)
- Bevidste insider (f.eks. en medarbejder, som med vilje misbruger sin adgang til systemer og data)
- Supply chain angreb (angreb via samarbejdspartnere eller leverandører)

Trusselsniveauet i Danmark vurderes som meget højt for cyberkriminalitet og cyberspionage (Styrelsen for Samfundssikkerhed, 2025, p. 6), og det anses som sandsynligt, at både virksomheder og myndigheder vil blive ramt af cyberkriminalitet. Derudover viser en undersøgelse af digital sikkerhed, at 52% af virksomhederne har været udsat for en IT-sikkerhedshændelse (Styrelsen for Samfundssikkerhed, 2024, p. 35).

SMV'er kan sikre sig mod cyberangreb ved at kombinere tekniske løsninger, klare procedurer og fokus på medarbejderadfærd. Først og fremmest er det afgørende at have en solid grundlæggende IT-sikkerhed, herunder løbende opdatering af software, brug af antivirus og firewall samt implementering af multifaktorgodkendelse, da mange angreb udnytter kendte sårbarheder. Derudover bør virksomheder arbejde systematisk med adgangsstyring gennem stærke og unikke adgangskoder samt begrænsning af brugerrettigheder for at reducere risikoen for uautoriseret adgang. Medarbejdertræning spiller også en central rolle, da mange angreb starter med phishing, hvorfor det er vigtigt at opbygge awareness og evnen til at genkende mistænkelige henvendelser (Mayer et al., 2023). Samtidig bør SMV'er etablere regelmæssige backups og en beredskabsplan, så de hurtigt kan gendanne data og drift i tilfælde af et angreb, særligt ved ransomware. Endelig kan man arbejde risikobaseret ved at identificere kritiske systemer og overvåge for unormal aktivitet samt stille krav til leverandørers sikkerhed, da mange angreb sker via forsyningskæder (Melnyk et al., 2022).

> **"Projektet har hjulpet os med at vurdere vores eget modenhedsniveau inden for både cybersikkerhed og risikostyring. Det har været en god øjenåbner."**
>
> *CEO Jes Gravesen, Engskov Maskinfabrik A/S*

2.5 Forretningskontinuitet

Forretningskontinuitet i danske produktions-SMV'er handler om virksomhedens evne til at opretholde eller hurtigt genoptage kritiske aktiviteter ved uforudsete hændelser som leverandørsvigt, cyberangreb, brand, pandemier, energikriser eller pludseligt bortfald af nøglemedarbejdere. For produktionsvirksomheder er kontinuitet særligt centralt, fordi værdiskabelsen er bundet op på fysiske faciliteter, maskiner, lagerbeholdninger og stabile leverancer i værdikæden. SMV'ers størrelse og organisering påvirker direkte, hvordan de arbejder med forretningskontinuitet. Ifølge Hiles (2014, p. 2), kan opnås følgende fordele ved integrere praksis med forretningskontinuitet:

- En mere robust driftsmæssig infrastruktur
- Overholdelse af lovgivningsmæssige, regulatoriske og kvalitetsmæssige krav til risikovurdering og risikostyring
- Evnen til fortsat at opfylde virksomhedens mission i tilfælde af en katastrofe
- Evnen til at fortsætte forretningen profitabelt i tilfælde af en katastrofe
- Evnen til at fastholde markedsandele i tilfælde af en katastrofe
- Forbedret medarbejdermoral, fordi man som medarbejder ved, at ledelsen beskytter jobbene.
- Beskyttelse af virksomhedens omdømme, image og brandværdi

Et centralt kendetegn ved produktions-SMV'er er afhængighed af få nøglepersoner og specialiserede kompetencer. Ofte besidder enkelte medarbejdere unik viden (og tavs viden) om maskinopsætning, kundespecifikationer eller produktionsflow. Hvis disse personer pludselig er fraværende, kan det lamme produktionen. Forretningskontinuitet kræver derfor systematisk videndeling, dokumentation af processer og eventuelt krydstræning, så flere medarbejdere kan varetage kritiske funktioner.

Leverandørafhængighed er en anden væsentlig risikofaktor. Mange produktions-SMV'er indgår som underleverandører i større værdikæder og er samtidig afhængige af specifikke råvarer eller komponenter. Globale forstyrrelser, som set under COVID-19 og energikrisen, kan skabe leveranceproblemer og prisudsving. Kontinuitetsarbejde indebærer derfor risikovurdering af forsyningskæden, alternative leverandører, lagerstrategier og kontraktuelle sikkerheder.

Digitalisering har øget effektiviteten i mange produktions-SMV'er, men også skabt nye sårbarheder. Produktionsstyring, ERP-systemer og automatiserede anlæg (styret af operationel teknologi - OT) er ofte forbundet til netværk. Cyberangreb kan derfor standse produktionen eller kompromittere data. Styrelsen for Samfundssikkerhed (2024) fremhæver, at også mindre virksomheder er mål for cyberkriminalitet. Forretningskontinuitet omfatter derfor backup-løsninger, adgangsstyring, beredskabsplaner og træning i cybersikkerhed.

Fysiske risici spiller også en central rolle. Brand, maskinnedbrud eller strømsvigt kan have umiddelbare og kostbare konsekvenser. For produktions-SMV'er betyder selv kortvarige afbrydelser ofte tab af omsætning og risici for bod over for kunder. En kontinuitetsplan bør derfor identificere kritiske aktiver, fastlægge genopretningstider og beskrive procedurer for midlertidig produktion, outsourcing eller samarbejde med partnere.

Ressourceknaphed er en udfordring for mange SMV'er. De har sjældent dedikerede risikochefer eller compliance-funktioner. Kontinuitetsarbejdet er derfor ofte uformelt og personafhængigt. Internationalt findes standarder som ISO 22301 for ledelsessystemer for forretningskontinuitet (Crask, 2024), men implementering kan opleves som ressourcekrævende. For danske produktions-SMV'er kan en pragmatisk tilgang være hensigtsmæssig: En enkel, skriftlig beredskabsplan, regelmæssig risikovurdering og test af nøgleprocedurer. Forretningskontinuitet bør ses som en integreret del af virksomhedens strategi

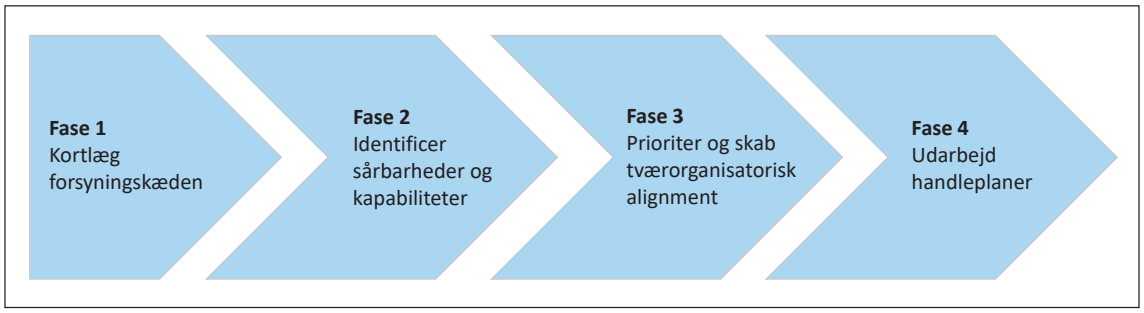
og ikke blot som et forsikringsmæssigt anliggende. En robust kontinuitetsindsats kan styrke kundetillid, konkurrenceevne og samarbejde i værdikæden. Flere større kunder stiller i dag krav om dokumenteret risikostyring hos deres leverandører, hvilket gør kontinuitetsarbejde til en kommerciel nødvendighed.

Sammenfattende er forretningskontinuitet i danske produktions-SMV'er tæt knyttet til håndtering af personafhængighed, leverandørrisici, digital sårbarhed og fysiske driftsforstyrrelser. Selvom ressourcerne ofte er begrænsede, kan en struktureret og systematisk tilgang reducere sårbarhed markant og bidrage til langsigtet stabilitet og bæredygtig vækst.

2.6 Supply chain resilience procesmodel

Supply chain resilience (SCRES) handler om en virksomheds evne til at forblive operationel, tilpasse sig og komme sig efter forstyrrelser i forsyningskæden. I stedet for blot at beskrive strategier eller teoretiske koncepter, foreslår Stentoft, Mikkelsen & Kjær (2023) og Stentoft & Mikkelsen (2024) et struktureret procesforløb — altså en model, der viser, hvordan virksomheder systematisk kan opbygge en resilient adfærd (se figur 2.2).

Figur 2.2 Supply chain resilience procesmodel



Kilde: Stentoft, Mikkelsen & Kjær (2023, p. 51)

SCRES procesmodellen består af fire hovedfaser, som bygger på empirisk forskning blandt 18 danske produktions-SMV'er: 1) kortlægning af forsyningskæden, 2) individuel identifikation af sårbarheder og kapabiliteter, 3) prioritering og tværorganisatorisk alignment og 4) udvikling af handleplaner. Processen begynder med kortlægning af forsyningskæden, hvor repræsentanter fra centrale funktioner i fællesskab udvikler et overblik over kunder, leverandører, flows og operationelle afhængigheder for at skabe en fælles forståelse af udfordringerne. Den anden fase fokuserer på at identificere sårbarheder og kapabiliteter, hvor deltagerne individuelt vurderer risici og nødvendige organisatoriske styrker understøttet af et struktureret, digitalt værktøj. I tredje fase

arbejdes der på tværs af funktioner i organisationen med at samle de individuelle vurderinger til en fælles prioritering og rangordning af de mest kritiske sårbarheder og tilhørende kapabiliteter. Endelig går modellen over i udviklingen af handlingsplaner, hvor prioriteringer omsættes til konkrete og tidsafgrænsede initiativer, der fordeler ansvar og understøtter implementeringen således, at forbedringer i resiliens integreres i organisationens løbende praksis.

> **"En stor styrke har været, at flere funktioner i virksomheden har været involveret. Det har givet en bredere forankring og større ejerskab til resultaterne."**
>
> *COO Søren Lind Therkildsen, GomSpace A/S*

2.6.1 Kortlægning af forsyningskæden

Formål
At skabe et samlet overblik over virksomhedens forsyningskæde og dens kritiske afhængigheder.

Indhold i fasen
- Identifikation af nøglekunder
- Identifikation af nøgleleverandører (direkte og evt. indirekte)
- Kortlægning af materialestrømme, informationsstrømme og finansielle strømme
- Identifikation af kritiske produkter, komponenter og flaskehalse
- Synliggørelse af geografiske og strukturelle koncentrationer

Praktisk pointe
Resiliens kan ikke styrkes uden transparens. Mange SMV'er har begrænset overblik over deres upstream-led (leverandørers leverandører), hvilket skaber skjulte sårbarheder.

Output
Et visuelt kort over forsyningskæden samt en liste over kritiske knudepunkter og afhængigheder.

2.6.2 Individuel identifikation af sårbarheder og kapabiliteter

Formål
At identificere, hvor forsyningskæden er sårbar – og hvilke interne styrker der kan kompensere.

Sårbarheder kan f.eks. være:

- Single sourcing
- Geografisk koncentration
- Lange lead-times
- Lav lagerbuffer
- Begrænset informationsdeling

Kapabiliteter kan f.eks. være:

- Fleksibel produktion
- Tæt leverandørsamarbejde
- Høj intern koordinering
- Digital transparens
- Hurtig beslutningstagning

Praktisk pointe

Modellen kobler risiko (sårbarhed) og kapabilitet (evne). Resiliens forstås ikke kun som risikoreduktion, men også som evnen til at absorbere, tilpasse og komme styrket ud af forstyrrelser.

Output

En systematisk vurdering (ofte workshop-baseret) af, hvor virksomheden er mest eksponeret – og hvor den har styrker.

2.6.3 Prioritering og tværorganisatorisk alignment

Formål
At skabe fælles forståelse og prioritering på tværs af funktioner (indkøb, produktion, salg, logistik, ledelse).

Hvorfor er denne fase central?
I mange SMV'er ligger viden om risici spredt i organisationen. Resiliens kræver:
- Fælles risikoforståelse
- Fælles prioritering af indsatsområder
- Ledelsesmæssig forankring

Typiske aktiviteter
- Tværfunktionelle workshops
- Diskussion af trade-offs (f.eks. lager vs. kapitalbinding)
- Fastlæggelse af, hvilke sårbarheder der er mest kritiske
- Beslutning om ambitionsniveau

Praktisk pointe
Resiliens er en organisatorisk proces og ikke blot et teknisk supply chain værktøj. Alignment reducerer silotænkning.

Output
En prioriteret liste over indsatsområder med ledelsesmæssig opbakning.

2.6.4 Udvikling af handleplaner

Formål
At omsætte analysen til konkrete tiltag.

Eksempler på handlinger:
- Dual sourcing
- Opbygning af sikkerhedslager
- Udvikling af alternative leverandører
- Investering i digital sporbarhed
- Formalisering af beredskabsplaner
- Styrket samarbejde med nøgleleverandører

Centralt i modellen
- Handlingsplanerne skal være realistiske for SMV'er
- Tiltag prioriteres efter effekt og praktisk gennemførlighed
- Processen er iterativ (resiliens er ikke en engangsøvelse)

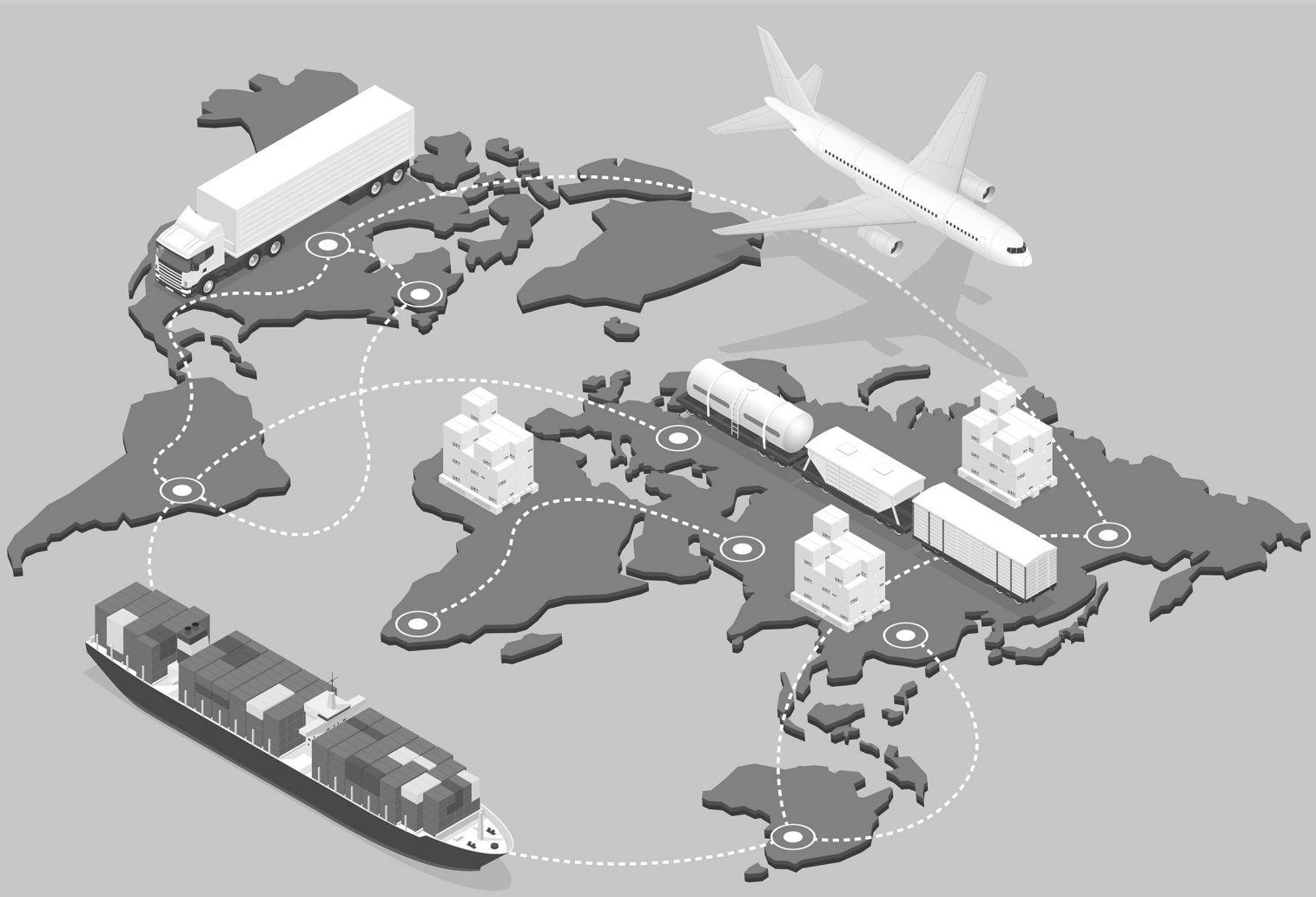
Output
Konkrete, tidsfastsatte initiativer med ansvar og opfølgning.

For at operationalisere modellen har vi udviklet en dedikeret webapplikation, der guider organisationer gennem hver fase af processen. Platformen muliggør koordinering af de deltagende teammedlemmer og understøtter en selvstændig gennemførelse af fase 2, så enkeltpersoner kan vurdere sårbarheder og kapabiliteter på et tidspunkt, der passer dem. Systemet genererer automatisk funktionsspecifikke rapporter og samler dem i et integreret miljø til datavisualisering og analyse i fase 3. I dette arbejdsrum kan deltagerne undersøge perspektiver på tværs af funktioner, identificere overlappende sårbarheder, sammenligne opfattede risici og afbødende kapabiliteter samt analysere forskellige prioriteringer på en struktureret måde. Efter alignment-workshoppen producerer systemet en omfattende, interaktiv rapport med mulighed for tilpassede visninger og skræddersyede outputs, som giver et praktisk grundlag for handlingsplanlægningen i fase 4. Applikationen er frit tilgængelig via projektets hjemmeside (**https://process-model.cyber-smv.dk/**), hvor der også findes materialer og dokumentation for virksomheder, der ønsker selv at hoste løsningen.

Parallelt har projektet udviklet et opdateret sæt af sårbarheder og kapabiliteter med særligt fokus på cybersikkerhed og forsyningskæders resiliens. Disse er baseret på gældende best practice og udledt af interviews med danske beslutningstagere, brancheorganisationer og virksomheder i kritiske sektorer, herunder forsvar, IT og telekommunikation. Formålet er at sikre, at modellen afspejler nye trusselslandskaber og regulatoriske forventninger, samtidig med at den forbliver praktisk anvendelig for virksomheder, der opererer i strategisk følsomme industrier.

2.7 Cybersikker supply chain risk management

NIST CSF 2.0 er et internationalt anerkendt rammeværk for cybersikkerhed udgivet af det amerikanske National Institute of Standards and Technology (NIST) i 2024. NIST CSF 2.0 er en praktisk vejledning til, hvordan organisationer kan styre og forbedre deres cybersikkerhed. Det er ikke en lov og ikke en certificering. Cybersikker supply chain risk management (C-SCRM) i NIST CSF 2.0 er en systematisk proces til at identificere, vurdere, håndtere og forbedre cybersikkerhedsrisici, som opstår gennem leverandører af teknologi, software, tjenester og komponenter. Det omfatter såvel fysiske produkter som digitale produkter og tjenester i supply chain-økosystemet. C-SCRM er ikke længere blot et supplement til cybersikkerhed, men integreres som en kategori under den nye Govern (GV)-funktion. Det betyder, at supply chain-risici nu betragtes som en kernekomponent i strategisk cybersecurity governance, ikke kun noget der håndteres ad hoc i IT-afdelingen.



NIST CSF 2.0 har samlet C-SCRM-praksisserne under Govern-funktionen som 10 specifikke subkategorier (de præcise praksisser/krav), som virksomheder bør implementere for at styre cybersikkerhedsrisici i deres forsyningskæder (NIST, 2024):

GV. Supply Chain-01: Etabler C-SCRM-program og governance
- Etabler et program, strategi, mål, politikker og processer for cybersikkerheds supply chain-risikostyring, som er aftalt med relevante organisatoriske interessenter.

GV. Supply Chain-02: Roller og ansvar
- Definer og kommuniker cybersikkerhedsroller og -ansvar for leverandører, kunder og partnere både internt og eksternt.

GV. Supply Chain-03: Integration i risiko- og forbedringsprocesser
- Integrer C-SCRM i både cybersikkerhedsrisikostyring, enterprise risk management, risikovurderinger og løbende forbedringsprocesser.

GV. Supply Chain-04: Kendskab til og prioritering af leverandører
- Kend og prioriter leverandører efter deres kritikalitet for virksomhedens mission og drift.

GV. Supply Chain-05: Sikkerhedskrav i kontrakter og aftaler
- Etabler, prioriter og integrer krav til cybersikkerhedsrisici i kontrakter og aftaler med leverandører og relevante tredjeparter.

GV. Supply Chain-06: Planlægning og due diligence før engagement
- Udfør planlægning og due diligence for at reducere risici, før formalisering af leverandør- eller samarbejdsrelationer.

GV. Supply Chain-07: Risikoanalyse og overvågning gennem leverandørrelationens levetid
- Forstå, registrer, prioriter, vurder, responder og overvåg de risici, en leverandør og dens produkter/tjenester udgør gennem hele samarbejdsperioden.

GV. Supply Chain-08: Hændelsesplanlægning, udrykning og genopretning med leverandører
- Inkluder relevante leverandører og tredjeparter i planlægning, respons og genopretningsaktiviteter omkring cybersikkerhedshændelser.

GV. Supply Chain-09: Overvågning gennem livscyklussen
- Integrer supply chain sikkerhedspraksis i cybersikkerheds- og enterprise risk management-programmer og monitorér deres performance gennem et produkt-/service-livscyklusperspektiv.

GV. Supply Chain-10: Efter afslutning af partnerskab eller serviceaftale
- C-SCRM-planer skal indeholde bestemmelser for aktiviteter efter en partnerskabsaftale eller serviceaftale er afsluttet.

På **https://www.cyber-smv.dk** under værktøjer, er ovenstående 10 praksisser operationaliseret i konkrete værktøjer.

2.8 Dynamiske kapabiliteter

Dynamiske kapabiliteter er et centralt begreb i strategisk ledelsesteori, som for alvor blev formuleret af Teece, Pisano & Shuen (1997). De definerer dynamiske kapabiliteter som virksomhedens evne til at integrere, opbygge og rekonfigurere interne og eksterne kompetencer for at imødekomme hurtigt forandrende omgivelser. Begrebet videreudvikles senere af Teece (2007), hvor han konkretiserer dynamiske kapabiliteter i tre overordnede processer: 1) sensing, 2) seizing og 3) transforming. I modsætning til den klassiske ressourcebaserede teori (RBV), der fokuserer på værdifulde, sjældne og svære at imitere ressourcer (Barney, 1991), retter dynamiske kapabiliteter fokus mod forandringsdimensionen. Det handler ikke kun om, *hvad* virksomheden har, men også om *hvordan*, den løbende tilpasser og fornyer sine ressourcer.

Teece (2007) opdeler, som nævnt tidligere, dynamiske kapabiliteter i tre hovedprocesser: 1) sensing, 2) seizing og 3) transforming (se tabel 2.1).

Tabel 2.1 Sensing, seizing og transforming

Sensing	Evnen til at identificere og fortolke muligheder og trusler i omgivelserne. Det indebærer overvågning af teknologiske, markedsmæssige og institutionelle ændringer. For produktions-SMV'er kan det eksempelvis være ændringer i handelsregimer, nye sikkerhedsstandarder eller fremvækst af digitale trusler.
Seizing	Evnen til at mobilisere ressourcer og træffe strategiske beslutninger på baggrund af de identificerede muligheder og trusler. Det kan være investering i nye teknologier, ændring af leverandørstruktur eller udvikling af nye sikkerhedsprocedurer.
Transforming	Evnen til løbende at omstrukturere organisationens aktiver, processer og relationer, så virksomheden forbliver konkurrencedygtig. Det kan indebære organisatoriske ændringer, nye samarbejdsformer eller ændring af forretningsmodel.

Kilde: Teece (2007)

Dynamiske kapabiliteter kan ses som metakapabiliteter, der styrer virksomhedens evne til at forny sine operationelle kapabiliteter. Produktions-SMV'er opererer i stigende grad i et globalt og digitaliseret risikobillede. To udviklingsområder er særligt centrale: geopolitik og cybersikkerhed.

2.8.1 Geopolitisk usikkerhed

Geopolitiske spændinger, handelsrestriktioner, sanktioner og regionalisering af værdikæder påvirker direkte forsyningssikkerhed og adgang til markeder. Eksempler er handelskonflikter mellem stormagter, krigen i Ukraine og øget fokus på strategisk autonomi i EU. For produktions-SMV'er, som ofte er stærkt afhængige af få leverandører eller bestemte regioner, kan geopolitisk ustabilitet føre til:

- Leveranceafbrydelser
- Stigende inputpriser
- Regulering og eksportkontrol
- Krav om dokumentation og compliance

Her bliver sensing afgørende for SMV'erne. Der bør ske en systematisk overvågning af politiske og regulatoriske ændringer. Seizing handler om at reagere – f.eks. ved praksisser som dual sourcing, nearshoring eller lageropbygning. Transforming kan indebære strategisk omlægning af hele supply chain-strukturen. Uden dynamiske kapabiliteter risikerer SMV'er at reagere for sent eller fragmenteret.

2.8.2 Cybersikkerhed som strategisk risikofaktor

Digitalisering af produktion (Industry 4.0, IoT, ERP-integration, cloud-løsninger) øger effektiviteten – men også sårbarheden. Cyberangreb kan lamme produktion, kompromittere data og skade relationer i værdikæden. Center for Cybersikkerhed har foretaget en trusselsvurdering mod Danmark ud fra fem typer angreb, som individuelt er trusselsvurderet: 1) cyberkriminalitet (MEGET HØJ), 2) cyberspionage (MEGET HØJ), 3) cyberaktivisme (HØJ), 4) destruktive cyberangreb (MIDDEL) og 5) cyberterror (INGEN) (Styrelsen for Samfundssikkerhed, 2025, p. 6). For produktions-SMV'er er udfordringen ofte begrænsede ressourcer og manglende specialiseret sikkerhedskompetence. Her bliver dynamiske kapabiliteter centrale, fordi cybersikkerhed ikke blot er et teknisk spørgsmål, men et organisatorisk lærings- og omstillingsspørgsmål:

- **Sensing:** Overvågning af trusselsbilledet og regulatoriske krav (f.eks. NIS 2-direktivet i EU)
- **Seizing:** Investering i sikkerhedssystemer, træning og governance-strukturer
- **Transforming:** Integrering af cybersikkerhed i virksomhedens strategi og kultur

Cybersikkerhed bliver dermed en del af virksomhedens strategiske resiliens.

3.
Metode

Det samlede projekt er blevet gennemført ved brug af forskellige metoder, der kort beskrives i de tre nedenstående delafsnit.

3.1 Tre hierarkiske analyseniveauer

Projektets metodiske tilgang er struktureret omkring tre hierarkiske analyseniveauer – det politiske niveau, industriniveauet og virksomhedsniveauet – for at sikre en sammenhængende oversættelse af abstrakte geopolitiske trusler til konkrete handlinger i SMV'erne. Denne struktur muliggør en systematisk nedbrydning af komplekse makroforhold til operationel praksis.

3.1.1 Det politiske beslutningsniveau

Processen indledtes med workshops, der involverede eksperter fra det danske forsvars- og udenrigspolitiske miljø, herunder repræsentanter fra Forsvarsakademiet og Udenrigsministeriet. Formålet var at identificere og definere de mest presserende geopolitiske drivkræfter og kriser for perioden 2025 - 2030 ved hjælp af PESTEL-variabler (politiske, økonomiske, sociale, teknologiske og juridiske). Gennem en usikkerheds-/konsekvensmatrix udvalgte deltagerne de scenarier, der kombinerede høj alvorlighed med høj usikkerhed, hvilket dannede grundlaget for projektets fem hovedscenarier.

Processen blev gennemført i to separate iterationer med forskellige ekspertgrupper. Det er væsentligt at bemærke, at den anden gruppe – uden at være blevet introduceret til resultaterne fra den første workshop – uafhængigt genererede nøjagtig de samme scenarier. Dette bemærkelsesværdige sammenfald kan tilskrives en kombination af høj strukturel determinisme i det nuværende trusselsbillede og eksistensen af et epistemisk fællesskab blandt danske sikkerhedspolitiske aktører. At to uafhængige grupper identificerer identiske drivkræfter indikerer, at de geopolitiske makro-trends (såsom stormagtsrivalisering og klimaforandringer) i øjeblikket fremstår med så høj betydning, at de dominerer den strategiske horisont på tværs af observatører. Det bekræfter, at scenarierne ikke blot er arbitrære spekulationer, men repræsenterer en konsolideret forståelse af de strukturelle vilkår, dansk industri navigerer i.

3.1.2 Industriniveauet (kontekstualisering)

De identificerede geopolitiske temaer blev herefter kvalificeret gennem workshops med brancheorganisationer og industrielle aktører, såsom DI og SMVdanmark. På dette niveau var opgaven at oversætte de brede politiske scenarier til specifikke sektorsårbarheder. Deltagerne diskuterede, hvilke cybersikkerhedsmæssige og forsyningskædemæssige implikationer de enkelte scenarier ville have for dansk industri, og identificerede hvilke kapabiliteter der ville være nødvendige for at imødegå dem. Dette sikrede, at scenarierne ikke blot var storpolitiske fortællinger, men indeholdt relevante industrielle risikofaktorer. Der blev også leveret værdifulde input til de udviklede scenarier, der styrkede fokusset på cybersikkerhed.

3.1.3 Virksomhedsniveauet

Det tredje niveau involverede direkte interaktion med danske produktions-SMV'er gennem to forløb (det første forløb med virksomhedsdeltagele i fire workshops fandt sted i november 2024, og det andet forløb med fire workshops fandt sted fra december 2025 til marts 2026). De otte workshops blev afholdt for 3-5 virksomheder på forskellige konferencelokationer i Danmark (Aalborg, Hobro, Brande, Middelfart, Kgs. Lyngby og Hvidovre). Agenden på disse samlinger var:

- Diskussion om cybersikkerhed (virksomhedsspecifik i grupperum)
- Overblik over fremtidsscenarier (i plenum)
- Arbejde med et eller flere fremtidsscenarier (virksomhedsspecifik i grupperum)
- Opsamling på fremtidsscenarier og på diskussioner om cybersikkerhed (i plenum)

Virksomhederne valgte det scenarie, de fandt mest relevant for deres forretningsmodel, og arbejdede systematisk med at identificere specifikke risici og sårbarheder i deres egen forsyningskæde. Metoden flyttede fokus fra generel risikoanalyse til konkrete diskussioner om mitigering og behovet for nye dynamiske kapabiliteter i en usikker fremtid.

Efter afslutningen af de fire workshops i hvert forløb blev virksomhederne samlet på Syddansk Universitet i Odense til en dag med cybertræning. Følgende emner blev behandlet:

- Indlæg fra Hotel Koldingfjord om deres cyberangreb (kun ved det første forløb)
- Cybersikkerhed – best practices og Q&A
- Cloud – best practices og Q&A
- Geopolitik og Q&A
- Supply chain risk management/forsyningskæde-resiliens og QA
- Værktøjer – en guidet gennemgang
- Case/pentesting inkl. Q&A (kun ved det andet forløb)
- Paneldebat
- Opsummering

> **”Vi deltog for at få et ærligt blik på vores sårbarheder – ikke i IT-systemerne, men i forretningen og i vores egen adfærd. Den energiske facilitering fra projektet ved brug af egne erfaringer skabte et nærvær og en troværdighed, der udløste overraskende mange AHA-oplevelser. Det fik ledelsesgruppen til både at tænke og føle.”**
>
> *Head of Legal & Compliance Ole Anker Aagaard, ExamVision A/S*

3.2 Fokusgruppediskussioner

Fokusgruppediskussioner med interessenterne nævnt i sektion 3.1 blev lydoptaget, krypteret og transskriberet ved hjælp af Whisper (lokalt, uden AI). Manuel verifikation sikrede en korrekt transskription. Transskriptionerne blev importeret til MAXQDA, et kvalitativt analyseværktøj. Kodning af data foregik over flere cyklusser. Første kodningsrunde kombinerede in-vivo-kodning (deltagernes egne ord) og indledende kodning for at generere åbne koder på tværs af interessentniveauer. Anden kodningsrunde anvendte aksial kodning til at undersøge relationer mellem koderne. Fokuseret kodning fremhævede tilbagevendende mønstre i dataene, mens teoretisk kodning løftede disse til bredere, indbyrdes forbundne temaer. Kodningerne blev derefter reorganiseret i tematiske kategorier og samlet i overordnede temaer. To seniorforskere gennemgik løbende de fremvoksende temaer, og der blev ført en detaljeret audit trail. Den udviklede kodebog, som beskriver alle koder, definitioner og eksempelcitater, blev stillet til rådighed som supplerende materiale for at sikre gennemsigtighed og reproducerbarhed.

3.3 Spørgeskemaundersøgelser

I projektet er der gennemført to landsdækkende spørgeskemaundersøgelser med fokus på cybersikkerhed blandt danske produktions SMV'er (Stentoft et al., 2024 og 2026). Målgrupperne var danske produktionsvirksomheder med 20-250 ansatte inden for NACE-branchekoder 10-33. Virksomhederne blev identificeret via databasen Navne & Numre Erhverv, som omfatter alle momsregistrerede virksomheder i Danmark. 248 virksomheder deltog i undersøgelsen fra 2024 og 155 i undersøgelsen fra 2026.

4.
Resultater

4.1 Forskellige opfattelser af cybersikkerhed hos tre interessentgrupper

Projektets formål er at styrke cybersikkerheden i danske produktions-SMV'er. Det begyndte med et særligt fokus på SMV'er inden for forsvarsindustrien vel vidende, at projektets resultater skulle kunne bruges af alle industrier og virksomhedsstørrelser. I det følgende præsenteres resultaterne af en undersøgelse af interessenter i Danmarks forsyningskæde inden for forsvar. Studiet omfattede fokusgruppediskussioner med 45 deltagere fra tre interessentgrupper:

1) *Det politiske beslutningsniveau* (n=6) som er repræsentanter for national sikkerhed og Udenrigsministeriet. De bidrager med strategiske indsigter om national cybersikkerhed og internationalt samarbejde.
2) *Industriniveauet* (n=11) er brancheeksperter fra forsvarssektoren, som identificerer mønstre og validerer trusler.
3) *Virksomhedsniveauet* (n=28 fra 12 SMV'er) som er ledere, mellemledere og medarbejdere i SMV'er, som rapporterer om operationelle realiteter.

Analysen kortlagde mentale modeller på tværs af disse grupper, undersøgte opfattelser af cybersikkerhed og identificerede misforhold, som kan bidrage til sårbarheder. Disse misforhold har praktiske konsekvenser for omsætning af politik til konkret handling. For at strukturere resultaterne guider to temaer dette afsnit: (1) sårbarheder og kapabiliteter og (2) mentale modeller for cybersikkerhed på tværs af interessentniveauer. Praktiske implikationer diskuteres løbende.

4.1.1 Sårbarheder og kapabiliteter

Et sårbarheds–/kapabilitetsperspektiv baseret på teorien om forsyningskæderesiliens (Pettit, Fiksel, & Croxton, 2010; Pettit, Croxton & Fiksel, 2013), blev anvendt til at kortlægge resultaterne. De kan ses som supplement til de supply chain relaterede sårbarheder og kapabiliteter fra Stentoft, Mikkelsen & Kjær (2023). Sårbarhederne fremgår af tabel 4.1. Sårbarheder er strukturelle forhold, der gør organisationer modtagelige for forstyrrelser. Kapabiliteter er egenskaber, der hjælper organisationer med at forudse og håndtere disse forstyrrelser. Med udgangspunkt i Pettit, Fiksel, & Croxtons (2010) og Pettit, Croxton & Fiksels (2013) analyseramme med sårbarheder og kapabiliteter viser fokusgruppedataene en tydelig ubalance: 27 organisatoriske sårbarheder fordelt på fem kategorier, men kun 10 kapabiliteter fordelt på tre kategorier. Kløften er størst på SMV-niveau, hvor virksomheder har få formelle cybersikkerhedskapabiliteter. I stedet er de afhængige af handlekraft, backup-løsninger, outsourcet IT, cyberforsikring og uformel krisekommunikation.

Tabel 4.1 Cyberrelaterede sårbarheder

Menneskelige og kulturelle sårbarheder

- Usikker og upassende adfærd
- Manglende cybersikkerhedstræning
- Manglende prioritering
- Forældet ledelsesmæssig beslutningstagning
- Modvilje mod at dele sårbarheder med myndigheder

Driftsmæssige og regulatoriske sårbarheder

- Overvældende regulatoriske byrder
- Cybersikkerhed som en sekundær prioritet
- Utilstrækkelig beredskabsplanlægning
- Kommunikationshuller
- Begrænsede ressourcer/ressourceknaphed
- Manglende robusthed i kritisk digital infrastruktur
- Kompleksitet i internationale standarder
- Usikkerhed om eksportkontrol

Tekniske sårbarheder

- Overafhængighed af specifikke teknologier
- Forældede systemer (legacy-systemer)
- Risici ved disruptive teknologier
- Høj grad af digitalisering
- Hacking og ransomware
- Flere adgangspunkter

Sårbarheder i forsyningskæden

- Leverandørafhængighed (vendor lock-in)
- Sårbarheder hos tredjeparter
- Manglende gennemsigtighed i forsyningskæden
- Afhængighed af et begrænset antal IT-leverandører/virksomheder

Geopolitiske sårbarheder

- Danmarks geopolitiske positionering
- Sårbarhed i Grønland og Færøerne
- Risiko for udenlandsk indblanding
- Branchespecifikke trusler

Kilde: Kankam-Boateng et al. (2026)

Som det fremgår af tabel 4.1, er sårbarhederne inddelt i fem områder:

1. *Menneskelige og kulturelle sårbarheder* er den største kategori og går på tværs af alle tre interessentgrupper. Lav generel bevidsthed, kulturel over-tillid og omkostningsdrevne syn på cybersikkerhed blev identificeret på alle niveauer. Problemets karakter varierer dog mellem grupperne. Beslutningstagere og policy-aktører fremhæver systemiske udfordringer såsom mangel på kompetencer, aldrende ledelse og fragmenteret cybersikkerhedsuddannelse. SMV'er peger på lokale udfordringer: ujævn medarbejderbevidsthed, begrænset ledelsesengagement og ureguleret brug af mobile enheder. Danmarks højtillidskultur er tveægget. Den muliggør hurtigt samarbejde og uformel kommunikation, men reducerer den skepsis, der er nødvendig for at beskytte mod insidertrusler og social engineering.

2. *Driftsmæssige og regulatoriske sårbarheder.* Cybersikkerhed opfattes ofte som uden for kerneforretningen. Der er begrænset scenarieplanlægning og fragmenteret samarbejde. Afhængighed af enkelte leverandører eller nøglepersoner skaber skrøbelighed. Dette gælder især for SMV'er, hvor cybersikkerhedsviden ofte er samlet hos én person, typisk direktøren. Det komplekse regulatoriske landskab, NIS 2, ISO 27001, NIST og NATO-standarder, opfattes som en barriere for effektiv implementering. Én virksomhed brugte over 500 timer blot på at forstå NIS 2. Uklarhed om Styrelsen for Samfundssikkerheds (SAMSIK) ansvarsområder skaber yderligere forvirring. Ingen SMV'er nævnte SAMSIK og det nationale koordineringspunkt for cybersikkerhed, trods dets fremtrædende rolle blandt beslutningstagere.

3. *Tekniske sårbarheder.* Kombinationen af moderne systemer og ældre infrastruktur skaber systemiske risici og enkelte fejlpunkter. Overafhængighed af visse teknologier, især Microsoft, øger risikoen. De fleste deltagere udtrykte bekymring for, at nye teknologier som AI og kvantecomputing udvikler sig hurtigere end de defensive tiltag. Danmarks høje digitaliseringsniveau er en styrke, men udvider også angrebsfladen og overhaler ofte eksisterende sikkerhedsforanstaltninger.

4. *Sårbarheder i forsyningskæden*. Afhængighed af et lille antal IT-leverandører skaber koncentrationsrisiko, især når verifikationsprocesser er svage. Afhængigheder relateret til compliance i forsyningskæden gennem NIS 2 samt begrænset indsigt i underleverandørers praksis øger eksponeringen.

5. *Geopolitiske sårbarheder.* Danmarks internationale alliancer (NATO, støtte til Ukraine m.v.) øger synligheden over for statssponsorerede trusler. Beslutningstagere og policy-aktører udtrykte bekymring for robustheden i Grønland og på Færøerne, hvilket ikke fremgik i SMV'ernes svar.

Kapabilitetslandskabet er markant begrænset på SMV-niveau (se tabel 4.2). På nationalt niveau identificerede beslutningstagere væsentlige aktiver: centraliseret hændelseshåndtering, fordele ved NATO-deltagelse og avanceret digital infrastruktur. Aktører på det politiske beslutningsniveau identificerede

tilsvarende styrker. Disse når dog ikke frem til de SMV'er, de er tiltænkt at understøtte. Dette fører til det, som analysen betegner som et oversættelsesproblem i kapabiliteter. Oversættelsen fejler mellem det politiske beslutningsniveau og industriniveauet, når strategier opstiller mål uden at specificere, hvordan de skal operationaliseres. Den fejler også mellem industriniveauet og virksomhedsniveauet (SMV'erne), da vejledning ikke pålideligt når frem til de virksomheder, der har størst behov. Uklarhed om fordelingen af cybersikkerhedsansvar mellem offentlige og private aktører forstærker problemet.

Tabel 4.2 Cyberrelaterede kapabiliteter

Strategiske kapabiliteter

- Deltagelse i internationale initiativer
- Offentlig-private partnerskaber
- Strategiske investeringer i compliance
- Engagement i cybersikkerhedsindustrien
- Organisatorisk agilitet

Menneskelige og kulturelle kapabiliteter

- Cybersikkerhedstræning for ledelsen
- Awareness-programmer om cybersikkerhed
- Gennemsigtighed og en responsiv kultur
- Tillidsbaseret videndeling og indflydelse

Tekniske kapabiliteter

- Udnyttelse af avanceret digital infrastruktur

Kilde: Kankam-Boateng et al. (2026)

Praktiske implikationer. Forholdet 27:10 mellem sårbarheder og kapabiliteter kvantificerer en kvalitativ realitet. Disse SMV'er ved mere om, hvad der truer dem, end hvad der beskytter dem. At adressere dette kræver differentierede tiltag. Beslutningstagere bør supplere regulering med praktisk implementeringsstøtte tilpasset SMV'ers kapacitet og anvende kortere, mere responsiv strategicyklusser. Politiske beslutningstagere bør udvikle sektorspecifik, forenklet vejledning og facilitere erfaringsudveksling mellem SMV'er. SMV'er bør selv udpege en ansvarlig for cybersikkerhed, udvikle basale beredskabsplaner og bruge eksisterende uformelle kapabiliteter som fundament for mere strukturerede praksisser. To af virksomhederne investerede i formelle programmer og rapporterede stigende gevinster i medarbejderadfærd og beredskab. Dette tyder på, at barrieren i mindre grad handler om ressourcer og i højere grad om framing og prioritering. Et koordineret nationalt cybersikkerhedsøkosystem kan bidrage til at håndtere forsyningskæderisici og muliggøre fælles hændelseshåndtering.

4.1.2 Mentale modeller for cybersikkerhed på tværs af interessentniveauer

Mentale modeller er de indre forestillinger, som mennesker bruger til at forstå og ræsonnere om komplekse områder. De former, hvordan cybersikkerhedsrisici forstås og håndteres. Vi præsenterer den første empiriske kortlægning af mentale modeller for cybersikkerhed på tværs af tre interessentniveauer i en forsyningskæde inden for forsvarsindustrien. Den afdækker uoverensstemmelser, som er med til at forklare vedvarende kløfter mellem politiske intentioner og faktiske sikkerhedsresultater. Analysen viste markante forskelle i, hvordan interessentgrupper konceptualiserer og tilgår cybersikkerhed. Beslutningstagere beskrev en afkobling mellem nationale strategier og deres implementering på SMV-niveau, især i forhold til risikoforståelse og ressourceallokering. Brancheeksperter fremhævede udfordringer med koordinering, begrænsede investeringer i forskning og udvikling samt vanskeligheder ved at tilpasse nationale og internationale standarder. Repræsentanter fra SMV'er indtog en reaktiv tilgang. De reagerede ofte på regulering eller kundekrav. De rapporterede også mangler i hændelseshåndtering, risikovurdering i forsyningskæden og integration af cybersikkerhed i beredskabs- og kontinuitetsplanlægning. Tabel 4.3 viser de væsentligste manglende overensstemmelser i den mentale model.

Tabel 4.3 Centrale manglende overensstemmelser i mentale modeller

Dimension	Det politiske niveau	Industriniveauet	Virksomhedsniveauet
Framing af cybersikkerhed: Skellet mellem omkostning og investering	Strategiske investeringer	Økonomisk byrde	Økonomisk byrde og compliance
"Sildeeffekten"	Proaktiv, sammenkoblet	Bevidsthed om SMV'ers udfordringer	Reaktiv "sildeeffekt"
Forskelle i trusselsopfattelser	Statslige og ikke-statslige aktører	Statslige og ikke-statslige aktører	Kun ikke-statslige aktører
Regulering	Håndterbart	Bevidsthed om SMV'ers belastning	Overvældende, uoverskueligt og forvirrende

Kilde: Baseret efter Kankam-Boateng et al. (2026)

Opdelingen mellem omkostning og investering. Der fremkom en tydelig forskel i, hvordan interessenter opfatter cybersikkerhed. Beslutningstagere ser det som en strategisk investering, mens industriniveauet og SMV'erne primært betragter det som en økonomisk byrde. De fleste SMV'er ser cybersikkerhed som en omkostning drevet af regulatorisk compliance eller behov for cyberforsikring, snarere end som noget, der kan skabe forretningsværdi. Dette omkostningsfokus står i kontrast til den voksende evidens for, at investeringer i sikkerhed kan give positive afkast gennem øget kundetillid, regulatorisk compliance, der åbner markedsmuligheder, samt reducerede omkostninger ved sikkerhedsbrud. Denne framing er vigtig, fordi den påvirker, hvordan SMV'er allokerer ressourcer. Når cybersikkerhed ses som en omkostning, der skal reduceres, frem for en kapabilitet, der skal udvikles, vil investeringsbeslutninger typisk følge en minimum-compliance-tilgang frem for en strategisk tilgang.

"Sildeeffekten": Kollektiv anonymitet som sikkerhedsstrategi. En gennemgående indsigt var, at SMV'er i højere grad baserer sig på kollektiv anonymitet frem for individuelle forsvarsmekanismer. Industriniveauet beskrev, hvordan mindre virksomheder opfører sig som en stime sild – i håb om ikke at blive udvalgt af rovdyret. Denne reaktive tilgang udspringer af flere barrierer: Begrænsede ressourcer, manglende opmærksomhed og vanskeligheder ved at navigere i komplekse regulatoriske rammer. Kun tre ud af tolv deltagende SMV'er havde implementeret formelle træningsprogrammer i cybersikkerhedsbevidsthed. De fleste baserede sig på uformel kommunikation under møder og frokoster. Det er væsentligt, at dette ikke skyldes uvidenhed, men et bevidst valg, der afspejler ressourcebegrænsninger og organisationskultur. Deltagerne fremhævede eksplicit, at deres størrelse gjorde uformel kommunikation tilstrækkelig.

Forskelle i trusselsopfattelse. Det politiske niveau og industriniveauet ser et omfattende og sammenhængende trusselslandskab, der kræver proaktiv årvågenhed. De mener, at SMV'er undervurderer både truslernes omfang og deres egen værdi som mål. SMV'er fokuserer derimod primært på trusler fra ikke-statslige aktører, såsom ransomware og opportunistiske angreb, mens det politiske niveau og industriniveauet også anerkender, at statslige aktører er målrettet SMV'er f.eks. med henblik på teknologityveri eller implementering af "kill switches" i deres systemer. Den geopolitiske dimension af cybersikkerhed var helt fraværende i SMV'ernes diskussioner, men central i diskussionerne på det politiske niveau og industriniveauet. Denne kløft betyder, at SMV'er ikke implementerer beskyttelsestiltag mod systemiske trusler, som de ikke opfatter som relevante.

Regulatorisk kompleksitet som sårbarhed. Det regulatoriske miljø styrker paradoksalt nok ikke sikkerheden, men svækker den ved at overbelaste SMV'ers kapacitet til at reagere. Rammer, der er designet til at forbedre sikkerheden, fungerer som barrierer, når SMV'er mangler ressourcer til at fortolke og implementere dem. Resultatet er det, der kan kaldes "compliance-teater" – organisationer opfylder formelle krav, men forsømmer reel sikkerhed. Når konsulenter hyres til at udfylde mangler i compliance-dokumentation, opbygger SMV'erne ikke intern viden eller kapacitet inden for cybersikkerhed.

Kulturel kontekst: Høj tillid som et tveægget sværd

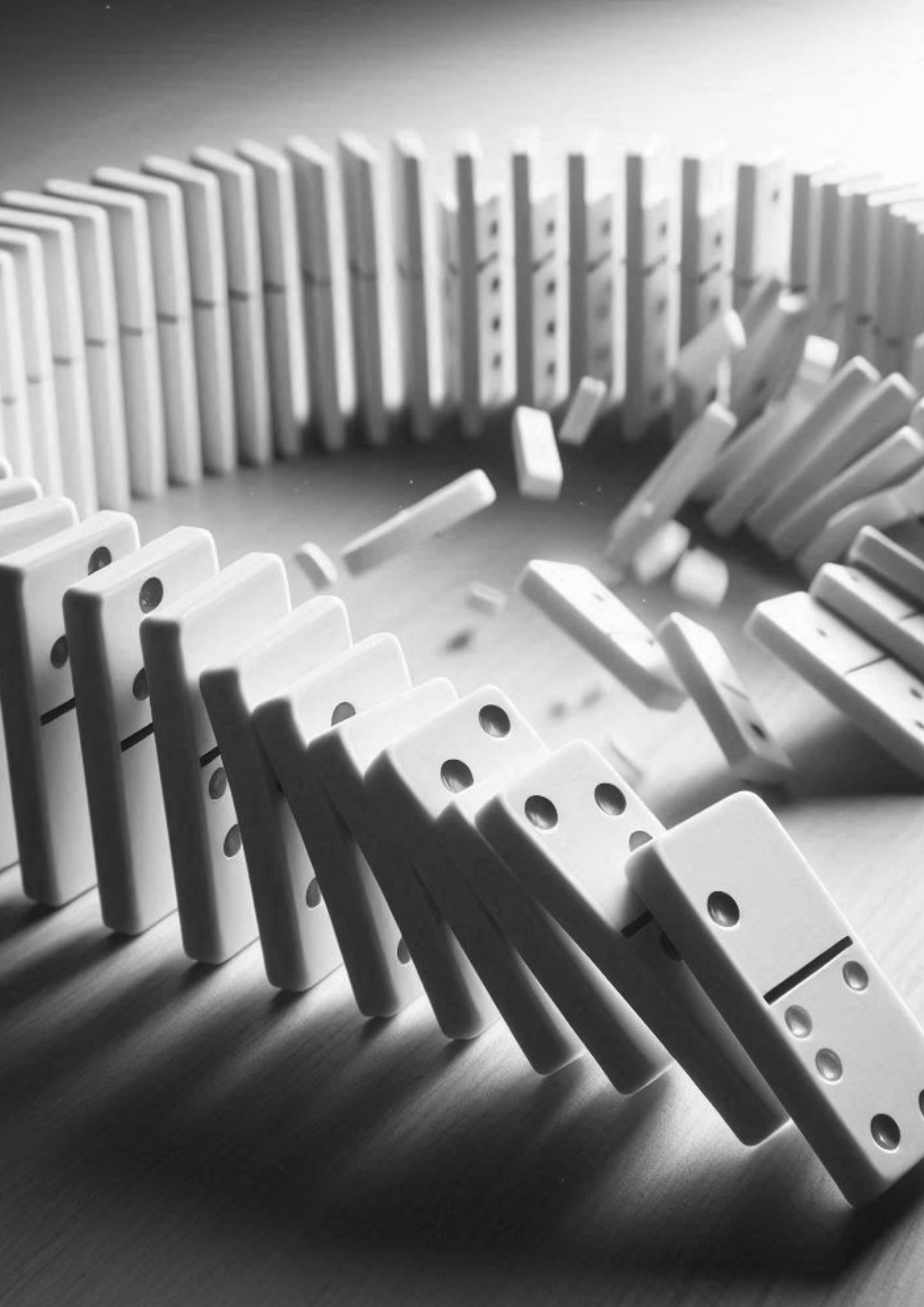
Danmarks høj-tillidskultur præger både de grundlæggende mentale modeller og dynamikken i cybersikkerhedsstyring. Den tillidsbaserede og åbne tilgang i det danske samfund fremmer samarbejde og hurtig, uformel kommunikation, men skaber også sikkerhedssårbarheder. Medarbejdere kan frit dele følsomme oplysninger med personer, der fremstår som en del af organisationen – en fordel for samarbejde, men en risiko for sikkerheden. Forskning i danske SMV'ers arbejdspraksis viser, at medarbejdere deler adgangskoder for at undgå forstyrrelser i arbejdsgange og bevidst bryder regler i mindre skala for at bevare fleksibilitet. Dette peger på sofistikerede uformelle sikkerhedspraksisser, som formelle politikker ikke nødvendigvis anerkender eller understøtter. Den høje tillid bidrager også til den førnævnte "sildeeffekt", hvor kollektiv frem for individuel handling er normen.

Praktiske implikationer

Disse divergerende mentale modeller peger på, at uens opfattelser bidrager til fragmenterede indsatser og ujævn parathed på tværs af cybersikkerhedslandskabet. Der følger flere implikationer heraf. For det første bør cybersikkerhed omrammes som en forretningsmæssig driver: SMV'er i forsvarssektoren opnåede høje standarder, når de var motiveret af sektorens krav, hvilket indikerer, at synliggørelse af forretningsværdi kan overvinde ressourcebegrænsninger. For det andet peger "silde-effekten" på behovet for kontekstualiserede mikro-læringsmoduler (5-10 minutter) frem for omfattende træningsforløb, leveret via mobile platforme og søgbare efter emne. For det tredje bør læringsnetværk udnytte avancerede SMV'er som mentorer. For det fjerde bør beslutningsstøtteværktøjer levere kontekstuelt relevante anbefalinger baseret på organisationens størrelse, sektor og trusselsprofil. For det femte bør værktøjer til compliance-mapping synliggøre, hvordan opfyldelse af én standard samtidig kan dække krav i andre, hvilket reducerer den oplevede byrde. For det sjette bør nationale cybersikkerhedsaktører skærpe deres offentlige profil og etablere klare kommunikationsveje, så SMV'er ved, hvor de skal henvende sig. Træningsprogrammer bør i højere grad tilpasses SMV'ers behov med fokus på praktiske kompetencer inden for beskyttelse, detektion, respons og kontinuitetsplanlægning. Endelig kan en integration af cybersikkerhed i forretningsplanlægningen samt en styrkelse af en sikkerhedsbevidst kultur øge robustheden mere effektivt end isolerede oplysningskampagner.

4.2 Supply chain risk management: Nye indsigter fra geopolitik

Dette afsnit sammenfatter projektgruppens arbejde med at identificere nye typer risici i forsyningskæderne afledt af geopolitikken i en ny verdensorden. Afsnittet baserer sig på Stentoft, Schmitt & Keating (2024).



4.2.1 En ny strategisk konkurrence

Afslutningen på Den Kolde Krig markerede et afgørende vendepunkt for den globale økonomi og udviklingen af moderne forsyningskæder. Sovjetunionens kollaps skabte en optimisme omkring en ny verdensorden præget af liberal kapitalisme og øget global integration. I denne periode blev det antaget, at der ikke fandtes nogen reel ideologisk konkurrent til den vestlige økonomiske model, og at nationale grænser ville blive mindre betydningsfulde i takt med stigende handel, investeringer og teknologisk udvikling. Denne udvikling førte til en adskillelse mellem økonomisk politik og sikkerhedspolitik. Handelsliberalisering og etableringen af internationale institutioner som WTO og EU bidrog til mere stabile og forudsigelige rammer for virksomheder. Samtidig opstod en form for "transnational styring", hvor stater samarbejdede om regulering og standarder, hvilket gjorde det lettere for virksomheder at operere globalt. Virksomheder begyndte i stigende grad at betragte sig selv som internationale frem for nationale aktører, hvilket muliggjorde outsourcing og globale forsyningskæder baseret primært på økonomiske hensyn.

Et centralt begreb i denne periode var *gensidig afhængighed*. Tanken var, at øget økonomisk integration ikke blot skabte velstand, men også reducerede risikoen for konflikter, fordi stater og befolkninger ville have for meget at miste ved krig. Denne idé understøttede forestillingen om, at økonomi og sikkerhed kunne adskilles, og at globalisering i sig selv ville bidrage til stabilitet. Selvom denne orden ikke var uden udfordringer, skabte den et relativt stabilt og forudsigeligt miljø for virksomheder. Beslutninger om forsyningskæder blev primært truffet ud fra økonomiske kriterier frem for politiske hensyn. I det seneste årti er denne forståelse imidlertid blevet udfordret. Den internationale orden er under pres fra stigende geopolitisk konkurrence, hvor nye magter udfordrer den vestligt dominerede verdensorden. Eksempler som Ruslands invasion af Ukraine og spændinger mellem USA og Kina illustrerer, at sikkerhedspolitiske hensyn igen spiller en central rolle. Samtidig opstår nye internationale institutioner og øget politisk fragmentering, hvilket skaber usikkerhed om de eksisterende regler. Resultatet er, at den tidligere adskillelse mellem økonomi og sikkerhed ikke længere kan opretholdes. Den globale orden er i forandring, og en ny virkelighed er ved at tage form, hvor virksomheder i højere grad må forholde sig til geopolitik i deres strategiske beslutninger. Dette har væsentlige implikationer for supply chain risk management (SCRM), som fremover må integrere både økonomiske og sikkerhedspolitiske hensyn.

4.2.2 Sikkerhed er blevet vigtigere end før

Stormagtskrigens tilbagevenden. En central konsekvens af den nye internationale orden er, at risikoen for storkrig mellem stormagter er markant øget. I perioden efter Den Kolde Krig blev militærmagt primært anvendt som et risikostyringsværktøj mod mindre trusler som terrorisme, pirateri og skrøbelige stater. Militære operationer handlede i højere grad om at håndtere og begrænse risici end om klassisk krig mellem stater. I dag er denne situation ændret. Magtbalancen er under forandring, og grundlæggende internationale normer

udfordres. Overgangen væk fra en USA-domineret verdensorden øger risikoen for konflikter mellem stormagter. Samtidig påvirkes beslutninger om krig af faktorer som ideologi, indenrigspolitik, historiske erfaringer og fejlvurderinger. Kort sagt er et internationalt system med flere konkurrerende magter og uenighed om spillereglerne mere konfliktpræget end et system domineret af én supermagt.

Sammenkobling af velstand og sikkerhed. Den nye strategiske konkurrence foregår i en verden med stærkt sammenflettede økonomier. Globaliseringen har medført outsourcing af produktion, integration af nye markeder som Kina og Indien samt friere kapitalbevægelser. Dette har skabt økonomisk vækst globalt, men også øget ulighed, hvor nogle grupper har vundet markant mere end andre. Et centralt resultat af globaliseringen er, at kilderne til velstand og sikkerhed er blevet adskilt. Hvor økonomiske og sikkerhedspolitiske relationer tidligere hang tæt sammen, er handel i dag omfattende - også mellem potentielle rivaler. Kina er f.eks. blevet en af EU's vigtigste handelspartnere. Denne situation skaber nye udfordringer. For det første kan lande være økonomiske konkurrenter, selvom de er sikkerhedspolitiske allierede. For det andet tvinges beslutningstagere i stigende grad til at balancere mellem økonomiske interesser og sikkerhedshensyn. Endelig har den tætte økonomiske integration åbnet mulighed for, at stater kan bruge økonomiske relationer som politiske våben.

Når økonomisk afhængighed bliver et våben. Begrebet "weaponized interdependence" beskriver, hvordan globale økonomiske netværk kan udnyttes politisk (Farrell & Newman, 2019). Globaliseringen har skabt asymmetriske netværk, hvor visse lande kontrollerer centrale knudepunkter i strømmen af varer, kapital og information. Disse positioner kan bruges til at overvåge, påvirke eller begrænse andre aktører. To centrale mekanismer er identificeret:

- Panoptikon-effekten, hvor stater kan overvåge informationsstrømme gennem netværk, de kontrollerer.
- Chokepoint-effekten, hvor stater kan begrænse eller blokere adgangen til kritiske netværk og dermed udøve pres.

Disse mekanismer ses bl.a. i kontrol over finansielle systemer, teknologi og infrastruktur. Stater kan f.eks. udnytte deres position i globale forsyningskæder eller teknologiske netværk til at opnå politisk indflydelse. Samtidig er denne udvikling ikke midlertidig. Infrastruktur og økonomiske netværk er i stigende grad genstand for vedvarende geopolitisk konkurrence. Stater forsøger aktivt at styrke deres positioner i forskellige netværk for at opnå strategiske fordele.

En ny æra for økonomisk sikkerhed. I den nye geopolitiske virkelighed anvender stater i stigende grad økonomiske værktøjer som strategiske redskaber. Hvor virksomheder tidligere primært har opereret med en økonomisk logik, må de nu forholde sig til, at handel, investeringer og finansielle systemer også bruges politisk. Centrale økonomiske instrumenter omfatter handelspolitik, investeringspolitik, sanktioner, direkte støtte, pengepolitik, lovgivning og kontrol over råstoffer.

Handelspolitik er et klassisk magtmiddel, der både kan bruges til at skabe samarbejde og til at lægge pres på andre stater. Eksempler ses i Ruslands brug af importforbud over for nabolande og Kinas anvendelse af adgang til sit store marked som politisk presmiddel. På samme måde spiller investeringer en stigende rolle, hvor stater opkøber aktiver i andre lande gennem f.eks. statslige investeringsfonde. Dette giver mulighed for politisk indflydelse, hvilket har ført til øget kontrol med udenlandske investeringer globalt. Sanktioner er et andet centralt værktøj, som både signalerer politiske grænser og svækker modstandere økonomisk. De kan være rettet mod handel, individer eller finansielle systemer, men deres effekt afhænger af, hvor tæt økonomier er forbundet. Samtidig bruges direkte støtte og bistand til at skabe afhængighedsforhold mellem stater, mens pengepolitik kan påvirke både egne og andre landes økonomiske handlemuligheder. Derudover anvendes lovgivning og retssystemer i stigende grad strategisk, herunder gennem ekstraterritorial lovgivning. Endelig spiller kontrol over naturressourcer som energi en væsentlig rolle, hvor f.eks. gas og olie bruges som politiske pressionsmidler.

4.2.3 Konsekvenser for supply chain risk management

Fremkomsten af en ny verdensorden skaber nye risici for både offentlige og private forsyningskæder. For at strukturere analysen kan disse risici opdeles i makro- og mikrofaktorer (f.eks. efterspørgsel, produktion, leverancer, information, transport og finans). De nye risici udspringer især af fire overordnede udviklinger: 1) tilbagevenden af storkrig, 2) øget strategisk konkurrence, 3) "weaponized interdependence" og 4) økonomisk sikkerhed. Disse faktorer hænger tæt sammen og afspejler et grundlæggende dilemma mellem økonomisk åbenhed (velstand) og sikkerhed.

Storkrigens tilbagevenden. Større krige udgør en alvorlig trussel mod globale forsyningskæder. Krig kan ødelægge produktionsanlæg, infrastruktur og transportnetværk, hvilket skaber mangel på ressourcer og forstyrrer handel. Samtidig kan krigsøkonomier føre til markedsforvridninger og ændrede handelsstrømme. Aktuelle risici inkluderer konflikter mellem USA og Kina (f.eks. omkring Taiwan), krige i Mellemøsten, som USA's og Israels angreb på Iran og fortsatte konflikter i Europa, herunder mellem Rusland og Ukraine. Disse konflikter kan eskalere gennem stormagtsindblanding. Eksempler viser tydeligt konsekvenserne. Krigen i Ukraine har påvirket handel via Sortehavet og ødelagt kritisk infrastruktur, mens konflikten i Gaza medførte omdirigering af skibstransport og længere leveringstider. Konflikten i Iran har skabt alvorlige forstyrrelser for den internationale skibstrafik, primært gennem trusler og direkte angreb i strategisk vigtige områder som Hormuzstrædet og Det Røde Hav, men også en voldsom stigning i oliepriserne. Samtidig har alternative transportveje, f.eks. jernbane gennem Rusland, skabt nye etiske og omdømmemæssige udfordringer for virksomheder. For at håndtere disse risici kræves proaktiv risikostyring, løbende overvågning af politiske forhold og evne til hurtigt at tilpasse sig ændringer.

Ny strategisk konkurrence. Den stigende konkurrence mellem stater om geopolitisk indflydelse, økonomisk magt og teknologisk dominans påvirker i høj grad globale forsyningskæder. Særligt konkurrencen om teknologi (f.eks. kunstig intelligens, cybersikkerhed og avanceret produktion) skaber konflikter om viden, data og kontrol. Dette medfører øgede cyberrisici, herunder angreb på virksomheder og forsyningskæder. Samtidig forsøger stater i stigende grad at koble økonomiske og sikkerhedspolitiske interesser, hvilket betyder, at politiske beslutninger får direkte konsekvenser for virksomheder. Et eksempel er USA's pres på europæiske lande for at begrænse samarbejde med Kina inden for mikrochip-industrien. Her bruges sikkerhedspolitiske relationer til at påvirke økonomiske beslutninger. Konsekvensen er, at virksomheder ikke længere kan træffe beslutninger udelukkende ud fra økonomiske hensyn, men også må tage højde for nationale sikkerhedsinteresser og politisk pres.

Når afhængighed bliver et våben. "Weaponized interdependence" beskriver, hvordan økonomiske afhængigheder bruges strategisk til at opnå politisk indflydelse. I en globaliseret økonomi er lande forbundet gennem komplekse netværk af handel, finans og teknologi, og disse forbindelser kan udnyttes. Eksempler inkluderer energiforsyning, hvor lande kan begrænse leverancer for at lægge politisk pres, eller kontrol over digitale platforme og finansielle systemer, som virksomheder er afhængige af (f.eks. betalingssystemer og online markedspladser). Andre eksempler er restriktioner på teknologi (f.eks. halvledere), desinformationskampagner og kontrol over kritiske råmaterialer som sjældne jordarter. For virksomheder betyder dette, at de skal kortlægge deres afhængigheder, diversificere leverandører, styrke cybersikkerhed og samarbejde tættere med myndigheder og partnere for at håndtere geopolitisk risiko.

Økonomisk sikkerhed. Økonomisk sikkerhed handler om, at stater bruger økonomiske værktøjer til at beskytte nationale interesser og opnå strategiske mål. Dette kan påvirke forsyningskæder gennem ændringer i markeder, produktion og sourcing. Flere lande, herunder USA, Kina, Japan, og EU udvikler nationale strategier for økonomisk sikkerhed. EU arbejder f.eks. med investeringsscreening og overvejer yderligere regulering, hvilket kan skabe nye handelsbarrierer. Stater anvender også tiltag, der forvrider markeder, f.eks. støtte til nationale industrier. Et eksempel er USA's Inflation Reduction Act, som fremmer indenlandsk produktion. For nogle virksomheder betyder dette øget usikkerhed: markeder kan pludselig lukke, leverandører kan blive utilgængelige, og virksomheder kan blive mål for politisk eller juridisk pres. For at håndtere disse risici bør virksomheder overvåge geopolitik, diversificere deres forsyningskæder, styrke robusthed og arbejde med scenarieplanlægning. Samarbejde med myndigheder og brancheorganisationer er også centralt.

4.2.4 Geopolitik og supply chain risk management

Supply chain risk management har fået betydelig opmærksomhed i det seneste årti som følge af store forstyrrelser såsom den globale COVID-19-pandemi og øgede geopolitiske spændinger, herunder Brexit, handelskrigen mellem USA og Kina, Ruslands invasion af Ukraine samt ustabilitet i Det Røde Hav

og Mellemøsten. Tabel 4.4 indeholder de nye risikofaktorer i forsyningskæder, som virksomheder og myndigheder bør tage højde for, og som er identificeret ved at betragte geopolitik som en integreret faktor, baseret på de foregående analyser af den nye verdensorden, vi befinder os i.

Tabel 4.4 Forsyningskæderisici i et geopolitisk perspektiv

Tilbagevenden til storkrig	Afbødning (Mitigation)
Risikofaktorer • Kritisk infrastruktur • Omfordeling af ressourcer i krisesituationer • Handelsforstyrrelser • Markedsforvridning • Intens konkurrence om knappe ressourcer	
Ny strategisk konkurrence *Risikofaktorer* • Uforudsete eksportkontrolregler, især for teknologiske produkter • Tyveri af data og intellektuel ejendom • Datamanipulation og misinformation • Begrænset adgang til højt kvalificeret arbejdskraft • Øget volatilitet i forretningsmiljøet	• Systematisk overvågning af politiske risici • Systematisk analyse af værdifulde og sårbare aktiver • Udvikling af en fælles risikovillighed i virksomheden • Relevante cybersikkerhedspolitikker • Lobbyarbejde og public affairs-aktiviteter • Politikker for håndtering af information og dataanalyse • Metodiske værktøjer til at understøtte kritisk beslutningstagning (f.eks. red teaming, scenarieopbygning m.m.) • Etablering af triggerpunkter og beredskabsprotokoller samt træning i krisesituationer • Samarbejde med interessenter • Alternative handelsruter
Når afhængighed bliver et våben (weaponized interdependence) *Risikofaktorer* • Sårbarhed i forretningsnetværk • Teknologisk infrastruktur • Begrænsninger i teknologioverførsel • Lammet beslutningstagning pga. misinformation • Knaphed på naturressourcer	
Økonomisk sikkerhed *Risikofaktorer* • Begrænsede markedsmuligheder pga. handelsbarrierer (f.eks. screening af udenlandske investeringer) • Tvungen ændring af forsyningskæder som følge af politisk regulering • Omdømmerisici (f.eks. ved handel med sanktionerede aktører) • Afhængighed af globale reservevalutaer • Øget statslig indblanding og reguleringsusikkerhed	

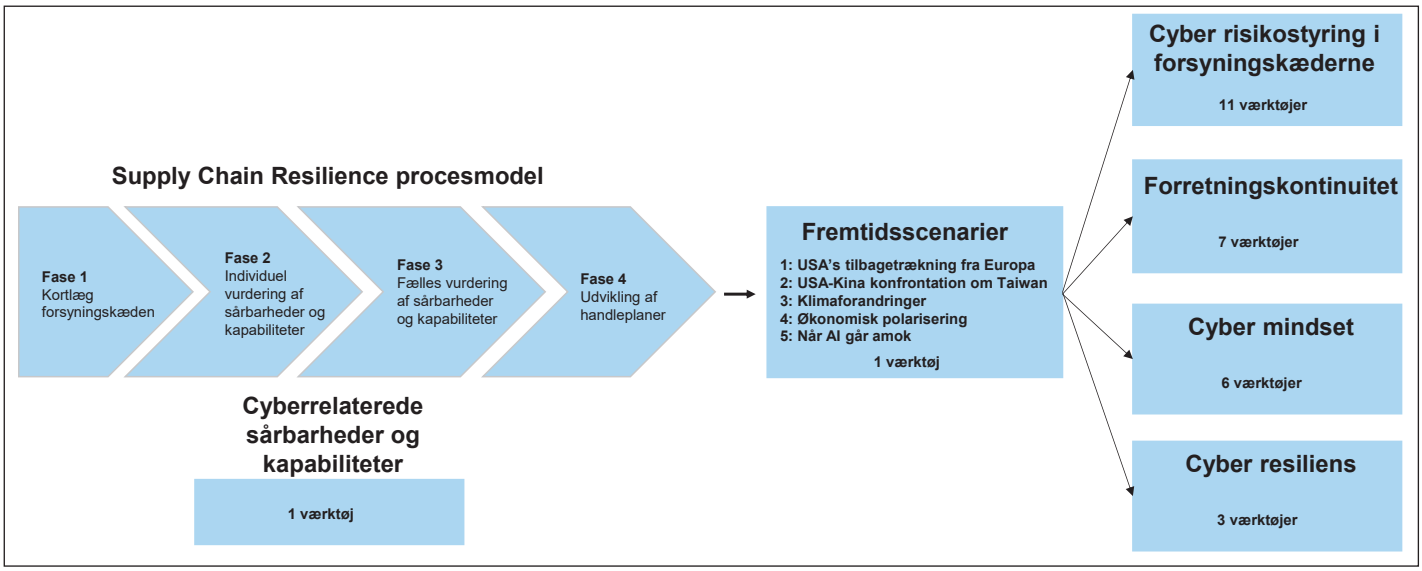
Kilde: Stentoft, Schmitt & Keating (2024)

Generelt er der for de fire områder i tabel 4.4 behov for yderligere forskning i, hvilke nye kompetencer der er nødvendige for supply chain managers i en ny verdensorden præget af stigende geopolitiske spændinger.

4.3 Værktøjer

Projektet har udviklet værktøjer fordelt på seks områder, som det fremgår af figur 4.1. Virksomheder anbefales først at arbejde med supply chain resilience procesmodellen for at skabe en tværorganisatorisk forankring af arbejdet. Her er det muligt at vælge et nyt sæt af cyberrelaterede sårbarheder og kapabiliteter, at vælge supply chain relaterede sårbarheder og kapabiliteter eller kombinere dem. Derefter er det forslaget, at et tværorganisatorisk team arbejder med fremtidsscenarier. Herefter kan man vælge at gå flere veje indenfor de fire områder med cyber supply chain risk management, forretningskontinuitet, cyber mindset og cyber resiliens. I de følgende delafsnit beskrives værktøjerne nærmere.

Figur 4.1 Oversigt over udviklede værktøjer



4.3.1 Supply chain resilience procesmodel software

Den webapplikation, der operationaliserer fase 2 og 3 i procesmodellen, er tilgængelig på denne adresse: **https://process-model.cyber-smv.dk/** og kan anvendes gratis til ikke-kommercielle formål (se projektets hjemmeside for databeskyttelsespolitik og slutbrugerlicens). Brug af applikationen kræver registrering som virksomhed. Når der er oprettet en virksomhedskonto, bliver det muligt at administrere et team af brugere, som kan inviteres til at deltage i vurderingsprocessen og bidrage på tværs af de relevante faser. Platformen

understøtter gentagen anvendelse af modellen, hvilket gør det muligt for virksomheder at gennemføre flere vurderinger over tid og dermed opbygge en struktureret historik af resultater, som kan bruges til at følge udviklingen, genbesøge prioriteringer og overvåge forbedringer i forsyningskædens robusthed. En detaljeret brugervejledning er tilgængelig på projektets hjemmeside.

4.3.2 Fremtidsscenarier

På baggrund af analyser på både politisk niveau og i industrien er der udviklet fem mulige fremtidsscenarier. De er lavet som fortællinger, der skal få medarbejdere i virksomhederne til at tænke over, hvordan fremtiden også kan se ud – ikke kun som en forlængelse af det, vi kender i dag. I modsætning til traditionelle prognoser, der ofte bygger på, at udviklingen fortsætter nogenlunde som hidtil, handler scenarieplanlægning om at undersøge, hvad der kan ske, hvis der opstår større forandringer eller brud i omgivelserne. Dette skel er centralt for at forstå forskellen på risiko og usikkerhed. Hvor risiko refererer til situationer, hvor sandsynligheder kan kvantificeres objektivt baseret på historiske data (eksempelvis ved markedsudsving), er den nuværende geopolitiske situation præget af fundamental usikkerhed. Her er variablerne ukendte, og udfaldene kan ikke måles eller forudsiges med statistisk sikkerhed.

Formålet med de udviklede scenarier er at operationalisere 'sensing'-kapabiliteten under teorien om dynamiske kapabiliteter (se afsnit 2.8). I en geopolitisk kontekst er sensing ikke begrænset til traditionel markedsovervågning, men kræver en evne til at afkode svage signaler om statslige hensigter og strukturelle skift, før de rammer forsyningskæden. Ved at anvende plausible, men fiktive narrativer, fungerer scenarierne som en kognitiv træningsbane, der hjælper beslutningstagere med at overvinde ukritiske antagelser som f.eks., at nuværende stabile forhold vil fortsætte uændret.

> **"Arbejdet med fremtidsscenarier gjorde det tydeligt, hvor hurtigt trusselsbilledet kan ændre sig. Det har gjort os mere bevidste om behovet for løbende tilpasning."**
>
> *Andreas Kürzel, Indkøb og IT, Dansk Gummi Industri A/S*

Gennem denne proces transformerer virksomheden abstrakt, geopolitisk usikkerhed til mere håndterbare risikobilleder. Scenarierne gør det muligt for ledelsen at øve sig i at genkende mønstre i et uforudsigeligt miljø (sensing), hvilket er forudsætningen for efterfølgende at kunne mobilisere ressourcer (seizing) og omstille organisationen (transforming). Uden denne narrative ramme risikerer virksomheder at overse geopolitiske trusler, fordi de udelukkende navigerer efter en økonomisk markedslogik, der ikke kan forudsige statslig indgriben og konflikt. I alt er fem scenarier udviklet: 1) USA's tilbagetrækning fra Europa, 2) USA-Kina-konfrontation om Taiwan, 3) Klimaforandringer, 4) Økonomisk polarisering og 5) Når AI går amok.

USA's tilbagetrækning fra Europa. Dette scenarie beskriver en verden, hvor USA trækker sig tilbage fra NATO og europæisk sikkerhed for at fokusere på Indo-Stillehavsregionen og interne forhold. For danske virksomheder betyder det et fragmenteret Europa, der må stå for egen sikkerhed, hvilket medfører øgede forsvarsbudgetter, men også en markant øget risiko for cyberangreb og sabotage fra Rusland mod kritisk infrastruktur og forsyningskæder i Norden og Baltikum.

USA-Kina-konfrontation om Taiwan. Scenariet tager udgangspunkt i en eskalering af konflikten om Taiwan og Det Sydkinesiske Hav, der udvikler sig til en fuld blokade. Dette fører til et sammenbrud i de globale forsyningskæder for elektronik og mikrochips, hvor vestlige virksomheder fanges i krydsilden af sanktioner, handelsblokader og gensidige cyberangreb mellem stormagterne.

Klimaforandringer. Her fokuseres på de direkte og indirekte konsekvenser af ekstreme vejrfænomener. Scenariet beskriver en virkelighed med massive nedbørsmængder og oversvømmelser, der fysisk ødelægger infrastruktur og forstyrrer logistikken. Samtidig udnytter cyberkriminelle det kaos, der opstår efter naturkatastrofer, til at udføre angreb på sårbare systemer, hvilket skaber en "dobbelt krise" for virksomhederne.

Økonomisk polarisering. Dette scenarie omhandler en verden præget af stigende økonomisk ulighed og svindende middelklasser i Vesten, hvilket fører til politisk ustabilitet og protektionisme. Cybertruslen i dette scenarie drives af desillusionerede aktører og statsstøttede hackergrupper fra sanktionsramte økonomier (som Rusland), der angriber vestlige virksomheder som led i en asymmetrisk økonomisk krigsførelse.

Når AI går amok. Scenariet udforsker sårbarheden ved overdreven afhængighed af automatisering og kunstig intelligens. Det beskriver en situation, hvor en udbredt AI-tjeneste eller chatbot kompromitteres gennem et supply chain attack eller malware, hvilket fører til massive datalæk og finansielle tab for virksomheder, der blindt har stolet på tredjepartsleverandører uden tilstrækkelig due diligence.

4.3.3 Cybersikker supply chain risk management

Et tredje sæt af værktøjer handler om cybersikkerhedspraksisser, der anlægger et supply chain perspektiv. Projektarbejdet har operationaliseret de 10 praksisser om cybersikkerhed i et forsyningskædeperspektiv foreslået af NIST (2024). Værktøjerne er:

- Struktureret efter NIST-rammeværket
- Oversat til konkrete handlinger, der kan bruges i hverdagen
- Målrettet samarbejde med leverandører og partnere

Fokus er på at gøre cybersikkerhed praktisk, prioriterbar og anvendelig. De 10 praksisser fremgår af tabel 4.5.

Tabel 4.5 10 cybersikkerhedspraksisser med et supply chain fokus

#	Praksis
1	En strategi for risikostyring af cybersikkerhed i forsyningskæderne er etableret og accepteret af virksomhedens interessenter.
2	Cybersikkerhedsroller og ansvarsområder for leverandører, kunder og samarbejdspartnere fastlægges, kommunikeres og koordineres internt og eksternt.
3	Risikostyring af cybersikkerhed i forsyningskæderne er integreret i virksomhedens generelle risikostyring og forbedringsprocesser.
4	Leverandører er kendte og prioriteret efter, hvor kritiske de er.
5	Krav til håndtering af cybersikkerhedsrisici i forsyningskæder fastlægges, prioriteres og integreres i kontrakter og andre typer aftaler med leverandører og andre relevante tredjeparter.
6	Planlægning og due diligence (detaljerede undersøgelser) gennemføres for at reducere risici, inden der indgås formelle leverandør- eller andre tredjepartsrelationer.
7	Risici forbundet med en leverandør, dens produkter og tjenester samt andre tredjeparter identificeres, registreres, prioriteres, vurderes, besvares og overvåges i løbet af relationen.
8	I tilfælde af hændelser (incidents) inddrages relevante leverandører og andre tredjeparter i planlægning i modsvar og i aktiviteter med at genoprette praksis.
9	Sikkerhedspraksis i forsyningskæderne er integreret i vores generelle risikostyring, og produkters og serviceydelsers performance overvåges gennem hele deres livscyklus.
10	Planer for styring af cybersikkerhedsrisici i forsyningskæderne inkluderer bestemmelser for aktiviteter, der finder sted efter ophør af et partnerskab eller en serviceaftale.

Kilde: NIST (2024, p. 17)

Et søsterprojekt i cyberporteføljen: Cybersikre forsyningskæder

Mange SMV'er oplever i dag stigende krav til cybersikkerhed, både fra større kunder og nye regler.

SUCCESS: Værktøjer til sikkerhed i leverandørkæden er et projekt ledet af **Copenhagen Business School** og støttet af Industriens Fond, Dansk Erhverv og Dansk Industri. Projektet hjælper SMV'er med at få overblik over cyberrisici i leverandørkæden og komme i gang med konkrete løsninger.

Cyberangreb rammer i stigende grad leverandører som indgang til større virksomheders netværk. Samtidig stiller NIS 2-direktivet krav om, at virksomheder i kritisk infrastruktur kan dokumentere, hvordan de håndterer cyberrisici. Når større virksomheder tilpasser sig de nye krav, mærker mange SMV'er det indirekte gennem skærpede sikkerhedskrav fra kunder og samarbejdspartnere.

Mange SMV'er er afhængige af eksterne leverandører til f.eks. cloud-løsninger, lønadministration og IT-support, der kan få adgang til følsomme data og forretningskritiske systemer uden at deres sikkerhed vurderes systematisk.

På baggrund af erfaringer fra over 25 danske SMV'er samt input fra forskere, regulatoriske eksperter og større virksomheder er der udviklet konkrete værktøjer, guides og workshops målrettet SMV'er.

Materialerne er gratis og hjælper virksomheder med at styrke sikkerheden i deres leverandørkæder og leve op til krav fra både myndigheder og kunder.

Find værktøjenerne her

4.3.4 Forretningskontinuitet

Det fjerde sæt af værktøjer har fokus på forretningskontinuitet, der handler om virksomhedens evne til at:

- Opretholde eller hurtigt genoptage kritiske funktioner
- Håndtere alvorlige forstyrrelser som:
  - IT-nedbrud
  - Cyberangreb
  - Brand
  - Leverandørsvigt

Cybersikkerhed i produktions-SMV'er handler således ikke kun om teknik, men også om overblik, prioritering og evnen til at handle, når noget går galt. Værktøjerne er bevidst opbygget, så man:

- Forstår forretningen
- Identificerer risici
- Prioriterer afhængigheder
- Planlægger handling
- Træner beslutninger

De følgende syv værktøjer udgør tilsammen en pragmatisk tilgang, der hjælper produktions-SMV'er med at beskytte drift, leverancer og forretning.

Business Impact Analyse (BIA). En BIA identificerer, hvilke forretningsprocesser og systemer der er mest kritiske, og hvilke konsekvenser nedbrud har for produktion, økonomi og kunder. Den danner fundamentet for alle efterfølgende tiltag.

Risiko- og sårbarhedsanalyse. Her vurderes, hvilke cybertrusler virksomheden realistisk står overfor, og hvor sårbarheder findes – både i IT- og Operational Technology (OT). Analysen hjælper med at fokusere indsatsen dér, hvor risikoen er størst.

Leverandørkritikalitetsanalyse. Produktions-SMV'er er ofte afhængige af eksterne leverandører. Denne analyse klarlægger, hvilke leverandører der er forretningskritiske, og hvordan deres IT- eller OT-sikkerhed kan påvirke produktionen.

Kontinuitetsplaner. Sådanne planer beskriver, hvordan virksomheden opretholder eller hurtigt genstarter driften, hvis systemer eller produktion bliver ramt. Fokus er på praktiske løsninger – også når IT ikke er tilgængelig.

Scenarieplanlægning. Her omsættes analyser til praksis ved at gennemgå realistiske cyberhændelser (f.eks. ransomware eller IT→OT-spredning) og afklare beslutninger, roller og handlinger på forhånd.

Cyberberedskabsplanlægning. Her samles det hele i én operativ drejebog, der beskriver, hvordan virksomheden opdager, håndterer, kommunikerer og genopretter efter en cyberhændelse.

Tabletop-øvelser. Tester beredskabet i praksis uden at påvirke driften. Ledelse, IT og produktion gennemgår et cyberangreb trin for trin for at sikre, at planer, beslutninger og samarbejde fungerer under pres.

4.3.5 Cyber mindset

Det femte sæt af værktøjer fokuserer på mentale modeller og adfærd og består af seks værktøjer udviklet til awareness-træning. Cybersikkerhed handler ikke kun om teknologi og politikker. Det handler i høj grad om menneskelig adfærd i en hverdag præget af:

- Travlhed
- Kompleksitet
- Konstante afbrydelser

De fleste cyberangreb lykkes ikke, fordi teknologien fejler, men fordi mennesker presses til at handle hurtigt, ureflekteret eller i god tro. Værktøjerne giver medarbejdere:

- Enkle og genkendelige tankeprincipper
- Støtte til at stoppe op og tænke sig om
- Hjælp til konkrete situationer, før der klikkes, deles, betales eller på anden måde reageres

Antag kompromittering. Formålet er her at skabe realistisk risikoforståelse og fokus på konsekvensreduktion frem for fejlfrihed.

Angriberens perspektiv. Formålet er at øge forståelsen for social engineering (manipulation til at give adgang til følsomme data), at forstå hvordan angribere tænker og arbejder og at blive bedre til at opdage manipulation, før skaden sker.

Lag på lag (Defense in Depth). Formålet er at forstå, hvorfor sikkerhed er et samspil mellem mennesker, processer og teknologi og at fjerne idéen om "det ene rigtige værktøj".

Pause-knappen (Slow Down). Formålet er at skabe et refleksionsrum før handling, at modstå pres og manipulation og at modvirke impulshandlinger udløst af stress, frygt og hast.

Normalisering af fejl (Just Culture). Formålet er at fremme rapportering og læring frem for skyld og tavshed og at blive trygge ved at tale åbent om fejl, nærved-hændelser og usikkerhed.

Signal vs støj (Attention Economics). Formålet er at kunne skelne mellem væsentlige sikkerhedssignaler og almindelig baggrundsstøj, at erkende at opmærksomhed er en begrænset ressource, at prioritere hvad der kræver handling, og hvad der kan ignoreres samt at mindske risikoen for at overse kritiske advarsler i en travl hverdag.

4.3.6 Cyber resiliens

Det sjette sæt af værktøjer har fokus på cyber resiliens, dvs. virksomheders evne til at modstå cyberangreb. Cyber resiliens afhænger i stigende grad af, hvor godt interne beskyttelsesforanstaltninger er afstemt, hvordan styring af forsyningskæden er etableret, og hvordan tredjeparter håndteres med rettidig omhu. De tre cyber resiliensværktøjer, vi stiller til rådighed, udgør samlet en struktureret tilgang, der gør det muligt for virksomheder at styrke deres evne til at forebygge, modstå og komme sig efter cyberhændelser og i sidste ende udvikle en forsvarsstrategi, der reducerer risikoen for vellykkede cyberangreb.

Beskyttelse af intellektuel ejendom. Dette værktøj hjælper virksomheder med systematisk at identificere, klassificere og beskytte deres mest værdifulde aktiver, så de kan forstå, hvor kritisk intellektuel ejendom (IP) befinder sig, hvem der har adgang til den, og hvordan den kan beskyttes i den daglige drift. Ved at kortlægge medarbejderes viden, minimere insider-relaterede risici og indføre passende sikkerhedsforanstaltninger for data i hvile, under overførsel og i brug styrker virksomheder deres evne til at forhindre lækager og beskytte følsomme oplysninger under de ressourcebegrænsninger, som er typiske for mange SMV'er. Værktøjet guider desuden virksomheder i at udarbejde beredskabs- og genopretningsplaner, så de effektivt kan reagere på tab eller kompromittering af IP, opretholde driftsstabilitet og gendanne højværdifuld information. Samlet set gør det virksomheder i stand til at reducere sandsynligheden for og konsekvenserne af IP-relaterede angreb, øge bevidstheden om fortrolighed blandt interne og eksterne interessenter og opbygge en mere robust modstandsdygtighed over for trusler som insider-misbrug, uautoriseret dataudtræk og kompromittering via forsyningskæden.

Sikkerhed i forsyningskæden ud fra et produkt-/service-livscyklusperspektiv. Dette værktøj understøtter virksomheder i at integrere cybersikkerhed i alle faser af produktets eller tjenestens livscyklus, så de kan håndtere leverandørrelaterede cyberrisici helhedsorienteret og proaktivt. Ved at indarbejde forsyningskædesikkerhed i governance-strukturer, definere klare krav tidligt i designfasen og gennemføre risikobaseret leverandørklassificering og due diligence kan organisationer sikre, at de vælger de rette partnere og fastsætter håndhævelige sikkerhedskrav. Værktøjet styrker også robustheden ved at vejlede virksomheder i at implementere sikre udviklings- og leveringspraksisser, verificere produktintegritet før accept og løbende overvåge sårbarheder og leverandørers performance. Gennem veldefinerede kontrakter, samarbejde om håndtering af hændelser og sikre afslutningsprocesser bevarer virksomheder kontrol over kritiske afhængigheder gennem hele relationen. Dermed opnår de en mere gennemsigtig, forudsigelig og robust forsyningskæde, som reducerer mulighederne for manipulation, forfalskede komponenter, usikre opdateringer eller kompromittering i efterfølgende led, hvilket markant styrker den samlede cyber resiliens.

Risikoreduktion ved indgåelse af leverandør- eller andre tredjepartsrelationer. Dette værktøj giver organisationer mulighed for at vurdere og reducere cyberrisici, før de indgår nye partnerskaber. Dermed sikres det, at tillid, adgang og datadeling kun gives, når risikoniveauet er acceptabelt. Ved at analysere

forretningskritikalitet, datasensitivitet, adgangsmodeller, leverandørers cybersikkerhedsmodenhed, evne til hændelseshåndtering samt juridiske eller jurisdiktionsmæssige forhold opnår virksomheder en helhedsforståelse af deres eksponering, før der indgås aftaler. Dette gør det muligt at tilpasse kontraktkrav, stille krav om passende sikkerhedsdokumentation, fastsætte realistiske krav til varsling og samarbejde samt afvise højrisikoleverandører eller indføre kompenserende kontrolforanstaltninger, når det er nødvendigt. Værktøjet fremmer også langsigtet robusthed ved at understøtte gennemsigtighed omkring afhængigheder, underleverandører og softwarekomponenter samt ved at fremhæve de kulturelle og samarbejdsmæssige aspekter, der indikerer, om en partner vil håndtere sikkerhed ansvarligt. I sidste ende hjælper det organisationer med at undgå skjulte risici, forebygge fremtidige driftsforstyrrelser og etablere tredjepartsrelationer, der styrker deres cyber resiliens frem for at svække den.

4.4 Spørgeskemaundersøgelser om cybersikkerhed

I projektet er der gennemført to landsdækkende spørgeskemaundersøgelser (Stentoft et al., 2024, 2026). I dette afsnit bringes resultaterne af tre områder fra 2026-undersøgelsen: 1) cybersikker supply chain risk management, 2) cybersikkerheds dynamiske kapabiliteter og 3) geopolitiske dynamiske kapabiliteter. Resuméer af resultater fra de to undersøgelser fremgår af tabel 4.6.

Tabel 4.6 Resuméer af resultater fra to spørgeskemaundersøgelser om cybersikkerhed

Kilde: Stentoft et al. (2024, 2026)

Note: Tal i parentes angiver gennemsnitsværdier på en 5-punkts Likert-skala, hvor 1 = i meget lav grad og 5 = i meget høj grad.

2024-undersøgelsen

Krav til cybersikkerhed
- Bestyrelsen spiller en moderat rolle (3,43), men fokus er ikke stærkt.
- Lavere krav fra investorer (2,91) og kunder (2,55).
- 17% oplever krav om standarder (f.eks. ISO27001, GDPR).
- 18% følger frivilligt standarder (f.eks. NIS 2, D-mærket).

Cyberangreb
- 20% har været udsat for cyberangreb de seneste år.

Cybersikkerhed som kvalifikator
- Opfattes som vigtig for virksomhedens image (3,44).
- Meget lave krav til leverandører (2,01) → fokus er primært internt.

Opmærksomhed på cybersikkerhed
- Høj bevidsthed om vigtigheden (alle ~4,2+).
- Virksomheder anerkender behov for sikkerhedspraksis og foranstaltninger.

Supply chain risk management (cyber)
- Generelt lavt niveau (2,0–3,08).
- Kun begrænset fokus på leverandørers cybersikkerhed.
- Stort udviklingsbehov.

Supply chain orientering
- Generelt god (3,40 samlet).
- Fokus på samarbejde og langsigtede relationer.
- Godt udgangspunkt for at forbedre cybersikkerhed i forsyningskæden.

Intern integration
- Høj intern integration (3,75).
- Mindre silotænkning → godt fundament for cybersikkerhedsarbejde.

Geopolitik
- 60% har fokus, men 40 % mangler fokus.
- Moderat påvirkning af forretning (3,33).
- 45% påvirkes af udenlandsk lovgivning (f.eks. GDPR, NIS 2).
- Udviklingsbehov i strategisk håndtering.

Drift vs. udvikling
- Drift prioriteres højere (3,74) end udvikling (3,30).
- Klassisk dilemma: kortsigtet drift vs. langsigtet cybersikkerhedsudvikling

2026-undersøgelsen

Teknisk kompleksitet i cybersikkerhed
- Opleves generelt som lav (1,62–2,12).
- Godt niveau ift. opdateringer, overblik over enheder og OT-tilpasning.

IT-/OT-integration
- Generelt god styring.
- Styrker: Overblik over aktiver, sikre protokoller og netværkssegmentering.

Cyberangreb
- 25% har været udsat for cyberangreb de seneste år.

NIS 2-compliance
- 22% er omfattet, 67% er ikke, 11% er usikre.
- Krav fra interessenter.
- Drives primært af ledelsen.
- Bestyrelsens fokus er stadig begrænset.

Krav til kunder og leverandører
- Meget få cybersikkerhedskrav i værdikæden.
- Indikerer lav modenhed.

Supply chain risk management (cyber)
- Lavt niveau (1,82–2,86).
- Stort udviklingsbehov.

Cybersikre dynamiske kapabiliteter
- Generelt lave (sensing 2,0/seizing 1,94/transforming 2,4).
- Begrænset evne til at håndtere og tilpasse sig cybertrusler.

Geopolitiske markedskræfter
- Moderat til lav påvirkning (~2,25–2,98).
- Størst påvirkning fra cybertrusler og konflikter.

Dynamiske kapabiliteter (geopolitik)
- Lave niveauer (ca. 2,04–2,36).
- Begrænset evne til at reagere strategisk.

Geopolitisk risikostyring
- Svagt udviklet (1,67–2,81).
- Behov for styrket strategisk fokus.

4.4.1 Cybersikker supply chain risk management

De 10 praksisser i tabel 4.5 har indgået i en national spørgeskemaundersøgelse gennemført i 2026 (Stentoft et al., 2026). Resultaterne af respondenternes svar på deres brug af de 10 praksisser fremgår af figur 4.2. I tilfælde af hændelser (incidents) inddrages relevante leverandører og andre tredjeparter i planlægning, i modsvar og i aktiviteter med at genoprette praksis i nogen grad med et gennemsnit på 2,95 på en 5-punkts Likert-skala (hvor 1 = i meget lav grad og 5 = i meget høj grad). Risikostyring af cybersikkerhed som en del af virksomhedens samlede risikostyring scorer i gennemsnit 2,93. Resultatet peger på, at der er behov for forbedringer. Den relativt lave score kan hænge sammen med, at den generelle risikostyring også halter. Det ses også i forhold til arbejdet med en egentlig strategi for cybersikkerhed i forsyningskæden, som ligger på 2,37 i gennemsnit.

Overvågning af risici fra leverandører og andre samarbejdspartnere sker kun i begrænset omfang (2,20), og det samme gælder for tydelig fordeling af roller og ansvar inden for cybersikkerhed (2,19). Derudover bliver produkters og serviceydelsers performance også kun i lav grad fulgt gennem hele deres livscyklus (2,15). Mere dybdegående vurderinger af cyberrisici gennemføres sjældent (2,02), og endnu sjældnere inden indgås der formelle aftaler med leverandører (1,94). Det peger på et klart forbedringsområde i forhold til at få informationssikkerhed ind i både nye og eksisterende samarbejdsaftaler. Den laveste score (1,88) handler om manglende klarhed over, hvad der sker med data, når samarbejdet med en ekstern partner ophører. Samlet set tyder resultaterne på, at udfordringerne skyldes en kombination af begrænsede ressourcer, lav organisatorisk modenhed og komplekse forsyningskæder i SMV'er. Mange SMV'er har hverken økonomi eller kompetencer til at arbejde systematisk med cybersikkerhed, og fokus ligger ofte på den daglige drift frem for sikkerhed.

Samtidig mangler der ofte faste processer for håndtering af leverandører, herunder krav til deres cybersikkerhed og løbende risikovurderinger (Melnyk et al., 2022). Produktionsvirksomheder arbejder desuden ofte med komplekse og ofte internationale forsyningskæder samt gør brug af ældre og manuelle systemer, hvilket gør det svært at skabe overblik over risici. Historisk har der også været begrænset regulering på området for SMV'er, hvilket har mindsket incitamentet til at arbejde strategisk med cybersikkerhed. Derudover bliver cybersikkerhed ofte set som et rent IT-ansvar i stedet for et fælles ansvar på tværs af organisationen. Alt i alt peger de lave scorer derfor mere på lav modenhed i arbejdet med cybersikkerhed i forsyningskæden end på nødvendigvis dårlig teknisk sikkerhed.

Figur 4.2 Cybersikker supply chain risk management

Kilde: Stentoft et al. (2026)

Det er overraskende, at resultaterne fra 2026-undersøgelsen (figur 4.2) generelt set er lavere med et samlet gennemsnit på 2,25 end tilsvarende resultater fra 2024-undersøgelsen, hvor det samlede gennemsnit var på 2,31 (Stentoft et al., 2024, 2025). De lave gennemsnit kan skyldes manglende ressourcer og/eller viden til at omsætte praksisserne til konkret handling.

Kronik: No trust – no buy: Cyberangreb truer den sidste del af salgstragten (sammendrag)

Du kender salgstragten: Know – Like – Trust – Buy. Men når virksomheder rammes af cyberangreb, rammes især det næstsidste og afgørende trin: tilliden. Uden tillid – intet køb.

Danske virksomheder oplever i stigende grad cyberangreb med alvorlige konsekvenser. Et eksempel er elektronik- og hvidevarekæden Power, der på Black Friday blev ramt af et massivt angreb med 628 millioner købsforespørgsler, som lagde systemerne ned. Ejendomsmæglerkæden EDC har ligeledes været udsat for et angreb, hvor personlige dokumenter fra mere end 1.300 personer blev stjålet.

Cyberangreb kan antage mange former. DDoS-angreb kan overbelaste systemer og lamme digitale platforme. Man-in-the-middle-angreb kan opsnappe fortrolig kommunikation mellem parter. Phishing forsøger at lokke medarbejdere til at afsløre følsomme oplysninger via falske mails eller beskeder. Og malware kan give hackere adgang til virksomhedens systemer og data. Fælles for angrebene er, at de kan få store konsekvenser for drift, omdømme og konkurrenceevne.

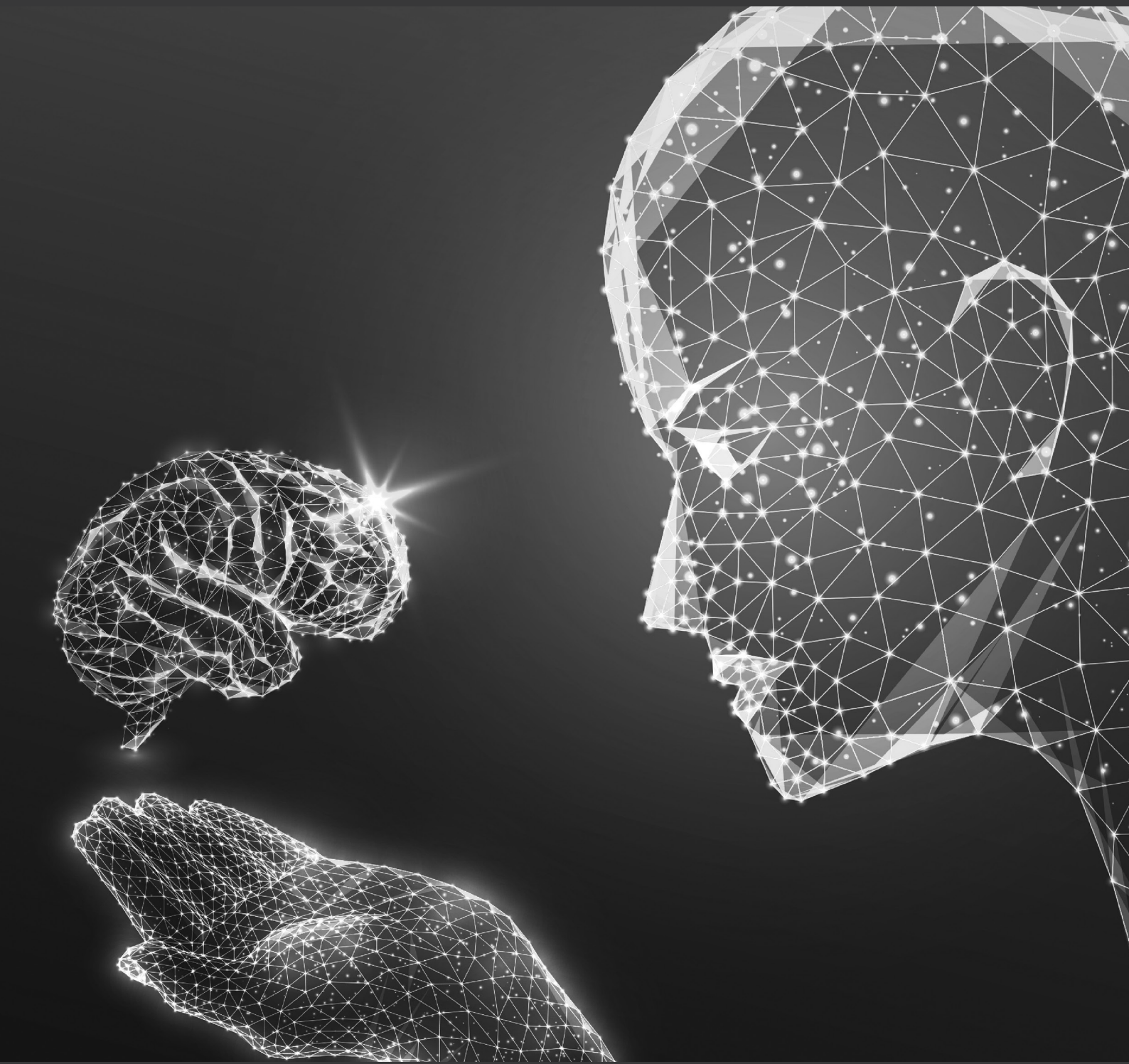
Det er derfor ikke kun en opgave for IT-afdelingen. Salgs- og marketingafdelinger bør også tage cybersikkerhed alvorligt. De arbejder tæt på kunderne og håndterer ofte følsomme oplysninger som kundedata, forretningshemmeligheder og strategiske planer. Hvis disse kompromitteres, kan det skade virksomhedens omdømme og underminere kundernes tillid.

Tillid er et centralt element i relationen mellem kunde og leverandør. Hvis kunderne ikke føler sig trygge ved at dele data med en virksomhed, kan det direkte påvirke salget. Omvendt kan en stærk cybersikkerhedsindsats signalere ansvarlighed og professionalisme og dermed styrke relationen til kunderne.

Arbejdet med cybersikkerhed bør begynde med at identificere virksomhedens mest kritiske processer og vurdere sårbarhederne. Indsatsen bør forankres i topledelsen og involvere hele organisationen, da cyberrisici kan ramme alle dele af virksomheden.

Cybersikkerhed koster ressourcer. Men alternativet – driftstop, datalæk og tab af tillid – kan i sidste ende true virksomhedens eksistens.

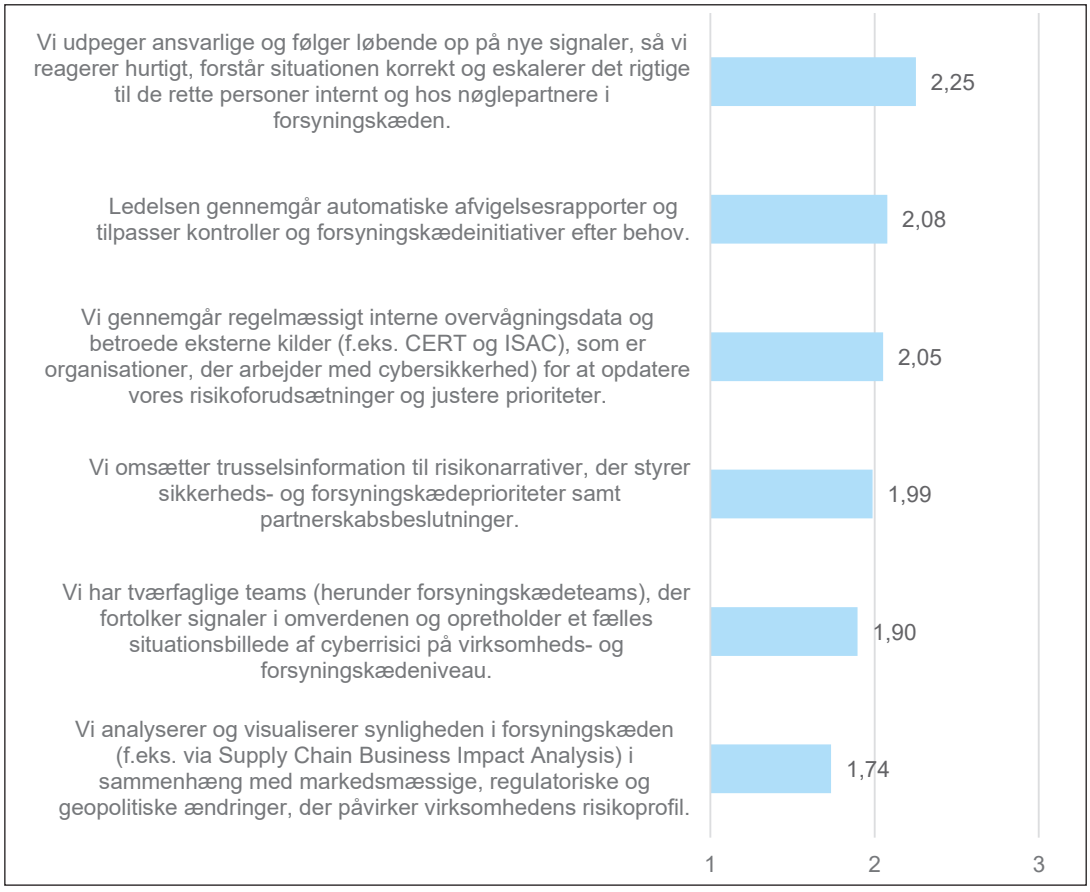
Kilde: Stentoft, Peressotti & Mayer (2024) Læs kronikken her



4.4.2 Cybersikkerheds dynamiske kapabiliteter

Projektet har også foreslået en operationalisering af dynamiske kapabiliteter for cybersikkerhed omkring sensing, seizing og transforming jf. afsnit 2.8. Figur 4.3 viser resultaterne for virksomhedernes evne til at opdage og følge med (sensing) i cybertrusler i forsyningskæden. Den gennemsnitlige score for de seks statements er 2,00, hvilket tyder på, at virksomhederne kun i begrænset grad overvåger og forstår signaler om cybertrusler i deres omgivelser. Det peger på, at meget få virksomheder arbejder systematisk med at indsamle og analysere trusselsinformation, f.eks. gennem tværgående samarbejde internt. Samtidig mangler e fleste både værktøjer og processer til at holde øje med nye trusler, vurdere samarbejdspartneres sikkerhedsniveau eller bruge ekstern viden aktivt i deres risikovurderinger. Resultatet understreger desuden, at evnen til at opdage og forstå trusler, stadig er svagt udviklet, selvom den er helt central for at opbygge robusthed på cyberangreb i forsyningskæder. For at stå stærkere kræver det bl.a. bedre indsigt i risici, større gennemsigtighed i forsyningskæden og en mere aktiv brug af trusselsinformation. Uden disse elementer bliver det svært for virksomheder at identificere risikofyldte samarbejdspartnere, forstå deres digitale afhængigheder og reagere rettidigt på nye trusler. Det peger på et tydeligt strategisk hul. Samtidig tyder resultaterne på, at virksomheder i begrænset omfang arbejder proaktivt med at indsamle viden om trusler eller indgår i samarbejder, hvor de kan lære af andre. Det gør dem mere sårbare, fordi de i højere grad risikerer at opdage trusler senere end mere modne organisationer. Derfor er der et klart behov for at styrke den løbende overvågning af cybertrusler, bl.a. gennem brug af eksterne informationskilder og en bedre forståelse af risici og sårbarheder i hele forsyningskæden.

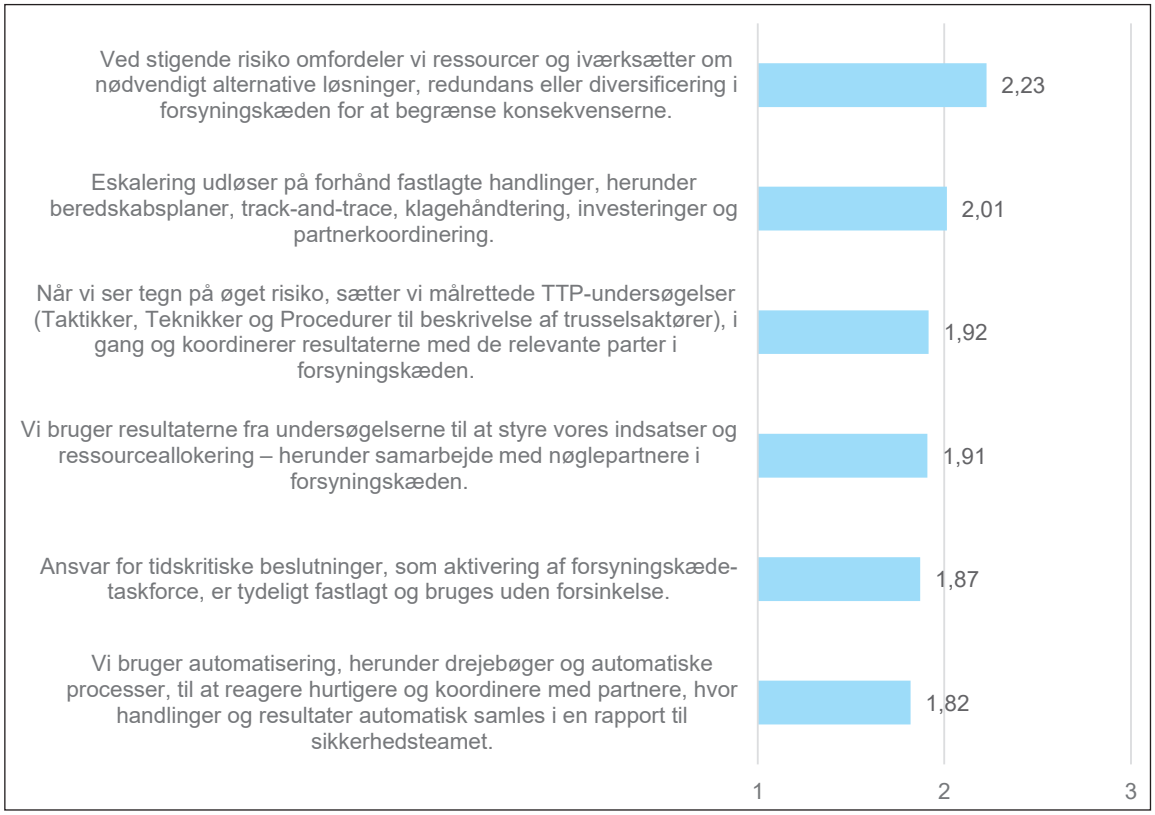
Figur 4.3 Cyber sensing kapabiliteter



Kilde: Stentoft et al. (2026)

Seizing-kapabiliteterne ligger på samme lave niveau som sensing (se figur 4.4). Det kan virke logisk, at når evnen til at opdage trusler er lav, så er evnen til at handle på dem også lav, men det viser samtidig, at SMV'erne ikke opvejer mangler i sensing ved at være bedre til at reagere. Alle målepunkter for seizing ligger i gennemsnit under 3 (under middel), og den samlede score for de seks statements er faktisk 1,96, hvilket er endnu lavere end for sensing. Især områder som at oprette taskforces og automatisere processer, der kan sikre hurtig reaktion på hændelser, scorer meget lavt. Det tyder på, at evnen til at handle hurtigt og effektivt på cybertrusler er meget begrænset i danske SMV'er. Selvom de lavest-scorende områder naturligt bør prioriteres først, viser de generelt lave scorer, at der er behov for forbedringer på tværs af alle områder. Samtidig peger resultaterne på, at det giver mening at starte med at styrke sensing. Hvis virksomhederne bliver bedre til at opdage og forstå trusler, får de også et stærkere grundlag for at udvikle deres evne til at handle på dem.

Figur 4.4 Cyber seizing kapabiliteter

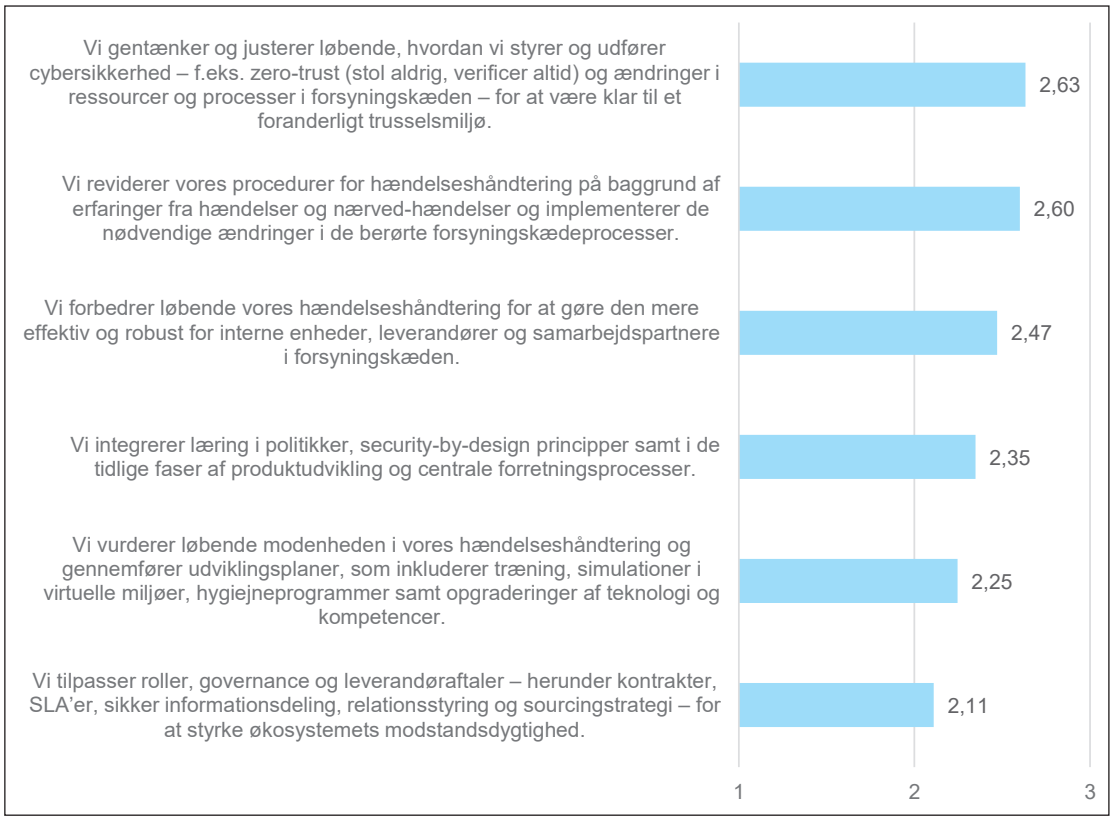


Kilde: Stentoft et al. (2026)

Figur 4.5 viser resultaterne af respondenternes svar på deres transformation-praksisser. Det er interessant, at de deltagende SMV'er vurderer deres evne til at tilpasse sig (transforming) højere end både deres evne til at opdage og reagere (sensing og seizing) på cybersikkerhedstrusler. Men med en gen-

nemsnitlig score på 2,40 for de seks statements og generelt lave vurderinger på de enkelte områder, ligger niveauet stadig tydeligt under midten af skalaen. Det viser, at der fortsat er et stort behov for forbedringer. Transformation handler her om virksomhedernes evne til løbende at tilpasse organisation, processer og teknologi i takt med nye cybertrusler. Det kan f.eks. være gennem ændringer i struktur, opbygning af kompetencer og ved at tænke cybersikkerhed ind i den overordnede forretningsstrategi. Respondenterne har vurderet seks forskellige områder. Løbende justering og gentænkning af cybersikkerhed scorer højest med 2,63, mens tilpasning af roller, styring og leverandøraftaler ligger lavest med 2,11. Særligt det lave fokus på cybersikkerhed i samarbejdet med leverandører er bekymrende, da det peger på svagheder i håndteringen af risici i forsyningskæden – noget der også hænger sammen med de lave scorer på sensing og seizing. Derudover fremstår automatisering af cybersikkerhedsreaktioner som et vigtigt område at forbedre. Samlet set viser resultaterne, at SMV'er kun i begrænset grad formår at tilpasse sig strategisk og organisatorisk til cybertrusler. Især de mere langsigtede og strukturelle ændringer halter, hvilket kan gøre det svært at håndtere et stadigt mere komplekst trusselsbillede.

Figur 4.5 Cyber transformation kapabiliteter



Kilde: Stentoft et al. (2026)

Sammenfattede kan det udledes af ovenstående, at der indtil data ikke synes at være en bevidsthed om at anskue cybersikkerhed som dynamiske kapabiliteter. Dette indikerer et udviklingspotentiale for virksomhederne.

4.4.3 Geopolitiske dynamiske kapabiliteter

Dette cyberprojekts fokus på dynamiske kapabiliteter indikerer, at den eksisterende forståelse af dynamiske kapabiliteter, som primært er udviklet til at håndtere markedsvolatilitet og teknologisk disruption, er utilstrækkelig i den nuværende globale orden. Hvor konventionelle dynamiske kapabiliteter fokuserer på virksomhedens evne til at tilpasse sig ændringer i udbud og efterspørgsel (markedslogik), kræver den nye virkelighed, at virksomheder navigerer i et miljø præget af *weaponized interdependence og economic statecraft.* I dette paradigme er statslige aktører ikke blot regulatorer, men strategiske modstandere, der aktivt manipulerer økonomiske netværk for at opnå sikkerhedspolitiske mål. Dette nødvendiggør udviklingen af en særskilt kategori af kompetencer: *Geopolitiske Dynamiske Kapabiliteter (GDC)*.

GDC adskiller sig fundamentalt fra markedsorienterede kapabiliteter ved at adressere trusler, der er eksogene i forhold til markedet, men endogene i forhold til statslige sikkerhedsdilemmaer. Med dette menes, at truslerne ikke udspringer af markedets egne mekanismer som konkurrence og udbud/efterspørgsel, og derfor er de eksogene i forhold til markedet. Derimod opstår de indefra i den sikkerhedspolitiske dynamik mellem stater, hvor oprustning, mistillid og strategiske modsvar skaber gensidige spændinger; derfor er de endogene i forhold til statslige sikkerhedsdilemmaer. Pointen er, at den samme trussel kan være ekstern i én kontekst og intern i en anden afhængigt af hvilket system, man analyserer. For at forstå behovet for GDC er det nødvendigt først at afdække de to modstridende logikker, der i dag præger det globale forretningsmiljø: 1) markedslogikken og 2) den geopolitiske logik.

Markedslogikken (Den liberale verdensorden)

Den konventionelle teori om dynamiske kapabiliteter hviler på antagelserne fra den liberale verdensorden. Her er den primære styringsmekanisme markedet, og det ultimative mål er effektivitet.

- *Rationalitet*: Aktører antages at være økonomisk rationelle og profitmaksimerende. Relationer er 'positive-sum', hvilket betyder, at handel skaber gensidig gevinst.
- *Statens rolle*: Staten fungerer som en neutral regulator, der håndhæver regler og sikrer fri konkurrence. Politik og økonomi betragtes som adskilte sfærer.

Hvad betyder det for de dynamiske kapabiliteter? Det betyder, at sensing er gearet til at opdage markedsmuligheder; seizing indebærer, at virksomheden aktivt investerer i og restrukturerer sine ressourcer for at udnytte nye muligheder. Tiltag som stordriftsfordele eller just-in-time kan være en del af denne proces, hvis de indgår som strategiske valg snarere end blot operationel effektivisering. Transforming handler om løbende optimering af forretningsmodellen for at slå konkurrenterne på pris eller innovation.

Den geopolitiske logik (Den kommende geoøkonomiske orden)

I modsætning til markedslogikken opererer den geopolitiske logik under vilkår af anarki og sikkerhed. Her er den primære styringsmekanisme sikkerhed, hvor målet ikke kun er profit, men overlevelse og relativ styrke.

- *Rationalitet:* Aktører (stater) prioriterer sikkerhed. Relationer er ofte 'zero-sum', hvor modpartens økonomiske gevinst ses som en sikkerhedstrussel.
- *Statens rolle:* Staten er en strategisk aktør, der intervenerer direkte i markedet. Økonomiske afhængigheder (som gasledninger, digitale netværk og forsyningskæder) kan være "weaponized" – omdannet til pressionsmidler.

Hvad betyder det for de dynamiske kapabiliteter? Markedsoptimerede kapabiliteter bliver sårbarheder i denne logik. En effektiv, global forsyningskæde (god markedskapabilitet) kan være et let mål for en fjendtlig stat (dårlig geopolitisk kapabilitet). Konflikten mellem de to logikker skaber et strategisk dilemma for SMV'er. Virksomheder, der udelukkende navigerer efter markedslogikken, vil sense prissignaler, men overse politiske signaler. De vil seize effektiviseringsgevinster ved at outsource til lavtlønslande, men derved utilsigtet gøre sig sårbare over for chokepoints i weaponized interdependence.

Derfor skal de dynamiske kapabiliteter, efter forfatternes opfattelse, rekonfigureres således:

- **Sensing:** Hvor konventionel sansning fokuserer på at identificere nye markedssegmenter eller disruptive teknologier, kræver GDC en systematisk kapacitet til at afkode politiske signaler og statslige intentioner. For SMV'er indebærer dette at overvåge udviklingen i national og ekstraterritorial sikkerhedslovgivning, identificere latente sårbarheder i dybe forsyningskæder *(n-tier)* og forudse, hvor fremtidige eksportkontroller eller sanktioner kan ramme. Det handler om at opbygge et geopolitisk varslingssystem, der kan identificere en politisk risiko, før den materialiserer sig som en logistisk eller juridisk forstyrrelse.
- **Seizing:** Traditionelt dikterer denne fase, at virksomheder skal allokere ressourcer for at maksimere profit og markedsandele, ofte gennem aggressiv omkostningsoptimering. Under GDC-paradigmet må virksomheder i stedet gribe muligheden for at opbygge strategisk robusthed, hvilket ofte sker på direkte bekostning af den kortsigtede indtjening. Dette indebærer yderst vanskelige operationelle afvejninger, såsom overgangen fra *just-in-time* til kapitalbindende *just-in-case* lagerføring, etablering af omkostningstunge *dual-sourcing* netværk og det bevidste fravalg af højteknologiske leverandører, der befinder sig i politiske højrisikozoner.
- **Transforming:** Den klassiske transformationsevne har historisk været rettet mod at integrere virksomheden dybere og mere gnidningsløst i globale netværk. GDC kræver i mange tilfælde det stik modsatte: Evnen til strategisk afkobling og kontrolleret fragmentering. Virksomheder skal designe en organisationsstruktur og en forsyningskæde, der hurtigt kan isolere kompromitterede dele af netværket. Dette kan omfatte tvungen regionalisering

af produktionen *(friend-shoring)*, opbygning af parallelle it-systemer eller ændring af selve produktarkitekturen, så produktionen gøres uafhængig af kritiske råmaterialer fra rivaliserende stormagter.

Overgangen til GDC er således ikke blot en tilføjelse af nye værktøjer, men et fundamentalt skifte i virksomhedens kognitive og operationelle mindset – fra en logik baseret på velstandsskabelse gennem handel til en logik baseret på overlevelse gennem strategisk autonomi.

Podcast: Cybersecurity Awareness (uddrag)

De mest almindelige cyberangreb

Ifølge Marco Peressotti, lektor ved Institut for Matematik og Datalogi, Syddansk Universitet, er det mest almindelige cyberangreb i dag phishing, herunder kompromittering af forretnings-e-mails. Phishing betragtes ofte som den mest udbredte cybertrussel i verden, da den let og billigt kan skaleres. Barrieren for cyberkriminelle til at gå ind i phishing-arenaen er meget lav på grund af eksistensen af 'phishing-as-a-service'-operationer, hvor hackere kan få phishing-kits, der i bund og grund fungerer som enhver anden service, man kan få på internettet. Andre cyberangreb tager form af malware, ransomware og distribueret denial of service (DDoS).

Bevidsthed og adfærdsændring

Med det øgede niveau af cyberangreb i danske virksomheder er det afgørende, at medarbejdere øger deres bevidsthed om cybersikkerhed. En sådan proces kan også føre til et behov for at ændre adfærd. "En af de mest værdifulde ting, virksomheder kan gøre, er at forsøge at fremme en sikkerhedskultur. Det vil sige, at alle medarbejdere forstår, at sikkerhed er en vigtig del af at holde virksomheden kørende, og at alle gør deres bedste for at holde virksomheden sikker", siger Peter Mayer, adjunkt ved Institut for Matematik og Datalogi, Syddansk Universitet. En del af dette er også, at der ikke er et 'blame game', hvis noget sker. Det vil sige at undgå fokus på, hvis skyld det er, men snarere en skyldfri evaluering af, hvad der gik galt, og hvordan det kan ændres, så det ikke går galt igen.

Sikkerhed og antagelser

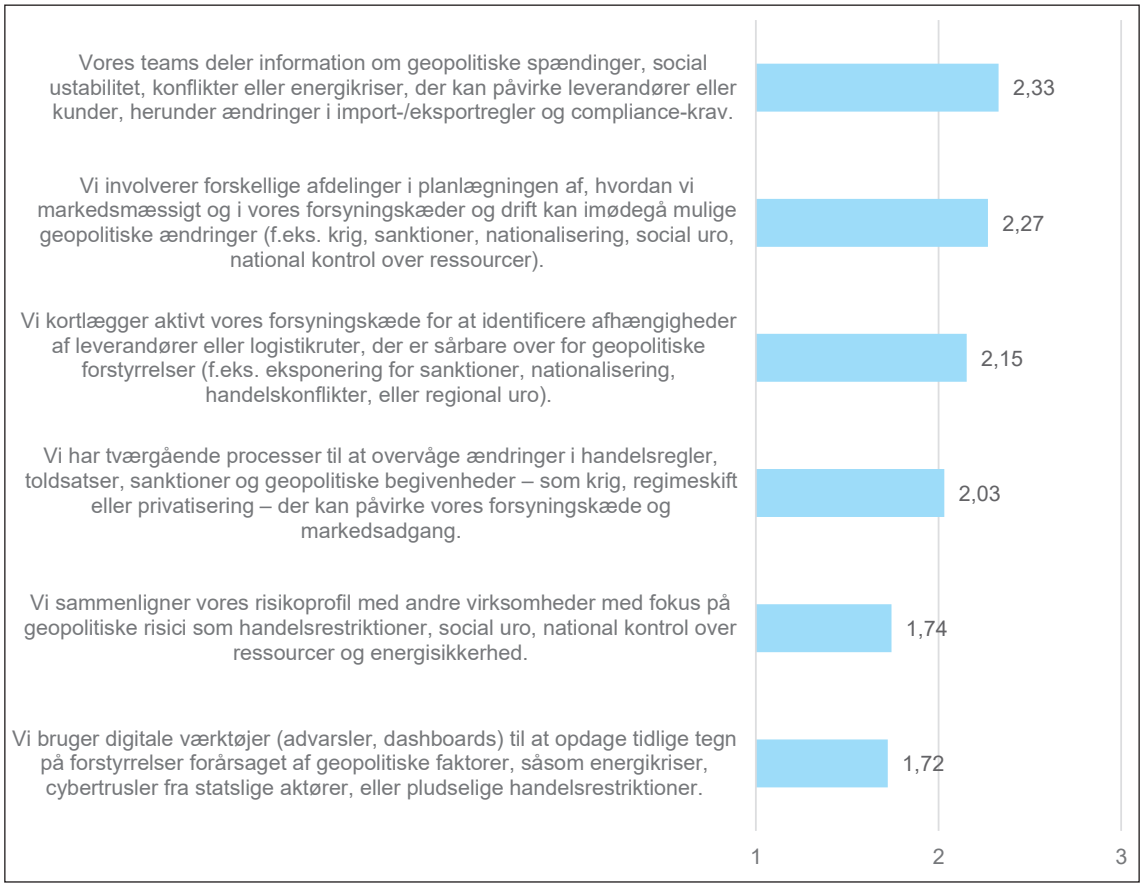
Det er vigtigt at bemærke, at begrebet sikkerhed kun eksisterer med udgangspunkt i antagelser. Hvis man antager, at ingen af e-mail-kontiene bliver kompromitteret, kan selv fortrolige oplysninger opbevares i indbakken. Man kunne også antage, at ingen af maskinerne i netværket bliver kompromitteret, og så kan en ressource bare være tilgængelig på det interne netværk.

"Derfor, kunne det være et interessant første skridt at gøre folk opmærksomme på, at de har gjort disse antagelser - måske ikke eksplicit, men implicit - og måske at nedskrive, hvad de antager ikke vil ske for dem", siger Peter Mayer.

Kilde: Peressotti et al. (2024) Hør podcasten her

Geopolitiske dynamiske kapabiliteter blev også undersøgt i 2026-undersøgelsen. Virksomhedernes evne til at opfange geopolitiske trusler (sensing) er desværre ret lav (se figur 4.6). De deler i nogen grad information om spændinger (gennemsnit 2,33), men det sker ikke særlig systematisk. Samtidig bruger de næsten ikke digitale værktøjer til at opdage tidlige tegn på forstyrrelser (1,72), og de sammenligner sjældent deres risikoniveau med andre virksomheder (1,74). Det peger på en tydelig blind vinkel: Når virksomhederne ikke arbejder datadrevet med at opdage risici, øger det risikoen for, at de bliver overrasket af geopolitiske spændinger, før det begynder at påvirke deres drift.

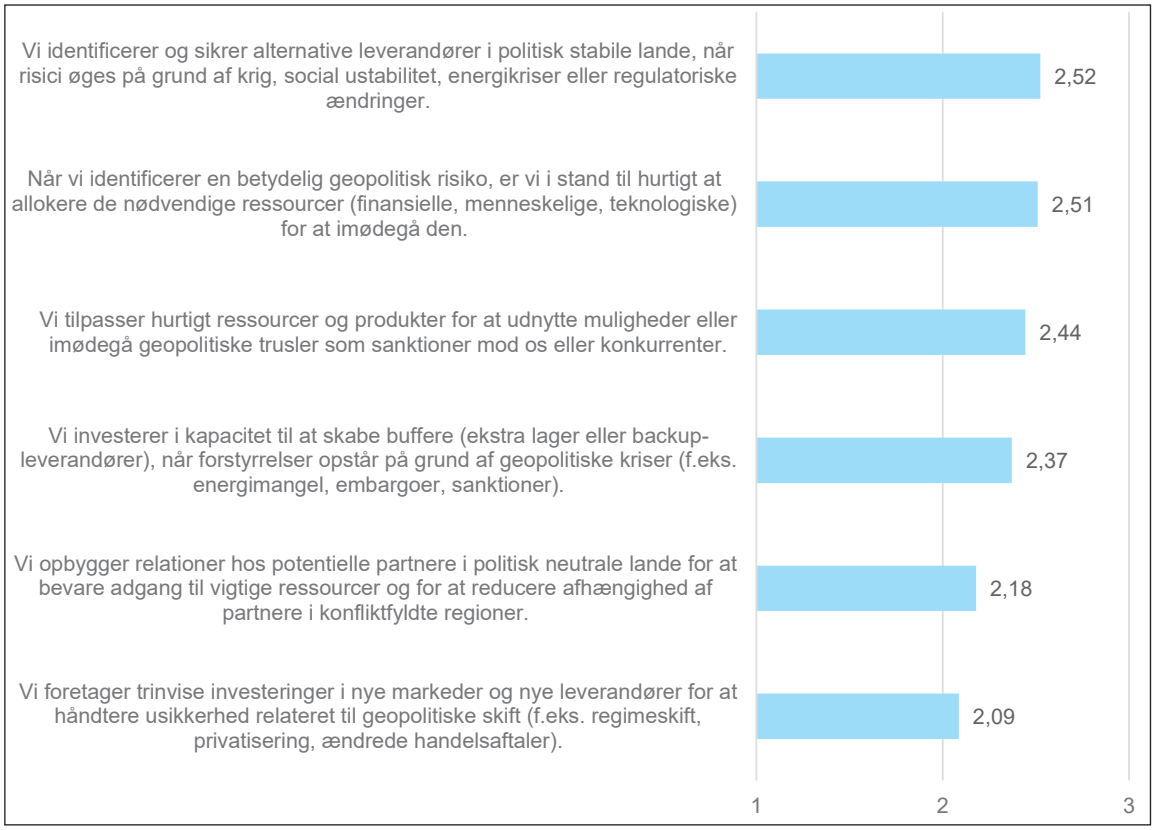
Figur 4.6 Geopolitiske sensing kapabiliteter



Kilde: Stentoft et al. (2026)

Den samlede score for geopolitisk seizing er en smule højere med et gennemsnit på 2,36 (se figur 4.7). Det kan hænge sammen med, at virksomhederne er vant til at reagere hurtigt, når der opstår problemer. Men alle seks områder ligger stadig under 3, hvilket viser, at niveauet generelt er lavt. Virksomhederne synes i nogen grad de er gode til at finde alternative leverandører i stabile lande (2,52) og til at opbygge ekstra lager i krisesituationer (2,51). Det er værre, når det gælder mere langsigtede og strategiske investeringer i nye markeder og leverandører, som kun scorer 2,37. Det tyder på, at indsatsen ofte er præget af kortsigtet krisehåndtering frem for en mere planlagt og langsigtet opbygning af robusthed.

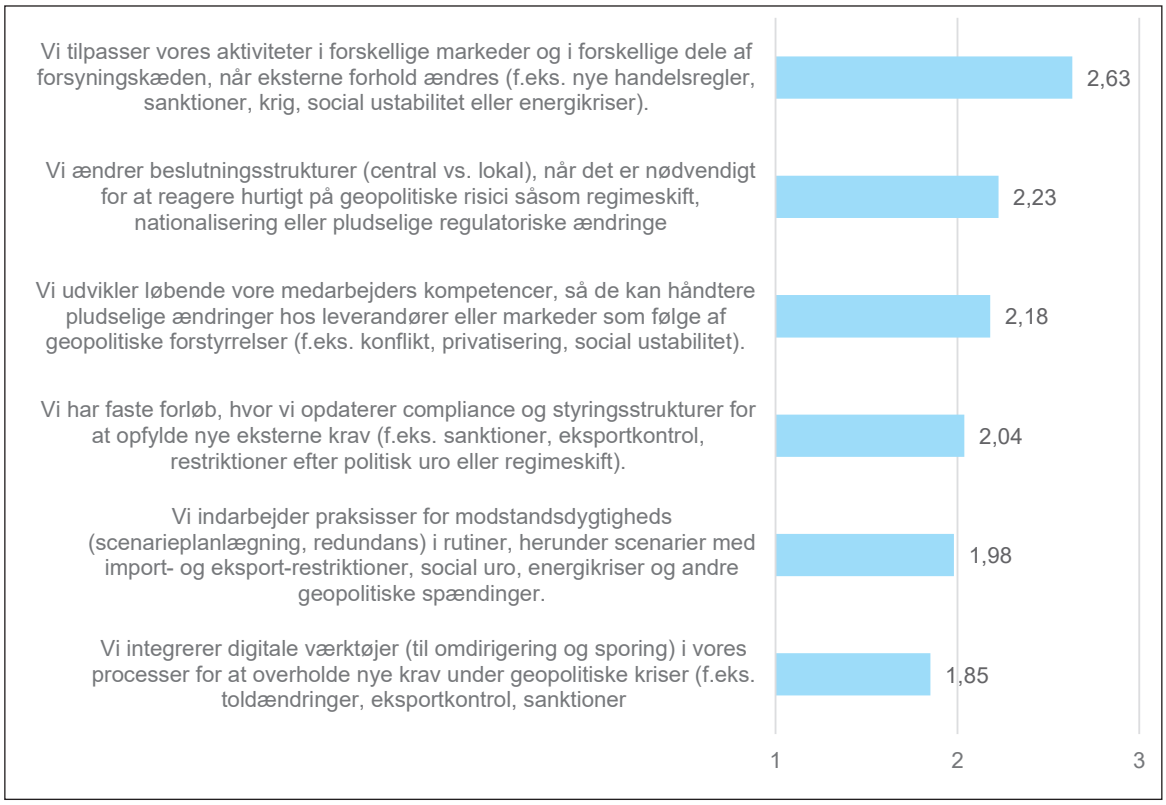
Figur 4.7 Geopolitiske seizing kapabiliteter



Kilde: Stentoft et al. (2026)

Evnen til at omstille driften er også ret begrænset jf. figur 4.8. SMV'erne tilpasser godt nok deres aktiviteter, når der sker ændringer i omgivelserne (2,63), men det sker uden klare og faste procedurer. Samtidig er der udfordringer med at få mere strukturerede tiltag ind i hverdagen. F.eks. er brugen af scenarieplanlægning stadig lav (1,98), og der mangler digitale værktøjer til at følge og overholde nye eksportregler (1,85). Det tyder på, at mange SMV'er stadig arbejder ret uformelt, når det gælder risikostyring, frem for at have klare systemer og processer på plads.

Figur 4.8 Geopolitiske transformation kapabiliteter



Kilde: Stentoft et al. (2026)

5.
Konklusion

Dette treårige forskningsprojekt om Cybersikkerhed og Forretningskontinuitet, der er støttet af Industriens Fond, har haft til formål at styrke opmærksomheden og den konkrete praksis med cybersikkerhed i et forsyningskædeperspektiv. Der er tale om et projekt, der har haft stort fokus på praktisk relevant forskning. Det betyder, at projektet har haft en stærk involvering af virksomheder med henblik på at udvikle værktøjer, der kan bidrage til styrket cybersikkerhed og konkurrenceevne ikke blot for de deltagende virksomheder i projektet, men også for den øvrige industri, der kan tilgå de udviklede værktøjer samt et software til brug for gennemførslen af en supply chain resilience procesmodel, som er tilgængelig på projektets hjemmeside **https://www.cyber-smv.dk.**

Projektet har bestået af forskellige fagpakker som landsdækkende spørgeskemaundersøgelser, udarbejdelse af fremtidsscenarier og afdækning af mentale modeller for forståelsen af cybersikkerhed (det politiske niveau), evaluering af fremtidsscenarierne (industriniveauet), konkret anvendelse af fremtidsscenarierne (virksomhedsniveauet) samt vidensprednin af projektets resultater gennem artikler, podcasts, præsentationer på konferencer og hos erhvervsorganisationer og i de danske erhvervshuse samt præsentationer for det offentlige og private konsulentmarked.

Værktøjer

Der er udviklet en samlet pakke med 30 praktiske og anvendelige værktøjer, der hjælper produktionsvirksomheder med at styrke deres cybersikkerhed – ikke kun teknisk, men også organisatorisk, strategisk og menneskeligt. Værktøjerne er udviklet med udgangspunkt i virkelighedens i SMV'er med:

- Begrænsede ressourcer
- Komplekse forsyningskæder
- Et stigende pres fra både digitale og geopolitiske risici

Værktøjspakken hjælper produktions-SMV'er med at:

- Forstå deres reelle cyberrisici
- Styrke forsyningskæder og kontinuitet
- Kombinere teknologi, organisation og menneskelig adfærd
- Omsætte cybersikkerhed til konkret handling

Ved værktøjer forstås praktisk anvendelige fremgangsmåder i form af skemaer, checklister og processer med konkrete skridt. Til hvert værktøj følger en beskrivelse af formål, deltagere og anvendelse.

Den samlede værktøjspakke består af 30 værktøjer, der fordeler sig som følgende:

1. Supply chain resilience procesmodel
   a. Open-source software til brug for procesmodellens fase 2 og 3
   b. Cyberrelaterede sårbarheder og kapabiliteter

2. Fremtidsscenarier
   a. USA's tilbagetrækning fra Europa
   b. USA-Kina-konfrontation om Taiwan
   c. Klimaforandringer
   d. Økonomisk polarisering
   e. Når AI går amok

3. Cyberrisikostyring i forsyningskæderne
   a. Overblik
   b. Strategi for risikostyring og interessentanalyse
   c. Cybersikkerhedsroller og ansvarsområder
   d. Integration af cybersikkerhed i risikostyring og forbedringsprocesser
   e. Leverandørprioritering
   f. Cybersikkerhed i kontrakter
   g. Cybersecurity due diligence mod nye kunder
   h. Cybersecurity due diligence mod nye leverandører
   i. Cybersikkerhedsregister
   j. Involvering af partnere ved cyberhændelser
   k. Integrering af supply chain cybersikkerhed gennem hele produktlivscyklussen
   l. Tjekliste for ophør af samarbejde

4. Forretningskontinuitet
   a. Business Impact Analyse (BIA)
   b. Risiko- og sårbarhedsanalyse
   c. Leverandørkritikalitetsanalyse
   d. Kontinuitetsplaner
   e. Scenarieplanlægning
   f. Cyberberedskabsplanlægning
   g. Tabletop-øvelser

5. Cyber mindset
   a. Antag kompromittering
   b. Angriberens perspektiv
   c. Lag på lag (Defense in Depth)
   d. Pause-knappen (Slow Down)
   e. Normalisering af fejl (Just Culture)
   f. Signal vs støj (Attention Economics)

6. Cyber resilience
   a. Beskyttelse af intellektuel ejendomsret
   b. Risikoreduktion ved indgåelse af leverandør eller andre tredjeparts-relationer
   c. Sikkerhedspraksisser i forsyningskæden set fra et produkt og tjeneste-livscyklusperspektiv

Spørgeskemaundersøgelser

De to spørgeskemaundersøgelser fra henholdsvis 2024 og 2026 viste, at 20% af respondenterne rapporterede om cyberangreb i 2024-undersøgelsen, mens dette var steget til 25% i 2026-undersøgelsen. Dette vidner om relevansen at et fokus på cybersikkerhed. Sammenligningen mellem 2024- og 2026-undersøgelsen viser også, at virksomhederne generelt har en høj bevidsthed om cybersikkerhed og et relativt solidt internt fundament – særligt i form af god intern integration og styr på tekniske forhold som IT/OT-integration og systemoverblik. Samtidig opleves cybersikkerhed ikke længere som teknisk komplekst, hvilket indikerer en vis modenhed på det operationelle niveau. På trods af denne udvikling er der fortsat væsentlige strukturelle og strategiske udfordringer. Cybersikkerhed er stadig primært forankret internt i virksomhederne, og der stilles kun i begrænset omfang krav til leverandører og kunder. Dette peger på en lav modenhed i håndteringen af cybersikkerhed i værdikæden, hvilket understøttes af det vedvarende lave niveau inden for cybersikker supply chain risk management i begge undersøgelser. Derudover er der kun sket begrænset fremgang i den strategiske forankring. Bestyrelsens engagement er fortsat moderat, og arbejdet drives primært af ledelsen. Samtidig viser resultaterne fra 2026, at virksomhedernes dynamiske kapabiliteter – både i forhold til cybersikkerhed og geopolitik – er lave. Det betyder, at virksomhederne i begrænset grad evner at identificere, udnytte og tilpasse sig nye trusler og muligheder.

Arbejdet med geopolitisk risikostyring er fortsat svagt udviklet, og mange virksomheder mangler et strategisk fokus på eksterne risikofaktorer, herunder regulering og globale spændinger. Samlet set peger resultaterne på et klart udviklingsbehov: Virksomhederne skal i højere grad løfte cybersikkerhed fra et internt, operationelt fokus til et strategisk og forsyningskædeorienteret anliggende. Dette kræver styrket ledelses- og bestyrelsesengagement, øget fokus på leverandører og samarbejdspartnere samt opbygning af dynamiske kapabiliteter, der gør virksomhederne bedre i stand til at håndtere både cyber- og geopolitiske risici på lang sigt.

6.
Perspektivering

En relevant perspektivering af projektet peger på flere oplagte retninger for videre forskning og udvikling. For det første vil det være relevant at undersøge, hvordan cybersikkerhed i forsyningskæder håndteres i andre lande, særligt i økonomier med høj digital modenhed som i Danmark. En sådan komparativ analyse kan afdække, om de udfordringer, danske SMV'er oplever, f.eks. manglende strategisk forankring og lav leverandørintegration, er generelle eller kontekstspecifikke.

Derudover kan der med fordel forskes i andre sektorer end produktionsindustrien f.eks. sundhedssektoren, finanssektoren eller kritisk infrastruktur, hvor konsekvenserne af cyberangreb ofte er endnu mere alvorlige, og hvor reguleringskrav spiller en større rolle. Tilgangen i dette projekt vil kunne gentages i andre sektorer. Dette kan bidrage til at nuancere forståelsen af, hvordan sektorforskelle påvirker cybersikkerhed og forretningskontinuitet.

En anden vigtig retning er at undersøge, hvordan virksomheder konkret kan udvikle deres dynamiske kapabiliteter, særligt i relation til håndtering af nye trusler som kunstig intelligens, geopolitisk ustabilitet og øgede regulatoriske krav (f.eks. NIS 2-direktivet). Her kan fremtidig forskning fokusere på, hvilke ledelsespraksisser og organisatoriske strukturer der understøtter en mere strategisk tilgang til cybersikkerhed.

Endelig kan det være relevant at analysere implementeringen og effekten af de udviklede værktøjer over tid. Det kan bestå i at undersøge, i hvilken grad virksomheder faktisk ændrer adfærd, forbedrer deres sikkerhedsniveauer og opnår øget robusthed i deres forsyningskæder. Her kan studier over tid eller casestudier bidrage med en dybere indsigt i, hvad der virker i praksis, og hvilke barrierer der fortsat eksisterer. Samlet set peger perspektiveringen på, at cybersikkerhed i stigende grad bør forstås som et strategisk og tværorganisatorisk anliggende, der rækker ud over den enkelte virksomhed og kræver både internationalt, sektorielt og organisatorisk fokus.

Projektets tværfaglige natur: Fordele og udfordringer

Dette projekt repræsenterer et komplekst tværfagligt samarbejde, der integrerer ledelse af forsyningskæder og forretningsforståelse (Institut for Erhverv og Bæredygtighed), statskundskab og internationale relationer (Center for War Studies), samt datalogi og cybersikkerhed (Institut for Matematik og Datalogi). Denne konstellation er fundet afgørende, da nutidens sikkerhedsudfordringer i globale forsyningskæder udgør et problem, som er for flerdimensionelt til at kunne løses fyldestgørende inden for rammerne af en enkelt akademisk disciplin.

Fordele ved den tværfaglige integration

Kombinationen af disse tre forskningsfelter skaber unikke synergier, som strukturelt udvider den traditionelle forståelse af virksomhedsdrift og trusselshåndtering.

- Integrationen af statskundskab og ledelse af forsyningskæder og forretningsforståelse gør det muligt at oversætte makropolitiske spændinger til forsyningskædestrategier på virksomhedsniveau. Hvor traditionel forskning om forsyningskæder kan siges at anlægge et mere snævert, markedsdrevet og disciplinært perspektiv, tilføjer statskundskaben en fundamental forståelse for statslig magtanvendelse. Dette gør virksomheder i stand til at navigere i et miljø, der er præget af politisk styrede markedsforstyrrelser frem for blot økonomiske udsving. Statskundskaben giver nye begreber og forståelser, som kan styrke arbejdet med aktørerne i forsyningskæderne mens ledelse af forsyningskæder og forretningsforståelse leverer den konkrete empiri på virksomhedsniveauet.

- Krydsfeltet mellem datalogi og ledelse af forsyningskæder og forretningsforståelse bygger en kritisk bro mellem de tekniske infrastrukturer og de organisatoriske processer i virksomhederne. Datalogien kan levere avancerede løsninger til at sikre de informationsstrømme, som forsyningskæder bygger på, hvilket er et område, som traditionelle supply chain-eksperter ofte mangler tekniske forudsætninger for at adressere mere holistisk. På den anden side kan dette samspil også give input til, hvad der reelt foregår i virkeligheden, så man i højere grad mere målrettet kan fokusere en indsats på det, der er praktisk relevant.

- Samarbejdet mellem statskundskab og datalogi muliggør en markant dybere forståelse af cybertrusler. I dette krydsfelt analyseres cyberangreb ikke udelukkende som tekniske anomalier, der skal patches, men i høj grad som politiske instrumenter og integrerede elementer i en asymmetrisk geopolitisk magtkamp.

Udfordringer og iboende risici ved den tværfaglige integration

På trods af de tværgående fordele er interdisciplinært arbejde fundamentalt udfordrende og bærer betydelige iboende risici, som aktivt skal identificeres og håndteres for at undgå analytiske svagheder.

- Det traditionelle metodiske sammenstød mellem datalogiens formelle, kvantitative systemlogikker og samfundsvidenskabernes systemiske og fortolkende tilgange blev i dette projekt markant minimeret. Dette skyldtes primært, at de involverede dataloger forskningsmæssigt var orienteret mod cybersikkerhedens sociologi og slutbrugernes mentale modeller. Denne fælles interesse for den menneskelige og adfærdsmæssige dimension lettede den epistemologiske integration betydeligt. Dog opstår der i dette delvist overlappende felt en ny analytisk udfordring: at balancere mikro-perspektivet (den enkelte brugers interaktion med sikkerhedssystemer) over for makro-perspektivet (organisationers og staters strategiske ageren i forsyningskæder). Hvis disse niveauer sammenblandes ukritisk, risikerer analysen at miste sin forklaringskraft.
- Uagtet den stærke metodiske konvergens forbliver tidsmæssige og institutionelle rammebetingelser en universel udfordring. **Den fulde syntetisering af viden på tværs af supply chain management, sikkerhedspolitik og human-centric computing kræver en iterativ og tidskrævende oversættelsesproces.** Under faste projektdeadlines lurer risikoen for instrumentel tværfaglighed fortsat, hvor forskningsgrupperne, trods fælles interesser, kan blive presset tilbage i faglige siloer for at sikre rettidige leverancer, hvilket i yderste konsekvens forringer den holistiske værdiskabelse.

Referencer

Barney, J.B. (1991), “Firm resources and sustained competitive advantage”, *Journal of Management*, Vol. 17 No. 1, pp. 99–120.

Christopher, M. & Peck, H. (2004), “Building the resilient supply chain”, *The International Journal of Logistics Management*, Vol. 15 No. 2, pp. 1-13.

Crask, J. (2024), *Business Continuity Management: A Practical Guide to Organization Resilience and ISO 22301*, Kogan Page Ltd., London.

Espersen, I.N., Sjøberg, M. & Kaastrup, J. (2026), *Usynlig fjende - Hackerangreb og hemmelige netværk,* Politikens Forlag, København V.

Europa-Kommissionen (2003), https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX%3A32003H0361, tilgået 12. februar 2026.

Fan, Y. & Stevenson, M. (2018), ”A review of supply chain risk management: definition, theory, and research agenda”, *International Journal of Physical Distribution & Logistics Management*, Vol 48 No. 3, pp. 205-230.

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.

Hiles, A. (2014), *Business Continuity Management: Global Best Practices*, 4. udg. Rothstein Publishing, Brookfield.

Kankam-Boateng, J., Peressotti, M., Stentoft, J., Wickstrøm, K.A., Keating, V.C., Tumchewics, L.A., Schmitt, O., Theussen, A. & Mayer, P. (2026). “It’s Confusing, Insecure, and Messy” – Mapping the Gaps Between Stakeholders’ Cybersecurity Mental Models in the Danish Defence Sector. In: *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems (CHI ‘26),* Barcelona, Spain. ACM. Association for Computing Machinery, New York, Article 76, 1-26.

Mayer, P., Zou, Y., Lowens, B.M., Dyer, H.A., Le, K., Schaub, F. & Aviv, A.J. (2023), “Awareness, intention, (in)action: individuals’ reactions to data breaches”, *ACM Transactions on Computer-Human Interaction*, Vol.30 No.5, pp.1-53.

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.

Narasimhan, R., Nair, A., Griffith, D.A, Arlbjørn, J.S. & Bendoly, E. (2009), “Lock-in situations in supply chains: A social exchange theoretic study of sourcing arrangements in buyer–supplier relationships”, *Journal of Operations Management*, Vol. 27 No. 5, pp. 374-389.

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

NIST (National Institute of Standards and Technology) (2026), https://csrc.nist.rip/glossary/term/cybersecurity?utm_source=chatgpt.com (tilgået 18. marts, 2026).

Peressotti, M., Mayer, P., Kjær, T.B.H. & Stentoft, J. (2024), "SCM Agendaen – Cybersecurity Awareness", podcast publiceret på: https://www.scm.dk/scm-agendaen, tilgået 8. april 2026.

Pettit, T.J., Croxton, K.L. & Fiksel, J. (2013), "Ensuring supply chain resilience: Development and implementation of an assessment tool", *Journal of Business Logistics*, Vol. 34 No. 1, pp. 46-76.

Pettit, T.J., Fiksel, J. & Croxton, K.L. (2010), "Ensuring supply chain resilience: Development of a conceptual framework", *Journal of Business Logistics,* Vol. 31 No. 1, pp. 1-21 (2010).

Schmitt, O., Keating, V., Kjær, T.B.H. & Stentoft, J. (2024), "SCM Agendaen – Geopolitiske spændinger og cybersikkerhed", podcast publiceret på https://www.SCM.dk, tilgået 8. april 2026.

SMVdanmark, https://smvdanmark.dk/analyser/temaanalyser/smver-er-rygraden-i-dansk-erhvervsliv?utm_source=chatgpt.com, tilgået 14. februar 2026.

Stentoft, J. & Mikkelsen, O.S. (2024), Towards supply chain resilience: A structured process approach, *Operations Management Research,* Vol. 17, pp. 1421-1443.

Stentoft, J., Keating, V., Peressotti, M. & Mayer, P. (2025), "Hvordan sikrer vi, at cybersikkerhed bliver taget alvorligt?", kronik, *Erhverv+ Fyn*, 6. februar, p. 16.

Stentoft, J., Mikkelsen, O.S. & Kjær, T.H. (2023), *Supply Chain Resilience i små og mellemstore danske produktionsvirksomheder,* Institut Entreprenørskab og Relationsledelse, Syddansk Universitet.

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

Stentoft, J., Mikkelsen, O.S. & Wickstrøm, K.A. (2025a), " Et svagt led kan lamme os alle – derfor kræver forsyningskæder stærk cybersikkerhed", Kronik, *Erhverv+ Sydjylland*, 9. oktober, p. 20.

Stentoft, J., Mikkelsen, O.S. & Wickstrøm, K.A. (2025b), "Reshoring manufacturing: The influence of industry 4.0, Covid 19, and made in effects", *Operations Management Research*, Vol. 18 No. 1, pp. 353-372.

Stentoft, J., 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, Syddansk Universitet, Center for War Studies, Syddansk Universitet, Institut for Matematik og Datalogi, Syddansk Universitet samt Forsvarsakademiet.

Stentoft, J., Mikkelsen, O.S., Wickstrøm, K.A., Keating, V., Tumchewics, L., Theussen, A., Peressotti, M., Mayer P. & Kankam-Boateng, J. (2026), *Cybersikkerhed i praksis: Indsigter fra danske produktionsvirksomheder*, Institut for Erhverv og Bæredygtighed, Syddansk Universitet, Center for War Studies, Syddansk Universitet, Institut for Matematik og Datalogi, Syddansk Universitet samt Forsvarsakademiet.

Stentoft, J., Peressotti, M. & Mayer, P. (2024), "Derfor skal NETOP DU være ekstra på vagt", kronik, *Business Danmark*, 10. januar.

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, J., Schmitt, O. & Keating, V. (2024), "Supply chain risk management and geopolitics: A new research agenda", artikel præsenteret på den 36. NOFOMA conference organiseret af Swedish Defence University and KTH Royal Institute of Technology, Gøteborg, den 13-14. juni.

Styrelsen for Samfundssikkerhed (2024), https://www.sikkerdigital.dk/virksomhed, tilgået 12. februar 2026.

Styrelsen for Samfundssikkerhed (2025), *Trusselsvurdering: Cybertruslen mod Danmark 2025,* Styrelsen for Samfundssikkerhed, Birkerød.

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

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

Woods, M. (2022), *Risk Management in Organisations: An Integrated Case Study Approach*, Routledge, New York.

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 ansat som 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 fort Erhverv og Bæredygtighed inden for organisationsteori. 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 Syddansk Universitet.

Vincent Keating, ph.d., er lektor ved Center for War Studies, 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, ph.d., er post.doc. ved Center for War Studies, Syddansk Universitet. Louise er ph.d. i krigsstudier fra King's College London. Hendes forskning fokuserer på krig og teknologi, økonomisk krigsførelse og civil-militære relationer. Før hun kom til Syddansk Universitet, 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 by-krigsførelse, og så er hun forfatter til to kommende bøger.

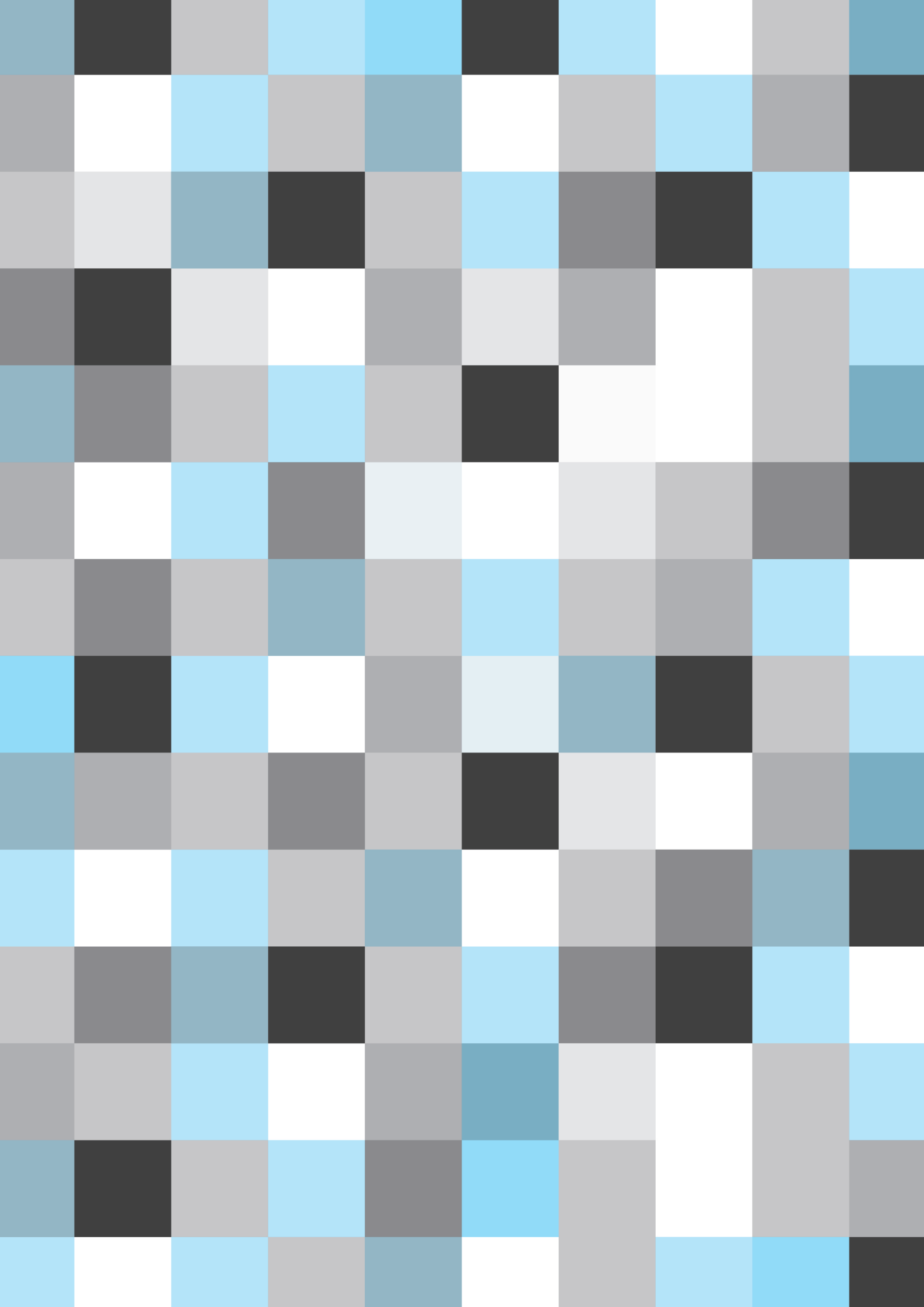
Olivier Schmitt, ph.d. er professor og forskningsleder ved Institut for Militære Operationer på Forsvarsakademiet. Han er også Senior Non-Resident Associate Fellow ved NATO Defence College og Associate ved RAND Europe. Hans forskning fokuserer på europæisk sikkerhed, militær transformation og krigsførelsens skiftende karakter.

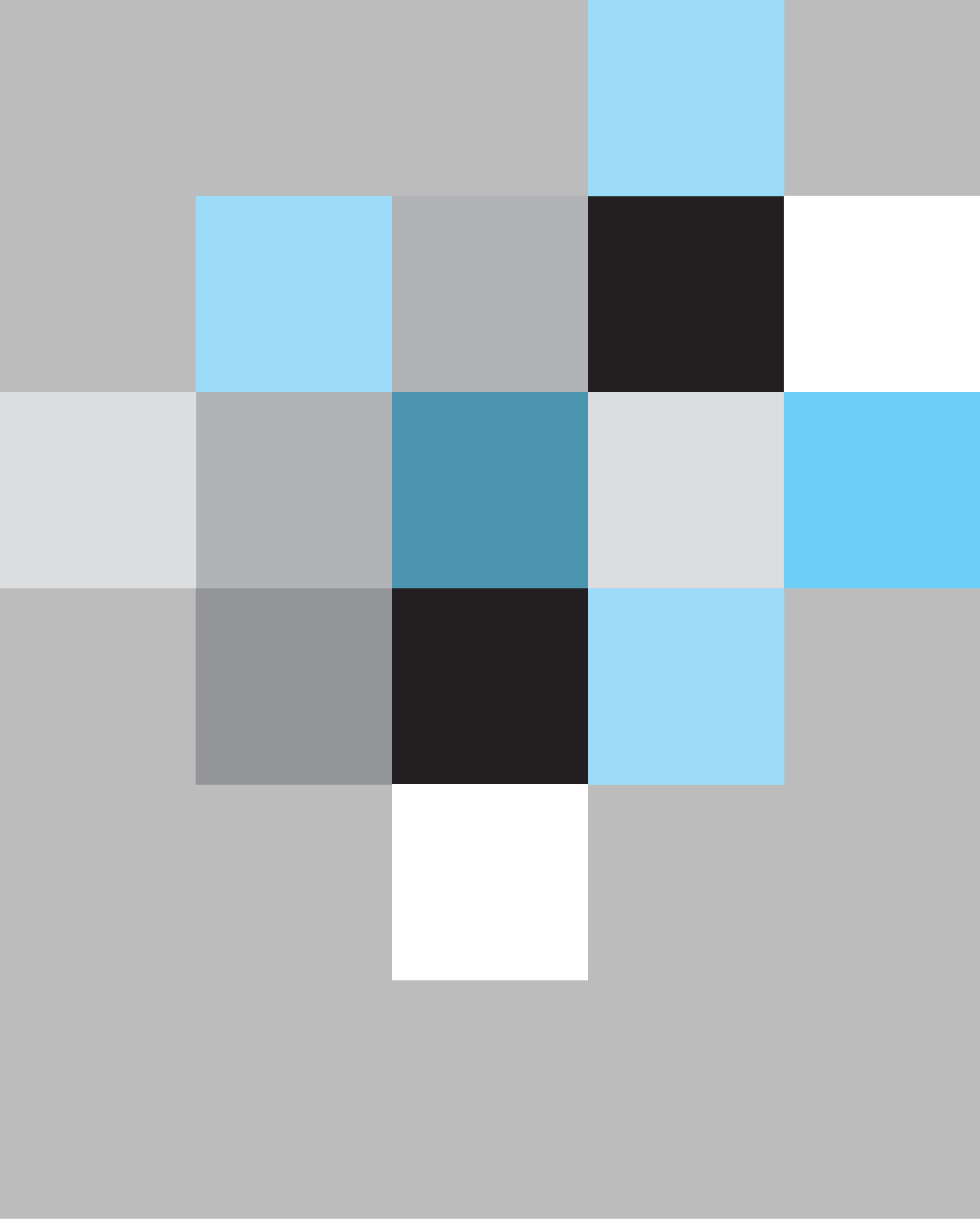
Amelie Theussen, ph.d., er lektor ved Forsvarsakademiet. Hun forsker i sikkerhedssituationen i Arktis og Østersøregionen, dansk og tysk sikkerheds- og forsvarspolitik og spørgsmålet om, hvordan krig forandrer sig, og hvilke konsekvenser det har for politiske og juridiske normer omhandlende magtanvendelse. 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”. Forskningen er uafhængig af, om slutbrugeren af en sikkerhedsløsning er lægmand, administrator eller udvikler. Fokus er 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 er forståelsen af slutbrugeres mentale modeller, dvs., på hvilke måder de tror, cybersikkerhed påvirker dem, samt hvor effektive modforanstaltningerne 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 ’kunstig intelligens’, ’Machine Learning’ og ’Blockchain Technologies’. Hun har ekspertise indenfor ERP Microsoft Dynamics NAV 2018, og så har hun erfaring som Business Analyst, Product Owen og Scrum Master.





SDU INDUSTRIENS FOND FORSVARSAKADEMIET