CYBERSIKKERHED OG FORRETNINGSKONTINUITET

Cybersikkerhed og Forretningskontinuitet i små og mellemstore danske produktionsvirksomheder:

Indsigter fra første iteration med virksomhedsinddragelse

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

September 2025

SDU

INDUSTRIENS FOND

FORSVARSAKADEMIET

Cybersikkerhed og Forretningskontinuitet i små og mellemstore danske produktionsvirksomheder: Indsigter fra første iteration med virksomhedsinddragelse

ISBN: 978-87-85268-87-7

Korrektur og opsætning:
Tina Højrup Kjær, Tekst og Web

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

Projektets hjemmeside er:
www.cyber-smv.dk

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

INDHOLDSFORTEGNELSE

Forord

I en verden, hvor digitalisering og globalisering er blevet uadskillelige drivkræfter for erhvervslivet, står mange små og mellemstore virksomheder (SMV'er) over for en kompleks og ofte overset udfordring: cybersikkerhed i forsyningskæder. Disse virksomheder er ikke blot en del af globale værdikæder; de er også sårbare led i kæden, da cyberangreb kan få alvorlige konsekvenser for både dem selv og deres samarbejdspartnere.

Denne rapport præsenterer en model for Supply Chain Resilience, der understreger vigtigheden af tværorganisatorisk samarbejde for at identificere og mitigere de digitale risici, der truer SMV'ernes position i forsyningskæderne. Modellen fokuserer på at skabe en fælles forståelse af sårbarheder på tværs af funktioner som markeder, salg, distribution, produktion, indkøb, produktudvikling, økonomi og IT. Denne helhedsorienterede tilgang er essentiel for at kunne udvikle scenarier, der adresserer de geopolitiske spændinger og cybertrusler, som i stigende grad påvirker det globale erhvervsliv.

Rapporten bygger på et omfattende datagrundlag indsamlet på tre niveauer: 1) et politisk beslutningsniveau, 2) et industriniveau og 3) et virksomhedsniveau. Dette flerstrengede fundament giver et nuanceret billede af de udfordringer og muligheder, SMV'er står overfor i arbejdet med at styrke deres cybersikkerhed.

Vi takker Industriens Fond for den økonomiske støtte, der har gjort dette projekt muligt, samt de mange deltagere, hvis indsigt og erfaringer har været uvurderlige i udviklingen af rapporten.

Forfatterne – september 2025

1. Introduktion

I en tid præget af hastige teknologiske fremskridt, skiftende politiske landskaber og et stigende antal cybertrusler er forsyningskæders modstandsdygtighed blevet et centralt fokus for organisationer verden over. I takt med den øgede digitalisering har vi paradoksalt nok set, at mens digitalisering og automatisering har forbedret produktiviteten og konkurrenceevnen i forsyningskæder, har de også øget virksomhedernes sårbarhed og eksponering for sikkerhedstrusler. Antallet af cyberangreb på både private og offentlige virksomheder er steget markant i de senere år. I en undersøgelse fra Allianz Risk Barometer 2024, baseret på svar fra 3.069 eksperter i risikostyring fra 92 lande, blev cyberhændelser vurderet som den største globale forretningsrisiko. Seneste forskning inden for Supply Chain Management (SCM) har kastet lys over geopolitiske overvejelser for bedre at forberede sig på risici. Den udbredte stigning i geopolitiske spændinger og cyberkriminalitet har afsløret sårbarheder i globale netværk, hvilket har forstyrret handel, kompromitteret følsomme data og udfordret virksomhedernes evne til at tilpasse sig et stadigt udviklende risikomiljø. I denne sammenhæng er integration af scenarieplanlægning i Supply Chain Risk Management (SCRM) blevet et væsentligt værktøj, der giver organisationer mulighed for at forudse forstyrrelser, udvikle proaktive strategier og opretholde operationel kontinuitet.

Forskning i cybersikkerhed i konteksten af SCM er under hastig udvikling. Aktuel forskning fremhæver behovet for større fokus på cybersikkerhed i konteksten af SMV'er og de måder, hvorpå de kan beskyttes (Stentoft et al., 2025). Det drejer sig om emner som risikostyringsstrategier udløst af cyberangreb på forsyningskæder, forskning på tværs af sektorer og virksomhedsstørrelse, hvordan virksomheder kan tilpasse sig turbulente forretningsmiljøer ved at udvikle kapabiliteter til at identificere risici, opbygge kompetencer og generere nye ressourcer. Eksisterende forskning fremhæver også vigtigheden af intern integration og tværfunktionelt samarbejde for at forbedre cybersikkerhed i SCRM samt etablering af kontinuitetsteams for at forbedre integration og risikostyringskultur (Colicchia, Creazza & Menachof, 2019; Creazza et al., 2022).

I Europa defineres SMV'er som virksomheder med færre end 250 ansatte, med en samlet omsætning, der ikke overstiger 50 millioner EUR, og en årlig balance, der ikke overstiger 43 millioner EUR. SMV'er er interessante af flere grunde. For det første er der langt flere SMV'er end store virksomheder, og derfor er det en betydelig målgruppe for at undersøge gode cybersikkerhedspraksisser. For det andet har SMV'er typisk færre ressourcer og mindre erfa-

ring med at håndtere nye teknologier sammenlignet med store virksomheder. For det tredje er direktørerne ofte involveret i den daglige drift, de tager ofte en reaktiv tilgang til strategi, og de er domineret af et operationelt fokus på bekostning af udviklingsorienterede aktiviteter. For det fjerde spiller SMV'er en kritisk rolle i de fleste forsyningskæder ud over det antal job, de tilbyder, og deres bidrag til den samlede økonomi. For det femte gennemfører SMV'er sjældent cyberrisikovurderinger, og deres IT- og forretningsledelse taler ofte ikke sammen, når det gælder cybersikkerhedsrisikostyring.

SMV'er er særligt sårbare over for cyberangreb på grund af deres begrænsede økonomiske og menneskelige ressourcer sammenlignet med store virksomheder. Derudover mangler mange SMV'er bevidsthed om deres risici og ser ofte cybersikkerhed som et anliggende for store organisationer. Dette gør dem til et attraktivt mål for cyberkriminelle, der udnytter deres svagheder. Cybersikkerhed er afgørende for SMV'er af flere grunde:

- **Beskyttelse af følsomme data**: SMV'er håndterer ofte kundedata, der skal beskyttes mod uautoriseret adgang.

- **Økonomiske konsekvenser**: Cyberangreb kan føre til betydelige økonomiske tab, herunder direkte finansielle tab og omkostninger forbundet med genopretning.

- **Omdømme og kundetillid**: Et angreb kan skade virksomhedens omdømme og føre til tab af kundetillid.

- **Driftsforstyrrelser**: Angreb kan forstyrre virksomhedens drift og føre til nedetid og tab af produktivitet med store økonomiske følger.

SMV'er er en integreret del af globale forsyningskæder som leverandører, underleverandører og partnere (Melnyk et al., 2022). Deres digitale tilstedeværelse gør dem til potentielle indgangspunkter for hackere, der kan kompromittere hele forsyningskæden. Derfor er det afgørende, at SMV'er implementerer robuste cybersikkerhedsforanstaltninger for at beskytte sig selv og deres partnere mod potentielle trusler. SMV'er er derfor ofte det svageste led i de flerledede forsyningskæder, hvilket kan gøre dem til hovedmål for cyberangreb og andre driftsmæssige forstyrrelser. SMV'ernes ejere og ledere finder ofte, at cybersikkerhedsspørgsmål kun er et anliggende for store organisationer, og de finder ligeledes, at investering i cybersikkerhed er spild af penge.

Uddrag af kronik:

Er din virksomhed forberedt på geopolitiske chok?

Den internationale geopolitiske orden er i hastig forandring. Efter den kolde krigs afslutning oplevede verden et "unipolært øjeblik", hvor USA stod som eneste supermagt, og globaliseringen blev drevet frem af vestlig dominans. Dette førte til økonomisk vækst og fattigdomsreduktion i det globale syd, men også til stigende ulighed og svækkelse af middelklassen i Vesten.

Med Ruslands invasion af Ukraine synes denne æra afsluttet. Nye magtcentre som Kina, Rusland, Indien og andre udfordrer den vestlige dominans. Der tegner sig et mere fragmenteret system med et "Globalt Vest", et "Globalt Øst" og et "Globalt Syd", som vælger side alt efter interesser. I modsætning til den kolde krigs klare blokopdeling er nutidens økonomiske og sikkerhedsmæssige relationer tæt sammenflettede. Stater kan både være handelspartnere og sikkerhedstrusler på samme tid, hvilket øger kompleksiteten.

For små og mellemstore virksomheder (SMV'er), der er afhængige af globale forsyningskæder, betyder dette større sårbarhed. Tre typer chok er centrale: efterspørgselschok (f.eks. markedslukning eller eksportkontroller), forsyningschok (mangel på råvarer og komponenter) samt chok i forbindelser (f.eks. cyberangreb eller trusler mod transport).

SMV'er bør derfor arbejde mere strategisk med geopolitik. De kan reducere risici og opbygge resiliens i forsyningskæderne, forberede alternative markeder og organisere sig, så de kan fungere på nedsat kapacitet under kriser. Samtidig er der behov for, at erhvervsorganisationer og klynger styrker SMV'ers bevidsthed og handlekraft på området.

Kilde: Schmitt, Keating & Stentoft (2024). Læs kronikken her.

2. Centrale begreber

2.1 Forretningskontinuitet

Forretningskontinuitet, eller Business Continuity Management (BCM), er en holistisk tilgang til at identificere potentielle trusler mod en organisation og de konsekvenser, disse trusler kan have for forretningsdriften (Hiles, 2014). For SMV'er er BCM særligt vigtigt, da disse ofte opererer med begrænsede ressourcer og ikke har den samme modstandsdygtighed eller redundans som større virksomheder. Det centrale mål med BCM er at sikre, at kritiske forretningsfunktioner kan fortsætte under og efter en forstyrrelse, og at man dermed minimerer nedetid og økonomiske tab (Crask, 2024).

Processen med BCM starter typisk med en risikovurdering og en *impact*-analyse. Dette indebærer at identificere nøgleprocesser, aktiver og afhængigheder samt at vurdere konsekvenserne af forskellige typer forstyrrelser såsom cyberangreb, naturkatastrofer, strømafbrydelser eller sammenbrud i forsyningskæden. Med denne forståelse kan SMV'er prioritere deres mest essentielle funktioner og udvikle strategier for at opretholde eller hurtigt genoptage driften.

En central del af BCM er udarbejdelsen af en forretningskontinuitetsplan (Hiles, 2014). Denne plan beskriver de procedurer og ressourcer, der er nødvendige for at reagere effektivt på hændelser, herunder roller og ansvar, kommunikationsprotokoller, mål for genopretningstid samt backup-løsninger for IT-systemer, data og fysiske faciliteter. Regelmæssig træning, test og opdatering af planen sikrer, at medarbejderne er forberedte, og at organisationen kan tilpasse sig ændrede risici.

For SMV'er handler BCM ikke kun om at beskytte driften. Det handler også om at opbygge tillid hos kunder, partnere og myndigheder. Evnen til at håndtere kriser styrker troværdigheden og kan give en konkurrencefordel. Derudover kræver mange forsyningskæde- og kontraktrelationer nu dokumentation for kontinuitetsplanlægning som en del af due diligence.

Sammenfattende gør BCM det muligt for SMV'er at være proaktive frem for reaktive. Det reducerer effekten af uventede forstyrrelser, understøtter hurtigere genopretning og beskytter både omdømme og økonomisk stabilitet. I et stadig mere usikkert forretningsmiljø er BCM derfor en essentiel del af en bæredygtig forretningsstrategi.

2.2 Cybersecurity Supply Chain Risk Management

Cybersecurity Supply Chain Risk Management (C-SCRM) har fokus på styring af cybersikkerhedsrisici, der opstår gennem virksomheders forsyningskæder. I en globaliseret og digitalt forbundet verden er IT-systemer, hardware, software og tjenester sjældent isolerede. De er afhængige af et komplekst netværk af leverandører, underleverandører og tredjepartsserviceudbydere. Det betyder bl.a., at sårbarheder ét sted i en kæde kan udnyttes til at kompromittere hele forretningssystemet.

I 2024 offentliggjorde den amerikanske organisation National Institute of Standards and Technology (NIST) en opdateret udgave af deres Cybersecurity Framework – NIST CSF 2.0 – som nu også eksplicit inkluderer cybersikkerhed i et SCRM-perspektiv. Formålet med opdateringen er at afspejle et mere moderne cybersikkerhedslandskab, adressere nye trusler og teknologier samt sikre, at frameworket fortsat er relevant og effektivt i arbejdet med at styrke virksomheders overordnede cybersikkerhed (NIST, 2024). Dette fokus på cybersikkerhed i forsyningskæden understøtter anbefalinger i den akademiske litteratur (Colicchia, Creazza & Menachof, 2019; Ghadge et al., 2020).

Ifølge NIST (2024) er C-SCRM en systematisk proces til at håndtere eksponering for cybersikkerhedsrisici gennem hele forsyningskæden og til at udvikle passende responsstrategier, politikker, processer og procedurer. Gennem C-SCRM søger man at reducere risikoen for cyberangreb eller brud, der udspringer af forsyningskæder. C-SCRM er derfor i sin natur dynamisk, da forsyningskæder er komplekse, forbundne og sårbare over for forstyrrelser. C-SCRM fokuserer på at identificere, vurdere og mitigere disse risici gennem hele livscyklussen for produkter og tjenester – fra udvikling og produktion til distribution, integration og drift. Det omfatter både tekniske tiltag som sikkerhedsstandarder, adgangskontrol og softwarevalidering samt organisatoriske tiltag som leverandørkrav, kontraktstyring, revisioner og kontinuerlig overvågning.

Cybertruslerne spænder fra bevidste angreb såsom ondsindet kode indlejret i software til utilsigtede risici som mangelfuld patching (processen med at installere en softwareopdatering) eller svage processer hos underleverandører. Geopolitiske spændinger og organiseret cyberkriminalitet øger kompleksiteten, da angreb kan være strategisk motiverede og ramme kritiske forsyningskæder. C-SCRM kræver et helhedsorienteret tværorganisatorisk samarbejde samt en risikobaseret tilgang, hvor kritiske aktiver prioriteres. Ved at kombinere tekniske løsninger med den rette *governance* og løbende leverandørvurdering kan organisationer reducere sårbarheder og styrke modstandsdygtigheden mod cybertrusler i forsyningskæden.

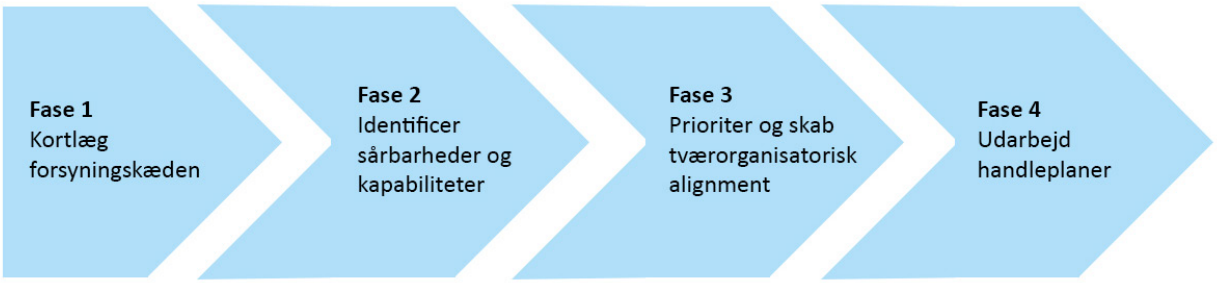
En undersøgelse fra 2024 omkring cybersikkerhed i danske produktions SMV'er viste mangel på strategisk forankring og praktisk implementering af cybersikkerhedsinitiativer med et forsyningskædeperspektiv (Stentoft et al.,

2024). På baggrund af de stigende trusler på området er der derfor et betydeligt arbejde forude med at udvikle og gennemføre strategier, som i højere grad integrerer cybersikkerhed i hele forsyningskæden.

2.3 Procesmodel til Supply Chain Resilience

Stentoft, Mikkelsen & Kjær (2023) har udviklet en procesmodel, der kan hjælpe især SMV'er med systematisk at styrke deres modstandsdygtighed i forsyningskæden. Modellen er udviklet gennem en iterativ forskningsproces baseret på to faser af case-studier i danske virksomheder, og den giver en praktisk ramme for, hvordan organisationer kan arbejde struktureret med Supply Chain Reilience. Procesmodellen består af fire faser (se figur 1).

***Figur 1**: Procesmodel til at skabe Supply Chain Resilience*



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

Den første fase handler om kortlægning af forsyningskæden, hvor virksomhedens netværk af leverandører, kunder, processer og materialestrømme beskrives. Denne kortlægning skaber et fælles organisatorisk overblik og danner grundlag for at forstå kompleksitet og afhængigheder.

I den anden fase arbejder de enkelte funktioner i virksomheden – eksempelvis indkøb, produktion, salg, IT og økonomi – med at identificere sårbarheder og kapabiliteter. Her fremhæves både styrker og svagheder, hvilket giver et nuanceret billede af, hvordan forskellige dele af organisationen bidrager til eller hæmmes af risici i forsyningskæden.

Den tredje fase omfatter prioritering og tværfunktionel tilpasning. Efter at hver funktion har givet sit perspektiv, samles organisationen i workshops eller dialogfora for at skabe fælles forståelse. Denne proces er afgørende, fordi individuelle vurderinger ofte varierer, og diskussionerne muliggør konsensus om, hvilke udfordringer der er mest kritiske, og hvor indsatsen skal koncentreres.

I den fjerde fase udarbejdes konkrete handlingsplaner. Her omsættes indsigterne til praktiske tiltag, der kan reducere sårbarheder, udnytte styrker og op-

bygge organisatorisk modstandskraft. Handlingsplanerne kan spænde fra investeringer i alternative leverandører til forbedring af interne processer eller etablering af beredskabsplaner.

En vigtig pointe i procesmodellen er, at den fremmer tværfunktionel inddragelse og skaber et fælles sprog om resiliens (Stentoft & Mikkelsen, 2024). I de gennemførte cases oplevede medarbejdere, at processen ikke blot identificerede risici, men også styrkede samarbejde og gensidig forståelse på tværs af organisationen. Modellen kan dermed ses som et praktisk redskab, der både øger robustheden over for forstyrrelser og understøtter organisatorisk læring. Samlet set bidrager procesmodellen med en struktureret tilgang, som gør begrebet Supply Chain Resilience håndgribeligt og operationelt. Den skaber en balance mellem analytisk kortlægning, individuel refleksion og fælles prioritering, og den giver virksomheder et konkret grundlag for at udvikle tilpassede strategier til at håndtere fremtidige forstyrrelser.

Uddrag af kronik:

Cybersikkerhed i forsyningskæderne: Har det relevans for SMV'er?

Små og mellemstore virksomheder (SMV'er) spiller en central rolle i samfundet gennem vækst, jobskabelse og innovation. I Danmark findes ca. 300.000 SMV'er, der beskæftiger omkring 1 mio. ansatte. Sammenlignet med større virksomheder har SMV'er færre ressourcer og mindre viden om IT, hvilket gør dem særligt sårbare over for cybertrusler.

Cybersikkerhed handler om at beskytte systemer og data mod uautoriseret adgang, manipulation eller afbrydelser. Angreb som ransomware kan lamme driften, mens datalæk kan udløse bøder og skade omdømme. SMV'er udgør et stigende mål for cyberkriminelle, dels fordi de ofte har svagere sikkerhed, dels fordi de kan bruges som adgangsvej til større virksomheder. Samtidig håndterer de følsomme data, som gør dem til attraktive mål.

En ny undersøgelse blandt danske produktions-SMV'er viser, at hver femte har oplevet cyberangreb (Stentoft et al., 2024). Selvom opmærksomheden på cybersikkerhed generelt er høj, er praksis svag, især i et forsyningskædeperspektiv. Der mangler risikostyring, krav til leverandører og systematisk integration af cybersikkerhed i kontrakter og samarbejder.

Cybertruslerne er stigende, drevet af bl.a. kunstig intelligens, geopolitiske spændinger og hacktivisme. Det understreger behovet for øget træning og forankring af cybersikkerhed i bestyrelser og ledelser. Ressourceknaphed kan være en barriere, men der findes støtteinitiativer som SMV:Digital, D-mærket, erhvervshuse og brancheforeninger. Cybersikkerhed er derfor ikke blot et teknisk spørgsmål, men en strategisk nødvendighed. For SMV'er handler det om at sikre drift, beskytte kunder og styrke resiliens i en stadig mere digital og kompleks verden.

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

2.4 Det systemiske perspektiv – de tre niveauer

Cybersikkerhed i SMV'er er ikke blot et teknisk anliggende. Det er også en kompleks samfundsmæssig problemstilling, hvor forskellige aktører opererer med forskellige mål, forståelser, og rationaler. Med udgangspunkt i et systemisk perspektiv undersøger projektet omfanget og karakteren af divergerende mentale modeller og prioriteringer på tre niveauer: det politiske niveau, industriniveauet og virksomhedsniveauet.

Det politiske niveau er ofte centreret omkring strategisk styring og en reguleringslogik. Dette er forbundet med et fokus på den nationale sikkerhedsarkitektur og derved på trusselsbilleder, kritisk infrastruktur samt overholdelse af internationale forpligtelser. Samtidig er der fokus på at skabe de bedste rammebetingelser for dansk erhvervsliv – herunder SMV'er.

Industriniveauet er ofte kendetegnet ved brancheorganisationers og sektornetværks formidlings-, standardiserings-, og sektorlogik. Her ses cybersikkerhed som både en nødvendighed og en mulighed for at styrke konkurrenceevne og tillid. Ofte er perspektivet her forbundet med standarder, certificeringer (f.eks. D-mærket) samt sektorbaseret videndeling.

På **virksomhedsniveauet**, som her omfatter SMV'er, er de mentale modeller orienteret omkring operationel praksis og forretningslogik. Her ses cybersikkerhed ofte som en omkostning, der skal minimeres, frem for en strategisk investering. Der er således et overordnet fokus på driftssikkerhed og compliance. Mens der er stor opmærksomhed på cybersikkerhed, så er mangel på ressourcer en central barriere for implementering.

Set fra virksomhedsperspektivet kan udfordringen beskrives ud fra teorien om *Dynamic Capabilities* (Teece, 2007; Teece, Pisano & Shuen, 1997), som består af en teoretisk ramme til at forstå virksomheders evne til hurtigt at tilpasse sig skiftende omgivelser. Teorien fokuserer på virksomheders kapabiliteter til løbende at sanse muligheder og trusler (*sensing*), gribe dem gennem strategiske beslutninger og ressourceallokering (*seizing*) samt transformere deres strukturer og processer for at sikre vedvarende tilpasning (*transforming*). Perspektivet er særligt relevant i konteksten af cybersikkerhed, hvor trusselsbilledet er dynamisk, teknologierne komplekse og kravene til organisatorisk omstilling høje.

For SMV'er udgør hver af de tre faser nogle særlige udfordringer, da deres kapabiliteter ofte er begrænsede, og deres evne til at reagere på politiske og teknologiske forandringer varierer betydeligt. Ved at anvende *Dynamic Capabilities* som analytisk ramme kan man belyse risikoen for, at der opstår en afkobling mellem politiske cybersikkerhedsinitiativer og SMV'ers faktiske praksis.

Et af de spændingsfelter, der kan opstå imellem de tre niveauer, er, at regule-

ringslogikken kan kollidere med SMV'ernes daglige realiteter, hvor ressourcer, kompetencer og risikoforståelse er begrænsede. En udfordring, som er forbundet med *sensing*kapabiliteter, er, at der kan være stor variation i den indsigt, som SMV'er har i de trusselsbilleder, som ligger til baggrund for politisk styring og regulering, og at mange SMV'er kan have svært ved at oversætte, hvordan disse trusselsbilleder konkret kan komme til at øve indflydelse på deres forretning.

En anden udfordring relaterer sig mere specifikt til SMV'ers mangel på ressourcer til at eksperimentere med og implementere nye praksisser (manglende *seizing*- og *transforming*kapabiliteter). Dette er specielt en udfordring i tilfælde, hvor politisk regulering ikke ledsages af konkrete værktøjer og støtteordninger, og hvor der er stor risiko for, at regulering bliver opfattet som en bureaukratisk byrde snarere end som støtte. Brancheaktørerne har her en central rolle som brobyggere mellem politik og praksis, men der kan opleves spændinger mellem politiske krav og virksomheders modtagelighed.

Med henblik på at afdække systemiske kilder til cyberusikkerhed undersøger projektet:

1. Hvilke generelle indbyrdes forbundne temaer, der kan identificeres på tværs af de tre niveauer, som kan bidrage til at forklare cybersikkerhedsudfordringer, som danske SMV'er står over for.

2. Hvilke forskelle i mentale modeller, der de tre niveauer imellem udfordrer arbejdet med at styrke cybersikkerheden hos danske SMV'er.

3. Hvilke specifikke sårbarhedsområder, der kan identificeres hos danske SMV'er.

2.5 Det geopolitiske perspektiv

Formålet med dette projekt er at adressere en kritisk sårbarhed i hjertet af den danske økonomi: SMV'ers eksponering for et stadig mere komplekst landskab af geopolitik og cybertrusler. SMV'er udgør rygraden i Danmarks kritiske forsvars- og IT-sektorer, men de mangler ofte ressourcerne til at forudse og afbøde risici, der rækker ud over konventionelle forretningsudfordringer. Mange finder, at cybersikkerhedsproblemer er vanskelige at forstå og kræver store investeringer, der er svære at retfærdiggøre.

Brugen af scenarier (Kahan, 2021, p. 613; Khakee, 1991, p. 460; Kohler, 2021, p. 11) har traditionelt set været et stærkt redskab til at styrke virksomheders parathed til at imødegå fremtidige strategiske udfordringer (Schoemaker, 1993). En central begrænsning ved scenarieplanlægning er dog, at man i høj grad er afhængig af virksomhedens evner og ressourcer til at opfan-

ge signaler fra omgivelserne, f.eks. nye trusler, teknologiske muligheder eller regulatoriske ændringer.

Mange SMV'er har i den forbindelse begrænsede *sensing*kapabiliteter, idet de ikke har dedikerede ressourcer til overvågning af cybertrusler eller forståelse af regulatoriske ændringer. Som konsekvens heraf er det vanskeligt for SMV'er at vurdere de potentielle sårbarheder i deres strategiske planlægning og initiativer for at skabe en højere grad af modstandsdygtighed i deres forsyningskæder.

For at angribe denne problemstilling er det formålet med dette projekt at udfærdige et sæt af scenarier, der tager udgangspunkt i et mere bredt systemisk synsfelt. Nogle scenarier, der tager udgangspunkt i den viden, der ligger på såvel det politiske niveau, industriniveauet og virksomhedsniveauet. Scenarierne har til formål at styrke SMV'ers *sensing*kapabiliteter og derved skabe et bedre fundament for SMV'ernes udvikling af robuste forsyningskæder.

Et centralt element i udviklingen af disse scenarier er integrationen mellem geopolitik, cybersikkerhed og viden om forretningskontinuitet i forsyningskæder. Det er ambitionen, at disse scenarier skal indgå som et værktøj, der kan medvirke til, at deltagende SMV'er kan transformere deres tilgang til cybersikkerhed fra et reaktivt omkostningsorienteret perspektiv til en proaktiv kilde til at skabe konkurrencefordele og modstandsdygtighed. Denne rapport skitserer den praktiske metode, innovative værktøjer og håndgribelige fordele, som projektet leverer i kraft af integrationen med det geopolitisk perspektiv.

3. Metode

3.1 Dataindsamling på tre niveauer

Undersøgelsen, der ligger til grund for denne rapport, anvendte en fokusgruppetilgang for at udforske interessenternes perspektiver på danske SMV'ers cybersikkerhedspraksis og -udfordringer. Undersøgelsen involverede tre forskellige deltagergrupper med henblik på at indfange forskellige synspunkter på tværs af cybersikkerhedsøkosystemet:

1. På det politiske niveau leverede centrale aktører fra blandt andet Forsvarsakademiet, Styrelsen for Samfundssikkerhed, Udenrigsministeriet og Dansk Industri indsigt på højt niveau omkring den nationale cybersikkerhed og det internationale samarbejde om cybersikkerhed.

2. På industriniveauet bidrog brancheeksperter fra brancheorganisationer i forsvarssektoren og konsulenter med deres ekspertise i at identificere tilbagevendende mønstre og validere realistiske trusselsscenarier, som SMV'er kan udsættes for.

3. På virksomhedsniveauet delte virksomhedsledere og funktionsansvarlige i SMV'er deres erfaring med operationelle udfordringer og implementeringsrealiteter.

Den kvalitative analyse fokuserede på at kortlægge mentale modeller på tværs af interessentgrupperne med det formål at identificere områder med uoverensstemmelser, der kan være kilder til cybersikkerhedssårbarheder. Data på det politiske niveau og industriniveauet blev indsamlet i første halvår af 2024 mens, der blev arbejdet på virksomhedsniveauet i anden halvdel af 2024.

3.2 Udvikling af scenarier

Projektets struktur blev designet til at omsætte geopolitisk analyse på højt niveau til konkrete, handlingsrettede strategier for SMV'er gennem de tre nedenstående faser. Denne tilgang sikrer, at de værktøjer og den træning, der tilbydes, ikke blot er teoretiske, men også udformet i samarbejde med og derfor relevante for den nationale sikkerhedsstrategi og industripolitik.

Fase 1: Opbygning af et ekspertdrevet fundament baseret på velkendte scenario-bygning-processer (Spaniol and Rowland, 2018). Først blev relevante eksperter engageret for at etablere et troværdigt fundament for scenarierne. Det udmøntede sig i en fokusgruppeworkshop med repræsentanter fra det danske forsvarsmiljø, herunder bl.a. embedsmænd fra offentlige institutioner som Udenrigsministeriet og Forsvarsakademiet. Det centrale værktøj var scenarieplanlægning efter "Intuitiv Logik"-tilgangen (Wack, 1985), som sigter mod at overvinde kognitive bias for at udforske fremtider, der adskiller sig fra de aktuelle tendenser. Deltagerne afgrænsede først problemet "Forbedring af forretningskontinuiteten for danske SMV'er i forsvarssektoren mod cyber- og forsyningskædetrusler over en femårig tidshorisont". Herefter identificerede de årsagsfaktorer vha. bl.a. en PESTEL-analyse (politisk, økonomisk, socialt, teknologisk, miljømæssigt, juridisk) (Zalengera et al., 2014). Årsagsfaktorerne rangordnede de slutteligt vha. en usikkerheds-/alvorlighedsmatrix for at isolere potentielle fremtidige både meget alvorlige og meget usikre kriser. Den ekspertdrevne proces sikrede, at scenarierne var baseret på realiteter inden for national sikkerhed samtidig med, at der blev fokuseret på udfordrende wildcard-begivenheder, der kunne overrumple uforberedte virksomheder.

Fase 2: Sikring af industriel relevans. For at bygge bro mellem den nationale strategi og den industrielle virkelighed blev scenarierne underkastet en "syretest" i en workshop med brancheeksperter. Disse var repræsentanter fra Styrelsen for Samfundssikkerhed, Dansk Industri, Business Kolding, DigitalLead og store virksomheder som Terma A/S. I denne workshop vurderede deltagerne scenarierne og diskuterede og identificerede de specifikke cybersikkerhedsrelaterede sårbarheder, der kunne opstå for dansk industri, hvis begivenhederne ville indtræffe. Hermed blev de abstrakte geopolitiske trusler fra den første fase omsat til et konkret operationelt sprog om forsyningskæder, markedsadgang og cyberrisiko, hvilket sikrede, at de endelige scenarier ville give mening for SMV'erne.

Fase 3: Levering af direkte værdi til SMV'erne. Her deltog SMV'erne i en række Strategic Foresight workshops. På workshopsene blev temas fra virksomhederne introduceret til konceptet bag scenarierne og inviteret til at vælge det, de fandt mest relevant for deres forretning. Målet var ikke at "løse" det fiktive problem, men at bruge historien som et struktureret værktøj til refleksion over deres egen virksomheds sårbarheder og strategier for modstandsdygtighed, vejledt af et sæt fokuserende spørgsmål. Denne proces blev understøttet af projektets firefasede procesmodel for Supply Chain Resilience, hvilket er et praktisk værktøj, der guider SMV'er til at kortlægge deres forsyningskæder, identificere sårbarheder, skabe organisatorisk sammenhæng og udvikle konkrete handlingsplaner. Arbejdet med procesmodellen færdiggjorde SMV'erne inden workshoppen i fase 3, så alle var enige om deres egen virksomheds udfordringer før de engagerede sig i de risici, der var forbundet med scenarierne. Kombinationen af reflekterende scenarieengagement og en struktureret procesmodel gjorde det muligt for SMV'erne aktivt at opbygge deres evne til at forudse og forberede sig på fremtidige forstyrrelser.

Uddrag af kronik:

Har du kompetencerne til at se ind i fremtiden?

Efter årtier med politisk stabilitet og frihandel har verden de seneste år oplevet markante forandringer. Coronapandemien afslørede skrøbeligheder i globale forsyningskæder, Ruslands invasion af Ukraine har påvirket fødevare- og energiforsyning, og konflikter i Mellemøsten har forstyrret international skibsfart. Samtidig forventes en mere protektionistisk amerikansk handelspolitik og en eskalerende konflikt med Kina, hvilket øger usikkerheden for danske virksomheder.

I dette landskab er cybersikkerhed blevet en kritisk sårbarhed. Hvor cyberangreb tidligere primært rettede sig mod offentlige institutioner, rammer de nu i stigende grad private virksomheder – også SMV'er. Disse udgør ofte en del af større forsyningskæder og kan derfor fungere som indgangspunkter til større mål. Truslerne forstærkes af nye teknologier som kunstig intelligens samt sofistikerede manipulationsteknikker.

Her bliver Strategic Foresight afgørende. Metoden, der længe er brugt politisk og militært, hjælper organisationer med at udforske og forberede sig på mulige fremtidsscenarier. Ved hjælp af værktøjer som prognoser, backcasting, horisontscanning, megatrends-analyser og scenariearbejde kan virksomheder identificere tidlige tegn på trusler og muligheder. For SMV'er handler det om at opbygge evner til at se fremad, skabe robuste strategier og integrere cybersikkerhed i risikostyringen.

Da mange SMV'er er begrænset af ressourcer, bliver støtte fra erhvervsorganisationer, konsulenter og uddannelsesudbydere vigtig. Et øget fokus på Strategic Foresight kan styrke deres kompetencer til at forstå og håndtere fremtidens risici og derved øge modstandsdygtigheden mod både geopolitiske og digitale trusler.

Kilde: Tumchewics et al. (2024). Læs kronikken her.

De udviklede scenarier indeholder citater, der er anonymiseret idet de indgår i den danske kritiske infrastruktur.

4. Analyse

4.1 Generelle temaer

Fokusgruppediskussionerne afdækkede adskillige indbyrdes forbundne temaer, der kan bidrage til at forklare de cybersikkerhedsudfordringer, som danske SMV'er står over for:

- Et almindeligt observeret mønster var en passiv holdning til sikkerhed, hvor investeringer i cybersikkerhed mere var en følge af hændelser snarere end foregribelse af dem, hvilket potentielt efterlod organisationer sårbare i fasen før hændelsen.

- Deltagerne bemærkede også en kulturel spænding mellem Danmarks samfundsnormer med høj tillid og indførelsen af Zero Trust-cybersikkerhedsmodeller (i en Zero Trust-tilgang antages det ved hver interaktion, at brugeren ikke er til at stole på, før der er foretaget en kontrol), hvilket kan påvirke organisationers holdninger til risici.

- Ressourcebegrænsninger blev ofte nævnt, hvor mange SMV'er blev opfattet som værende i mangel af kapacitet og ressourcer til at håndtere omfanget og kompleksiteten af nye trusler.

- Territoriale forskelle blev også fremhævet. Især i forhold til Grønland og Færøerne, hvor geopolitiske og infrastrukturelle forskelle kan bidrage til ujævne sikkerhedskapaciteter.

- Forsyningskæder viste sig at være et væsentligt problemområde, hvor begrænset leverandørdiversitet og verifikationspraksis blev set som en øget eksponering for cybertrusler.

- Derudover blev tvetydighed omkring fordelingen af cybersikkerhedsansvar mellem offentlige og private aktører set som en barriere for effektiv koordinering. Nogle deltagere pegede på en driftsmæssig skrøbelighed som følge af afhængigheder af enkeltleverandører eller nøglepersonale.

- Og selvom Danmarks avancerede digitalisering blev anerkendt som en national styrke, blev den også set som en kilde til nye sårbarheder, der kan overgå eksisterende sikkerhedsforanstaltninger.

Samlet set tyder observationerne på, at cybersikkerhedsrisici formes af en kombination af kulturelle, strukturelle og operationelle faktorer. Der vil derfor kunne drages fordel af mere skræddersyede, kontekstfølsomme reaktioner.

4.2 Forskelle i mentale modeller

Analysen viser bemærkelsesværdige forskelle i, hvordan forskellige interessentgrupper konceptualiserer og griber cybersikkerhed an:

- **Politikere** beskrev ofte en mangel på sammenhæng mellem nationale strategier og deres implementering på SMV-niveau, især med hensyn til risikoopfattelse og ressourceallokering.

- **Brancheeksperter** understregede udfordringer relateret til koordinering, begrænsede investeringer i forskning og udvikling samt vanskeligheder med at tilpasse nationale og internationale standarder. De pegede også på vedvarende problemer med at håndtere både menneskelige og teknologiske sårbarheder på tværs af sektorer.

- **SMV-repræsentanter** havde en tendens til at indtage en reaktiv holdning og reagerede ofte på eksternt pres såsom lovgivningsmæssige krav eller kundernes forventninger. Denne gruppe rapporterede om kapacitetsmangler inden for områder som hændelsesrespons, risikovurdering i forsyningskæden og integration af cybersikkerhed i bredere planlægning af forretningskontinuitet.

Disse divergerende perspektiver tyder på, at forskelle i mentale modeller kan bidrage til fragmenterede indsatser og ujævne niveauer af beredskab på tværs af cybersikkerhedslandskabet.

4.3 Sårbarhedsområder

Seks tematiske områder af opfattede sårbarheder blev identificeret:

- **Teknologiske**: Deltagerne henviste ofte til lagdeling af moderne systemer på ældre infrastruktur, hvilket kan introducere systemiske risici og enkeltstående fejlpunkter.

- **Forsyningskæde**: Afhængighed af et lille antal IT-leverandører blev set som en potentiel koncentrationsrisiko, især hvor verifikationsprocesserne er svage.

- **Operationelle**: Cybersikkerhed blev ofte beskrevet som perifer i forhold til kerneforretningsfunktioner med begrænset scenarieplanlægning og fragmenteret samarbejde.

- **Menneskelige faktorer**: Mangel på kvalificerede medarbejdere og lav organisatorisk bevidsthed var tilbagevendende bekymringer sammen med observationer om ledelsens manglende digitale færdigheder.

- **Geopolitisk eksponering**: Danmarks internationale alliancer (f.eks. NATO, Ukraine mv.) blev af nogle opfattet som en øget synlighed over for statsstøttede trusler. Der blev også rejst bekymringer om den digitale infrastrukturs modstandsdygtighed i Grønland og Færøerne.

- **Regulering**: Kompleksiteten og fragmenteringen af det regulatoriske landskab blev set som barrierer for effektiv implementering, især i forsvarssektoren.

4.4 Scenarierne: Konkretisering af abstrakte trusler

Et centralt resultat af projektet er et sæt af fem detaljerede narrative scenarier, der opstod fra projektets første iteration. Disse scenarier er ikke en række forudsigelser om den geopolitiske fremtid, men udformede historier på 1.000 ord, der er designet som "narrative provokationer", der udfordrer antagelser og gør abstrakte risici håndgribelige. Ved at placere en relaterbar dansk hovedperson i centrum for hver krise forbinder scenarierne komplekse globale begivenheder med en virksomheds daglige drift.

4.4.1 Scenarie 1: USA's tilbagetrækning fra Europa

Dette scenarie forestiller sig virkeligheden efter en hypotetisk sejr i 2024 for præsident Donald Trump, der implementerer den isolationistiske politik fra "Projekt 2025". USA reducerer dramatisk sit bidrag til europæisk sikkerhed, trækker tropper tilbage til Indo-Stillehavsområdet og skaber et lederskabsvakuum i NATO. Den umiddelbare forretningsmæssige indvirkning er en ny universel handelstold, der rammer dansk eksport hårdt, især inden for medicinalindustrien og præcisionsbearbejdningsindustrien. Som reaktion herpå er europæiske nationer, herunder Danmark, tvunget til at øge forsvarsudgifterne til 3% af BNP og foretage omfattende nedskæringer i det sociale velfærdssystem for at finansiere det. For SMV'er bliver miljøet farligt; uden den amerikanske sikkerhedsparaply står de nordiske og baltiske lande over for en konstant byge af cyberangreb fra Rusland. Angreb, der er rettet mod alt fra banksystemer til forsvarsproduktionsvirksomheder.

4.4.2 Scenarie 2: Konfrontation mellem USA og Kina om Taiwan

Dette scenarie illustrerer, hvordan et fjernt geopolitisk brændpunkt kan ud-

løse katastrofale forstyrrelser i forsyningskæden. Historien begynder med et mindre maritimt sammenstød nær Spratlyøerne, der involverer Filippinerne og Kina, som hurtigt eskalerer. Kina indfører en fuldstændig militærblokade af Taiwan, som er et globalt knudepunkt for produktion. For hovedpersonen, Anna, en senior designingeniør hos en dansk medicinsk robotvirksomhed, er virkningen direkte: Hendes firma kan ikke længere få de nødvendige computerchips fra Taiwan, hvilket stopper al produktion. I hendes desperate søgen efter alternative leverandører bliver indkøbsteamet mål for et sofistikeret phishing-angreb forklædt som en e-mail fra en ny leverandør. Angrebet fører til en ugelang driftsnedlukning og tab af en større kontrakt. Scenariet demonstrerer levende, hvordan geopolitisk konflikt øjeblikkeligt kan afbryde kritiske forsyningslinjer og skabe et modent miljø for cyberkriminalitet rettet mod sårbare virksomheder.

4.4.3 Scenarie 3: Klimaændringer

Denne fortælling udforsker de følgerisici, der er ved miljøkriser set gennem hovedpersonen Hans' øjne. Hans er fjerdegenerations dansk svineavler. Fortællingen bevæger sig ud over abstrakt miljøbevidsthed og beskriver konkrete forretningsmæssige konsekvenser. Vådere vejr fra en skiftende jetstrøm fører til flere dyresygdomme og højere dyrlægeregninger. Ekstreme vejrbegivenheder, som f.eks. oversvømmelser på den tyske autobahn, ødelægger hele forsendelser af Hans' produkter. Forsikringsselskaber begynder at nægte at dække skader fra sådanne "almindelige" klimarelaterede begivenheder. Det mest afgørende led er cyberdimensionen: For at opfylde emissionsmålene for CO2 stopper EU beregningsintensiv kunstig intelligens, herunder programmer, der bruges til at opdage cyberangreb, hvilket gør virksomheder mere sårbare. Cyberkriminelle udnytter ustabiliteten efter større klimabegivenheder, og Hans' foderleverandør kommer til at lide under et ransomware-angreb. Angrebet medfører en suspendering af Hans' ordre, og det tvinger ham til at finde en dyr alternativ leverandør med et øjebliks varsel.

4.4.4 Scenarie 4: Økonomisk polarisering

Dette scenarie fokuserer på socioøkonomiske tendenser og deres sikkerhedsmæssige konsekvenser. Hovedpersonen, Christina, er marketingchef hos Danstol, en mellemklasse møbelvirksomhed. Virksomhedens kundebase, den europæiske middelklasse, skrumper. Den er presset af skatter og økonomisk usikkerhed, hvilket får salget hos Danstol til at styrtdykke. Denne udbredte økonomiske uro giver næring til politisk ekstremisme. Den direkte cybertrussel opstår ud fra, at med høj arbejdsløshed og vrede i sanktionerede økonomier som Rusland, tyr mange teknologisk dygtige unge mennesker til cyberkriminalitet for profit. De rekrutteres af organiserede bander til at iværksætte ransomware-angreb på vestlige virksomheder. Christinas egen virksomhed oplevede dette, da deres leverandør af skruer og bolte blev ramt af et sådant angreb, hvilket stoppede Danstols produktion i tre uger og forårsagede et betydeligt økonomisk tab.

4.4.5 Scenarie 5: AI ude af kontrol

Denne historie fremhæver farerne ved uforsigtig teknologiadoption. Peter, lederen af en dansk stempelproducent, Stempelkraft, der udvikler specialkomponenter til forsvarssektoren, beslutter sig for at implementere et generisk AI-aktiveret softwaresystem til at håndtere lagerstyring. Han vælger det system, der er baseret på branchens omdømme og brugervenlighed. Efter et års problemfri brug og bortskaffelse af redundante lagerstyringssystemer lider lagerstyringssystemets eksterne server under et tre uger langt ransomware-angreb, og Stempelkraft kan ikke få adgang til sine lageroplysninger. Virksomheden er tvunget til at sætte produktionen på pause. Dette er dog blot et symptom på en langt mere alvorlig underliggende krise, da det medfører økonomiske vanskeligheder og omdømmeskade.

Uddrag af kronik:

Det bugner med tilbud om cybersikkerhed - hvordan griber vi dem og sikrer fremdrift?

Cybersikkerhed er blevet et forretningskritisk område, der rækker langt ud over IT-afdelingen. Cyberangreb rammer både store og små virksomheder, og når produktionen stopper, eller kunder mister tilliden, kan det true virksomhedens overlevelse. Særligt SMV'er er udsatte, da de ofte mangler ressourcer og fungerer som leverandører i større værdikæder. Derfor skal cybersikkerhed ses som en investering i robusthed – på linje med en brandforsikring – og ikke blot som en omkostning.

Industriens Fond har sat fokus på området gennem projekter som Cybersikkerhed og Forretningskontinuitet og Cyber Safe Robotics, hvor løsninger udvikles i tæt samarbejde med virksomhederne. Alligevel viser undersøgelser, at SMV'er har svært ved at mobilisere ressourcer og implementere løsninger. De scorer relativt lavt på evnen til at udnytte muligheder (Seizing) og til at omstille sig (Transforming), selvom interessen for cybersikkerhed er til stede.

For at styrke SMV'ernes digitale modstandsdygtighed er der behov for støtte i form af økonomiske incitamenter, teknisk rådgivning og praktisk træning. Erhvervsfremmeaktører, brancheorganisationer og GTS-institutter spiller en central rolle i at bringe viden helt ud på fabriksgulvet og i bestyrelseslokalet. Målet er at gøre cybersikkerhed til en integreret del af forretningsudviklingen og til et konkurrenceparameter i en tid præget af geopolitisk uro og stigende trusselsbillede. Cybersikkerhed er i sidste ende en forudsætning for at drive virksomhed i en digital tidsalder. Det kræver ledelsesmæssig opbakning, fælles handling og en erkendelse af, at robusthed og tillid er lige så vigtige som effektiv produktion.

Kilde: Stentoft & Kjær (2025). Læs kronikken her.

4.5 Forventede fordele og praktisk effekt for danske SMV'er

Projektet er designet til at levere varige, praktiske fordele, der forbedrer konkurrenceevnen og sikkerheden for de deltagende SMV'er og dermed den bredere danske industribase. SMV'ernes engagement i scenarierne giver følgende fordele:

- **Forbedret specifik risikobevidsthed**: Deltagerne går ud over generiske advarsler om cybersikkerhed for at forstå, hvordan specifikke geopolitiske begivenheder kan skabe direkte trusler. Scenarierne gør forbindelserne mellem geopolitik og cyberrisk levende og uforglemmelige. Som en deltager sagde, "påpegede scenarierne alle de trusler, vi tænker på i dagligdagen, og de blev meget mere levende og skabte en bevidsthed."

- **Proaktiv strategisk planlægning**: Ved at engagere sig i scenarierne stresstester SMV'erne deres operationer. Workshopdiskussioner afslørede en klar forståelse af behovet for at skifte fra "just-in-time"-effektivitet til "just-in-case"-modstandsdygtighed, hvor nogle endda opfandt udtrykket "just-with-friends" for at beskrive en fremtid, hvor handel dikteres af geopolitiske alliancer.

- **Forbedrede interne processer**: Projektet fremhævede betydelige interne sårbarheder. SMV'erne anerkendte deres tendens til at indføre nye teknologier ved at følge større virksomheders eksempel. Ofte uden uafhængig sikkerhedsverifikation. Workshops'ene ansporede til samtaler om behovet for bedre due diligence hos tredjepartsleverandører og risikoen for at miste afgørende tavs viden inden for deres organisationer, efterhånden som de i stigende grad anvender AI-løsninger.

- **Et skift i tankegang for at opnå konkurrencefordel**: Scenarierne omtaler fundamentalt ikke cybersikkerhed som en IT-omkostning, men som en afgørende komponent i forretningsstrategien. I et miljø, hvor angreb i forsyningskæden er almindelige, bliver det at kunne demonstrere robust sikkerheds- og modstandsdygtighedsplanlægning en stærk konkurrencefordel, hvilket gør en SMV til en mere attraktiv og pålidelig partner for større virksomheder og offentlige kontrakter.

- **Adgang til holdbare værktøjer og viden**: Projektets resultater er designet til at holde længe. De fem scenarier og tilhørende træningsmaterialer er dokumenteret og tilgængelige for virksomheder til fremtidige interne strategisessioner. Derudover udvikles en webapplikation til at automatisere den firefasede procesmodel, og dens kode vil blive udgivet open source, hvilket muliggør bred implementering og fortsat udvikling af tredjeparter.

5. Konklusion

Verden er fundamentalt forandret for danske SMV'er. De engang adskilte domæner geopolitik, forsyningskædestyring og cybersikkerhed er ved at konvergere, og de afslører et sammenkoblet trusselslandskab. Som denne rapport har beskrevet, er SMV'er, der udgør rygraden i den danske økonomi, unikt udsatte for denne nye virkelighed. De mangler dog ofte ressourcerne til at omsætte abstrakte globale risici til konkret forretningsstrategi. Arbejdet, der er beskrevet i denne rapport, er designet til at bygge bro over dette kritiske hul og omdanne overordnede trusselsvurderinger til praktisk, handlingsrettet information for virksomhedslederne.

Tilgangen er forankret i en unik analyse på flere niveauer, der integrerede trategiske perspektiver fra nationale politikere og brancheeksperter med SMV'ernes egne operationelle realiteter. Det sikrede, at de genererede indsigter ikke kun er teoretiske, men også baseret SMV'ernes oplevede erfaringer.

Kernen i denne indsats var udviklingen af fem detaljerede narrative scenarier. Disse var ikke udformet som forudsigelser, men som "narrative provokationer" eller strategiske sparringspartnere, der får fjerne geopolitiske brændpunkter som f.eks. en amerikansk tilbagetrækning fra Europa eller en konflikt om Taiwan til at føles umiddelbare og håndgribelige. Ved at placere en relaterbar dansk hovedperson i centrum af hver krise, fremtvang scenarierne en praktisk og presserende refleksion over specifikke sårbarheder. Som en deltager bemærkede, "gjorde denne metode truslerne meget mere levende og skabte en bevidsthed" om risici, der tidligere blot var overskrifter.

Et vigtigt udgangspunkt for at kunne arbejde effektivt med scenarierne er, at man i den enkelte virksomhed har arbejdet tværfagligt med etableringen af et overblik over virksomhedens forsyningskæde. Med det menes, at man har vurderet nuværende sårbarheder og kapabiliteter samt udarbejdet en strategisk plan for vedligeholdelse og udbygning af forsyningskædens robusthed. Her er virksomhedernes arbejde med procesmodellen et vigtigt element i forberedelsen til arbejdet med scenarierne. Scenarierne fungerer efterfølgende som en trykprøve på den strategiske handlingsplan.

Fordelene ved denne proces for de deltagende virksomheder er klare, håndgribelige og varige:

- **Fra abstrakt trussel til specifik indsigt**: Arbejdet bevægede virksomhederne ud over generiske advarsler om cyberkriminalitet til en specifik for-

ståelse af, hvordan en bestemt geopolitisk begivenhed direkte kan udløse en forsyningskædefejl eller skabe de præcise betingelser for et målrettede cyberangreb på deres operationer.

- **Opbygning af proaktiv krisehåndtering**: At engagere sig i plausible fremtider gjorde det muligt for virksomheder at stressteste deres egne operationer og strategier. Det udløste ny strategisk tænkning, hvor deltagerne reflekterede over en mulig fremtid, hvor f.eks. kommercielle partnerskaber er stærkt dikteret af geopolitiske alliancer.

- **Fremme af intern tilpasning og modstandsdygtighed**: Processen afslørede kritiske interne sårbarheder som tendensen til at indføre nye teknologier uden uafhængig sikkerhedsverifikation eller risikoen for at miste tavs institutionel viden. Endnu vigtigere var det, at det brød interne siloer ned, hvilket tvang essentielle samtaler mellem ledelse, IT, indkøb og salg til at skabe en fælles, tværfunktionel forståelse af risici og en mere integreret tilgang til forretningskontinuitet.

- **Omformulering af modstandsdygtighed som en konkurrencefordel**: Det måske vigtigste resultat er den grundlæggende omformulering af cybersikkerhed og modstandsdygtighed i forsyningskæden. De ses ikke længere som byrdefulde omkostningscentre, men som en kernekomponent i forretningsstrategien og en stærk konkurrencefordel. I en tid, hvor cyberangreb i forsyningskæden er udbredte, gør evnen til at demonstrere robust sikkerheds- og beredskabsplanlægning en SMV til en mere attraktiv, troværdig og pålidelig partner for store kunder og kritiske offentlige kontrakter.

Værdien leveret af dette arbejde er designet til at være holdbar gennem oprettelsen af et sæt praktiske værktøjer, herunder de fem detaljerede scenarier og den firefasede procesmodel for modstandsdygtighed i forsyningskæden, som virksomheder kan bruge i fremtidige interne strategimøder. I sidste ende giver det arbejde, der er beskrevet i denne rapport, danske SMV'er både en ny linse til at forstå verden og et praktisk værktøjssæt til at navigere i den. Ved at anvende en proaktiv og integreret tilgang til risiko kan SMV'er ikke blot beskytte deres drift mod et komplekst netværk af trusler, de kan også transformere deres virksomheder til en tid med hidtil uset usikkerhed og dermed udnytte de nødvendige muligheder for at opbygge mere robuste, agile og konkurrencedygtige virksomheder.

6. Litteraturliste

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

Crask, J. (2024), *Business Continuity Management: A Practical Guide to Organizational Resilience and ISP 22301*, 2. udg., KoganPage, London.

Creazza, A., Colicchia, C., Spiezia, S. & Dallari, F. (2022), "Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era", *Supply Chain Management: An International Journal*, Vol. 27 No. 1, pp. 30-53.

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

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

Kahan J.P. (2021), "Bouncecasting: A seminar gaming approach to foresight", *Foresight*, Vol. 23 No. 6, pp. 613–627.

Khakee, A. (1991), "Scenario construction for urban planning", *Omega*, Vol. 19 No. 5, pp. 459-469.

Kohler, K. (2021), *Strategic Foresight: Knowledge, Tools, and Methods for the Future*, CSS Risk and Resilience Reports, ETH Library, https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/505468/RR-Reports-2021-StrategicForesight.pdf?sequence=2&isAllowed=y (Accessed, January 5, 2025).

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.

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

Schmitt, O., Keating, V. & Stentoft, J. (2024), "Er din virksomhed forberedt på geopolitiske chok?", Kronik i *Erhverv+*, 22. februar. Læs kronikken her.

Schoemaker, P.J. (1993), "Multiple scenario development: Its conceptual and behavioral foundation", *Strategic management journal*, Vol. 14 No. 3, pp. 193-213.

Spaniol, M.J. & Rowland, N.J. (2018), "The scenario planning paradox", *Futures*, Vol. 95, pp. 33-43.

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

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*, Erhverv og Bæredygtighed, SDU, Center for War Studies, SDU, Institut for Matematik og Datalogi, SDU samt Forsvarsakademiet. Læs rapporten her.

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

Stentoft, J. & Kjær, T.H. (2025), "Det bugner med tilbud om cybersikkerhed – hvordan griber vi dem og sikrer fremdrift?", Kronik i *Erhverv+*, 29. maj. Læs kronikken her.

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*, EarlyCite.

Stentoft, J., Peressotti, M. & Mayer, P. (2024), "Cybersikkerhed i forsyningskæderne: Har det relevans for SMV'er?", Kronik i *Erhverv+*, 22. august. Læs kronikken her.

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.

Tumchewics, L., Theussen, A., Kankam-Boateng, J. & Stentoft, J. (2024), "Har du kompetencerne til at se ind i fremtiden?", Kronik i *Erhverv+*, 28. november. Læs kronikken her.

Wack, P. (1985), "Scenarios: Uncharted waters ahead", *Harvard Business Review*, Vol. 63 No. 5, pp. 73–89.

Zalengera, C., Blanchard, R.E., Eames, P.C., Juma, A.M., Chitawo, M.L. & Gondwe, K.T. (2014), "Overview of the Malawi energy situation and a PESTLE analysis for sustainable development of renewable energy", *Renewable and Sustainable Energy Reviews*, Vol. 38, pp. 335-347.

Industriens Fonds fokus på cybersikkerhed

Nærværende projekt "Cybersikkerhed og Forretningskontinuitet" (www.cyber-smv.dk) er del af en samlet portefølje i Industriens Fonds Action:Call med fokus på cybersikkerhed i værdikæder (læs her).

De øvrige fire projekter i porteføljen er:

Styrket Cybersecurity for SMV'er

Formål: At give danske SMV'er og deres værdikæder mulighed for at styrke deres digitale sikkerhed.

Leverance: Et CS Tool, som er et simpelt modenhedsværktøj for SMV'er tænkt som et dialogisk og handlingsorienteret værktøj målrettet SMV'er. Link til værktøjet: eh.enablor.dk

Projektejer/-leder: Erhvervshus Midtjylland/Dorte Damgaard Hansen

Projekthjemmeside: https://erhvervshusmidtjylland.dk/styrket-cybersikkerhed-for-smver

Cybersikre fødevareværdikæder

Formål: At styrke danske fødevarevirksomheders cybersikkerhed og konkurrenceevne.

Leverance: En webplatform, virksomheds- og værdikædeanalyser, et RAT (Risk Assessment Tool), en risikostyringsmodel samt illustrative brugscases til formidling af værktøjer.

Projektejer/-leder: Food & Bio Cluster Denmark/Eva Nautrup

Projekthjemmeside: https://www.cybersikrefoedevarevaerdikaeder.dk

Cyber Safe Robotics

Formål: At bidrage til øget konkurrencekraft i robot-, automations- og droneindustrien ved at styrke virksomhedernes cybersikkerhed internt og i forsyningskæderne.

Leverance: Konkrete, virksomhedsnære værktøjer indenfor de 6 temaer: 1) det regulatoriske landskab, 2) det konkurrencemæssige potentiale, 3) cybersikkerhed som en ledelsesopgave, 4) samarbejde i forsyningskæden, 5) sikkerhed i softwareudvikling og 6) når det går galt/beredskabsplaner.

Projektejer/-leder: Odense Robotics/Tina Højrup Kjær

Projekthjemmeside: https://www.odenserobotics.dk/cyber-safe-robotics

Cybersikkerhed i forsyningskæden

Formål: At tilbyde praktiske værktøjer og vejledninger til danske SMV'er - især dem uden erfaring med cybersikkerhed, compliancestandarder eller budget.

Leverance: SUCCESS-værktøjet til overblik og risikovurdering, dialogværktøjer til samtaler med leverandører samt skabeloner til risikovurdering og politik for håndtering af risici i forsyningskæden. Udviklet på baggrund af indsigter fra SMV'er, større virksomheder og myndigheder.

Projektejer/-leder: CBS/Jan Lemnitzer

Projekthjemmeside: https://www.danskindustri.dk/supply-chain-project