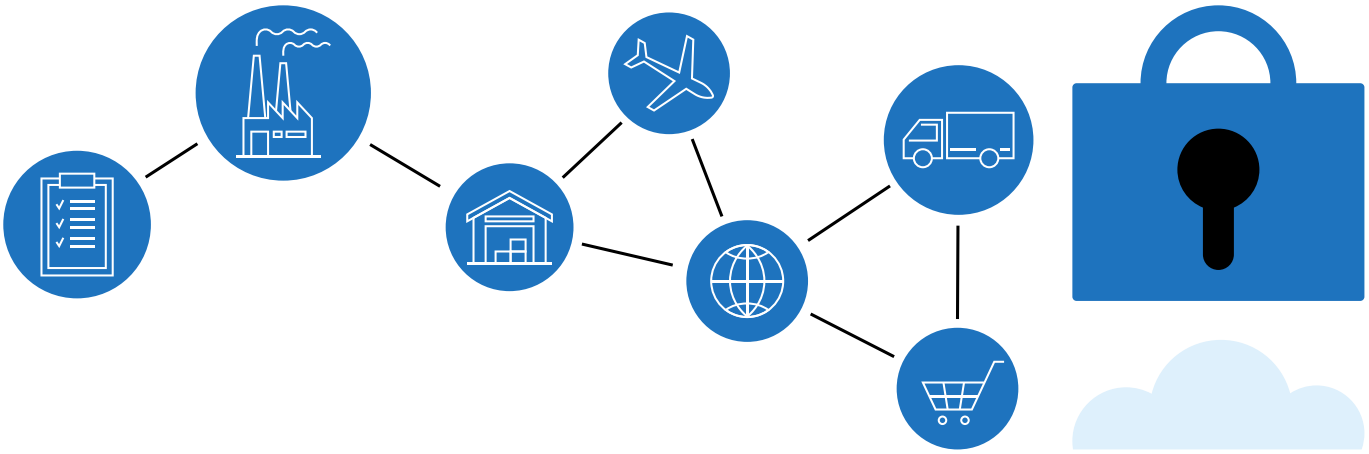
CYBERSIKKERHED OG FORRETNINGSKONTINUITET

Cybersikkerhed og Forretningskontinuitet i små og mellemstore danske produktionsvirksomheder



Indsigter fra anden iteration med virksomhedsinddragelse

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

Juni 2026

INDUSTRIENS FOND

SDU

FORSVARSAKADEMIET

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

ISBN: 978-87-85464-25-5

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 takt med at digitalisering og globalisering i stigende grad væver virksomheder sammen på tværs af lande og sektorer, er forsyningskæder blevet både mere effektive og samtidig mere sårbare. For små og mellemstore virksomheder (SMV'er) er denne udvikling ikke blot en mulighed, men også en kritisk udfordring. Cybersikkerhed er ikke længere et internt anliggende; det er et fælles ansvar på tværs af værdikæder, hvor ét svagt led kan kompromittere hele systemet.

SMV'er indtager ofte en central, men udsat position i disse kæder. De fungerer som nødvendige leverandører og samarbejdspartnere, men har sjældent samme ressourcer til at håndtere avancerede cybertrusler, som større virksomheder har. Konsekvenserne af et cyberangreb rækker derfor ofte langt ud over den enkelte virksomhed og kan skabe forstyrrelser i hele forsyningskæden med økonomiske, operationelle og strategiske implikationer.

Denne rapport sammenfatter resultaterne af andet forløb med virksomheder i projektet Cybersikkerhed og Forretningskontinuitet, der er støttet af Industriens Fond. Rapportens analyser og anbefalinger er baseret på et datagrundlag indsamlet på tre niveauer: 1) det politiske beslutningsniveau, 2) industriniveauet og 3) virksomhedsniveauet. Denne flerstrengede tilgang muliggør en dybdegående forståelse af både strukturelle rammevilkår og konkrete praksisser, som præger SMV'ers arbejde med cybersikkerhed.

Ved at koble organisatoriske perspektiver med eksterne faktorer som geopolitiske spændinger og et eskalerende trusselsbillede, giver rapporten et operationelt grundlag for at identificere sårbarheder og udvikle scenarier, der styrker modstandsdygtigheden. Ambitionen er ikke blot at beskytte den enkelte virksomhed, men at bidrage til mere robuste og bæredygtige forsyningskæder som helhed.

Vi retter en særlig tak til Industriens Fond for den økonomiske støtte, der har muliggjort projektet. Ligeledes takker vi de mange virksomheder og eksperter, der har bidraget med værdifuld viden, erfaringer og perspektiver. Uden jeres engagement ville rapportens indsigter ikke have været mulige.

Forfatterne – juni 2026

1. Introduktion

I takt med at danske produktionsvirksomheder i stigende grad digitaliserer deres processer og indgår i komplekse, globale forsyningskæder, er cybersikkerhed blevet en afgørende forudsætning for både driftssikkerhed og konkurrenceevne (Stentoft et al., 2025). Teknologier som automatisering, IoT og datadrevne systemer har skabt markante produktivitetsgevinster, men har samtidig udvidet virksomhedernes angrebsflade og gjort dem mere eksponerede over for cybertrusler. Nyere forskning understreger tydeligt, at cybersikkerhed ikke længere kan betragtes som et isoleret teknisk anliggende, men må forstås som en integreret del af organisationers strategiske ledelse og værdiskabelse. F.eks. viser nyere studier inden for strategisk cybersikkerhed, at effektiv håndtering af cybertrusler kræver en kobling mellem tekniske, organisatoriske og ledelsesmæssige dimensioner, hvor cybersikkerhed indgår som en central del af virksomhedens overordnede strategi og risikostyring (AlDaajeh & Alrabaee, 2024).

Nyere empiriske studier viser, at virksomheder i stigende grad opfatter cybersikkerhed som en kilde til konkurrencefordele og strategisk differentiering, snarere end blot en omkostning eller compliance-opgave (Chotia et al., 2025; Hasani et al., 2023). Samlet peger denne nyere litteratur på et skifte fra en snæver IT-forståelse til en bredere strategisk tilgang, hvor cybersikkerhed er tæt koblet til governance, forretningskontinuitet og organisatorisk performance. Dermed er cybersikkerhed i dag en central forretningskritisk disciplin, der kræver såvel ledelsesmæssig forankring som tværorganisatorisk integration.

Flere undersøgelser understreger alvoren af denne udvikling. PwC's Global Digital Trust Insights 2026 (PwC, 2026) viser, at en stigende andel af virksomheder oplever alvorlige cyberhændelser med betydelige økonomiske konsekvenser, hvor databrud i stigende grad medfører milliontab. Samtidig peger en undersøgelse fra 2024 på, at cyberangreb både bliver hyppigere og mere komplekse, mens mange virksomheder fortsat har et utilstrækkeligt beredskab til at håndtere truslerne (Munich RE, 2024). Udviklingen forstærkes yderligere af, at en stigende andel af cyberhændelser kan spores til tredjepartsrelationer i forsyningskæder, hvor virksomheder i praksis kun er så sikre som deres mindst beskyttede samarbejdspartner (ENISA, 2023).

For danske produktions-SMV'er er konsekvenserne særligt mærkbare. En undersøgelse fra 2026 viser, at en fjerdedel har haft et cyberangreb indenfor de seneste par år (Stentoft et al., 2026). Sådanne angreb kan føre til produktionsstop og økonomiske tab, hvilket understreger, at cybersikkerhed ikke

alene handler om databeskyttelse, men i høj grad også om at sikre kontinuitet i produktionen og stabilitet i forsyningskæderne. Særligt små og mellemstore virksomheder (SMV'er), som udgør rygraden i dansk industri, befinder sig i en udsat position (SMVdanmark, 2026a). De spiller en central rolle som leverandører og samarbejdspartnere, men har ofte begrænsede ressourcer og mangler systematiske tilgange til cybersikkerhed og risikostyring (Melnyk et al., 2022). Dette gør dem til attraktive mål for cyberkriminelle og til potentielle indgangspunkter for angreb, der kan sprede sig på tværs af hele forsyningskæder (Junior, Becker & Johnson, 2025; Tetteh, 2024). Forskning peger også på, at SMV'er ikke i tilstrækkelig grad er opmærksomme på deres cyberrisici (Button et al., 2025; Latsiou & Lambrinoudakis, 2026) samt løsninger, der kan styrke dem (Heidt, Gerlach & Buxmann, 2019). Nyere forskning peger samtidig på, at effektiv håndtering af cyberrisici kræver en helhedsorienteret tilgang, hvor cybersikkerhed integreres på tværs af organisationens funktioner og i samarbejdet med eksterne partnere (Colicchia, Creazza & Menachof, 2019; Creazza et al., 2022). For produktionsvirksomheder betyder det, at cybersikkerhed skal tænkes ind i alt fra indkøb og produktion til distribution og kundesamarbejde, og at robusthed i stigende grad afhænger af evnen til at forstå og håndtere risici på tværs af værdikæden (Jazairy et al., 2024; Latsiou & Lambrinoudakis, 2026).

Denne rapport tager afsæt i netop denne problemstilling og undersøger, hvordan danske produktionsvirksomheder, med særligt fokus på SMV'er, kan styrke deres cybersikkerhed i en forsyningskædekontekst. Formålet er at skabe indsigt i de udfordringer, virksomhederne står overfor, samt at identificere konkrete tiltag til at opbygge større modstandsdygtighed i et stadigt mere digitalt og risikofyldt erhvervsmiljø.

2. Centrale begreber

2.1 Små og mellemstore virksomheder

Forskningen peger på en tydelig strukturel forskel mellem små og mellemstore virksomheder (SMV'er) og store virksomheder, når det gælder cybersikkerhed (Heidt, Gerlach & Buxmann, 2019). SMV'er er typisk karakteriseret ved begrænsede økonomiske og menneskelige ressourcer, en lavere grad af formalisering og manglende adgang til specialiserede IT-sikkerhedskompetencer, hvilket medfører et mere ad hoc-præget og reaktiv tilgang til sikkerhedsarbejde (Löfving, Säfsten & Winroth, 2014; Zach, Munkvold & Olsen, 2014). Derimod har større virksomheder ofte dedikerede sikkerhedsteams, formaliserede processer og strategisk forankrede investeringer i cybersikkerhed. Samtidig er beslutningsprocesserne i SMV'er ofte tæt knyttet til ejerlederens prioriteringer og kortsigtede driftsbehov, hvilket kan reducere fokus på langsigtet risikostyring (de Araújo Lima, Crema & Verbani, 2020). Disse forskelle resulterer i en såkaldt "security divide", hvor SMV'er generelt har et lavere sikkerhedsniveau og dermed udgør et mere sårbart led - særligt i forsyningskæder, hvor deres svagheder kan få konsekvenser for større aktører (Heidt, Gerlach & Buxmann, 2019).

Et litteratur-review af Junior, Becker & Johnson (2025) af videnskabelige artikler om cybersikkerhed i et SMV-perspektiv identificerede følgende temaer:

- Mangel på opmærksomhed
- Underfinansierede og ressourcebegrænsede cybersikkerhedsprogrammer
- Begrænset forståelse
- Stigende cyberangreb på SMV'er
- Mangel på skræddersyede løsninger og rammeværk
- Litteraturen har overset SMV-specifikke behov
- Lav opfattelse af cyberrisici
- Overbelastet, begrænset eller ikke-eksisterende cybersikkerhedsledelse
- Utilstrækkelige sikkerhedsoperationer
- Stigende økonomiske tab som følge af cyberangreb
- Cloud-adoption minimerer cybersikkerhedsudfordringer
- Lovgivning og oplysning styrker cybersikkerheden

2.2 Cybersikkerhed: Fra et internt til et eksternt perspektiv

Et traditionelt virksomhedsperspektiv på cybersikkerhed er ofte kendetegnet ved et internt fokus, hvor beskyttelse af egne systemer, data og netværk er centralt, og hvor ansvaret typisk er forankret i IT-funktionen. Denne tilgang afspejler en klassisk informationssikkerhedsforståelse, hvor cybersikkerhed primært opfattes som en teknisk disciplin med fokus på kontrol, forebyggelse og compliance med standarder såsom ISO/IEC 27001 (von Solms & van Niekerk, 2013). Litteraturen beskriver dette som en perimeter-baseret tilgang, hvor organisationer søger at beskytte deres informationsaktiver ved at etablere grænser mellem interne og eksterne netværk (Rose et al., 2020).

I kontrast hertil fremhæver nyere forskning inden for supply chain management og informationssikkerhed et mere systemisk perspektiv, hvor cybersikkerhed forstås som et tværorganisatorisk anliggende. Studier viser, at virksomheders sikkerhed i stigende grad afhænger af deres relationer til leverandører, IT-partnere og digitale platforme, som alle kan fungere som indgangspunkter for cyberangreb (Boyson, 2014). Dette perspektiv understreger, at cybersikkerhed ikke kan håndteres isoleret, men kræver koordination og samarbejde på tværs af værdikæder (NIST, 2024).

Desuden peger forskningen på, at et forsyningskædeperspektiv indebærer et skifte fra fokus på beskyttelse til fokus på resiliens og forretningskontinuitet. Sheffi & Rice (2005) og senere Ponomarov & Holcomb (2009) argumenterer f.eks. for, at virksomheders evne til at modstå og tilpasse sig forstyrrelser afhænger af deres samlede netværk frem for den enkelte virksomhed. Inden for cybersikkerhed betyder dette, at robusthed skabes gennem fælles risikoforståelse, informationsdeling og tværorganisatorisk koordinering (Colicchia, Creazza & Menachof, 2019; Creazza et al., 2022).

Samlet set repræsenterer overgangen fra et virksomhedsperspektiv til et forsyningskædeperspektiv et skifte fra kontrol til koordination, hvor cybersikkerhed udvikler sig fra en intern teknisk funktion til en strategisk og relationel disciplin, der er afgørende for værdikædens samlede robusthed.

”Vi står stærkere i dag, når det gælder beredskab over for både cybertrusler og forstyrrelser i forsyningskæden. Projektet har gjort os mere robuste og bedre forberedte på det uforudsete.”

CEO Thomas Molsen, Geovent A/S

2.3 Forretningskontinuitet

I en tid med stigende cybertrusler, digitalisering og usikre forsyningskæder er Business Continuity Management (BCM) blevet afgørende – især for SMV'er. BCM handler om at sikre, at virksomheden kan fortsætte driften eller hurtigt komme tilbage efter en krise (Crask, 2024, p. 4). På cyberprojektets hjemmeside (www.cyber-smv.dk) er foreslået syv værktøjer til arbejde struktureret med BCM på en konkret og praktisk måde.

Arbejdet starter med en **Business Impact Analyse (BIA)**. BIA bruges til systematisk at identificere virksomhedens kritiske forretningsfunktioner og kortlægge deres indbyrdes afhængigheder for at skabe overblik over operationelle prioriteter (Hiles, 2014, p. 150). Samtidig vurderer analysen både de finansielle konsekvenser, såsom tabt omsætning, bøder og genopretningsomkostninger, og de ikke-finansielle konsekvenser, herunder omdømmeskade, brud på lovgivning og tab af kunder. Denne kvantificering gør det muligt at lave en mere kvalificeret cost-benefit-vurdering af investeringer i genopretning og beredskab. BIA fastlægger også, hvor lang nedetid der kan accepteres, samt hvor meget datatab virksomheden kan tåle. På den måde opstilles klare og målbare genopretningsmål, som balancerer forretningsmæssige behov med tekniske muligheder og økonomiske begrænsninger. Det giver realistiske rammer for både IT- og driftsteams. Endelig fungerer BIA som et centralt beslutningsgrundlag for prioritering af ressourcer og valg af risikoreducerende tiltag. Resultaterne fra analysen danner direkte grundlag for virksomhedens forretningskontinuitetsplaner og krisehåndteringsprocedurer og er dermed afgørende for at sikre operationel robusthed og kontinuitet, hvor virksomheden identificerer sine vigtigste processer og vurderer konsekvenserne ved nedbrud. Herefter følger en **risiko- og sårbarhedsanalyse**, som skaber overblik over trusler som f.eks. cyberangreb, samt en **leverandørkritikalitetsanalyse**, der tydeliggør afhængigheder i forsyningskæden. På baggrund af dette udvikles **kontinuitetsplaner** og **cyberberedskabsplaner**, som beskriver, hvordan virksomheden konkret skal reagere og genoprette driften. Disse planer kvalificeres gennem **scenarieplanlægning** og testes i praksis via **tabletop-øvelser**, hvor virksomheden træner sin krisehåndtering.

Capparelli, Chionna & Riglietti (2022) peger på, at effektiv BCM ikke kun handler om at have de rigtige værktøjer og planer. De fremhæver, at mange virksomheder fejler, fordi BCM bliver en skrivebordsøvelse præget af dokumentation og compliance. I stedet bør BCM forstås som et organisatorisk og kulturelt anliggende, hvor succes afhænger af, om arbejdet er forankret i hele virksomheden. Dette perspektiv er centralt i anvendelsen af de syv værktøjer. Værktøjerne skaber ikke værdi i sig selv, men først når de bliver integreret i virksomhedens daglige praksis. Samlet set viser koblingen mellem teori og praksis, at BCM ikke kun handler om at være forberedt på kriser, men om at skabe en organisation, der kan reagere fleksibelt og effektivt. For SMV'er er dette særligt vigtigt, da selv mindre forstyrrelser kan få store konsekvenser for drift og overlevelse.

”Projektet har hjulpet os med at prioritere vores indsatser. Vi har fået en klarere retning for, hvor vi skal investere tid og ressourcer for at styrke både sikkerhed og kontinuitet.”

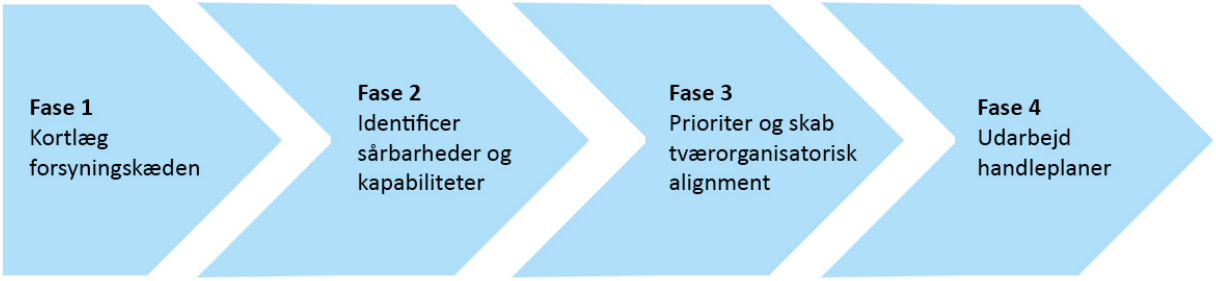
Director of Supply Chain & QA Kirsten Spang, Cryptera A/S

2.4 Procesmodel til supply chain resilience

Stentoft, Mikkelsen & Kjær (2023) præsenterer en procesorienteret tilgang til at styrke Supply Chain Resilience (SCR) i små og mellemstore produktionsvirksomheder. Modellen er udviklet gennem en iterativ forskningsproces med case-studier i danske virksomheder og bidrager dermed med en praksisnær operationalisering af et ellers ofte abstrakt begreb (Eryarsoy et al., 2022; Stentoft & Mikkelsen, 2024). Dette ligger i forlængelse af den bredere SCR-litteratur, hvor resiliens forstås som forsyningskædens evne til at forberede sig på, reagere på og komme sig efter forstyrrelser, samtidig med at centrale funktioner opretholdes (Ponomarov & Holcomb, 2009; Tukamuhabwa et al., 2015).

Procesmodellen består af fire sammenhængende faser (se figur 1), som tilsammen udgør en struktureret tilgang til at identificere, analysere og håndtere risici i forsyningskæden.

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



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

Den første fase omhandler en systematisk kortlægning af forsyningskæden. Her identificeres og visualiseres virksomhedens netværk af leverandører, kunder, interne processer og materialestrømme. Formålet er at skabe et fælles organisatorisk overblik over forsyningskædens struktur og kompleksitet. Dette trin er centralt, da tidligere forskning peger på, at manglende transparens i forsyningskæden ofte øger sårbarheden over for forstyrrelser (Christopher & Peck, 2004). Kortlægningen fungerer således som et fundament for at forstå kritiske afhængigheder og potentielle risikopunkter.

I den anden fase gennemføres en intern analyse, hvor forskellige funktioner i organisationen, f.eks. indkøb, produktion, salg, IT og økonomi, identificerer

både sårbarheder og kapabiliteter til at håndtere sårbarhederne. Denne fase understøtter en differentieret forståelse af risici, idet den fremhæver, hvordan forskellige organisatoriske enheder både påvirkes af og bidrager til forsyningskædens robusthed. Dette perspektiv er i tråd med litteraturen, der understreger, at resiliens ikke alene er et strukturelt fænomen, men også afhænger af organisatoriske kompetencer og læring (Ambulkar, Blackhurst & Grawe, 2015; Sheffi & Rice, 2005).

Den tredje fase fokuserer på prioritering og tværfunktionel koordinering. Her samles de enkelte funktioners vurderinger i en fælles workshop. Formålet er at skabe en fælles forståelse og opnå konsensus om, hvilke risici der er mest kritiske, og hvor ressourcerne bør allokeres. Denne fase er særlig vigtig, da forskning viser, at effektiv håndtering af forsyningskæderisici kræver tæt samarbejde og informationsdeling på tværs af organisatoriske grænser (Jüttner & Maklan, 2011). Den tværfunktionelle dialog bidrager desuden til at reducere silo-tænkning og styrke beslutningskvaliteten.

I den fjerde og afsluttende fase omsættes analyser og prioriteringer til konkrete handlingsplaner. Disse planer kan omfatte tiltag såsom diversificering af leverandørbasen, investering i redundans, forbedring af interne processer eller etablering af beredskabsstrategier. Denne operationalisering af resiliens er afgørende, da tidligere studier har påpeget, at mange organisationer har vanskeligt ved at omsætte risikobevidsthed til konkrete handlinger (Wieland & Wallenburg, 2013).

En væsentlig styrke ved procesmodellen er dens fokus på tværfunktionel inddragelse og udvikling af et fælles organisatorisk sprog omkring resiliens (Stentoft & Mikkelsen, 2024). I de empiriske cases fremhæves det, at processen ikke blot bidrog til identifikation af risici, men også styrkede samarbejdet og den gensidige forståelse mellem funktioner. Dette peger på, at modellen ikke alene understøtter risikostyring, men også fremmer organisatorisk læring og kapabilitetsopbygning – elementer, som anses for centrale i udviklingen af resiliente supply chains (Ambulkar, Blackhurst & Grawe, 2015).

”Vi har fået et fælles sprog og brugbare værktøjer til håndtering af risici og sårbarheder både internt og i den samlede supply chain. Det gør det meget lettere at arbejde på tværs af funktioner og træffe beslutninger.”

COO Lars Torrild, Dolle A/S

2.5 Det systemiske perspektiv: Tre analyseniveauer

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 initiativer om cybersikkerhed og SMV'ers faktiske praksis.

Et af de spændingsfelter, der kan opstå imellem de tre niveauer, er, at reguleringslogikken kan kollidere med SMV'ernes daglige realiteter, hvor ressour-

cer, 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.

2.6 Det geopolitiske perspektiv

Formålet med dette projekt er at adressere en kritisk sårbarhed i hjertet af den danske økonomi: SMV'ers eksponering for et stadigt mere komplekst landskab, hvor geopolitik og cybertrusler smelter sammen. Vi befinder os i en overgangsfase fra en post-koldkrigsæra domineret af liberal kapitalisme og en ren markedslogik, til en fremvoksende geoøkonomisk orden styret af en geopolitisk logik.

I denne nye virkelighed udnyttes asymmetriske globale netværk strategisk af stater gennem fænomenet weaponized interdependence. De infrastrukturer og forsyningskæder, der blev etableret under den liberale verdensorden, udnyttes nu til at skabe panoptikon- eller chokepoint-effekter. For danske SMV'er medfører dette et fundamentalt strategisk dilemma: De kapabiliteter, der tidligere skabte markedsmæssig effektivitet, såsom just-in-time leverancer og single sourcing, udgør nu kritiske sårbarheder over for økonomisk statecraft, sanktioner, og geopolitisk motiverede cyberangreb.

Udfordringen for mange SMV'er er imidlertid, at de besidder begrænsede ressourcer til systematisk at forudse og afbøde disse strukturelle risici. For at imødegå dette er det afgørende at udvikle virksomhedernes geopolitiske dynamiske kapabiliteter. Dette indebærer et markant skift. Det er ikke tilstrækkeligt udelukkende at forbedre evnen til at opfange svage geopolitiske signaler (sensing). Virksomhederne må sideløbende opbygge kapaciteten til at gribe ind og mobilisere ressourcer for at sikre strategisk robusthed (seizing), hvilket kan kompromittere den kortsigtede indtjening. Ultimativt kræver det en evne til at omstrukturere processer og forsyningskæder (transforming) for at bevare forretningskontinuiteten, når asymmetriske chok indtræffer.

Som et led i at styrke særligt sensing-kapabiliteten hos SMV'er introducerer dette projekt et sæt af scenarier, der tager udgangspunkt i et bredere systemisk synsfelt. Disse scenarier er ikke blot abstrakte fortællinger, men fungerer som strukturelle provokationer designet til at bygge bro over oversættelseskløften mellem makrogeopolitiske trusler og operationelle sårbarheder. Ved at integrere geopolitik, cybersikkerhed og forsyningskæderesiliens er det ambitionen, at disse scenarier tillader deltagende SMV'er at transformere deres tilgang fra en reaktiv omkostningsfokusering til en proaktiv kilde til strategisk autonomi og konkurrencefordele.

3. Metode

3.1 Dataindsamling på tre niveauer

For at adressere det strategiske spændingsfelt mellem den nye geoøkonomiske orden og SMV'ers operationelle virkelighed, er projektets metodiske rammedesign struktureret omkring tre hierarkiske analyseniveauer: det politiske niveau, industriniveauet og virksomhedsniveauet. Formålet er systematisk at nedbryde komplekse, abstrakte geopolitiske trusler til konkrete sårbarheder og handlingsanvisninger for danske produktions-SMV'er.

1. **Det politiske beslutningsniveau (makro-identifikation)**
   Processen indledtes med at engagere centrale aktører fra det danske forsvars- og udenrigspolitiske miljø. Formålet var at identificere de strukturelle geopolitiske drivkræfter, der vil forme trusselsbilledet fremover. Gennem struktureret scenarieplanlægning (blandt andet via PESTEL-variabler) isolerede eksperterne de kriser, der kombinerer høj alvorlighed med høj usikkerhed.

2. **Industriniveauet (sektoriel kontekstualisering)**
   For at bygge bro mellem den nationale sikkerhedsarkitektur og virksomhedernes realiteter blev de geopolitiske makro-trends herefter underkastet en "syretest" af brancheeksperter og konsulenter. På dette niveau blev de abstrakte scenarier oversat til et operationelt sprog, der fokuserer på specifikke cybersikkerhedsmæssige og forsyningskædemæssige implikationer for sektoren. Formålet var at identificere, hvordan systemiske stød forplanter sig som konkrete sektor-sårbarheder.

3. **Virksomhedsniveauet (operationel forankring)**
   Det tredje niveau involverede direkte interaktion med SMV-ledere og funktionsansvarlige. Frem for blot at registrere operationelle udfordringer, blev de kontekstualiserede scenarier anvendt som et refleksivt værktøj. Metoden hjalp virksomhederne til at flytte fokus fra en reaktiv, omkostningsfokuseret forståelse af cybersikkerhed til en proaktiv diskussion om strategisk afbødning og behovet for nye dynamiske kapabiliteter.

3.2 Udvikling af scenarier

Som et led i at validere de strategiske rammebetingelser for projektets anden iteration, blev det første analyseniveau (det politiske og strategiske makroniveau) gentaget. Metodisk indebar dette, at en ny, uafhængig kohorte af ak-

tører og domæneeksperter blev bragt sammen for at gennemføre en fornyet scenarieudvikling af det geopolitiske trusselslandskab.

Til trods for udskiftningen af deltagerne resulterede denne proces i en bemærkelsesværdig konvergens: Den nye gruppe af aktører identificerede, prioriterede og formede nøjagtig de samme kernescenarier som den oprindelige gruppe. Dette enstemmige sammenfald på tværs af uafhængige aktørgrupper er et afgørende analytisk fund i sig selv. Det vidner om en udtalt strukturel determinisme i det moderne trusselsbillede.

Den kognitive konsensus på makroniveauet indikerer, at de identificerede trusler ikke er et produkt af en midlertidig diskurs eller en specifik gruppes idiosynkratiske opfattelser. Snarere demonstrerer det den makrostrukturelle tyngde af den igangværende overgang til en geoøkonomisk orden. Denne strukturelle uundgåelighed forstærker projektets hovedargument: Fordi chokkene fra det internationale system fremstår som statiske og uomtvistelige grundvilkår, er det strategiske råderum udelukkende placeret på mikroniveauet. SMV'ernes overlevelse og forretningskontinuitet afhænger derved ikke af at forudsige alternative makrofremtider, men derimod af deres evne til at opbygge de dynamiske kapabiliteter, der kræves for at absorbere de uundgåelige stød fra de identificerede scenarier.

"Det har været en stor fordel med ekstern facilitering af supply chain resilience processen. Det har sikret fremdrift og givet os nye perspektiver, som vi ikke selv havde fået frem."

CEO John Holm, PL Beton A/S

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 en 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 disse observationer 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.

Afsnit 2.2 i rapporten redegør for den nødvendige strategiske transition fra et snævert, internt fokus på cybersikkerhed til et bredere, eksternt perspektiv på forretningskontinuitet. De empiriske data fra case-virksomhederne understøtter entydigt nødvendigheden af dette paradigmeskifte. Observationerne indikerer, at SMV'er ofte lider af en strukturel blindhed over for systemisk skrøbelighed. Workshopforløbene demonstrerede imidlertid, at konfrontationen med indirekte og kaskaderende kriser udgjorde den mest skelsættende erkendelse for deltagerne. Det var bemærkelsesværdigt, at det ikke var truslen om et direkte, isoleret cyberangreb, der fremprovokerede den dybeste strategiske refleksion. Tværtimod skete dette, når virksomhederne blev præsenteret for de afledte effekter af geopolitiske og klimamæssige chok i deres bredere økosystem. Virksomhederne udviste udtalt overraskelse over sårbarheder relateret til underleverandørers pludselige produktionsstop på grund af ekstremt vejr, globale logistiksammenbrud og den deraf følgende tilbagetrækning af forsikringsdækning ved klimaskader. Når trusselsbilledet udvides til at omfatte asymmetriske chok – såsom transportsektorens sårbarhed, pludselige regulative stramninger i eksportmarkederne eller en underleverandørs kompromittering – tvinges ledelsen til at anerkende en ubehagelig virkelighed. Deres egen modstandsdygtighed er uløseligt bundet til robustheden af det samlede netværk, de indgår i.

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 og anden fase. 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. Scenarierne kan tilgås her.

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 udløse 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 cyber-

kriminalitet 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.

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.

4.5.1 Divergerende sensing-kapabiliteter: Det strategisk udsyn over for operationel fastlåsning

En af de mest kritiske indsigter fra case-virksomhedernes evaluering af de geopolitiske fremtidsscenarier er den markante asymmetri i deltagernes sensing-kapabiliteter og deres deraf følgende evne til at bygge bro over metodens indbyggede oversættelseskløft. Inden for rammeværket af dynamiske kapabiliteter er sensing forudsætningen for at afkode eksterne trusselsbilleder, mens oversættelseskløften betegner den analytiske distance fra præsentationen af et abstrakt narrativ til virksomhedens formulering af konkrete, afbødende strategier. De empiriske observationer dokumenterer, at succesfuld strategisk fremtidssikring kræver beherskelse af begge dimensioner, hvilket i praksis viste sig at være i nogen grad divergerende blandt SMV'erne.

I de succesfulde forløb fungerede scenarierne som en effektiv katalysator for systemisk refleksion, hvor virksomhederne udviste en højtudviklet analytisk parathed. Disse deltagergrupper formåede lynhurtigt at abstrahere fra det specifikke narrativ for at identificere strukturelle makrorisici, såsom afhængigheden af amerikansk-kontrolleret digital infrastruktur og asiatiske produktionskæder. Afgørende for deres succes var imidlertid, at de ikke stoppede ved den abstrakte trusselsidentifikation. De krydsede aktivt oversættelseskløften ved øjeblikkeligt at transformere de geopolitiske risici til operationelle konsekvenser i deres egne forsyningskæder, herunder forventede indtægtstab, leverandørsvigt og logistiske flaskehalse. Denne organiske selvanalyse resulterede i konkrete løsningsforslag såsom diversificering af leverandører og redesign af produkter.

I kontrast hertil blotlagde et par workshopforløb metodens potentielle sårbarheder, når virksomhederne var ramt af operationel fastlåsning eller manglede den kognitive båndbredde til abstrakt refleksion. I et af forløbene blev den fremtidsorienterede sensing-funktion reelt paralyseret af nuværende driftsforstyrrelser. Frem for at engagere sig i det eksterne scenarie, konverterede

denne gruppe workshoppen til et forum for fejlfinding domineret af frustrationer over komplicerede ERP-systemer, ineffektive prissætningsprocesser og intern datakvalitet. Den geopolitiske refleksion blev afkoblet til fordel for en eksklusiv fokusering på daglig drift, hvilket understreger, at strategisk sensing er betinget af et vist niveau af operationel stabilitet.

Nogle gange, når virksomheder uden operationel fastlåsning engagerede sig i teksten, faldt de ofte i en bogstavelig fælde, der forhindrede translation. Nogle grupper behandlede scenariet stringent og opgaveorienteret som en tjekliste over elementer i selve fortællingen. Selvom de identificerede cybertrusler i teksten, formåede de kun i meget begrænset omfang at koble disse fiktive hændelser til deres egen forretningskontekst.

Disse spændingsfelter peger på, at Strategic Foresight ikke automatisk skaber proaktiv resiliens i en SMV-kontekst. Uden stram, målrettet facilitering og integration af strukturerede rammeværker, såsom den firefasede procesmodel for Supply Chain Resilience, risikerer fremtidsscenarier at miste deres effekt. Scenarierne formår ikke at gennemtvinge oversættelsen fra geopolitisk fiktion til lokal handling, hvis ledelsens opmærksomhed enten forbruges af operationel friktion eller strander i en udelukkende tekstnær læsning.

Selvom scenariemetoden har nogle svagheder i relation til operationel fastlåsning, formår den for de fleste af de SMV'er, der deltog i workshoppen, at synliggøre de skjulte, afledte effekter og andenordenskonsekvenser, som konventionelle, interne risikovurderinger systematisk overser. Udfordringen for virksomhederne er efterfølgende at integrere denne systemiske forståelse i deres formelle leverandørkrav og beredskabsplaner, hvilket nogle gange kan kræve et markant opgør med eksisterende ressourceprioriteringer.

5. Træningsdag på SDU

Præsentationer fra træningsdagen på SDU den 25. marts 2026.

5.1 Best practice indenfor cybersikkerhed

Ved lektor Peter Mayer:
Danske produktions-SMV'er opererer i stadig mere digitaliserede og sammenkoblede miljøer, samtidig med at de ofte mangler dedikerede ressourcer til cybersikkerhed og specialiseret ekspertise. Samtidig står de over for stigende cybertrusler, voksende afhængigheder i forsyningskæden og skærpede regulatoriske krav, herunder potentielle forpligtelser under NIS2. På denne baggrund fokuserede præsentationen på at omsætte aktuel forskning om cybersikkerhed, regulatoriske udviklinger og indsigt fra virkelige angreb til handlingsorienteret vejledning for organisationer. Til dette formål kombinerede den adfærdsindsigter, evidensbaserede best practices, regulatoriske krav og praktiske cases med det formål at styrke organisationers cyberresiliens.

Et centralt tema i træningen var betydningen af menneskelig beslutningstagning for resultater indenfor cybersikkerhed. Med udgangspunkt i adfærdsøkonomi viste sessionen, hvordan kognitive bias – især tabsaversion – påvirker organisationers risikobeslutninger. Deltagerne blev præsenteret for, at organisationer ofte accepterer betydelige og usikre genopretningsomkostninger efter cyberhændelser, mens de tøver med at investere i forudsigelige, forebyggende sikkerhedstiltag. Denne indsigt positionerer investeringer i cybersikkerhed som en strategisk risikostyringsbeslutning frem for en ren teknisk omkostning.

For at vejlede fremtidige investeringer og indsatser inden for cybersikkerhed bør evidensbaserede best practices for awareness og træning inddrages. Langsigtede studier, der blev gennemgået i sessionen, viste, at traditionelle årlige opfriskningskurser er utilstrækkelige. I stedet indikerer forskningen, at viden og færdigheder inden for cybersikkerhed forringes markant og bør opdateres med seks måneders intervaller. Derudover er personaliserede og rollebaserede træningstiltag mere effektive end ensartede træningsmetoder, da de gør det muligt for medarbejdere med forskellige udgangsniveauer at opnå sammenlignelige kompetencer indenfor cybersikkerhed, samtidig med at det samlede træningsomfang reduceres.

En faldgrube ved valg af tiltag til at styrke cybersikkerheden er at basere sig på lavkvalitets eller forældet sikkerhedsrådgivning. Almindeligt tilgængelig online vejledning – især inden for områder som anti-phishing og adgangskodepraksis – er ofte inkonsistent eller modstridende. Derfor er det afgørende kun at vælge tiltag, hvis effektivitet er dokumenteret. Samtidig er det vigtigt at undgå udbredte, men forældede praksisser såsom obligatoriske, periodiske ændringer af adgangskoder. Moderne cybersikkerhedsstandarder fraråder disse til fordel for overvågning, nulstilling af adgangskoder ved databrud og forbedrede detektionsmekanismer.

En yderligere central overvejelse for SMV'er er rammeværker til cybersikkerhed og regulatoriske krav. Særlig opmærksomhed bør rettes mod EU's NIS2-direktiv. Sessionen tydeliggjorde virksomheders forpligtelser, herunder tidsfrister for hændelsesrapportering, ledelsesansvar samt obligatoriske awareness- og træningsaktiviteter. Det blev understreget, at organisationer selv er ansvarlige for at afgøre, om de er omfattet af direktivet, og at manglende overholdelse kan medføre betydelige sanktioner. Supplerende rammeværker – herunder NIST Cybersecurity Framework (CSF) 2.0, Cybersecurity Capability Maturity Model (C2M2) og ISO/IEC 27001 – blev præsenteret som strukturerede tilgange til at vurdere, forbedre og styre kapaciteter til cybersikkerhed ud over rene compliancekrav.

Den afsluttende del af præsentationen fokuserede på cybersikkerhedsangreb i praksis, med særlig vægt på trusler i forsyningskæden. Med udgangspunkt i empiriske undersøgelser og interviews gennemført i Danmark og Ukraine blev den stigende udbredelse af kompromitteringer i forsyningskæden som angrebsvektor tydelig. Cases – herunder Log4Shell-sårbarheden, SolarWinds-angrebet og statsrelaterede angreb via forsyningskæder – illustrerer, hvordan organisationer kan blive påvirket, selv når deres egne interne sikkerhedskontroller er robuste. Disse eksempler understreger behovet for systematisk tredjepartsrisikostyring, reduceret implicit tillid til leverandører og kunder samt løbende overvågning af afhængigheder på tværs af den digitale forsyningskæde.

Opsummering af centrale budskaber:

- Menneskelige kognitive bias påvirker beslutninger om cybersikkerhed og kan føre til underinvestering i forebyggelse.
- Awareness for cybersikkerhed bør opdateres mindst hver sjette måned for at forblive effektiv.
- Personaliseret træning lukker kompetencegab hurtigere end ensartede programmer.
- Evidensbaserede sikkerhedstiltag er mere effektive end almindelig lavkvalitetsrådgivning.

- Regelmæssige, obligatoriske adgangskodeændringer giver begrænset sikkerhed og frarådes i moderne standarder.
- NIS2 øger markant organisationers, ledelsers og rapporteringsmæssige ansvar.
- Rammeværker som NIST CSF, C2M2 og ISO 27001 understøtter struktureret udvikling af kapabiliteter.
- Kompromittering af forsyningskæder er en væsentlig angrebsvektor, der kræver styrket tredjepartsrisikostyring.

5.2 Digitalisering og cloud computing: Risici og best practice

Ved lektor Marco Peressotti:

Digitalisering og anvendelsen af cloud computing bliver i stigende grad centrale for driften af danske SMV'er og giver klare fordele i form af fleksibilitet, skalerbarhed og adgang til avancerede digitale værktøjer. Cloudløsninger muliggør et skifte fra store forudgående kapitalinvesteringer til forbrugsbaserede omkostningsmodeller, samtidig med at de understøtter samarbejde på tværs af lokationer og giver adgang til analyseværktøjer, automatisering og AI-tjenester. Når de implementeres effektivt, kan de også styrke organisationers tilpasningsevne gennem on-demand skalering, redundans og strukturerede gendannelsesmuligheder.

Som fremhævet i de foregående præsentationer opererer SMV'er i et mere usikkert og politisk påvirket miljø. I denne kontekst er cloud computing ikke blot en neutral teknologisk opgradering, men en del af den samme bredere udvikling, der påvirker fysiske forsyningskæder. Digitale infrastrukturer er indlejret i globale systemer præget af koncentration, indbyrdes afhængighed og sårbarhed over for forstyrrelser. Brug af cloud computing er derfor ikke kun drevet af effektivitetsgevinster, men også af eksterne pres som stigende cybertrusler, skærpet regulering (f.eks. GDPR og NIS2) samt øget afhængighed af et lille antal globale leverandører. Dette løfter cloud computing fra at være et teknisk valg til et strategisk valg med konsekvenser for driftskontinuitet, sikkerhed og kontrol over kritiske data og systemer. En central konsekvens er en omfordeling af ansvar. Selvom leverandører håndterer den underliggende infrastruktur, forbliver organisationer ansvarlige for databeskyttelse, systemkonfiguration og compliance. I praksis betyder det, at mange hændelser opstår som følge af interne beslutninger snarere end leverandørfejl. Fejlkonfiguration, svage adgangskontroller og dårligt systemdesign identificeres konsekvent som primære kilder til sårbarhed. Dette afspejler mønstre fra forsyningskæder, hvor risici ofte er indlejret i systemernes opbygning snarere end udelukkende at stamme fra eksterne chok.

SMV'er må derfor træffe bevidste valg om, hvad der skal flyttes til skyen, hvilke leverandører der skal anvendes, og hvordan man balancerer kontrol

med bekvemmelighed. Hybride løsninger foretrækkes typisk og afspejler et skifte væk fra ren effektivitet mod en mere balanceret tilgang, der også inkluderer robusthed. I denne sammenhæng fremstår digital suverænitet som en central problemstilling. Afhængighed af et begrænset antal dominerende - primært ikke-europæiske - leverandører skaber strukturel eksponering. Disse afhængigheder kan begrænse kontrol over data og infrastruktur og i ekstreme tilfælde skabe muligheder for politisk eller økonomisk pres. Som diskuteret i den geopolitiske kontekst kan indbyrdes afhængighed udnyttes strategisk; digital infrastruktur er ingen undtagelse. Digital suverænitet bør ikke forstås som fuld teknologisk uafhængighed, men som evnen til at håndtere kritiske afhængigheder.

For SMV'er betyder det, at cloud-beslutninger ikke kun skal vurderes ud fra pris og funktionalitet, men også i forhold til langsigtet kontrol og eksponering. Muligheden for, at adgang til centrale digitale tjenester kan blive politiseret, er stadig usandsynlig, men ikke længere rent hypotetisk. Robusthed i en digital kontekst afhænger derfor mindre af én enkelt teknisk løsning og mere af kvaliteten af de strategiske valg. Organisationer skal forstå, hvor de er eksponerede, hvor kritiske disse eksponeringer er, og hvor stor risiko de er villige til at acceptere. Dette kan indebære diversificering af leverandører, kombination af cloud- og on-premises-løsninger eller selektiv prioritering af alternativer, hvor kontrol er særligt vigtig. For at understøtte dette skitserer præsentationen en række best practices med fokus på governance og struktureret risikostyring. Disse omfatter bevidste valg af leverandører, robust datastyring (f.eks. kryptering, redundans og automatiske backups), klart definerede og testede gendannelsesprocedurer samt omfattende datastyringsrammer, der dækker adgang, klassificering, opbevaring og håndtering af hændelser. Afgørende er det, at disse tiltag løbende vedligeholdes og tilpasses.

Samlet set tilbyder cloud computing betydelige fordele, men øger samtidig integrationen i globale systemer præget af asymmetrier i magt og kontrol. Ligesom med fysiske forsyningskæder opnås robusthed ikke længere alene gennem optimering, men gennem en bevidst balance mellem effektivitet, sikkerhed og autonomi. For danske SMV'er kræver dette, at cloud-strategi integreres i en bredere tilgang til risikostyring i et stadig mere komplekst driftsmiljø.

Opsummering af centrale budskaber:

- Cloud computing er indlejret i de samme strukturelle ændringer, der påvirker forsyningskæder.
- Digital infrastruktur skaber nye former for afhængighed og eksponering.
- Digital suverænitet handler om at håndtere – ikke eliminere – afhængigheder.
- Brug af cloud-teknologi er en strategisk beslutning med driftsmæssige og

governance-mæssige konsekvenser.

- Cloud-strategi bør være forankret i en bredere tilgang til risiko og robusthed.
- Governance, datastyring og gendannelsesevne er centrale elementer.
- Robusthed afhænger af en balance mellem effektivitet, sikkerhed og kontrol.

5.3 Den strategiske nødvendighed af geopolitiske dynamiske kapabiliteter i danske SMV'er

Ved lektor Vincent Keating:

Den globale, liberale orden efter Den Kolde Krig, som var funderet på en forventning om adskillelse af økonomi og sikkerhedspolitik, er brudt sammen. Vi befinder os nu i en fremvoksende geoøkonomisk orden, hvor stater systematisk genkobler sikkerhedspolitik og økonomisk strategi. For danske SMV'er betyder dette et fundamentalt skift: De opererer ikke længere udelukkende under en *markedslogik* præget af effektivitet og "positive-sum"-relationer, men i stigende grad under en *geopolitisk logik* defineret af anarki, overlevelse og statslige "zero-sum"-kalkuler.

I denne nye virkelighed udnyttes de globale netværk og infrastrukturer, som blev bygget for at fremme frihandel, nu til strategisk tvang. Dette miljø forstærker også cyberrisici, da cyberangreb i stigende grad anvendes som asymmetriske våben i stormagtsrivaliseringen og økonomisk statecraft. Konsekvensen for danske SMV'er er, at højt optimerede forsyningskæder, der var strategiske fordele under markedslogikken (f.eks. just-in-time produktion og outsourcing), nu kan udgøre kritiske sårbarheder. For at overleve denne systemiske forstyrrelse er det ikke længere tilstrækkeligt at besidde konventionelle dynamiske kapabiliteter, der primært håndterer markedsvolatilitet. Virksomhederne må udvikle *Geopolitiske Dynamiske Kapabiliteter (GDC)*, som adresserer trusler, der er eksogene i forhold til markedet, men endogene i forhold til statslige sikkerhedsdilemmaer.

Udviklingen af GDC kræver en radikal rekonfigurering af de klassiske dynamiske processer:

Sensing (opfangelse): Frem for blot at identificere markedstrends eller disruptive teknologier, kræver GDC en systematisk kapacitet til at afkode politiske signaler og statslige intentioner. SMV'er skal kunne forudse, hvordan internationale spændinger eller ekstraterritorial lovgivning kan omsættes til forstyrrelser i deres dybe forsyningskæder (n-tier) og i form af cybertrusler.

Seizing (griben ind): Hvor konventionel seizing fokuserer på profitmaksimering og ressourceallokering for at vinde markedsandele, dikterer GDC, at virksomheder skal opbygge strategisk robusthed, ofte på direkte bekostning

af kortsigtet indtjening. Dette indebærer svære operationelle trade-offs, såsom skiftet til dual-sourcing, etablering af sikkerhedslagre (”just-in-case”) og fravalg af leverandører i politiske højrisikozoner.
Transforming (omstilling): Klassisk transformation handler om gnidningsløs integration i globale netværk. GDC kan derimod kræve evnen til strategisk afkobling eller kontrolleret fragmentering, f.eks. gennem regionalisering af produktion (’friend-shoring’) eller opbygning af redundante it-infrastrukturer for at isolere kompromitterede netværksdele.

Overgangen til GDC markerer et kognitivt og operationelt paradigmeskifte for SMV’er: fra en logik baseret på velstandsskabelse gennem handel til at investere i langsigtet overlevelse og strategisk autonomi i et permanent usikkert, geoøkonomisk system.

Opsummering af centrale budskaber:

- Den liberale verdensorden er under afvikling til fordel for en geoøkonomisk orden styret af statslige sikkerhedslogikker frem for traditionelle markedslogikker.
- Globale forsyningskæder og digitale infrastrukturer udnyttes aktivt som strategiske tvangsmidler gennem blandt andet panoptikon- og chokepoint-effekter.
- Omkostningsoptimerede og integrerede forsyningskæder udgør i dag kritiske sårbarheder i et erhvervsmiljø præget af asymmetrisk stormagtsrivalisering.
- Strategisk overlevelse kræver udvikling af Geopolitiske Dynamiske Kapabiliteter (GDC), der specifikt adresserer trusler uden for det konventionelle markedssystem.

5.4 Supply chain resilience og cybersikker supply chain risk management

Ved professor Jan Stentoft:
Danske produktions-SMV’er indgår i komplekse forsyningskæder med mange indbyrdes afhængigheder. Disse omfatter relationer til kunder, leverandører af både direkte og indirekte varer, IT-leverandører, finansielle partnere, offentlige myndigheder samt logistikvirksomheder. Denne kompleksitet øger behovet for systematisk arbejde med supply chain management og særligt risikostyring i forsyningskæden. En central forudsætning for effektiv risikostyring er en grundig kortlægning af forsyningskæden på tværs af flere led såvel upstream fra leverandører som downstream mod kunder. Selvom denne opgave kan virke omfattende, er det afgørende at visualisere og optegne relationerne for at skabe overblik over potentielle sårbarheder. Kortlægningen bør ske tværorganisatorisk og involvere funktioner som salg, produktion, indkøb, økonomi, IT og produktudvikling for at sikre en helhedsorienteret tilgang.

Dette arbejde danner grundlag for en systematisk risikovurdering af forsyningskæden. I denne sammenhæng er det vigtigt at prioritere indsatsen, da ikke alle risici kan håndteres aktivt. Nogle risici bør mitigere gennem konkrete tiltag, mens andre må accepteres som en del af virksomhedens samlede risikoprofil, ofte på grund af begrænsede ressourcer. Ved andre typer risici kan man arbejde med at reducere sandsynligheden for, at de indtræffer, f.eks. ved at finde og godkende alternative leverandører eller sprede indkøb på flere geografiske områder. Endelig kan virksomheder anvende instrumenter som kontrakter, forsikringer og hedging til at overføre eller dele risici.

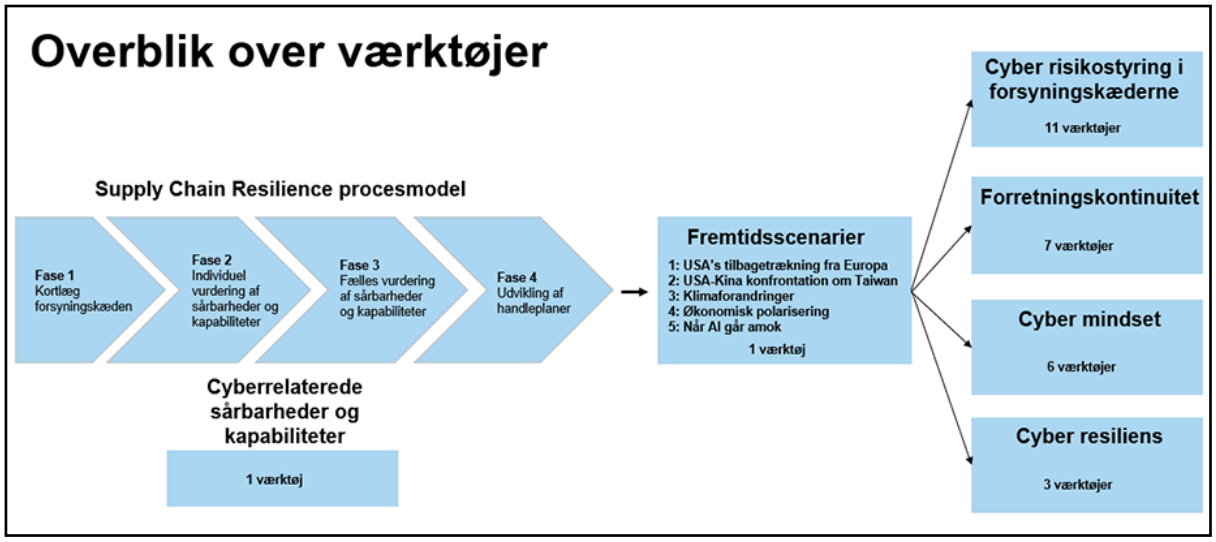
I en mere geopolitisk urolig verden er betydningen af supply chain resilience blevet markant forstærket. Forstyrrelser som COVID-19-pandemien, krigen i Ukraine og et uroligt Mellemøsten har tydeliggjort, hvor hurtigt globale forsyningskæder kan bryde sammen. Tidligere angreb fra Houthi-bevægelsen i Det Røde Hav gjorde det risikabelt at sejle gennem Suezkanalen. Det tvang mange rederier til at omlægge deres ruter og i stedet sejle syd om Afrika, hvilket medførte længere transporttid, højere omkostninger og øget usikkerhed i leverancer. Ligeledes har stigende energipriser og handelsrestriktioner haft direkte konsekvenser for produktionsomkostninger og leveringssikkerhed. For danske produktions-SMV'er betyder dette, at selv indirekte afhængigheder, som f.eks. underleverandører i tredje led, kan skabe uforudsete flaskehalse. Arbejdet med risikostyring hænger derfor tæt sammen med udviklingen af supply chain resilience, hvor virksomheder styrker deres evne til både at forebygge, absorbere og tilpasse sig forstyrrelser. En procesmodel med fire faser (se figur 1) foreslås som ramme for dette arbejde. Denne tilgang understøtter samtidig virksomhedens forretningskontinuitet ved at sikre, at kritiske funktioner kan opretholdes under og efter hændelser som leverandørsvigt, transportstop eller cyberangreb.

Cybersikkerhed spiller en stadig vigtigere rolle i forsyningskæder, hvor digitale forbindelser mellem aktører skaber nye og ofte skjulte sårbarheder. Angreb på én aktør kan hurtigt sprede sig til resten af kæden. Et konkret eksempel er ransomware-angreb mod logistik- eller IT-leverandører, som kan lamme hele distributionssystemer. Ligeledes kan kompromitterede leverandører give adgang til følsomme data eller produktionssystemer hos andre virksomheder i kæden. I takt med at cyberkriminalitet og geopolitik i stigende grad overlapper, ses også flere statssponsorerede angreb rettet mod kritisk infrastruktur og erhvervsliv.

En spørgeskemaundersøgelse baseret på 10 praksisser fra NIST-frameworket for cybersikkerhed viser dog generelt lave scorer omkring niveau 2 på en 5-punkts Likert-skala, hvilket indikerer, at virksomheder kun i lav grad arbejder systematisk med cybersikkerhed i et forsyningskædeperspektiv. Dette kan blandt andet forklares med, at området er ressourcekrævende, samt at der mangler viden og kompetencer. Samtidig peger resultaterne på et væsentligt forbedringspotentiale, da utilstrækkelig cybersikkerhed ikke blot udgør en teknisk risiko, men en forretningskritisk trussel mod drift, omdømme og samarbejdsrelationer.

Samlet set understreger udviklingen, at danske SMV'er i stigende grad må integrere supply chain resilience, cybersikkerhed og forretningskontinuitet som centrale elementer i deres strategiske arbejde. Evnen til at håndtere usikkerhed og opretholde drift under pres er ikke længere blot en operationel disciplin, men en afgørende konkurrenceparameter i en mere uforudsigelig global økonomi. Endelig blev der gennemført en guidet tur i projektets udviklede værktøjer, som fremgår af figur 2. Værktøjerne er tilgængelige på www.cyber-smv.dk.

***Figur 2**: Udviklede værktøjer*



Opsummering af centrale budskaber:

- Forsyningskæder er komplekse og sårbare
- Kortlægning er nødvendig for overblik
- Risici skal prioriteres (mitigere, acceptere eller overføre)
- Geopolitik øger risikoen for forstyrrelser
- Supply chain resilience er afgørende
- Forretningskontinuitet sikrer drift under kriser
- Cybersikkerhed er en kritisk svaghed
- Resiliens og sikkerhed er nu strategisk nødvendige
- Manglende ressourcer og viden er væsentlige barrierer, men der findes hjælp på www.cyber-smv.dk

5.5 Penetration testing

Ved Security & Risk Management Consultant Susanna Forti og sikkerhedskonsulent Atilla Taner, Reversec:

Penetrationstest, eller pentest, er en type sikkerhedsvurdering, der simulerer tekniske angreb på applikationer, netværk og andre aktiver for at identificere sårbarheder og svagheder, som kan udgøre risici for virksomheden og dens kunder. Pentests kan udføres inden for mange områder, herunder webapplikationer, mobilapplikationer, netværk, hardware, mainframes, OT (operational technology), GenAI, cloud, fysisk sikkerhed og social engineering. Pentests flytter sikkerhed fra teori til evidens ved at vise, hvad en angriber faktisk kan få adgang til og misbruge, hvilket hjælper organisationer med at prioritere risici i forretningen. Ud over pentests findes der også andre typer sikkerhedsvurderinger, såsom:

- **Purple teaming**, som tester evnen til at opdage og reagere på hændelser.
- **Attack path mapping**, som identificerer og teknisk verificerer de ruter, angribere kan tage.
- **Red teaming**, som er en omfattende test for modne organisationer, der simulerer realistiske angreb og forsvarsaktiviteter.

For at afgøre hvilke typer af test, der er mest relevante for en virksomhed, kan en risikoanalyse identificere risici på tværs af virksomheden, en trusselsvurdering kan fremhæve højt prioriterede systemer, og en pentest kan afsløre systemets sårbarheder samt vurdere effektiviteten af eksisterende kontroller. Mens compliance fastsætter et minimumsniveau af krav, går pentesting et skridt videre ved at besvare spørgsmålet: "Virker vores kontroller faktisk i praksis?" Ud over compliance bidrager pentests også til organisatorisk robusthed ved at afdække problemer, forbedre afhjælpning, detektion og respons samt understøtte forretningskontinuitet gennem beskyttelse af kritiske tjenester og produkter.

Pentesting-processen består af flere trin. Den starter med afgrænsning (scoping), hvor pentestere, udviklere og ledelse bliver enige om, hvad der skal og ikke skal testes, hvilke metoder der anvendes, og hvad de største bekymringer er. Derefter udarbejdes en formel Statement of Work, der er et formelt dokument, der beskriver, hvad testen skal omfatte, hvordan den udføres, og hvilke rammer der gælder. Når testen er gennemført, dokumenteres alle fund, risici og anbefalinger i en rapport. Den sidste fase er risikohåndtering, hvor udviklings- og ledelsesteamet beslutter, hvordan de identificerede risici skal håndteres.

Der er flere forhold, man skal være opmærksom på i forbindelse med penetrationstest:

- Det kan være udfordrende at definere det rette scope og tidsramme
- Omkostninger skal tages i betragtning
- Udviklingsteams kan føle sig utrygge ved at få testet deres systemer, især hvis sårbarheder tilskrives dem – men pentestere er der for at hjælpe gennem samarbejde
- En almindelig faldgrube er at gøre pentesting til en tjeklisteøvelse, hvilket det ikke er
- Der kan i sjældne tilfælde opstå nedbrud i systemer under testen

6. Temaer fra virksomhederne

I arbejdet med case-virksomhederne gennem de to kursusdage (den første gennemført i hhv. Hobro, Vejle, Middelfart og Hvidovre, og den anden gennemført i Odense for alle virksomhederne) stillede virksomhederne en række meget relevante spørgsmål i relation til projektets tematikker. Disse spørgsmål er medtaget nedenfor som inspiration til andre virksomheder, og der er givet mulige svar på spørgsmålene. Det er vigtigt at bemærke, at svarene ikke må læses som værende udtømmende.

"Det har været afgørende for os, at resultaterne er til at arbejde videre med. Vi står ikke bare med analyser, men med noget vi faktisk kan implementere. De første tiltag er allerede igangsat."

Kvalitetschef Brian Nygaard Pedersen, ME Production A/S

1. ***Hvordan sikrer vi, at vores aftaler med IT-leverandører er dækkende cybersikkerhedsmæssigt?***

   Sørg for, at aftalerne indeholder klare krav til sikkerhedsstandarder (f.eks. NIST/ISO 27001), adgangskontrol, databeskyttelse, incident response og løbende audit/revision. Derudover bør der være ansvarsplacering, rapporteringspligt ved brud og krav til IT-leverandører og disses underleverandører. Se appendix 1 for en template med spørgsmål man kan stille virksomhedens IT-leverandør(er).

2. ***Hvad er relevansen af cyberforsikringer?***

   Cyberforsikringer er blevet stadig mere relevante i takt med den stigende digitalisering og de voksende cybertrusler. For mange virksomheder, særligt for SMV'er, kan et cyberangreb som ransomware, datalæk eller nedbrud i IT-systemer få alvorlige økonomiske og driftsmæssige konsekvenser. En cyberforsikring kan bidrage til at dække omkostninger forbundet med f.eks. genopretning af data, driftstab, juridisk bistand og håndtering af sikkerhedsbrud. Det er dog vigtigt at understrege, at cyberforsikringer ikke kan stå alene. De fungerer bedst som et supplement til et solidt cybersikkerhedssetup, da forsikringsselskaber ofte stiller krav til virksomhedens dokumenterede sikkerhedsniveau. Samtidig kan forsikringer være med til at skabe incitament til at arbejde mere systematisk med cybersik-

kerhed og risikostyring. Dog er det vigtigt at læse betingelserne grundigt igennem for at sikre sig den rette dækning og kende til de betingelser, der gør sig gældende.

En deltager nævnte f.eks., at det er vigtigt at være opmærksom på, om cyberforsikringens dækningsperiode er tilstrækkelig i forhold til virksomhedens Recovery Time Objective (RTO). Hvis genopretningen af systemer og drift tager længere tid end den periode, forsikringen dækker driftstab og omkostninger, kan virksomheden stå med væsentlige udækkede tab. Derfor bør dækningsperioden afstemmes med realistiske scenarier for nedetid og genopretning, herunder worst-case hændelser.

3. ***Hvad er NIS2?***

NIS2 er et EU-direktiv, der stiller skærpede krav til cybersikkerhed, risikostyring og rapportering af hændelser for virksomheder inden for kritiske og vigtige sektorer (f.eks. energi, transport, sundhed, produktion og digitale tjenester). Formålet er at øge robustheden over for cybertrusler i hele EU. For at vurdere om man er omfattet, bør man:

- afklare, om virksomheden opererer i en sektor omfattet af NIS2
- vurdere, om man falder ind under kategorien om at være en "væsentlig" eller "vigtig" enhed. En væsentlig enhed er typisk en større organisation inden for kritiske sektorer som energi, sundhed eller transport, hvor driftsforstyrrelser kan få alvorlige samfundsmæssige konsekvenser. En vigtig enhed har også betydning, men er enten mindre eller opererer i mindre kritiske sektorer, og konsekvenserne ved nedbrud er derfor mindre omfattende. Klassificeringen afhænger især af virksomhedens størrelse, sektor og samfundskritiske rolle.
- undersøge nationale implementeringer (i Danmark via lovgivning og myndigheder)

Hvis man er i tvivl, er det en god idé at lave en screening eller gabanalyse op mod NIS2-kravene, fordi mange virksomheder indirekte bliver påvirket gennem deres rolle i forsyningskæder.

4. ***Bliver NIS2 opdateret/outdated?***

NIS2 bliver outdated, da det handler om virksomhedsprocesser. NIS2 bliver løbende opdateret og viderudviklet. NIS2 er designet som en rammelov, der løbende kan tilpasses et hurtigt foranderligt cybertrusselsbillede (European Commission, 2026). Da truslerne udvikler sig kontinuerligt, justeres og videreudvikles reglerne også over tid. EU har allerede i 2026 foreslået ændringer og udvidelser af NIS2, herunder skærpede krav og en tydeligere afgrænsning af, hvilke aktører der er omfattet. Samtidig bevæger fokus sig fra selve implementeringen mod løbende opdatering, efterlevelse og håndhævelse.

5. ***Hvad er bestyrelsens rolle angående cybersikkerhed?***

   Ifølge Bestyrelsesforeningen (2022) har bestyrelsen det overordnede ansvar for virksomhedens cybersikkerhed og skal sikre, at arbejdet forankres strategisk og systematisk. Det indebærer, at bestyrelsen skal fastlægge og følge op på en cybersikkerheds- og risikostyringsstrategi samt føre løbende tilsyn med, at direktionen implementerer relevante tiltag. Derudover skal bestyrelsen sikre fokus på risikostyring, forretningskontinuitet, kriseberedskab og leverandørsikkerhed. Endelig har bestyrelsen ansvar for at sikre de nødvendige kompetencer og understøtte en stærk cybersikkerhedskultur i organisationen, så virksomheden er i stand til at håndtere og modstå cybertrusler.

6. ***Hvordan får vi en bedre procesforståelse og modenhed?***

   En produktions-SMV kan opnå en højere procesforståelse og procesmodenhed ved systematisk at arbejde med kortlægning, måling og løbende forbedring af sine kerneprocesser. Først og fremmest er det centralt at skabe transparens gennem anvendelse af kortlægningsværktøjer som brown paper workshops, hvor medarbejdere i fællesskab visualiserer processer, samt Value Stream Mapping, der giver indsigt i flow, spild og værdiskabende aktiviteter. Dette bidrager til en fælles forståelse af, hvordan arbejdet faktisk udføres i praksis og danner grundlag for at bevæge organisationen fra et lavt modenhedsniveau præget af ad hoc-arbejde til mere strukturerede og definerede processer. Herefter bør virksomheden etablere enkle, men relevante målepunkter, som gør det muligt at følge performance og identificere forbedringsområder, hvilket understøtter en udvikling mod et højere modenhedsniveau, hvor processer i stigende grad bliver målt og styret. Med afsæt i dette kan virksomheden arbejde struktureret med kontinuerlige forbedringer, f.eks. gennem en iterativ metode som PDCA (Plan, Do, Check, Act), samtidig med at medarbejdere aktivt inddrages for at skabe ejerskab og læring i organisationen. Standardisering af arbejdsgange bidrager yderligere til at reducere variation og er et centralt element i at opnå stabile og reproducerbare processer, som er karakteristisk for højere procesmodenhed. Samlet set understøtter disse tiltag en bevægelse fra umodne, uformelle processer mod en mere moden, datadrevet og optimeret processtyring, hvilket er i tråd med principperne inden for Business Process Optimization, hvor fokus er på systematisk forbedring, transparens og styring af forretningsprocesser (Stentoft & Haug, 2019).

7. ***Hvordan håndteres balancen mellem drift og udvikling?***

   Virksomheder står ofte over for et grundlæggende dilemma mellem at sikre løbende udvikling og forbedring af forretningsgange og samtidig håndtere den daglige drift. I en travl hverdag vil ressourcer, tid og ledelsesmæssig opmærksomhed typisk være bundet op på at sikre stabil produktion, levering og kundeservice, hvilket kan gøre det vanskeligt at prioritere strategiske initiativer som procesoptimering, digitalisering og

styrket risikostyring. Konsekvensen kan være, at nødvendige forbedringer udskydes, selvom de på længere sigt er afgørende for virksomhedens robusthed og konkurrenceevne. Omvendt kan for stort fokus på udvikling gå ud over den kortsigtede drift og performance. Dilemmaet kræver derfor en bevidst prioritering, hvor virksomheder arbejder struktureret med både drift og udvikling, f.eks. gennem klare ansvarsfordelinger, dedikerede ressourcer og integration af forbedringsarbejde i de daglige processer (O'Reilly & Tushman, 2004). Man kan også bruge risikovurderinger til at afgøre, hvilke udviklingsaktiviteter der er mest nødvendige (f.eks. cybersikkerhed og supply chain resilience).

8. ***Hvordan skal man angribe opgaven med at styrke cybersikkerheden?***

En produktions-SMV kan angribe arbejdet med cybersikkerhed pragmatisk ved først at skabe et simpelt overblik over de mest forretningskritiske IT- og OT-systemer og derefter fokusere indsatsen dér, hvor et nedbrud vil få størst konsekvens for driften. I stedet for at starte med komplekse standarder kan man vælge at implementere de mest effektive basistiltag, såsom multifaktor-login, sikre og testede backups, løbende opdateringer samt grundlæggende adgangsstyring, da disse tiltag reducerer en stor del af de typiske trusler. Samtidig bør medarbejdere inddrages gennem enkel awareness, da de spiller en central rolle i den daglige sikkerhed. I produktionsvirksomheder er det desuden vigtigt at tænke IT og OT sammen, f.eks. ved at begrænse adgang til produktionssystemer og skabe adskillelse mellem netværk. Hvis virksomheden er underlagt compliance-krav, bør arbejdet struktureres med udgangspunkt i et simpelt framework og ledsages af nødvendig dokumentation, mens virksomheder uden sådanne krav med fordel kan fokusere mere direkte på risikoreduktion frem for dokumentation. Uanset udgangspunkt bør cybersikkerhed udvikles gradvist gennem små, prioriterede forbedringer, så der over tid opbygges en højere modenhed uden at overbelaste de begrænsede ressourcer. Tjek også værktøjer på www.cyber-smv.dk.

9. ***Hvad koster det?***

Cybersikkerhed opleves ofte som en omkostning, men bør i praksis forstås som risikostyring frem for klassisk afkast. For en produktions-SMV er de direkte omkostninger typisk relativt begrænsede og består primært af basale sikkerhedstiltag som multifaktor-login, backup, opdateringer og eventuel ekstern IT-support, mens den største omkostning ofte er organisatorisk prioritering frem for teknologi. Til gengæld kan konsekvenserne ved et cyberangreb være betydelige. Danske analyser viser f.eks., at et ransomwareangreb i gennemsnit kan koste omkring 376.350 kr. for SMV'er (SMVdanmark, 2026b). Samtidig har hver fjerde danske produktions-SMV oplevet en sikkerhedshændelse inden for de seneste par år (Stentoft et al., 2026), og op mod 60% af virksomhederne vurderer, at de ikke kan opretholde deres kerneforretning uden adgang til centrale IT-systemer (MSSB, 2026). Det indikerer, at de største omkostninger ofte

ligger i driftsforstyrrelser og tab af forretningskontinuitet frem for selve angrebet. Derudover peger danske rapporter på, at investeringer i cybersikkerhed ikke kun reducerer risiko, men også kan skabe konkurrencefordele og styrke virksomheders position i markedet (Dahl et al., 2024). Helt pragmatisk kan man arbejde med dette ved at tage udgangspunkt i få konkrete og realistiske scenarier, f.eks. et ransomwareangreb eller nedbrud i produktionen, og derefter groft estimere de økonomiske konsekvenser, såsom tabt omsætning ved et par dages produktionsstop. På den baggrund kan man sammenholde disse potentielle tab med omkostningen ved at implementere enkle sikkerhedstiltag som multifaktor-login, backup og opdateringer. Formålet er ikke at lave præcise beregninger, men at skabe et overblik over størrelsesforholdet mellem risiko og investering. Hvis en relativt lille investering kan reducere en potentiel stor konsekvens, giver det et klart beslutningsgrundlag for ledelsen. På den måde bliver cybersikkerhed gjort konkret og forretningsnær ved at synliggøre, hvad det faktisk kan koste virksomheden ikke at handle.

10. *Hvornår er vi gode nok?*

Udgangspunktet er her, at det ikke er eksakt videnskab. Vi vurderer, at en virksomhed er "god nok" på cybersikkerhed, når de mest forretningskritiske systemer er identificeret og er tilstrækkeligt beskyttet, og der samtidig er etableret en evne til hurtigt at gendanne driften i tilfælde af nedbrud eller angreb. Det indebærer også, at man har styr på adgangsstyring og håndtering af data, så uvedkommende ikke får adgang til kritiske informationer. For virksomheder, der er underlagt krav, vil det desuden være nødvendigt at kunne dokumentere, at relevante compliance-krav er opfyldt. Det centrale er dog, at modenhed inden for cybersikkerhed ikke handler om at opnå et perfekt sikkerhedsniveau, men om at have kontrol over de væsentligste risici og løbende arbejde med forbedringer i takt med virksomhedens udvikling.

7. Ny masteruddannelse i cybersikkerhed og risikostyring

Denne nye masteruddannelse på SDU blev udviklet som et direkte svar på et voksende behov i det danske samfund for fagfolk, der kan arbejde på tværs af de tekniske, organisatoriske og strategiske dimensioner af cybersikkerhed. Uddannelsen udsprang af det tværfaglige samarbejde etableret gennem dette forskningsprojekt, som samlede forskere fra SDU's Institut for Matematik og Datalogi, Center for War Studies og Institut for Erhverv og Bæredygtighed. Projektets samarbejde med danske virksomheder, brancheorganisationer og offentlige aktører afdækkede et betydeligt gab mellem eksisterende uddannelser indenfor cybersikkerhed og de kompetencer, som danske virksomheder i stigende grad har behov for i et miljø præget af digital afhængighed, geopolitisk ustabilitet, udvidet regulering og voksende cyberrisici.

Projektets samlede dataindsamling, som beskrevet tidligere, spillede en central rolle i at motivere og forme uddannelsen. Gennem spørgeskemaundersøgelser blandt danske virksomheder, workshops, fokusgrupper og direkte samarbejde med beslutningstagere og brancheaktører identificerede projektet flere tilbagevendende udfordringer. Disse omfattede begrænset bevidsthed om cybersikkerhed, vanskeligheder med at integrere cybersikkerhed i organisatoriske strategier, utilstrækkelige kompetencer inden for risikostyring og forretningskontinuitet samt mangel på personale, der effektivt kan kommunikere på tværs af tekniske og ledelsesmæssige områder. Projektet fremhævede også, hvordan cybersikkerhed i stigende grad rækker ud over rent tekniske problemstillinger og i stedet må forstås i relation til forsyningskæder, krisestyring, organisatorisk robusthed, regulatorisk compliance og geopolitisk usikkerhed. Disse resultater havde direkte indflydelse på uddannelsens struktur, pædagogiske tilgang og tematiske prioriteter.

Uddannelsen er derfor ikke blot designet som en teknisk cybersikkerhedsuddannelse, men som en tværfaglig uddannelse med fokus på at styrke robustheden i danske virksomheder og offentlige institutioner. Formålet er at uddanne fagfolk, der kan bygge bro mellem IT-specialister, ledelse og organisatoriske beslutningstagere. På den måde afspejler uddannelsen et bredere skifte inden for cybersikkerhed fra en snæver IT-funktion til en strategisk og organisatorisk disciplin forbundet med governance, driftskontinuitet og samfundsmæssig robusthed.

Uddannelsens struktur afspejler denne tværfaglige ambition. Første semester etablerer et fælles fundament blandt studerende med forskellige professio-

nelle baggrunde. Da uddannelsen optager både teknisk orienterede ansøgere og ansøgere fra organisatoriske, administrative eller politisk relaterede områder, følger de studerende suppleringskurser tilpasset deres tidligere erfaring. Studerende med teknisk baggrund tager kurser i strategisk organisation og optimering af forretningsprocesser, mens studerende fra erhverv, administration eller governance tager kurser i programmering, IT-systemer, computernetværk og cloud computing. Alle studerende gennemfører det fælles kursus *Principles of Cybersecurity*, som introducerer grundlæggende begreber som fortrolighed, integritet og tilgængelighed (CIA-triaden), risikobevidsthed og kommunikation af problemer m3ed cybersikkerhed på tværs af virksomheder.

Andet semester fokuserer på integrationen af teknisk cybersikkerhed og organisatorisk risikostyring. Kurser som *Threat Modelling* and *Risk Management* og *Company Security Architecture* giver de studerende praktiske og analytiske værktøjer til at identificere sårbarheder, vurdere trusler og udvikle sikkerhedsarkitekturer i overensstemmelse med organisatoriske mål. Fokus ligger ikke kun på teknologiske beskyttelsesmekanismer, men også på governance-strukturer, beslutningsprocesser og organisatorisk robusthed. Dette afspejler resultaterne fra forskningsprojektet, hvor deltagende virksomheder gentagne gange understregede behovet for medarbejdere, der både forstår operationelle sikkerhedsudfordringer og bredere forretningsmæssige konsekvenser.

Gennem tredje semester udvides uddannelsens tværfaglige profil yderligere gennem kurser i empiriske metoder, *Strategic Foresights* og specialiserede temaområder. De studerende kan specialisere sig i emner som robusthed i forsyningskæder, cyberkonflikter i gråzoner, etik og privatliv, sikker softwaredrift eller anvendt cybersikkerhed. Inkluderingen af *Strategic Foresights* og geopolitiske dimensioner afspejler endnu en central indsigt fra forskningsprojektet: Danske virksomheder opererer i stigende grad i en kontekst, hvor cyberrisici ikke kan adskilles fra bredere geopolitiske spændinger, forstyrrelser i globale forsyningskæder, hybride trusler og langsigtet strategisk usikkerhed. Uddannelsen søger derfor ikke blot at forberede kandidater til at reagere på aktuelle trusler, men også til at forudse og tilpasse sig nye udfordringer.

Et kendetegn ved uddannelsen er dens stærke fokus mod praksis og anvendt problemløsning. Uddannelsens design er blevet formet gennem løbende dialog med danske virksomheder og offentlige aktører involveret i forskningsprojektet. Som resultat prioriteres driftsmæssig relevans, tværfunktionel kommunikation og evnen til at implementere cybersikkerhedstiltag i organisationer. Kandidater forventes at udvikle kompetencer inden for sikkerhedsgovernance, hændelsesrespons, planlægning af forretningskontinuitet, trusselsmodellering og organisatorisk kommunikation samtidig med, at de kan arbejde med regulatoriske rammer som NIS2, GDPR og ISO 27001.

Uddannelsen repræsenterer i sidste ende et eksempel på forskningsdrevet uddannelsesudvikling tæt forbundet med samfundsmæssige behov. I stedet

for udelukkende at være designet ud fra eksisterende akademiske traditioner blev uddannelsen formet gennem empirisk samarbejde med danske virksomheder, brancheorganisationer og beslutningstagere i projektet. Resultatet er en masteruddannelse, der direkte adresserer dokumenterede kompetencegab i Danmark, og som søger at styrke kapaciteten indenfor cybersikkerhed, organisatorisk robusthed og forretningskontinuitet på tværs af både private og offentlige sektorer. Uddannelsen gennemføres på engelsk.

8. Konklusion

Denne rapport viser tydeligt, at cybersikkerhed ikke længere kan betragtes som et isoleret teknisk anliggende, men må forstås som en strategisk og organisatorisk disciplin tæt forbundet med forsyningskæder, forretningskontinuitet og geopolitisk udvikling. For danske produktions-SMV'er er cybersikkerhed i stigende grad blevet en forudsætning for både driftssikkerhed, robusthed og konkurrenceevne i et globalt erhvervsmiljø præget af stigende kompleksitet og usikkerhed. Digitalisering, cloud computing og tæt integrerede forsyningskæder har skabt betydelige effektiviseringsmuligheder, men samtidig øget virksomhedernes eksponering over for cybertrusler, leverandørafhængigheder og geopolitiske forstyrrelser.

Projektets analyser og workshops dokumenterer, at mange SMV'er fortsat arbejder reaktivt med cybersikkerhed og ofte mangler både ressourcer, kompetencer og systematiske tilgange til risikostyring. Samtidig peger resultaterne på, at virksomhedernes største sårbarheder ikke nødvendigvis ligger i de enkelte tekniske systemer, men i de komplekse relationer og afhængigheder, som forbinder virksomheder med leverandører, kunder, IT-partnere og globale infrastrukturer. Særligt arbejdet med scenarier og Strategic Foresight har synliggjort, hvordan indirekte og kaskaderende effekter fra geopolitiske konflikter, klimaforandringer, cyberangreb og regulatoriske ændringer kan få alvorlige konsekvenser for danske SMV'ers drift og forretningskontinuitet.

Rapporten understreger derfor nødvendigheden af et paradigmeskifte fra et snævert internt sikkerhedsfokus mod et bredere supply chain resilience-perspektiv. Robusthed skabes ikke alene gennem tekniske sikkerhedsforanstaltninger, men gennem organisatorisk læring, tværfunktionelt samarbejde, systematisk risikostyring og evnen til at forudse og håndtere forstyrrelser på tværs af hele værdikæden. I denne sammenhæng fremhæves især betydningen af Business Continuity Management, scenarieplanlægning, leverandørstyring og udviklingen af dynamiske kapabiliteter såsom sensing, seizing og transforming.

Projektet viser samtidig, at arbejdet med cybersikkerhed ikke blot bør opfattes som compliance eller omkostning, men som en strategisk investering i virksomhedens modstandsdygtighed og langsigtede konkurrenceevne. Evnen til at demonstrere robusthed, sikkerhed og forretningskontinuitet bliver i stigende grad en konkurrenceparameter i både nationale og internationale forsyningskæder. Virksomheder, der formår at integrere cybersikkerhed og resiliens i deres strategiske arbejde, vil stå stærkere i mødet med fremtidige kriser og usikkerheder.

Endelig understreger rapporten behovet for styrket samarbejde mellem virksomheder, brancheorganisationer, myndigheder og uddannelsesinstitutioner. De identificerede kompetencegab og den stigende kompleksitet i cybertrusselsbilledet kræver nye tværfaglige kompetencer, hvor teknologisk forståelse kombineres med organisatorisk indsigt, risikostyring og strategisk beslutningstagning. Et konkret resultat af projektet er derfor udviklingen af den nye masteruddannelse i cybersikkerhed og risikostyring på SDU, som skal bidrage til at styrke Danmarks fremtidige kapacitet inden for cybersikkerhed, organisatorisk robusthed og forretningskontinuitet.

Samlet set peger rapporten på, at danske SMV'ers fremtidige robusthed afhænger af deres evne til at arbejde helhedsorienteret med cybersikkerhed, supply chain resilience og geopolitisk risikoforståelse. I en mere uforudsigelig og digitaliseret verden er resiliens ikke længere et supplement til forretningen – det er blevet en grundlæggende strategisk nødvendighed.

Referencer

AlDaajeh, S. & Alrabaee, S. (2024), "Strategic cybersecurity", *Computers & Security*, Vol. 141, 103845.

Ambulkar, S., Blackhurst, J. & Grawe, S. (2015), "Firm's resilience to supply chain disruptions: Scale development and empirical examination", *Journal of Operations Management*, Vol. 33-34, pp. 111-122.

Bestyrelsesforeningen (2022), *Cybersikkerhed for bestyrelse og direktion: Vejledning og anbefalinger til styrkelse af strategiske cyberkompetencer (V4.0)*, https://kromannreumert.com/files/media/document/Cyber_Bestyrelsesvejledning-December%202022_0.pdf (tilgået 8. april, 2026).

Boyson, S. (2014), "Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems", *Technovation*, Vol. 34 No. 7, pp. 342-353.

Button, D.J., Ophoff, J., Irons, A. & McDonald, S. (2025), "Mind the gap: Exploring perceptions of cyber security in the SME context", *Information and Computer Security*, Early Cite.

Capparelli, J., Chionna, G. & Riglietti, G. (2022), "What makes for effective business continuity implementation?", *Journal of Business Continuity & Emergency Planning*, Vol. 15 No. 4, pp. 302-311.

Chotia, V., Khoualdi, K., Broccardo, L. & Yaqub, M.Z. (2025), "The role of cyber security and digital transformation in gaining competitive advantage through Strategic Management Accounting", *Technology in Society*, Vol. 81, 102851.

Christopher, M. & Peck, H. (2004), "Building the resilient supply chain," *The International Journal of Logistics Management*, Vol. 15 No. 2, pp. 1-14.

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., Kogan Page, 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.

Dahl, A.M., Taarnborg, R., Astrupgaard, C. & Pommerencke-Vilmand, L. (2024), *Cyberbarometer 2024: Cybersikkerhed & konkurrencefordele blandt danske SMV'er*, Analyse & Tal F.M.B.A, København NV.

de Araújo Lima, P.F., Crema, M. & Verbano, C. (2020), "Risk management in SMEs: A systematic literature review and future directions", *European Management Journal*, Vol. 38 No. 1, pp. 78-94.

ENISA (European Union Agency for Cybersecurity) (2023), *ENISA Threat Landscape 2023*, Brussels, Belgium.

Eryarsoy, E, Torgalöz, A.Ö., Acar, M.F. & Zaim, S. (2022), "A resource-based perspective of the interplay between organizational learning and supply chain resilience", *International Journal of Physical Distribution & Logistics Management*, Vol. 52 No. 8, pp. 614-637.

European Commission (2026), *NIS2 Directive: Securing Network and Information Systems*, https://digital-strategy.ec.europa.eu/en/policies/nis2-directive?utm_source=chatgpt.com (tilgået den 8. april, 2026).

Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D. & Levallet, N. (2023), "Evaluating the adoption of cybersecurity and its influence on organizational performance", *SN Business & Economics*, Vol. 3, article 97.

Heidt, M., Gerlach, J.P. & Buxmann, P. (2019), "Investigating the security divide between SME and large companies: How SME characteristics influence organizational IT security investments", *Information Systems Frontiers*, Vol. 21, pp. 1285-1305.

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

Jazairy, A., Brho, M., Manuj, I. and Goldsby, T.J. (2024), "Cyber risk management strategies and integration: toward supply chain cyber resilience and robustness", *International Journal of Physical Distribution & Logistics Management*, Vol. 54 No. 11, pp. 1-29.

Junior, C.R., Becker, I. & Johnson, S.D. (2025), "Unaware, unfunded, untrained and unsupported: A systematic review of SME cybersecurity", *Journal of Cyber Security*, 1–31. doi: 10.48550/arXiv.2309.17186.

Jüttner, U. & Maklan, S. (2011), "Supply chain resilience in the global financial crisis: An empirical study", *Supply Chain Management: An International Journal*, Vol. 16 No. 4, pp. 246-259.

Latsiou, A. & Lambrinoudakis, C. (2026), "Cyber supply chain risk management: From threats to treatment", *International Journal of Information Security*, Vol. 25 article 40.

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

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

MSSB (Ministeriet for Samfundssikkerhed og Beredskab) (2026), https://mssb.dk/nyheder/nyhedsarkiv/2025/februar/markant-behov-for-at-styrke-smvernes-digitale-sikkerhed/?utm_source=chatgpt.com (tilgået 8. april, 2026).

Munich RE (2024), *Munich Re Global Cyber Risk and Insurance Survey 2024: Bridging the gap in cyber protection*, Münchener Rückversicherungs-Gesellschaft, München.

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.

O'Reilly, C.A. & Tushman, M.L. (2004), "The ambidextrous organization", *Harvard business Review*, Vol. 82 No. 4, pp. 74-81.

Ponomarov, S.Y. & Holcomb, M.C. (2009), "Understanding the concept of supply chain resilience", *The International Journal of Logistics Management*, Vol. 20 No. 1, pp. 124-143.

PwC (2026), *New World, New Rules: Cybersecurity in an Era of Uncertainty: 2026 Global Digital Trust Insights: C-suite Playbook and Findings*, PwC United States.

Rose, S., Borchert, O., Mitchell, S. & Connelly, S. (2020), *Zero Trust Architecture (NIST Special Publication 800-207)*, National Institute of Standards and Technology, Gaithersburg, MD.

Sheffi, Y. & Rice, J.B. Jr. (2005), "A supply chain view of the resilient enterprise", *MIT Sloan Management Review*, Vol. 47 No. 1, pp. 41-48.

SMVdanmark (2026a), https://smvdanmark.dk/analyser/temaanalyser/smver-er-rygraden-i-dansk-erhvervsliv, tilgået 6. april, 2026.

SMVdanmark (2026b), https://smvdanmark.dk/analyser/temaanalyser/cyberangreb-kan-blive-en-dyr-omgang-for-smverne?utm_source=chatgpt.com, tilgået 8. april, 2026.

Stentoft, J. & Haug, A. (2019), *Business Process Optimisation*, Hans Reizels Forlag, København K.

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

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

Stentoft, J., Keating, V., Tumchewics, L., Peressotti, M., Mayer, P., Kankam-Boateng, L., Schmitt, O., Theussen, A., Mikkelsen, O.S. & Wickstrøm, K.A. (2025), *Cybersikkerhed og Forretningskontinuitet i små og mellemstore danske produktionsvirksomheder: Indsigter fra første iteration med virksomhedsinddragelse*, Institut for 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. & 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., 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.

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.

Tetteh, A.K. (2024), "Cybersecurity needs for SMEs", *Issues in Information Systems*, Vol. 25 No. 1, pp. 235-246.

Tukamuhabwa, B.R., Stevenson, M., Busby, J. & Zorzini, M. (2015), "Supply chain resilience: Definition, review and theoretical foundations for further study", *International Journal of Production Research*, Vol. 53 No. 18, pp. 5592-5623.

von Solms, R. & van Niekerk, J. (2013), "From information security to cyber security", *Computers & Security*, Vol. 38, pp. 97-102.

Wieland, A. & Wallenburg, C.M. (2013), "The influence of relational competencies on supply chain resilience: a relational view", *International Journal of Physical Distribution & Logistics Management*, Vol. 43 No. 4, pp. 300-320.

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.

Appendix 1: Spørgeramme til IT- og cybersikkerhed

Spørgerammen til IT-sikkerhed og cybersikkerhed er lavet til et eksternt IT-hus.

1. Overordnet sikkerhedsstrategi og ansvar
Formål: Afklare roller, ansvar og modenhed.

1. Hvilke sikkerhedsstandarder arbejder I efter? (f.eks. ISO 27001, CIS Controls, NIST CSF)
2. Har I en dokumenteret informationssikkerhedspolitik?
3. Hvem har det overordnede ansvar for vores sikkerhed hos jer?
4. Hvordan adskiller I ansvar mellem jer og os? (ansvarsfordelingsmatrix)
5. Har I en dokumenteret risikovurdering for vores setup?
6. Hvordan håndterer I sikkerhed i forhold til både kontor-IT og produktions-IT (OT)?

2. Adgangsstyring og brugerrettigheder
Formål: Minimere risikoen for uautoriseret adgang.

1. Anvendes multifaktor-login (MFA) på:
    a. E-mail?
    b. VPN?
    c. Serveradgang?
    d. Admin-konti?
2. Hvordan håndteres oprettelse og lukning af brugere?
3. Hvor hurtigt lukkes adgange ved fratrædelse?
4. Har I princippet om "mindst mulige rettigheder" implementeret?
5. Overvåges administrative handlinger?
6. Hvordan sikres fjernadgang til vores miljø?

3. Backup og gendannelse (kritisk for produktion)
Formål: Sikre drift ved ransomware eller nedbrud.

1. Hvor ofte tages backup?
2. Er backup:
    a. Krypteret?

    b. Adskilt fra driftsmiljøet?
    c. Beskyttet mod ransomware (immutable/offline backup)? (*Immutable (uforanderlig) og offline backup er en databeskyttelsesmetode, hvor sikkerhedskopier låses i en skrivebeskyttet tilstand i en bestemt periode*).
3. Hvor opbevares backup fysisk/geografisk?
4. Hvornår er backup sidst testet ved en reel restore-test? (*En reel restore-test (gendannelsestest) er en kontrolleret proces, hvor man faktisk gendanner data fra en backup for at verificere, at dataene ikke er korrupte, og at de kan bruges i virkelige scenarier*).
5. Hvor lang tid tager det at genskabe:
    a. Servere?
    b. Produktionssystemer?
    c. Økonomisystem?
6. Hvad er vores:
    a. RPO (Recovery Point Objective - genopretningspunktsmål) - hvor meget data man maksimalt kan tåle at miste)?
    b. RTO (Recovery Time Objective) - målsætning for genopret ningstid - hvor hurtigt det skal være oppe at køre igen.

4. Overvågning og trusselsdetektion
Formål: Opdage angreb tidligt.

1. Har vi aktiv overvågning (24/7)?
2. Anvender I EDR/XDR på vores enheder? (*EDR (End point Detection and Response) og XDR (Extended Detection and Response) er avancerede cybersikkerhedsløsninger designet til at opdage, undersøge og reagere på moderne trusler, som traditionel antivirus ofte misser*). *EDR fokuserer specifikt på at overvåge og beskytte "endpoints" - altså enheder som bærbare computere, servere og telefoner. XDR er en udvidelse af EDR, der samler data fra flere sikkerhedslag (netværk, cloud, e-mail, identitet) i én samlet løsning for et holistisk overblik*.
3. Overvåges netværkstrafik?
4. Hvordan opdager I ransomware?
5. Hvor hurtigt reagerer I ved mistænkelig aktivitet?
6. Får vi besked ved sikkerhedshændelser – og hvordan?

5. Patch management og opdateringer
Patch management er en struktureret proces til at identificere, teste og installere opdateringer (patches) på software, operativsystemer og enheder.
Formål: Lukke kendte sårbarheder.

1. Hvor ofte opdateres:
    a. Servere?
    b. PC'er?

    c. Firewall?
    d. Produktionsudstyr?
2. Hvor hurtigt patches kritiske sårbarheder?
3. Hvordan håndteres opdateringer i produktionen, så drift ikke påvirkes?
4. Overvåger I aktivt for nye kritiske sårbarheder?

6. Netværkssikkerhed (særligt vigtigt for produktion)
Formål: Beskytte produktionsmiljøet (OT – Operational Technology).

1. Er vores netværk segmenteret?
    a. Er produktion adskilt fra kontor-IT?
2. Hvilken firewall anvendes?
3. Er der IDS/IPS aktiveret? *IDS (Intrusion Detection System) og IPS (Intrusion Prevention System) er cybersikkerhedsværktøjer, der overvåger netværkstrafik for ondsindet aktivitet*.
4. Er der adgang direkte fra internettet til produktionsudstyr? IDS Overvåger og analyserer netværkstrafik for mistænkelige mønstre eller kendte trussels-signaturer. IPS Overvåger trafikken i realtid og sammenligner den med en database over trusler.
5. Hvordan sikres leverandøradgang til maskiner?

7. E-mail og phishing-beskyttelse
Formål: Reducere den mest almindelige angrebsvej.

1. Har vi avanceret spam- og phishing-beskyttelse?
2. Er DMARC, SPF og DKIM korrekt opsat? *DMARC, SPF og DKIM er tre supplerende tekniske sikkerhedsstandarder, der bruges til at autentificere e-mails, forhindre spoofing (falske afsendere) og beskytte mod phishing og spam*.
3. Simulerer I phishing-tests?
4. Tilbyder I awareness-træning til medarbejdere?

8. Incident response og beredskab
Formål: Vide, hvad der sker, når noget går galt.

1. Har I en dokumenteret beredskabsplan?
2. Har vi en incident response-plan?
3. Hvem kontakter hvem ved et angreb?
4. Har I erfaring med ransomware-håndtering?
5. Har I cyberforsikring?
6. Samarbejder I med ekstern sikkerhedspartner ved større angreb?

9. Hosting og datacenter
Formål: Sikre, at hostingmiljøet er robust.

1. Hvor hostes vores data (land/region)?
2. Hvilken compliance er datacentret certificeret efter?
3. Er data krypteret:
    a. I transit?
    b. I hvile?
4. Hvem har fysisk adgang til serverne?
5. Er der redundans (strøm, netværk, hardware)?

10. Compliance og lovgivning (Danmark/EU)
Formål: Undgå regulatoriske risici.

1. Er vi korrekt dækket ift. GDPR?
2. Har I databehandleraftale klar?
3. Er der underdatabehandlere?
4. Kan vi få dokumentation til revisor?
5. Er vi omfattet af NIS2, og hvordan hjælper I os?

11. Kontrakt og SLA
Formål: Sikre klare forpligtelser.

1. Hvad er jeres garanterede responstid?
2. Er der defineret sikkerhedsniveau i kontrakten?
3. Hvad er jeres ansvar ved sikkerhedsbrud?
4. Er der bod eller kompensation ved alvorlige fejl?
5. Kan vi få dokumenteret sikkerhedsrapport kvartalsvis?

12. Strategiske spørgsmål (modenhed og fremtidssikring)

1. Hvordan vurderer I vores nuværende sikkerhedsniveau?
2. Hvor er vores største risiko?
3. Hvad vil I anbefale som næste investering?
4. Hvad koster et realistisk "minimum forsvar" for en produktions-SMV?
5. Hvordan beskytter vi os konkret mod ransomware i produktionen?

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: Klik her.

Projektejer: Erhvervshus Midtjylland.

Projekthjemmeside: Klik her.

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: Food & Bio Cluster Denmark.

Projekthjemmeside: Klik her.

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: Odense Robotics.

Projekthjemmeside: Klik her.

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: CBS

Projekthjemmeside: Klik her.

INDUSTRIENS FOND
SDU
FORSVARSAKADEMIET