CYBERSIKKERHED OG FORRETNINGSKONTINUITET

Cybersikkerhed i små og mellemstore danske produktionsvirksomheder

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

Juni 2024

FORSVARSAKADEMIET

INDUSTRIENS FOND

SDU Syddansk Universitet

Cybersikkerhed i små og mellemstore danske produktionsvirksomheder

ISBN: 978-87-94345-93-4

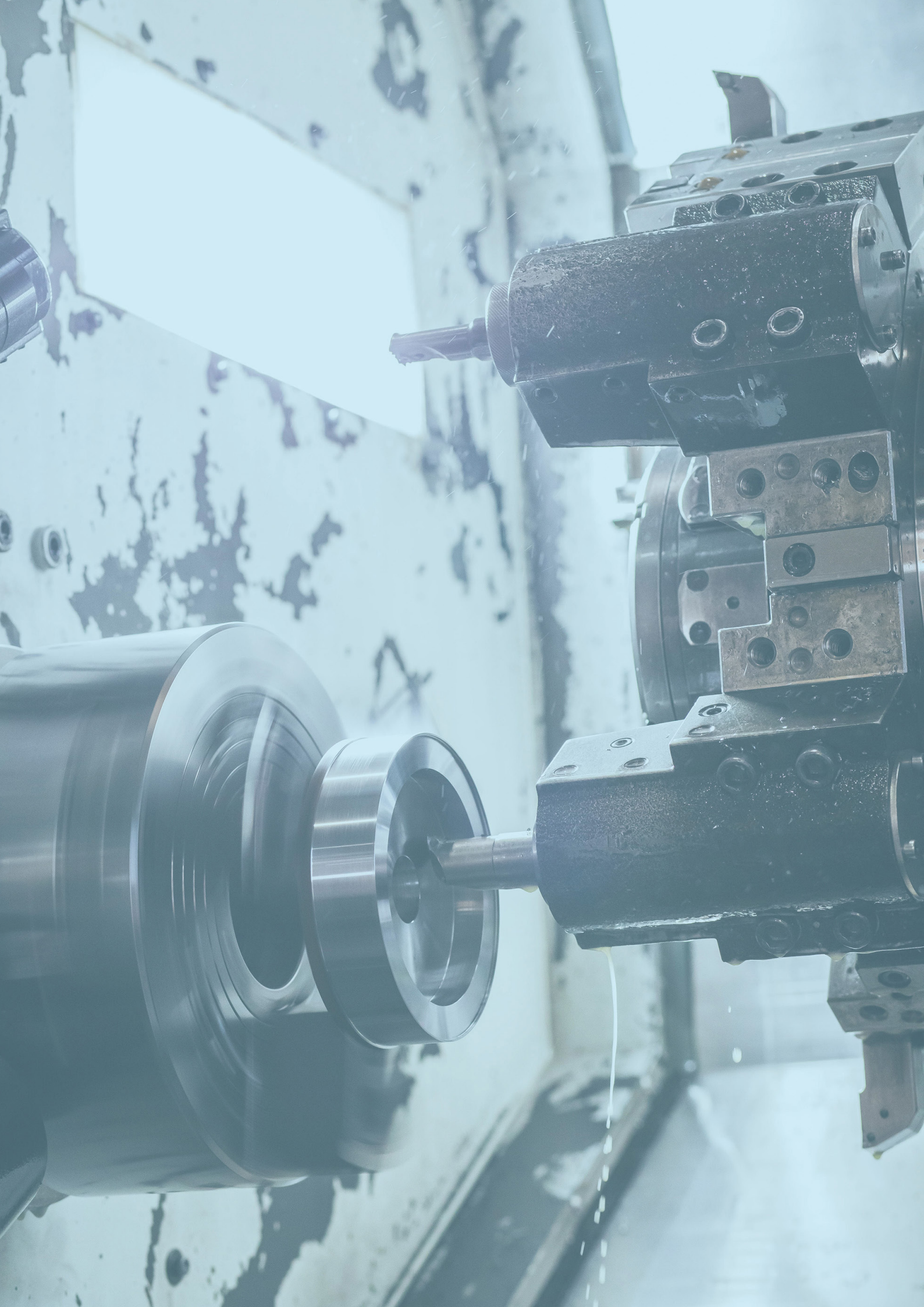
Korrektur og opsætning:
Tina Højrup Kjær, Tekst og Web

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



Resumé

Denne rapport behandler resultaterne af en landsdækkende spørgeskemaundersøgelse, der har fokus på danske små og mellemstore produktionsvirksomheders praksis med cybersikkerhed. I alt har 248 virksomheder deltaget i undersøgelsen. Specifikt søger rapporten svar på ni overordnede spørgsmål:

1. Hvilke krav til cybersikkerhed og brug af standarder oplever virksomhederne?
2. I hvilket omfang har virksomhederne oplevet cyberangreb?
3. I hvilken grad opleves cybersikkerhed som en kvalifikator?
4. Hvor opmærksomme er virksomhederne på cybersikkerhed?
5. I hvilket omfang har virksomhederne fokus på cybersikkerhed supply chain risk management?
6. I hvilket omfang har de deltagende virksomheder en supply chain orientering?
7. I hvilket omfang er virksomhederne internt integreret?
8. I hvilket omfang har virksomhederne fokus på geopolitik?
9. Hvorledes har virksomhederne balanceret drifts- og udviklingsopgaver?

Krav til cybersikkerhed og brug af standarder

Resultaterne af spørgsmål om hvilke krav, der er til cybersikkerhed, viser, at bestyrelsen spiller en vigtig rolle i at få arbejdet med cybersikkerhed igangsat med et gennemsnit på 3,43 på en fem-punkts Likert-skala, hvor 1 = i meget lav grad og 5 = i meget høj grad. Imidlertid udtrykker gennemsnitsværdien på 3,43 ikke et særligt stærkt fokus fra bestyrelsen på trods af den massive opmærksomhed, der er rettet på denne problemstilling i medierne de seneste år. Endnu lavere gennemsnit opnås ved krav fra investorer med et gennemsnit på 2,91 og fra kunder på 2,55. Hvad angår krav om brug af standarder indenfor cybersikkerhed svarer 17 procent af deltagerne, at de stilles sådanne krav. Eksempler på standarder er NIST I&II, ISO27001/27002, CMMC og GDPR. 18 procent af respondenterne svarer, at de frivilligt har valgt at følge standarder indenfor cybersikkerhed, som f.eks. D-mærket, NIS2, Cyber Resilience Act og Cyber Security Act.

Cyberangreb

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

Cybersikkerhed som en kvalifikator

Respondenterne ser cybersikkerhed som en kvalifikator til at drive virksomheden med et gennemsnit på 3,44 på en fem-punkts Likert-skala. Dette indikerer, at cybersikkerhed kan styrke virksomhedens image. I forhold til leverandører stiller virksomhederne ikke de store krav til cybersikkerhed, idet der her kun opnås et gennemsnit på 2.01. Dette indikerer, at den nuværende cybersikkerhedspraksis primært er fokuseret mod det interne virksomhedsperspektiv, og i meget begrænset omfang har fokus på forsyningskæderne.

Opmærksomhed på cybersikkerhed

Undersøgelsen viser, at respondenterne i stor grad er opmærksomme på cybersikkerhed, idet tre gennemsnitsværdier ud af fem scorer over 4,2. Disse gennemsnitsværdier viser, at respondenterne forstår, at det er afgørende at følge sikkerhedspraksisser for at beskytte sig mod cyberangreb med et gennemsnit på 4,32, at de anerkender, at de skal træffe sikkerhedsforanstaltninger for at beskytte sig mod cyberangreb med et gennemsnit på 4,29, og at de er bevidste om, at sikkerhedspraksisser er nødvendige for at kunne håndtere cybertrusler og -risici med et gennemsnit på 4,23.

Cybersikkerhed supply chain risk management

Denne undersøgelse indeholder spørgsmål om konkret praksis med cybersikkerhed supply chain risk management, hvilket er en ny begrebsdannelse, hvor der til dato kun foreligger sparsom empiri. Respondenterne er blevet bedt om at tage stilling til ti udsagn omkring cybersikkerhed supply chain risk management og resultatet viser, at kun ét udsagn opnår en gennemsnitsværdi omkring 3,0 (i nogen grad), mens de øvrige ligger med gennemsnit mellem 3,0 og 2,0. Det højeste gennemsnit er på 3,08 og handler om, at leverandører er kendte og prioriterede efter, hvor kritiske de er. Det samlede resultat peger på et stort udviklingsbehov i virksomhederne til at anlægge et supply chain fokus på cybersikkerhed.

Supply chain orientering

Respondenterne har også skullet tage stilling til en række udsagn omkring virksomhedens supply chain orientering, dvs. i hvilken grad, virksomheden forstår de strategiske implikationer af aktiviteter og processer, der er involveret i de forskellige flows i forsyningskæderne. Supply chain orientering er målt på ti udsagn, hvoraf fem opnår gennemsnit fra 3,52 op til 3,85, hvilket indikerer en generel god supply chain orientering. Dette vedrører f.eks. samarbejde med nøglepartnere, performanceforbedring gennem samarbejde og etablering af langvarige relationer. Det er positivt, at der opnås et samlet gennemsnit på 3,40 for de ti udsagn om supply chain orientering. Det er et godt

udgangspunkt for at styrke arbejdet med cybersikkerhed supply chain risk management, som, undersøgelsen viser, er på at relativt lavt niveau.

Intern integration

Det er vigtigt, at cybersikkerhed er godt forankret tværorganisatorisk i virksomhederne, da det er et anliggende for alle medarbejdere. Man er f.eks. kun ét forkert klik væk fra et angreb (Ekmann, 2022). Derfor har det været interessant at undersøge respondenternes opfattelse af, hvor internt integrerede deres virksomheder er. Her er det brugt 11 udsagn til at belyse den interne integration. Der opnås generelt høje gennemsnitsværdier for den interne integration fra 3,52 til 4,03, hvilket er et meget positivt udgangspunkt til at styrke arbejdet med cybersikkerhed. Den samlede gennemsnitsværdi for de 11 udsagn er på 3,75, hvilket indikerer, at det synes at være lykkedes med at få bugt med en udpræget silokultur, hvor der sker suboptimeringer indenfor de respektive funktioner i virksomheden.

Fokus på geopolitik

60 procent af respondenterne svarer, at de har fokus på geopolitiske forhold i deres måde at drive virksomheden på. Sådanne forhold er f.eks. relateret til markeder og kunder, sourcing, lagring, risikostyring og geografisk spredning. Imidlertid er det bemærkelsesværdigt, at 40 procent ikke har fokus på geopolitiske forhold, hvilket indikerer et udviklingsbehov for nye ledelsesmæssige agendaer, der eksplicit sætter fokus på geopolitik. Respondenterne har haft mulighed for at beskrive deres kilder til geopolitiske forhold og har f.eks. her angivet brancheforeninger, Dansk Industri, kunder, leverandører og Udenrigsministeriet. På spørgsmålet om, hvorvidt geopolitiske risici påvirker virksomhedernes forretninger, opnås der et gennemsnit på 3,33, hvilket igen indikerer et udviklingsbehov. 45 procent svarer, at de er påvirket af lovgivning fra andre lande som f.eks. GDPR, lægemiddellovgivning, hvidvasklovgivning, EU-sanktioner og NIS2.

Drift og udvikling

At sikre en virksomheds cybersikkerhed kræver, at der prioriteres ressourcer til arbejdet. Et sådant udviklingsarbejde sker i skarp konkurrence med dagligе driftsopgaver. Respondenterne har derfor skullet tage stilling til en række udsagn om både drifts- og udviklingsopgaver. De seks udsagn om driftsorientering opnår gennemsnit fra 3,44 til 4,10 og lander samlet på 3,74, mens de seks udsagn om udviklingsopgaver opnår gennemsnit fra 3,13 til 3,54 med et samlet gennemsnit på 3,30. Det svarer til tidligere undersøgelser, hvor driftsopgaverne opnår de højeste gennemsnit. Dette er også naturligt, fordi det er den daglige drift, der skaber den nødvendige omsætning. Men bevidstheden om, at udvikling er nødvendig for at sikre langsigtet overlevelse, er vigtig at være opmærksom på. I arbejdet med cybersikkerhed er det således vigtigt at være opmærksom på det dilemma, der kan være mellem drift og udvikling.

Forord Industriens Fond

Danske virksomheder handler og samarbejder i stort omfang med deres kunder og leverandører – herhjemme såvel som globalt. Samhandelen og den tiltagende digitalisering betyder, at virksomhederne i dag er meget tæt sammenkoblede. Både i den fysiske verden og i cyberspace.

Halvfabrikater, sensorer og serviceydelser fra eksterne leverandører bruges i stor stil i danske produkter og produktionsanlæg. Og det samme gælder den modsatte vej, hvor løsninger fra danske virksomheder benyttes af kunder i hele verden.

Den omfattende og tætte integration – hvor data og knowhow flyder frem og tilbage – er en god ting og gør det muligt for virksomhederne at skabe konkurrencedygtige forretningsmodeller og levere markedsledende produkter af høj kvalitet.

Men der er et aber dabei. De tætte bånd i værdikæderne betyder, at danske virksomheder skal være ekstra vågne og ekstra varsomme. En kæde er jo aldrig stærkere end det svageste led, og er der bøvl med sikkerheden hos en leverandør, så smitter det hurtigt. Derfor er koblingen af cybersikkerhed og værdikæder afgørende.

Virksomheder bør ikke betragte cybersikkerhed som en lokal opgave, der kan håndteres inden for egne fire vægge. Det er naturligvis godt at have styr på sikkerheden i egen butik og produktportefølje. Men det kan ikke stå alene. I en verden, hvor virksomheder bindes tæt sammen via internettet, er cybersikkerhed derfor i høj grad noget, der også skal håndteres gennem værdikædesamarbejder.

Det er en svær øvelse, og i disse år ser vi desværre, at flere og flere hacker-angreb kommer via værdikæderne og andre samarbejdsrelationer. Dermed kan et hullet sikkerhedsværn hos én virksomhed hurtigt blive de cyber-kriminelles springbræt ind i systemerne hos vigtige leverandører og store kunder.

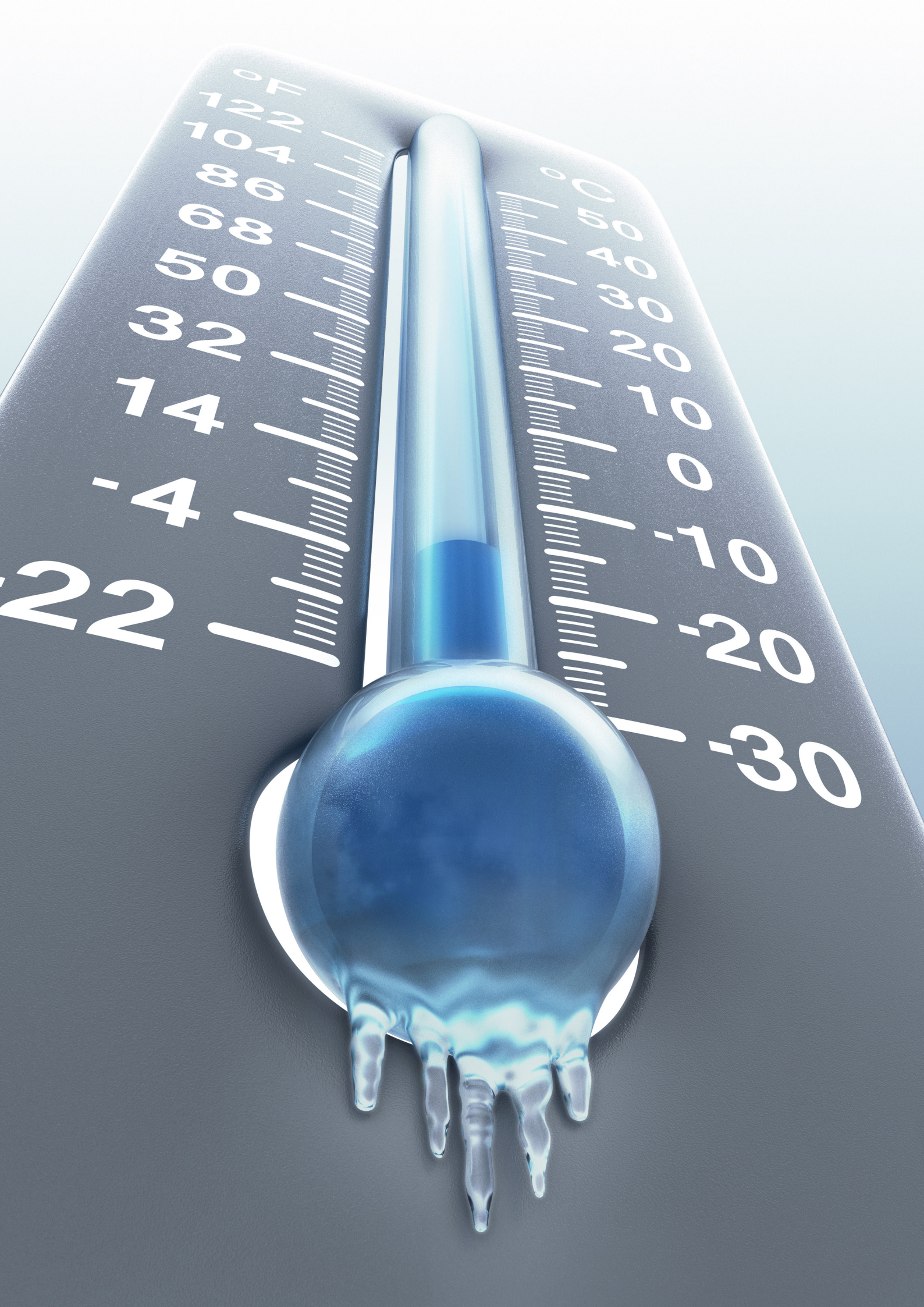
Nærværende rapport ser nærmere på lige præcis ovennævnte sammenhænge. Rapporten udspringer af projektet *Cybersikkerhed og Forretningskontinuitet*, der er ét af i alt fem initiativer, vi igangsatte sidste år, med fokus på netop cybersikkerhed i værdikæden og konsekvenserne for små og mellemstore virksomheder.

Selvom rapporten viser, at der fortsat er lang vej igen i forhold til at cybersikre danske virksomheders værdikæder, så tillader jeg mig at fokusere på nogle af rapportens positive observationer. For eksempel angiver virksomhederne i undersøgelsen, at de anser cybersikkerhed som en kvalifikator i forhold til at kunne operere på markedet, og som derved er noget, der styrker virksomhedens image. Og undersøgelsen viser også, at virksomhederne er opmærksomme på, at cybersikkerhed skal højt op på agendaen, at det er vigtigt at træffe sikkerhedsforanstaltninger, og at det er af afgørende betydning at følge sikkerhedspraksisser.

På den baggrund håber jeg, at bevægelsen mod højere cybersikkerhed i dansk erhvervsliv accelereres. Der er rigeligt at tage fat på, og det kan gøres på mange forskellige måder. Men det vigtigste er at komme i gang med det samme og starte dialogen med sine samarbejdspartnere om cybersikkerhed.

God læselyst!

Malene Stidsen
Programchef
Industriens Fond


°F
12
10
8
6
5
3
14
-4
22
°C
50
40
30
20
10
0
-10
-20
-30

Forfatternes forord

Denne rapport har til formål at tage temperaturen på danske små og mellemstore virksomheders (SMV'er) praksis med at sikre cybersikkerhed.

Cybersikkerhed er afgørende for SMV'er af flere grunde. For det første bliver SMV'er i stigende grad mål for cyberkriminelle, som ofte opfatter dem som lettere mål sammenlignet med større virksomheder med mere robuste sikkerhedsforanstaltninger. En sådan sårbarhed kan føre til betydelige økonomiske tab samt dyre produktionstab. Samtidig kan SMV'er være attraktive for hackere, da de via SMV'ernes systemer eller produkter måske kan opnå adgang til de større virksomheders systemer. Derudover håndterer SMV'er ofte følsomme kundedata og forretningsoplysninger, som, hvis de bliver kompromitteret, kan skade deres omdømme og udhule kundernes tillid. For det andet bliver lovkravene stadig mere strenge, hvilket kræver, at SMV'er overholder databeskyttelseslove som f.eks. GDPR. Manglende overholdelse kan resultere i store bøder og juridiske konsekvenser, hvilket yderligere understreger behovet for robuste cybersikkerhedspraksisser. Investering i cybersikkerhed øger også en SMV's samlede modstandsdygtighed, hvilket gør det muligt for dem at opretholde forretningskontinuitet i lyset af cybertrusler og reducere risikoen for driftsforstyrrelser. For det tredje har den stigende afhængighed af digitale værktøjer og online platforme udvidet SMV'ers angrebsflade, hvilket gør cybersikkerhed til en væsentlig del af deres operationelle strategi. Beskyttelse af digitale aktiver og sikring af integriteten og tilgængeligheden af online tjenester er afgørende for at opretholde forretningsdriften og den medfølgende konkurrencefordel. Der er således vigtige argumenter for, at SMV'er øger deres indsigt i og praksis med cybersikkerhed i et forsyningskædeperspektiv.

Der rettes en stor tak til alle respondenterne i undersøgelsen. Jeres tid og svar er meget værdsat i vores bestræbelser på at skabe ny viden om cybersikkerhed blandt danske produktions SMV'er. Der rettes ligeledes en stor tak til Industriens Fond for økonomiske midler til at gennemføre projektet om Cybersikkerhed og Forretningskontinuitet (www.cyber-smv.dk), som denne spørgeskemaundersøgelse er en delleverance af. Endelig skal der rettes en stor tak til kommunikationskonsulent Tina Højrup Kjær, Tekst og Web for korrekturlæsning, redigering og opsætning.

Jan Stentoft, Ole Stegmann Mikkelsen, Olivier Schmitt, Vincent Keating, Amelie Theussen, Marco Peressotti, Peter Mayer, Judith Kankam-Boateng og Louise Tumchewics - Juni 2024.

1. Introduktion

1.1 Baggrund

Omgivelserne for danske produktions SMV'er er under kraftig forandring. Vi er gået fra en lang periode med et lavt niveau af internationale konflikter til et mere konfliktfyldt niveau, hvor USA spiller en vigtig rolle blandt vestlige allierede, og hvor fokus på kritisk infrastruktur har fået en ny strategisk vigtighed. Den digitale økonomis opståen har skabt nye sårbarheder for danske produktions SMV'er. De er ofte afhængige af eksport for at vækste deres forretning, hvorfor geopolitiske kriser som supply chain forstyrrelser og restriktioner til markedsadgang (i tilfælde af internationale sanktioner) vil få større konsekvenser for dem. Yderligere er SMV'er særligt sårbare overfor cyberangreb som tyveri af IPR, sabotage og ransomware. Ny forskning afslører mangel på viden om cybersikkerhed blandt danske produktions SMV'er, samt at der mangler viden om cybersikkerhed i et forsyningskædeperspektiv (Stentoft et al, 2023a, p. 103). Også det nye EU NIS2-direktiv indeholder strengere krav om cybersikkerhed til virksomheder, som også omfatter danske produktions SMV'er.

Virksomheder i dag, herunder SMV'er, er stærkt afhængige af IT både til håndtering af interne processer og kommunikation, men også i forbindelse med outsourcing og samhandel med eksterne partnere, leverandører og kunder. IT-teknologi og internettet – og den brede anvendelse heraf – har gjort interaktionen, koordineringen og integrationen med omgivelserne både nemmere, hurtigere og billigere. Dog indebærer dette også en stadigt tiltagende, øget eksponering overfor cybertrusler. Den geopolitiske udvikling øger ligeledes risikoen for cyberangreb fra såvel stater som cyberkriminelle (ransomware, industrispionage, terrorisme osv.). Vi har således set, hvordan både store virksomheder og SMV'er har været udsat for f.eks. ransomware, som har gjort det umuligt at opretholde produktionen og levering af produkter og services med store tab til følge. Performancetabet er ikke isoleret til den enkelte virksomhed. Det påvirker også kundernes performance negativt og dermed performance for downstream supply chain. Lige så kritisk er tabet af troværdighed overfor nuværende og potentielle kunder – en konsekvens, der kan være direkte ødelæggende for virksomhederne (Stentoft et al., 2023b). Et styrket niveau indenfor cybersikkerhed og en øget opmærksomhed på sårbarhedsrisici bør altså ikke anses som en omkostning for SMV'erne, men en investering i at (ved)blive at være en attraktiv og sikker samarbejdspartner i ens supply chain netværk – på linje med god kvalitet, fokus på miljø og social ansvarlighed. Cybersikkerhed og konkurrencefordele går hånd i hånd (Dahl

et al., 2023, p. 8). Der er således behov for at tilføre SMV'er ny viden om sikkerhedsforanstaltninger som f.eks. adgangskontrol, autentificering, certificering af hard- og software, forebyggelse af forfalskning, databeskyttelse, firewall og gateway, reguleringer og standarder, leverandøraudits, interaktion og samarbejde med supply chain partnere, realtidsovervågning samt data backup.

1.2 Formål med undersøgelsen

Formålet med undersøgelsen er at afdække danske små og mellemstore produktionsvirksomheders praksis med cybersikkerhed. Denne viden vil indgå i udarbejdelsen af træningsforløb i cybersikkerhed for danske produktions SMV'er.

2. Teoretisk referenceramme

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

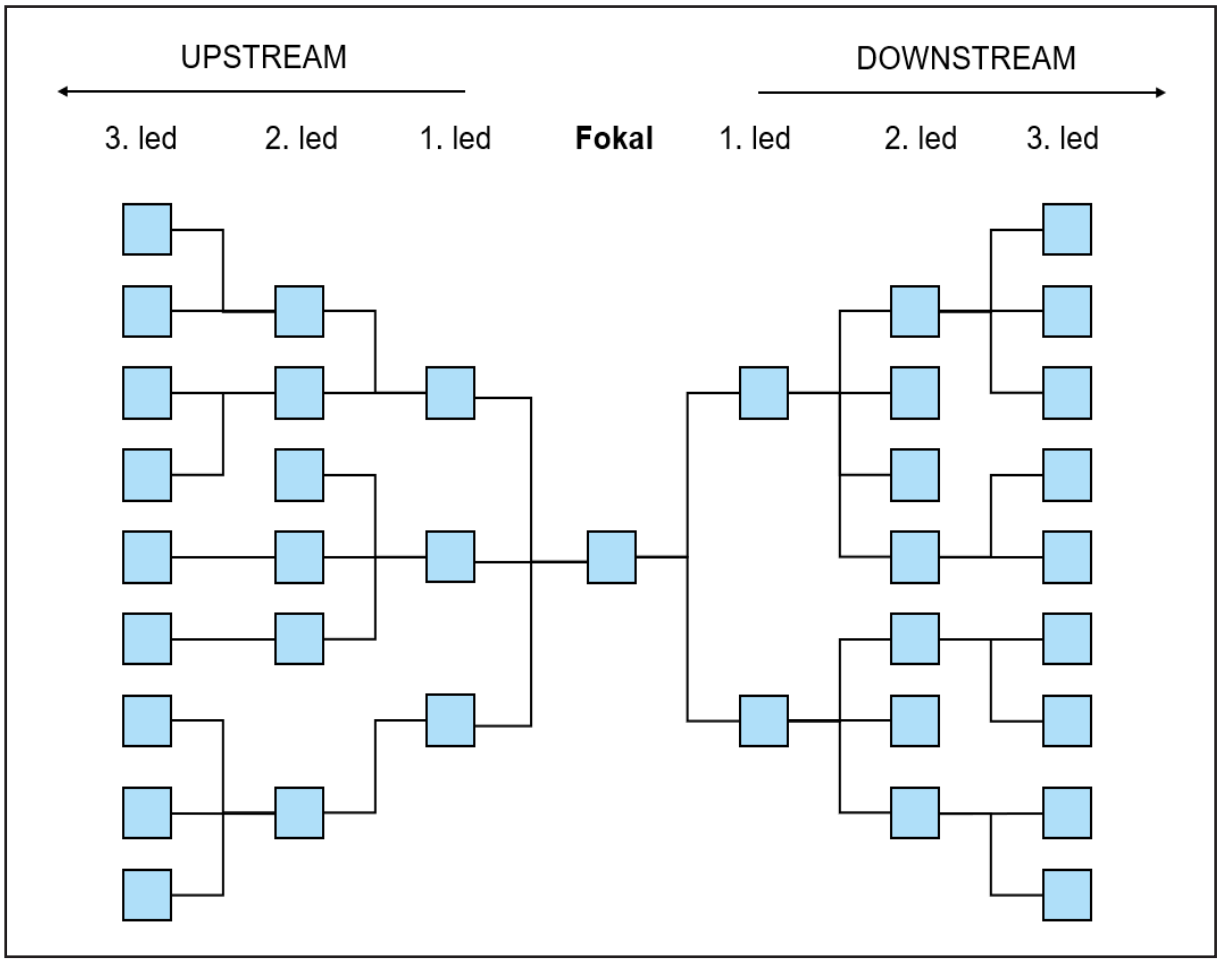
2.1 Supply chain management

Supply chain management (SCM) har fokus på processer med at styre vare-, informations- og finansielle strømme af varer, tjenester og information fra oprindelsesstedet til forbrugsstedet. Det omfatter en bred vifte af aktiviteter og involverer flere interessenter, herunder leverandører, producenter, logistikudbydere, distributører og detailhandlere. Det primære mål med SCM er at optimere hele forsyningskæden for at forbedre effektiviteten, reducere omkostningerne og sikre rettidig levering af produkter for at imødekomme kundernes efterspørgsel. En definition af SCM er:

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

Ovenstående definition henviser til, at SCM er efterspørgselsrettet. Det starter med kunders behov for varer og tjenesteydelser. Dernæst lægges vægt på, at der er tale om differentieret ledelse, hvilket betyder, at bl.a. tilgangen til kunder og leverandører ikke skal ske på samme måde for dem alle. Endelig peger definitionen på, at SCM søger at reducere omkostninger, levere den bedste kvalitet samt at levere varer og serviceydelser til det rette tidspunkt. Virksomheder indgår i forsyningsnetværk som illustreret i figur 2.1, hvor produktions SMV'er er de fokale virksomheder. Cybersikkerhed i forsyningskæderne har således fokus på, hvordan virksomhederne kan forbedre deres cybersikkerhed i de forskellige led af leverandører frem mod virksomheden (*upstream*) og fra virksomheden mod forskellige led af kunder (*downstream*).

Figur 2.1: Forsyningskædernes netværksstruktur



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

2.1.1 Supply chain orientering

Supply chain orientering refererer til den strategiske og operationelle tilgang, som en organisation tager for at styre og optimere sine forsyningskædeprocesser (Mentzer et al., 2001). Det indebærer et omfattende perspektiv, der integrerer alle aktiviteter fra indkøb af råmaterialer til den endelige levering af produkter til kunderne, og det sikrer effektivitet og værdiskabelse (Esper et al., 2010). Med andre ord udtrykker supply chain orientering i hvilken grad, der er et bevidst ledelsesmæssigt fokus på SCM i virksomheden – et tværorganisatorisk SCM-mindset.

Centrale elementer i supply chain orientering er:

- Kundefokus - prioritering af kundernes behov og forventninger for at forbedre tilfredshed og loyalitet.
- Samarbejde - opbygning af stærke partnerskaber med leverandører, distributører og andre interessenter for at sikre nødvendig koordinering og kommunikation.
- Integration af processer – såvel interne som eksterne.
- Informationsdeling – gennem anvendelse af teknologi til at dele information på tværs af forsyningskæden, hvilket muliggør bedre beslutningstagning og reaktionsevne.
- Procesoptimering - løbende forbedring af processer for at reducere omkostninger, eliminere spild og øge hastighed og pålidelighed.

Mangel på supply chain orientering kan ifølge Stentoft et al. (2018, p. 485) sammenfattes til:

- Mangel på tværfunktionelt samarbejde grundet en udpræget silokultur.
- Mangel på de rette medarbejdere.
- Mangel på færdigheder til at kvantificere og kommunikere værdien af SCM til topledelsen og bestyrelsen.
- For stort fokus på drift på bekostning af udviklingsorienterede aktiviteter.

2.1.2 Intern integration

Intern integration i en virksomhed refererer til koordineringen af centrale interne processer mellem afdelinger. Det skal sikre, at forskellige funktioner som logistik, marketing og salg, produktion, indkøb, økonomi og produktudvikling arbejder sammen mod fælles mål, hvor man bør undgå at suboptimeringer fører til silodannelse. Den interne integration kan styrke det interne samarbejde mellem afdelinger, hvilket kan reducere fejl og forsinkelser og forbedre time-to-market med nye produkter, kapacitetsstyring og leveringsevne. Intern integration er essentiel for at skabe en sammenhængende, effektiv og adræt virksomhed. Ved løbende at have fokus på at justere processer, forbedre kommunikation og udnytte fælles systemer kan virksomheder forbedre deres konkurrenceevne ved at opfylde de to mål om både at øge omsætningen (toplinjen) gennem serviceforbedringer og reducere omkostningerne (bundlinjen) (Stentoft et al., 2018, p. 20).

2.2 Karakteristika ved SMV'er

SMV'er spiller en afgørende rolle i samfundet og den socioøkonomiske udvikling, og de udgør 99 procent af alle virksomheder blandt OECD-medlemslande (OECD, 2023, p. 9). SMV'er beskæftiger typisk mellem 10 og 250 personer og genererer en omsætning på mellem 10 og 50 millioner EUR og/eller har en årlig balance på højst 43 millioner EUR (European Commission, 2020). SMV'er adskiller sig fra store virksomheder på flere områder. SMV'er har færre menneskelige, finansielle og teknologiske ressourcer (Forsman, 2008; Zach et al., 2014) og opererer under højere ekstern usikkerhed (Storey, 1994, p. 74). De mangler ofte beslutningsrelevant information, har begrænsede ledelsesmæssige ressourcer og opererer med at svagere cash flow (Pal et al., 2014). En praksis præget af mange brandslukninger kan hæmme deres evne til at forfølge langsigtede strategiske målsætninger (Kull et al., 2018). Desuden møder SMV'er et udfordrende politisk miljø, hvor de ofte bliver overset af beslutningstagere (Polyviou et al., 2020). På trods af sådanne udfordringer har SMV'er også en række fordele. De er typisk mindre bureaukratiske, opererer med hurtig beslutningstagning og højere risikotolerance, opretholder hurtig og effektiv intern kommunikation og har kortere beslutningsprocesser (Vossen, 1998). Derudover udviser SMV'er en evne til at lære og tilpasse sig skiftende markedsbehov, hvilket gør dem mere fleksible og tilpasningsdygtige (Pal et al., 2014).

2.3 Cybersikkerhed

2.3.1 Beskyttelsesmål og opmærksomhedsområder

I vores digitaliserede tidsalder er det afgørende at sikre cyberaktiver både i forretningslivet og privatlivet. Derfor berører cybersikkerhed alle, og det er derfor vigtigt i det mindste at have en grundlæggende forståelse af cybersikkerhed. Cybersikkerhed omfatter i sin kerne de praksisser, teknologier og processer, der er designet til at beskytte netværk, enheder, programmer og data mod angreb. Det kan f.eks. være, at nogen gør skade skade på eller får uautoriseret adgang til ens systemer. Ligesom fysisk sikkerhed er cybersikkerhed en form for risikostyring, dvs. angreb udgør visse risici, og vi skal beslutte, hvilke af disse risici vi afbøder, og hvilke vi accepterer. I disse beslutninger kan flere faktorer spille en rolle. Af største betydning er den skade, der kan opstå, sandsynligheden for et angreb samt omkostningerne ved afbødning.

I virksomheder med en dårlig cybersikkerhedsholdning vil disse beslutninger for det meste blive truffet ad hoc og reaktivt i stedet for at blive planlagt forud med proaktive foranstaltninger. Virksomhederne venter på, at angriberne foretager deres træk og forsøger derefter at afbøde den skade, der er sket. Dette svarer til ikke at børste tænder og i stedet gå til tandlægen, når der er et hul. Det kan være en kortsigtet gevinst ikke at skulle bruge penge på tandpasta eller tid på at børste tænder hver morgen og aften. Men på lang sigt er det ikke en bæredygtig strategi. Derfor børster vi alle tænder hver dag. Vi lærer

og forstår let, at skaden kan være at miste en tand; at sandsynligheden for et hul er høj, og at omkostningerne til afbødning kan være betydelige i tid og penge. Mens skaden, sandsynligheden og omkostningerne ved afbødning er mindre håndgribelige at forstå, når det kommer til cybersikkerhed, er det på dette abstraktionsniveau meget lig med at børste tænder. Det er ikke sjovt at gøre; det giver ikke en direkte fordel, det repræsenterer en omkostning, og virkningerne af ikke at gøre det viser sig først på længere sigt, men da med drastiske konsekvenser. Så hvordan får en organisation en proaktiv tilgang til cybersikkerhed? Det første skridt er at tænke over, hvad aktiverne i virksomheden er. Disse kan f.eks. være produktionsmaskiner, operativ IT, intellektuel ejendom eller kundedata. Det næste skridt er derefter at begynde at tænke på risici i relation til disse aktiver. I cybersikkerhed spiller tre typer risici en vigtig rolle, som relaterer til de tre fundamentale cybersikkerhedsbeskyttelsesmål: 1) risici for informations fortrolighed, 2) risici for datas integritet og 3) risici for tilgængelighed af data og tjenester. Overvej følgende eksempler som illustrationer af disse tre typer risici.

Informationsfortrolighed betyder, at information kun er tilgængelig for autoriserede personer. Når man tænker på dette beskyttelsesmål for ens aktiver, kan man spørge, hvad en afsløring af et aktiv vil betyde, hvis nogen specifik intellektuel ejendom bliver stjålet i et cyberangreb.

Dataintegritet betyder, at data er nøjagtige og uændrede under opbevaring eller transit. Når man overvejer dette beskyttelsesmål i relation til ens aktiver, så kan man vurdere, hvilken indvirkning ændrede data kan have f.eks. i et supply chain angreb, hvis information eller software, man leverer til kunder (eller som man får fra en anden virksomhed), ændres og kompromitterer deres eller ens egne operationer.

Tilgængelighed af data og tjenester betyder, at data og tjenester er tilgængelige for autoriserede brugere, når de er nødvendige. Dette beskyttelsesmål kan let relateres til produktionsfaciliteter eller operationer i virksomheder, f.eks. omkostningerne ved en virksomheds e-mail-, booking- eller salgssystem, der ikke er tilgængeligt i en dag eller i en uge. Især SMV'er kan føle sig overvældet af cyberrisici og have svært ved at komme ind i en proaktiv måde at håndtere cybersikkerhed på. De fleste virksomheder deler dog nogle udfordringer på grund af udbredelsen af de respektive angreb og påkrævede opgaver.

Genopretning efter en hændelse. Når en virksomhed rammes af et cyberangreb, der giver driftsforstyrrelser, eller hvor data, som kan være underlagt GDPR-bøder, lækker, er en koordineret respons af afgørende betydning. Derfor bør det være klart, hvem der er ansvarlig for hvilken del af responsen, før en sådan hændelse opstår. Under alle omstændigheder er en fungerende backup-løsning til at afbøde de udbredte ransomware-angreb og have testet den, før den er nødvendig, altid en god investering.

Bekæmpelse af *social engineering-angreb*. Social engineering-angreb som phishing og kompromittering af forretnings-e-mails er blandt de hyppigst forekommende angreb. Ofte anvendes bevidsthedsmålinger til dette formål. Kvaliteten af disse foranstaltninger varierer dog meget, og det skal sikres, at de virkelig øger medarbejdernes bevidsthed og viden om cybersikkerhed i stedet for blot at føre til tidsspilde. På samme måde skal alle sikkerhedsforanstaltninger være i sync med medarbejdernes arbejdsgange. Hvis arbejdsgange besværliggøres, og medarbejdere føler, at de bliver forhindret i at være produktive, vil de søge måder at omgå sikkerhedsforanstaltningerne på, og disse foranstaltninger vil snarere mindske sikkerheden end øge den.

Dækning af grundlæggende sikkerhedsdrift. Ud over sikkerhedsforanstaltninger, der hjælper med genopretning efter angreb (såsom backups), bør nogle få foranstaltninger være på plads i enhver virksomhed. For det første forhindrer rettidige opdateringer tekniske sårbarheder i at blive udnyttet af angribere, og de anses generelt for at være en af de vigtigste sikkerhedsforanstaltninger. For det andet bør der ikke anvendes standardadgangskoder nogen steder i virksomheden, og for det tredje bør især konti med administrative rettigheder i IT-afdelingen være særligt beskyttet med to-faktor-godkendelse. Mange flere foranstaltninger er tilrådelige, men de førnævnte tre er de absolut grundlæggende.

Ved, hvad du antager. Når man vurderer risici, har mange virksomheder implicitte antagelser om deres infrastruktur eller potentielle angribere. F.eks. er "Min virksomhed er for lille til at blive angrebet" en almindelig myte. Et mål i risikovurderingen bør være at dokumentere så mange af disse antagelser som muligt for at gøre dem eksplicitte og muliggøre diskussioner om, hvorvidt antagelsen er rimelig eller ej.

2.3.2 Cybersikkerhedsstandarder

Cybersikkerhedsstandarder er etablerede retningslinjer og best practice designet til at beskytte informationssystemer mod cybertrusler. Ved at følge disse standarder har virksomheder mulighed for effektivt at sikre deres data og IT-infrastruktur. De dækker et bredt spektrum af områder, herunder netværkssikkerhed, databeskyttelse, adgangskontrol og hændelsesrespons. Ved at overholde disse standarder kan organisationer sikre, at de implementerer tilstrækkelige sikkerhedsforanstaltninger, såsom kryptering, firewall og multifaktorautentifikation.

Cybersikkerhedsstandarder udvikles af forskellige organisationer, såsom International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST) og European Union Agency for Cybersecurity (ENISA). Eksempler på sådanne standarder er ISO 27001 om styring af informationssikkerhed, NIST, Cybersecurity Framework (CSF) 2.0, NIS2 og digitale identitetsstandarder (Alamillo et al., 2023). Standarderne hjælper organisationer med at overholde lovgivningsmæssige krav, forbedre deres

sikkerhedsstatus og reducere risikoen for databrud og cyberangreb. Implementeringen af standarderne fremmer også en kultur af sikkerhedsbevidsthed og løbende forbedring indenfor organisationen, hvilket sikrer, at cybersikkerhedspraksis udvikler sig i takt med fremkommende trusler og teknologiske fremskridt.

2.3.3 Cybersikkerhed supply chain risk management

Cybersikkerhed supply chain risk management indebærer at identificere, vurdere og afbøde de risici, der er forbundet med samhandel med supply chain aktører som kunder, leverandører og andre tredjeparter. Det inkluderer en omfattende tilgang til at sikre, at alle elementer i forsyningskæden, herunder hardware, software og tjenester, overholder sikkerhedsstandarder for at forhindre potentielle sårbarheder. Processen kan indeholde evalueringer af såvel kunders som leverandørers sikkerhedspraksis, sikre overholdelse af lovkrav og implementere kontrolforanstaltninger for en effektiv håndtering af risici. Målet er at beskytte mod trusler, der kan opstå fra tredjepartsrelationer, såsom databrud, malware og uautoriseret adgang, og dermed beskytte integriteten, fortroligheden og tilgængeligheden af kritiske aktiver i hele forsyningskæden. Ved at opretholde kontinuerlig overvågning og fremme samarbejde med kunder og leverandører kan virksomheden forbedre dens overordnede sikkerhedsstatus og sikre modstandsdygtighed mod cybertrusler.

2.4 Cybersikkerhed og geopolitik

Cyberspace er blevet en integreret del af vores daglige liv. Vi tjekker e-mails, streamer film, køber dagligvarer, bestiller rejser, betaler regninger, får adgang til offentlige tjenester, overvåger lagerbeholdninger, kontrollerer termostater eller stiller timeren på kaffemaskiner. Vi er dermed blevet afhængige af cyberspace til en bred vifte af værktøjer og opgaver.

Den digitale verden udviklede sig i slutningen af 1990'erne og begyndelsen af 2000'erne i en æra af globalisering. De relativt lave omkostninger og krav til færdigheder til at bruge cyberkapabiliteter åbnede cyberspace for en bred vifte af aktører - enkeltpersoner, SMV'er, multinationale selskaber og regeringer. Internettet tilbød en helt ny måde at kommunikere hurtigt på, behandle transaktioner, flytte og gemme information og levere tjenester.

Ved sin spæde start var der en antagelse om, at cyberspace ville forblive tilgængeligt og frit i et rum ud over nationale grænser. Men i en æra med stigende geopolitisk konkurrence og konflikt tilbyder cyberspace nu et miljø, hvor en række onde aktører, stater og ikke-statslige aktører, kriminelle organisationer og enkeltpersoner kan målrette angreb mod rivaler og modstandere. Cyberangreb er en måde at infiltrere kritiske systemer på ved at forstyrre, deaktivere og destabilisere en modstander uden de samme risici og konsekvenser som ved et fysisk angreb.

Cyberangreb kan spænde fra databrud, malware, ransomware og til denial-of-service-angreb, der lammer essentielle tjenester og infrastruktur. I en højt digitaliseret og integreret økonomi som i et samfund som Danmark rammer virkningerne af cyberangreb ud over deres oprindelige mål. De kan mærkes af organisationer og enkeltpersoner, der ikke er det direkte mål, men som er afhængige af forskellige tjenester eller information. Cyberangreb og genoprettelsesindsatser koster verdensøkonomien over 1 billion USD om året. Med så store omkostninger rangerer cyberhændelser som den største risiko for virksomheder i 19 lande inklusive Danmark, hvor SMV'er virksomheder er særligt sårbare (Allianz, 2023).

I modsætning til f.eks. fysiske, aggressive angreb er cyberspace kendetegnet ved en relativ høj uigennemsigtighed, hvilket gør det svært at identificere en angriber og respondere på angrebet. Metoder til at respondere på cyberangreb er ikke så klare, som de er for fysiske angreb på mennesker, ejendom eller territorium. Der mangler etablerede og håndgribelige normer til at respondere på cyberangreb og regulere adfærd i cyberspace. Den hurtige teknologiske udvikling har overgået anvendeligheden af eksisterende lovgivning, og udviklingen af de lovgivningsmæssige rammer har ikke holdt trit med ændringer i teknologi eller skifte i det geopolitiske landskab. Forsøg på at etablere regler og løse sikkerhedsudfordringen i cyberspace gennem FN-arbejdsgrupper er stort set stagneret på grund af manglende samarbejde og gennemsigtighed blandt stater som Kina, Rusland og USA (Ruhl et al., 2020).

Anonymiteten og asymmetrien betyder, at cyberangreb vil forblive en del af staters og ikke-statslige aktørers arsenal, og de vil supplere konventionelle operationer. F.eks. har Rusland med invasionen af Ukraine i februar 2022 målrettet regeringsstøttede cyberoperatører mod den ukrainske regering og den militære og civile cyberinfrastruktur for at opnå fordele og påvirke holdninger til konflikten. Uden for Ukraine er NATO-lande også blevet ramt med en stigning i spear-phishing-angreb (Google Threat Awareness Group, 2023).

I en tid med stigende geopolitisk flygtighed vil risikoen for cyberangreb fortsætte med at stige. Cyberspaces natur og den stadigt udviklende karakter af cyberangreb gør cyberspace til et kritisk sårbart miljø - en frontlinje i en ny æra af geopolitisk indhold og konflikt.

2.5 Drift versus udvikling

Problemstillingen med samtidig at forfølge to forskellige, men komplementære kapabiliteter, henholdsvis de konkrete driftsopgaver og opgaver med forretningsudvikling, er udfordrende at balancere. Driftsopgaver indebærer ofte optimering og forbedring af eksisterende processer for at sikre effektivitet og pålidelighed, mens udviklingsopgaver har fokus på innovation, tilpasningsevne og reaktion på skiftende markedsforhold. En vellykket balancering af disse to kapabiliteter gør det muligt for virksomheder at opretholde

en konkurrencemæssig fordel og opnå langsigtet succes. I organisatoriske og teoretiske sammenhænge er dette dilemma benævnt ambidexterity, som vedrører evnen til både at kunne exploite (udnytte) og explore (udforske) (March, 1991). Det er introduceret som en central ledelsesmæssig opgave i at sikre langsigtet overlevelse.

Litteraturen diskuterer forskellige former for ambidexterity, herunder sekventiel og simultan, som vist i tabel 2.1. Sekventiel ambidexterity betyder, at man adskiller drifts- og udviklingsopgaver tidsmæssigt. Organisatorisk fokuserer man i nogle perioder mere på driftsopgaver og i andre perioder mere på udviklingsopgaver. Sekventiel ambidexterity er specielt relevant i perioder med stabilitet og for mindre virksomheder, som ikke i samme omfang som mellemstore og store virksomheder kan afsætte ressourcer til sådanne forskelligartede opgaver (O'Reilly & Tushman, 2013). Simultan ambidexterity betyder, at man opererer med både drifts- og udviklingsorienterede ressourcer på samme tid (f.eks. samtidige drifts- og udviklingsafdelinger). Ifølge O'Reilly & Tushman (2013, p. 330) er en sådan organisering velegnet for virksomheder i dynamiske omgivelser, hvor betingelser løbende ændres.

Tabel 2.1: Sekventiel og simultan ambidexterity

	Sekventiel	**Simultan**
Balancested	Organisationsniveau	Organisationsniveau
Balancemekanisme	Sekventielle skift over tid mellem drift og udvikling	Separate enheder, der har fokus på henholdsvis drift og udvikling
Ledelsesrolle	Proaktiv ledelse er essentiel	Proaktiv ledelse er essentiel
Udfordringer	Ledelse af overgange mellem drift og udvikling og fjerne internt pres	Koordinering på tværs af enheder og ledelse af modstridende forhold i senior-ledelsesteamet
Anvendelse	Især egnet i stabile omgivelser/ for mindre virksomheder	Især egnet i dynamiske omgivelser/for store virksomheder

Kilde: O'Reilly & Tushman (2004, 2013).

3. Metode

Denne undersøgelse om cybersikkerhed i danske produktions SMV'er er gennemført som en landsdækkende spørgeskemaundersøgelse fra december 2023 til februar 2024. Der er trukket en liste af virksomheder (NACE branchekoder fra 10 til 33) fra virksomhedsdatabasen "Navne og Numre Erhverv" af virksomheder fra 20 til 250 ansatte. En bruttoliste på 1.402 virksomheder blev identificeret via virksomhedsdatabasen, som dækker alle momsregistrerede virksomheder i Danmark. Listen blev renset for bagerier og virksomheder, der ikke længere er aktive, hvilket førte til en nettoliste på 1.293 virksomheder. Der blev sendt e-mails til de administrerende direktører eller Supply Chain Managers. I de situationer, hvor kontaktoplysningerne ikke var tilgængelige for disse personer, blev der sendt en e-mail til virksomhedernes hoved-e-mailadresse adresseret "Til hvem det måtte vedrøre". I alt accepterede 314 at deltage i spørgeskemaundersøgelsen, hvoraf 248 har leveret fulde svar. Det giver en svarprocent på 19,2 ud af de kontaktede virksomheder og en svarprocent på 78,9 ud af de virksomheder, der accepterede at deltage i undersøgelsen. Karakteristika ved respondenterne og virksomhederne er medtaget i tabel 3.1 og 3.2.

Tabel 3.1 viser jobtitlerne for de 248 respondenter. "Ejer/CEO", "Ejer og adm. direktør" samt "Adm. direktør" udgør godt 38 procent af respondenterne, mens gruppen "Andet" udgør knap 62 procent. Dette resultat er interessant, idet det indikerer, at det organisatoriske ansvar for cybersikkerhed er forskelligt placeret ud fra den forudsætning, at dem, der har deltaget i undersøgelsen, også sidder med det konkrete ansvar. Hos 23 respondenter var der mere end én person involveret i udfyldelsen af spørgeskemaet. Respondenten blev informeret i introduktionsbrevet om, hvilke emner spørgeskemaet indeholdt, så de kunne være forberedte og eventuelt inddrage kolleger i besvarelsen af spørgeskemaet. Kun syv respondenter har ikke noget ledelsesansvar med deres angivne jobtitler som "medarbejdere" og "ledelsesassistenter". Tabel 3.2 viser fordelingen af virksomheder på tværs af industrier. Tabellen indikerer en bred repræsentation af industrier, dog med et flertal af virksomheder indenfor "Anden fremstillingsvirksomhed", "Fremstilling af maskiner og udstyr" og "Jern- og metalvareindustri, undtagen maskiner og udstyr ".

Tabel 3.1: Karakteristik af respondenterne

Respondenternes jobtitler	Antal
Ejer/CEO	12
Ejer og adm. direktør	43
Adm. direktør	40
Andet	153
I alt	**248**

Tabel 3.2: Undersøgelsens brancherepræsentation

Branche	Antal	%
Fremstilling af fødevarer (10)	22	8,9
Fremstilling af drikkevarer (11)	2	0,8
Fremstilling af tobaksprodukter (12)	2	0,8
Fremstilling af tekstiler (13)	4	1,6
Fremstilling af beklædningsartikler (14)	3	1,2
Fremstilling af læder og lædervarer (15)	0	0,0
Fremstilling af træ og varer af træ og kork, undtagen møbler; fremstilling af varer af strå og flettematerialer (16)	3	1,2
Fremstilling af papir og papirvarer (17)	1	0,4
Trykning og reproduktion af indspillede medier (Grafiske industri) (18)	1	0,4
Fremstilling af koks og raffinerede mineralolieprodukter (19)	0	0,0
Fremstilling af kemiske produkter (20)	5	2,0
Fremstilling af farmaceutiske råvarer og farmaceutiske præparater (21)	3	1,2
Fremstilling af gummi- og plastprodukter (22)	11	4,4
Fremstilling af andre ikke-metalholdige mineralske produkter (23)	0	0,0
Fremstilling af metal (24)	5	2,0
Jern- og metalvareindustri, undtagen maskiner og udstyr (25)	40	16,1
Fremstilling af computere, elektroniske og optiske produkter (26)	5	2,0
Fremstilling af elektrisk udstyr (27)	18	7,3
Fremstilling af maskiner og udstyr i.a.n. (28)	51	20,6
Fremstilling af motorkøretøjer, påhængsvogne og sættevogne (29)	2	0,8
Fremstilling af andre transportmidler (30)	1	0,4
Fremstilling af møbler (31)	6	2,4
Anden fremstillingsvirksomhed (32): Hvilken?	60	24,2
Reparation og installation af maskiner og udstyr (33)	3	1,2
I alt	**248**	**100**

Note: Tal i parentes angiver branchens NACE-kode.

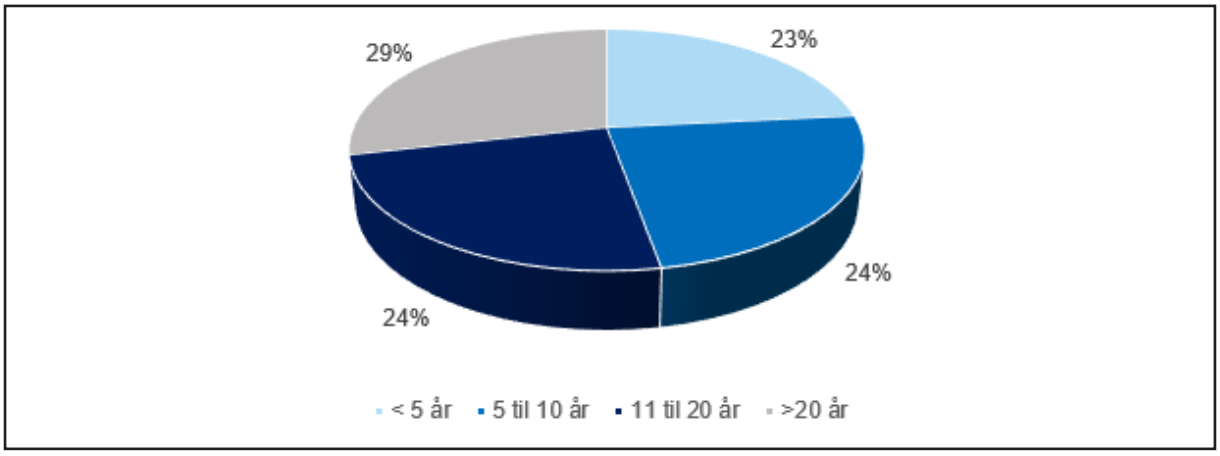
De 62 procent af respondenterne, der svarer til 153 jf. tabel 3.1, fordeler sig i følgende kategorier som vist i tabel 3.3.

Tabel 3.3: Uddybning af jobområder for kategorien "Andet" jf. tabel 3.1

Jobområder	Antal
CIO/IT-chef/CTO	35
Supply Chain Manager/Supply Chain Director	21
CFO/Controller	17
Fabrikschef/Produktionschef	14
Indkøber/Sourcing Manager/Category Manager	12
Senior Manager (Compliance, Sales, Marketing)	12
COO	8
Logistikchef/Planlægningschef/Planning Director	1
Andet	33
I alt	**153**

Respondenterne er spurgt ind til anciennitet i nuværende job. Svarene hertil fremgår af figur 3.1. Her ses en jævn spredning i ancienniteten i forhold til det nuværende job. Således har 23 procent bestridt det nuværende job i under 5 år, mens 24 procent har været i det nuværende job i 5 til 10 år samt i 11 til 20 år. Kun kategorien 'over 20 år' stikker lidt ud, idet hele 29 procent af respondenterne angiver at have været i det nuværende job i over 20 år.

Figur 3.1: Anciennitet i nuværende job



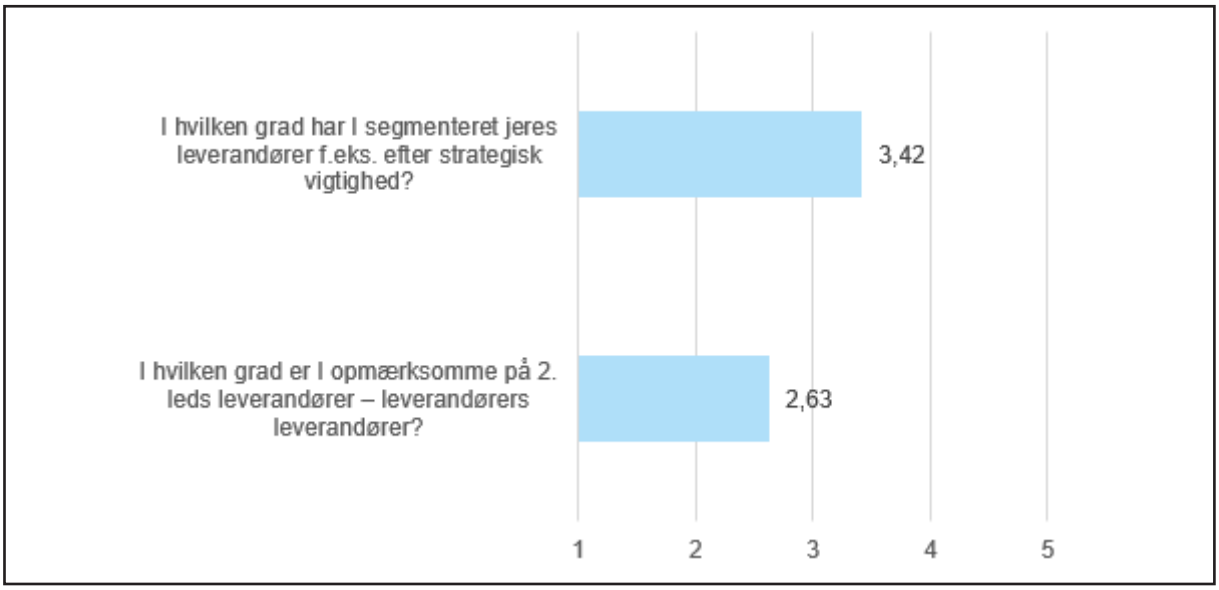
4. Analyse

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

4.1 Leverandørsegmentering

Respondenterne er blevet spurgt ind til, hvorvidt de segmenterer deres leverandører ud fra strategisk vigtighed, samt i hvilken grad de er opmærksomme på leverandørernes leverandører. En praksis med at segmentere leverandører fortæller noget om, hvor bevidste virksomhederne er om at differentiere arbejdet med leverandører f.eks. i forhold til ressourceallokering, risikostyring og relationsledelse. Det næste spørgsmål om opmærksomheden på leverandørers leverandører er medtaget for at få data om, i hvilken grad der er bevidsthed om cybertrusler længere tilbage i forsyningskæden. En undersøgelse om supply chain resilience blandt danske produktions SMV'er fra 2023 afslørede, at produktions SMV'er i stor grad kun har fokus på leverandører i første led, hvilket øger deres sårbarhed (Stentoft et al., 2023).

Figur 4.1: Segmentering af leverandører

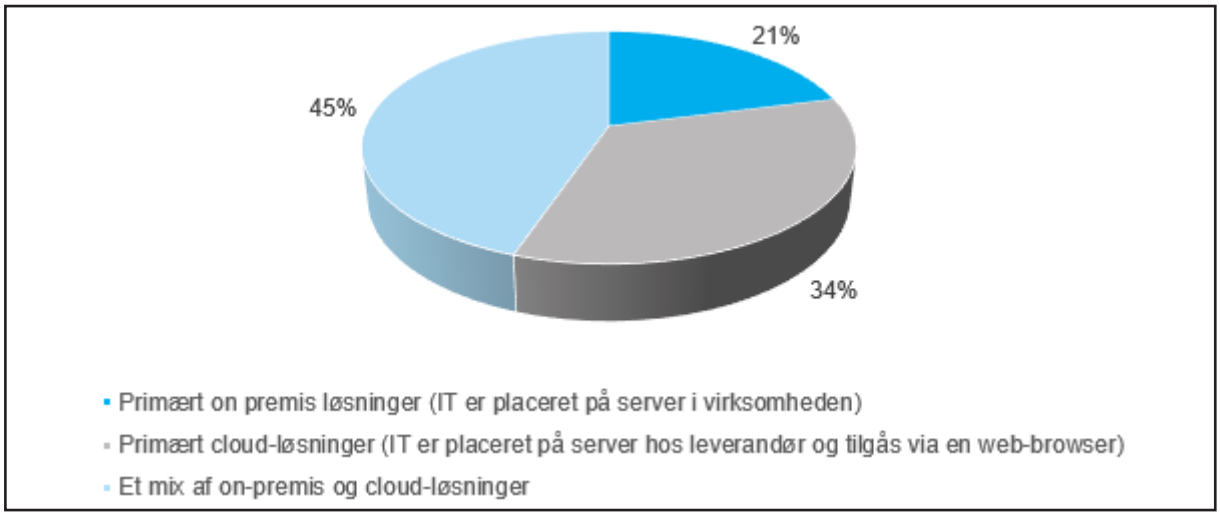


Som det fremgår af figur 4.1, ligger gennemsnittet i forhold til segmentering af leverandørbasen på 3,42 point på en fem-punkts Likert-skala, hvor 1 = i meget lav grad og 5 = i meget høj grad. I undersøgelser af denne type opfattes gennemsnitsværdier på 3,5 og derover som værende signifikante (betydningsbærende). 3,42 ligger således lidt over i nogen grad (som er lig med 3,0). Opmærksomheden på leverandørerne i andet led angives af respondenterne til kun 2,63. Idet en kæde ikke er stærkere end det svageste led, tyder begge de ovenstående tal på, at der er potentiale for forbedringer.

4.2 It-løsninger og deres drift

Respondenterne er også spurgt ind til hvilken hosting af IT-løsninger, de anvender. Er virksomhedens IT-løsninger opbevaret på egen lokation (on-premis), eller tilgås systemer i skyen hos en tredjepart? Figur 4.2 indeholder de respektive svar herpå.

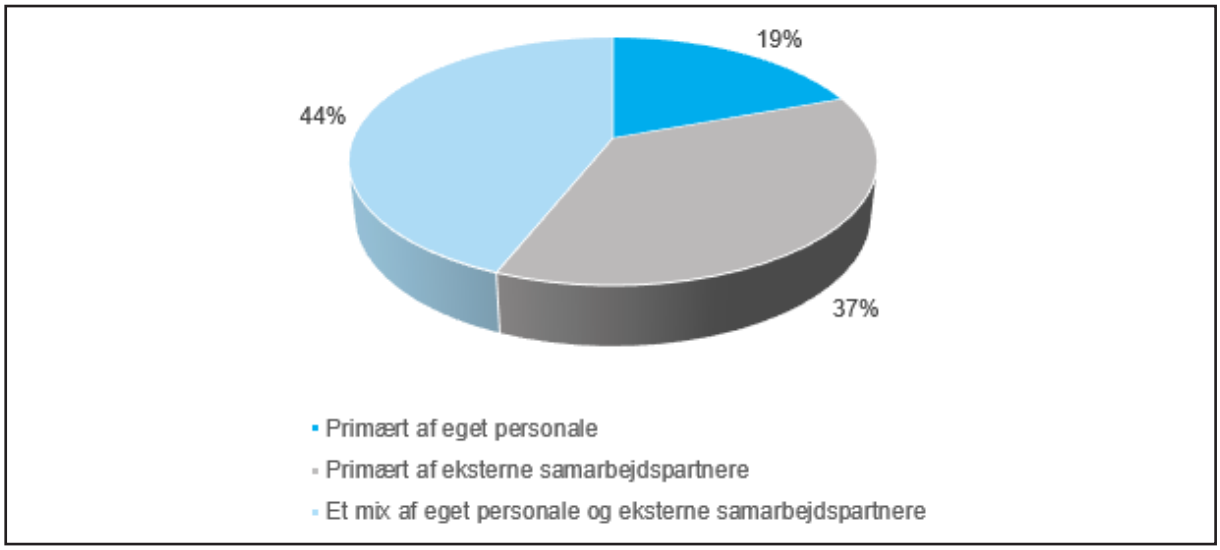
Figur 4.2: On-premis vs. cloud-løsninger



Som det fremgår af figur 4.2, angiver 45 procent af virksomhederne, at deres IT-løsninger især er et mix, hvor en del ligger placeret på servere i virksomheden og noget andet er lagret i skyen. Herefter angiver 34 procent af virksomhederne, at de primært har en cloudløsning, hvor IT er placeret på eksterne servere ved en leverandør og som tilgås via en browser. De sidste 21 procent af virksomhederne har en løsning, hvor virksomhedens IT-løsning primært ligger på interne servere. Med cloud-løsninger skal man også være opmærksom på risikoen for cyberangreb og hændelser. Hvis f.eks. en standard cloud-løsning angribes af malware, bør man have kontrol over ens data. Derfor er det vigtigt grundigt at få undersøgt forhold som databeskyttelse, infrastruktur og adgangskontrol samt ansvarsfordelingen mellem cloud-leverandøren og kunden i løsninger som *Infrastructure as a Service (IaaS), Platform as a Service (PaaS)* og *Software as a Service (SaaS)* (Pedersen & Vandrup, 2022, p. 146).

Undersøgelsens deltagere er endvidere blevet spurgt om, hvem der håndterer virksomhedens IT-driftsservice. Svarene herfor fremgår af figur 4.3.

Figur 4.3: Drift af virksomhedens IT-løsninger



Som det fremgår af figur 4.3, ligger respondenternes svar tæt op ad de tidligere svar på, hvor virksomhedens IT-systemer er lokaliseret. Dette virker umiddelbart også logisk, idet det ikke giver meget mening at stå for driften af et system, som er placeret ved en leverandør. Omvendt kunne man måske forestille sig, at enkelte virksomheder har outsourcet selve driften af systemerne uden at have systemerne placeret eksternt. Det synes dog ikke at være en udpræget løsning, idet det er 21 procent af virksomhederne, der har systemerne placeret internt (jf. figur 4.2), mens 19 procent af virksomhederne angiver, at det primært er eget personale, som håndterer driftsansvaret af IT-systemerne. På samme måde ses, at 37 procent angiver et mix af, at eget personale og eksterne samarbejdspartnere håndterer driftsansvaret af IT-systemerne. Dette svarer ligeledes godt overens med svarene i figur 4.2, hvor 34 procent angiver et mix af intern og ekstern placering. Det er desværre ikke muligt, på baggrund af de foreliggende data, at udlede, hvor stor en andel af IT-systemerne, der er placeret ved leverandørerne, eller hvor stor en andel som håndteres henholdsvis internt eller eksternt.

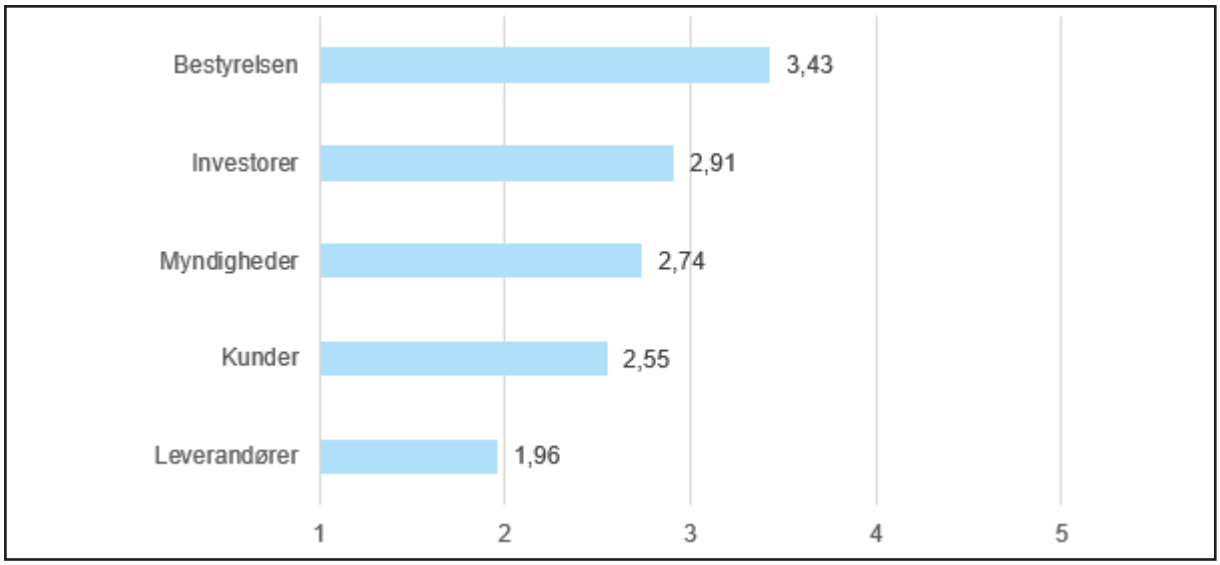
4.3. Krav til cybersikkerhed, brug af standarder og cyberangreb

4.3.1 Krav til cybersikkerhed

I den senere tid er cyberangreb oftere blevet peget på som en reel trussel mod virksomhederne og disses forsyningskæder. På europæisk plan forventes det nye NIS2-direktiv implementeret i 2024. Formålet med NIS2-direktivet

er at styrke og ensarte cybersikkerheden og modstandsdygtigheden overfor cybertrusler på tværs af EU-landende. Direktivet er målrettet virksomheder, der anses for at have en kritisk rolle i forhold til økonomien og samfundet. NIS2 indeholder bl.a. krav om, at virksomheder implementerer foranstaltninger omkring cybersikkerhed, og at de foretager hændelsesrapportering. Det er derfor naturligt at spørge ind til, hvorfra krav til virksomhedernes cybersikkerhed opstår. Respondenternes svar hertil fremgår af figur 4.4.

Figur 4.4: Krav til cybersikkerhed



Som det fremgår af figur 4.4, er det især bestyrelsen, der stiller krav om cybersikkerhed. Dog er den gennemsnitlige forventning kun angivet til 3,43 på en fem-punkts Likert-skala (hvor 1 = i meget lav grad og 5 = i meget høj grad). Set i lyset af den megen omtale i medierne omkring trusselsbilledet indenfor cybersikkerhed samt det relativt lave beredskab i danske SMV'er (Stentoft et al., 2023a), synes tallet ikke at være højt. Kravet fra investorer ligger endnu lavere på 2,91, som er tæt på "i nogen grad" fulgt af myndighedskrav på 2,74. Lavest ligger krav fra kunder og leverandører på henholdsvis 2,55 og 1,96 i gennemsnit. Især springer tallet 2,55 i forhold til krav fra kunder i øjnene. Undersøgelsen er målrettet danske produktions SMV'er, hvoraf en stor del leverer produkter ind til de store virksomheder i såvel Danmark som udlandet (eksport). Man kunne derfor forvente, at de store virksomheder ville stille krav om et vist niveau for cybersikkerhed eller sågar specifikke krav til brug af standarder og/eller certificeringer indenfor cybersikkerhed. Resultatet indikerer et efterslæb blandt SMV'er i forhold til de store virksomheder.

8 trends inden for cyberkriminalitet i 2024

1 **Den kunstige intelligens' stigende rolle i cyberangreb**

Den udbredte anvendelse af kunstig intelligens fremhæver ikke kun den igangværende revolution, men øger også bekymringer til dets bredere implikationer og sikkerhedsrisici. *Deepfakes* og stemmekloning kommer i fuld fokus, når man adresserer sikkerhedsudfordringer med kunstig intelligens.

2 **Cyberkriminelle udnytter alle nye teknologier**

Selvom kunstig intelligens er århundredets innovation, så fokuserer cyberkriminelle ikke kun på det. De udvider deres horisont for at udnytte en række nye teknologier. Målet er at udvide angrebsfladen og nå så meget som muligt. Derfor bliver hver ny teknologi både et værktøj og et mål for sofistikerede cybertrusler.

3 **Cyberkriminalitet bliver mere professionaliseret**

Professionaliseringen af cyberkriminalitet fortsætter med at gøre stabile fremskridt og vil nå et nyt niveau af modenhed i 2024. Denne eskalering drives delvist af tilgængeligheden og udvidelsen af *Ransomware as a Service (RaaS)* tilbud. Sådanne værktøjer sænker ikke kun indgangsbarrieren for potentielle cyberkriminelle, men repræsenterer også en betydelig ændring i angrebenes kompleksitet og påvirkning.

4 **Hacktivist-bevægelsen vinder momentum**

Trusselslandskabet strækker sig ud over enkeltpersoner, der forfølger økonomiske eller personlige mål. Eskalerende politiske og sociale spændinger øger fremkomsten af en anden betydelig fraktion i den digitale sfære: *Hacktivister*. Motiveret af et ønske om at udtrykke uenighed eller støtte til sager, som væbnede konflikter eller sociale uretfærdigheder, udnytter disse individer sårbarheder og sikkerhedshuller for at fremsætte deres udsagn.

5 Disinformation as a Service (DaaS)

DaaS er en taktik, som indebærer en bevidst spredning af falske oplysninger. Det bliver i stigende grad brugt af mange forskellige aktører til at manipulere den offentlige mening, skade omdømmer og påvirke forretnings- og politiske landskaber.

6 Udfordringer for den offentlige sektor og kritisk infrastruktur

Selvom *hacktivismen* er en velkendt trussel mod offentlige sektorers institutioner, er dette kun ét aspekt af de udfordringer, der er. Den offentlige sektor må også håndtere trusler fra statsstøttede cyberkriminelle og uafhængige hackere, der sigter mod datanedbrydning, forstyrrelser, økonomiske gevinster og spionage – alt sammen med alvorlige konsekvenser.

7 Pretexting og multichannel taktikker

Sofistikerede *social engineering* som *pretexting*, hvor hackere udgiver sig for at være nogen, offeret stoler på, og bruger en falsk historie til at narre dem, bliver i stigende grad brugt af cyberkriminelle til at udnytte og manipulere ofrer for sikre økonomiske gevinster eller begå tyveri af følsomme data.

8 Stigende udbrændingsrater udfordrer cybersikkerhedsteams som aldrig før

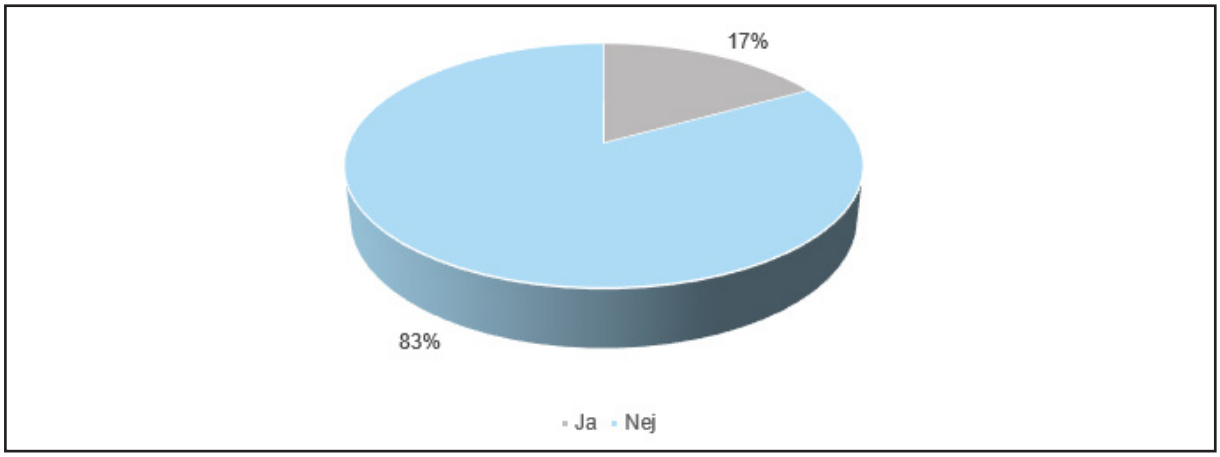
De seneste globale spændinger og den fortsatte professionalisering af cyberkriminalitet, nu drevet af værktøjer baseret på kunstig intelligens, gør ikke kun angreb mere komplekse og svære at opdage, men lægger også et hidtil uset pres på sikkerhedsprofessionelle. I denne vedholdende bølge af udfordringer bliver sådanne teams' modstandskraft og tilpasningsevne testet som aldrig før.

Kilde: Sosafe (2024).

4.3.2 Forpligtelse til at bruge standarder

I forhold til cybersikkerhed er virksomhederne blevet spurgt om, hvorvidt de er forpligtede til at overholde forskellige standarder. Som det fremgår af respondenternes svar i figur 4.5, er 17 procent af virksomhederne underlagt overholdelse af en eller flere standarder indenfor cybersikkerhed.

Figur 4.5: Forpligtelser til at overholde én eller flere standarder indenfor cybersikkerhed



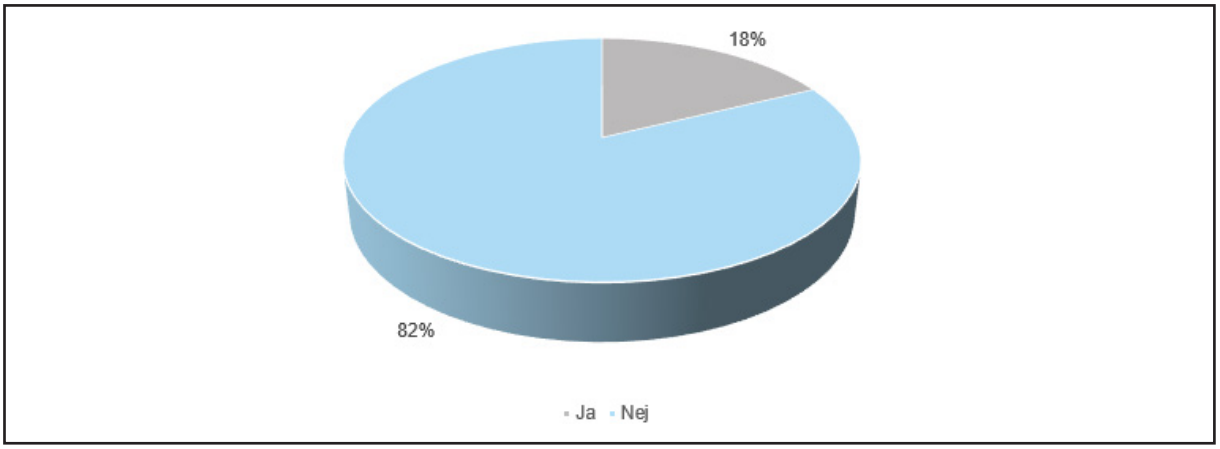
De, som har svaret ja, har haft mulighed for at angive, hvilke standarder det drejer sig om. Svarene fremgår af tabel 4.1.

Tabel 4.1: Standarder, der følges omkring cybersikkerhed

• **CMMC** (Cybersecurity Maturity Model Certification)
• **DFARS** (Defense Federal Acquisition Regulation Supplement)
• **GDPR** (General Data Protection Regulation)
• **IEC62443** (Industrial communication networks - Network and system security)
• **ISO 15408** (Almindelige kriterier til evaluering af informationsteknologisikkerhed)
• **ISO 62443** (Cybersecurity for operational technology in automation and control systems)
• **ISO27001/27002** (Information Security Standards)
• **ISO27011** (Standard for Telecommunications Organizations)
• **ISO9001** (Kvalitetsledelse)
• **NIST I&II** (National Institute of Standards and Technology)
• **SOC 2** (System and Organization Controls)

Men én ting er, hvorvidt den enkelte virksomhed er underlagt eksterne krav. En anden ting er, om virksomhederne selv frivilligt vælger at adoptere og overholde forskellige standarder. Respondenterne er derfor også blevet spurgt ind til, hvorvidt de frivilligt har valgt at overholde en eller flere standarder indenfor cybersikkerhed. Som det fremgår af figur 4.6, har 18 procent af virksomhederne valgt frivilligt at overholde en eller flere standarder indenfor cybersikkerhed.

Figur 4.6: Frivilligt valg af at følge standarder indenfor cybersikkerhed



Godt halvdelen af de respondenter, der svarer, at de møder krav om at bruge standarder indenfor cybersikkerhed, svarer, at de samtidig vælger at følge standarder indenfor cybersikkerhed, som der ikke er specifikke krav om. Således svarer godt 9 procent af respondenterne, at de har valgt at følge cybersikkerhedsstandarder, selvom de ikke møder krav om det. Samlet følger godt 26 procent af respondenterne således cybersikkerhedsstandarder enten som følge af eksterne krav eller frivilligt. Respondenterne, som har angivet et ja, har også her haft mulighed for at angive hvilke standarder, der er tale om. Svarene herfor fremgår af tabel 4.2.

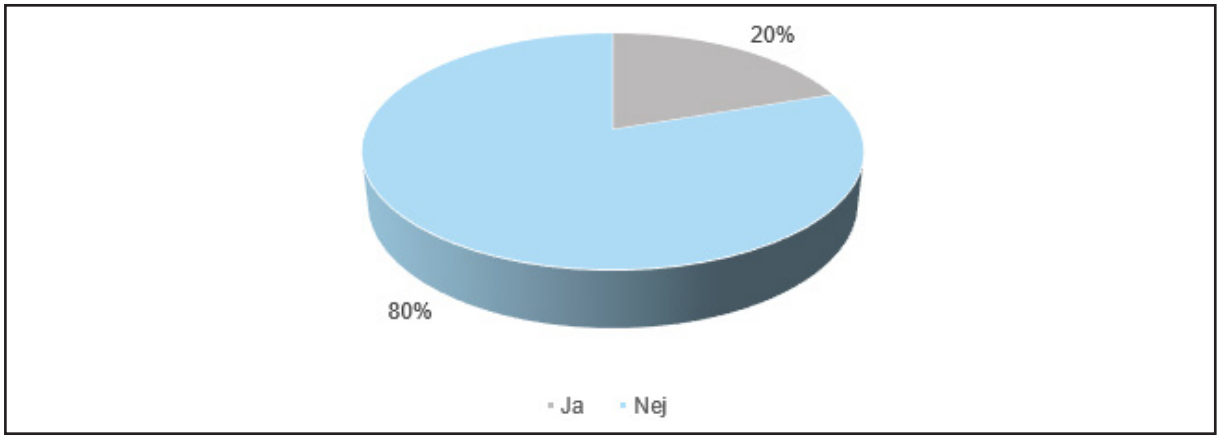
Tabel 4.2: Standarder, der frivilligt følges

- **CER-2**
- **CIS18**
- **CIS20**
- **Cisco AnyConnect**
- **CMMC Level 3**
- **D-mærket**
- **GDPR**
- **ISO27001/27001**
- **NIS2**
- **SOC 2**
- **Cyber Resilience Act**
- **Cyber Security Act**

4.3.3 Cyberangreb

I den seneste tid har medierne rapporteret om en kraftig vækst i antallet af cyberangreb som f.eks. phishing, smishing, malware, ransomware og Distributed Denial of Service (DDS). Virksomheder er blevet mere sårbare i takt med produkters og udstyrs stigende tilkobling til internettet. Det er i undersøgelsen derfor fundet interessant at spørge ind til dette. På spørgsmålet om, hvorvidt virksomhederne har været ramt af cyberangreb indenfor de seneste par år, har respondenterne svaret som vist i figur 4.7. Her fremgår det, at 20 procent har været udsat for cyberangreb indenfor de seneste par år. 80 procent af virksomhederne angiver, at de ikke har været udsat for cyberangreb de seneste par år. Dette kan selvfølgeligt skyldes, at de ikke har været udsat for cyberangreb, mens en anden mulig forklaring kan være, at man ikke ønsker at svare på dette, idet det kan bidrage til at forringe virksomhedens omdømme.

Figur 4.7: Har jeres virksomhed været ramt af cyberangreb indenfor de seneste par år?

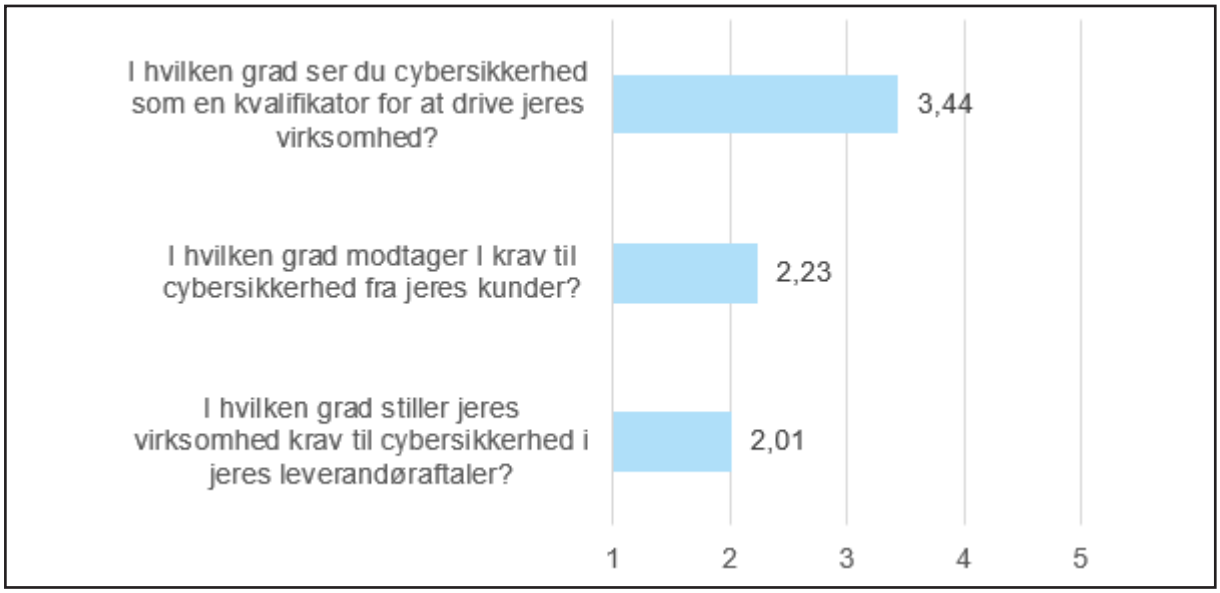


4.4 Cybersikkerhed som en kvalifikator

Hill (1986) skelner mellem kriterier, der kvalificerer til at få en ordre og kriterier, der direkte er med til at vinde ordrer. Ordrekvalifikatorer er forhold, som får et produkt og/eller serviceydelse ind på markedet eller på kundens liste over mulige produkter. Ordrevinderkriterier differentierer et produkt og/eller en serviceydelse fra konkurrenternes, ved at de gør produktet/serviceydelsen mere attraktiv for kunden. Over tid ser man en udvikling fra, at ordrevinderkriterier bliver basale kvalifikatorer som f.eks. ved udbredelsen af ISO 9001 op gennem 90'erne.

Respondenterne angiver i figur 4.8, at de i lidt mere end nogen grad anser cybersikkerhed som en kvalifikator i forhold til at kunne operere på markedet (3,44 på en fem-punkts Likert-skala, hvor 1 = i meget lav grad og 5 = i meget høj grad). Selvom virksomhederne i lidt over nogen grad anser cybersikkerhed som en kvalifikator, er dette ikke udsprunget af kundernes krav, idet krav fra kunderne kun angives i mindre grad (2,23). Dette stemmer overens med, at det især er fra bestyrelsen, at kravene til cybersikkerhed udspringer (med 3,43 jf. figur 4.4 ovenfor). Samtidig ses det af figur 4.8, at selvom cybersikkerhed i lidt over nogen grad anses som en kvalifikator, sendes denne forventning kun i mindre grad videre til leverandørerne (med et gennemsnit på 2,01). Da en kæde kun er så stærk som det svageste led, synes der her at være en oplagt mulighed for forbedring.

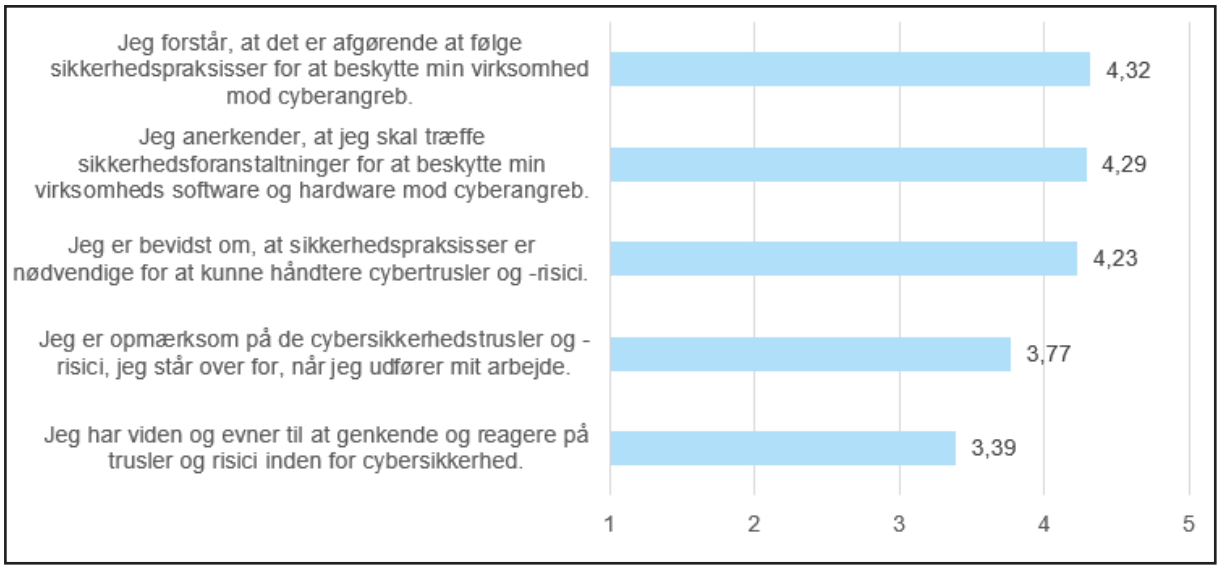
Figur 4.8: Cybersikkerhed som en kvalifikator og krav til cybersikkerhed



4.5 Opmærksomhed på cybersikkerhed

I undersøgelsen er der også spurgt ind til respondenternes egen opmærksomhed på cybersikkerhed. Svarene hertil fremgår af figur 4.9, og de er alle angivet som gennemsnit på en fem-punkts Likert-skala, hvor 1 = i meget lav grad og 5 = i meget høj grad. Som det fremgår, forstår respondenterne i mere end høj grad, at de skal træffe sikkerhedsforanstaltninger med et gennemsnit på 4,29. De finder det også af afgørende betydning at følge sikkerhedspraksisser med et gennemsnit på 4,32, og så ser de de angivne sikkerhedspraksisser som nødvendige for virksomhedens cyberforsvar med et gennemsnit på 4,23. De tre nævnte kan anses som passive elementer. I lidt mindre grad angiver respondenterne aktive elementer, som at de er opmærksomme på de cybertrusler og -risici, de står overfor i deres arbejde (3,77). Ligeledes angiver respondenterne, at de kun i godt og vel nogen grad (3,39) har kompetencer, via viden og evner, til at genkende og reagerer på trusler og risici indenfor cybersikkerhed. Samlet set opnår de fem udsagn om cyberopmærksomhed tilsammen et gennemsnit på 4,0, hvilket indikerer en god opmærksomhed på cybersikkerhed.

Figur 4.9: Opmærksomhed på cybersikkerhed



4.6 Cybersikkerhed supply chain risk management

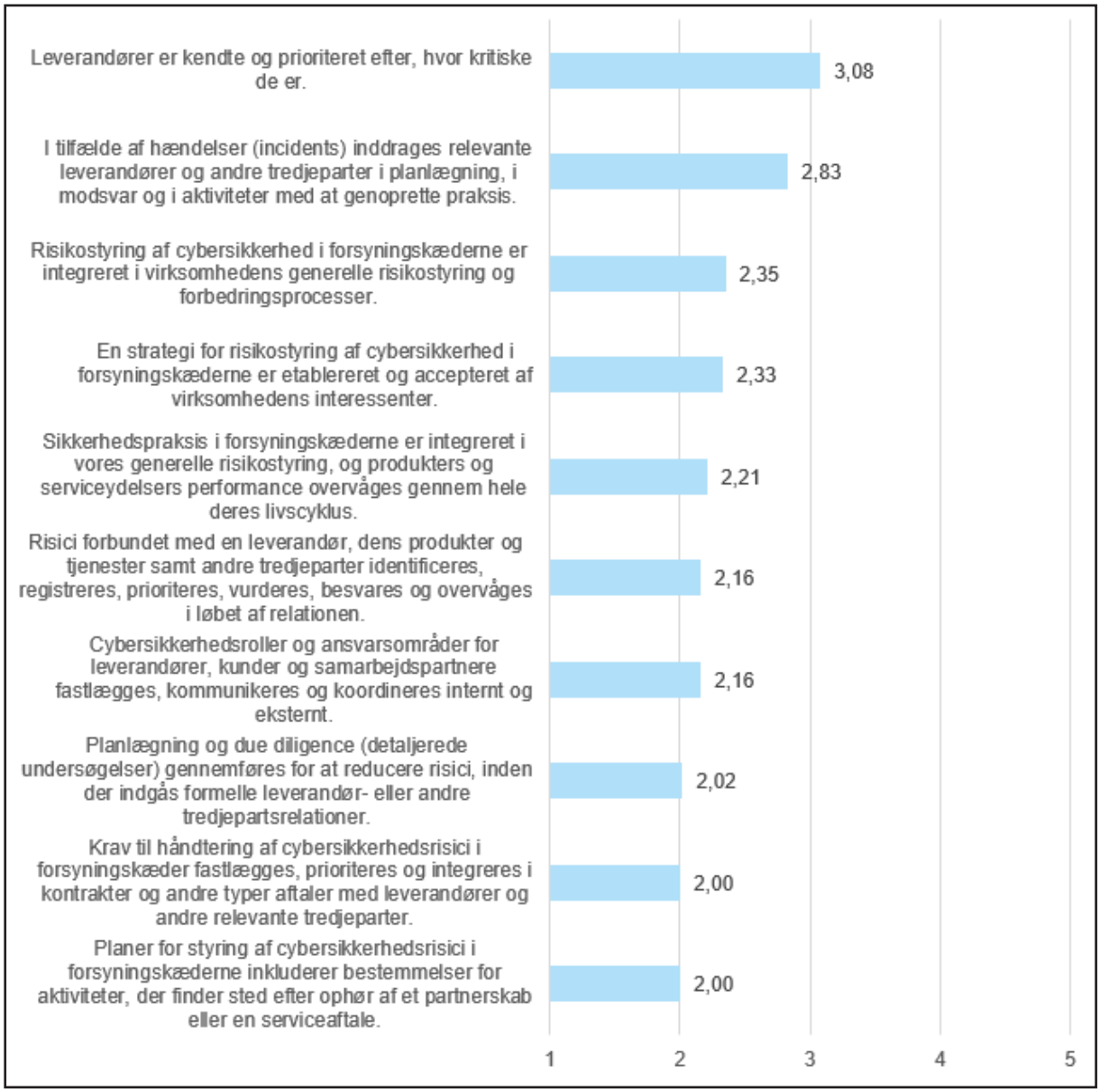
Respondenterne er også blevet spurgt ind til deres risikostyring i et forsyningskædeperspektiv. Den amerikanske organisation National Institute of Standards and Technology (NIST) har i 2024 udgivet et opdateret Cybersecurity Framework, som også indeholder spørgsmål om cybersikkerhed supply chain risk management. Det nye framework er benævnt NIST CSF 2.0. Denne opdatering sigter mod bedre at afspejle det moderne cybersikkerheds-

landskab og adressere nye trusler og teknologier for at sikre, at frameworket er relevant og effektivt til at hjælpe virksomheder med at forbedre deres overordnede cybersikkerhedsposition (NIST, 2024). Med det nye NIST-fokus på cybersikkerhed supply chain risk management rettes opmærksomheden mod forsyningskæden, hvilket er anbefalet i den akademiske litteratur (Chadge et al., 2020; Colicchia et al., 2019). Svar på de ti udsagn om cybersikkerhed supply chain risk management fra NIST CSF 2.0 fremgår af figur 4.10. Resultaterne viser, at leverandørerne kun i nogen grad er kendte og prioriteret efter, hvor kritiske de er (gennemsnitlig 3,08 på en fem-punkts Likert-skala). Tæt herefter angives inddragelse af relevante leverandører og andre tredjeparter i forhold til at genoprette praksis ved en hændelse med en gennemsnitlig score på 2,83. Med andre ord prioriteres leverandørerne kun i nogen grad efter kritiskhed, og hvis der sker en hændelse, inddrages de også kun i nogen grad. Der synes her at være en oplagt mulighed for forbedringer.

Endnu værre ser det ud, hvis vi ser på svarene i forhold til, hvorvidt risikostyring i forhold til cybersikkerhed i forsyningskæderne er integreret i virksomhedens almindelige risikostyring og forbedringsprocesser. Her angives 2,35 i gennemsnit, hvilket kun ligger lige over "i lav grad", som er 2,0. Man kunne så håbe på, at virksomhederne havde udviklet en strategi for ovenstående, og at det 'blot' er et spørgsmål om implementering. Tallene i figur 4.10 viser dog, at dette ikke er tilfældet, idet det gennemsnitlige svar på, om der er udviklet en strategi for ovenstående spørgsmål, ligger på 2,33 på Likert-skalaen. Givet det øgede fokus på og risici omkring cybersikkerhed i forsyningskæderne venter der et stort arbejde med at udvikle strategier for cybersikkerhed, der også indeholder et forsyningskædeperspektiv og ikke mindst konkret arbejde med at implementere strategierne.

Rolle- og ansvarsfordelingen omkring cybersikkerhed i forhold til leverandører, kunder og andre samarbejdsparter fastlægges, kommunikeres og koordineres internt og eksternt kun i mindre grad med et gennemsnit på 2,16. Dette er forventeligt, idet virksomhederne endnu ikke har udviklet strategier, som de kan læne sig op ad i forhold hertil. Det samme gælder for en integreret sikkerhedspraksis i forsyningskæderne i forhold til den generelle risikostyring, som ligeledes kun foregår i mindre grad (2,16).

Figur 4.10: Cybersikkerhed supply chain risk management



Det er overraskende, at der ikke i større grad sker en planlægning og gennemførelse af due diligence (detaljeret undersøgelse) for at mindske risici, inden der indgås formelle leverandør- eller tredjepartsrelationer. Respondenterne svarer hertil, at dette kun finder sted i mindre grad med et gennemsnit på 2,02. Ligeledes fastlægges krav til, hvordan cybersikkerhedsrisici i forsyningskæden håndteres i kontrakter også kun i mindre grad med et gennemsnit på 2,00. Dette kan dog sandsynligvis tillægges den manglende strategi og implementering heraf, som nævnt ovenfor. Det samme gør sig gældende for, hvordan et relationsophør skal håndteres i forhold til cybersikkerhed. Her angives ligeledes 2,00 i forhold til, hvorvidt cybersikkerhedsplanerne indeholder bestemmelser herfor. Samlet set indikerer resultaterne om cybersikkerhed supply chain risk management, at der er en lav praksis på dette område med et samlet gennemsnit på 2,30 for de ti udsagn. Dette resultat afviger væsentligt fra In-

dustriens Fonds cyberbarometer fra 2023, der konkluderer, at en betydelig del af SMV'erne har et supply chain fokus på cybersikkerhed (Dahl et al., 2023, p. 10). Der er således behov for, at der udvikles metoder og værktøjer, der kan hjælpe produktions-SMV'erne med at få konkrete indsatser igangsat på området. Respondenterne har også haft mulighed for at skrive kommentarer til emnet omkring cybersikkerhed. Tabel 4.3 indeholder relevante citater, der kan medvirke til refleksion over egen praksis på området.

Tabel 4.3: Udvalgte udsagn fra respondenter om cybersikkerhed

Der er umiddelbart stor forskel på strategiske ydelsesleverandører som IT, revision, bank, forsikring, m.m. og så over til råvareleverandører, hvor vi ofte vil have alternative leverandører at kunne gå til.
Der afholdes uddannelse online med eksempler såsom videoer om hacker, phishing, password for alle medarbejdere uanset titel.
Cybersikkerhed koster, men man sover bedre.
Det er jo interessant, at vi som virksomhed i høj grad vurderer vores kritiske leverandører, men i meget lav grad har cyber risk med i denne vurdering. Derfor er denne undersøgelse relevant og interessant.
Cybersikkerhed er et fokusområde for bestyrelsen. Vi er påbegyndt en række tiltag og har implementeret en række (primært tekniske) sikkerhedstiltag, ligesom vi har et struktureret samarbejde med flere eksterne cybersikkerhedsvirksomheder.
Vedtagelsen af NIS2 vil øge kravet til håndtering af cybersikkerhed i vores industri.
Det eneste incident, vi har haft, var på en gammel ubeskyttet PC. Det skal naturligvis ikke ske igen.
Vi er usikre på, hvordan vi er beskyttet, og forstår umiddelbart ikke den information, vi modtager fra vores leverandør af IT.
Vi har i vores SWOT-analyse anerkendt cybersikkerhed som en af vores allerstørste risici.
Vi håber vores dataleverandør har styr på det.
Vi er meget opmærksomme på vores cybersikkerhed, men har ikke rettet særligt fokus på vores leverandører i den forbindelse, snarere på vores egen praksis og sikkerhed.
Omend det har stor vigtighed med cybersikkerhed i forsyningskæden, så er vi ikke på et modenhedsstadie endnu, hvor det får den korrekte opmærksomhed.
Som ansvarlig for IT i vores gruppe har vi fokus på processerne i vores egne selskaber og læner os op ad CIS18. IT-afdelingen er dog ikke involveret i overvejelser omkring business continuity, da dette sorterer under vores indkøbsafdeling. Jeg ser her en problemstilling i, at vores indkøbsafdeling ikke er klædt på til at varetage opgaven. Jeg oplever, at de spørgeskemaer, som vi modtager fra kunder, svarer til de punkter, som er listet i ISO27000/CIS18/NIS2. Dette giver selvfølgelig god mening, da der ikke er grund til at opfinde noget selv, hvis man kan trække på eksisterende standarder. Jeg

tænker derfor, at IT-certificering vil blive måden, hvorpå man sikrer sig, at underleverandører lever op til et givet niveau af cyber resilience, fordi en indkøbsafdeling vil ikke have kompetence til at auditere en underleverandørs IT-sikkerhed.

Vi har fået lavet en statusrapport fra en ekstern rådgiver og arbejder nu målrettet med cybersikkerhed og udbedring af de identificerede findings.

Der er løbende intern træning i dette emne.

Vi er nærmest paniske over risikoen for cyberangreb. Vi er dagligt udsat for ca. 5-700 forsøg på/angreb for at komme på vores server.

Generelt er der et efterslæb af IT-relevante aktiviteter, der skal gøres for at komme op på et acceptabelt sikkerhedsniveau.

Det er svært for mindre virksomheder at afsætte de helt store formelle ressourcer. Man læser lidt op på det og snakker om det, men det er svært at få tid til at inkorporere det formelt.

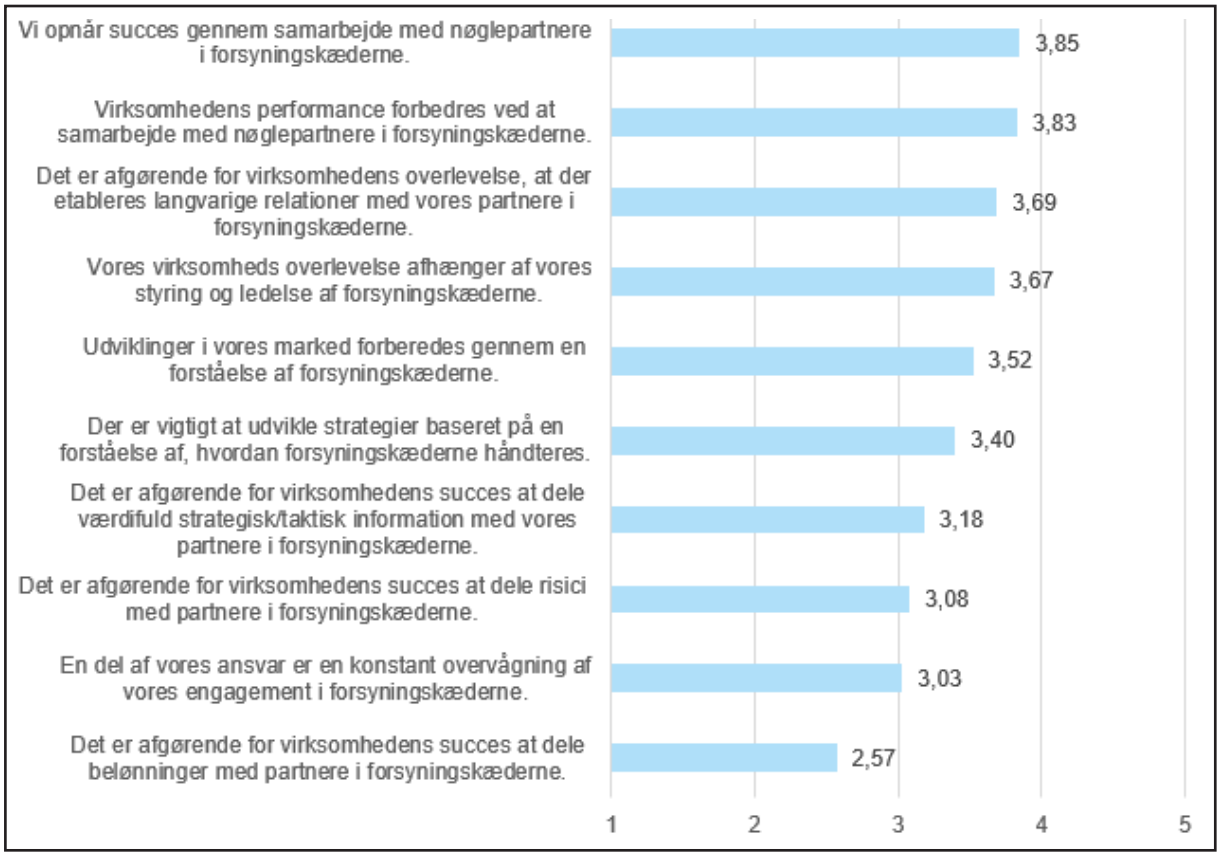
Det er måske lidt en sovepude for SMV´er, som føler sig sikre på forsyningskæden hos de store producenter.

Bestyrelsen har gennemgået og deltaget på informationsmøde omkring cybersikkerhed. Direktionen er bevidst om truslen. Området virker uoverskueligt, og man kan let både over- og underkompensere.

4.7 Supply chain orientering

Respondenterne er også spurgt ind til deres supply chain orientering ved at skulle svare på ti udsagn omkring dette (se figur 4.11). Som det fremgår af figur 4.11, er det især samarbejde med nøgleaktører og langvarige relationer som respondenterne tillægger værdi. Succes gennem samarbejde med nøglepartnere i forsyningskæderne angives således med en gennemsnitsværdi på 3,85, mens samarbejde med nøglepartnere i forsyningskæderne for forbedret performance opnår et gennemsnit på 3,83. Langvarige relationer med partnere i forsyningskæderne, der er afgørende for virksomhedens overlevelse, opnår et gennemsnit på 3,69. Lige herefter kommer vigtigheden af styring og ledelsen af forsyningskæderne for virksomhedens overlevelse med en gennemsnitsværdi på 3,67. Knap så højt tillægges værdien af, at en forståelse af forsyningskæderne påvirker udviklinger i markedet med et gennemsnit på 3,52. Vigtigheden af udvikling af strategier for, hvordan forsyningskæderne håndteres, tillægges lidt mindre værdi med et gennemsnit på 3,40. Deling af strategisk information samt risici med partnere i forsyningskæderne opnår gennemsnit svarende til ”i nogen grad” med henholdsvis 3,18 og 3,08. Respondenterne anser ligeledes i nogen grad med et gennemsnit på 3,03, at de har et ansvar for en konstant overvågning af virksomhedens engagement i forsyningskæderne.

Figur 4.11: Supply chain orientering



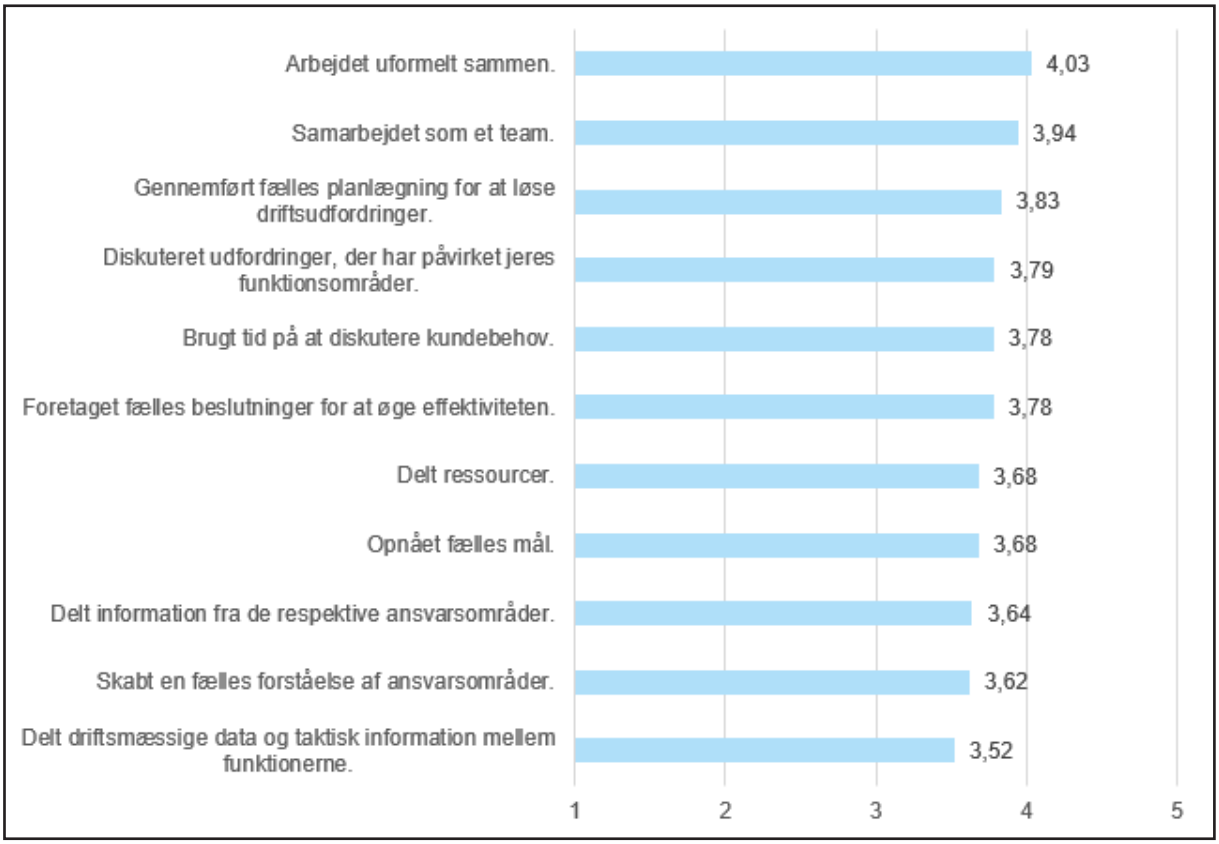
Slutteligt mener respondenterne ikke, at virksomhedens succes i så høj grad hænger sammen med at dele belønninger med partnerne i forsyningskæderne, hvilket kun opnår en gennemsnitsværdi på 2,57.

4.8 Intern integration

Cybersikkerhed er ikke noget, der alene vedrører IT-afdelingen eller en sikkerhedsansvarlig (Shortridge & Rinehart, 2023, p. 73). Det er et anliggende for hele virksomheden. Derfor er der spurgt ind til, hvor internt integreret man opfatter, at virksomhederne er, idet den interne integration er væsentlig for at sikre en tværorganisatorisk forankring for cybersikkerheden. Respondenternes svar på 11 udsagn om intern integration fremgår af figur 4.12. Alle 11 udsagn opnår signifikante gennemsnitsværdier (her vurderet fra 3,50) fra 3,52 til 4,03. Uformelt samarbejde ligger i toppen med et gennemsnit på 4,03 (i høj grad) tæt fulgt af samarbejde som team med et gennemsnit på 3,94, mens deling af driftsmæssige data og taktiske informationer ligger i bunden med et gennemsnit på 3,52. Den samlede gennemsnitsværdi for de 11 udsagn er 3,75, hvilket indikerer en god intern integration i virksomhederne, som bør udnyttes for at skabe større cybersikkerhed. Dette understøtter lignende resultater fra en undersøgelse i 2023 (Stentoft et al., 2023a) samt vigtigheden af intern forankring, som konkluderet i cyberbarometeret fra Industriens Fond i 2023

(Dahl et al., 2023, p. 9). I danske produktions SMV'er kan man synliggøre de 11 udsagn blandt virksomhedens medarbejdere og relatere dem til, hvordan disse integrationselementer kan fremme opmærksomheden og praksis med cybersikkerhed.

Figur 4.12: Intern integration

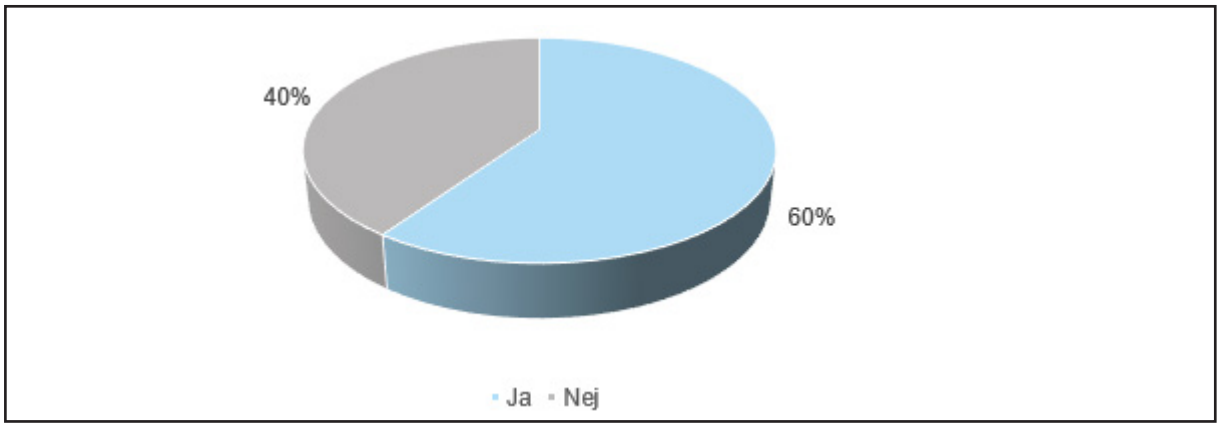


4.9 Geopolitik

Geopolitiske spændinger fylder mere og mere i produktions SMV'ernes daglige drift af de forsyningskæder, de er deltagere i. Det er forhold som Ruslands invasion i Ukraine, konflikten i Gaza, Houthiernes bombninger i Suezkanalen samt spændinger mellem USA og Kina. Geopolitiske spændinger øger brugen af cyberangreb. Respondenterne er derfor blevet introduceret til geopolitik på følgende måde: "Med geopolitiske forstyrrelser/risici forstår vi de chok/udfordringer, der forekommer i det internationale forretningssystem afledt af krige, militærangreb, våbenkontrol, terrorisme, cyberangreb og diplomatiske kriser". Med afsæt i denne beskrivelse af geopolitik er respondenterne blevet spurgt om, hvorvidt de tager højde for geopolitiske risici i den måde, de driver forretning på. Svarene hertil fremgår af figur 4.13, som viser, at 60 procent tager højde for geopolitiske forstyrrelser/risici. Det efterlader på den anden side 40 procent, som ikke tager højde for geopolitiske risici i den

måde forretningen drives på. Det kan skyldes, at det reelt ikke er nødvendigt at tage højde for geopolitiske forhold, eller at der mangler opmærksomhed og/eller viden om området.

Figur 4.13: Tager I højde for geopolitiske risici i ledelsen af virksomheden?



De virksomheder, som har svaret 'ja' har haft mulighed for at angive, hvordan de tager højde for de geopolitiske forhold. Eksempler herpå fremgår af tabel 4.4.

Tabel 4.4: Udsagn om, hvordan der tages højde for geopolitiske risici

IT-løsninger
- *Firewall, multifaktorautentificering og AV-løsninger har mulighed for at blokere data til forskellige lande.*
- *Vi har et godt SPAM-filter, hvor jeg holder ekstra øje med mails, der har afsendere fra lande, det geopolitisk kan give mening at holde øje med.*

Kina
- *Vi har fabrik i Kina, så den er altid på radaren.*
- *Vi spreder risici især i forhold til Kina.*
- *Vi undgår f.eks. indkøb og direkte samarbejde med Kina.*

Sekundære forsyningskilder
- *Vi forsøger at tage højde for udfordringer ved at arbejde på sekundære forsyningskilder. F.eks. fik vi udelukkende ståleverancer fra Kina før i tiden, men nu har vi også en mindre produktion i Østeuropa, der kan skaleres op.*

Ledelse
- *Emnet drøftes løbende på ledermøder.*
- *Early Warning meetings.*
- *Geopolitiske trusler skaber nye angrebsvektorer, der skal beskyttes imod.*

Markeder og kunder

- *Vi screener markeder.*
- *Stort fokus på, hvilke lande vi leverer til.*
- *Vi evaluerer, hvilke markeder vi køber og sælger vores produkter på.*
- *Validering af kunder og deres tilhørsforhold.*
- *Markedsovervågning, risikovurdering på supply og omkostninger.*
- *Vi fravælger forretninger med f.eks. Rusland.*
- *Vi scanner den politiske situation i forhold til markedet.*
- *Vi har fravalgt projekter i risikozoner.*

Sourcing strategi

- *Valg af leverandører inkl. geografisk position, dual sourcing strategy, løsning af leveringsudfordringer til krigsprægede områder etc.*
- *Valg af lande vi outsourcer til.*
- *Insourcing ifm. Kina/Taiwan problematikken.*
- *Nearshoring.*
- *Vi sourcer indenfor EU.*
- *Lokal sourcing.*
- *Regional supply chain strategi.*
- *Sourcer mere fra nærområder.*
- *Vi bruger lokale leverandører eller leverandører fra EU. IKKE fra Kina og Rusland.*
- *Vi multisourcer og forsøger generelt hele tiden at holde os informeret om, hvad der sker i nær og fjern.*
- *Vi forsøger at ændre vores sourcing til friendshoring fra blot outsourcing.*
- *Vi har flere leverandører på samme produkter, men med forskellige lokaliseringer i verden.*
- *Langsigtede indkøb, planlægningshorisonten er steget til 1 år.*

Lagre

- *Vi har udvidet lageret af kritiske komponenter.*
- *Opbygning af lagre.*

Geografisk spredning

- *Ved at sprede vores produktions-sites.*
- *Geografisk spredning af aktiviteter og overvågning af leverandørers muligheder for at overholde aftaler på trods af internationale kriser (f.eks. krig og pandemi).*
- *Gennem et regionalt produktions-setup (Kina, USA, EU).*
- *Vi forsøger at sikre, at leverandører af samme produkter er placeret geografisk i forskellige dele af verden.*

Governance

- *Leverandører forpligter sig til at overholde international lov og restriktioner, som vi skal overfor vores kunder også.*
- *Vi følger FN's sanktionslister. Som producent af medicinsk udstyr har vi meget at gøre med hospitaler, hvorfor det spiller en stor rolle.*
- *Via godkendelse af flere leverandører.*
- *Vi har geografiske områder, som vi ikke kan/må samhandle med.*

Prisudvikling

- *Gaspriser fylder en del.*
- *Energi- og råvarepriser overvåges.*
- *Håndtering af udsving i råvarepriser og vores egen prissætning.*
- *Monitorerer en lang række prisindeks.*

Risikostyring

- *Analyse af risici for disruptions på markeder, transportudfordringer, krig m.m.*
- *ERM-analyser (Enterprise Risk Management).*
- *Vi prøver at undgå afhængighed af leverandører fra "risikoområder".*
- *Vi er bevidste om risikoen og lever med den.*
- *Vi forsøger i videst muligt omfang at placere vore forretning i "sikre" områder.*
- *Opmærksomhed på risikoen for råvaremangel.*
- *Vi er opmærksomme på forsyningssikkerhed af kritiske komponenter.*
- *Vi forsøger efter bedste evne at forholde os til ændringerne i takt med, at de bliver synlige for os (muligheder og trusler).*
- *Lead-times og forsyningssikkerhed.*

Kilde: Respondenter fra spørgeskemaundersøgelsen.

Respondenterne er ligeledes spurgt om, hvor de finder informationer om geopolitiske risici. Eksempler på sådanne kilder fremgår af tabel 4.5.

Tabel 4.5: Kilder til information om geopolitiske forhold

Ambassader
Brancheforeninger **Børsen**
Center for cybersikkerhed **CSR-rapporter**
DanishCare **Dansk Industri** **Danske Bank**

Dialog i branchen

ERFA-grupper
Erhvervsministeriet
EU-orienteringer

Fagpressen
FET (Forsvarets Efterretningstjeneste)

Generelle nyheder
Gennem speditører/rederier
Gennem vores risk-management proces

Information fra finansielle institutioner, myndigheder etc.
Interesseorganisationer
Internationale relationer

Konferencer
Kunder

Leverandører
Leverandør-opfølgninger (supply-demand reviews)
Lokale medarbejdere i Øst Europa og Asien

Markedsinformation fra forretningspartnere
Market intelligence

Netaviser
Netværk
Nyhederne
Nyhedsbreve

OECD
OSINT (Open-Source Intelligence)

Podcast
Proaktiv information fra partnere

Snak med leverandører
Sociale medier
Statistikker
Symposier

The Economist
Tilgængelige informationer på nettet

Udenrigsministeriet
Uvildige konsulenter

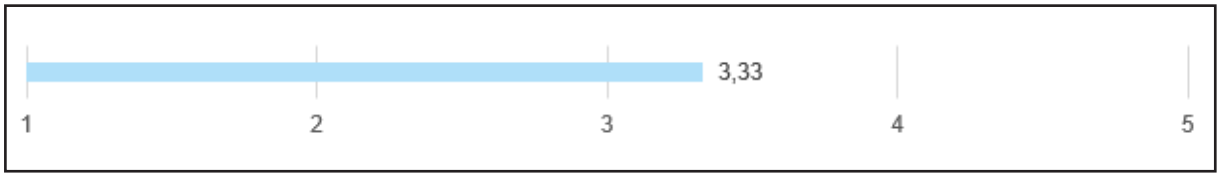
Vi har en afdeling, som kun arbejder med dette.
Vi har en løbende dialog med forretningsforbindelser, hvor vi afstemmer vores syn på udviklingen.
Via gratis og betalte indeks og datakilder monitorerer vi de udviklinger, der hele tiden sker i forhold til den geopolitiske udvikling.

Webinarer via samarbejdspartnere

Kilde: Respondenter fra spørgeskemaundersøgelsen.

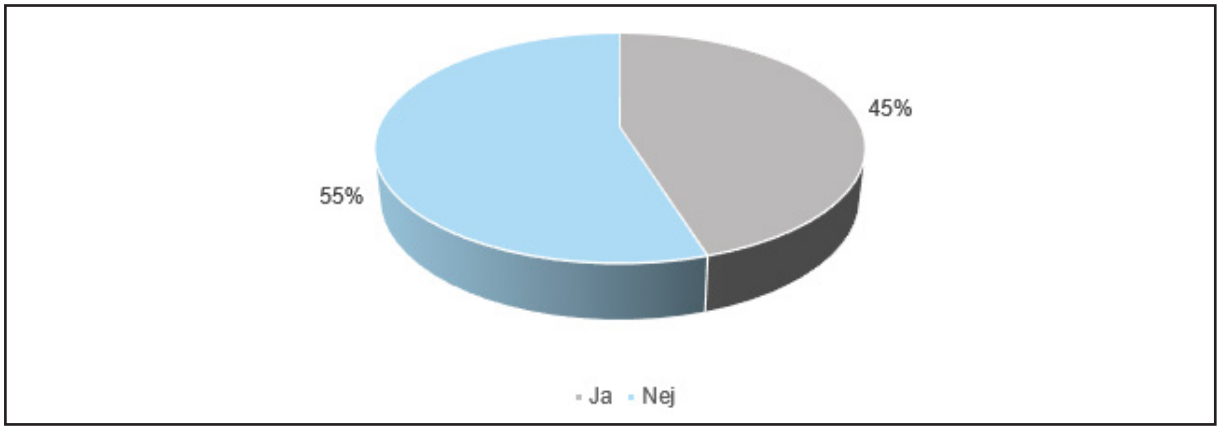
Respondenterne er endvidere blevet spurgt om i hvilken grad, de har viden om, hvordan geopolitiske risici kan påvirke forretningen. Svarene hertil fremgår af figur 4.14, som viser, at virksomhederne kun i lidt mere end nogen grad har denne viden med et gennemsnit på 3,33 på en fem-punkts Likert-skala, hvor 1 = i meget lav grad og 5 = i meget høj grad. Dette svar indikerer et behov for kompetenceudvikling om geopolitiske risici, og hvordan de kan håndteres for at styrke virksomhedernes supply chain resilience.

Figur 4.14: Grad af viden om hvordan geopolitiske risici kan påvirke forretningen



Respondenterne har også svaret på, om dansk og/eller europæisk lovgivning har påvirket deres samarbejdsrelationer i andre lande. Som det fremgår af figur 4.15, viser svarene, at 45 procent af respondenterne svarer 'ja' til dette.

Figur 4.15: Påvirkning fra lovgivning til samarbejdspartnere i andre lande



Hvad angår lovgivningen har de respondenter, som har svaret 'ja', kunnet angive i fritekst hvilken lovgivning og hvordan, det har påvirket.

Tabel 4.6: Eksempler på lovgivning der påvirker relationer med internationale samarbejdspartnere

BR18 – Udenlandske leverandører der skal kunne leve op til den danske byggelovgivning
Brexit

CBAM (Carbon Border Adjustment Mechanism)
CSRD (Corporate Social Responsibility Directive)

Databehandleraftale, hvor US-underleverandører er uønskede

EUDR (Deforestation-Free Regulation)
Efterspørgsel efter mere bæredygtige produkter fra underleverandører, der er funderet i strammere EU-lovgivning, som også påvirker vores branche (byggeri)
EN-normer og regler
ESG (Environmental, Social & Governance)
EU-emballage- og miljødirektiv
EU-MDR (The European Union Medical Device Regulation)
EU-pakkedirektiv
EU-sanktioner

GDPR dataopbevaring

HS-koder (Tarifkoder)
Hvidvask-lovgivning

IFS-certificering kræves af alle aktører i vores branche
Importtold på kinesiske varer

Kemisk lovgivning fra Echa. Labelling m.m. (European Chemicals Agency)
Konkurrencelovgivning
Krav om momsregistrering i lande, hvorfra vi eksporterer

Lægemiddellovgivning (DK/EU)

Maskindirektivet samt standarder indenfor forskellige områder omkring vores virke

NIS2 (Net- og informationssikkerhed)

PFAS (Perfluorerede og polyfluorerede alkylstoffer)

Rusland embargo

Transport (EU-mobilitetspakker, kilometerafgift)

Udvidet lovgivning på tobaksområdet herunder Tobacco Track & Trace direktivet

Vejskat i Tyskland

Kilde: Respondenter fra spørgeskemaundersøgelsen.

Tabel 4.7 viser udsagn fra respondenterne, der viser deres forståelse af geopolitik.

Tabel 4.7: Udvalgte udsagn om geopolitik fra respondenterne

Global footprint

- *En del af vores sourcing sker fra Kina, så der arbejdes aktivt på alternative sourcing-kanaler på kritiske komponenter.*
- *Flytter produktion rundt i lande som: Kina, Indien, Ukraine, Tyrkiet, Bulgarien osv.*
- *Vi er bevidste om de risici, der er på globalt plan og har bl.a. derfor også igangsat et projekt, der hedder "Supply Chain Closer to Home".*
- *Vi har en strategi om at tage underleverandørproduktion hjem fra hhv. asien (Kina) og Mellemøsten.*
- *Vi har produktion i Kina, som vi er meget afhængig af, idet der leveres komponenter og færdige produkter til Europa. Vi er bevidste om risikoen, men det, at skulle mitigere den, er utrolig ressourcekrævende (omfang 48% af indkøbsvolumen), og derfor er opgaven blevet udskudt mange gange. Vi har dog som strategisk indsatsområde, at der skal arbejdes med at opbygge netværk af alternative leverandører i Europa/Nordafrika.*

Lovgivning

- *Vi er i dialog med forskellige stakeholders ift. lovgivning, så vi overholder det, der kræves i vores eksportlande.*
- *Arbejdsmiljø i 3. lande influerer på salg i f.eks. Norge/Sverige (monopolet/systemet).*
- *Flere beder om compliance på PFAS og større fokus på overholdelse af EU-lovgivning såsom REACH (Registration, Evaluation, Authorisation and Restriction of Chemicals) m.v.*
- *Vi oplever, at US lovgivning (ITAR - International Traffic in Arms Regulations) påvirker os.*
- *Vores råvarer fra Rusland er ikke sanktioneret af EU og USA, men virksomhedens aktionærer har valgt, trods dette, ikke at arbejde med firmaer i Rusland og Belarus.*
- *Vi skal være meget agile i forhold til de hurtige beslutninger, der tages fra EU's side og krav til bæredygtighed for vores leverandører, som der også kommer mere af.*

Politisk uro

- *Vi er meget opmærksomme på, hvad en konflikt mellem Taiwan og Kina kan betyde for forsyningssikkerheden.*
- *Vi analyserer og er opmærksomme på kommende problemer.*
- *Vi oplever udsving i tilfælde af krig eller finanskrise, men ikke noget der adskiller sig nævneværdigt fra andre virksomheder i samme branche.*
- *Ca. 80% af virksomhedens omsætning eksporteres. Geopolitik, international økonomi, krig og konflikter har stor betydning for planlægning og prioritering af afsætning og forsyning af råvarer. En del af den resterende omsætning forarbejdes i Danmark og videreeksporteres. Geopolitik for vores kunder i Danmark er også vigtig at forstå.*

Flere forstyrrelser

- *Vi er alle i stigende grad følsomme overfor selv små geopolitiske situationer og ser gentagne gange chok-reaktioner, som påvirker forsyningskæderne. Det virker til, at der bliver kortere mellem udsving, og at de let kan få større udsving. Der er behov for høj grad af agilitet.*
- *Økonomisk afmatning er lige så slemt.*
- *Var meget udfordret sidste år i forbindelse med mangel på elektronikkomponenter. Vi følger dette marked relativt tæt og søger gennem produktudvikling at undgå komponenter, der kan opstå mangel på.*
- *Vores kunder er blevet ramt af bl.a. Covid-19; strejke blandt filmpersonale i USA; ændring i rentesituationen og global reduktion af lagre efter 2021/22, som slår igennem hos os.*

Ressourcer

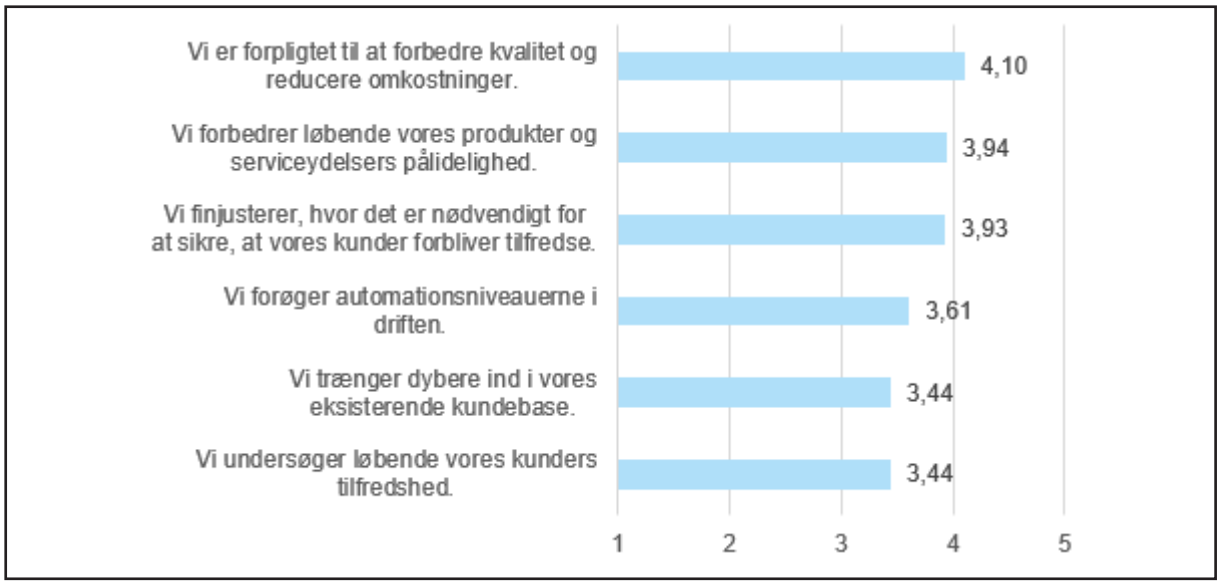
- *SMV'er kan kun iagttage og reagere reaktivt på geopolitik. Vi har ikke organisation eller kræfter til andet.*

Kilde: Respondenter fra spørgeskemaundersøgelsen.

4.10 Drift versus udvikling

Mange virksomheder, store som små, har udfordringer med at gennemføre konkret udvikling af forretningsgange samtidig med, at der er fokus på driftsopgaver. At styrke en virksomheds cybersikkerhed vil som oftest kræve, at der skal igangsættes udviklingstiltag, som skal prioriteres i en travl hverdag med drift. Derfor er det interessant at belyse, hvorledes respondenterne opfatter deres prioritering mellem drift og udvikling. I figur 4.16 fremgår resultaterne af respondenternes svar på seks udsagn vedrørende deres driftsorientering.

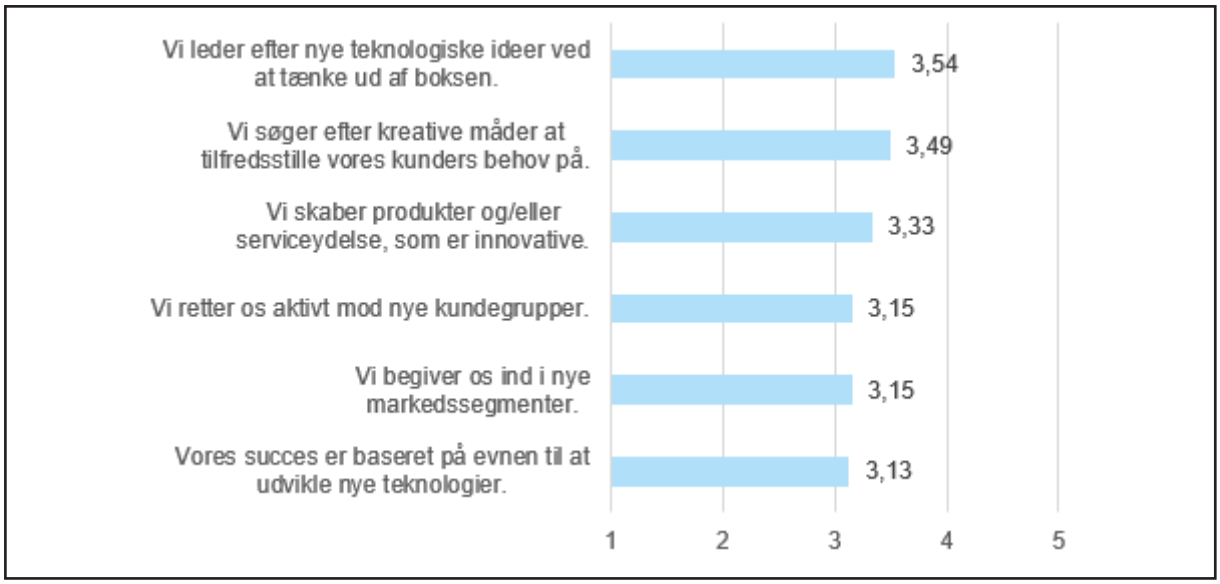
Figur 4.16: Driftsorientering



Respondenterne angiver, at de i høj grad er forpligtede til at forbedre kvaliteten og reducere omkostninger med et gennemsnit på 4,10, mens de tæt på "i høj grad" angiver, at de løbende optimerer på produkternes og serviceydelsernes pålidelighed med et gennemsnit på 3,94. Yderligere finjusterer de for at sikre tilfredse kunder med et gennemsnit på 3,93. Lidt lavere med et gennemsnit på 3,61 forøger virksomhederne automatiseringsniveauerne i driften. Sidst angiver virksomhederne, at de i lidt over "i nogen grad" trænger dybere ind i de eksisterende kundebaser med et gennemsnit på 3,44, og at de løbende undersøger kundernes tilfredshed ligeledes med et gennemsnit på 3,44. Det sidste kan synes lidt paradoksalt, idet virksomhederne samtidig i høj grad angiver, at de finjusterer for at sikre tilfredse kunder med et gennemsnit på 3,93. Dette kan måske skyldes, at respondenterne agerer aktivt i forhold til, hvis/når kunder kommer med ændringsforslag, hvorimod de ikke er nær så proaktive i løbende vurderinger af kundetilfredsheden.

Figur 4.17 indeholder respondenternes svar på deres opfattelser af deres virksomheders udviklingsorientering. Noget af det første, der lægges mærke til, er, at respondenterne angiver, at de generelt er mere driftsorienterede, end de er udviklingsorienterede. Det samlede gennemsnit for driftsorientering i figur 4.17 er på 3,74, mens det samlede gennemsnit for udviklingsorientering i figur 4.17 er på 3,30.

Figur 4.17: Udviklingsorientering



Resultaterne af svar i forhold til udviklingsorientering i figur 4.17 viser, at det kun er temaet omkring at lede efter nye teknologiske ideer ved at tænke ud af boksen, der opnår en gennemsnitsværdi på over 3,50 på en fem-punkts Likert-skala (helt præcist 3,54). Dette er tæt fulgt af udsagnet om, at virksomhederne søger efter kreative måder at tilfredsstille kundernes behov på med et gennemsnit på 3,49. Herefter følger skabelsen af produkter og/eller service-

ydelser, som er innovative, med et gennemsnit på 3,33. Nye kundegrupper og markedssegmenter følger herefter i nogen grad med en gennemsnitsværdi for hver på 3,15. De ovenstående svar har alle handlet om, hvad virksomhederne gør aktivt (leder, søger, skaber, retter og begiver). Den laveste score med et gennemsnit på 3,13 opnår udsagnet om deres evne til at udvikle nye teknologier. Det er vigtigt at pointere, at en balance mellem drift og udvikling ikke kræver, at der opnås de samme gennemsnitsværdier for henholdsvis drift og udvikling. Et balancepunkt kan godt være 75 procent på drift og 25 procent på udvikling. Tidligere forskning har vist, at jo højere grad af teknologiintensivitet en virksomhed har, jo større fokus er der også på udviklingsaktiviteter (Stentoft et al., 2017, p. 47). Fordelen ved at være bevidst om en driftsorientering kontra en udviklingsorientering er, at det kan give virksomheden et overblik over, hvordan dette konkret prioriteres. Respondenterne har også haft mulighed for at kommentere problemstillingen mellem drift og udvikling, hvilket er medtaget i tabel 4.8.

Tabel 4.8: Kommentarer til drift og udvikling

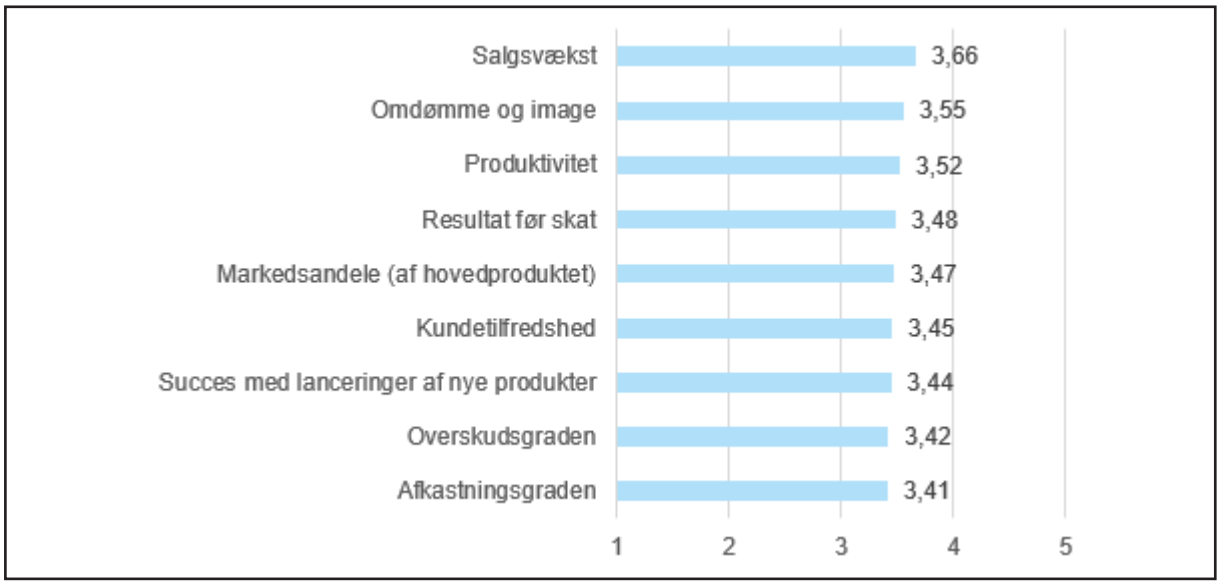
- *Vi søger samarbejder uden for virksomheden for at opnå indsigt i nye teknologier, materialer, bæredygtighedsagendaen m.m. Vi er en mindre virksomheden, der ikke kan være "dygtig til alt", derfor søger vi samarbejde med institutioner, brancheforeninger og andre private aktører.*
- *Vi forsøger at integrere mod slutkunden ved at arbejde mere helheds- og løsningsorienteret for at låse kunderne.*
- *Det kreative består i at optimere tiden, der anvendes på omstilling, og i udnyttelse af måleudstyret.*
- *Som underleverandør har vi ikke mulighed for at opsøge nye områder til at forøge vores indtjening.*
- *Vi er i B2B-markedet og udvikler ikke selv produkter som udgangspunkt, men producerer alene kundedefinerede produkter.*
- *Vi er gået fra mange små kunder til færre store kunder og bevæger os mod fastholdelse og udbygning af de store kunder eller potentielt store kunder.*
- *Vores B2B-kunder ændrer sig ikke meget.*
- *Vores produkt servicerer en niche.*
- *Vi har ikke behov for at finde andre kundegrupper.*
- *Møbelbranchen i vores segment er ret fastlåst.*
- *Vores produkter er rettet mod præcisionslandbrug. Den teknologiske udvikling på GPS satellitstyring af maskiner er derfor en vigtig driver for vores produktudvikling.*

Kilde: Respondenter fra spørgeskemaundersøgelsen.

4.11 Performanceudvikling

I undersøgelsen er respondenterne også blevet spurgt om, hvordan de opfatter deres virksomheders performanceudvikling på en række nøgleområder over de seneste tre år. Svarene fremgår af figur 4.18 (hvor 1 = meget værre, 2 = værre, 3 = status quo, 4 = bedre og 5 = meget bedre). Som det fremgår af figur 4.18, er ingen af performanceområderne blevet forværret over de seneste tre år. Det er især indenfor salgsvækst med et gennemsnit på 3,66, omdømme og image med et gennemsnit på 3,55 samt produktivitet med et gennemsnit på 3,52, at performance er blevet noget forbedret. De øvrige performanceområder er kun i mindre grad blevet forbedret over de seneste tre år. Det er interessant, at overskudsgraden (andelen af omsætning, der bliver til overskud) ikke synes at følge med den øgede salgsvækst og den øgede produktivitet. Det samme kan siges om afkastningsgraden. Men det kan selvfølgelig skyldes øgede materiale- og fragtomkostninger og/eller en øget aktivmasse.

Figur 4.18: Performanceudvikling over de seneste tre år



5. Konklusion

Denne rapport har haft til formål at undersøge praksis med cybersikkerhed i danske produktions SMV'er. Dette er sket gennem en landsdækkende spørgeskemaundersøgelse, hvor 1.293 SMV'er er kontaktet med henblik på deltagelse i undersøgelsen. 314 virksomheder ønskede at deltage i undersøgelsen, og ud af disse har 248 levereret fulde svar, hvilket fører til en svarprocent på 19,2 ud af de samlede kontaktede virksomheder og 78,9 procent ud af de virksomheder, der accepterede at deltage i undersøgelsen. Undersøgelsen søger at give svar på følgende spørgsmål:

1. Hvilke krav til cybersikkerhed og brug af standarder oplever virksomhederne?
2. I hvilket omfang har virksomhederne oplevet cyberangreb?
3. I hvilken grad opleves cybersikkerhed som en kvalifikator?
4. Hvor opmærksomme er virksomhederne på cybersikkerhed?
5. I hvilket omfang har virksomhederne fokus på cybersikkerhed supply chain risk management?
6. I hvilket omfang har de deltagende virksomheder en supply chain orientering?
7. I hvilket omfang er virksomhederne internt integreret?
8. I hvilket omfang har virksomhederne fokus på geopolitik?
9. Hvorledes har virksomhederne balanceret drifts- og udviklingsopgaver?

På spørgsmålet om, *hvilke krav virksomhederne oplever til cybersikkerhed og brug af standarder*, kan det konkluderes, at bestyrelsen i virksomhederne spiller den vigtigste rolle i at få arbejdet med cybersikkerhed igangsat med et gennemsnit på 3,43 på en fem-punkts Likert-skala. Gennemsnitsværdien på 3,43 udtrykker ikke et stærkt fokus fra bestyrelsen på trods af den massive opmærksomhed, der er rettet på denne problemstilling i medierne de seneste år. Krav fra investorer og krav fra kunder opnår endnu lavere gennemsnit på henholdsvis 2,91 og 2,55. Hvad angår krav til brug af standarder indenfor cybersikkerhed svarer 17 procent af deltagerne, at de modtager sådanne krav. Eksempler på sådanne standarder er NIST I&II, ISO27001/27002, CMMC og GDPR. 18 procent af respondenterne svarer, at de frivilligt har valgt at følge

standarder indenfor cybersikkerhed som f.eks. D-mærket, NIS2, Cyber Resilience Act og Cyber Security Act. På spørgsmålet, *i hvilket omfang virksomhederne har oplevet cyberangreb*, svarer 20 procent af respondenterne, at de indenfor de seneste par år har været udsat for cyberangreb. Cybersikkerhed kan også ses som en kvalifikator til at drive virksomhedens udvikling. Med et gennemsnit på 3,44 svarer respondenterne, at de lidt over "i nogen grad" ser *cybersikkerhed som en kvalifikator*, og som derved er noget, der kan styrke virksomhedens image. Respondenterne svarer med et gennemsnit på 2,01, at de stiller krav til cybersikkerhed hos deres leverandører, hvilket svarer til "i lav grad". Dette indikerer, at den nuværende cybersikkerhedspraksis primært er fokuseret på det interne virksomhedsperspektiv og i meget begrænset omfang har fokus på forsyningskæderne, hvilket indeholder et stort udviklingspotentiale.

På spørgsmålet om, *hvor opmærksomme virksomhederne er på cybersikkerhed*, kan det konkluderes, at respondenterne i høj grad er opmærksomme på cybersikkerhed med tre gennemsnitsværdier ud af fem, der scorer over 4,2. Respondenterne forstår, at det er afgørende at følge sikkerhedspraksisser for at beskytte sig mod cyberangreb med et gennemsnit på 4,32. Respondenterne anerkender, at de skal træffe sikkerhedsforanstaltninger for at beskytte mod cyberangreb med et gennemsnit på 4,29, og endelig er respondenterne bevidste om, at sikkerhedspraksisser er nødvendige for at kunne håndtere cybertrusler og -risici med et gennemsnit på 4,23. Respondenterne er blevet bedt om at tage stilling til ti udsagn om *cybersikkerhed supply chain risk management*, og resultatet viser, at kun ét udsagn opnår en gennemsnitsværdi omkring "i nogen grad", mens de øvrige ligger lavere med gennemsnit mellem 3,0 og 2,0. Det højeste gennemsnit er på 3,08 og handler om, at leverandører er kendte og prioriteret efter, hvor kritiske de er. Det samlede resultat peger på et lavt fokus på cybersikkerhed supply chain risk management og dermed et stort udviklingsbehov i virksomhederne. Respondenterne har også skulle tage stilling til en række udsagn omkring virksomhedens supply chain orientering, dvs. i hvilken grad, virksomheden forstår de strategiske implikationer af aktiviteter og processer, der er involveret i de forskellige flows i forsyningskæderne. Dette er sket for at kunne svare på spørgsmålet: *I hvilket omfang har de deltagende virksomheder en supply chain orientering?* Supply chain orientering er målt på ti udsagn, hvoraf fem opnår gennemsnit fra 3,52 op til 3,85, hvilket indikerer en generel god supply chain orientering. Eksempler er samarbejde med nøglepartnere, performanceforbedring gennem samarbejde og etablering af langvarige relationer. Det er positivt, at der opnås et samlet gennemsnit på 3,4 for de ti udsagn om supply chain orientering. Det er et godt udgangspunkt til at kunne begynde at styrke arbejdet med cybersikkerhed supply chain risk management, hvilket undersøgelsen, som beskrevet tidligere, viser, er på at relativt lavt niveau.

På spørgsmålet, *i hvilket omfang er virksomhederne internt integreret*, opnås der generelt høje gennemsnitsværdier for den interne integration fra 3,52 til 4,03 på de 11 udsagn om intern integration. Det er et meget positivt resultat

og udgangspunkt til at kunne styrke arbejdet med cybersikkerhed. Gennemsnitsværdien samlet for de 11 udsagn er på 3,75, hvilket indikerer, at det synes at være lykkes med at få greb om den udprægede silokultur, hvor der sker suboptimeringer indenfor de respektive funktioner i virksomheden. Undersøgelsen har også stillet et spørgsmål om, *i hvilket omfang virksomhederne har fokus på geopolitik*. 60 procent af respondenterne svarer, at de har fokus på geopolitiske forhold i deres måde at drive virksomheden på. Det er overraskende, at 40 procent ikke har fokus på geopolitiske forhold, hvilket indikerer et udviklingsbehov for at skabe nye ledelsesmæssige agendaer, der eksplicit sætter fokus på geopolitik. Respondenter svarer med et gennemsnit på 3,33 at geopolitiske risici påvirker virksomhedernes forretninger, hvilket indikerer et udviklingsbehov. 45 procent svarer, at de er påvirket af lovgivning fra andre lande, hvilket f.eks. er GDPR, lægemiddellovgivning, hvidvask-lovgivning, EU-sanktioner og NIS II. Det sidste spørgsmål, *hvorledes virksomhederne har balanceret drifts- og udviklingsopgaver*, viser ikke overraskende, at virksomhederne er mere driftsorienterede end udviklingsorienterede. De seks udsagn om driftsorientering opnår gennemsnit fra 3,44 til 4,10 og lander samlet på 3,74, mens de seks udsagn om udviklingsopgaver opnår gennemsnit fra 3,13 til 3,54 med et samlet gennemsnit på 3,3. I arbejdet med at sikre cybersikkerhed er det således vigtigt at være opmærksom på det dilemma, der kan være mellem drift og udvikling.

En undersøgelse som denne gennemføres ikke uden metodiske begrænsninger. For det første er der tale om en kvantitativ undersøgelse, der kun besvarer, hvor mange der udfører de adspurgte tiltag. Fremtidig forskning kan supplere denne med kvalitative undersøgelser såsom casestudier, der går i dybden med, hvordan og hvorfor virksomhedernes praksis er, som den er. For det andet er spørgeskemaet baseret på én enkelt respondent pr. virksomhed. Fremtidig forskning kan styrke resultaterne ved at inddrage flere respondenter pr. virksomhed. For det tredje tegner undersøgelsen et billede af cybersikkerhed baseret på de stillede spørgsmål f.eks. om cybersikkerhed i supply chain risk management. Dette område er relativt nyt, og der er således behov for at styrke begrebsdannelsen om cybersikkerhed i et forsyningskædeperspektiv.

6. Litteraturliste

Alamillo, I., Mouille, S., Röck, A., Soumelidis, N., Tabor, M. & Gorniak, S. (2023), *Digital Identity Standards: Analysis of Standardisation Requirements in Support of Cybersecurity Policy*, European Union Agency for Cybersecurity (ENISA), Attiki, Greece.

Allianz (2023), *Allianz Risk Barometer 2023 – Rank 1: Cyber Incidents*, Allianz, https://commercial.allianz.com/news-and-insights/expert-risk-articles/allianz-risk-barometer-2023-cyber-incidents.html

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

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

Dahl, A.M., Pommerencke-Vilmand, L., Nielsen, L.P., Rostved, N.E., Aaholst, V.B. & Astrupgaard, C. (2023), *Cybersikkerhed & konkurrencefordele blandt danske SMV'er 2023*, Analyse & Tal, København N.V.

Ekmann, K.T. (2022), "Medarbejderadfærd: En trussel mod cybersikkerheden?", I: Jacobsen, J.T. & Liebetrau, T. (red.) (2022), *Cybertrusler: Det digitale samfunds skyggeside*, Djøf Forlag, København K, pp. 209-229.

Esper, T.L., Defee, C.C. & Mentzer, J.T. (2010), "A framework of supply chain orientation", *The International Journal of Logistics Management*, Vol. 21 No. 2, pp. 161-179.

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

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

Google Threat Awareness Group (2023), *The Fog of War: How the Ukraine Conflict Transformed the Cyber Landscape*, https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf

Hill, T.J. (1986), "Teaching manufacturing strategy", *International Journal of Operations & Production Management*, Vol. 6 No. 3, pp. 10-20.

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

March, J.G. (1991), "Exploration and exploitation in organizational learning", *Organization Science*, Vol. 2 No. 1, pp. 71-87.

Mentzer, J.T., DeWitt, W., Keebler, J.S., Min, S., Nix, N.W., Smith, C.D. & Zacharia, Z.G. (2001), "Defining supply chain management", *Journal of Business Logistics*, Vol. 22 No. 2, pp. 1-25.

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

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

O'Reilly, C.A. & Tushman, M.L. (2013), "Organizational ambidexterity: Past, present, and future", *The Academy of Management Perspectives*, Vol. 27 No. 4, pp. 324-338.

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

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

Pedersen, A.Á. & Vandrup, K.D. (2022), *IT-sikkerhed i praksis: En introduktion*, Samfundslitteratur, Frederiksberg.

Polyviou, M., Croxton, K.L. & Knemeyer, A.M. (2020), "Resilience of medium-sized firms to supply chain disruptions: The role of internal social capital", *International Journal of Operations & Production Management*, Vol. 40 No. 1, pp. 68–91.

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

Shortridge, K. & Rinehart, A. (2023), *Security Chaos Engineering: Sustaining Resilience in Software and Systems*, O'Reilly, Boston.

Sosafe (2024), *Cybercrime Trends 2024: The Latest Threats and Security Best Practices*, Sosafe, Cologne.

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

Stentoft, J., Schmitt, O., Peressotti, M. & Theussen, A. (2023b), "Cybersikkerhed i forsyningskæden: Hvor piv-åben er din virksomhed?", *Kronik i Erhverv+, IT og Tech*, 9. november, p. 21.

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

Stentoft, J., Rajkumar, C. & Madsen, E.S. (2017), *Industry 4.0 in Danish Industry: An Empirical Investigation of the Degree of Knowledge, Perceived Relevance and Current Practice*, Department of Entrepreneurship and Relationship Management, University of Southern Denmark.

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

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

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

Om forfatterne

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

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

Olivier Schmitt, ph.d., er professor ved Center for War Studies, Syddansk Universitet, og research associate hos RAND Europe. Han er også associate editor af European Journal of International Security. Som reserveofficer i the French Air and Space Force var han Director for forskning og studier ved the French Institute for Higher National Defence Studies (IHEDN). Hans forskningsinteresser inkluderer militær magt, europæisk sikkerhed, transformationen af væbnede styrker og geoøkonomi. Han er forfatter til "Allies that Count. Junior Partners in Coalition Warfare" (Georgetown UP, 2018) og "French Defence Policy since the End of the Cold War" (Routledge, 2020, med Alice Pannier).

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

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

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

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

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

Louise Tumchewics er ph.d, og post.doc. hos Center for War Studies, Syddansk Universitet. Louise har opnået sin ph.d. i krigsstudier ved King's College London. Hendes forskning fokuserer på krig og teknologi, økonomisk krigsførelse og civil-militære relationer. Før hun kom til SDU, var Louise seniorforsker ved den britiske hærs Center for Konfliktforskning (CHACR), adjunkt ved Rabdan Academy i De Forenede Arabiske Emirater og Visiting Research Fellow ved King's College London. Louise er redaktør af Small Armies, Big Cities – en undersøgelse af moderne bykrigsførelse, og så er hun forfatter til to kommende bøger.

Projektet *Cybersikkerhed og Forretningkontinuitet* gennemføres som ét ud af fem projekter i en samlet portefølje af projekter i en temaindkaldelse fra Industriens Fond om cybersikkerhed i værdikæderne.

Læs mere hos Industriens Fond her: https://industriensfond.dk/vores-fokusomrader/cybersikkerhed.

De fem projekter er:

1. Cybersikkerhed og Forretningskontinuitet (læs mere her).
2. Cybersikre robotter (læs mere her).
3. Styrket cybersikkerhed for SMV'er. (læs mere her).
4. Cybersikre fødevareværdikæder (læs mere her).
5. Cybersikkerhed i forsyningskæderne (læs mere her).

Skriv til projektleder Jan Stentoft på stentoft@sam.sdu.dk eller ring til ham på 20 88 71 91 for mere information.

FORSVARSAKADEMIET

INDUSTRIENS FOND

SDU
Syddansk Universitet