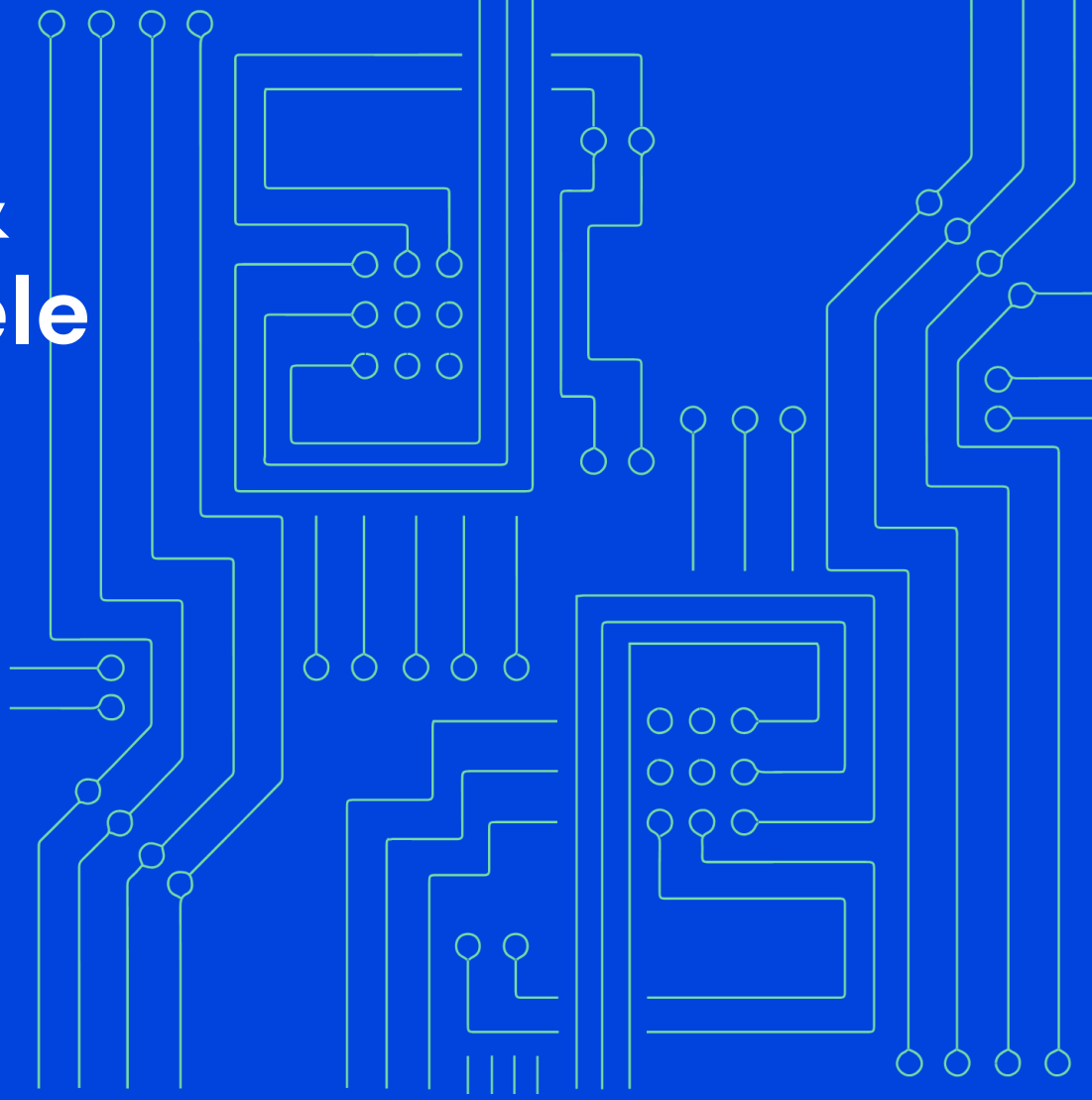
Cybersikkerhed & konkurrencefordele blandt danske SMV'er 2023



Rapport udarbejdet for Industriens Fond af
Analyse & Tal med sparring fra Grant Thornton

Analyse &Tal - November 2023

Udarbejdet af:

Analyse & Tal F.M.B.A
Lygten 39
2400 København NV
www.ogtal.dk

For mere information kontakt:

Lisbeth Palmhøj Nielsen
lisbeth@ogtal.dk

Dataindsamling, databehandling, analyse, tekst & design:

Amalia Montano Dahl, Line Pommerencke-Vilmand, Lisbeth Palmhøj Nielsen, Nadia Engelst Rostved, Valdemar Baes Aaholst og Cecilie Astrupgaard fra Analyse & Tal

Sparring:

Martin Brogaard Nielsen fra Grant Thornton

Indhold

1

Introduktion & hovedindsigter

Værdien af cybersikkerhed anno 2023

I en tid, hvor digitaliseringen har nået en hidtil uset hastighed, står små og mellemstore virksomheder (SMV'er) over for komplekse udfordringer i form af en voksende trussel fra cyberkriminalitet. Det spænder over målrettede phishingangreb til omfattende ransomware-episoder, der kan have en betydelig indvirkning på SMV'ers økonomiske stabilitet og omdømme.

I denne rapport udforsker vi, hvordan investeringer i cybersikkerhed ikke blot beskytter virksomhedens digitale aktiver og data, men også kan omsættes til konkurrencefordele.

For andet år i træk har vi indsamlet besvarelser blandt SMV'er i Danmark. Fundene bekræfter en stærk sammenhæng mellem cybersikkerhedstiltag og konkurrencefordele. Igen i år viser det sig ligeledes, at cybersikkerhedstiltag gavner alle brancher. Jo flere tiltag, des flere oplevede fordele. Mange virksomheder ser ligefrem cybersikkerhed som en nødvendighed for overhovedet at være på markedet.

I årets undersøgelse dykker vi dybere ned i cybersikkerhed i SMV'ernes værdikæder. Vi undersøger hvorvidt SMV'er har fokus på deres underleverandørers cybersikkerhed, og hvorvidt de oplever et ydre pres, eksempelvis fra deres kunder, for også at sikre sin værdikæde.

En stor del af SMV'erne er enige i at cybersikkerhed i værdikæden har betydning. Til spørgsmålet "Hvor vigtigt er cybersikkerhed, når I vælger underleverandører?" svarer 61 pct. af virksomhederne "vigtigt" eller "meget vigtigt". Omkring 35 pct. beretter desuden om at opleve et ydre pres, enten fra lovgivningen, kunder, samarbejdspartnere, deres bestyrelse, aktionærer eller investorer. Her er store forskelle på tværs af brancher, ikke blot i oplevet vigtighed af værdikædens cybersikkerhed, men også med hensyn til ydre krav.

Metodemæssigt griber vi undersøgelsen an ligesom sidste år. Vi har udsendt et spørgeskema til administrerende direktører (CEO's) og øverste ledelse i SMV'er i brancherne Fremstilling, Bygge- & anlæg, Information & kommunikation, Transport & Godshåndtering og Råstofudvinding. Gennem en indsats for at berige data, er det lykkedes at øge svarprocenten fra 10 pct. i 2022 til 12 pct. i 2023.

Som et supplement til vores spørgeskemaundersøgelse har vi gennemført interviews med syv CEO's for at få indblik i deres virksomheders arbejde med cybersikkerhed. Vi har valgt virksomheder på tværs af brancher, der repræsenterer forskellige tilgange og strategier. En fællesnævner for dem er dog, at de har omfattende og solide cyberforanstaltninger på plads.

God læselyst!

Nøglebegreber i rapporten

Cybersikkerhed

Cybersikkerhed skal beskytte virksomhedens data og IT – computere, servere, elektroniske systemer, mobile enheder, netværk – mod ondsindede angreb.

Cybersikkerhedstiltag er både Teknik (fx backup, opdateringer og foranstaltninger mod malware), Forankring & styring (fx beredskabsplaner, udpegning af ansvarlige, risikostyring) samt Rutiner & træning (fx opkvalificering af ledelse og ansatte, risikovurdering af leverandører).

Konkurrencefordele

Konkurrencefordele er fordele, en virksomhed har i forhold til sine konkurrenter, hvorved virksomheden kan generere større omsætning eller overskud og/eller holde på sine eksisterende kunder.

I undersøgelsen er konkurrencefordele inddelt i tre kategorier: Effektivitet & nytænkning (fx bedre implementering, simplere arbejdsgange, styrket innovation), Tillid (fx øget tillid fra bestyrelsen, kunder, investorer og aktionærer) og fordele, der rammer Bundlinjen (fx at virksomheden har kunne tiltrække nye kunder).

SMV

I undersøgelsen er små og mellemstore virksomheder, også kaldet SMV'er, karakteriseret ved at have ca. 500 eller færre medarbejdere.

Den gennemsnitlige virksomhed har omkring 60 ansatte. De fleste af virksomheder i undersøgelsen beskæftiger mellem 10-100 ansatte, mens kun 26 ud af 919 virksomheder i undersøgelsen har mere end 300 ansatte.

Værdikæde

Årets rapport har særligt fokus på SMV'ers sikring af cybersikkerhed i deres værdikæde. I undersøgelsen forstås værdikæden som de samlede aktiviteter og aktører, der er med til at skabe og give en virksomheds produkt eller tjenesteydelse værdi.

Værdikæden skal dermed ses som en kæde af aktiviteter, hvor forskellige aktører bidrager til processen af skabelsen et produkt eller tjenesteydelse. Det kan være leverandører, som leverer komponenter til produktet, men det kan også være andre samarbejdspartnere.

Hovedindsigter

#1 Cybersikkerhed og konkurrencefordele går hånd i hånd

#2 Intern forankring og eksternt udsyn skaber et solidt fundament

#3 SMV'er prioriterer cybersikkerhed i værdikæden

Hovedindsigt #1

Cybersikkerhed og konkurrencefordele går hånd i hånd

Årets undersøgelse viser, at der eksisterer en markant sammenhæng mellem SMV'ers investeringer i cybersikkerhed og deres oplevede konkurrencefordele. Konkurrencefordelene spænder fra øget effektivitet over højnet tillid til direkte positiv indvirkning på bundlinjen. Hele 72 pct. af SMV'er oplever én eller flere konkurrencefordele som følge af de cybersikkerhedstiltag, de har implementeret i løbet af de seneste to år. Resultaterne bekræfter de fund, der blev gjort i undersøgelsen fra 2022.

Der kan være en forestilling om, at det kun er stærkt digitaliserede brancher som Information & kommunikation, der har data at sikre. Men spørger vi SMV'erne selv, gælder følgende på tværs af brancher: Jo flere cybersikkerhedstiltag virksomheden indfører, desto flere konkurrencefordele oplever den.

Sammenhængen understreger vigtigheden af, at SMV'er fortsat prioriterer cybersikkerhed som en integreret del af deres forretningsstrategi. Det er ikke blot en beskyttelse mod potentielle trusler, men er også en afgørende faktor for at opnå og fastholde konkurrencefordele.

Hovedindsigt #2

Intern forankring og eksternt udsyn skaber et solidt fundament

I vores interviews med SMV'er, der succesfuldt har implementeret adskillige cybersikkerhedstiltag og opnået konkurrencefordele derved, fremhæves to centrale faktorer, der kan spille en afgørende rolle for at opnå stærk cybersikkerhed.

En afgørende faktor for effektiv cybersikkerhed er intern opbakning til initiativerne. Dette kræver, at nøglepersoner i virksomheden, uanset om det er CEO'en, revisoren eller IT-medarbejderen, viser interesse for cybersikkerhed og anerkender dens betydning. Flere fremhæver vigtigheden at have dedikerede og engagerede medarbejdere internt, der besidder viden om virksomhedens forretning og historie og kan drive det kontinuerlige arbejde med at implementere nye tiltag. Dette kan sikre, at implementeringen af cybersikkerhedstiltag forankres solidt i hele organisationen.

En anden vigtig faktor, der fremhæves, er behovet for at søge ekstern ekspertise for at holde sig ajour med risici inden for cyberområdet. Det kan både være gennem branchefællesskaber, bestyrelsen, eksterne konsulenter eller samarbejdspartnere. Det er alment anerkendt, at trusselbilledet ændrer sig konstant, og SMV'er kan have svært ved at følge med på egen hånd. Ved at have adgang til eksterne kilder til opdateret viden, kan SMV'er fokusere på deres kerneopgaver med ro i maven.

Kombinationen af intern forankring og ekstern ekspertise udgør dermed et solidt fundament for kontinuerligt at styrke cybersikkerheden.

Hovedindsigt #3

SMV'er prioriterer cybersikkerhed i værdikæden

Dette års undersøgelse har fokus på SMV'ers håndtering af cybersikkerhed i deres værdikæde. Med den kommende indførelse af NIS2-direktivet er virksomhederne ikke alene forpligtet til at beskytte deres egne data, men er også pålagt at tage ansvar for cybersikkerheden i hele deres forsyningskæde, herunder hos deres underleverandører.

Undersøgelsen viser, at hele 61 pct. af SMV'erne betragter cybersikkerhed som vigtigt eller endda meget vigtigt, når de vælger underleverandører. I vores interviews med CEOs er det også tydeligt, at flere har fokus på hvordan underleverandørers håndtering af data kan have direkte indflydelse på virksomhedens cybersikkerhed. De har således en udvidet forståelse af cybersikkerhed, og inkluderer eksterne samarbejdspartnere og leverandører i deres risikovurdering. Som konsekvens heraf bliver sikringen af data og systemer ofte et fælles anliggende på tværs af aktørerne i værdikæden.

Blandt SMV'erne undersøgelsen oplever 35 pct. eksterne krav fra blandt andet lovgivningen, bestyrelsen eller kunderne, som kræver, at også virksomhedens underleverandører opretholder et højt niveau af cybersikkerhed. Vi finder en stærk sammenhæng mellem hvor vigtig virksomheden anser underleverandørers cybersikkerhed for at være, og om de oplever eksterne krav eller ej. En tredjedel af SMV'erne synes hverken, at underleverandørers cybersikkerhed er vigtig eller oplever nogen eksterne krav. Denne gruppe findes især inden for branchen 'Bygge & anlæg'.

Om end det ikke gælder for alle SMV'er, tyder undersøgelsen på, at en betydelig andel af virksomhederne har forståelse for og tager aktive skridt mod at sikre deres underleverandører. Det indikerer et stigende fokus mod at skabe en samlet pålidelighed i hele sin værdikæden. Et fokus som flere af undersøgelsens interviewpersoner forventer vil fortsætte med at vokse i fremtiden.

Cybersikkerhed og konkurrencefordele

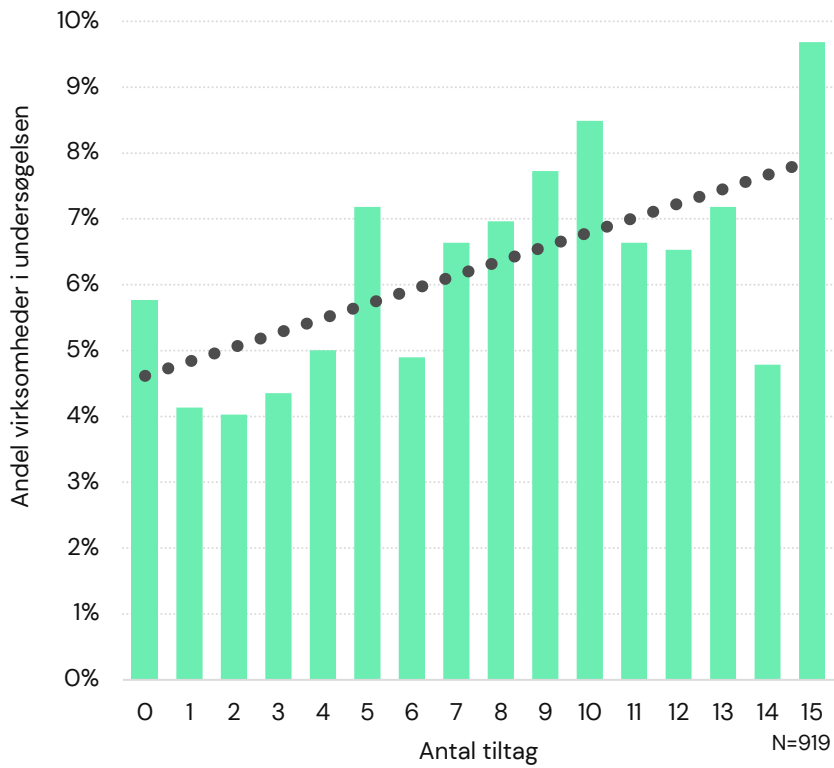
Stigende antal tiltag blandt SMV'er

Fra 2022 til 2023 er antallet af SMV'er, der har implementerer cybersikkerhedstiltag steget. I 2022 var der næsten 8 pct. af SMV'erne, der ikke havde nogen form for cybersikkerhedstiltag, mens dette tal er faldet til knap 6 pct. i 2023. Men det stopper ikke her. SMV'erne har også implementeret flere cybersikkerhedstiltag end i 2022. I 2022 havde lidt over 7 pct. af SMV'erne implementeret alle 15 tiltag, mens dette tal er steget til knap 10 pct. i 2023.

Som det fremgår af figur 1, er der en tendens mod en øget implementering af flere cybersikkerhedstiltag. I 2022 var der en mere jævn fordeling, hvor virksomhederne kunne have alt fra ét tiltag til alle 15 tiltag.

De cybersikkerhedstiltag, der er blevet implementeret, spænder bredt. De omfatter tekniske foranstaltninger som løbende opdatering af software og sikkerhedskopiering samt organisatoriske tiltag som udarbejdelse af it-beredskabsplaner og træningsinitiativer som opkvalificering af medarbejdere inden for IT-sikkerhed (se de 15 tiltag på side 18).

Figur 1: Fordeling af antal cybersikkerhedstiltag



Konkurrence-fordele ved cybersikkerhed

I 2023 oplever hele 72 pct. af SMV'erne en eller flere fordele ved de cybersikkerhedstiltag, de har implementeret. Det er en markant stigning i forhold til 2022. Her oplevede 56 pct. konkurrencefordele ved deres tiltag.

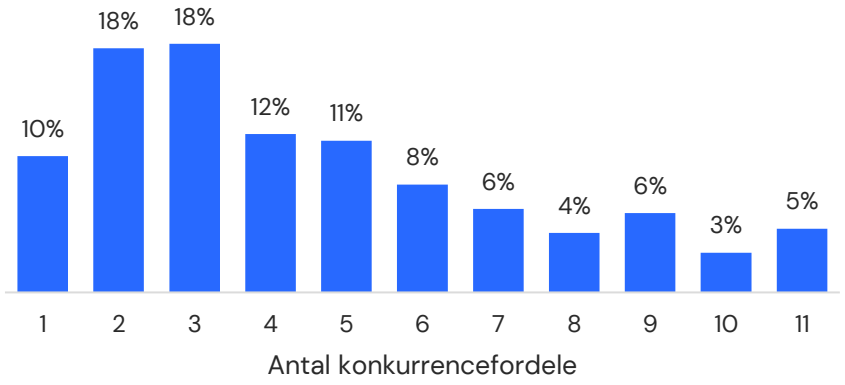
Det er dog vigtigt at bemærke, at stigningen kan skyldes øgede investeringer i cybersikkerhed, men at det også kan skyldes ændringer i undersøgelsens svarkategorier*. Der er således en øget oplevelse af gevinster ved cybersikkerhed blandt SMV'er, og fremgangen i tallet er sandsynligvis en kombination af en fremgang og en ændring i undersøgelsens svarkategorier.

På figur 3 kan man se, hvor mange forskellige konkurrencefordele SMV'erne har opnået gennem deres investeringer i cybersikkerhed. Blandt de virksomheder, der har indført cybersikkerhedstiltag, er der 28 pct., der *ikke* oplever konkurrencefordele af tiltagene (ikke vist på figur). Blandt de resterende SMV'er, som oplever fordele, ligger flertallet mellem 1-5 konkurrencefordele (68 pct.), mens hele 32 pct. af SMV'erne rapporterer flere end 5 konkurrencefordele som følge af deres cybersikkerhedstiltag.

* Læs mere om dette i afsnittet "Data og metode" side 53

Figur 2: Andele der oplever *en eller flere* konkurrencefordele ved at have indført cybersikkerhedstiltag

Figur 3: Fordeling af *antallet* af konkurrencefordele blandt de SMV'er, der oplever fordele ved at have indført cybersikkerhedstiltag,



N=866

Figur 4 viser, at der er en klar sammenhæng mellem, hvor mange cybersikkerhedstiltag virksomhederne har, og hvorvidt de oplever konkurrencefordele.

For virksomhederne, der har indført færrest tiltag (1-5), er der 39 pct., der oplever én eller flere konkurrencefordele af tiltagene. Blandt dem, der har indført 6-10 tiltag er der 79 pct., som oplever konkurrencefordele. Blandt SMV'er med flest tiltag, med 11-15 investeringer, oplever hele 89 pct. fordele.

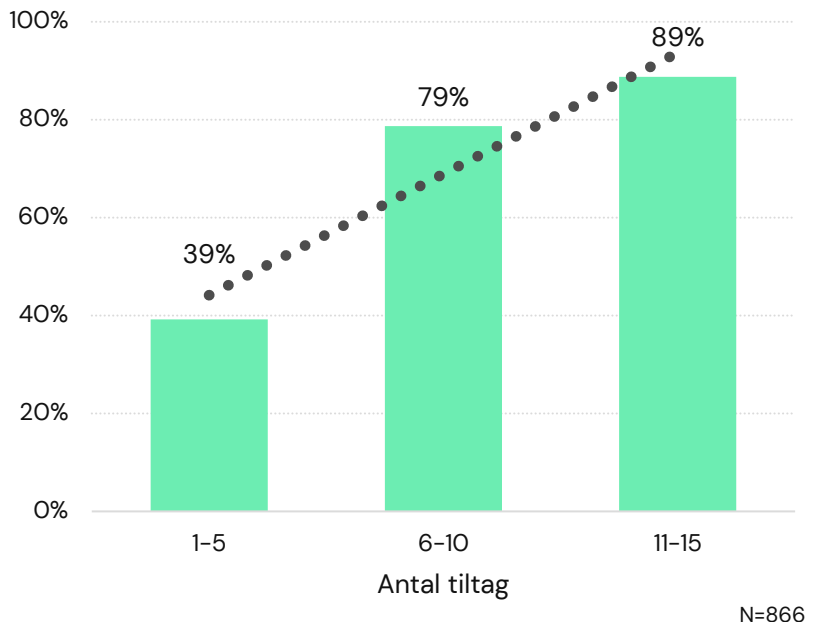
Det ser således ud til, at der allerede er mærkbare gevinster ved mindre investeringer. Dog er det vigtigt at bemærke, at der er en markant stigning i andelen af virksomheder, der oplever fordele, når de implementerer flere tiltag og bevæger sig ind i midterkategorien (6-10 tiltag). Det antyder, at konkurrencefordele særligt kan mærkes, når virksomheden har implementeret en vis mængde tiltag.

I interview med Mikkel Enevoldsen, CEO i Saxe Hansen, fremhæver han, at virksomheden ikke bliver valgt af kunderne på grundlag af deres cybersikkerhed alene. Dog mener han, at deres fokus på at sikre sig, har givet dem selvtillid til at byde på projekter, som deres konkurrenter med mindre fokus på cybersikkerhed ville gå udenom:

"Man kan sige, at det giver os modet til at byde på projekter, som andre virksomheder ville sige nej til, fordi de ikke havde tingene på plads. Sådan kan man jo sige, at det er en konkurrencefordel: Det gør os modige og sikrere, når vi byder på projekter. Vi er ikke bange for at gå ind i pharma, som ellers er noget af det, der er allerhøjst krav til. Det skyldes, vi har tingene på plads, og vi ved, at det fungerer"
Mikkel Enevoldsen, CEO, Fremstillingsvirksomhed

En stærk cybersikkerhedskultur kan således styrke selvtilliden og muligheden for at udforske nye forretningsmuligheder og markeder.

Figur 4: Andele der oplever én eller flere konkurrencefordele ved at have indført cybersikkerhedstiltag, fordelt på antal cybersikkerhedstiltag



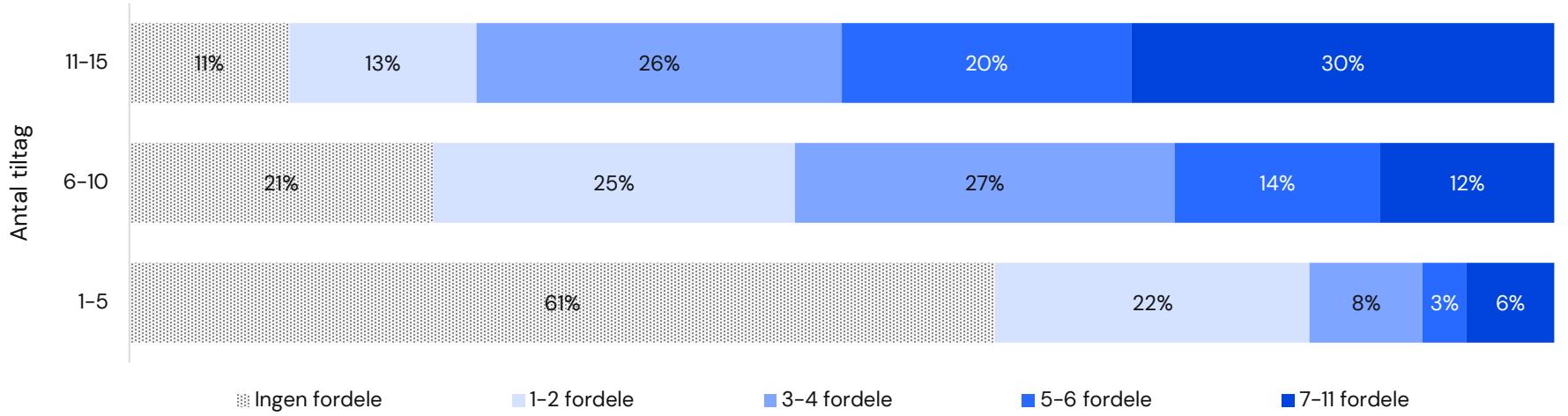
Jo flere cybersikkerhedstiltag, des flere konkurrencefordele

Figur 5 understreger forholdet mellem cybersikkerhedstiltag og de opnåede fordele. Her er SMV'er, der har indført cybersikkerhedstiltag, opdelt efter antallet af fordele, de oplever.

Det klare mønster viser, at SMV'er med flest tiltag (11-15) oplever flest konkurrencefordele (repræsenteret ved den mørkeblå farve). Hele 30 pct. i denne gruppe rapporterer mere end seks konkurrencefordele som resultat af deres tiltag

I modsætning hertil er det kun 12 pct. af midtergruppen med 6-10 tiltag, der oplever mere end seks fordele som følge af deres indsats. Lidt har også ret, men mere cybersikkerhed giver altså flere konkurrencefordele.

Figur 5: Oplevede konkurrencefordele fordelt på hvor mange cybersikkerhedstiltag virksomheden har indført



N=866

Forskellige former for cybersikkerhedstiltag og konkurrencefordele

Ligesom sidste års undersøgelse vil vi i dette kapitel gå i dybden med de individuelle spørgsmål om tiltag og fordele. I spørgeskemaet har vi fastholdt de samme spørgsmål om tiltag og fordele som sidste år. Konkret har vi spurgt SMV'erne, om de inden for en 2-årig periode har implementeret eller opdateret 15 specifikke cybersikkerhedstiltag. Tiltagene er opdelt i tre kategorier:

1. Teknik
2. Forankring & styring
3. Rutiner & træning

SMV'erne, der har implementeret mindst ét cybersikkerhedstiltag, blev bedt om at vurdere, om deres investering har ført til opnåelse af 11 specifikke konkurrencefordele. Disse fordele er også inddelt i tre kategorier:

1. Effektivitet & nytænkning
2. Tillid
3. Bundlinje

I det følgende går vi i dybden med først implementeringen af cybersikkerhedstiltag i SMV'erne og derefter de oplevede konkurrencefordele.

3 former for cybersikkerhedstiltag

Teknik

- Løbende opdateringer af virksomhedens software
- Vedligehold eller forbedring af automatisk backup
- Øget beskyttelse af administrative brugerkonti
- Øget netværkssikkerhed og kryptering
- Øget foranstaltninger mod malware

Forankring & styring

- Udpegning af ansvarlige personer for it-sikkerhed og dataanvendelse
- Øget indsats omkring it-risikostyring
- At føre en oversigt over virksomhedens data og systemer
- Udarbejdelse eller opdatering af politik for data- og it-sikkerhed
- Udarbejdelse eller opdatering af politikker for ansvarlig dataanvendelse og dataetik
- Udarbejdelse eller opdatering af it-beredskabsplan

Rutiner & træning

- At gennemføre tiltag så sikkerhed og ansvarlig datahåndtering indtænkes når en ny opgave igangsættes
- Risikovurdering af eller nye krav til leverandører/samarbejdspartnere om databehandling og it-sikkerhed
- Opkvalificering af den øverste ledelse i it-sikkerhed eller ansvarlig dataanvendelse
- Opkvalificering af ansatte i it-sikkerhed eller ansvarlig dataanvendelse

I figur 6 kan man se andelen af virksomheder, der har indført forskellige cybersikkerhedstiltag. De mest udbredte tiltag er inden for teknik, hvor hele 87 pct. af SMV'er løbende opdaterer virksomhedens software, mens 62 pct. har øget netværkssikkerhed og kryptering.

De mindst udbredte tiltag er inden for Rutiner & træning. Inden for denne kategori er der 41 pct. af SMV'er, der inden for de seneste 2 år har styrket cybersikkerheden gennem at gennemføre tiltag så sikkerhed og ansvarlig datahåndtering indtænkes når en ny opgave igangsættes. Det tiltag som færrest (29 pct.) SMV'er har indført er opkvalificering af ansatte i IT-sikkerhed eller ansvarlig dataanvendelse.

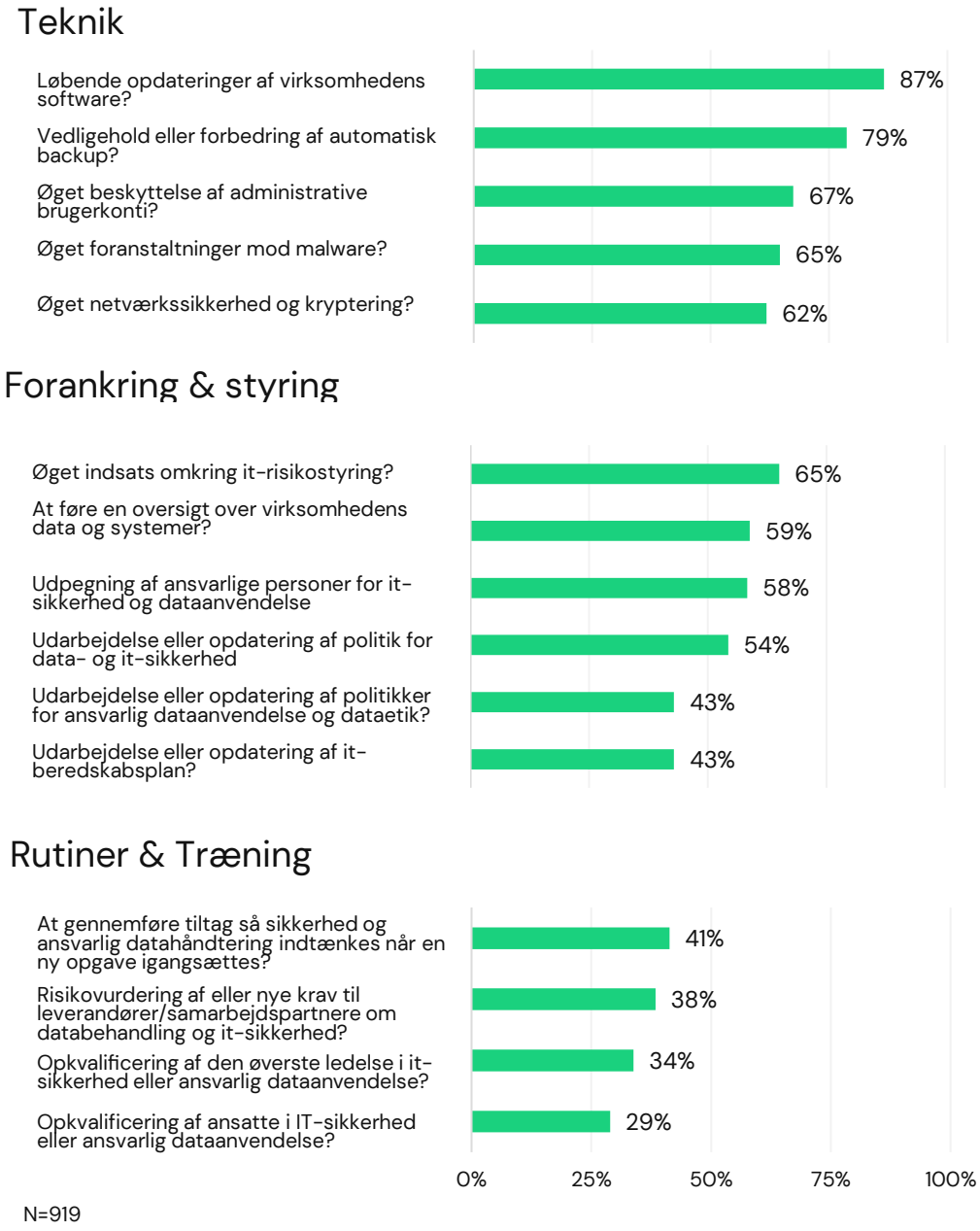
Fra 2022 til årets undersøgelse har der generelt været en gennemsnitlig stigning inden for alle tiltag på 4 procentpoint (ikke vist på figuren). Særligt to former for tiltag har oplevet en fremgang, nemlig "øget foranstaltninger mod malware" i kategorien Teknik, samt "risikovurdering af eller nye krav til leverandører/ samarbejdspartnere vedrørende databehandling og it-sikkerhed" i kategorien Rutiner & træning.

Direktør Jens Fricke fremhæver en oplevelse af at krav til underleverandører er blevet vigtigere:

"Vi har gennem tiden benyttet os af tre store leverandører af SIM-kort. Den ene leverandør har ikke de samme certifikater som de andre, og vi har derfor fravalgt dem. Vi snakker om sikkerhed med vores underleverandører, og de skal alle leve op til de gældende krav. Det er jo os, der har ansvaret, hvis ikke tingene er i orden. Når det drejer sig om datasikkerhed, så nytter ikke noget at spare 1 krone per SIM-kort. Jeg oplever desuden, at der bliver stillet flere og flere krav. Man skal kunne give en ekstraordinær service og sikre at produktet er sikkert"
Jens Fricke, direktør, IT- og kommunikationsvirksomhed

Stigningen i netop disse to tiltag afspejler muligvis behovet for øget cybersikkerhed i et år præget af betydelig usikkerhed og

Figur 6: Har virksomheden indenfor de seneste 2 år styrket cybersikkerheden gennem:



N=919

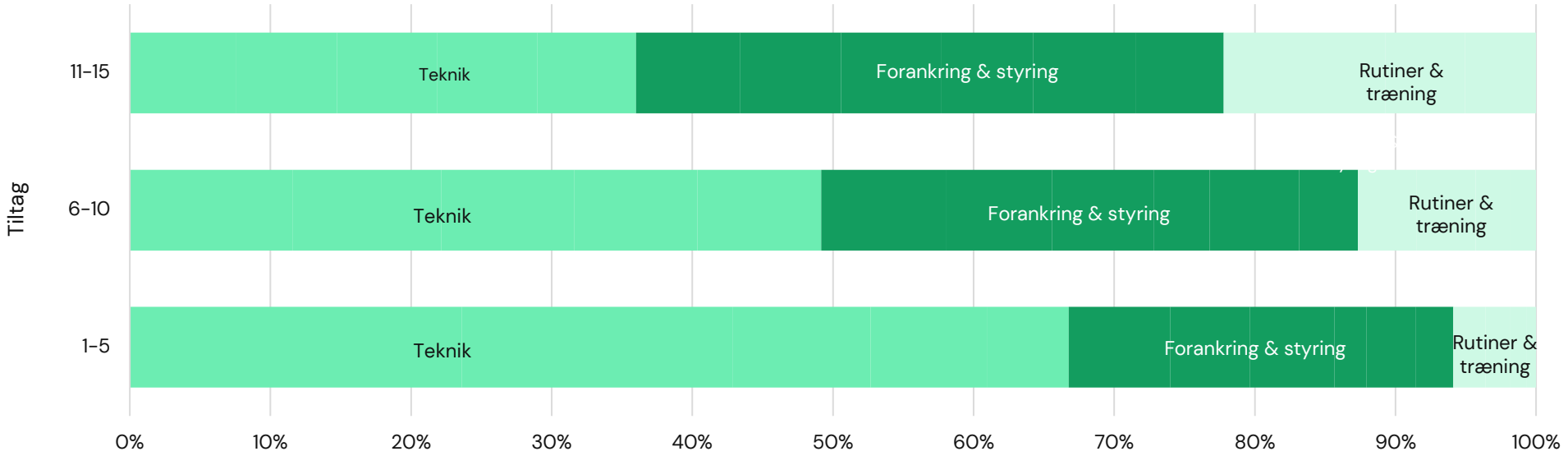
flere kendte sager om succesfulde hackerangreb. I oktober 2024 træder NIS2-direktivet i kraft, hvilket stiller flere krav til SMV'ernes værdikæde. Det kan være en medvirkende faktor til SMV'ernes øgede fokus på værdikæden.

I figur 7 er de forskellige tiltag opdelt efter, hvor mange tiltag SMV'erne har implementeret. Figuren viser et tydeligt mønster, hvor SMV'er, der har implementeret færrest cybersikkerhedstiltag, primært har fokuseret på tekniske foranstaltninger. Dette fund understøttes i interviews, der bekræfter at virksomheder ofte begynder arbejdet med cybersikkerhed med at implementere tekniske foranstaltninger. Tiltag inden for Rutiner & træning udgør kun 6 pct. af tiltagene blandt SMV'ere med 1-5 tiltag.

I midterste kategori af tiltag (6-10) udgør tiltag inden for Teknik cirka halvdelen af SMV'ernes tiltag, mens Rutiner & træning kun udgør 13 pct. Når vi ser på de virksomheder, der har indført flest tiltag (11-15), stiger andelen af tiltag særligt indenfor Forankring & styring, som udgør en større andel end tekniske tiltag, mens Rutiner & træning forbliver den mindste andel.

På de næste sider viser vi hvordan SMV'er oplever fordele af deres investeringer i cybersikkerhedstiltag.

Figur 7: Hvordan virksomheden har styrket cybersikkerheden fordelt på *antallet* af cybersikkerhedstiltag



3 former for konkurrence-fordele

Effektivitet & nytænkning

- At virksomheden er blevet bedre til at implementere og bruge nye teknologier
- At virksomheden har styrket sin nytænkning og innovation
- At arbejdsgange i virksomheden er blevet simplere eller mere effektive

Tillid

- At tilliden fra bestyrelsen til virksomhedens ledelse er øget
- At tilliden fra investorer og aktionærer til virksomhedens ledelse er øget
- At virksomheden har styrket relationen til eksisterende kunder
- At tilliden er øget fra virksomhedens samarbejdspartnere (herunder underleverandører)

Bundlinje

- At virksomheden har kunnet differentiere sig fra konkurrenter
- At virksomheden har kunnet tiltrække nye kunder
- At virksomheden har kunnet tiltrække nye kompetente medarbejdere
- At virksomheden har kunnet hæve prisen på de produkter virksomheden sælger

SMV'ernes oplevelse af konkurrencefordele ved cybersikkerhedstiltag, følger det samme mønster som i 2022. Som det fremgår af figur 8, ser SMV'erne særligt fordele inden for effektivitet og nytænkning. Over halvdelen af SMV'erne oplever, at virksomheden er blevet bedre til at implementere og anvende nye teknologier.

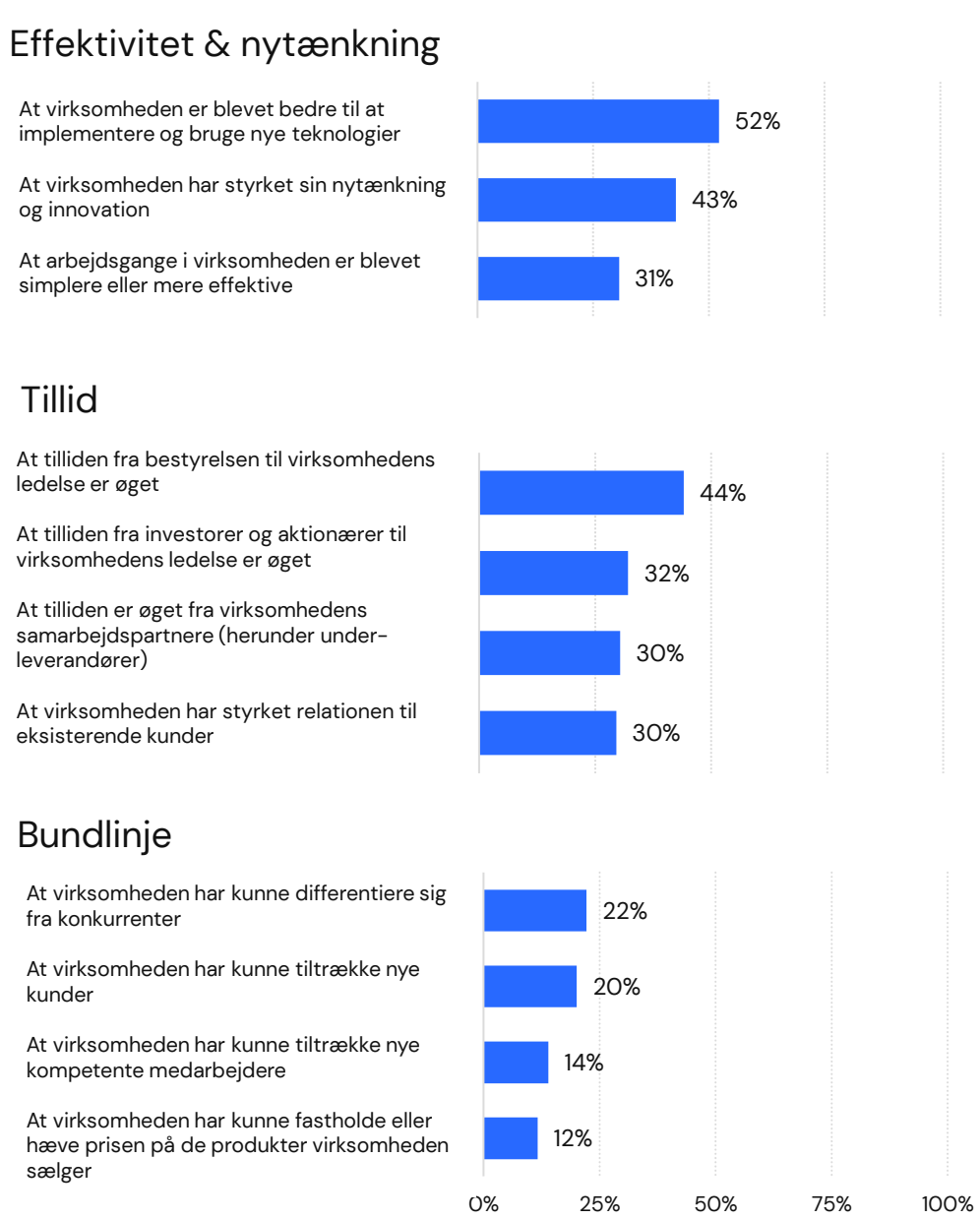
Efter effektivitet og nytænkning er der flest SMV'er, der har oplevet øget tillid som et resultat af deres cybersikkerhedstiltag. Dette omfatter tillid fra bestyrelsen, investorer, kunder og samarbejdspartnere. Især tilliden fra bestyrelsen til virksomhedens ledelse er noget, SMV'erne fremhæver.

Selvom virksomhederne oplever øget effektivitet og tillid, er der mange faktorer, der spiller ind, før dette slår igennem på bundlinjen. Ikke desto mindre angiver omkring hver femte SVM, at deres cybersikkerhedstiltag faktisk har givet dem en konkurrencefordel på bundlinjen. 22 pct. peger på, at deres tiltag har gjort det muligt for dem at differentiere sig fra konkurrenterne, og 20 pct. erklærer, at de har været i stand til at tiltrække nye kunder som følge af deres cybersikkerhedstiltag.

Når man sammenligner tallene fra 2022 og 2023, skal man være opmærksom på, at der er anvendt forskellige svarkategorier (se kapitel 7 om data og metode). Man kan dog se, at de største stigninger inden for konkurrencefordele netop omhandler bundlinjen, og at virksomhederne både har kunne tiltrække nye kunder og har kunne differentiere sig fra konkurrenter.

På næste side kan du læse mere om B.E. Installationer, hvor cybersikkerhed og effektivisering er uløseligt forbundet.

Figur 8: Hvor enig er du i, at virksomhedens indsatser for at styrke cybersikkerhed de seneste 2 år har bidraget til:



N=866

B.E Installationer

Bygge- og anlægsvirksomhed med 120 ansatte
Interview med CEO, Brian Bryrup

"Man kan cybersikre sig helt ihjel. På et tidspunkt, så giver det gener for medarbejderne, hvis man går med livrem og seler.

Vi er et eller andet sted midt imellem. **Hvor medarbejderne kan se, at det giver faktisk mening, det her.** Det kan godt være, det er lidt irriterende, men det giver mening."

Fokus på effektive og velorganiserede arbejdsgange

For Brian Bryrup, CEO og medejer i virksomheden B.E Installationer, er cybersikkerhed og effektivisering to sider af samme mønt. Når Brian og hans team arbejder for at beskytte deres data og systemer, er det med skarpt fokus på at skabe en mere strømlinet og produktiv arbejdsplads.

Effektivisering af arbejdsgange og systemer har været en central motivation for virksomhedens investeringer i cybersikkerhed. Det begyndte med et behov for at forbedre filadgang for virksomhedens medarbejderne. Ved at implementere løsninger som SharePoint har de fjernet de hindringer, der tidligere begrænsede deres brug af filer og arbejde uden for kontoret. Valget om øge sikkerheden, har således også forbedret fleksibiliteten for medarbejderne, der nu kan arbejde fra byggepladser og andre eksterne steder. Brian fremhæver desuden at systeminvesteringer har frigjort ressourcer ved at automatisere førhen tidskrævende manuelle opgaver inden for bogføring og regnskab. Det er værdifuld tid, som nu kan bruges mere effektivt i andre dele af virksomheden. Cybersikkerhed handler dermed ikke kun om risikohåndtering og -evaluering, men også om at optimere arbejdsgange i virksomheden.

For Brian er det essentielt at opretholde en balance mellem effektivitet og sikkerhed for at skabe en god arbejdsplads. Stærk cybersikkerhed handler derfor ikke kun om at implementere så mange sikkerhedsforanstaltninger som muligt, men om at integrere løsninger, som også forbedrer medarbejdernes arbejde og hverdag. Det giver medarbejderne mulighed for at se værdien og formålet med ændringerne, i stedet for at betragte ændringerne som byrder. Hos B.E Installationer er effektivisering således den absolut mest mærkbare gevinst ved investering i cybersikkerhed. For dem går de to hånd i hånd og sikrer en stærkere og mere innovativ virksomhedskultur.

Kendetegn

- Organiserede arbejdsgange
- Balance
- Innovation

Et godt råd

"Sikkerheden har været en del af pakken. Men det primære **fokus for os har været at få effektiviseret vores arbejdsgange.** På den måde kan man se økonomien i det, i stedet for at bare se det som en ekstra omkostning. Det ér en omkostning, men også en nødvendig omkostning, kan man sige. **Ligesom, at du skal købe værktøj til dine svende, så skal du også have det it-mæssige værktøj i orden**"

Flere former for tiltag medfører flere fordele inden for alle kategorier

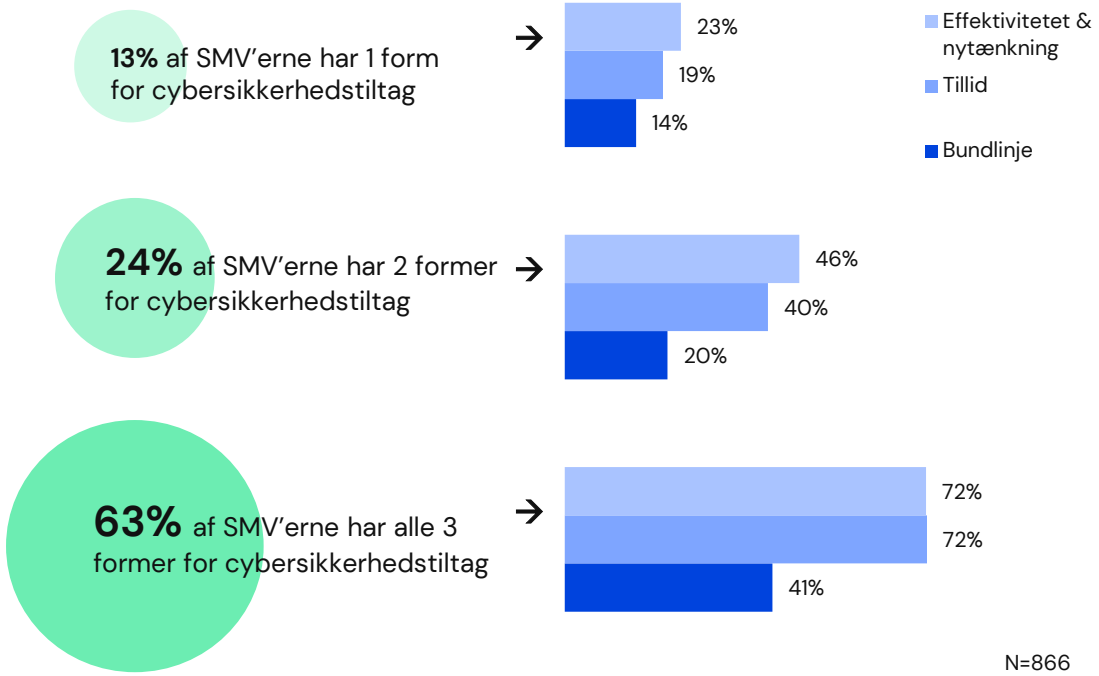
Sammenhængen mellem forskellige former for cybersikkerhedstiltag og konkurrencefordele i år ligner opgørelsen fra 2022. Kun 13 pct. af SMV'erne, der har implementeret tiltag, har kun indført én form for tiltag. 24 pct. har indført to former, mens 63 pct. har indført alle tre former for tiltag.

For SMV'erne med kun én eller to former for tiltag er mønsteret, at de oplever flest fordele inden for effektivitet, derefter tillid og mindst på bundlinjen.

For majoriteten af SMV'er, der har indført alle tre former for tiltag, viser der sig et andet billede. Udover at de oplever langt flere fordele, oplever de også lige så mange fordele inden for effektivitet som inden for tillid. Og færrest direkte på bundlinjen.

På næste side finder du en præsentation af virksomheden Uggerly, der har opnået en stærk cybersikkerhedskultur ved at have fokus på inddragelse og opkvalificering af medarbejdere.

Figur 9: SMV'er fordelt på antal af typer cybersikkerhedstiltag (grøn) kombineret med andel der oplever forskellige typer af konkurrencefordele (blå)



Uggerly

Bygge- og anlægsvirksomhed med 322 ansatte
Interview med administrationschef, Michael Seerup

"**I starten var det mig, der skulle drive alle ændringerne**. Det var mig, der måtte sige "Prøv at se her - kunne det her ikke også være smart? Vi kan faktisk også gøre sådan her"

Nu er det hele vendt rundt. Nu kan jeg læne mig tilbage, for der kommer en masse forslag fra organisationen om: "vi kan også effektivisere det her – vi kunne også gøre sådan"

Medarbejderne kan blive nøglen til innovation

Uggerly Installationer specialiserer sig i en bred vifte af installationsopgaver, der spænder fra mindre el- og VVS-opgaver til større byggeentrepriser. Virksomheden har opnået konkurrencefordele ved at digitalisere og automatisere opgaver med gentagelser, hvor de gør brug af robotteknologi. I dette teknologiske skift spiller cybersikkerhed en afgørende rolle i at opretholde tillid og samarbejde med virksomhedens kunder. I en organisation med mere end 300 ansatte er administrationschef Michael Seerup dog bevidst om, at menneskelige fejl altid vil udgøre cyberrisici, på trods af træning og uddannelse.

Men mennesker er ikke bare et svagt punkt, når det kommer til cybersikkerhed – de kan også være en stor ressource. I begyndelsen af Uggerlys rejse mod stærkere cybersikkerhed var Michael den primære initiativtager. Han igangsatte investering i sikkerhedsteknologi samt udvikling af politikker og procedurer for at beskytte Uggerlys digitale miljø. Men for Michael er cybersikkerhed også et spørgsmål om medarbejdernes engagement og tankegang.

Ved at implementere løsninger, der både sikrede og effektiviserede medarbejdernes arbejdsgange, skabte Michael en kultur, der opmuntrede medarbejderne til selv at finde løsninger. En digital platform blev udviklet, som muliggjorde, at medarbejdere kunne indsende forslag til forbedringer, herunder også tiltag til øget sikkerhed. Resultatet er, at medarbejderne i dag spiller en afgørende rolle i initiativet til og udviklingen af digitale løsninger. Dette skift fra at være afhængig af ledelsesinitiativer, til nu også at have medarbejderdreven innovation i sin cyberstrategi, sikrer en stærk forankring af cybersikkerhedstiltag. Dette er ikke bare en effektiv metode til at forbedre sikkerheden, men det skaber også en kultur, hvor medarbejderne er engagerede i at højne cybersikkerheden i deres egen hverdag.

Kendetegn

- Automatisering
- Medarbejderdrevet
- Præventiv cybersikkerhed

Et godt råd

"Helt grundlæggende, så er det nok at få styr på folks brugerkonto, og **kortlægge hvilke brugere, der har adgang til hvad**. Fordi så ville du jo sagtens kunne lukke en hel masse brugere ned, i tilfælde af at de bliver hacket. På den måde vil det dreje sig om det ganske få personer, du skal sørge for sikkerheden omkring. Det tror jeg er et godt sted at starte, for **lur mig om ikke mange har deres system sat op, så alle bare har adgang til alting?** "

Intern forankring og eksternt udsyn skaber robusthed

Mange virksomheder vælger at outsource al eller dele af deres drift og sikring af IT-systemer. Blot 10 pct. af virksomhederne i undersøgelsen håndterer al IT-drift (fx hjemmeside og økonomisystem) internt. Det er således typisk at outsource disse typer opgaver til eksterne leverandører.

41 pct. af virksomhederne i undersøgelsen har desuden 1-2 medarbejdere dedikeret til IT-drift. Dog er der også en andel (30 pct.), der slet ikke har medarbejdere dedikeret til opgaven.

I vores interviews med SMV'erne bliver det klart, at det er afgørende, at det kontinuerlige arbejde med at forbedre cybersikkerheden er godt integreret i organisationen og samtidig holdes ajour med udviklingen i virksomhedens omverden.

Flere af interviewpersonerne understreger vigtigheden af at have dedikerede og engagerede medarbejdere internt, der besidder viden om virksomhedens forretning og historie og kan drive det kontinuerlige arbejde med cybersikkerhed.

Derudover fremhæver interviewpersonerne, at for at opnå effektiv cybersikkerhed er det nødvendigt med kontinuerlig opdatering og en tæt forbindelse til den eksterne verden. Det er kritisk, at virksomheden forbliver opdateret og har "fingeren på pulsen," som en af interviewpersonerne udtrykker det. Dette er særligt vigtigt inden for et område, der konstant udvikler sig, og hvor trusselsbilledet kan ændre sig.

I interviewene om virksomhedernes tilgang til cybersikkerhed bliver det tydeligt, at der er variation i, hvordan cybersikkerhed forankres internt og hvordan ekstern ekspertise inddrages. Blandt de interviewede virksomheder, fremhæves flere interessante strategier. Det gælder blandt andet Vestfrost og Saxe Hansen, der har forskellige tilgange.

Hos Vestfrost fremhæver CFO Jannie Tholstrup, at interne medarbejdere ofte har en følelse af ejerskab og besidder en forståelse for virksomhedens historik og knowhow, der kan være af stor værdi for cybersikkerhedsindsatsen:

"Der er en sense of urgency og ejerskab. Vi har kompetencerne og folk, der er interesseret i det in-house. Selvfølgelig holder vi stadig ajour og sender vores folk på kursus for at få ny viden. Men det vigtige er at have interne, som kender systemlandskabet indefra. De kender svaghederne og de fejl, vi har haft over tid. De har en indsigt i historikken, der er relevant for at forstå hvad vi skal prioritere fremadrettet. Det er fint nok at have dele outsourcet, men forståelsen for organisationen er vigtig.
Jannie Tholstrup, CFO, Fremstilling

I Vestfrost lægges der således vægt på at have kompetencer internt for at sikre bedst mulig forståelse for organisationens behov og historie. Det giver dem kontrol over egen infrastruktur.

Samtidig ser Jannie dog værdien i at benytte eksterne ressourcer til særlige opgaver. Hun bruger eksterne ressourcer til at evaluere virksomhedens sikkerhedsinfrastruktur, hvilket hjælper med at identificere eventuelle sårbarheder eller mangler. Derudover initierer hun simulerede cyberangreb i samarbejde med eksterne eksperter, hvilket tester organisationens beredskab og evne til at reagere på trusler. Formålet er at sikre, at de er forberedte og kan handle hurtigt, hvis et ægte angreb skulle opstå.

De simulerede angreb tjener også som awareness-træning, der hjælper med at uddanne medarbejdere om vigtigheden af cybersikkerhed og hvordan man kan beskytte organisationen:

"Jeg laver simulerede cyberattacks uden at organisationen ved det (..) Jeg gør det ikke for at være urimelig. Jeg gør det for at holde dem skarpe, og det ved de godt. Det er hjælp til selvhjælp, og vi får en masse replay ud af det: Hvad var det, de gjorde? Hvorfor kunne det lade sig gøre? Den viden og erfaring er et kompetenceløft internt. Og på den måde bruger vi de eksterne til at udvikle og uddanne os til næste niveau."
Jannie Tholstrup, CFO, fremstilling

Vestfrost repræsenterer altså en tilgang, hvor der trækkes på eksterne ressourcer til evaluering og rådgivning, mens styringen af cybersikkerheden holdes in-house.

Hos Saxe Hansen lægger CEO Mikkel Enevoldsen større vægt på inddragelse af eksterne. Virksomheden har tidligere forsøgt at håndtere cybersikkerhed internt, men fandt det ineffektivt, da der stadig var behov for eksterne leverandører. Han værdsætter ekstern ekspertise og viden højt og ser den som noget, der er svært at opdyrke i en organisation med bare 60 medarbejdere. Derfor har Saxe Hansen tæt samarbejde med eksterne partnere:

"Vi har prøvet at have det in-house, og det fungerede ikke. Vi skulle stadigvæk benytte os af eksterne leverandører. Det er svært at have en person siddende, som er hundrede procent dedikeret til det. Der er vi alligevel ikke så store, at vi kan have en person til at gøre det. Der var simpelthen for meget for ham. Dem som vi samarbejder med på IT-området, de har ekspertviden, som vi ikke rigtig kan opbygge internt. Så det er simpelthen derfor, at vi har entreret med noget eksternt."
Mikkel Enevoldsen, CEO, Fremstilling

I Saxe Hansens tilfælde er eksterne en integreret del af beslutningsprocessen og er afgørende for at håndtere et komplekst og skiftende trusselsbilleder inden for cybersikkerhed. Det beskrives nærmere i casen på næste side.

Saxe Hansen

Fremstillingsvirksomhed med 65 ansatte
Interview med CEO, Mikkel Enevoldsen

”De IT-sikkerhedsforanstaltninger vi har taget, er **efter anbefaling fra** vores IT-leverandør. Det er dem, der har fingrene på pulsen. De ved hvad der sker, og hvad der er krævet (...)
Vi har et rigtig, rigtig godt forhold til vores eksterne leverandør af cybersikkerhed. Det er en af de ting, **vi vægter meget højt, at vi har en tæt relation til vores IT-provider**, for det er en central del af det, vi laver”

Beslutningsprocesser støttet af eksterne

Mikkel Enevoldsen er CEO i Saxe Hansen, der er specialiseret i maskiner til plastproduktion. Gennem årene har virksomheden aktivt arbejdet for at opnå en høj grad af modstandsdygtighed mod cybertrusler. Deres indsats blev intensiveret i 2006 som følge af krav fra virksomhedens kunder. Siden da har Saxe Hansen implementeret en række foranstaltninger, herunder flytning af deres data til skyen og serverhoteller, indførelse af antivirusprogrammer, GDPR-politik, brug af Multi-Factor Authentication (MFA) og totrinsgodkendelse for transaktioner. Mikkel Enevoldsen har desuden haft fokus på medarbejdernes arbejdsgange og rutiner, og hvordan disse kan forbedres gennem oplysningskampagner og tydelige retningslinjer.

Saxe Hansens solide cybersikkerhedsberedskab er resultatet af mange års dedikation og kontinuerlige investeringer. På rejsen har partnerskabet med en ekstern IT-leverandør spillet en afgørende rolle i beslutningsprocessen om investeringer i nye tiltag. Mikkel Enevoldsen fremhæver, at samarbejdet med eksterne rådgivere giver Saxe Hansen mulighed for at fokusere på deres kerneforretning. At alliere sig med specialister bidrager til at virksomheden er i overensstemmelse med de nyeste sikkerhedsstandarder og bedste praksis. En tæt og tillidsfuld relation mellem de to virksomheder er en afgørende faktor for at Mikkel kan bruge dem i sin beslutningsproces og løbende holde sig ajourført.

Samlet set repræsenterer Saxe Hansen en ambitiøs tilgang til cybersikkerhed med fokus på samarbejde med en kompetent ekstern partner for at beskytte sine kritiske data.

Kendetegn

- Eksterne eksperter
- Partnerskab
- Modstandsdygtig

Et godt råd

”Entrer med en ekstern virksomhed til at håndtere jeres IT-sikkerhed (...) Det kan være ekstremt farligt at udtrykke overfor medarbejdere, at hvis de tager telefonen og ringer til IT-support, så koster det penge. Det skal man holde sig fra at kommunikere ud. Den har vi i Saxe Hansen punkteret ved at sige, at vi har en fast pris pr. måned, og så tager vi en evaluering hen ad vejen (...) **Vi kan trygt sige til medarbejderne ”ring med det samme til IT-supporten, hvis der er et eller andet, du er i tvivl om** eller der er en mail, du ikke ved om du skal åbne”. Det er faktisk den billige løsning på langt sigt, især for mindre virksomheder og start-ups”

4

Værdikædens cybersikkerhed

Cybersikkerhed er højt prioritet ved valg af underleverandør

Med indførelsen af NIS2-direktivet i 2024 kommer der skærpede krav til virksomheders cybersikkerhed. Selvom kravene kun rammer nogle grupper virksomheder direkte, stiller direktivet øgede krav til disse virksomheders underleverandører. Det bliver blandt andet påkrævet at beskytte deres værdikæders cybersikkerhed.

Cybersikkerhed i værdikæden er også temaet for dette års undersøgelse. Vi søger svar på, hvorvidt SMV'er er opmærksomme på deres underleverandørers cybersikkerhed, hvilke incitamenter der driver dem til at prioritere værdikædens sikkerhed, og om de oplever krav fra til værdikæden fra deres kunder, bestyrelse eller samarbejdspartnere. Resultaterne fra vores undersøgelse viser, at hele 61 pct. af SMV'erne anser deres underleverandørers cybersikkerhed som vigtig eller meget vigtig. Det indikerer, at der generelt eksisterer en opmærksomhed på betydningen af underleverandørers cybersikkerhed.

Når vi spørger ind til, om omverdenen stiller krav til SMV'erne i forhold til deres underleverandørers cybersikkerhed, oplever 35 pct. af virksomhederne krav fra bestyrelsen, lovgivningen, samarbejdspartnere, nationale kunder, internationale kunder og/eller investorer samt aktionærer.

Figur 10: Hvor vigtigt er cybersikkerhed, når I vælger underleverandører?

61%

af SMV'erne mener, at cybersikkerhed er vigtigt eller meget vigtigt, når de vælger underleverandører

N=866. Kun SMV'er som har indført cybersikkerhedstiltag er blevet stillet spørgsmålet.

Figur 11: Oplever I krav til at jeres underleverandører skal have et højt niveau af cybersikkerhed?

35%

af SMV'erne oplever krav til, at deres underleverandører skal have et højt niveau af cybersikkerhed

N=866. Kun SMV'er som har indført cybersikkerhedstiltag er blevet stillet spørgsmålet. Note: Svarmuligheder: Ja, fra lovgivning; ja, fra bestyrelsen; Ja, fra samarbejdspartnere; Ja, fra vores internationale kunder; Ja, fra vores nationale kunder; Ja, fra vores aktionærer og/eller investorer; Ja, fra andre; Nej.

Af de 35 pct. af SMV'erne, der oplever krav vedrørende deres underleverandørers cybersikkerhed, varierer det hvem kravene kommer fra. Figur 12 præsenterer en opdeling af, hvor kraene stammer fra.

17 pct., oplever krav fra lovgivningen. Lovgivningen er det felt, hvorfra flest SMV'er oplever krav, hvilket tyder på, at lovgivning spiller en afgørende rolle for fokus på underleverandørers cybersikkerhed.

Næsten lige så mange (15 pct.) peger på bestyrelsen som en kilde til krav, hvilket indikerer at underleverandørers cybersikkerhed, såvel som virksomhedens egen cybersikkerhed, så småt har fået en plads på dagsordenen i bestyrelseslokalerne.

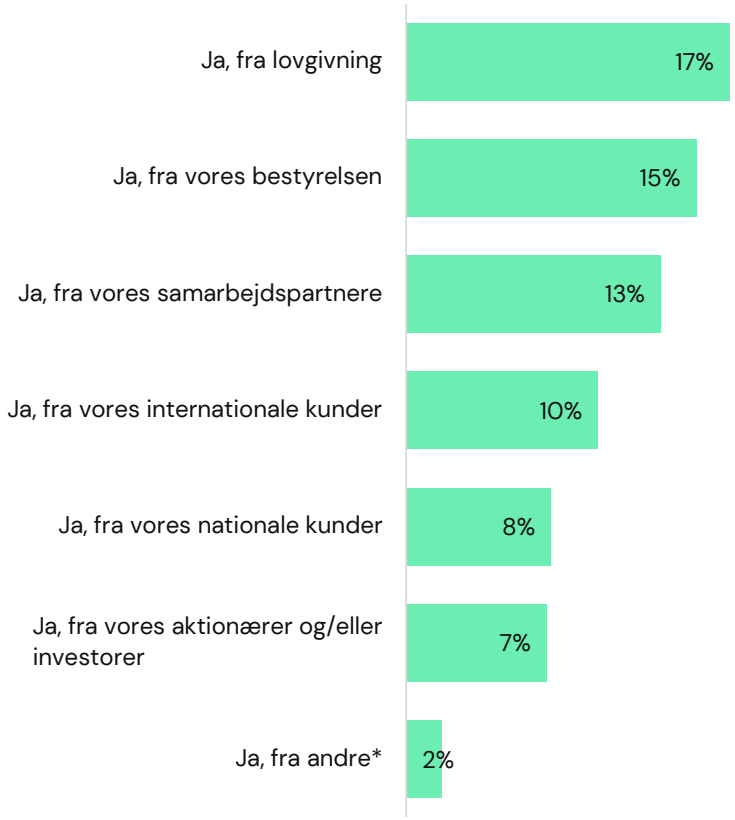
Derudover er der en andel, der møder krav fra samarbejdspartnere (13 pct.). Krav fra kunder, internationale og nationale, opleves ligeledes af omkring hver tiende (hhv. 10 pct. og 8 pct.).

At lovgivningen spiller en afgørende rolle for hvordan SMV'er håndterer cybersikkerhed, ser vi blandt andet hos virksomheden EWII. Direktør Claus Møller forklarer, hvordan virksomheden er underlagt lovgivningen:

"Vi er opdelt i forskellige kommercielle divisioner, hvor jeg er direktør for den ene. Derudover har vi TREFOR, som er vores regulerede forretningsområde. Inden for de regulerede forretningsområder er der forskellige instanser, herunder ministerier, der udstikker krav. De laver løbende test af, om vores stationer er videoovervågede, hvordan vores processer forløber osv. Der er løbende krav til at vi styrker sikkerheden, herunder også it-sikkerheden. Så der er nogen, der holder øje med os."
Claus Møller, Direktør, Information & Kommunikation

På næste side kan du læse mere om, hvordan EWII håndterer cybersikkerhed på et strengt reguleret marked.

Figur 12: Oplever I krav til at jeres underleverandører skal have et højt niveau af cybersikkerhed?



N=866. Kun SMV'er som har indført cybersikkerhedstiltag er blevet stillet spørgsmålet.

EWII

Energi- og kommunikationsvirksomhed med 600 ansatte
Interview med Direktør, Claus Møller

”Det er en underforstået ting, at vi er sikre på vores cybersikkerhed. **Det forventes.**

Ligesom hvis du køber et hus, så forventer du også, at der er strøm i stikkontakterne. **Det er en grundpræmi**s.”

Når kun 100% er godt nok

EWII har sit hovedkvarter i Trekantsområdet og leverer elektricitet, vand, fjernvarme, fiber, bredbåndstjenester samt varmepumper og ladestandere. Direktøren for kommerciel infrastruktur, Claus Møller, påpeger, at cyberangreb betragtes som en afgørende trussel mod virksomheden. Som udbyder af kritisk infrastruktur kan cyberhændelser potentielt lamme forsyningsinfrastrukturen og medføre store problemer for samfundet. Selv mindre afvigelser i driften har betydning, da EWII skal leve op til forbrugernes forventninger om pålidelighed og stabilitet.

EWII-koncernen omfatter både kommercielle divisioner og regulerede forretningsområder. De regulerede forretninger inkluderer selskaberne TREFOR Vand, -Varme og -Elnet, som er underlagt en række krav til cybersikkerhed i henhold til lovgivningen. I forsyningssektoren, der betragtes som kritisk, er omfattende regulering og tilsyn normal praksis for at sikre overholdelse af høje standarder for driftssikkerhed. Disse regulatoriske organer spiller selvsagt en væsentlig rolle i EWIIs arbejde med at sikre sine systemer. Blandt andet samarbejder EWII med Center for cybersikkerhed (CFCS), der støtter sikkerhedsniveauet og gennemfører regelmæssig kontrol. EWII har desuden interne cybersikkerhedssystemer, herunder en styrekomité og dedikerede medarbejdere, der løbende overvåger sikkerheden. Virksomheden følger desuden NIS2 og ISO 27001.

Dette tegner et billede af en virksomhed, der i høj grad har systematiseret sit arbejde med cybersikkerhed. En nødvendighed når man opererer i et reguleret marked og er underlagt høje krav fra lovgivningen. Som Claus Møller udtrykker det: ”Vi vil være 100% hele tiden. Du får ikke nødvendigvis noget ud af at være 110%, men hvis du er 90%, så gør det ondt”.

Kendetegn

- Kritisk infrastruktur
- Regulerede forretningsområder
- Driftssikkerhed

Et godt råd

”En af de ting, som brancheorganisationer kan, er at de har masser af kompetencer, som de deler ud af til virksomhederne. Eksempelvis indenfor IT-sikkerhed men også jura, eksport, import, EU-støtte osv. Altså der er rigtig meget at få. Og det gælder alle brancheorganisationer. Men de helt små virksomheder, de bruger det ikke, de melder sig bare ind, men får ikke trukket på organisationerne. Det ville de få meget ud af”

Ydre krav skaber opmærksomhed mod underleverandørers cybersikkerhed

En stor del af SMV'erne finder altså underleverandørers cybersikkerhed vigtig, mens en mindre del oplever ydre krav til selvsamme. Men hvordan påvirker eksterne krav *motivationen* til at prioritere underleverandørers cybersikkerhed?

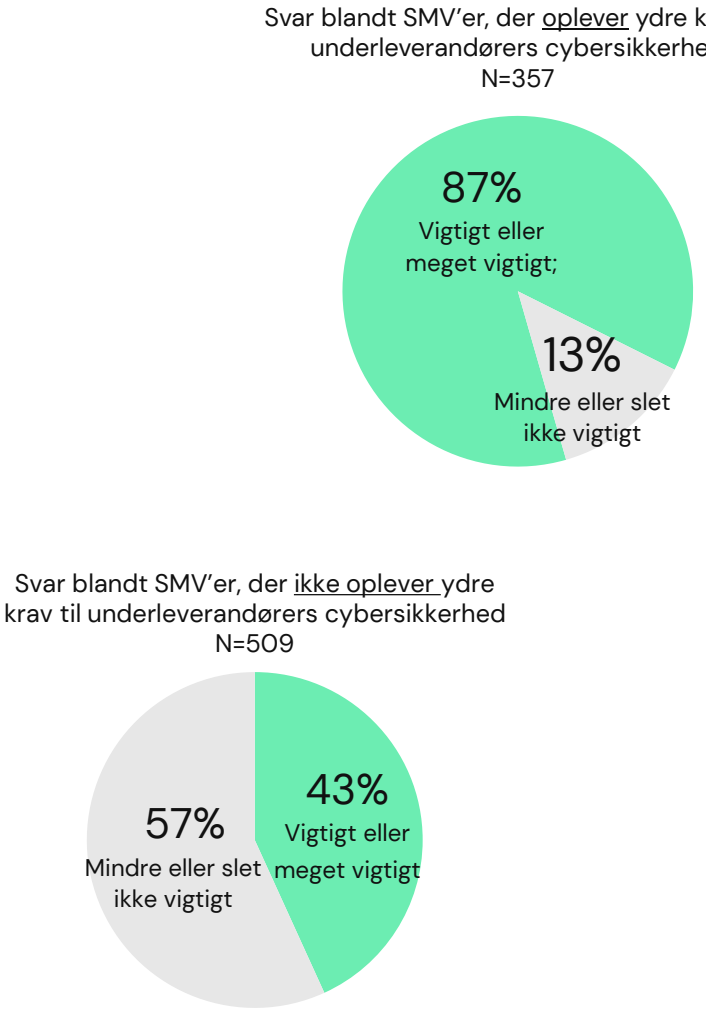
Figur 13 viser to cirkeldiagrammer, der opdeler SMV'erne i hvorvidt de oplever ydre krav til deres underleverandørers sikkerhed eller ej. For de to grupper har vi opgjort holdningen til vigtigheden af cybersikkerhed, når de vælger underleverandører.

Der ses et tydeligt mønster – de SMV'er, der oplever ydre krav, ser også deres underleverandørers cybersikkerhed som mere vigtig (de grønne andele).

Blandt SMV'erne, der oplever eksterne krav (øverste cirkel), finder hele 87 pct. underleverandørers cybersikkerhed vigtig eller meget vigtig. Dette står i kontrast til virksomheder uden ydre krav (nederste cirkel), hvor kun 43 pct. anser underleverandørers cybersikkerhed som vigtig eller meget vigtig. Her skal også bemærkes, at der er hele 57 pct., der finder deres underleverandørers cybersikkerhed mindre eller slet ikke vigtig. Det svarer til, at hver tredje SMV hverken oplever ydre krav til deres underleverandørers cybersikkerhed eller mener, at det er særlig vigtigt.

På næste side ser vi nærmere på virksomhedens Vestfrosts arbejde med cybersikkerhed, og blik for værdikæden.

Figur 13: Hvor vigtigt er cybersikkerhed, når I vælger underleverandører? Fordelt på, hvorvidt SMV'en oplever ydre krav eller ej.



Note: Spørgsmål til krav lyder: Oplever I krav til at jeres underleverandører skal have et højt niveau af cybersikkerhed? Med tilhørende svarmuligheder Ja, fra lovgivning; ja. frabestyrelsen; Ja, fra samarbejdspartnere; Ja, fra vores internationale kunder; Ja, fra vores nationale kunder; Ja, fra vores aktionærer og/eller investorer; Ja, fra andre; Nej.

Vestfrost Solutions

Fremstillingsvirksomhed med 201 ansatte
Interview med CFO, Jannie Tholstrup

”Lige så vel som at der kan komme et cyber-attack igennem vores egne leverandører eller servicepartnere, så **er vi jo også en faktor for vores kunder, når de kortlægger deres risikobillede.** Jeg mener derfor at det er en helt naturlig del i at have sin berettigelse som en professionel samarbejdspartner (...) det har jo også betydning for om de får produkter ud.”

Kunderne har fokus på cybersikkerhed gennem hele værdikæden

I danske Vestfrost Solutions, der er specialiseret i produktion af køle- og fryseløsninger, understreges vigtigheden af en helhedsorienteret tilgang til cybersikkerhed, der omfatter hele systemlandskabet. Virksomhedens CFO, Jannie Tholstrup, understreger at et stærkt forsvar om virksomhedens aktiver og data etableres ved både at have tekniske foranstaltninger samt klare procedure og retningslinjer for medarbejderadfærd.

I Vestfrost handler cybersikkerhed ikke kun om øjeblikkelige gevinster. Det er snarere opbyggelsen af grundlæggende forudsætninger for at være en professionel samarbejdspartner for store kunder som Electrolux og Red Bull. Disse kunder gennemfører regelmæssige audits og vurderinger af Vestfrost som underleverandør, og cybersikkerhed spiller en afgørende rolle i deres evaluering. Der stilles krav til governance, procedurer og beredskabsplaner til håndtering af potentielle cyberangreb.

Jannie fremhæver, at kundernes krav til cybersikkerhed er en del af en udvidet forståelse af cybersikkerhed. De tager ikke kun deres egen sikkerhed i betragtning, men inkluderer også eksterne samarbejdspartnere og leverandører, herunder Vestfrost, som en del af deres risikobillede. Den måde at arbejde med cybersikkerhed på indebærer løbende auditprocesser og dialog, som naturligt indgår i en fælles bestræbelse på at opretholde høje standarder for cybersikkerhed på tværs af værdikædens aktører.

Kendetegn

- Helhedsorienteret
- License to play
- Audits og evaluering

Et godt råd

”Jeg ville sikre mig, at hele min organisation - uanset om det drejer sig 9 personer eller 50 eller 100 - er bevidst om hvad cybersikkerhed er. **Så emnet ikke bliver elefanten i rummet.** Deri ligger en stor ledelsesmæssig kommunikationsopgave. På den måde kan du også finde talenter i organisationen, der har interesse for emnet og kan bære det videre. Det er en god måde at komme i gang på: **At du får det ud og leve i virksomheden, får flere til at interessere sig og at du vækker en nysgerrighed.** ”

Større tiltro til store underleverandørers cybersikkerhed

Det er gradvist blevet vigtigere og vigtigere at indtænke hele værdikæden, når man arbejder med cybersikkerhed. Man kan have sikret sine forretningshemmeligheder og systemer perfekt, men er værdikæden usikker, kan man alligevel risikere angreb.

En ting som undersøgelsens casevirksomheder peger på som vigtigt for værdikæden, er virksomhedernes størrelse. Virksomhedens egen størrelse i forhold til underleverandørers størrelse, og underleverandørers størrelse generelt, spiller ind på, hvordan man anskuer deres cybersikkerhed og hvilke krav man kan stille til dem. Mange forventer, at store underleverandører har styr på deres cybersikkerhed, og stiller derfor sjældent krav til dem. Modsat er det for de små virksomheder – de oplever ofte krav fra virksomheder, der er større end dem selv.

"Cybersikkerhed er en forudsætning for samarbejdet med især Vestfrosts store kunder."
Jannie Tholstrup, CFO, Fremstilling

Hos Fremstillingsvirksomheden Vestfrost fortæller CFO Jannie Tholstrup, at de som en del af kundernes værdikæde ofte møder krav og forventninger til niveauet af cybersikkerhed. Som leverandør og samarbejdspartner udgør virksomheden en potentiel sårbarhed for sine kunder, og derfor bliver auditering og løbende dialog en naturlig del af samarbejdet i at risikostyre og sikre cybersikkerheden på tværs af værdikæden. Hun fortæller:

"Lige præcis med de samarbejdspartnere - med den størrelse de har - er det klart, at vi løbende har en dialog om, hvad vi er for en partner. Vi bliver vurderet og auditeret løbende, og det gør vi på alle parametre inden for IT og sikkerhed. Ligesom på vores almindelige IT-certificeringer, som vi også har, får vi løbende auditbesøg fra de store samarbejdspartnere. "
Jannie Tholstrup, CFO, Fremstilling

Størrelsen spiller ligeledes ind, når SMV'erne selv skal stille krav til deres underleverandører. Her er tiltroen større til de store techgiganter end til den mindre OEM-virksomhed (OEM er en forkortelse af Original Equiment Manufacturer, svarende til producenten af det oprindelige produkt).

"De fleste af vores underleverandører er lige så store som vores OEM'ere, som har, jeg ved ikke hvor mange milliarder EURO i overskud. Så kommer vi som den lille kunde, der ikke kan stille de store krav, desværre. Men vi må gå ud fra, når man er i den størrelse at man ligesom har styr på tingene."
Anonym CEO, Fremstilling

På næste side ser vi på hvordan størrelse spiller ind på SMV'ernes blik på værdikæden.

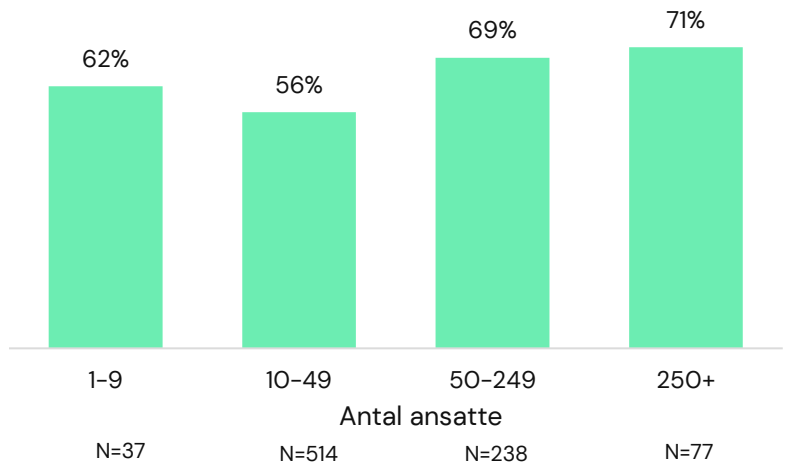
Når vi ser på forskellen mellem mikro, små og mellemstore virksomheders syn på *vigtigheden* af underleverandørers cybersikkerhed er forskellene forholdsvis små (15 procentpoints forskel fra de mindste til de største SMV'er).

På figur 14 kan man se, at blandt de større SMV'er med 250 eller flere ansatte er der 71 pct., som mener at cybersikkerhed er vigtig eller meget vigtig, når de vælger underleverandører. Lidt overraskende findes de laveste andel af virksomheder, der finder underleverandørers cybersikkerhed vigtig, blandt SMV'er med 10-49 ansatte (56 pct.)

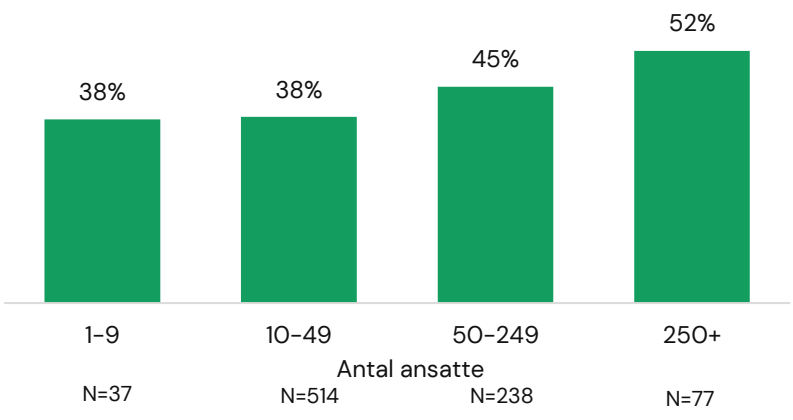
Der viser sig nogenlunde samme mønster, når man spørger virksomhederne til, hvorvidt de oplever ydre krav til deres underleverandørers cybersikkerhed på figur 15. Her er der også en overvægt af de større SMV'er, der oplever krav. Forskellene mellem forskellige størrelser virksomheder er dog små.

Resultaterne peger på at størrelse spiller ind på SMV'ernes forhold til cybersikkerhed i værdikæden, men som vi viser i kapital 6 spiller branche en større rolle.

Figur 14: Andel, der mener at cybersikkerhed er vigtigt eller meget vigtigt, når de vælger underleverandører, efter antal ansatte



Figur 15: Andel, der oplever krav til at deres underleverandører skal have et højt niveau af cybersikkerhed, efter antal ansatte



Motivation for cybersikkerhed

Kundekrav og fremtidssikring motiverer

I de kvalitative interviews peger flere på, at kundernes krav er en afgørende motivationsfaktor for at opnå og vedligeholde et højt niveau af cybersikkerhed. Flere af virksomhederne oplever at deres kunder forventer pålidelige og sikre IT-systemer:

"I første omgang, det var så før jeg kom, var det vores kunder, som krævede CFR 11 part 21. Det er et krav om at opbevare deres data i et sikkert sted i mindst 11 år. Det satte ligesom skub i nogle ting. De efterspurgte nogle services fra os, som var mere dokumentationstunge. Det skubbede os til at kigge på vores IT-sikkerhed på en anden måde. Det har været omkring 2006."
Mikkel Enevoldsen, CEO, Fremstilling

Fordi efterlevelsen af kundernes forventninger og krav er afgørende for SMV'ernes forretningsmæssige succes, bliver de ofte også vigtige retningslinjer for virksomhedens investeringer i cybersikkerhed.

Flere casevirksomheder anser desuden cybersikkerhed som en form for fremtidssikring, hvilket er en stærk motivationsfaktor.

De ser cybersikkerhed som en beskyttelse af virksomhedens aktiver, herunder forretningshemmeligheder og økonomiske ressourcer. Med et stigende trusselsniveau år for år, bliver cybersikkerhed også mere og mere nødvendigt:

Jannie Tholstrup fortæller at hun forventer at cybersikkerhed kommer til at blive helt afgørende i fremtiden:

"Jeg tror at cybersikkerhed kan blive et stort topic i fremtiden, ligesom man har set med bæredygtighedsrapportering. Det bliver en forudsætning for overhovedet at kunne skabe profit og have en berettigelse som virksomhed."
Jannie Tholstrup, CFO, Fremstilling

Også Michael Seerup, CEO i virksomheden Uggerly, forudser at cybersikkerhed vil få endnu mere opmærksomhed fremadrettet:

"Nu er det så den grønne omstilling, folk har fokus på nu. Så det med cybersikkerhed, det tror jeg bliver den næste ting, der kommer. Nu kører det på alt det her i ESG, om vi skal minimere CO2, og kan vi få nogen i vores værdikæde til at minimere deres og vores samlede produkt. Det er dér fokus, det ligger."
Michael Seerup, administrationschef, Bygge & anlæg

Cybersikkerhed opfattes altså som et vigtigt konkurrenceparameter, der vil få afgørende indflydelse i fremtiden på linje med den grønne omstilling.

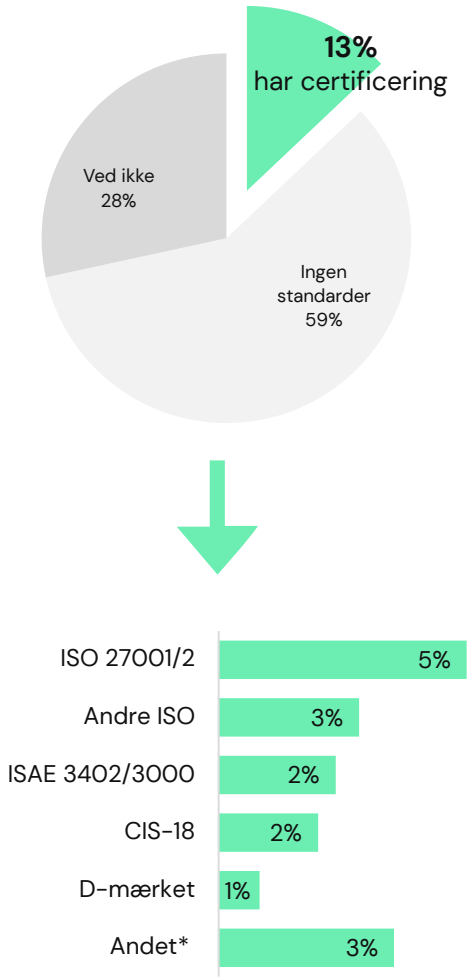
De færreste SMV'er har certificeringer

Figur 16 viser, at blot 13 pct. af SMV'erne har opnået certificeringer som eksempelvis ISO 27001/2, CIS-18 eller D-mærket.

Blandt de kvalitative interviews, hvor alle virksomhederne har stærk cybersikerhed, er der ligeledes få, der følger formelle certificeringsstandarder. De kender til standarderne og bruger dem som reference, når det er nødvendigt. For dem er det dog vigtige at følge forskellige kunders krav og forventninger (som beskrevet på forrige side).

En årsag til at så få SMV'er følger standarder kan derfor være, at mange møder skiftende krav i deres hverdag. Derfor bliver det vigtigere at følge forventninger fra en konkret kunde, frem for en certificering.

Figur 16: Andel af SMV'er med certificeringer



*Andet dækker over en masse certificeringer, der også omfatter product-og kvalitetskontrol, og også forskellige andre mindre kendte certificeringer. Respondeter kan svare forskellige standarder, hvorfor summen overstiger 100%.

Hver tredje ser cybersikkerhed som "license to play"

I afsnit 3 så vi at SMV'ers investeringer i cybersikkerhed hånd i hånd med konkurrencefordele. Ud over konkrete fordele indenfor kategorierne 'Effektivitet & Innovation', 'Tillid' og 'Bundlinje', har vi dog også undersøgt hvorvidt virksomhederne oplever at stærk cybersikkerhed bidrager til at have en position på markedet.

I den sammenhæng svarer knap hver tredje SMV (32 pct.), at virksomhedens cybersikkerhedsindsats i det store hele har bidraget til at fastholde eller styrke dens position på markedet.

Tallet stemmer overens med det, som flere interviewpersoner fremhæver: For nogle virksomheder er cybersikkerhed altså en forudsætning for at have sin berettigelse som leverandør, samarbejdspartner og virksomhed. For eksempel fortæller Claus Møller fra EWII, at cybersikkerhed er afgørende for deres eksistensgrundlag. Det betragtes som en selvfølgelighed, ligesom at man forventer strøm i sine stikkontakter.

"Det er en underforstået ting, at vi er sikre på vores cybersikkerhed. Det forventes. Ligesom hvis du køber et hus, så forventer du også, at der er strøm i stikkontakterne. Det er en grundpræmis."
Claus Møller, Direktør, Information & kommunikation

Det samme fremhæver CFO i Vestfrost, Jannie Tholstrup:

"Jeg ved ikke, om der er gevinster, men jeg vil sige, at for mig er det en forudsætning for at kunne være en professionel samarbejdspartner."
Jannie Tholstrup, CFO, Fremstilling

Forskel på tværs af brancher

Cybersikkerhed gavner alle brancher

I dette kapitel ser vi nærmere på de fire brancher*: Bygge & anlæg, Fremstilling, Transport & godshåndtering og Information & kommunikation, og hvor de er i deres rejse med cybersikkerhed og hvordan de oplever konkurrencefordelene af deres tiltag. I årets undersøgelse ser vi samme tendenser som sidste år, nemlig at Bygge & anlæg har indført færrest tiltag, men at der på tværs af alle brancher er en klar sammenhæng: Jo flere cybersikkerhedstiltag, des flere oplever konkurrencefordele.

Mens vi i kapitel 4 har vist, at størrelse spiller en rolle i forhold til, hvor interesseret man er i underleverandørers cybersikkerhed og hvor mange ydre krav fra omverdenden man oplever, gør det samme sig gældende for forskellige brancher. Nogle brancher er først lige begyndt på arbejdet med cybersikkerhed, mens andre har det som en del af deres DNA – det er simpelthen nødvendigt for at kunne være på markedet.

Vi zoomer ind på to virksomheder, der begge har indført flere cybersikkerhedstiltag de seneste to år i deres virksomheder, og også oplevet en del konkurrencefordele af dem, men som er i forskellige brancher og faser af arbejdet med cybersikkerhed.

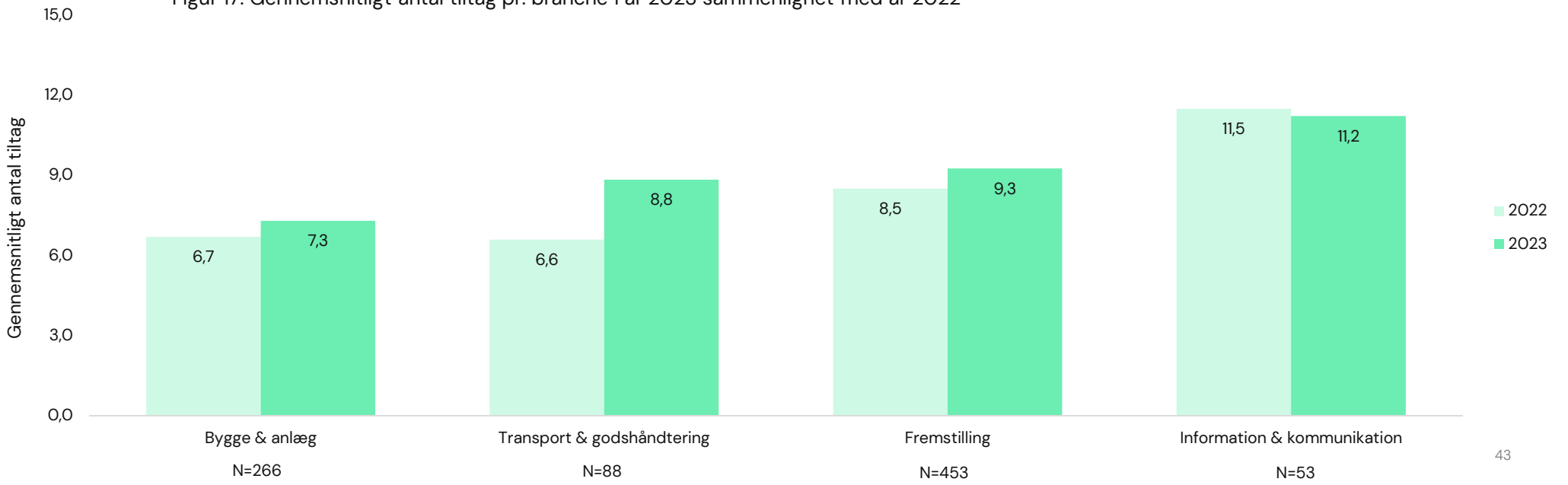
* Branchen råstofudvinding indgår også i undersøgelsen, men da branchen er lille, har vi for få besvarelser til at tegne et retvisende billede af branchen.

Figur 17 viser udviklingen i det gennemsnitlige antal tiltag på tværs af brancher. Fra 2022 til 2023 er der sket en stigning blandt virksomheder i både Bygge & anlæg, Fremstilling samt Transport & godshåndtering, mens der ses et lille fald for Information & kommunikation. Især Transport & Godshåndtering har oplevet en markant udvikling, hvor virksomheder nu i gennemsnit har 8,8 tiltag, sammenlignet med 6,6 tiltag i 2022.

Information & kommunikation er den eneste branche, hvor der har været en mindre tilbagegang eller stagnation (fra 11,5 til 11,2 tiltag). Det er dog værd at bemærke, at denne branche stadig opererer på et højt niveau af cybersikkerhedstiltag. De er begrænset til de 15 tiltag, vi spørger til, og for brancher, der allerede opererer på et avanceret niveau af cybersikkerhed, vil der være mindre udsving år for år.

Det er fortsat de samme brancher, der har henholdsvis færrest og flest cybersikkerhedstiltag som i 2022. Bygge & Anlæg har stadig det laveste antal tiltag pr. virksomhed, efterfulgt af Transport & godshåndtering og Fremstilling. Information & Kommunikation forbliver branchen med det højeste niveau af cybersikkerhedstiltag pr. virksomhed, som det var tilfældet i 2022. Dette vedvarende mønster kan tyde på, at der er forskel mellem branchernes tilgang til cybersikkerhed. Det kan være vigtigt for at forstå og målrette cyberindsatser effektivt.

Figur 17: Gennemsnitligt antal tiltag pr. branche i år 2023 sammenlignet med år 2022



Der kan være en tendens til at tro, at cybersikkerhed primært er nødvendig for IT-virksomheder, og at erhverv hvor digitalisering *ikke* er en kerneydelse dermed *ikke* drager fordele af deres cybersikkerhedsindsatser. Men når SMV'er selv vurderer fordele ved deres cybersikkerhedsinitiativer, er svarene ensartede på tværs af brancher: Jo flere initiativer de har implementeret, desto flere oplever konkurrencefordele. Det illustreres i Figur 18.

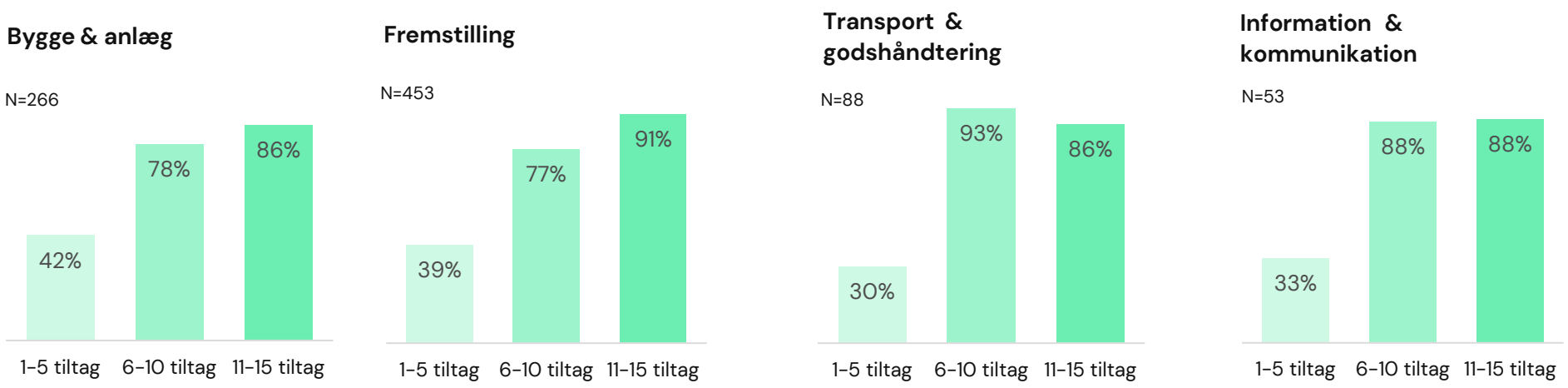
Der er dog små variationer mellem brancherne. Det ser ud til, at en større andel inden for Bygge- og anlæg og Fremstilling oplever fordele ved blot at have et begrænset antal initiativer (1-5) sammenlignet med Transport- & godshåndtering eller Information & kommunikationsbranchen.

Det tyder på, at cybersikkerhedstiltag som beskyttelse mod malware kan have positiv effekt, især inden for Bygge & anlæg samt Fremstilling. Det fungerer også som en opfordring til at komme i gang med cybersikkerhed i de to sektorer, for der er gevinster at hente tidligt.

I Transport & godshåndtering samt Information & kommunikationsbranchen ser det ud til, at de største fordele opleves, når virksomheder når op på mere end 5 initiativer. Her oplever en stor andel (hhv. 93 pct. og 88 pct.) fordele.

Der ses en lille tilbagegang i fordelene fra intervallet med 6-10 initiativer til intervallet med 11-15 initiativer for Transport & godshåndtering. Ikke desto mindre er begge disse grupper stadig betydeligt høje i andel, der oplever fordele, hvilket indikerer, at investering i cybersikkerhed fortsat er en fornuftig beslutning i disse brancher.

Figur 18: Andel, der oplever konkurrencefordele ved deres cybersikkerhedstiltag, fordelt på antal tiltag og branche



I nogle brancher er cybersikkerhed nyt

Vi taler med undersøgelsens interviewpersoner om, hvordan de oplever at cybersikkerhed bliver håndteret i deres branche.

På tværs af brancher er bygge & anlæg branchen med lavest gennemsnitlige antal tiltag. Det resultat præsenterer vi for B.E. Installationers CEO, Brian Bryrup. Han svarer:

"Jeg tror at mange i branchen har haft den antagelse, at de ikke havde noget, altså information, som var værd at stjæle. Men de sidste par år har vist, at det har man måske alligevel. Jeg har selv været i en virksomhed, som fik noget ransomware ind. Det kan koste rigtig mange penge. Jeg tror at det er et spørgsmål om, at der kommer nogle eksempler frem. På den måde tror jeg, at flere i byggebranchen vil få øjnene op for det"
Brian Bryrup, CEO, Bygge & anlæg

Ifølge Brian er det altså en udbredt antagelse i byggebranchen, og måske også i andre brancher, at man som virksomhed ikke besidder værdifuld information, som andre skulle have interesse i at stjæle. Dog mener han, at denne opfattelse måske er ved at ændre sig, især i de seneste år.

En mulig årsag til at implementeringen af cybersikkerhedstiltag ikke har samme udbredelse blandt bygge- og anlægsvirksomheder kan skyldes at digitalisering, og dermed også beskyttelse af digitale aktiver, er et relativt nyt emne i branchen.

Det pointerer Michael Seerup, CEO i Uggerly – en virksomhed, der har været frontløber inden for digitalisering ved at anvende robotteknologi for at opnå konkurrencefordele i automatiserede opgaver. Men den tilgang præger ikke branchen som helhed:

"Jeg kom fra Forsvaret og tænkte "Forsvaret - det må være en IT-dinosaur". Men så oplevede jeg byggebranchen (griner). For ti år siden skrev folk deres arbejdssedler i hånden (...) Og så sad der en stakkels pige og tastede alting ind. Men om der stod 4 eller 9, det var jo ikke til at vide. Så hver gang at der var løn, så ringede telefonen med fejl, som skulle rettes. Den dag vi digitaliserede holdt telefonen op med at ringe"
Michael Seerup, administrationschef, CEO, Bygge & anlæg

I kontrast til byggebranchen viser interviews med EWII og Telenabler - to virksomheder inden for Information & Kommunikation - at i brancher, hvor digitalisering og fokus på datasikkerhed har været til stede i lang tid, er der større bevidsthed om cybersikkerhed. De har begge IT som kerneydelse.

På den næste side præsenterer vi et eksempel på, hvordan cybersikkerhed kan styrkes gennem samarbejde i branchen.

Telenabler

IT- og kommunikationsvirksomhed med 16 ansatte
Interview med direktør, Jens Fricke

”Jeg er med i et netværk af kunder og leverandører. På vores konferencer kommer forskellige eksperter og taler om cybersikkerhed. **På den ene side, så sidder vi der som konkurrenter, men på den anden side, så er vi i samme båd.** Altså, vi køber trafik og net-kapacitet af TDC og Telenor. Hvis de bliver ramt, så er det måske 40% af salen, der også rammes. Det er den samme markedsandel, vi kæmper om, men vi er også i samme båd. Derfor er det til alles fordel, at vi er på forkant”

Cybersikkerhed som et fælles brancheanliggende

I telebranchen, hvor pålidelig og sikker kommunikation er afgørende for kunders og samarbejdspartneres tillid, har Telenabler skarpt fokus på cybersikkerhed. Jens Fricke, virksomhedens CEO, ser cybersikkerhed som en absolut nødvendighed. Den opfattelse forstærkes af, at han har set andre aktører i branchen, der har forsøgt at skære ned på sikkerhedsomkostninger for at levere billige produkter, har lidt alvorlige konsekvenser af succesfulde cyber-angreb. I stedet for at deltage i priskrig foretrækker Jens Fricke hellere ”at gå konservativt og midt på vejen” ved at gøre robust forsvar og dataintegritet til centrale elementer i virksomhedens strategi.

Telenablers cybersikkerhed drives frem af et samarbejde mellem CTO, der har teknisk ekspertise og systemforståelse, og CEO Jens Fricke, der træffer beslutninger om fremtidige investeringer baseret på markedsforståelse og indsigter i potentielle trusler.

Helt afgørende for Jens Frickes mulighed for at forudsige og reagere på nye tendenser, er hans aktive deltagelse i samarbejdsnetværk og konferencer med andre teleaktører, hvor der deles viden og erfaringer. Han er opmærksom på, at Telenabler er en del af et bredere netværk af kunder og leverandører, hvor cybersikkerhed er en gensidigt afhængig faktor. Televirksomheder benytter nemlig ofte samme netværk og teknologier. Som leverandører og partnere i hinandens værdikæder, er der derfor et kollektivt ansvar i at opretholde en høj standard for cybersikkerhed. For Telenabler er cybersikkerhed derfor ikke bare en udfordring for virksomheden, men er også et branchespørgsmål.

Kendetegn

- Branchefællesskab
- Sikker kommunikation
- Robust forsvar

Et godt råd

”Tag fat i nogen, der har været i samme situation. Altså en anden virksomhed, måske i samme branche, og spørg hvad de har af erfaring: Hvad har de gjort? Har de en IT-ansvarlig? **Få nogle råd og vejledning** af dem. Især i en mindre virksomhed, der skal begynde at fokusere på det her, skal man gå optimistisk og undersøgende ind i det. Lad være med kun at se hullerne i osten. Selvfølgelig skal I gøre noget ved cybersikkerhed, men I må ikke blive for bange, og bruge alle jeres penge på de dyreste løsninger. **Tag først en snak med nogen, der har stået i den samme suppedas som jer selv**”

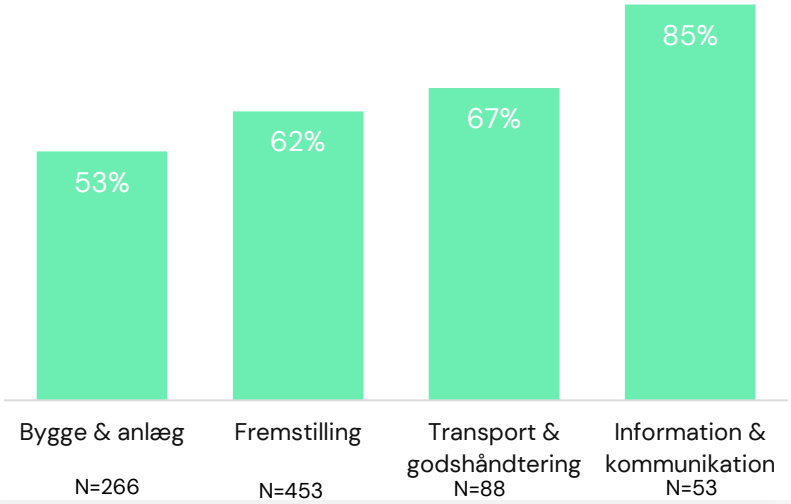
Hvor vi i kapitel 4 viste, at SMV'erne finder underleverandørers cybersikkerhed vigtig, ser interessen for værdikæden noget anderledes ud for flere brancher.

Figur 19 viser, at der er betydelige forskelle på tværs af brancher af, hvorvidt man finder underleverandørers cybersikkerhed vigtig eller ej. Det er lige over halvdelen af SMV'erne inden for Bygge & anlæg, der mener, at det er vigtigt, mens det for SMV'erne i Information & kommunikation er 85 pct.

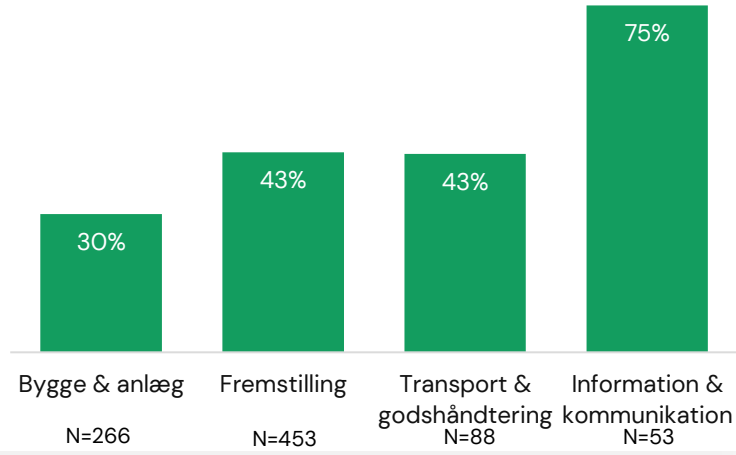
Og der viser sig også samme sammenhæng, som vist i kapitel 4. Brancher, som finder deres underleverandørers cybersikkerhed vigtig, er også brancher, som oplever ydre krav. I figur 20 er det tydeligt, at der særligt blandt Bygge & anlæg er få der oplever ydre krav til deres underleverandørers cybersikkerhed. Kun 30 pct. oplever ydre krav. Hos Fremstilling og Transport & godshåndtering er der 62-67 pct., der finder cybersikkerhed hos underleverandører vigtigt, og i begge brancher er der 43 pct., der oplever ydre krav. Inden for Information & Kommunikation er der hele 75 pct., der oplever ydre krav fra lovgivning, bestyrelse eller andetsteds.

På næste side dykker vi dybere ned i, hvor de ydre krav i brancherne stammer fra.

Figur 19: Andel, der mener at cybersikkerhed er vigtigt eller meget vigtigt, når de vælger underleverandører inden for brancher



Figur 20: Andel, der oplever krav til at deres underleverandører skal have et højt niveau af cybersikkerhed inden for brancher



Som vi så på forrige side er branchen, hvor færrest oplever krav til deres underleverandørers cybersikkerhed, Bygge & anlæg. Inden for den del af branchen, der alligevel oplever ydre krav, kan man i figur 21 se, at kravene hovedsageligt stammer fra lovgivning, mens kunder stort set ikke stiller krav.

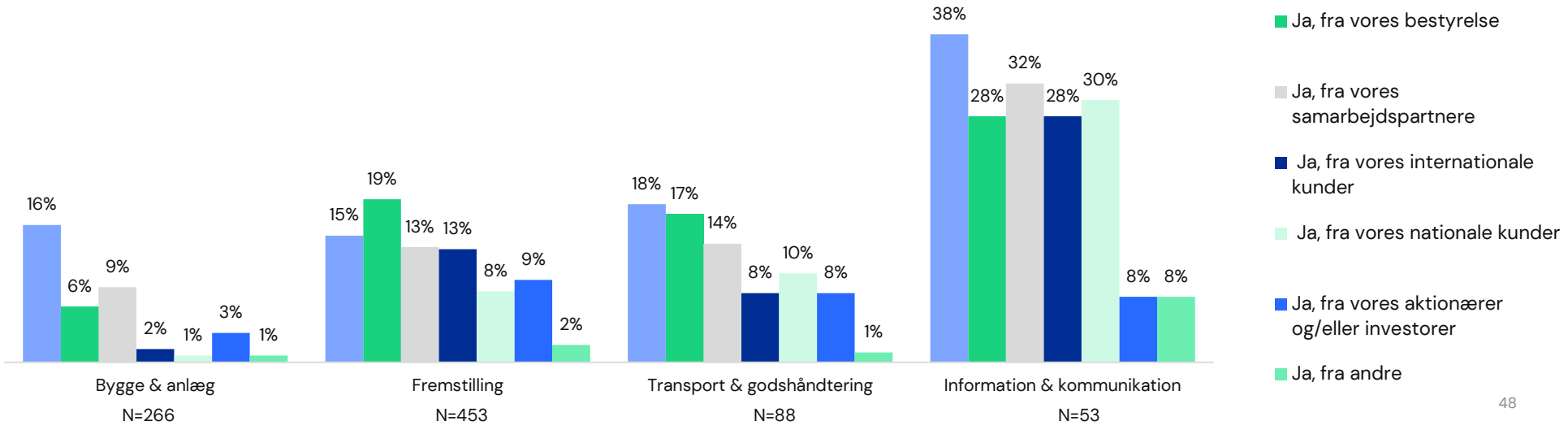
Selvom Fremstilling oplever forholdsvis få krav, kommer kravene flere steder fra. Hovedsageligt fra bestyrelsen (19 pct.), men en stor andel kommer også fra lovgivning (15 pct.), samarbejdspartnere (13 pct.) og international kunder (13 pct.).

For Transport & godshåndtering kommer kravene særligt fra lovgivning (18 pct.), bestyrelse (17 pct.) og samarbejdspartnere (14 pct).

I branchen Information & kommunikation, hvor flest virksomheder oplever ydre krav oplever de fleste krav fra lovgivning (38 pct.) og samarbejdspartnere (32 pct.). Branchen oplever også krav fra deres kunder – både nationale (30 pct.) og internationale (28 pct.).

At lovgivningen er en stor kilde til krav til cybersikkerhed på tværs af brancher kan handle om, at der indføres en de ny regulering på området i disse år, som virksomhederne forholder sig til.

Figur 21: Andel, der oplever krav til at deres underleverandører skal have et højt niveau af cybersikkerhed inden for hvem de oplever krav fra og brancher



Data & metode

Undersøgelsens fokus og metodevalg

Fokus på SMV'er i specifikke brancher

Formålet med undersøgelsen er at analysere sammenhængen mellem cybersikkerhedstiltag og konkurrencefordele i små og mellemstore virksomheder i Danmark. I den sammenhæng defineres små og mellemstore virksomheder, også kendt som SMV'er, som virksomheder med 1-600 medarbejdere. Der er desuden fokus på virksomheder inden for brancherne: 'Bygge og anlæg', 'Fremstilling', 'Information og kommunikation', 'Råstofudvinding' samt 'Transport og godshåndtering'.

Rapporten er en opfølgning på undersøgelsen fra 2022, og belyser således også *udviklingen* inden for cybersikkerhed og konkurrencefordele blandt danske SMV'er. Som en ny tilføjelse lægger denne rapport særlig vægt på at undersøge, hvordan virksomheder sikrer deres cybersikkerhed i deres værdikæde.

Undersøgelsesdesign
Undersøgelsen anvender en kombination af en repræsentativ spørgeskemaundersøgelse og kvalitative interviews. Den kvantitative del af undersøgelsen fokuserer på at kortlægge implementeringen af cybersikkerhedstiltag, konkurrencefordele og sikringen af værdikæden på tværs af brancher. De kvalitative interviews tilføjer nuancering af resultaterne og bidrager med indsigt i oplevelser, holdninger og motivation.

Nedenfor præsenteres udførelsen og de indsamlede data fra både spørgeskemaundersøgelsen og interviewene.

Spørgeskemaundersøgelse

Formål
Spørgeskemaundersøgelsen har til formål at kortlægge cybersikkerhedstiltag og oplevede konkurrencefordele i små og mellemstore virksomheder i brancherne: 'Bygge & anlæg', 'Fremstilling', 'Information & kommunikation', 'Råstofudvinding' samt 'Transport & godshåndtering'.

Rekruttering og besvarelse
Gennem CVR-registeret er der udtrukket e-mails på SMV'er indenfor de fem brancher. Disse er efterfølgende beriget manuelt med mails til virksomhedernes øverste ledelse, for bedst mulig kontakt.

Administrerende direktører/CEO's i virksomhederne er efterfølgende blevet inviteret til at deltage i spørgeskemaundersøgelsen via e-mail. Der er sendt invitationer til 7.919 virksomheder, og 919 har besvaret spørgeskemaet. Det er en svarprocent på 12 pct.. Det er en stigning fra 2022, hvor 729 virksomheder deltog.

En repræsentativ undersøgelse
Som man kan se på bortfaldsanalysen (side 56) har undersøgelsen en geografisk repræsentativ spredning. Den er ligeledes repræsentativ i forhold til virksomhedsstørrelse. Der er en lille overvægt af fremstillingsvirksomheder, og en tilsvarende undervægt af bygge- og anlægsvirksomheder.

Virksomheder i undersøgelsen
Som vist på næste side havde 46 pct. af de virksomheder, der deltog i undersøgelsen, en omsætning mellem 15 og 75 millioner kroner i det seneste regnskabsår. 29 pct. havde en omsætning på 75-375 millioner kroner. Knap 15 pct. omsatte for mindre end 15 millioner kroner og 10 pct. for mere end 375 millioner kroner. En lille andel på 4 pct. har ikke angivet deres omsætning.

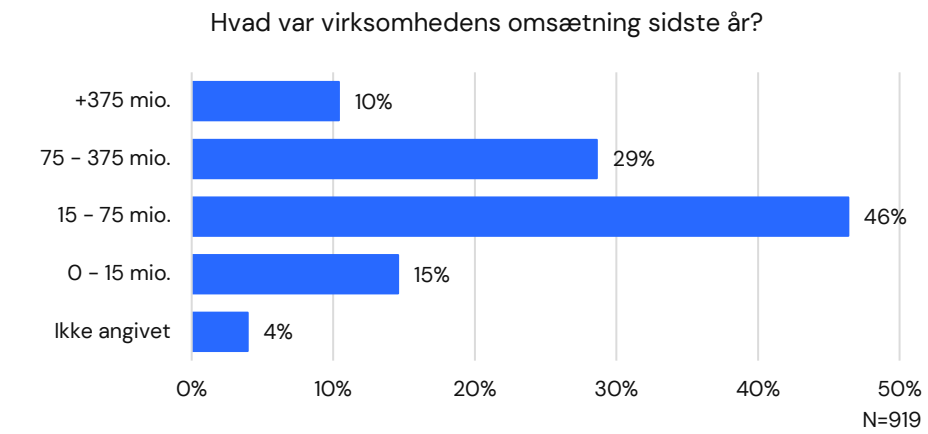
Fremstillingsvirksomheder udgør en betydelig del af undersøgelsen, med hele 50 pct. af virksomhederne. Bygge- og anlægsbranchen udgør 32 pct. af virksomhederne, mens Transport & godshåndtering udgør 11 pct. og Information & Kommunikation 6 pct. . Der er kun seks virksomheder fra råstofudvinding med i undersøgelsen, hvilket gør den til den mindste branche.

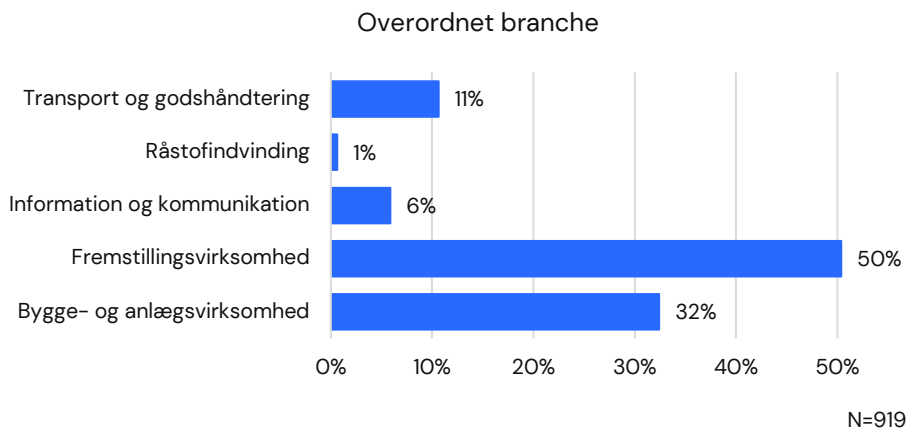
Blot 10 pct. af virksomhederne i undersøgelsen har al IT-drift, herunder hjemmesider og økonomisystemer, håndteret internt. Det er således typisk at outsource disse typer opgaver til eksterne leverandører.

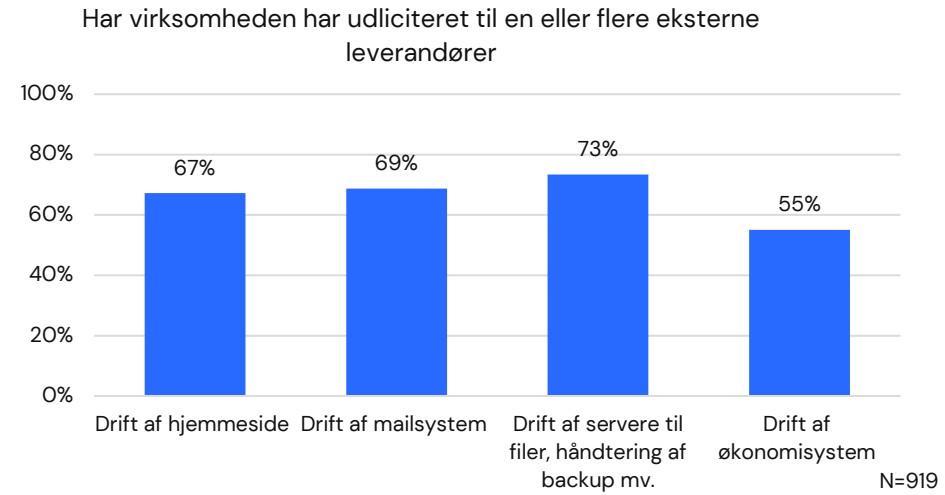
Hovedparten af virksomhederne i undersøgelsen har 1-2 medarbejdere dedikeret til IT-drift (41 pct.). Dog er der også en betydelig andel (30 pct.), der slet ikke har medarbejdere dedikeret til opgaven.

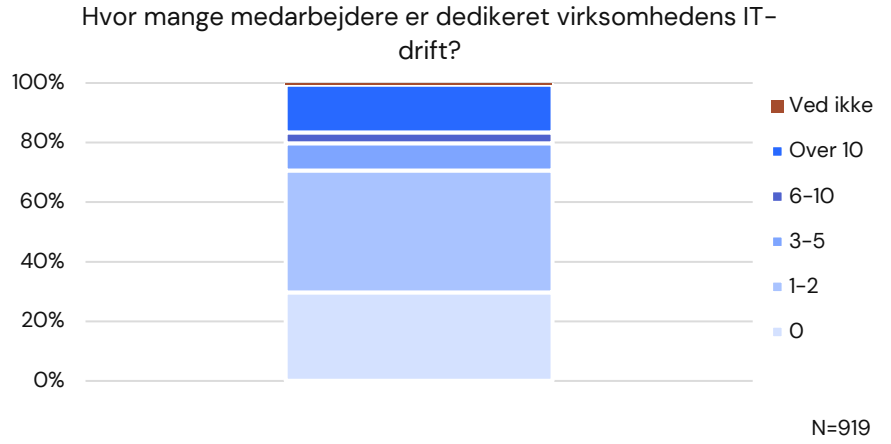
Virksomhederne i undersøgelsen

Figur 22: Beskrivende statistik om virksomhederne i undersøgelsen









Note: 10 PCT. af SMV'er i undersøgelsen har alt inhouse

Om ændring i svarkategorier inden for konkurrencefordele

I årets undersøgelse (2023) oplever hele 72 pct. af SMV'erne én eller flere fordele ved de cybersikkerhedstiltag, de har implementeret. Det er en betydelig stigning i forhold til 2022, hvor 56 pct. rapporterede at have oplevet konkurrencefordele.

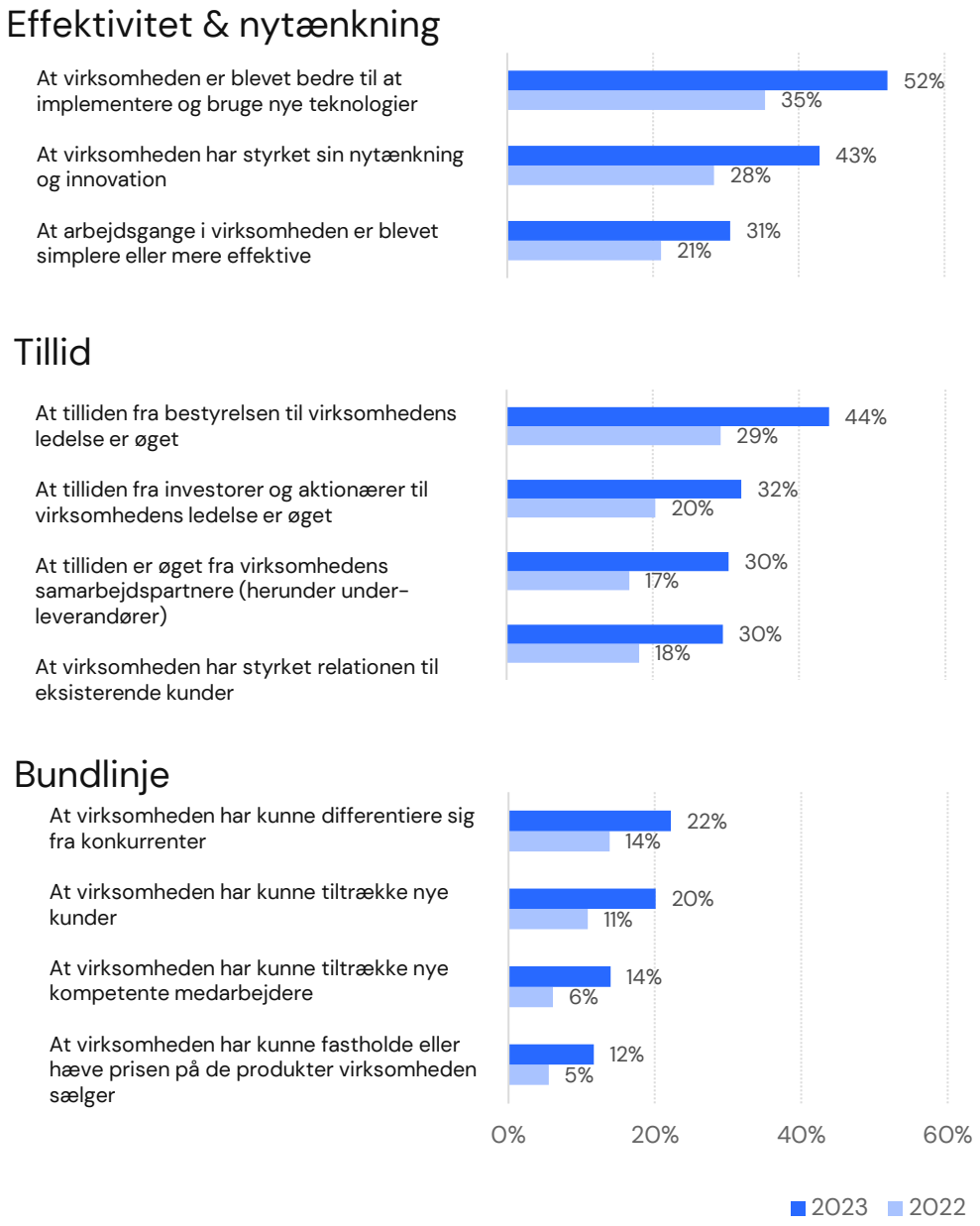
Det er vigtigt at bemærke, at stigningen delvis kan tilskrives ændringer i svarkategorierne i undersøgelsen. Fra 2022 til 2023 har vi foretaget mindre justeringer i svarkategorierne til spørgsmål om oplevede konkurrencefordele.

I 2022 omfattede svarkategorierne: 1) helt enig, 2) delvist enig, 3) hverken enig eller uenig, 4) delvist uenig, 5) helt uenig og 6) ved ikke.

Vi gennemførte en undersøgelse blandt de virksomheder, der i 2022 svarede "hverken enig eller uenig", ved hjælp af interviews. Resultaterne indikerede, at kategorien oftest blev brugt som en "ved ikke"-kategori eller som en måde at undlade at tage stilling til spørgsmålet. Af denne grund blev kategorien ændret i spørgeskemaet for 2023, så respondenterne tvinges til at erklære sig enten enige eller uenige, eller tage stilling til om de ikke ved det: 1) helt enig, 2) delvist enig, 3) delvist uenig, 4) helt uenig og 5) ved ikke.

Denne ændring kan have bidraget til en vis del af stigningen i andelen af virksomheder, der rapporterer konkurrencefordele.

Figur 23: Virksomheder, der er enige eller meget enige i, at virksomhedens indsatser for at styrke cybersikkerhed de seneste 2 år har bidraget til:



Kvalitative interviews

Formål

Vi har lavet kvalitative interviews med det formål at berige resultaterne fra spørgeskemaundersøgelsen, og give dybere indblik i sammenhængen mellem cybersikkerhed og konkurrencefordele. Yderligere belyser interviewene forestillinger, holdninger og motiver hos SMV'erne, som er for komplekst til at fange alene ved hjælp af et spørgeskema.

Rekruttering

Interviewdeltagere er udvalgt blandt de virksomheder, der har deltaget i spørgeskemaundersøgelsen. Som udvælgelseskriterie gjaldt at virksomheden:

1. Har implementeret mere end 7 cybersikkerhedstiltag
2. Har oplevet mere end 5 konkurrencefordele som resultat af deres investeringer i cybersikkerhed.
3. Havde en omsætning på mere end 15 millioner kroner i det seneste regnskabsår.

Virksomhederne er således udvalgt på baggrund af at være "best cases", der har opnået en stærk cybersikkerhedspraksis. De kan derfor virke som konkret inspiration for andre.

Der er desuden søgt repræsentation af forskellige brancher blandt de deltagende virksomheder.

Gennemførelse

Interviews er gennemført som semistrukturerede interviews, hvilket vil sige at de følger en overordnet interviewguide med en række spørgsmål, men at rækkefølgen kan variere, ligesom at der er mulighed for at stille uddybende spørgsmål undervejs. Det giver en interviewform, der tilpasses den enkelte virksomheds fokus inden for emnet.

Interviews har varet mellem 30 – 60 minutter.

Interviewpersoner i undersøgelsen

Interviewpersoner i undersøgelsen

Vi har i alt gennemført syv interviews med personer i den øverste ledelse af SMV'er i undersøgelsen. Interviewpersonerne har stillinger som administrerende direktører/CEO's, direktør, CFO og IT-chef. Vi har valgt den øverste ledelse, fordi vi forventede at de dermed både har indsigt i virksomhedens arbejde med cybersikkerhed og også den strategiske og ledelsesmæssige indsigt, hvorved de kan pege på de konkurrencemæssige fordele deraf.

Vi har rekrutteret interviewpersoner fra de tre største brancher (Fremstilling, Bygge & anlæg, Information & Kommunikation), mens det ikke har været muligt at rekruttere fra de to mindste brancher: Transport & godshåndtering og Råstofudvinding.

Til højre kan du se et overblik over de syv interviewpersoner i undersøgelsen. Én interviewperson har valgt at være med anonymt.

B.E. Installationer

Brian Bryrup, Ejer og CEO

Bygge- og anlægsvirksomhed

120 ansatte

EWII Fibernet A/S

Claus Møller, direktør

Information og kommunikation

600+ ansatte

Saxe Hansen

Mikkel Enevoldsen, CEO

Fremstillingsvirksomhed

65 ansatte

Telenabler

Jens Fricke, Direktør

Information og kommunikation

15 ansatte

Uggerly

Michael Seerup, Administrationschef

Bygge- og anlægsvirksomhed

322 ansatte

Vestfrost

Jannie Tholstrup, CFO

Fremstillingsvirksomhed

201 ansatte

Anonym virksomhed

Anonym interviewperson

Fremstillingsvirksomhed

Bortfaldsanalyse

Analyse & Tal har på vegne af Industriens Fond udsendt spørgeskema ud via e-mail til en samlet gruppe på 7.919 danske små og mellemstore virksomheder, som er registreret i Industriens Fonds database baseret på CVR-numre.

Knap 12 pct. af disse virksomheder har besvaret spørgeskemaet, hvilket resulterer i et analyseudvalg bestående af 919 virksomheder. Det er vigtigt at bemærke, at spørgeskemaerne primært er blevet besvaret af virksomhedsejere og direktører/CEOs, hvilket er en målgruppe, der normalt er svær at få kontakt til. I 2022 deltog 729 SMV'er i undersøgelsen, mens vi i årets undersøgelse er helt oppe på at 919 SMV'er deltager – det er 190 flere stemmer end sidste år. Derfor er det særdeles tilfredsstillende, at vi har opnået en svarprocent på 12 pct.

For at kunne sige noget generelt om SMV'er, skal analyseudvalget være repræsentativt. Og det er stort set lykkes. På den næste side er det illustreret at analyseudvalget både er repræsentativt på geografi og størrelse, mens undersøgelsen har lidt fra Fremstilling og lidt færre fra Bygge & anlæg. Der er også beskrivende statistik af, hvem der har deltaget i undersøgelsen.

7.919

virksomheder er blevet inviteret til undersøgelsen

919

virksomheder har i alt besvaret spørgeskemaet

12%

Er svarprocent for udsendte spørgeskema.

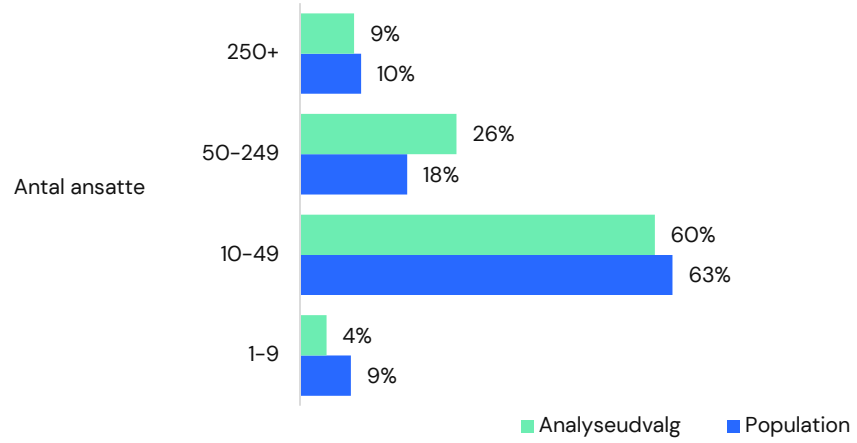
Alt i alt er undersøgelsen tæt på repræsentativ, hvor den største forskel mellem undersøgelsens besvarelser (analyseudvalget) og den samlede population er at der er lidt flere Fremstillingsvirksomheder og lidt færre fra Bygge & anlæg med i undersøgelsen.

Til højre på figur 24 kan man se, at repræsentationen i analyseudvalget afspejler populationen, hvad angår antal ansatte. Der er lidt flere mikrovirksomheder med i undersøgelsen, og lidt færre i kategorien med 50-249 ansatte. Forskellene er dog små.

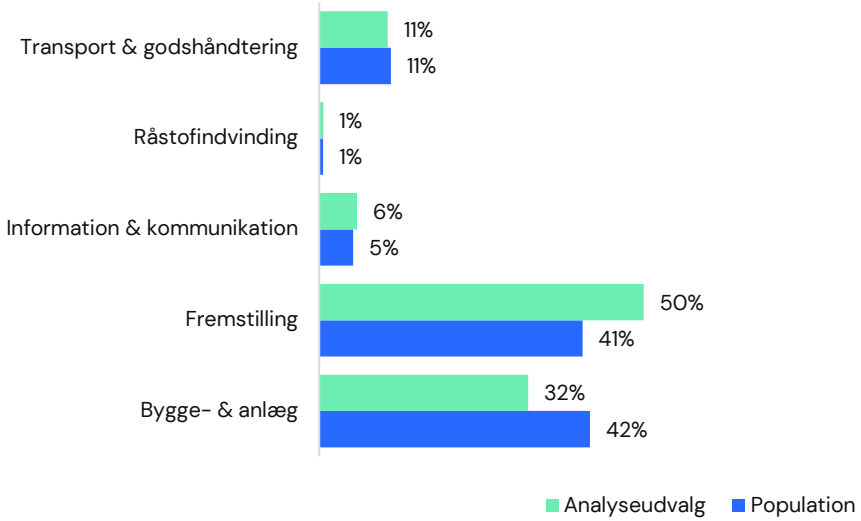
På figur 25 nederst til højre kan man se, at der er en mindre underrepræsentation af bygge og anlægsvirksomheder og en mindre overrepræsentation af Fremstillingsvirksomheder. Da fremstillingsvirksomhederne udgør den største branche, ville de også i en perfekt repræsentativ undersøgelse have stor vægt. Vi vurderer at den ekstra vægt, de byder ind med, er tilforladelig, og at repræsentativt billede af brancherne.

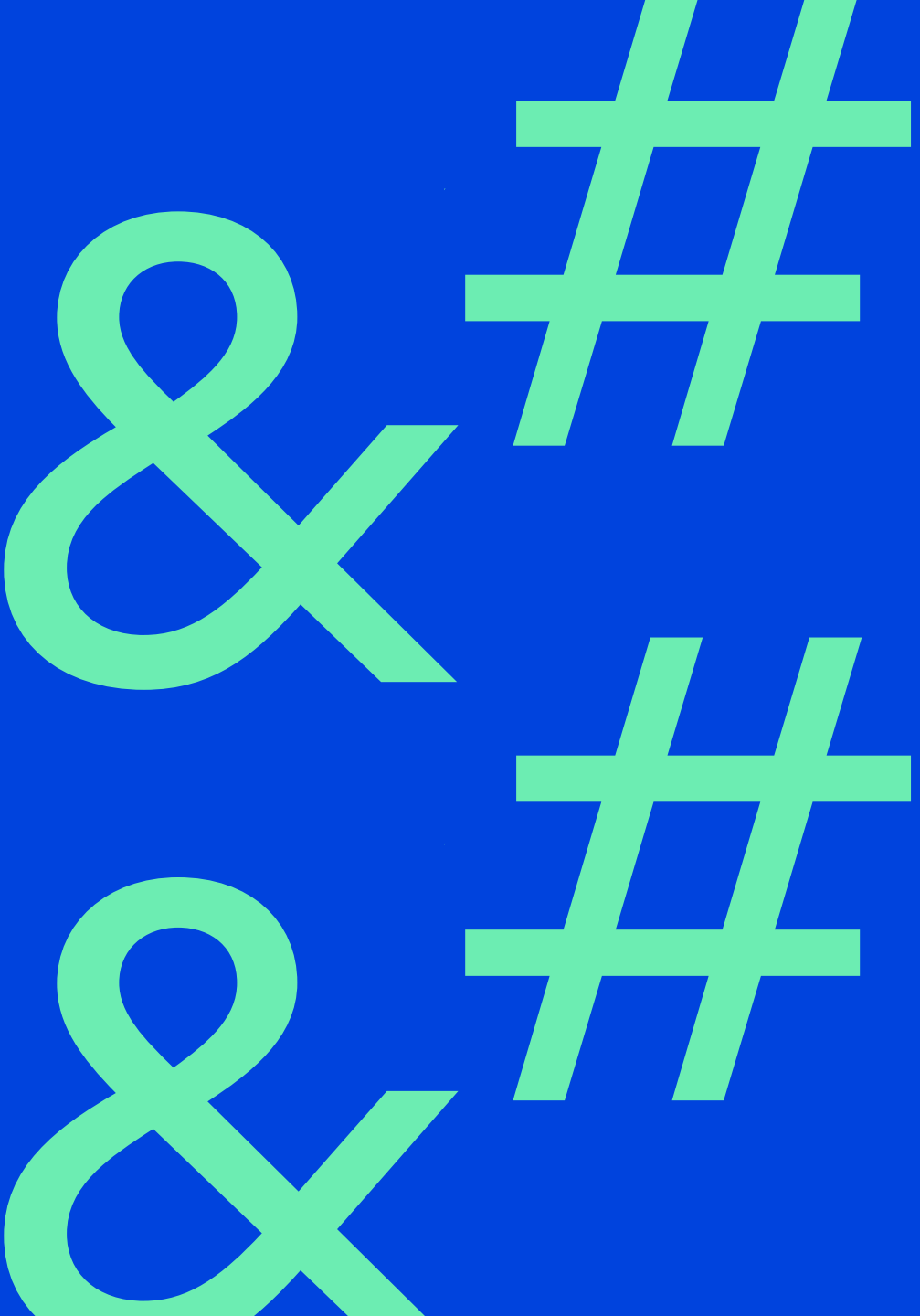
Geografisk er analyseudvalget også tilfredsstillende (ikke vist). Alle kommuner med undtagelse af Læsø, Samsø, Ærø og Vallensbæk er repræsenteret i undersøgelsen. Blandt de fire største kommuner - det vil sige København, Aarhus, Odense og Aalborg - er der en meget lille underrepræsentation af SMV'er fra Aarhus og København på henholdsvis 0,3 procentpoint og 1 procentpoint, . Odense kommune er ligeligt repræsenteret, mens Aalborg er lidt overrepræsenteret med 0,5 procentpoint. Der er tale om små forskelle, og vi vurderer at undersøgelsen er repræsentativ på geografi.

Figur 24: SMV'er fordelt på antal ansatte i hhv. populationen og analyseudvalget



Figur 25: SMV'er fordelt på brancher i hhv. populationen og analyseudvalget





Analyse & Tal

Analyse & Tal er et kooperativt analysebureau med kontorer i København, Aarhus og Oslo. Vi tæller dét, der er svært og kombinerer klassiske metoder med nye digitale.

Analyse & Tal har eksisteret siden 2014 og tæller i dag 30 medarbejdere. Vi er sociologer, statistikere, økonomer, programmører, kommunikatører og designere, og vi arbejder tværfagligt med vores projekter, blandt andet indenfor desinformation, online had og aktivisme, erhvervsanalyser og evalueringer af alt fra sociale indsatser til turismens klimaaftryk.

Analyse & Tals drøm er at skabe et mere demokratisk og lige samfund. Derfor har vi valgt at organisere os som et medarbejderejet kooperativ. Vi er stolte af at investere vores overskud i udviklingen af nye metoder, projekter og i demokratiseringen af vores samfund som helhed.