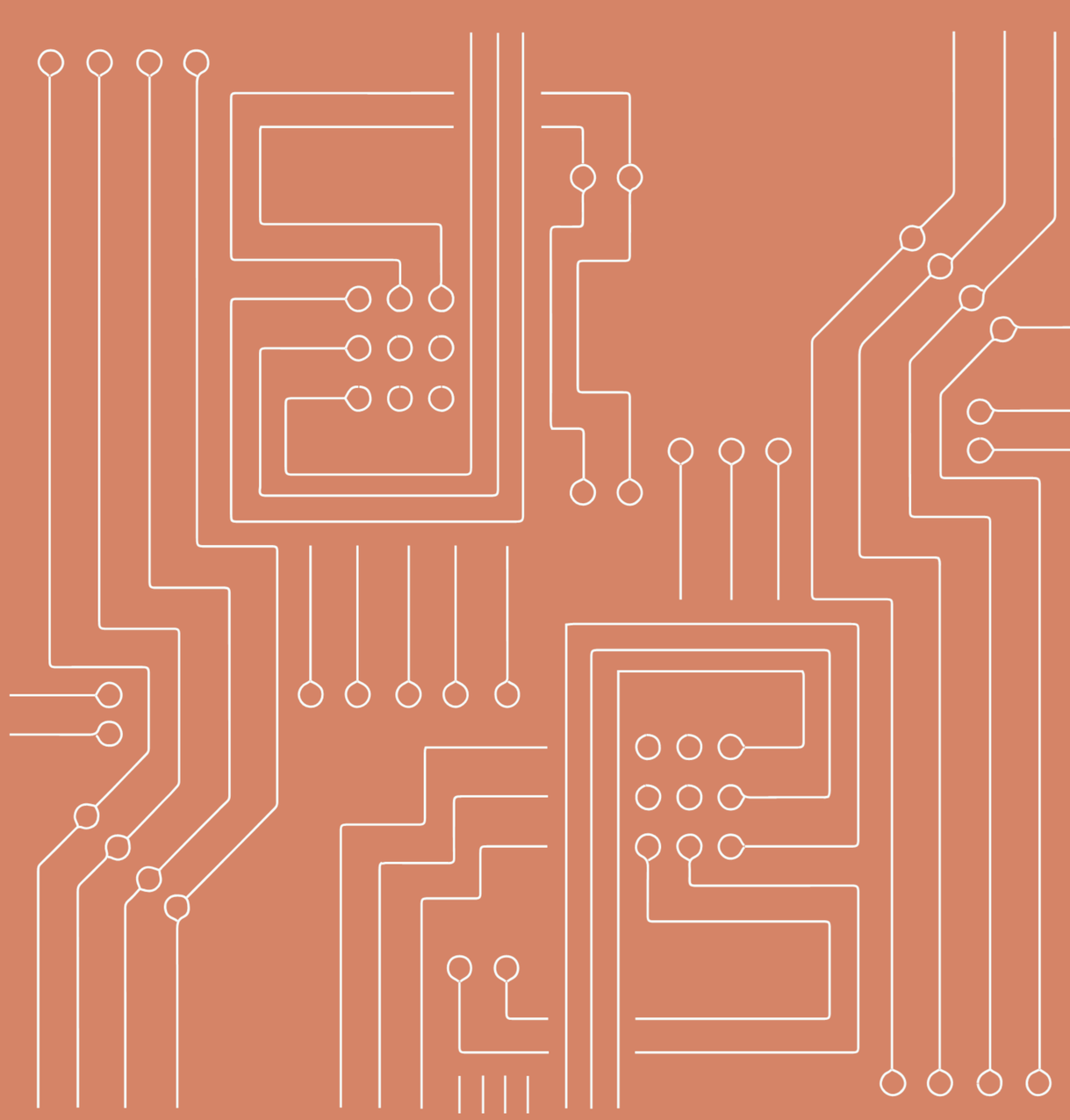
Cybersikkerhed & konkurrenceevne blandt danske SMVer 2022



Rapport udarbejdet for Industriens Fond af Analyse & Tal F.M.B.A.
med sparring fra Grant Thornton

Analyse & Tal – www.ogtal.dk – 15.11.2022

Indhold

Indledning

Presset på små og mellemstore virksomheders cybersikkerhed bliver større og større disse år. I Erhvervsstyrelsens årlige publikation "Digital sikkerhed i danske SMVere" står det klart, at omkring halvdelen af danske SMVere har et for lavt sikkerhedsniveau, og Center for cybersikkerhed vurderer at truslen for cyberkriminalitet er 'Meget høj' i Danmark. Der er altså behov for øget cybersikkerhed i de danske virksomheder.

Vores undersøgelse har *ikke* fokus på at vurdere, hvor sikrede SMVerne er mod cyberangreb, men den viser, at langt de fleste SMVere i Danmark (92 pct.) inden for de seneste to år, har indført én eller flere former for cybersikkerhedstiltag for at imødekomme truslen om cyberkriminalitet. Det er lige fra automatisk backup til beredskabsplaner og risikovurderinger og det gør de selvfølgelig for at sikre deres virksomhed mod angreb. Der er dog stor variation i hvor mange tiltag virksomhederne har indført.

I denne undersøgelse går vi skridtet videre fra virksomhedens sikkerhed til at undersøge om cybersikkerhedstiltag også fører til konkurrencefordele for virksomheden. Og det korte svar er, at det gør de. Den gennemgående konklusion er at flere cybersikkerhedstiltag fører til flere konkurrence-fordele.

Resultaterne i vores undersøgelse er de første af en række årlige målinger. Resultaterne indgår i et såkaldt cyberbarometer – cyberbarometer.dk - der opgør status og følger udviklingen mellem cybersikkerhed og konkurrencekraft over tid. Cyberbarometeret skal ikke blot måle, men også skubbe til udviklingen. I Cyberbarometerets univers kan man finde opdateret viden om cybersikkerhed og konkurrenceevne i Danmark.

Forud for denne undersøgelse ligger et større arbejde med at kortlægge den eksisterende viden om koblingen mellem investeringer i cybresikkerhed og konkurrenceevne. Her stod det klart, at der manglede empirisk belæg for denne sammenhæng. Ud fra vores viden er denne undersøgelse den første af sin art, der undersøger netop denne sammenhæng på baggrund af en bred dataindsamling blandt SMVer i hele 'produktionsdanmark' - inden for brancherne: Fremstilling, Bygge & anlæg, Transport & godshåndtering, Information & kommunikation og Råstofudvinding i alt 7.370 virksomheder.

De har alle modtaget en spørgeskemaundersøgelse og 729 har valgt at svare. SMVere er en broget flok af virksomheder og er notorisk svære at få fat i. Med øje for at svarene hovedsageligt kommer fra ledelsen, er en

10 pct. svarprocent et meget tilfredsstillende analyseudvalg. Og vigtigere end størrelse på analyseudvalget, er at den er repræsentativ for SMVerne både på branche, størrelse og geografi.

Som opfølgning på resultaterne i spørgeskemaundersøgelsen har vi interviewet CEOs i fire forskellige virksomheder: TimeLog, DEIF, Inno Aps og Varde Laks. Alle fire virksomheder har det til fælles, at de har indført mange cybersikkerhedstiltag og oplevet flere konkurrencefordele på baggrund af tiltagene. På trods af at de fire virksomheder er vidt forskellige, både i størrelse, brancher og deres produkter, bekræfter samtalerne med de fire CEOs, at cybersikkerhedstiltag er en nødvendighed for at overleve som virksomhed. TimeLog og DEIF har, i kraft af deres produkter, en dyb indsigt i IT og derfor også italesætter cybersikkerhed direkte, men det var spændende at høre hvordan alle fire virksomheder fik ekstern hjælp til at opnå en bedre sikkerhed. Interviewene bekræftede at flere cybersikkerhedstiltag fører til flere konkurrencefordele, eller ligefrem er en nødvendighed for at være på markedet.

Undersøgelsen er udført af analysebureauet Analyse & Tal med sparring fra Grant Thornton på vegne af Industriens Fond.

Rigtig god fornøjelse!

&#

I undersøgelsen er små og mellemstore virksomheder – SMVer - defineret ved at have færre end 600 ansatte. De fleste virksomheder har mellem 10-100 ansatte, og kun 10 virksomheder har flere end 300 ansatte.

Hovedindsigt #1

Jo flere cybersikkerhedstiltag, des flere konkurrencefordele

Langt de fleste virksomheder i undersøgelsen (92 pct.) har indført ét eller flere cybersikkerhedstiltag. Når vi sammenholder *antallet* af de tiltag, som vi har spurgt til, finder vi en klar positiv sammenhæng mellem antal tiltag og oplevelsen af én eller flere konkurrencefordele. Cybersikkerhedstiltag spænder mellem alt fra at installere anti-malware til at oprette interne processer for sikkerhed og at lave risikoanalyser.

Jo flere tiltag SMVerne indfører, des flere konkurrencefordele oplever de. Hvor kun 20 pct. af virksomheder med færrest tiltag (1-3 tiltag) oplever én eller flere konkurrencefordele, oplever hele 87 pct. af virksomheder med flest tiltag (13-15 tiltag) én eller flere konkurrencefordele.

De kvalitative interviews peger netop på at flere tiltag virkelig betyder flere fordele, og at der spreder sig en forståelse for cybersikkerhed blandt medarbejderne, som går ud over det enkelte tiltag. Det bliver en tankegang om at mindske risiko og sikre gode procedurer generelt. I virksomheden TimeLog beskriver CEO Per Henrik Nielsen at cybersikkerhed er blevet en del af virksomhedens DNA.

“More is more”

Hovedindsigt #2

Cybersikkerhed fører til konkurrencefordele i alle brancher

Man kunne forestille sig, at det udelukkende var virksomheder som fx sælger software eller IT-produkter, der oplevede en sammenhæng mellem cybersikkerhedstiltag og konkurrencefordele, men det forholder sig langt fra sådan. Den positive sammenhæng gør sig gældende for alle fire brancher i undersøgelsen.

Selvom trenden er stigende med antallet af tiltag i alle brancher, er der mindre forskelle mellem brancher. De SMVer, der har indført flest tiltag (11-15), oplever flest fordele i alle brancher - hele 94 pct. i Information & kommunikation, 84 pct. i Fremstilling, 79 pct. i Transport & godshåndtering og 75 pct. i Bygge & anlæg.

Virksomheder i Information & kommunikation ser ud til at opleve fordele allerede ved få tiltag (1-5), hvor 50 pct. oplever én eller flere konkurrencefordele, mens virksomheder i Transport & godshåndtering starter lavt, hvor kun 17 pct. oplever fordele ved 1-5 tiltag.

Der er mange veje fra cybersikkerhed til konkurrencefordele på tværs af brancher. I de kvalitative interviews peger CEO Per Henrik Nielsen i TimeLog i Information & kommunikation på at cybersikkerhed i deres produkt og interne processer er en nødvendighed for at være på markedet, mens CEO Claus Jørgensen fra Inno Aps i Bygge & anlægsbranchen i højere grad oplever konkurrencefordel ved at have styr på ordrer, fakturaer og sikring mod malware.

Hovedindsigt #3

Variation i tiltag påvirker også konkurrenceevnen positivt

For at undersøge hvilke tiltag, der har størst impact, har vi inddelt cybersikkerhedstiltag i tre former: Teknik, Forankring & styring og Rutiner & træning. De fleste SMVer har indført flere forskellige former for cybersikkerhedstiltag og 68 pct. har tiltag indenfor alle tre former. Virksomheder, der har indført alle tre typer af tiltag, oplever øgede konkurrencefordele. For at få et større indblik i hvilke kategorier af fordele de oplever, har vi inddelt konkurrencefordele i Effektivitet & nytænkning, Tillid og Bundlinje. Virksomheder, der har indført alle tre former for tiltag, oplever også flest konkurrencefordele inden for alle tre kategorier af konkurrencefordele.

Det er altså både *antallet* og *forskellige former* for cybersikkerhedstiltag, der bidrager til øgede konkurrencefordele og det er vel at mærke konkurrencefordele inden for alle kategorier. Det peger på, at ikke bare mange tiltag, men også variation i tiltag bidrager til konkurrencefordele.

Alle fire virksomheder, som vi har interviewet, bruger eksterne partnere til at hjælpe med deres cybersikkerhed i erkendelsen af, at de ikke selv har mulighed for at holde sig opdateret med de nyeste procedurer og sikkerhedsforanstaltninger. Variationen i tiltag er for stor til at de selv kan varetage opgaven.

"More is indeed more"

Nøglebegreber i rapporten

Hvad er cybersikkerhed?

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

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

Hvad er konkurrencefordele?

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

Konkurrencefordele spænder over Effektivitet & nytænkning (fx bedre implementering, simplere arbejdsgange, styrket innovation), til Tillid (fx øget tillid fra bestyrelsen, kunder, investorer og aktionærer), og helt til fordele der rammer Bundlinjen (fx at virksomheden har kunne tiltrække nye kunder).

Cybersikkerhed & konkurrencefordele

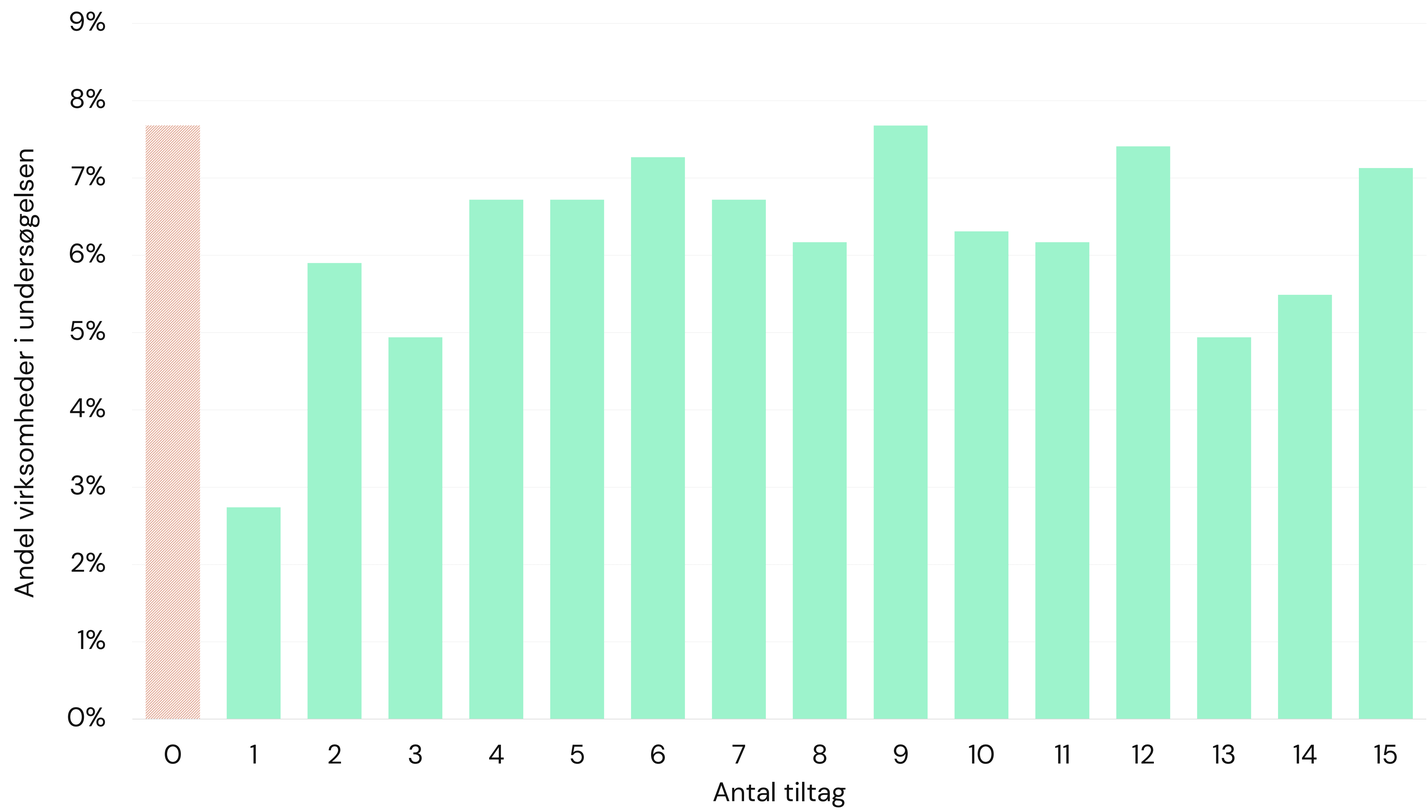
Jo flere cybersikkerhedstiltag, des flere oplever en konkurrencefordel

SMVerne har svaret på om de inden for en 2-årig periode har lavet eller opdateret 15 konkrete cybersikkerhedstiltag.

Der er kun knap 8 pct. af SMVerne i undersøgelsen, der *ikke* har indført nogen former for cybersikkerhedstiltag (den skraverede kolonne).

Der er dog stor variation i, hvor mange tiltag de resterende virksomheder har indført. Som man kan se på figur 1, er der en jævn fordeling af alt fra ét tiltag til alle 15 tiltag, vi har spurgt til. Tiltagene kan være alt fra at have løbende opdateringer af virksomhedens software til opkvalificering af ansatte i IT-sikkerhed (se side 24 for fuld liste og hvilke tiltag, der er mest udbredte).

Figur 1: Fordeling af antal cybersikkerhedstiltag blandt virksomheder i undersøgelsen



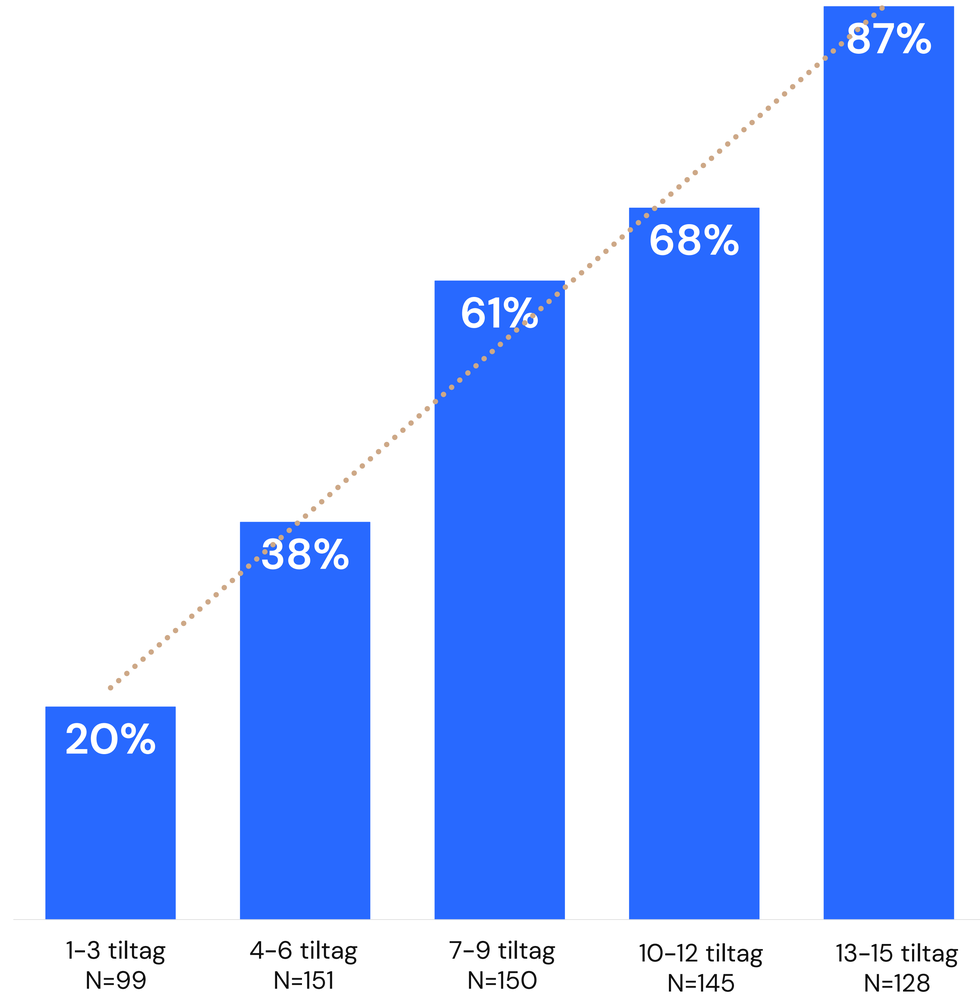
N= 729

SMVerne har også svaret på om deres investeringer i cybersikkerhedstiltag har medført 11 konkrete konkurrencefordele. Figur 2 viser andelen af virksomheder i undersøgelsen, der har oplevet én eller flere konkurrencefordele inddelt efter, hvor mange tiltag de har foretaget.

Ud fra figur 2 ser det ud til, at man som SMV blot skal give sig i kast med at indføre tiltag. Jo flere tiltag, des flere oplever fordele. Der er en tydelig sammenhæng mellem, hvor mange cybersikkerhedstiltag, virksomheden har indført, og hvorvidt de oplever én eller flere konkurrencefordele ved tiltagene. Som man kan se på figur 2 oplever kun 20 pct. af SMVer, der har indført 1-3 tiltag, konkurrencefordele, mens det for SMVer der har indført 13-15 tiltag, er hele 87 pct. der oplever én eller flere konkurrencefordele af tiltagene.

Der findes ud fra vores viden ingen empiriske studier af SMVer i Danmark, der påviser denne sammenhæng. Som man kan se på figur 2, er sammenhængen tæt på lineær. Man kunne ellers forestille sig at virksomhederne skulle indføre et vist niveau af tiltag for at opleve fordelene, men det lader ikke til at være tilfældet. Hver gang der indføres flere tiltag stiger oplevelsen af at opnå konkurrencefordele.

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



N= 673 (De 56 virksomheder som *ikke* har indført tiltag, er ikke blevet spurgt til fordele)

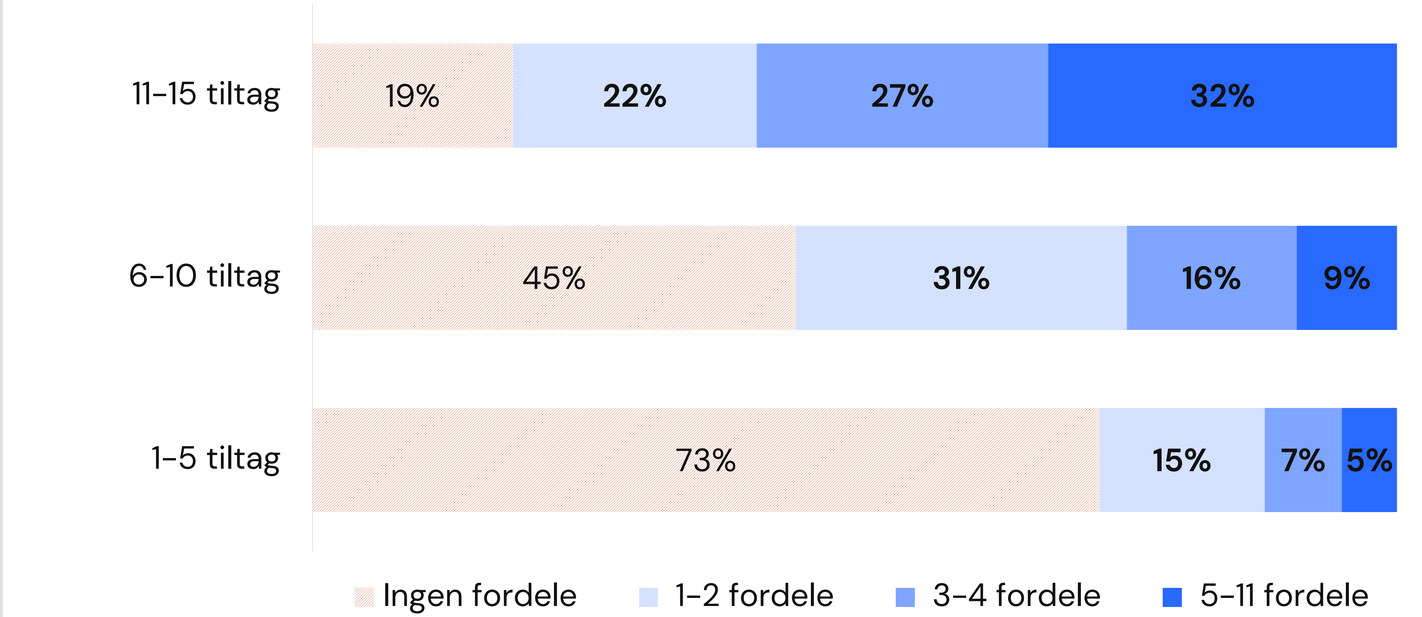
Jo flere cybersikkerhedstiltag, des flere konkurrencefordele

Det er ikke blot, at flere oplever en konkurrencefordel, des flere cybersikkerhedstiltag, de indfører. Virksomhederne oplever også *flere* konkurrencefordele. Som man kan se på figur 3 er der også en tydelig sammenhæng mellem antallet af tiltag og *antallet* af konkurrencefordele.

Blandt virksomheder med færrest tiltag (1-5 tiltag) oplever kun 5 pct. mange konkurrencefordele (5-11 fordele), mens hele 32 pct. af virksomheder med flest tiltag oplever mange konkurrencefordele.

At SMVer med flere tiltag også oplever flere konkurrencefordele understøtter, at man som SMV succesfuldt kan give sig i kast med at indføre tiltag, eller som virksomheden TimeLog finde partnere, der kan hjælpe med at indføre tiltag.

Figur 3: Oplevede konkurrencefordele fordelt på hvor mange cybersikkerheds-tiltag firmaet har indført



N=673

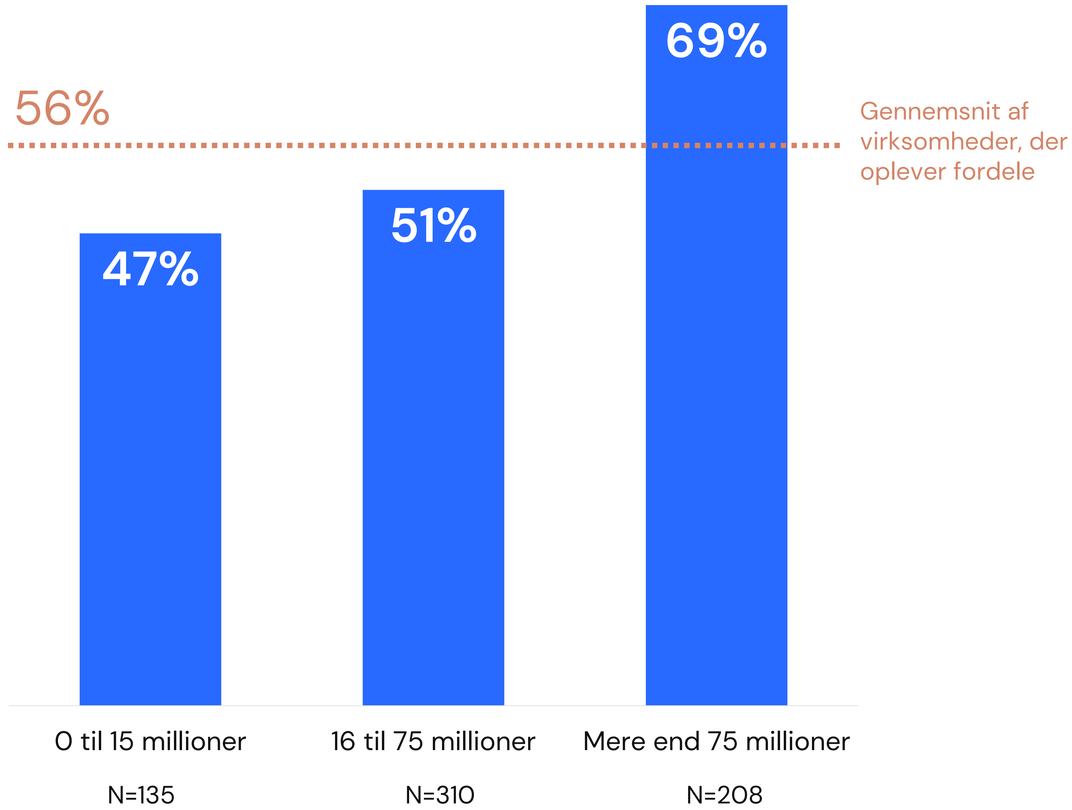
SMVer i undersøgelsen består både af helt små virksomheder med få ansatte og lille omsætning, og af de mellemstore virksomheder med en omsætning på mere end 75 mio. kr.

Der er 56 pct., der oplever én eller flere konkurrencefordele af deres cybersikkerhedstiltag. Figur 4 viser, at det særligt er de større SMVer der oplever minimum én konkurrencefordel.

Det er også de større SMVer, der har indført flest tiltag (ikke vist på figuren). Selvom en virksomhed er lille, er det ofte de samme krav til sikkerhed som større virksomheder. Flere små virksomheder beretter om at de finder opgaven overvældende, eller at de ser cybersikkerhed som noget sekundært for virksomhedens drift, fremfor noget primært.

"Det har indtil nu ikke været et emne som vore kunder har bragt på bane overhovedet, selvom to af vore største kunder har været udsat for ransomware" [CEO, SMV i undersøgelsen]

Figur 4: Andel virksomheder der oplever fordele – fordelt på omsætning



N= 653 (blandt virksomheder med tiltag, er der 20 virksomheder, der ikke ønsker at opgive deres omsætning)

2022

Cases på danske SMVers arbejde med cybersikkerhed

For at få en bedre forståelse af sammenhængen mellem cybersikkerhed og konkurrencefordele har vi interviewet fire virksomheder. Alle virksomheder har både indført mange tiltag og også oplevet konkurrencefordele. Virksomhederne TimeLog og DEIF har arbejdet direkte med cybersikkerhed i flere år. Cybersikkerhed for dem er en betingelse for at være på markedet, og de er opmærksomme på, hvordan cybersikkerhed fører til konkurrence-fordele.

Virksomhederne Inno Aps og Varde Laks arbejder også med cybersikkerhed, men mere indirekte, med et større fokus på at optimere virksomhedens drift og processer end decideret at sikre virksomheden mod angreb, men derigennem har de fået styrket deres processer også i en cybersikkerhedsforstand.

Fælles for de fire virksomheder er, at sikring af deres drift har medført cybersikkerhed og bedre processer i deres virksomheder – også bedre and de havde turde håbe på.

Cybersikkerhed blev en del af virksomhedens DNA

Case: TimeLog

Branche: Information og kommunikation; Udgivelse af computerspil og anden software; Anden udgivelse af software
Antal ansatte: 21-50
Omsætning:16-75 millioner

"Hvis ikke du har indstillingen, at det er et spørgsmål om hvornår du bliver kompromitteret og ikke om du gør, så er man arrogant" [TimeLog, lille SMV i Information & kommunikation, CEO Per Henrik Nielsen]

I interview med CEO Per Henrik Nielsen hos TimeLog fortæller han, at cybersikkerhedstiltag har ført til flere konkurrencefordele. En af fordelene har været et godt arbejdsmiljø, hvor de interne kurser i cybersikkerhed har skabt en følelse af community – en samværsfølelse. Medarbejderne er også stolte af, at virksomheden er dygtig til at beskytte dem og kunderne.

At de har styr på deres sikkerhed har også ført til at de får lov at byde på et internationalt marked. Per Henrik Nielsen fortæller, at deres tiltag handler om ordentlighed i virksomhedens DNA. De vil ikke dele det, som ikke skal deles. Det er en pligt at beskytte dem selv, medarbejderne og kunderne.

Per Henrik Nielsen fortæller, at de interne processer har fået en opstramning, som har ført til en modenhed i eget økosystem. Det har overrasket Per Henrik Nielsen, hvordan hele økosystemet i virksomhedens relationer har været med i udviklingen af cybersikkerhed, lige fra ildsjæle blandt medarbejderne, til leverandører, større virksomheder, konkurrenter og til kunder. Sikkerhed er simpelthen blevet en del af dialogen med kundebasen, og dialogen virker begge veje.

"Det er altså ikke noget, som vi bare laver for marketing. Det bliver også brugt i marketing og til salg, men det bliver lavet, fordi vi mener seriøst, at hvis ikke vi kan det her, så er det simpelthen ikke godt nok" [CEO Per Henrik Nielsen]

Når Per Henrik Nielsen skal pege på de mest betydningsfulde sammenhænge af deres øgede cybersikkerhedsindsats, er det at der skal være transparens i, hvorfor tiltagene bliver indført. Og så har det også resulteret i en større stolthed hos frontpersonalet, når de får henvendelser fra kunder. Han fortæller om en sag, hvor de på blot 20 minutter kunne rette en fejl i systemet. På trods af fejlen viste deres hurtige reaktionstid, at de havde styr på sikkerheden, og fejlen blev vendt til en konkurrencemæssig fordel, fordi de kunne reagere så hurtigt.

Hvis Per Henrik Nielsen skulle starte forfra i dag, ville virksomheden sætte flere tiltag i gang, mens de udviklede. Man bliver aldrig færdig med cybersikkerhed. Derfor kan man lige så godt få gode processer med ind fra starten.

Fra leverandør til partner for deres kunder

Case: DEIF
Branche: Fremstilling; Fremstilling af andet elektronisk udstyr; Fremstilling af udstyr til måling, afprøvning, navigation og kontrol
Medarbejdere: 101-590
Omsætning: Mere end 375 millioner

"Partnerskaber er per definition mere langsigtede"

[DEIF, mellemstor SMV i Fremstilling, CEO Christian Nielsen]

Cyberangreb er modsat energikriser og recessioner noget nyt for kunderne, mener CEO Christian Nielsen. Han oplever, at kunderne er gået fra at tale om pris til at tale om sikkerhed, hvor de efterspørger mere fra produktet og er parate til at betale for det, og her er det vigtigt, at man som virksomhed følger med. Christian Nielsen fortæller, at cybersikkerhed ses og anvendes som en af parametrene til at løfte virksomheden ud af priskonkurrence. Det er et konkurrenceparameter i sig selv. For tre år siden landede de et stort internationalt projekt, hvor de alene blev valgt på baggrund af deres cybersikkerhed. Det var her det gik op for Christian Nielsen, at cybersikkerhed kunne bruges til at differentiere sig fra andre virksomheder.

"Det her *[at cybersikkerhed er på plads]* er licens to play."

[CEO Christian Nielsen]

Siden er der opstået et tættere samspil mellem virksomheden og kunderne, hvor der er feedback begge veje. Dette har åbnet døren for partnerskaber med kunderne, frem for et egentligt kunde/leverandørforhold.

Christian Nielsen har fokuseret meget på at få hele organisationen med fra medarbejderne, der arbejder på produktet, til at få bestyrelsen til at se vigtigheden af cybersikkerhed.

"Vi har har jo ligefrem haft informationsmøder, hvor man normalt starter med økonomital, så har vi startet med cybersecurity."

[CEO Christian Nielsen]

Han ser cybersikkerhed som et glimrende sted at vise bestyrelsen, at der er styr på virksomhedens drift – også før de selv spørger. Han ser det som sin pligt at få bestyrelsen med ombord, og få forklaret hvad konsekvenserne kan være ved et sikkerhedsbrud, simpelthen fordi risikoen er så stor. Så kan de også kan være med i arbejdet om risikovurderinger, og hvordan man minimerer de risici.

Hvordan arbejdes der eksternt og internt med cybersikkerhed?

Eksterne konsulenter hjælper med cybersikkerheden

CEO hos TimeLog Per Henrik Nielsen fandt, at man som mindre virksomhed ikke kan bære arbejdet med cybersikkerhed alene. Selvom virksomheden kan håndtere almindelige hændelser, kan de ikke nå at holde sig opdateret med, hvad der foregår på alle områder. Han fortæller, at virksomheden i begyndelsen ikke var klædt på til opgaven, når de fandt noget, som ikke stemte. De manglede overblik over, hvem der kunne hvad. Derfor valgte de nogle eksterne partnere. Heldigvis fandt de gode partnere til at hjælpe og de delte også deres viden med andre små og mellemstore virksomheder.

Per Henrik Nielsen har kigget på større virksomheder og kunne godt tænke sig, at mindre virksomheder kunne få samme hjælp til deres cybersikkerhed. Han foreslår et nationalt samarbejde blandt mindre virksomheder, så man hjælper hinanden med opgaven.

"Måske kunne danske SMVere ligefrem markedsføre cybersikkerhed i DK, ligesom Tyskland er kendt for kvalitet i biler"
[TimeLog, CEO Per Henrik Nielsen]

Hos DEIF fortæller CEO Christian Nielsen også, at de bruger mange konsulenter til at holde sig opdateret. Han fortæller, at de har haft et stort fokus på at holde medarbejderne opdaterede på cybersikkerhed.

Medarbejdere ser stadig cybersikkerhed som noget træls

"Det [cybersikkerhed] er stadig i den daglige tale en udfordring og en træls ting [for de fleste i virksomheden], end det er noget, som er godt, for man skulle jo dybest set være glad for det."
[DEIF, CEO Christian Nielsen]

Hos DEIF, er det i dag, tre år efter de første konkurrencefordele manifesterede sig, stadig primært CEO Christian Nielsen, der ser cybersikkerhed som noget entydigt godt for produkterne. Han er ikke i tvivl om, at fordelene er der og at de er større end antaget, men de kan først rigtigt ses i bakspejlet. For medarbejderne er cybersikkerhed stadig ofte en træls forhindring i deres daglige arbejde.

Ledelsen hos DEIF arbejder målrettet med at etablere en kultur hvor alle er med og hvor der er plads til fejl. Som Christian Nielsen beretter, kan én medarbejder være årsagen til et gigantisk sikkerhedsbrist, og derfor er det vigtigt, at man skaber en kultur, hvor man kan bibeholde en stab, der udvikler sig og hvor medarbejderne har lov til at fortælle om deres fejl.

"Hvis der ikke er dialog [...mellem alle led i organisationen...], så mister du stille og roligt hen af vejen føling med, om vi har styr på situationen" [CEO Christian Nielsen]

Hos virksomheden TimeLog har en af de mest betydningsfulde tiltag været, at sikre transparens fra ledelsen til medarbejderne om, hvad sikkerhed er, og hvorfor de skal sikre virksomheden. Her har det været vigtigt at medarbejderne forstår vigtigheden af cyber-sikkerhed.

"Internt er det kun tungt hvis ikke toppen og bestyrelsen har meldt ud hvorfor det gøres. Vi er nødt til at forklare, hvad formålet med security er. Jeg hører det spørgsmål mere og mere sjældent: hvorfor vi skal gøre det. Det tror jeg, at vi i høj grad er ude over. " [TimeLog, CEO Per Henrik Nielsen]

To alternative veje fra cybersikkerhed til konkurrencefordele:

IT-sikkerhed

Case: Inno Aps
Branche: Bygge- og anlæg; Byggeentreprenører; Opførelse af bygninger
Antal ansatte: 11-20
Omsætning: 16-75 millioner

Kvalitetskontrol

Case: Varde Laks
Branche: Fremstilling; Fiskeindustri; Forarbejdning og konservering af fisk, krebsdyr og bløddyr, undtagen fiskemel
Antal ansatte: 21-50
Omsætning: 76-375 millioner

Både hos Inno Aps og hos Varde Laks har de fokuseret på at øge konkurrencefordelen gennem kvalitet i deres produkter, og ad den vej har det været naturligt at forbedre processerne omkring IT og cybersikkerhed. Et stærkt fokus på kvalitet har hjulpet dem ud af pris som den primære konkurrenceparameter.

Det er ikke sådan at cybersikkerhed har stået højt på listen over prioriteter, men når man vil kvalitet og grundighed, og vil optimere sine processer, så nytter det ikke at det roder i it-systemerne eller at cybersikkerheden mangler.

&#

"Når vi laver processer, som vi er i gang med nu, så betyder det, at vi konsekvent får en bedre indtjening, fordi vi har tjekket og optimeret på det vi laver, vi dokumenterer det vi laver, og at vi gemmer det, som vi laver på de rigtige steder. Aftaler bliver skrevet ned, bekræftet og gemt på sagerne."

[Inno Aps, lille SMV i Bygge & anlæg, CEO Claus Jørgensen]

[Inno Aps, lille SMV i Bygge & anlæg, CEO Claus Jørgensen]

"Kvalitetskontrol er ikke et mål; det er sådan set et krav fra de kunder, vi har, som er nogle meget store kæder, der ikke spiller med amatører. Og der skal du have kvalitetskontrol, så de over for deres bagland kan dokumentere, at der er nogen, der tager hånd om tingene"

[Varde Laks, lille SMV i Fremstilling, CEO Thomas Brink Jakobsen]

Begge virksomheder fortæller, hvordan struktur og ordentlighed har rykket ind i deres IT-systemer og ad den vej ind i måden de tænker og styrer deres cybersikkerhed på.

Hos Inno ApS har arbejdet med bedre struktur ført til at de har centraliseret deres IT, herunder mail og dokumenter, fakturaer og ordrer. Eksempelvis har indføring af fjernskrivebord betydet, at de meget nemmere kan holde styr på alt fra backup til beskyttelse mod malware.

Hos Varde Laks har arbejdet omkring at optimere deres processer betydet, at de har måtte indføre bedre kontroller, ikke kun i forhold til fakturering og betaling af regninger, men at de nu har kontroller på plads, der beskytter dem mod cybertrusler, der går mere direkte efter pengene. Styringen af disse kontroller ligger som en naturlig del af processerne omkring virksomhedens kvalitetsstyring.

Både hos Inno Aps og Varde Laks har man tilkøbt IT-systemer og sikkerhed eksternt af kyndige partnere, så CEOen kan fokusere mere på kerneydelsen frem for på cybersikkerhed.

33

Forskellige former for cybersikkerhedstiltag & konkurrencefordele

I dette kapitel går vi et spadestik dybere, og ser nærmere på de enkelte spørgsmål til tiltag og fordele. For at få indblik i SMVernes praksis inden for cybersikkerhedstiltag har vi helt konkret spurgt virksomhederne, om de indenfor en 2-årig periode har lavet eller opdateret 15 konkrete cybersikkerhedstiltag. Disse tiltag har vi inddelt i tre kategorier;

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

Ligeledes har vi spurgt om virksomhedernes investering i cybersikkerhedstiltag har medført 11 konkrete konkurrencefordele. Disse fordele er ligeledes inddelt i tre kategorier;

1. Effektivitet & nytænkning
2. Tillid
3. Bundlinje.

For at komme tættere på at kunne forklare den positive sammenhæng mellem tiltag og fordele, undersøger vi også sammenhængen mellem de forskellige *former* for cybersikkerhed og de forskellige *kategorier* af konkurrencefordele. Der tegner sig et billede af, at flere former for tiltag også giver flere konkurrence-fordele inden for alle tre kategorier.

3 former for cybersikkerheds-tiltag

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

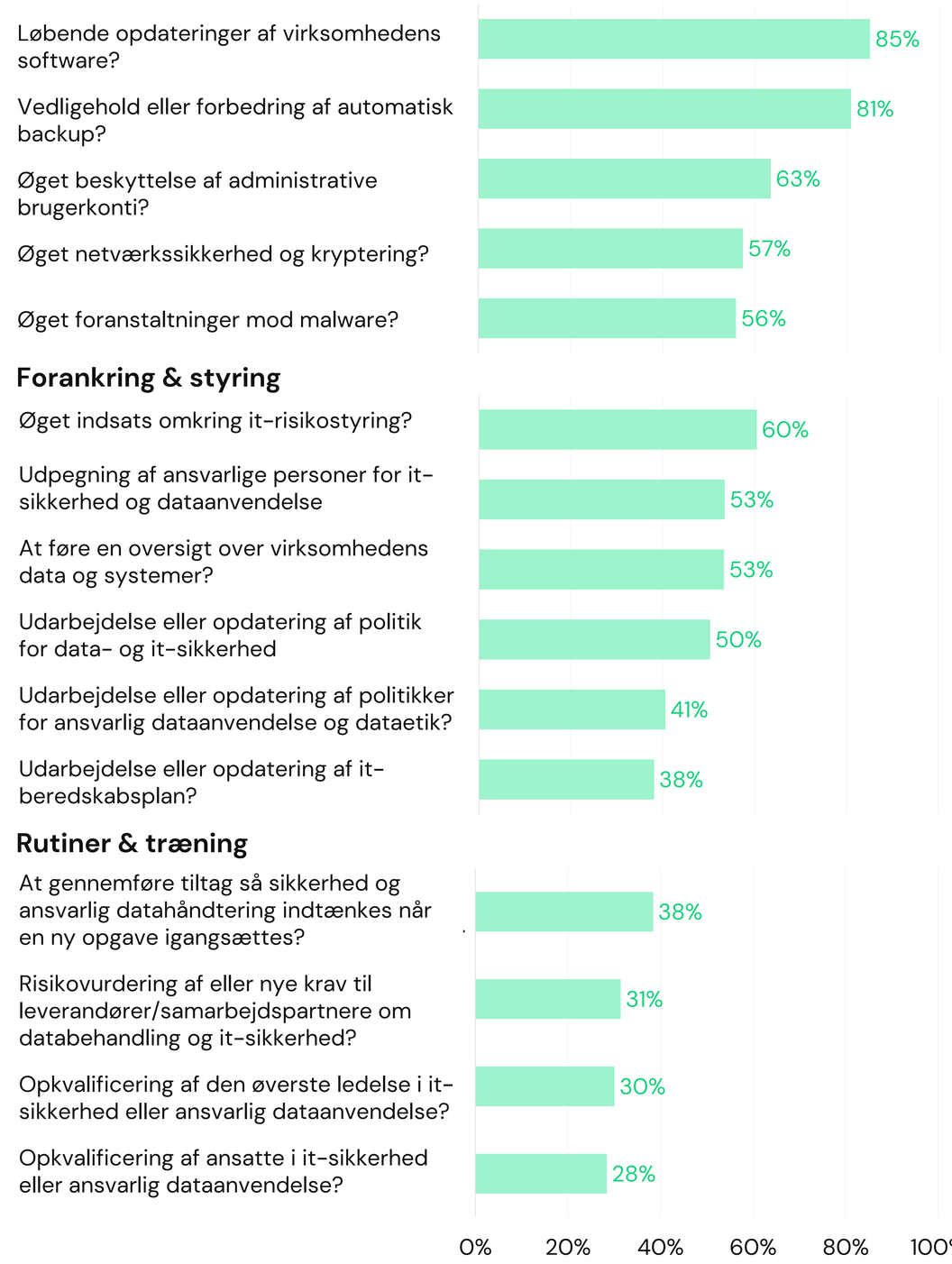
Rutiner & træning

- 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

Når man ser nærmere på de tre former for cybersikkerhedstiltag på figur 5, er det tydeligt, at SMV'erne starter med at indføre tekniske tiltag. Eksempelvis har 85 pct. af SMV'erne indført løbende opdateringer af virksomhedens software. Mere end halvdelen af alle virksomhederne har indført tekniske cybersikkerhedstiltag. Det næste SMV'erne giver sig i kast med er forankring og styring. Her er det særligt en øget indsats omkring it-risikostyring, som 60 pct. har indført, mens 38 pct. har udarbejdet eller opdateret deres beredskabsplan. De sidste former for tiltag omhandler rutiner og træning. For alle spørgsmålene her gælder, at mindre end 40 pct. af SMV'erne har indført det pågældende tiltag. Det ser ud til, at det er svært at få opkvalificeret den øverste ledelse i it-sikkerhed og ansvarlig dataanvendelse.

CEO Christian Nielsen hos DEIF ser cybersikkerhed som en kærkommen mulighed for at involvere bestyrelsen. Det kan også bruges til at skabe en mere generel tillid hos bestyrelsen, som med rette kan inddrages omkring de største cyberrisici. Han ser cybersikkerhed som så stor en risiko, at opgaven er på niveau med fx økonomien, hvor arbejdet omkring cybersikkerhed bliver en klassisk bestyrelsesopgave. Christian Nielsen har en god dialog med sin egen bestyrelse, men det er hans oplevelse, at bestyrelsen hovedsageligt har været interesseret i den interne del – den del der berører virksomheden og ikke kunderne.

Figur 5: Andele der har indført cybersikkerhedstiltag



Note: Spørgsmålet: Har virksomheden indenfor de seneste 2 år styrket cybersikkerheden gennem: []

N= 673

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

Af de tre kategorier af konkurrencefordele, er Effektivt & nytænkning de første konkurrencefordele SMV'erne oplever, tæt efterfulgt af kategorien Tillid. Det er de to såkaldte "bløde" konkurrencefordele. SMV'erne oplever, at deres tiltag i cybersikkerhed har medvirket til at de er blevet bedre til at implementere og bruge nye teknologier, og at arbejdsgangene er blevet simplere og mere effektive. De har øget tilliden fra bestyrelsen, investorer og aktionærerne til ledelsen, og relationen til eksisterende kunder er styrket.

De mere "hårde" konkurrencefordele som rammer bundlinjen, er der færre, der oplever. Det er også de fordele som tidsmæssigt sætter sidst ind. Hvor 14 pct. oplever, at deres tiltag har betydet, at virksomheden har kunne differentiere sig fra konkurrenter, er der bare 6 pct. der oplever, at deres tiltag har gjort, at de ligefrem kunne hæve prisen på deres produkter.

I interviews med SMVere beskriver flere cybersikkerhed som afgørende for overhovedet at være på markedet. Det er altså ikke sådan at cybersikkerhed har medført at de nødvendigvis har kunne hæve priserne, men derimod er det en forudsætning for at eksistere.

"Hvis ikke du har security som beskytter dig som individ og det firma, som du håndterer, så er du ikke bæredygtig"
[TimeLog, CEO Per Henrik Nielsen]

Figur 6: Andele der oplever konkurrencefordel

Note: Spørgsmålet: Hvor enig er du I, at virksomhedens indsatser for at styrke cybersikkerhed se seneste 2 år har bidraget til: []

N= 673

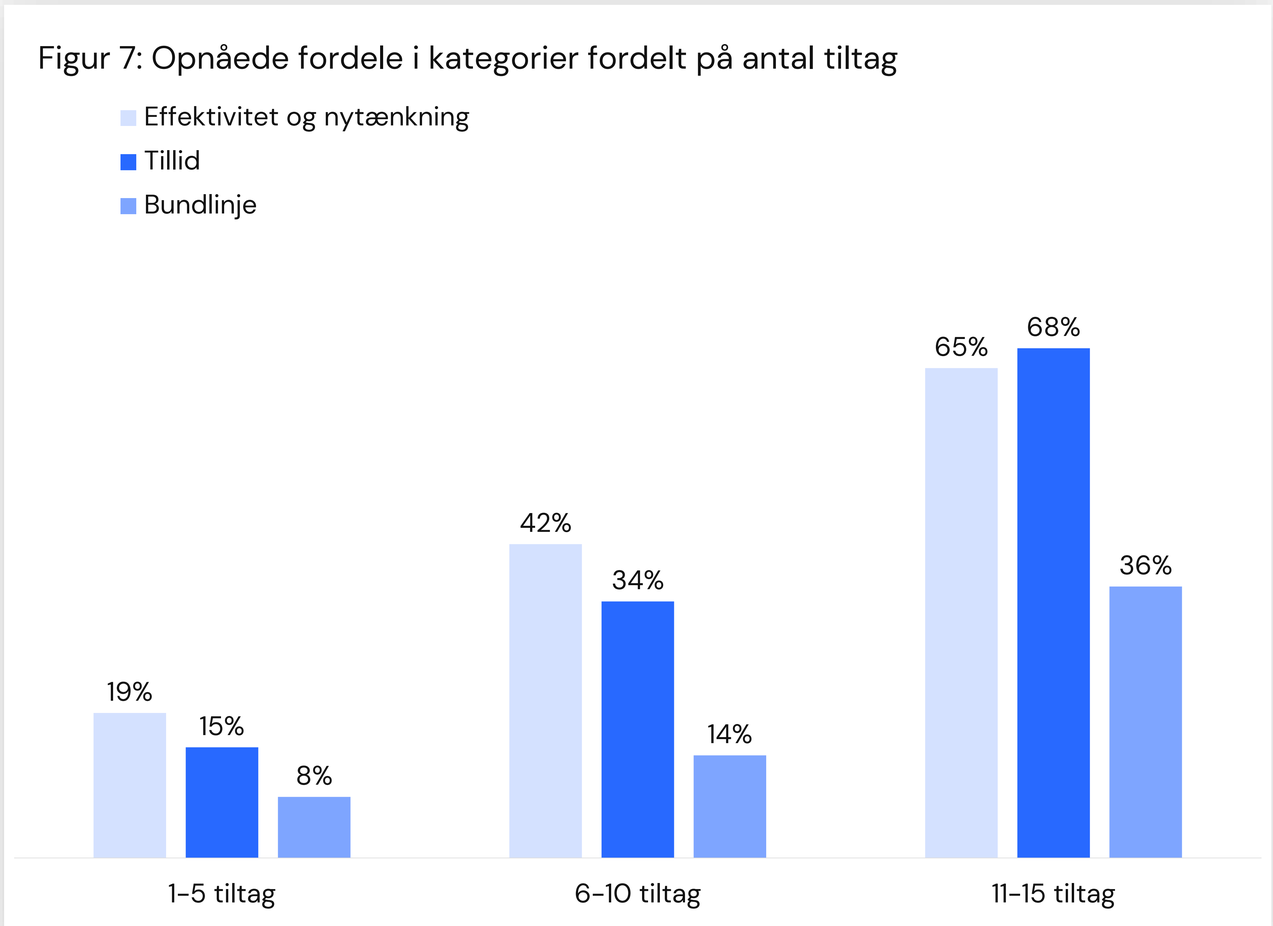
Jo flere cybersikkerhedstiltag, des flere konkurrencefordele inden for alle tre kategorier

Figur 7 viser sammenhængen mellem SMVers antal cybersikkerhedstiltag og deres oplevede konkurrencefordele i de tre kategorier: Effektivitet & nytænkning, Tillid, og Bundlinje.

Man kan se, at SMVer med 1-5 tiltag og 6-10 tiltag er det en form for trappe mellem kategorierne. Her oplever flest konkurrencefordele inden for Effektivitet & nytænkning (19 og 42 pct.), dernæst Tillid (15 og 34 pct.) og bundlinjen (8 og 14 pct.). For virksomheder med flest tiltag (11-15) ser det anderledes ud. Her overstiger Tillid kategorien Effektivitet & nytænkning, så de ligger side om side (65 og 68 pct.) Dette indikerer, at der eksisterer en grænse; når man overkommer dén, komplementerer tiltagene hinanden, så cybersikkerhed går op i højere enhed, og bedre struktur. Hos DEIF oplever CEO Christian Nielsen også at tillid til virksomhedens cybersikkerhed har øget deres konkurrenceevne.

"Kunder vil ikke samarbejde med virksomheder, som ikke kan forsvare sig selv" [DEIF, CEO Christian Nielsen]

Figur 7: Opnåede fordele i kategorier fordelt på antal tiltag



N= 673

> *Det er sådan en kamp, som du skal lære at leve med. Der findes ikke en første halvleg, anden halvleg og tredje halvleg. Der findes en rigtig lang halvleg, og den bliver ved, og det skal du lære at leve med.*
>
> [TimeLog, CEO Per Henrik Nielsen]

Når vi opdeler cybersikkerhedstiltag i forskellige former viser det sig, at de færreste SMVer kun indfører én type tiltag. På figur 8 på næste side er illustreret, hvordan kun 14 pct. har indført bare én form, 18 pct. har indført to former, mens størstedelen (68 pct.) har indført tiltag inden for alle tre former for tiltag.

Få virksomheder har udelukkende indført tekniske tiltag, mens stort set ingen SMVer udelukkende indfører tiltag inden for Forankring & styring eller rutiner & træning uden også at have tekniske tiltag. Det tyder på et hieraki, hvor de fleste virksomheder først indfører de tekniske tiltag som beskyttelse mod malware og løbende opdateringer, for så på et senere tidspunkt at indføre mere omfattende tiltag, der påvirker kulturen og tankegangen i virksomheden.

Flere SMVere på tværs af brancher påpeger, at cybersikkerhed er noget, man arbejder med på den lange bane og på mange fronter. Der er intet vidundermiddel, der kan udelukke hackerangreb, men man kan sikre sig med opkvalificering og ekstern hjælp; og så blive ved med at holde sig i gang.

"Der er ikke noget, der er perfekt. Vi bliver nødt til at finde, hvad der er forsvarligt her og nu" [DEIF, CEO Christian Nielsen]

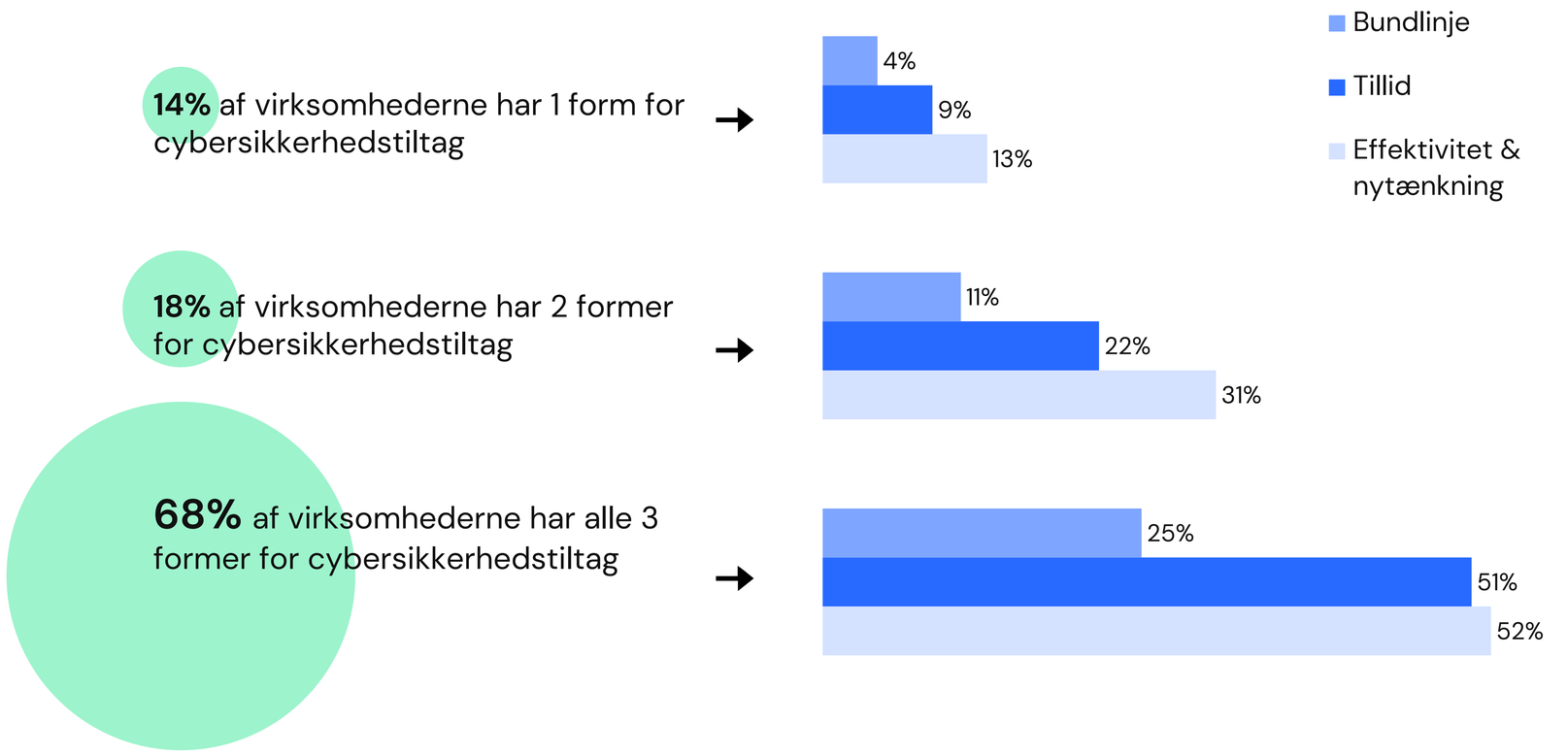
Jo flere former for tiltag, des flere fordele inden for alle kategorier

Som man kan se på figur 8, er virksomheder der oplever flest konkurrencefordele af deres cybersikkerhedstiltag de virksomheder, der har indført alle tre former.

Her kan man se, at det ikke blot er antallet af tiltag, men også forskelligheden i tiltag, der giver gevinst på både Effektivitet & nytænkning, Tillid og Bundlinje.

Fordi så mange virksomheder indfører flere former for tiltag og tilsvarende konkurrencefordele, er det *ikke* muligt at pege på et enkelt tiltag, der er vigtigere for konkurrencefordele end et andet.

Figur 8: Andele af virksomheder der oplever konkurrence-fordele indenfor 3 former

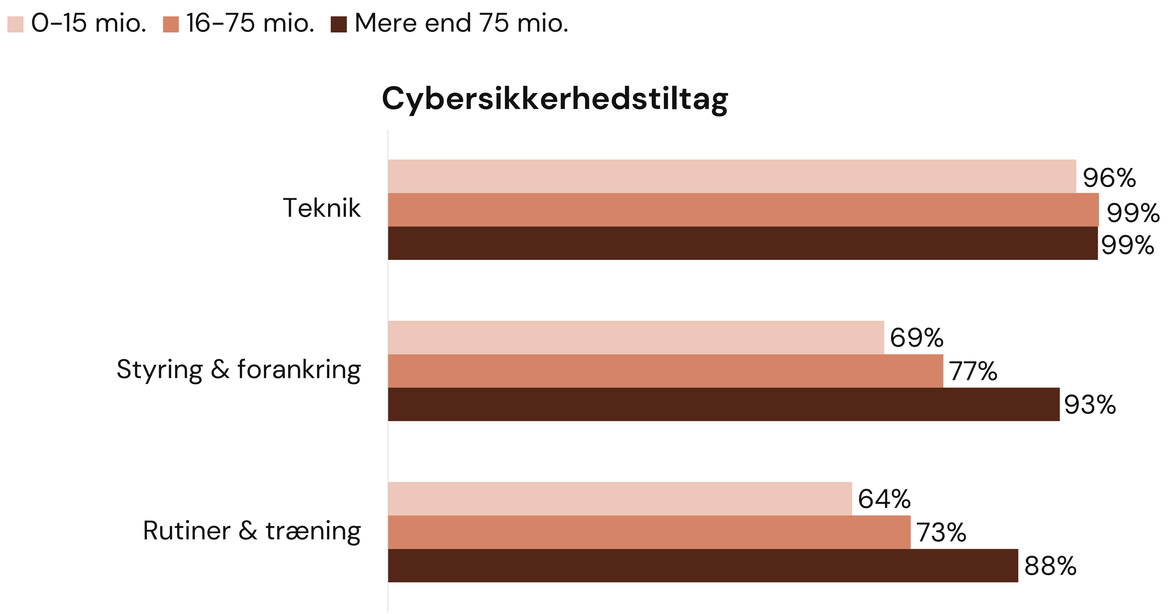


Note: Se inddeling i former for cybersikkerhedstiltag og kategorier af konkurrencefordele på side 24 og 26.

De største SMVere har flest former for tiltag og oplever flest fordele inden for alle kategorier

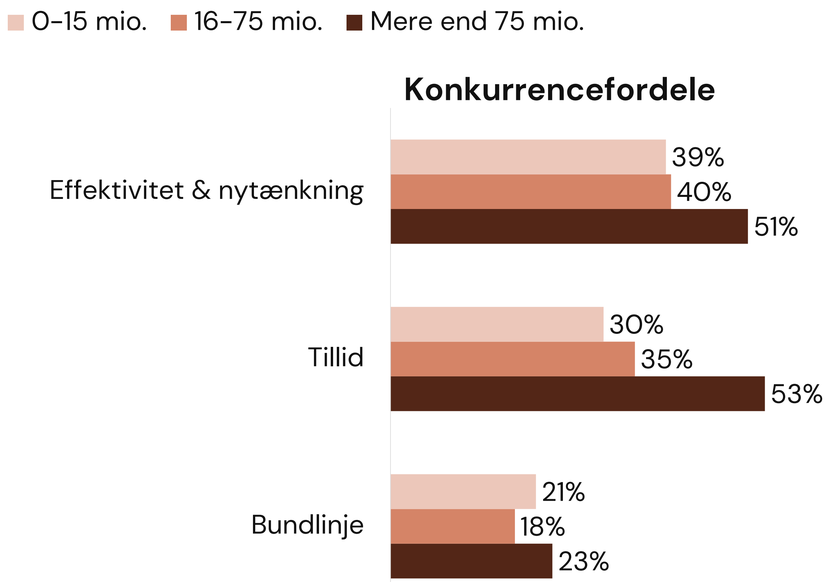
Det er de større SMVere, hvor flest har indført alle tre former for cybersikkerhedstiltag. Stort set alle virksomheder har dog indført mindst ét tiltag inden for Teknik, mens den store forskel ligger i Styring & forankring. Her er der væsentligt flere af de største SMVere, der har indført tiltag.

Figur 9.1: Andel af virksomheder der har mindst 1 tiltag indenfor de 3 kategorier, fordelt på virksomhedernes omsætning



Og der er også flest større SMVere, der oplever konkurrencefordele inden for alle tre kategorier. Særligt oplever de flere konkurrence-fordele inden for Effektivitet & nytænkning og Tillid, mens der kun er små forskelle på Bundlinjen. Det kan hænge sammen med at konkurrencefordele på bundlinjen er de sidste i rækken af fordele, der træder i kraft, og i mange tilfælde en konsekvens af øget effektivitet og tillid.

Figur 9.2: Andel af virksomheder der oplever mindst 1 konkurrencefordel indenfor de 3 former, fordelt på virksomhedernes omsætning



N= 653 (blandt virksomheder med tiltag, er der 20 virksomheder, der ikke ønsker at opgive deres omsætning)

44

Brancher

Der er SMVer, hvor cybersikkerhedstiltag umiddelbart er mere oplagte end for andre. Eksempelvis vil det være oplagt at fx IT-virksomheder har brug for at sikre deres produkt med forskellige tiltag. Men der findes efterhånden ingen virksomheder, der ikke på den ene eller anden måde har noget data, de skal beskytte, lige fra kundeoplysninger til forretningshemmeligheder.

I dette kapitel ser vi nærmere på sammenhængen mellem cybersikkerhedstiltag og konkurrencefordele inden for forskellige brancher. Ligesom vi har gjort i de forrige kapitler, grupperer vi også former for tiltag og kategorier af fordele.

Vi ser, at der inden for alle brancher viser sig samme mønster som vi har set tidligere i rapporten; nemlig at de SMVer der har indført flest tiltag også oplever flest konkurrencefordele.

Vi har inddelt SMVerne i fire brancher[1]:

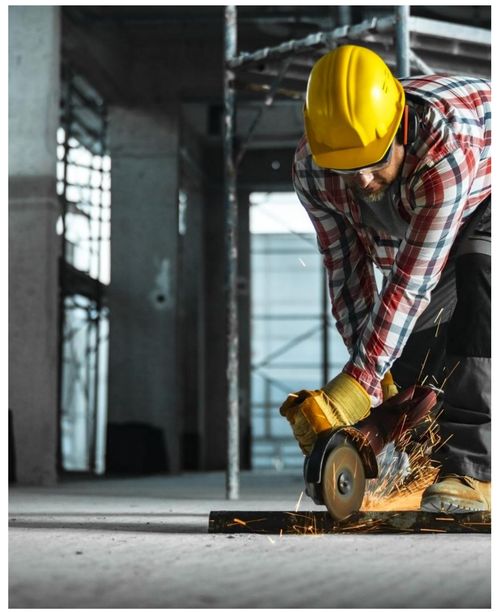
- Fremstilling udgør 44 pct.
- Bygge & anlæg 39 pct.
- Transport & godshåndtering 13 pct.
- Information & kommunikation 4 pct.

I kapitel 5 kan man finde fakta om hver enkelt branche.

[1] Branchen Råstofudvinding indgår også i undersøgelsen, men fordi branchen kun udgør 0,6 pct. af SMVere er stikprøven for lille til at lave statistik på. Se side 40 for mere information.

Fremstilling

Bygge & anlæg



Transport & godshåndtering

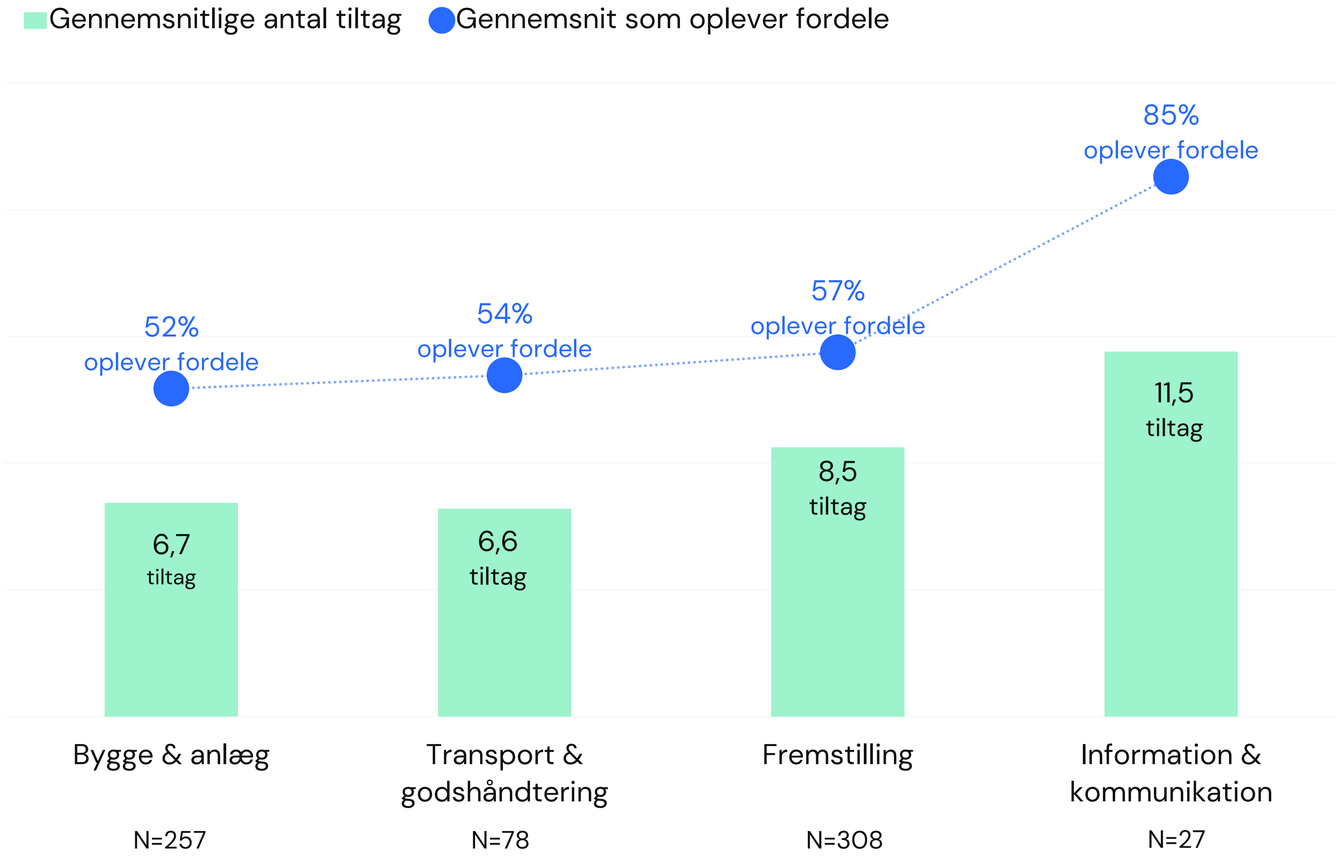
Information & kommunikation

På tværs af brancher oplever flere konkurrencefordele, når de indfører flere cybersikkerhedstiltag

Figur 10 viser gennemsnitlige antal tiltag og andelen, der oplever én eller flere konkurrencefordele fordelt på de fire brancher[1]. Branchen der har indført flest tiltag er Information & kommunikation (11,5 tiltag i gennemsnit) , og det er også den branche, hvor flest oplever en konkurrencefordel (85 pct.).

Der er en tydelig sammenhæng mellem fordele og tiltag inden for alle brancher, men det lader til, at Fremstillingsbranchen har lidt mindre gevinst af sine tiltag end de andre brancher. På trods af et højt gennemsnit på 8,5 tiltag, er der kun lige over halvdelen, der oplever konkurrencefordele.

Figur 10: Cybersikkerhedstiltag og konkurrencefordele, fordelt på branche



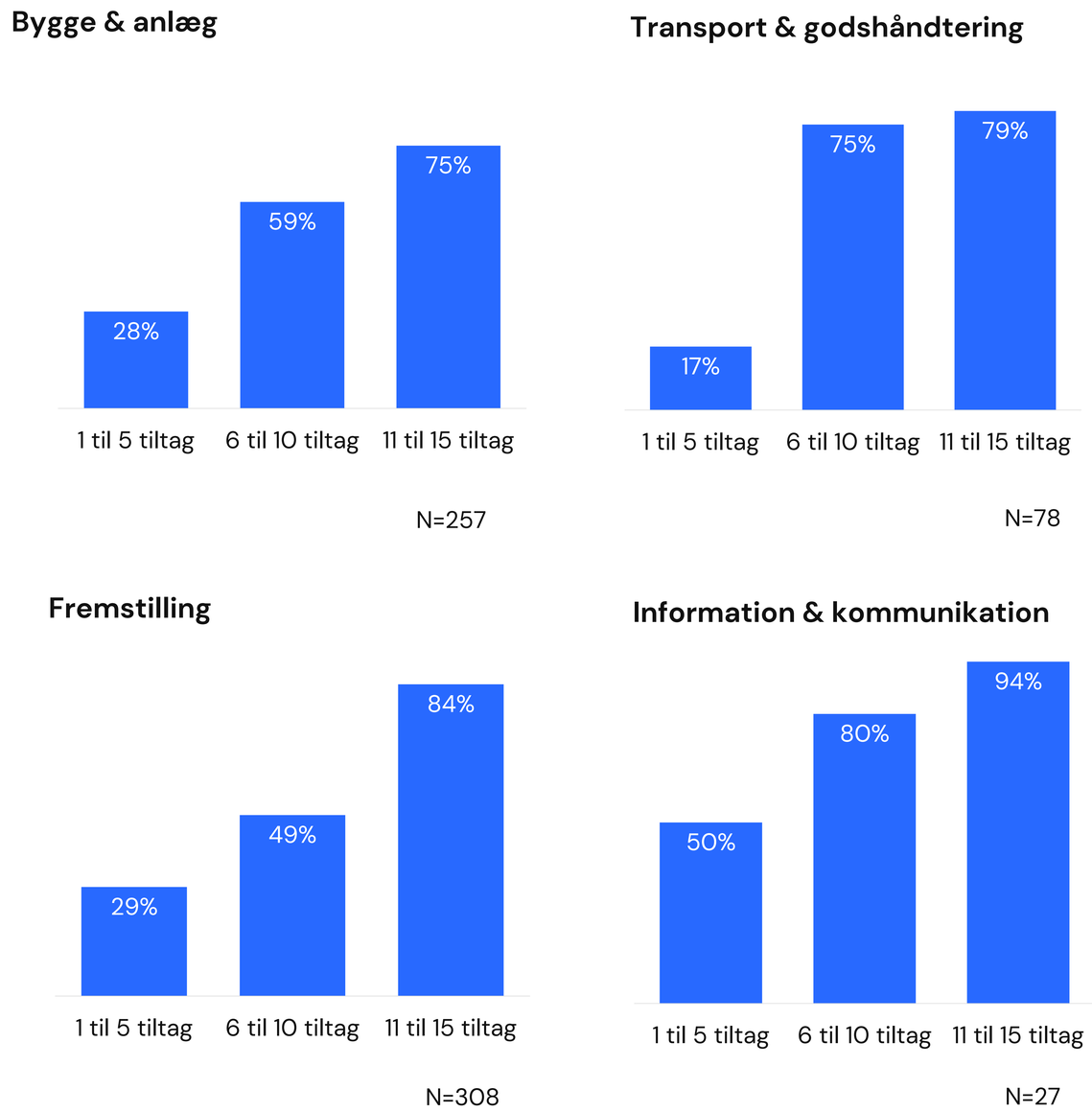
[1] Branchen Råstofudvinding indgår også i undersøgelsen, men fordi branchen kun udgør 0,6 pct. af SMVere er stikprøven for lille til at lave statistik på. Se side 40 for mere information.

Ved at opgøre SMVere i antal cybersikkerhedstiltag og hvor mange, der oplever konkurrencefordele for hver branche, kan man se, at sammenhængen er universel. Der er samme mønster på tværs af branche – SMVer med flere cybersikkerhedstiltag oplever også flere konkurrencefordele, ligesom figur 11 viser.

Hvor SMVerne i de to største branche – Fremstilling og Bygge & anlæg - har en tæt på lineær stigning, hvor flere SMVere også oplever konkurrencefordele i takt med tiltag, ser det anderledes ud for den tredjestørste branche - Transport & godshåndtering. Her er der færre, kun 17 pct., der oplever konkurrencefordele ved de første 1-5 tiltag. Til gengæld er der væsentligt flere (75 pct.), der oplever konkurrencefordele allerede ved 6-10 tiltag og kun lidt flere (79 pct.) ved 11-15 tiltag.

I den mindste branche - Information & kommunikation - oplever virksomhederne generelt et højere niveau af konkurrencefordele, sandsynligvis fordi cybersikkerhed er en del af flere virksomheders produkt.

Figur 11: Andele af virksomheder i hver branche, der oplever fordele fordelt efter antal tiltag.

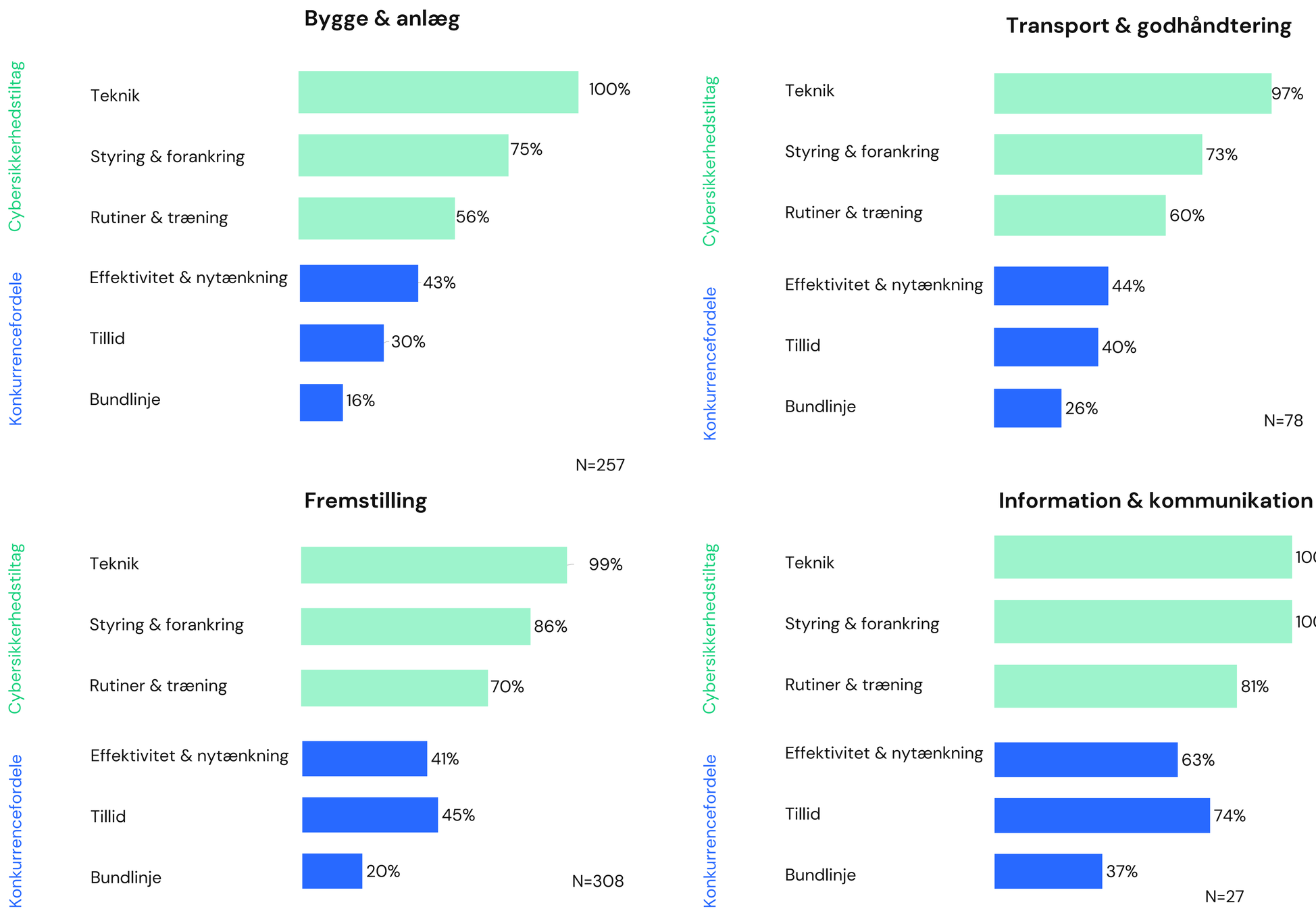


På næste side har vi opgjort forskellige former for cybersikkerhedstiltag og konkurrencefordele for brancherne (kategorierne er defineret på side 24 og 26). Den største branche Fremstilling følger et trappemønster i tiltag. De fleste SMVere har tiltag inden for Teknik – hvilket gør sig gældende i alle brancher. Lidt færre (96 pct.) har tiltag inden for Styring & forankring, og 70 pct. inden for Rutiner & træning. Tiltagene munder ud i at flest oplever fordele inden for Tillid (45 pct.), skarp efterfulgt af Effektivitet & nytænkning (41 pct.) og færrest på Bundlinjen (20 pct.). Både brancherne Bygge & anlæg og Transport & godshåndtering følger samme mønster, dog lidt lavere niveau ift. former for tiltag, men her oplever flere en fordel inden for Effektivitet & nytænkning (hhv. 43 pct. og 44 pct.) fremfor Tillid (hhv. 30 pct. og 40 pct.).

Den mindste branche i analysen og generelt – Information & kommunikation – har flere tiltag inden for både Styring & forankring (hele 100 pct.) og Rutiner & træning (81 pct.). Som for Fremstilling viser der sig en anden fordeling i konkurrencefordele. I de to brancher overstiger antallet, der oplever øget Tillid som en konsekvens af tiltagene, antallet der oplever øget Effektivitet & nytænkning. Det peger på, at tillid kræver lidt flere tiltag, og diverse tiltag, end fx Effektivisering af arbejdsgange. Hos virksomheden DEIF har arbejdet med cybersikkerhed været en mulighed for at vise bestyrelsen, at ledelsen har overblik og kan prioritere de største risici. Det skaber tillid hos bestyrelsen.

Branche overblik

Figur 12: Andele af virksomheder i hver branche, der har indført tiltag indenfor 3 former (grøn) samt andele af virksomheder i hver branche, der har oplevet konkurrencefordele indenfor 3 former (blå)



55

Data & metode

Spørgeskema-undersøgelse med en tilfredsstillende stikprøve

Industriens Fond har via mail udsendt spørgeskemaundersøgelsen til i alt 7.370 danske små og mellemstore virksomheder som optræder i Industriens Fonds database – udtrukket via CVR. Knap hver tiende virksomhed har besvaret undersøgelsen, og vi ender med et analyseudvalg på 729 virksomheder.

Spørgeskemaerne er hovedsageligt besvaret af ejere af virksomheder og CEOs, hvilket er en svær målgruppe at få fat i, og derfor er et analyseudvalg på 10 pct. særdeles tilfredsstillende.

For at kunne sige noget generelt om SMVerne, skal analyseudvalget være repræsentativ. Og det er lykkes. På de næste sider er illustreret at analyseudvalget både er repræsentativt på geografi, branche og størrelse. Der er også lidt beskrivende statistik af, hvem der har deltaget i undersøgelsen.

&#

Nøgletal på svarstatistik:

7.370 virksomheder er blevet inviteret til undersøgelsen

729 besvarelser i alt

Dette giver en svarprocent på **10%** af udsendte spørgeskemaer

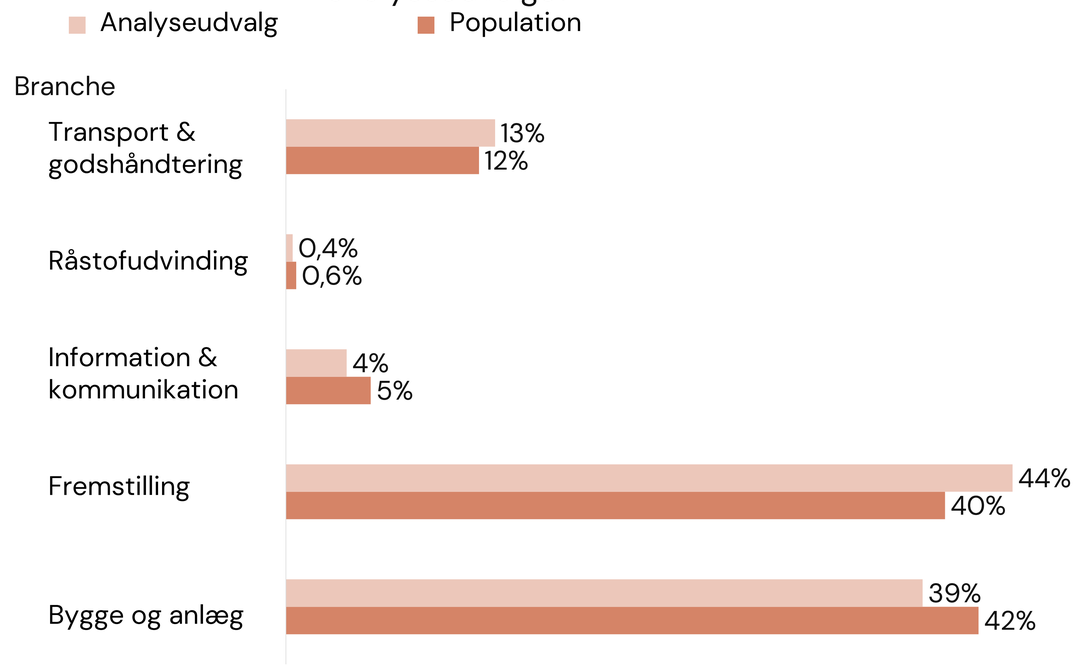
På figur 16 og 17 kan man se, at repræsentationen i analyseudvalget er yderst tilfredsstillende, både hvad angår branche og størrelse på virksomhederne.

Der er en mindre overrepræsentation af Fremstillingsvirksomheder og en mindre underrepræsentation af bygge-og anlægsvirksomheder, men stadig er forskellene så tilpas små, at det vurderes at analyseudvalget kan give et repræsentativt billede af brancherne.

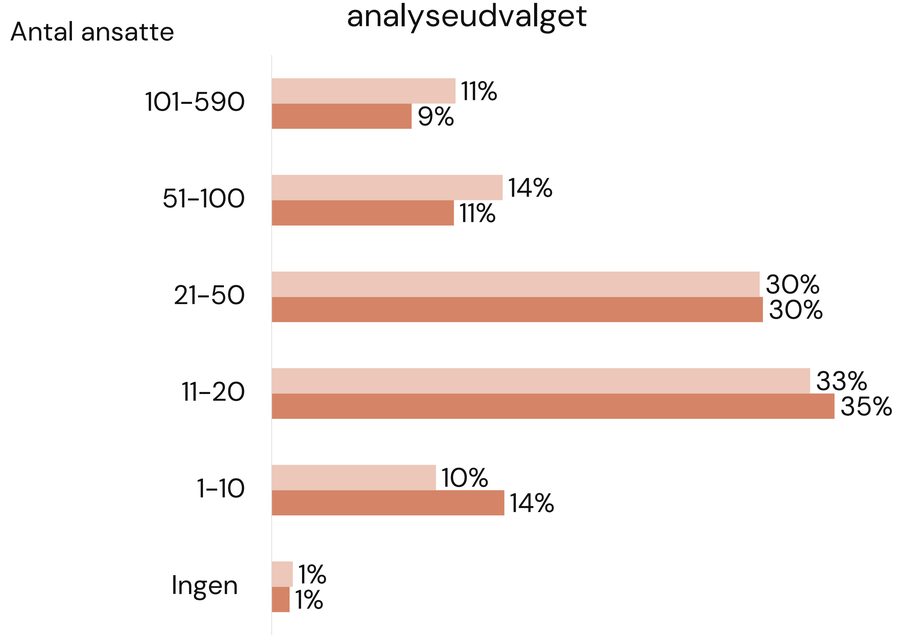
Ligeledes er der i analyseudvalget en lille overvægt af de største SMVere med flere end 51 ansatte og en lille underrepræsentation af de mindre virksomheder med 1-20 ansatte. Igen er forskellene så små, at stikprøven i høj grad repræsenterer SMVerne.

Geografisk er analyseudvalget også tilfredsstillende. På figur 18 på næste side, er illustreret hvor tæt populationen og analyseudvalget ligger. Kun i de farvede områder afviger analyseudvalget fra populationen med mere end 0,6 pct.-point. De mørkere farver optræder udelukkende i Aarhus og København, og her er afvigelsen kun hhv. 1,8 og 1,4 pct.-point, og som de eneste over 1 pct.-point afvigende fra populationen. Det er også de to byer, hvor flest SMVer befinder sig. På baggrund af en skæv geografisk fordeling blev der udsendt flere spørgeskemaer i udvalgte byer, og det har rettet analyseudvalget så meget op, at den nu er tilfredsstillende.

Figur 16: SMVer fordelt på brancher i hhv. populationen og analyseudvalget

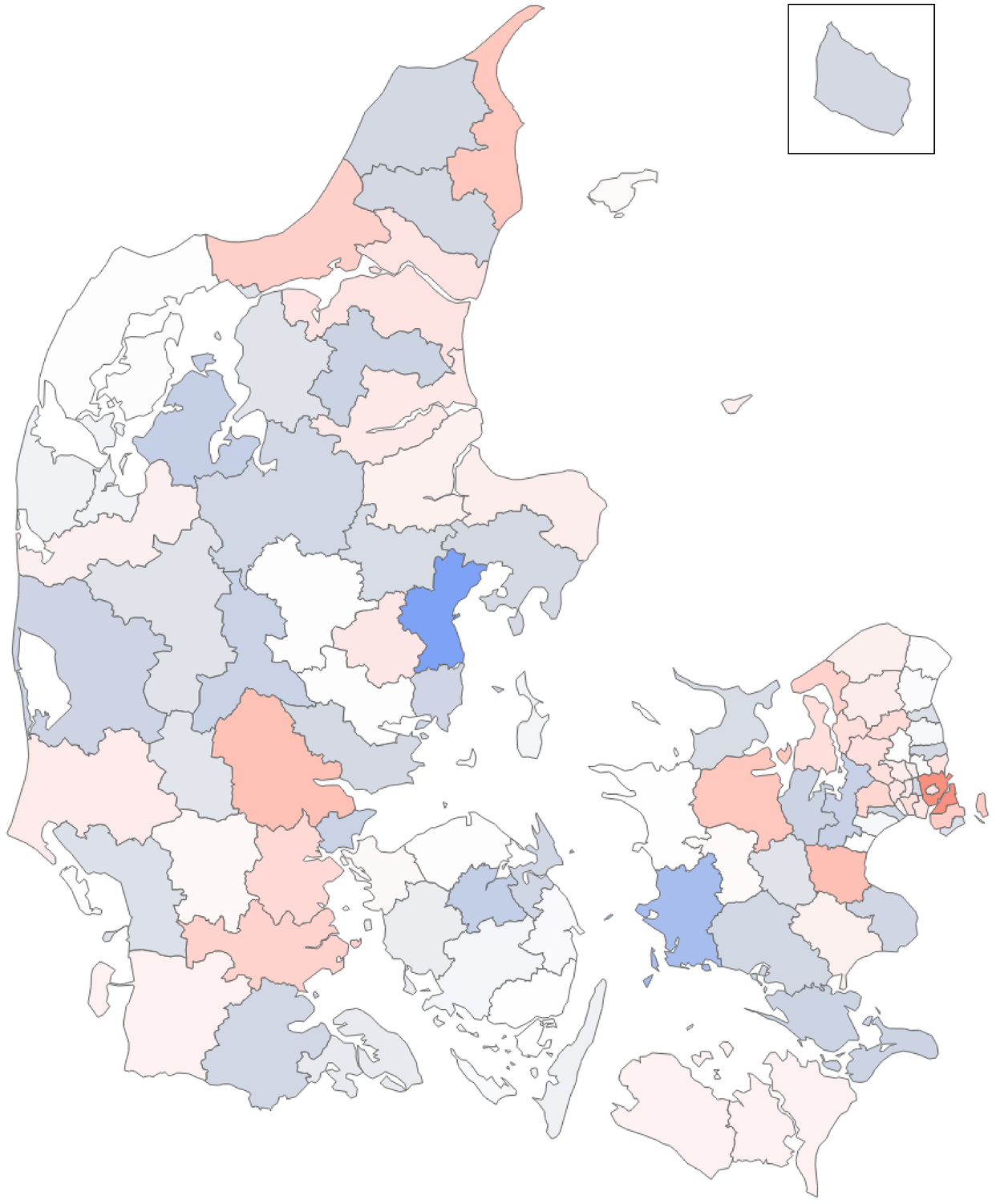


Figur 17: SMVer fordelt på antal ansatte i hhv. populationen og analyseudvalget



Figur 18: Geografisk repræsentativitet

- Underrepræsenteret med 1-1,4 pct.-point
- Underrepræsenteret med 0,5-1 pct.-point
- Underrepræsenteret med 0,1-0,5 pct.-point
- Lige repræsenteret med 0-0,1 pct.-point
- Overrepræsenteret med 0,1-0,5 pct.-point
- Overrepræsenteret med 0,5-1 pct.-point
- Overrepræsenteret med 1-1,8 pct.-point



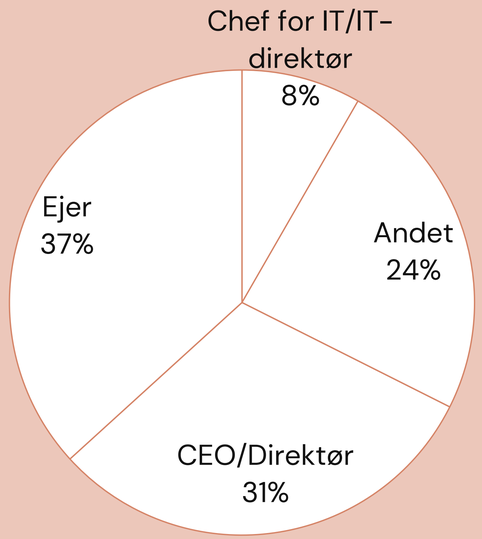
Hvem er virksomhederne i undersøgelsen?

Det har været vigtigt, at respondenterne både kender til de cybersikkerhedstiltag, som virksomheden har indført, og også de oplevede konkurrencefordele på et mere strategisk niveau. Derfor er det også tilfredsstillende, at det i høj grad er ejere (37 pct.) og CEOs og direktører (31 pct.), der har besvaret undersøgelsen (se figure 19).

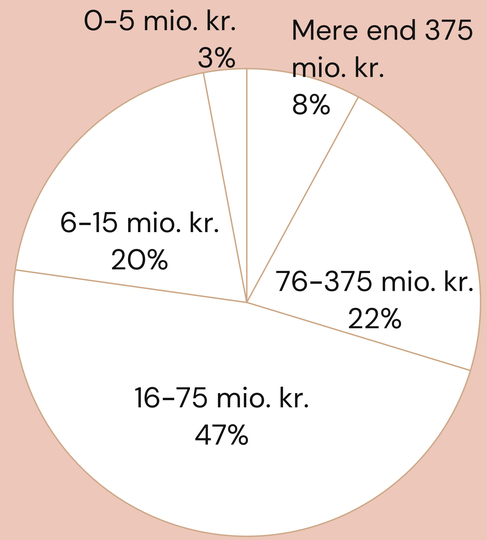
Når man ser på omsætning udgør svarene fra den midterste kategori (16-75 mio. kr.) omkring halvdelen af besvarelserne. Den anden halvdel er jævnt fordelt på både mindre og større virksomheder, som man kan se på figur 20.

Som man kan se på de tre nederste nøgletal behandler to ud af tre virksomheder forretningskritiske data eller personfølsomme oplysninger, 11 pct. udvikler software, algoritmer eller AI, mens kun 7 pct. af virksomhederne følger eksisterende standarder inden for cybersikkerhed. Her er rum for forbedring.

Figur 19: Titler på besvarere af undersøgelsen



Figur 20: Omsætning blandt SMVere i undersøgelsen



63%

behandler forretningskritiske data eller følsomme personoplysninger

11%

udvikler software, algoritmer eller AI

7%

følger eksisterende standarder for cybersikkerhed

Hvorfor størrelsen på virksomheder måles i omsætning fremfor antal ansatte i rapporten

Man kan opgøre størrelsen på en virksomhed på mange måder, og vi har både muligheden for at opgøre størrelsen ved antal ansatte eller omsætningen.

Korrelationen måler hvor stort sammenfald der er mellem antal ansatte og størrelsen på omsætningen. Korrelationen kan ligge mellem -1 og +1. Hvis den er lig 1, er der perfekt sammenfald – så måler de altså præcis det samme.

Vi får en korrelation på 0,68, hvilket også er højt og som logisk giver mening. Selvfølgelig har virksomheder med høj omsætning i mange tilfælde også mange ansatte. Fordi både antal ansatte og størrelsen på omsætning er et udtryk for størrelse på virksomheden, har vi valgt at gå videre med kun omsætning. Det har vi gjort, fordi sammenhængen mellem cybersikkerhed, konkurrencefordele og størrelse er tydeligere, når vi bruger omsætning end antal ansatte. Der er derfor kun små forskelle i resultaterne alt efter om man bruger omsætning eller antal ansatte.

Korrelationen mellem antal ansatte og omsætningen er **0,68**. Det betyder en stor sammenhæng mellem antal ansatte og omsætning.

Tabel 2: Omsætning og antal ansatte

	Omsætning		
	0-15 mio. kr.	16-75 mio. kr.	Mere end 75 mio. kr.
0-20 ansatte	127	144	21
21-50 ansatte	.	145	47
Mere end 50 ansatte	.	24	139

Note: Der er færre end fem virksomheder med en omsætning på 0-15 mio. kr. med mere end 20 ansatte, hvorfor vi ikke kan vise tallet.

Kvalitative interviews til at kvalificere spørgeskema-undersøgelsen både før og efter

Som en del af udviklingen af spørgeskemaet blev der afholdt en workshop med tre vidt forskellige typer SMVere, og de har sammen med et litteraturgennemgang og sparring fra eksperter dannet grundlag for spørgsmålene i spørgeskemaet.

Efter indsamling af besvarelserne har vi yderligere interviewet fire SMVere:

- TimeLog
- DEIF
- Inno Aps
- Varde Laks

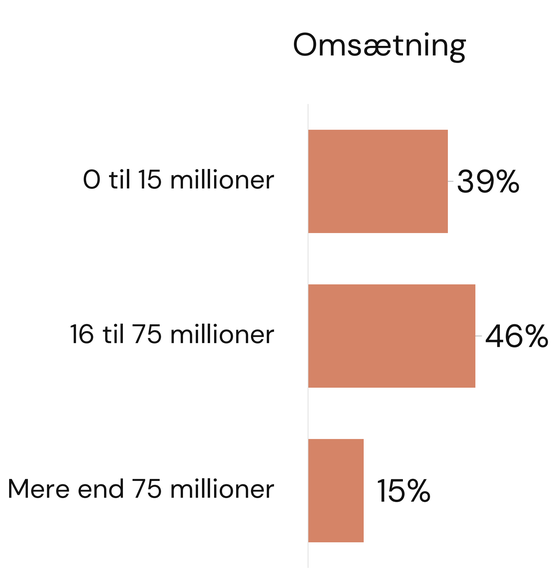
De fire virksomheder er vidt forskellige SMVere, men de udmærker sig ved at have indført mange cybersikkerhedstiltag og også opleve en øget konkurrenceevne af tiltagene. De er en form for best practice på området.

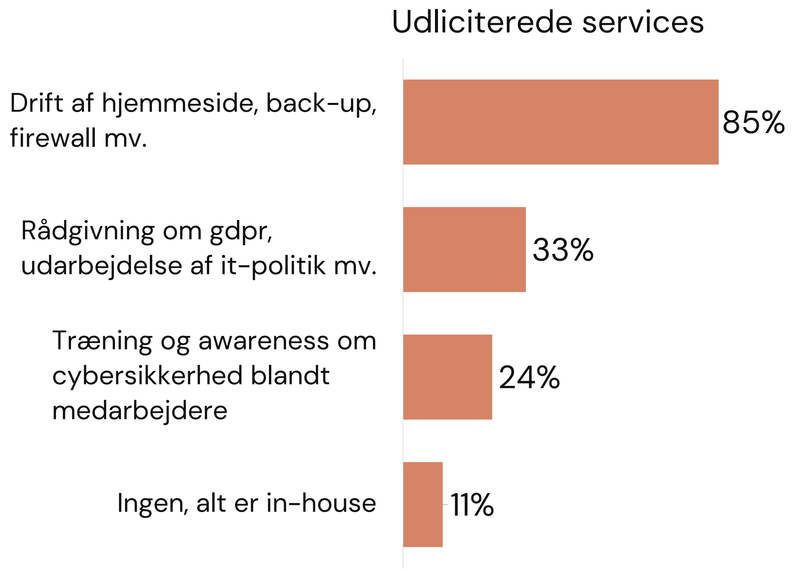
66

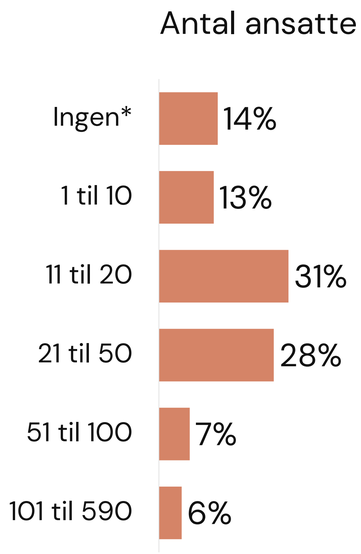
Fakta om brancher

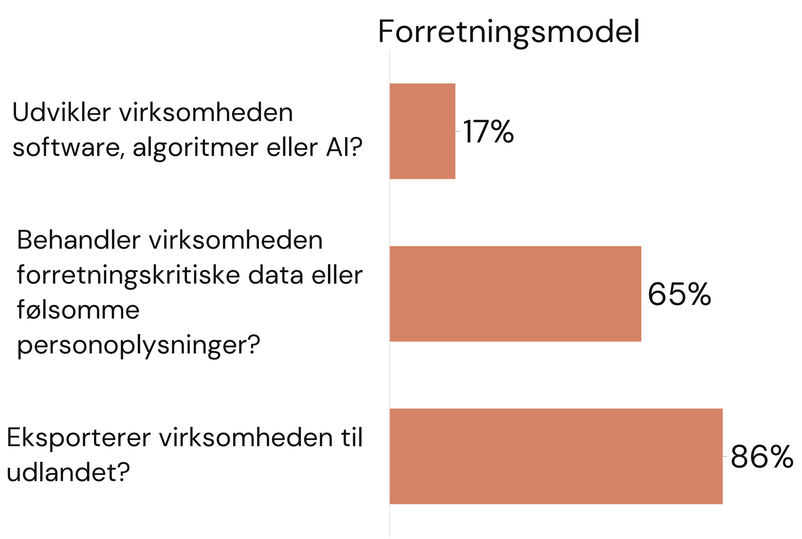
Fremstillings-virksomheder i tal

Figur 16: Andel af fremstillingsvirksomheder indenfor omsætning, udliciterering af services, antal ansatte samt forretningsmodel







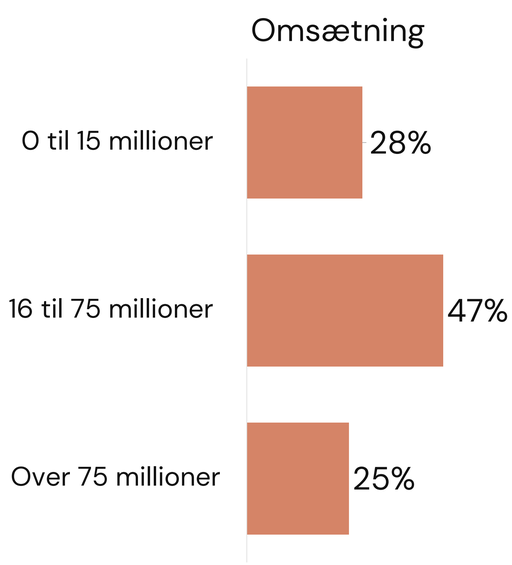


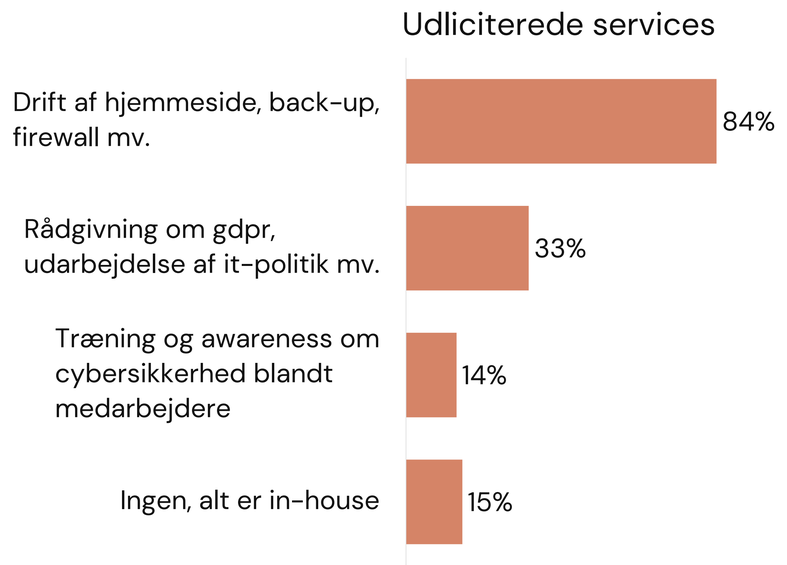
Note: Der indgår 308 fremstillingsvirksomheder med i undersøgelsen

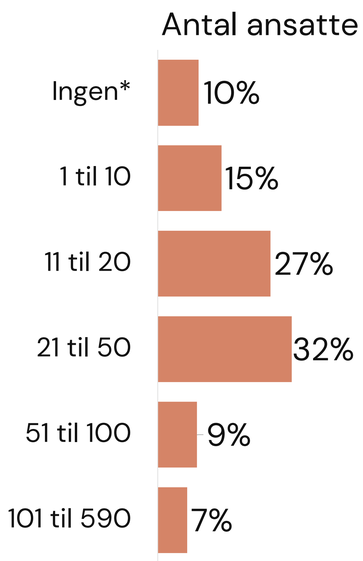
Bygge- & anlægs-branchen i tal

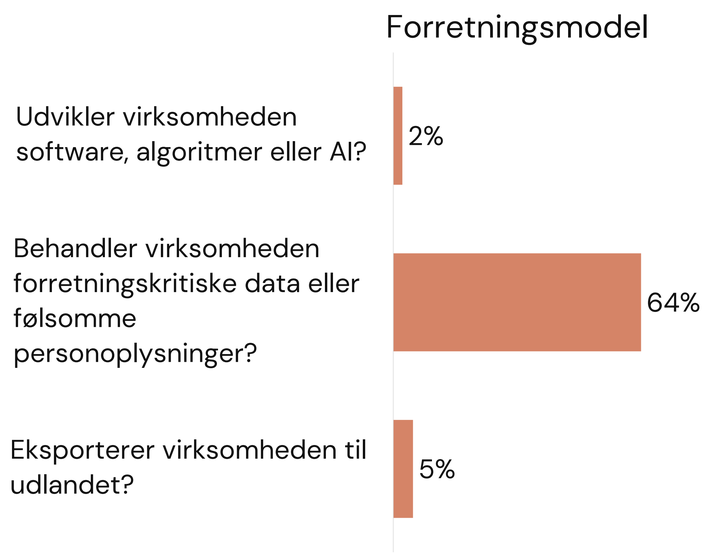
&#

Figur 17: Andel af virksomheder i bygge- og anlægsbranchen indenfor omsætning, udlicitering af services, antal ansatte samt forretningsmodel







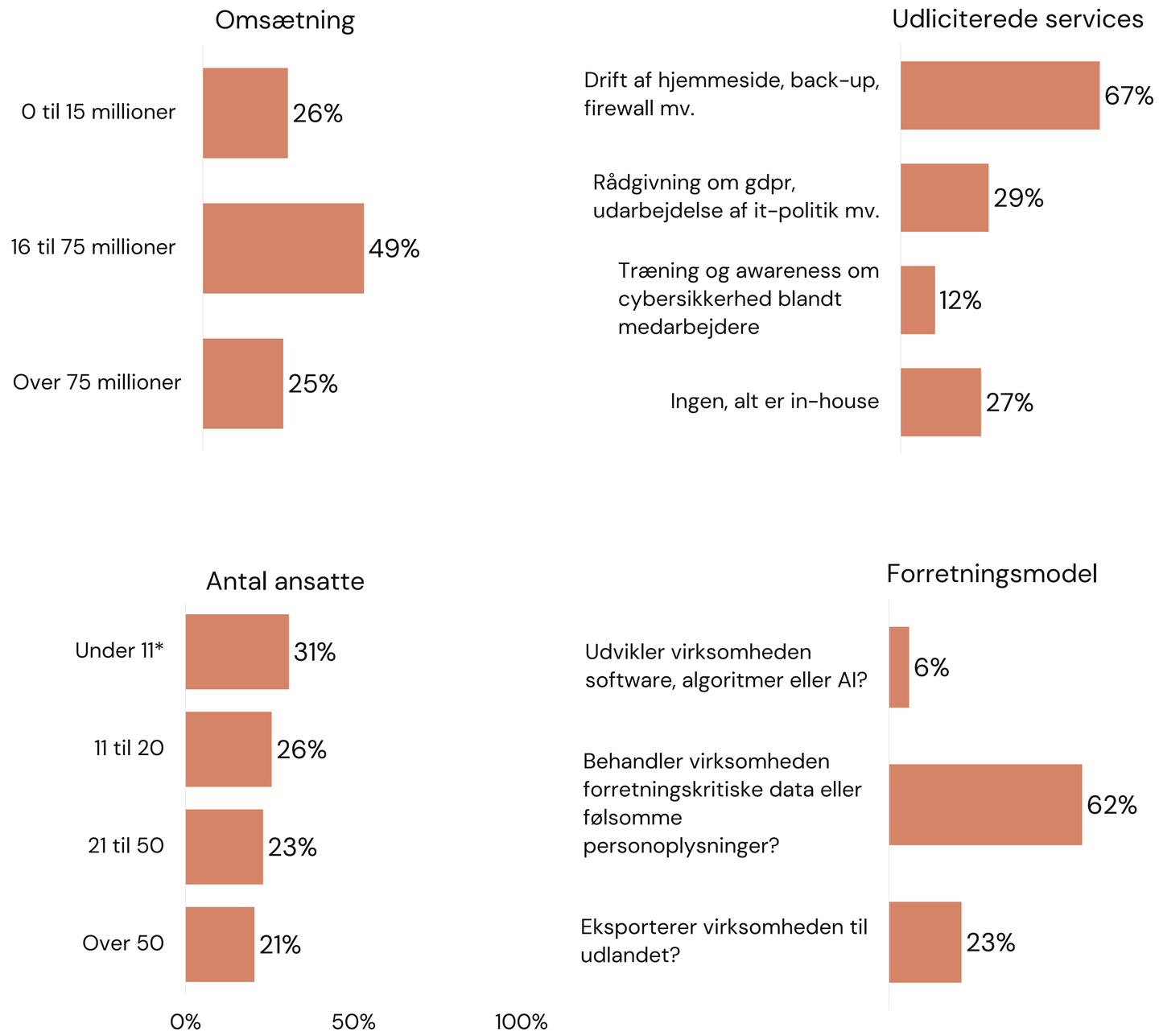


Note: Der indgår 257 bygge og anlægsvirksomheder med i undersøgelsen

Transport & godshåndtering i tal

&#

Figur 18: Andel af virksomheder i transportbranchen indenfor omsætning, udliciterering af services, antal ansatte samt forretningsmodel

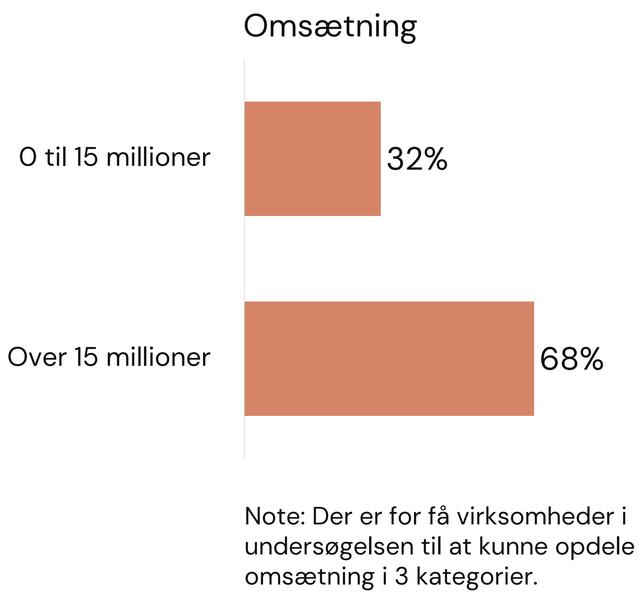


Note: Der indgår 78 transport og godshåndtreingsvikrsomheder med i undersøgelsen

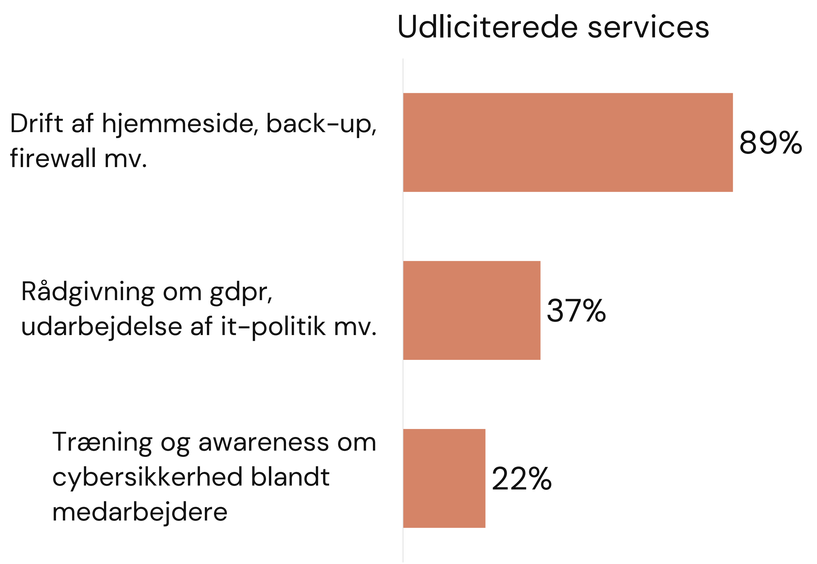
Information & kommunikation i tal

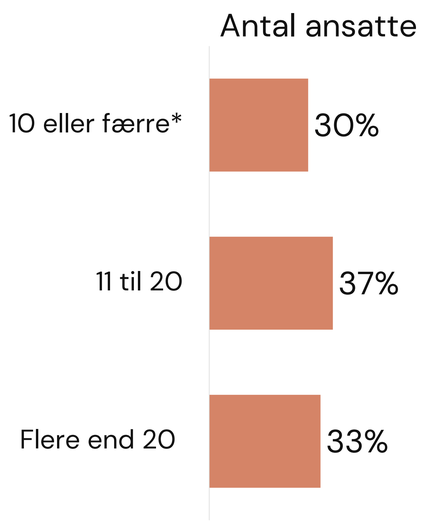
&#

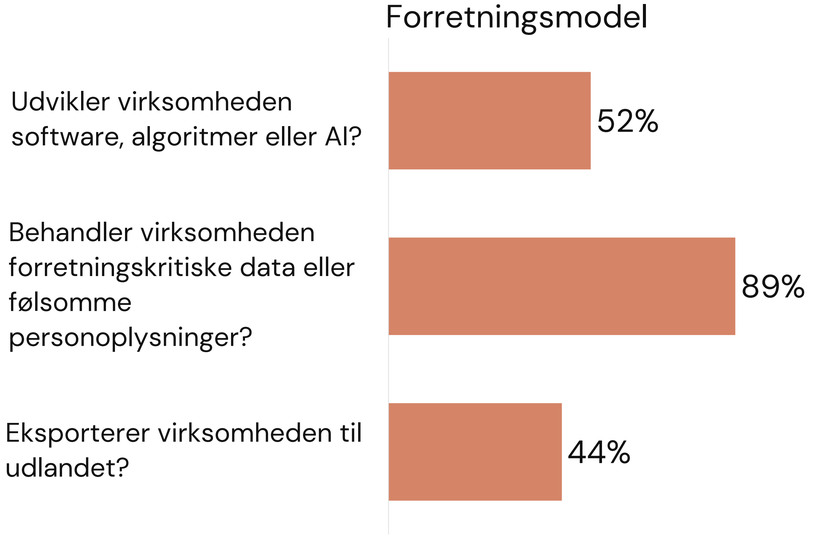
Figur 19: Andel af information- og kommunikationsvirksomheder indenfor omsætning, udliciterering af services, antal ansatte samt forretningsmodel



Note: Der er for få virksomheder i undersøgelsen til at kunne opdele omsætning i 3 kategorier.







Note: Der indgår 27 informations og kommunikationsvirksomheder i undersøgelsen

Rapporten er udarbejdet af 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 de fleste af 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.

Grant Thornton DANMARK

Grant Thornton er et af verdens førende revisions- og rådgivningshuse. Vores IT Risk Assurance & Advisory Services i Gran Thornton Danmark, har mangeårig erfaring inden for cybersikkerhed, risk, governance og compliance.

Vi er funderet på dygtige og engagerede medarbejdere, som indgår i proaktive teams ledet af uformelle partnere. Hermed sikrer vi en høj grad af motivation og tidssvarende kompetencer fra kolleger, der er lige så forskellige som vores kunder.

At andre vil anbefale os som rådgivere og auditører er det største kvalitetsstempel, vi kan få. Derfor værner vi om vores relationer, men vi er samtidig ikke bange for at gå forrest i feltet, når det gavner vores kunder.

Vi er nemlig tæt på deres kerneforretning, tæt på deres passion og tæt på det samfund, som de og vi indgår i.

36 partnere

290 medarbejdere

3 kontorer
– ét i København, ét i Hillerød og ét i Viby Sjælland

Udarbejdet af:
Analyse & Tal F.M.B.A
Hejrevej 34A
2400 København NV
www.ogtal.dk

For mere information kontakt:
Lisbeth Palmhøj Nielsen
lisbeth@ogtal.dk

Databehandling, analyse & tekst:
Nadia Engelst Rostved og Lisbeth Palmhøj Nielsen

Kvalitative interviews og sparring:
Nicolai Elberling fra Grant Thornton

Opdragsgiver:
Industriens Fond
Frederiksgade 17
1265 København K
www.industriensfond.dk

For mere information kontakt:
Nadika Bulathsinhala
nb@industriensfond.dk