

Cybersikkerhed som konkurrencefordel i Danmark

Udarbejdet for Industriens Fond,
maj 2026



Executive summary

Cybertruslen er i dag et grundvilkår, som alle virksomheder må forholde sig til. Danske virksomheder investerer også i stigende omfang i cybersikkerhedstiltag. Tilgangen til at arbejde med cybersikkerhed er dog meget forskellig blandt virksomhederne. Nogle investerer først og fremmest i tekniske løsninger, mens andre også har fokus på at forankre cybersikkerhed bredt i organisationen, bl.a. gennem træning og nye rutiner.

Denne analyse undersøger, hvordan virksomhedernes forskellige tilgange til at investere i cybersikkerhedstiltag hænger sammen med opnåelsen af konkurrencefordele.

Cybersikkerhed styrker virksomhedernes konkurrenceevne

Overordnet viser analysen en klar sammenhæng mellem cybersikkerhedstiltag og styrkede konkurrencefordele. Virksomheder, der arbejder systematisk med en bred vifte af cybersikkerhedstiltag, oplever i højere grad gevinster i form af øget effektivitet, tillid fra kunder og samarbejdspartnere samt styrkede økonomiske resultater. Analysen dokumenterer også, at virksomheder med mange cybersikkerhedstiltag oplever højere vækst i både beskæftigelse og omsætning. Analysen viser samtidig, at tekniske tiltag primært udgør et nødvendigt fundament, men at det først er, når der oveni arbejdes med organisatorisk forankring, træning og kompetenceopbygning, at de fulde gevinster realiseres.

Fire arketyper viser forskellige tilgange og gevinster

Analysen identificerer fire arketyper blandt danske virksomheder, der arbejder med cybersikkerhed. Arketyperne illustrerer forskellige måder, virksomheder arbejder med cybersikkerhed på, og hvordan indsatsen omsættes til konkurrencefordele. Forskellene afspejler både variationer i virksomhedernes prioriteringer, ressourcer og organisatoriske forankring samt de rammer og krav, de opererer under, herunder stigende regulatoriske krav til cybersikkerhed.

Et fortsat fokus på cybersikkerhed er afgørende

Samlet viser analysen, at cybersikkerhedstiltag bidrager til at styrke virksomhedernes konkurrenceevne. Virksomheder kan opnå større gevinster ved at arbejde mere målrettet og helhedsorienteret med cybersikkerhed og ved at integrere indsatsen i organisation, ledelse og kompetencer. Analysen viser samtidig, at virksomheder kan udvikle sig over tid og bevæge sig mod mere værdiskabende tilgange til cybersikkerhed. Det understreger betydningen af et vedvarende og strategisk fokus på cybersikkerhed i virksomhedernes arbejde.

HOVEDRESULTATER



Cybersikkerhed giver virksomheder konkurrencefordele

Virksomheder med flere cybersikkerhedstiltag opnår generelt flere konkurrencefordele både i form af forbedret effektivitet, øget tillid og styrket bundlinje.



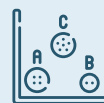
Virksomheder med en høj cybersikkerhedsindsats har større vækst i beskæftigelse og omsætning

Der ses en tydelig tendens til, at virksomheder med mange tiltag har højere vækst end virksomheder med få tiltag.



De største konkurrencefordele opstår, når cybersikkerhed forankres bredt i virksomheden

Tekniske tiltag er et nødvendigt fundament, som ved kombination med forankring samt bred opkvalificering, giver store konkurrencefordele.



Virksomheder kan opdeles i fire arketyper med forskellige profiler for cybersikkerhed og gevinster

Arketyperne synliggør systematiske forskelle i virksomhedernes tilgang til cybersikkerhed og deres opnåede konkurrencefordele.



En målrettet indsats kan løfte virksomheder til et højere niveau af cybersikkerhed og konkurrencefordele

En målrettet indsats for cybersikkerhed i virksomheden hænger sammen med bevægelser mod arketyper med flere konkurrencefordele.

Baggrund og formål med analysen

Gennem Cyberbarometeret er der siden 2022 indsamlet data om danske virksomheders arbejde med cybersikkerhed og de gevinster, de oplever som følge af indsatsen.

Med tre års dataindsamling foreligger der nu et solidt datagrundlag, som gør det muligt at analysere mønstre på tværs af virksomheder og over tid. Denne analyse belyser betydningen af cybersikkerhed for danske virksomheder og har to overordnede formål:

- **For det første** undersøges sammenhængen mellem virksomhedernes cybersikkerhedstiltag og deres konkurrencefordele samt økonomiske udvikling.
- **For det andet** identificerer analysen arketyper, der viser forskellige måder, som virksomhederne arbejder med cybersikkerhed på, og hvordan indsatsen omsættes til konkurrencefordele.

I Cyberbarometeret måles virksomhedernes cybersikkerhedstiltag og oplevede konkurrencefordele på tværs af tre fokusområder og tre dimensioner, som illustreret i figuren til højre.

Cybersikkerhedstiltag dækker både tekniske løsninger, forankring og styring samt rutiner og træning. Det omfatter bl.a. tekniske tiltag som opdatering af systemer og backup samt organisatoriske tiltag som udvikling af politikker, ansvarsplacering og opkvalificering af medarbejdere.

Konkurrencefordele måles på tre dimensioner og dækker bredt over virksomhedernes gevinster. Det omfatter bl.a. øget effektivitet og styrket innovation, øget tillid fra kunder og samarbejdspartnere samt økonomiske resultater, såsom flere kunder og mulighed for højere priser.

Datagrundlaget omfatter mere end 1.200 besvarelser fra virksomheder indsamlet i perioden 2022–2024 og giver dermed et solidt grundlag for at analysere sammenhænge på tværs af virksomheder og over tid.

CYBERSIKKERHEDSTILTAG – 3 FOKUSOMRÅDER



TEKNIK

Tekniske cybersikkerhedstiltag, der bl.a. omfatter løbende opdatering af software, styrket backup og beskyttelse af systemer, brugerkonti og netværk.



FORANKRING OG STYRING

Tiltag omfatter bl.a. at udpege ansvarlige personer for it-sikkerhed, få overblik over virksomhedens data og systemer samt udvikling af politikker og beredskabsplaner for it-sikkerhed og dataanvendelse.



RUTINER OG TRÆNING

Tiltag omfatter bl.a. udvikling af risikovurdering af nye krav til samarbejdspartnere samt opkvalificering af både ansatte samt øverste ledelse i it-sikkerhed og ansvarlig dataanvendelse.

KONKURRENCEFORDELE – 3 DIMENSIONER



EFFEKTIVITET OG NYTÆNKNING

Fordele i form af øget effektivitet og styrket innovation, herunder bedre udnyttelse af nye teknologier, mere effektive arbejdsgange og øget evne til nytænkning.



TILLID

Fordele i form af øget tillid fra centrale interessenter, fx bestyrelse, investorer, kunder og samarbejdspartnere samt styrkede relationer til eksisterende kunder.



BUNDLINJE

Fordele i form af styrket markedsposition og økonomiske resultater, herunder øget kundetiltrækning, differentiering fra konkurrenter og højere priser for produkter/services.



Sammenhæng mellem
cybersikkerhed og
konkurrencefordele

Sådan omsættes cybersikkerhed til konkurrencefordele og indtjening

Effekter af investeringer i cybersikkerhedstiltag

Figuren til højre illustrerer, hvordan investeringer i cybersikkerhed kan omsættes til konkurrencefordele og forretningsmæssige gevinster.

Udgangspunktet er, at cybersikkerhedstiltag ikke alene styrker cybersikkerheden, men også bidrager til organisatoriske forandringer og operationelle forbedringer.

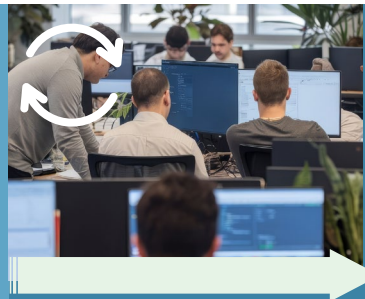
Dette skaber konkurrencefordele for virksomhederne, blandt andet i form af øget effektivitet og styrket tillid fra kunder og samarbejdspartnere. Samlet set kan disse konkurrencefordele understøtte højere vækst og forbedret indtjening.

Der er med afsæt i Cyberbarometeret gennemført en dybdegående analyse af sammenhængen mellem investeringer i cybersikkerhed, hvordan virksomhederne oplever, at det fører til konkurrencefordele, og hvordan det styrker deres økonomiske udvikling. Analyserne udfoldes på de følgende sider.



Cybersikkerhedstiltag

- Implementering af tekniske løsninger
- Etablering af politikker, ansvar, risikostyring, mv.
- Træning og kompetenceopbygning



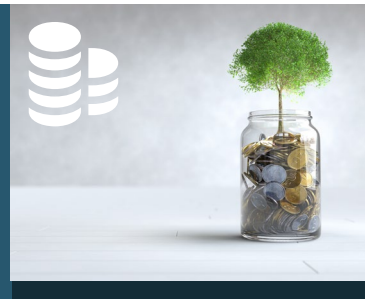
Organisatoriske forandringer og operationelle forbedringer

- Bedre overblik over data, systemer og risici
- Klar ansvarsfordeling og beslutningsprocesser
- Øget sikkerhedsadfærd hos medarbejdere
- Færre nedbrud og sikkerhedshændelser
- Hurtigere håndtering af incidents



Konkurrencefordele

- Øget effektivitet og styrket innovation, fx bedre udnyttelse af nye teknologier og mere effektive arbejdsgange
- Øget tillid fra bestyrelse, kunder og samarbejdspartnere
- Styrket bundlinje og økonomiske resultater, fx øget kundetiltrækning, differentiering fra konkurrenter og højere priser



Styrket vækst i omsætning og beskæftigelse

- Øget salg og eksport
- Lavere omkostninger (fx nedetid, databrud)
- Effektiv og stabil drift
- Bedre fundament for skalerbar vækst

Cybersikkerhedstiltag: Sammenhæng mellem cybersikkerhedstiltag og konkurrencefordele

Klar sammenhæng mellem cybersikkerhedstiltag og konkurrencefordele

Analysen viser, at der er en sammenhæng mellem investeringer i cybersikkerhedstiltag og oplevede konkurrencefordele, som illustreret i figuren til højre.

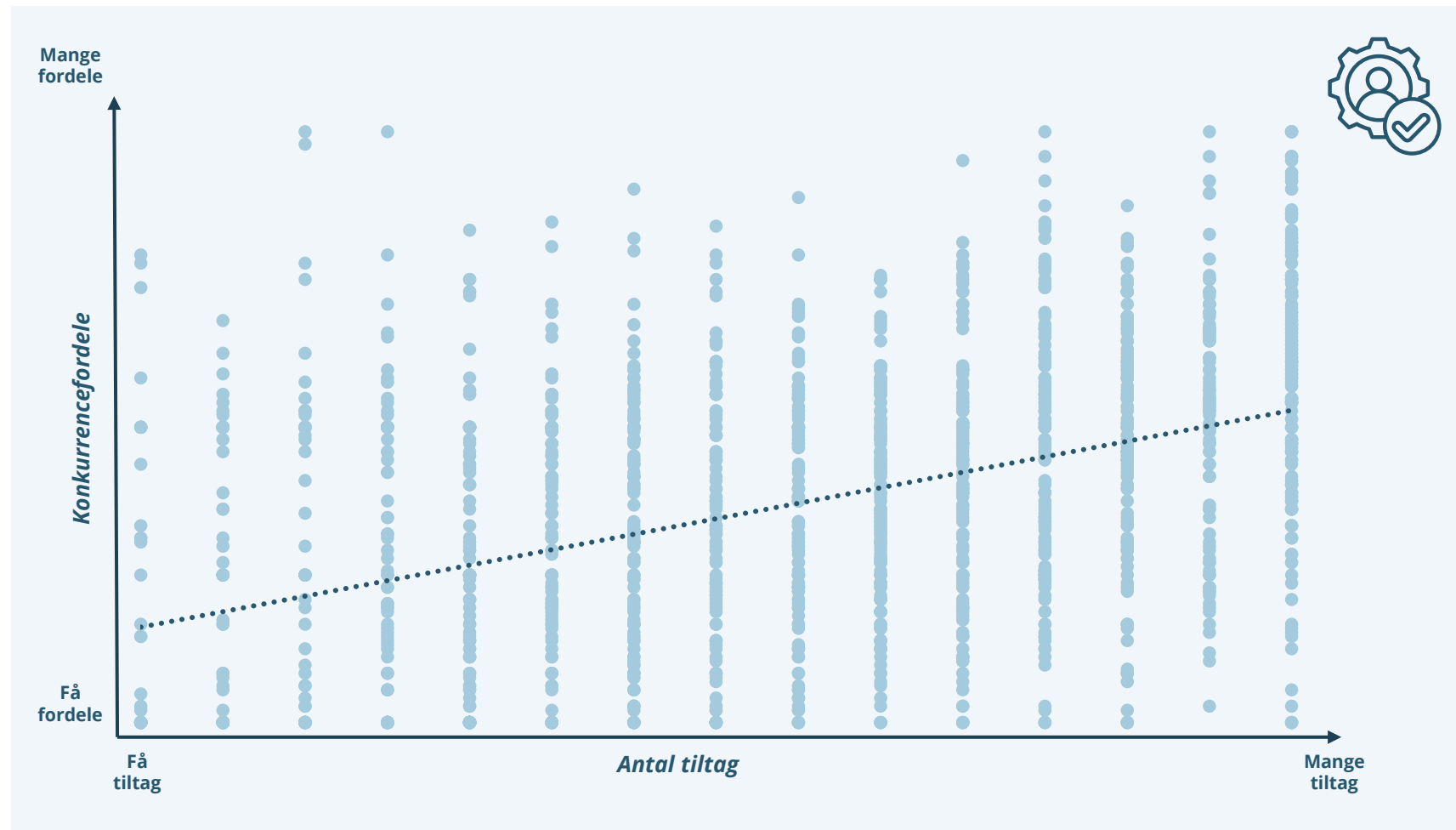
Analysen er baseret på data fra Cyberbarometeret. Virksomheder er blevet spurgt til, om de har implementeret en række forskellige cybersikkerhedstiltag og deres oplevede konkurrencefordele i form af øget effektivitet, øget tillid og styrket bundlinje.

Hver prik repræsenterer en virksomhed, mens den indtegnede regressionslinje viser den overordnede tendens i data.

Der ses en klar positiv sammenhæng mellem antallet af cybersikkerhedstiltag og virksomhedernes konkurrencefordele.

Analysen viser, at et højere ambitionsniveau for cybersikkerhed hænger sammen med stærkere konkurrencefordele.

Sammenhæng mellem cybersikkerhedstiltag og konkurrencefordele



Kilde: IRIS Group på baggrund af Cyberbarometeret.
Note: N = 1.198 virksomheder

Forandringer: Hvilke cybersikkerhedstiltag skaber konkurrencefordele?

Cybersikkerhedstiltag giver konkurrencefordele

Som vist på forrige side er der en klar sammenhæng mellem cybersikkerhedstiltag og konkurrencefordele. I denne analyse ser vi nærmere på, hvordan de forskellige typer af tiltag hænger sammen med virksomhedernes konkurrencefordele.

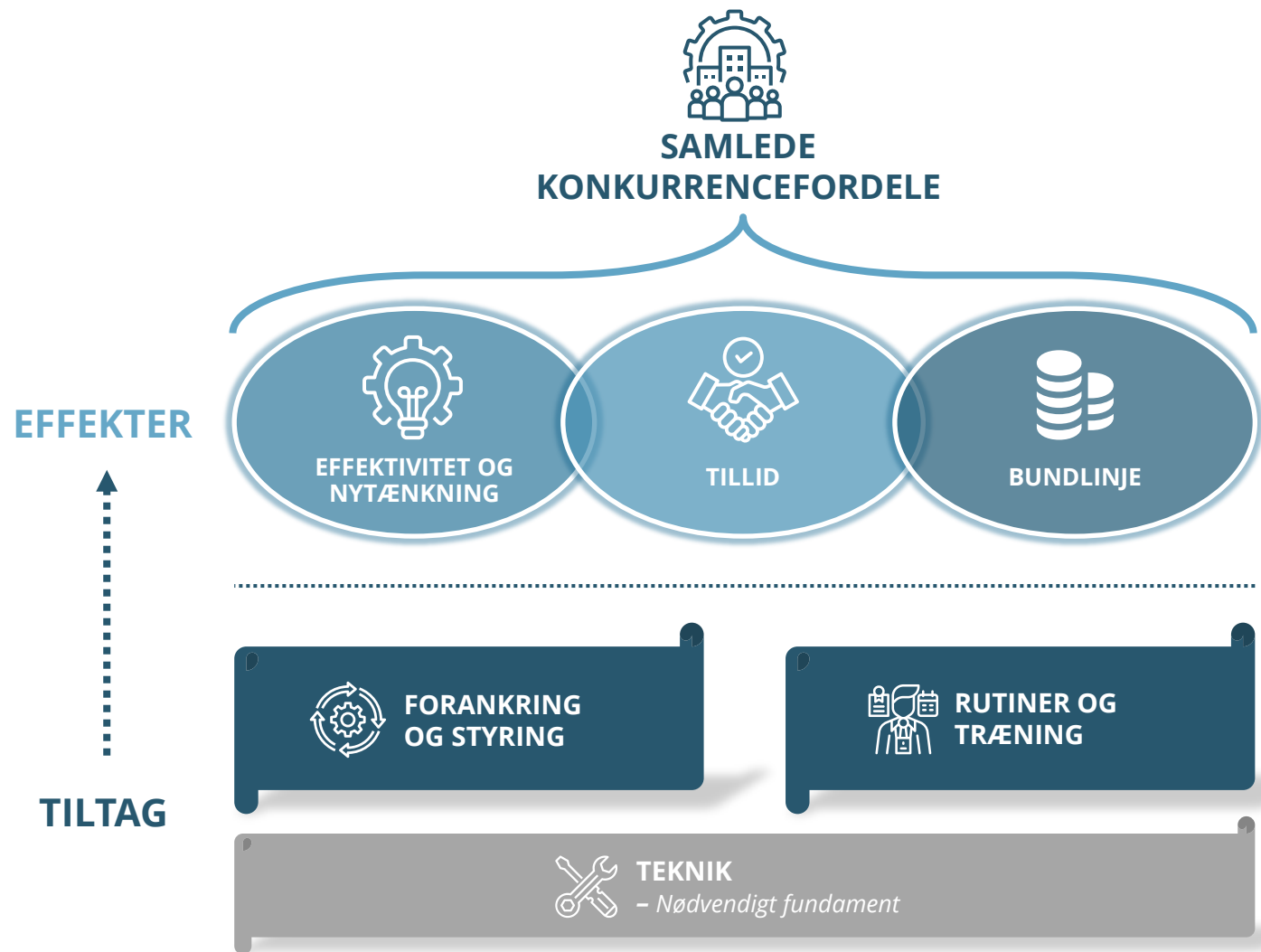
Analysen viser, at alle typer af cybersikkerhedstiltag er positivt forbundet med konkurrencefordele – en øget indsats inden for cybersikkerhed bidrager altså generelt til flere konkurrencefordele.

Analysen viser samtidig, at tekniske tiltag udgør et nødvendigt fundament, men ikke i sig selv er tilstrækkelige til at skabe de største gevinster. Virksomheder, der alene arbejder med tekniske løsninger, opnår ikke samme udbytte som virksomheder, der arbejder bredere med cybersikkerhed.

De største gevinster opstår, når tekniske tiltag kombineres med organisatoriske indsatser, herunder forankring og styring samt udvikling af rutiner og træning af medarbejdere. Når tiltag inden for alle tre fokusområder kombineres, oplever virksomheder store konkurrencefordele.

Sammenhængene er statistisk signifikante på tværs af de fleste typer af tiltag og dimensioner af konkurrencefordele. Styrken af sammenhængene varierer dog, hvilket peger på, at virksomheder i gennemsnit opnår flere gevinster, men ikke i samme omfang.

1. Se baggrundsrapport for en nærmere gennemgang af metode og resultater.



Værdiskabelse: Udvikling i beskæftigelse for virksomheder, der har implementeret cybertiltag

Større vækst i beskæftigelse blandt virksomheder med mange cybertiltag

For at belyse betydningen af cybersikkerhed for virksomhedernes vækst er der gennemført en analyse af, hvordan antallet af cybersikkerhedstiltag hænger sammen med udviklingen i virksomhedernes beskæftigelse.

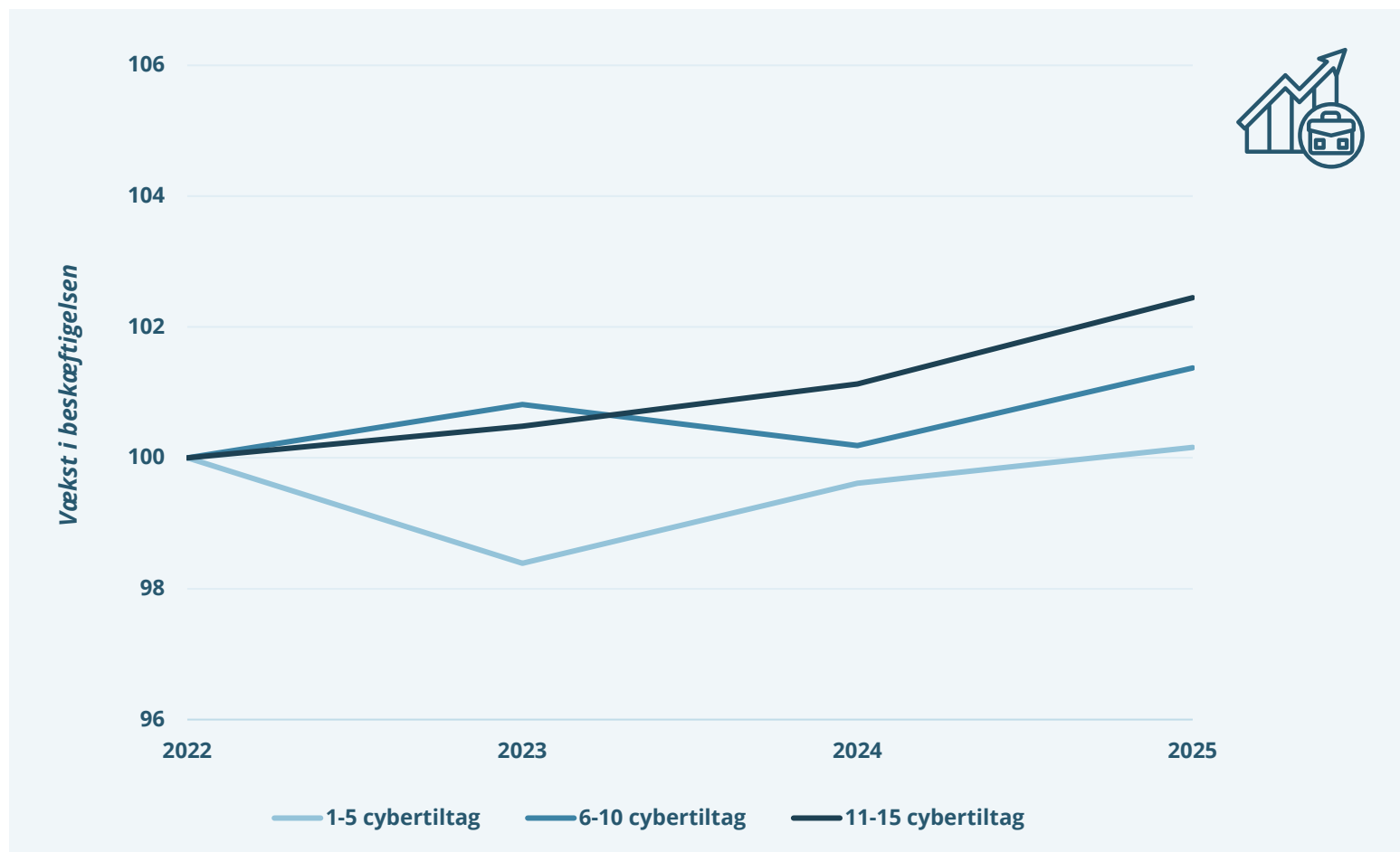
Analysen omfatter virksomheder, der har besvaret Cyberbarometeret i 2022, opdelt i tre grupper efter antal implementerede tiltag. I figuren følges virksomhedernes udvikling i antal ansatte frem mod 2025.

Udviklingen er opgjort som en indekseret gennemsnitsudvikling med udgangspunkt i virksomhedernes beskæftigelse i 2022.

Resultaterne viser en klar tendens til, at virksomheder med flere cybersikkerhedstiltag har en højere vækst i antal ansatte over tid.

Virksomheder med mange tiltag (11-15) har haft en samlet vækst i beskæftigelsen på lidt over 2 pct. siden 2022, mens virksomheder med få tiltag (1-5) har haft en stort set uændret udvikling i samme periode. Virksomheder med et mellemniveau af tiltag ligger mellem de to grupper.

Beskæftigelsesudvikling blandt virksomheder med cybersikkerhedstiltag (2022=100)



Kilde: IRIS Group på baggrund af Cyberbarometeret.
Note: N = 559 virksomheder

Værdiskabelse: Udvikling i omsætning for virksomheder, der har implementeret cybertiltag

Virksomheder med mange cybertiltag har en stor vækst i omsætning

Der er ligeledes gennemført en analyse af sammenhængen mellem cybersikkerhedstiltag og virksomhedernes omsætningsudvikling.

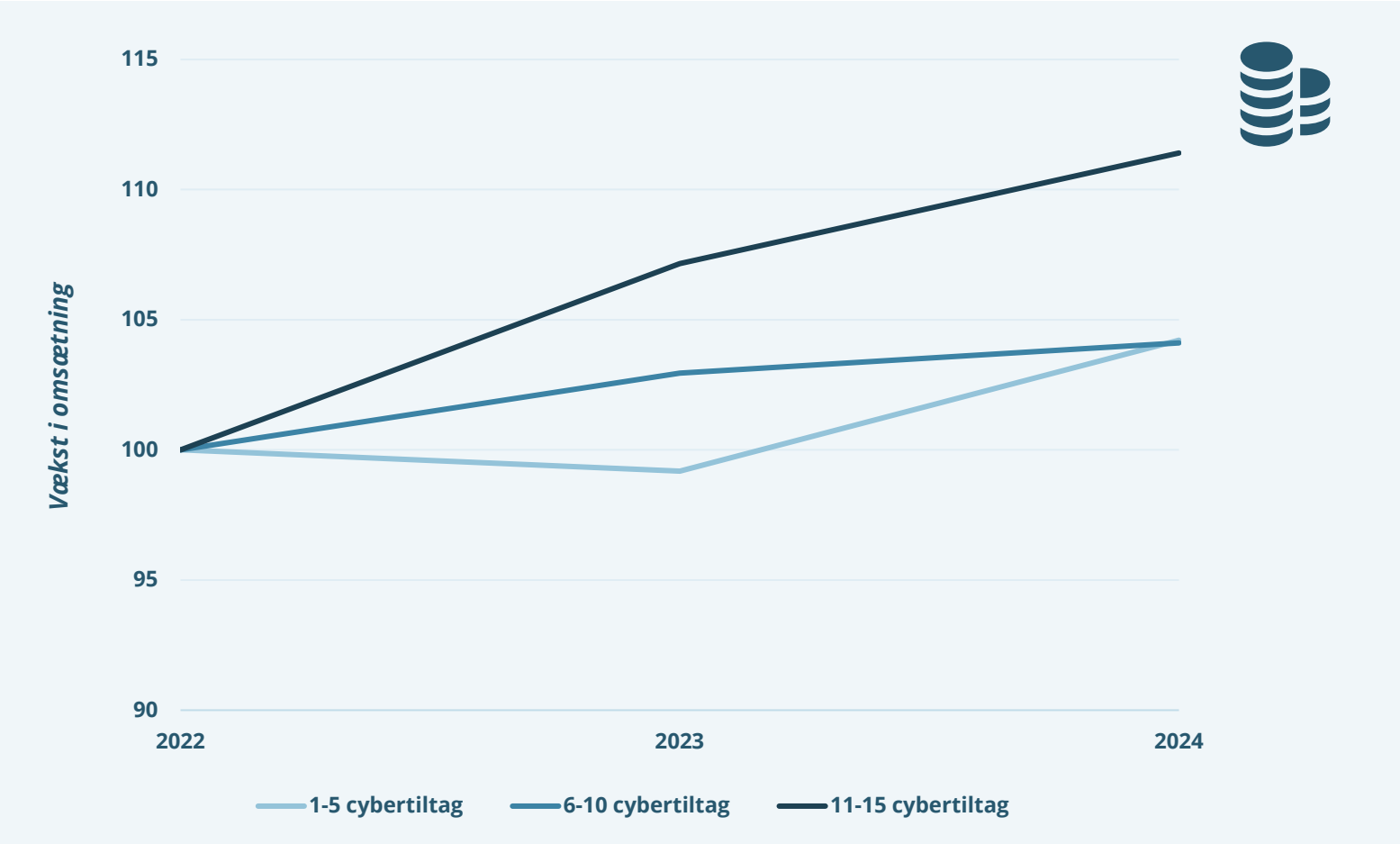
Analysen tager udgangspunkt i samme inddeling af virksomhederne efter antal implementerede tiltag og følger deres omsætningsudvikling frem mod 2024.

Resultaterne viser en tendens til, at virksomheder med flere cybersikkerhedstiltag også har haft en højere vækst i omsætningen.

Virksomheder med mange tiltag (11-15) har haft en vækst på omkring 11 pct., mens virksomheder med færre tiltag har haft en mere afdæmpet udvikling. Der ses dog ikke væsentlige forskelle mellem virksomheder med få (1-5) og flere tiltag (6-10).

Omsætning påvirkes af en række forhold, og resultaterne skal derfor fortolkes med forsigtighed. Cybersikkerhed er ét blandt flere forhold, der har betydning for virksomhedernes økonomiske udvikling.

Udvikling i omsætning blandt virksomheder med cybersikkerhedstiltag (2022=100)



Kilde: IRIS Group på baggrund af Cyberbarometeret.
Note: N = 492 virksomheder

De fire arketyper



Analysen har identificeret fire arketyper blandt danske virksomheder

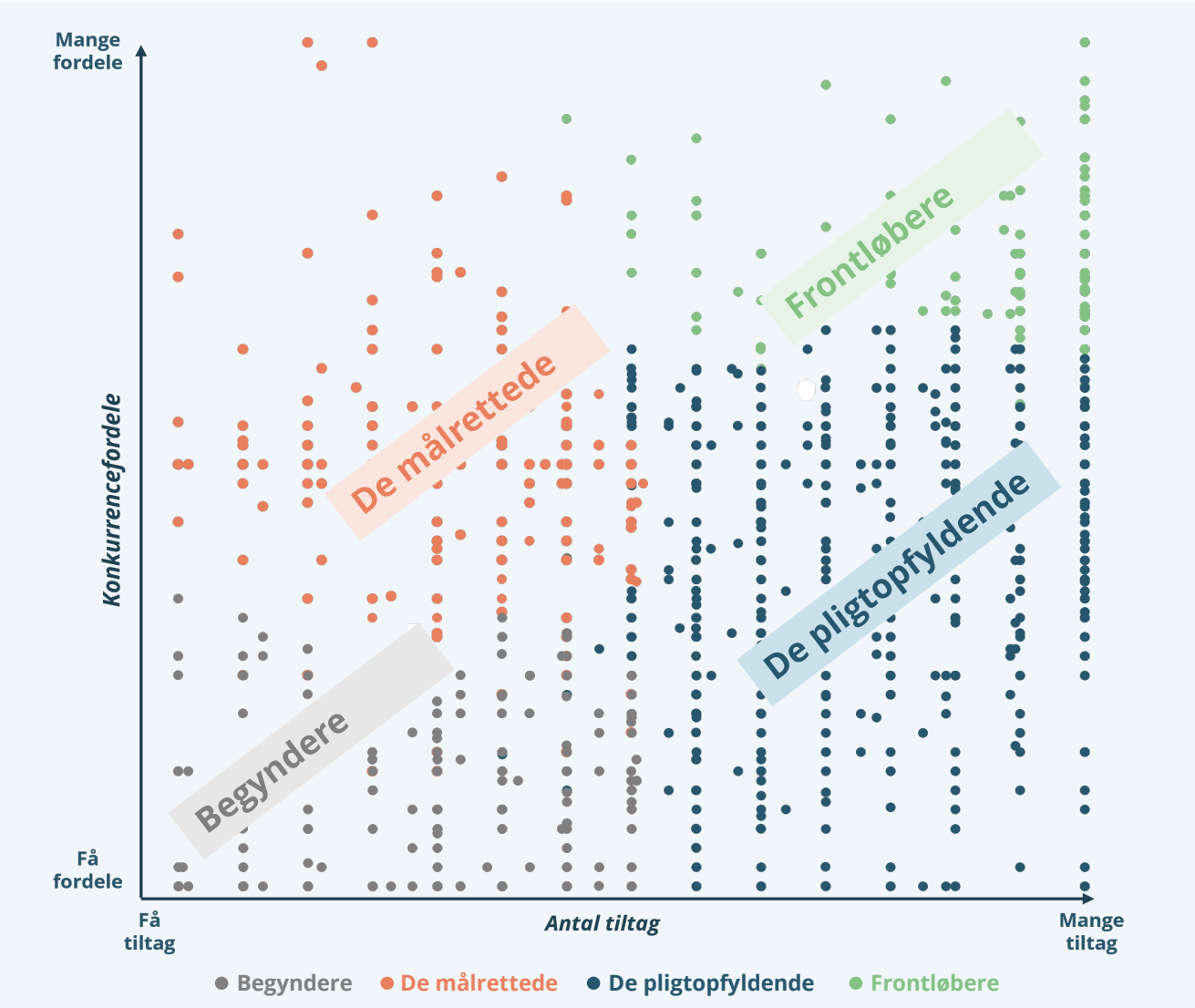
Fire arketyper

Denne del af analysen har til formål at identificere arketyper blandt virksomheder baseret på deres arbejde med cybersikkerhed og konkurrencefordele med henblik på bedre at forstå forskelle mellem virksomheder og målrette indsatser.

Analysen bygger på data fra Cyberbarometeret 2022–2024, hvor virksomhederne er grupperet efter omfanget af cybersikkerhedstiltag og konkurrencefordele ved hjælp af en statistisk klyngeanalyse.

I analysen identificeres fire arketyper, der er illustreret i figuren til højre, hvor virksomheder er inddelt efter antal cybersikkerhedstiltag (x-akse) og konkurrencefordele (y-akse). De fire arketyper kan beskrives som:

- Frontløbere:** Virksomheder, der har implementeret mange tiltag og oplever store konkurrencefordele.
- De pligtopfyldende:** Virksomheder, der har implementeret flere tiltag, men mangler at opleve store konkurrencefordele.
- De målrettede:** Virksomheder, der har implementeret få til nogle tiltag, men som oplever flere konkurrencefordele.
- Begyndere:** Virksomheder, der har implementeret færrest tiltag og i begrænset omfang oplever konkurrencefordele.



Kilde: IRIS Group på baggrund af Cyberbarometeret.
Note: N = 1.198 virksomheder

ARKETYPER

Hvordan de fire arketyper adskiller sig fra hinanden

De fire arketyper

De to figurer til højre illustrerer, hvordan de fire arketyper adskiller sig både med hensyn til implementerede cybersikkerhedstiltag og oplevede konkurrencefordele.

Begyndere arbejder med et begrænset antal tiltag. Indsatsen er relativt koncentreret inden for tekniske tiltag og kun få arbejder med tiltag inden for kategorien "rutiner og træning". Det er samtidig kun få begyndere, der oplever konkrete gevinster af deres indsats.

De målrettede har gennemført cybersikkerhedstiltag på nogenlunde samme niveau som begynderne, men opnår i betydeligt større omfang konkurrencefordele. Omkring halvdelen oplever effektivitetsgevinster og øget tillid fra kunder og samarbejdspartnere, mens omkring en fjerdedel oplever effekter på bundlinjen.

De pligtopfyldende har implementeret mange tiltag både inden for teknik samt forankring og styring. Omkring 60 pct. af de pligtopfyldende oplever forbedringer i både effektivitet og tillid, men andelen, der oplever effekter på bundlinjen, er forholdsvis lav.

Frontløbere skiller sig ud ved at have mange tiltag inden for både teknik, forankring og styring samt rutiner og træning. Næsten alle frontløbere opnår samtidig mange gevinster – både i forhold til effektivitet, tillid samt styrket bundlinje.

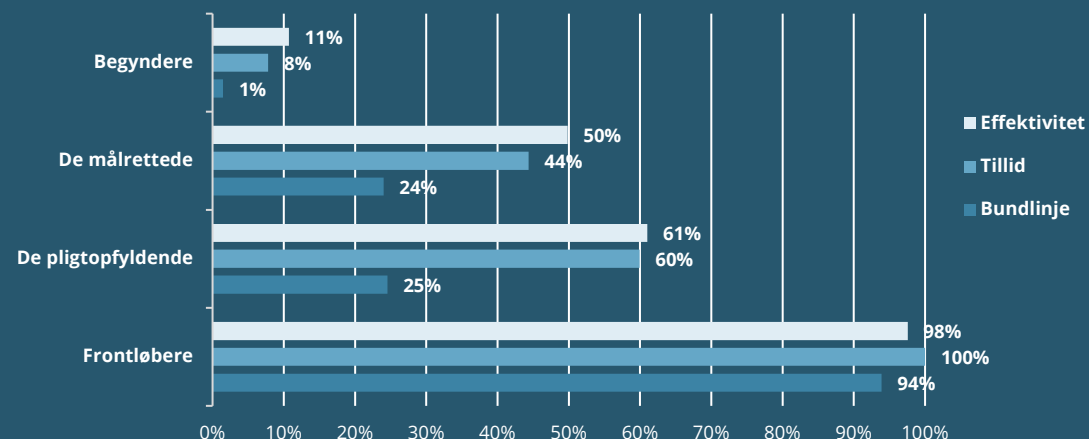
De fire arketyper illustrerer en tydelig progression, hvor implementering af flere tiltag giver flere konkurrencefordele.

Cybersikkerhed & konkurrencefordele

Antal implementerede cybersikkerhedstiltag



Andel, der oplever konkurrencefordele



Kilde: IRIS Group på baggrund af Cyberbarometeret.
Note: N = 1.198 virksomheder

ARKETYPE 1

Begyndere

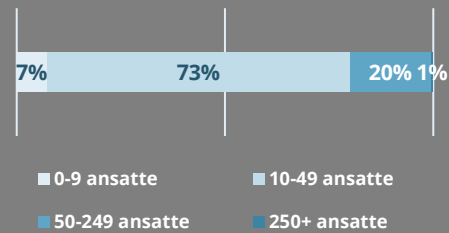
Arketypen 'Begyndere' er virksomheder, der har implementeret få cybersikkerhedstiltag og kun i meget begrænset omfang oplever konkurrencefordele. De har typisk kun implementeret tekniske tiltag, mens der i mindre grad er arbejdet med forankring og styring samt rutiner og træning.

Begyndere opfatter ikke cybersikkerhed som et forretningskritisk område. De er typisk mindre virksomheder med få ressourcer til it og cybersikkerhed. Over halvdelen af virksomhederne (54 pct.) har ikke dedikerede it-medarbejdere. Få virksomheder bruger standarder (4 pct.), hvilket indikerer, at virksomhederne i mindre grad arbejder med formaliserede processer og strukturer. Endelig har lidt under halvdelen (43 pct.) eksportaktiviteter.

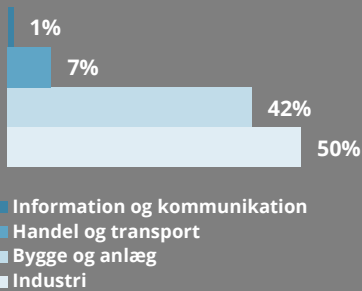
Deres risikoforståelse for konsekvenserne af cybersikkerhed er lav, og investeringer i tiltag sker derfor ofte først, når virksomhederne mødes af konkrete eksterne krav fra kunder og samarbejdspartnere eller som reaktion på hændelser.

Arketypens karakteristika

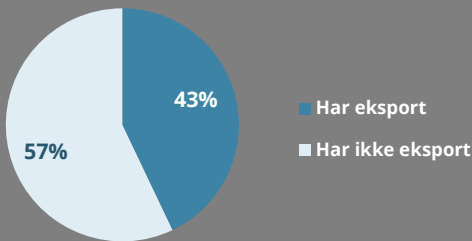
Virksomhedsstørrelse



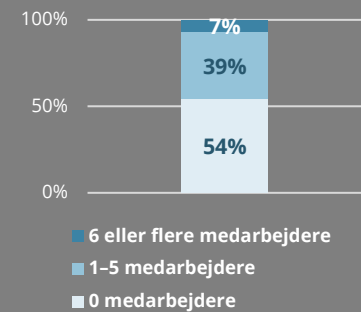
Brancher



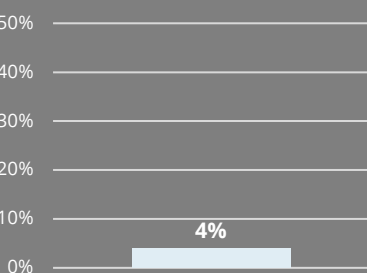
Eksport



Dedikerede medarbejdere til it-drift



Brug af standarder

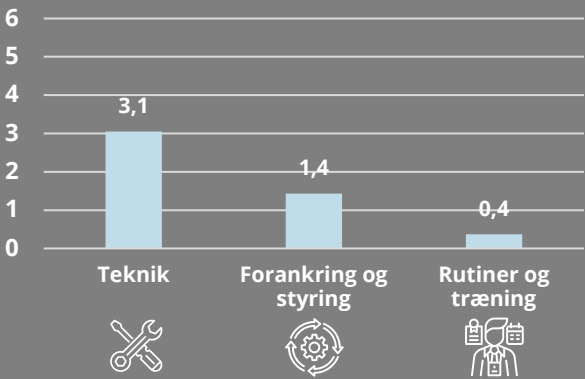


Bestyrelse med eksterne kompetencer

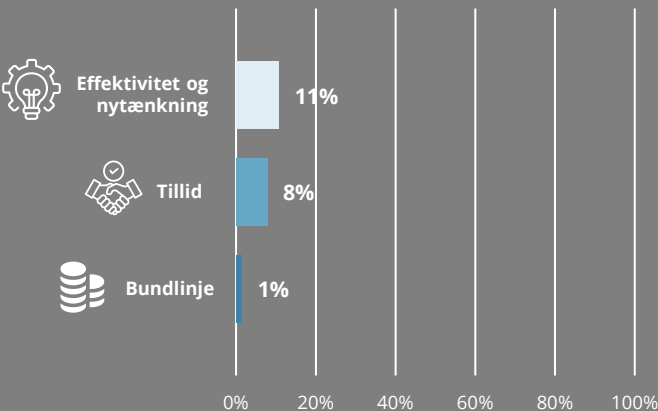


Cybersikkerhed & konkurrencefordele

Antal implementerede cybersikkerhedstiltag



Andel, der oplever konkurrencefordele



Kilde: IRIS Group på baggrund af Cyberbarometeret.
Note: N = 205 virksomheder

ARKETYPE 2

De målrettede

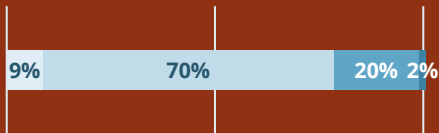
Arketypen 'De målrettede' består af virksomheder med et moderat niveau af cybersikkerhedstiltag og relativt høje oplevede konkurrencefordele. De har implementeret en række tiltag på tværs af både tekniske og organisatoriske områder, men bevidst i et mere begrænset omfang.

De målrettede er typisk mindre virksomheder med et begrænset ressourcegrundlag, som arbejder selektivt med cybersikkerhed ud fra en klar cost-benefit-betragtning. Cybersikkerhed ses som et middel til at understøtte forretningen, og indsatsen fokuserer oftest på tiltag, der kan dokumenteres og synliggøres over for kunder. De er typisk virksomheder mellem 10-49 ansatte, hvor knap to tredjedele har dedikerede it-medarbejdere.

Motivationen er tæt koblet til konkrete forretningsmæssige gevinster, hvor cybersikkerhed anvendes til at skabe en konkurrencefordel – enten ved at styrke virksomhedens position over for konkurrenter eller som adgang til nye markeder med specifikke krav.

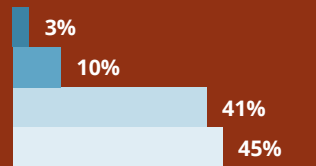
Arketypens karakteristika

Virksomhedsstørrelse



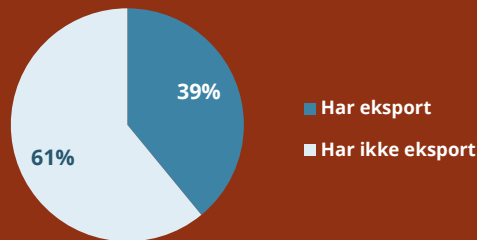
■ 0-9 ansatte
■ 10-49 ansatte
■ 50-249 ansatte
■ 250+ ansatte

Brancher



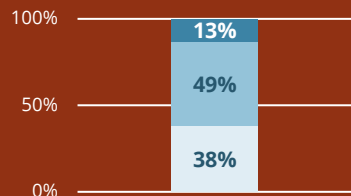
■ Information og kommunikation
■ Handel og transport
■ Bygge og anlæg
■ Industri

Eksport



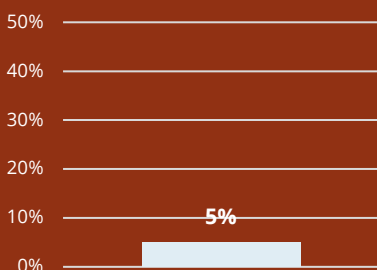
■ Har eksport
■ Har ikke eksport

Dedikerede medarbejdere til it-drift



■ 6 eller flere medarbejdere
■ 1-5 medarbejdere
■ 0 medarbejdere

Brug af standarder



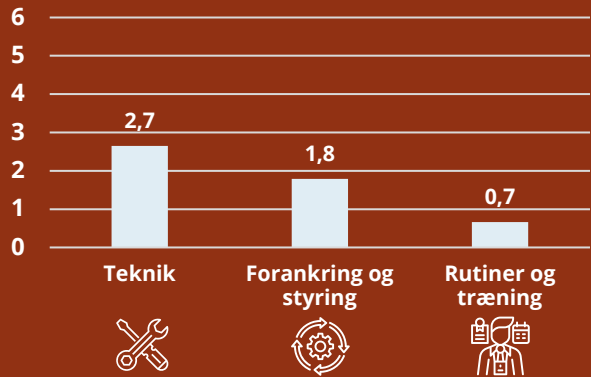
Bestyrelse med eksterne kompetencer



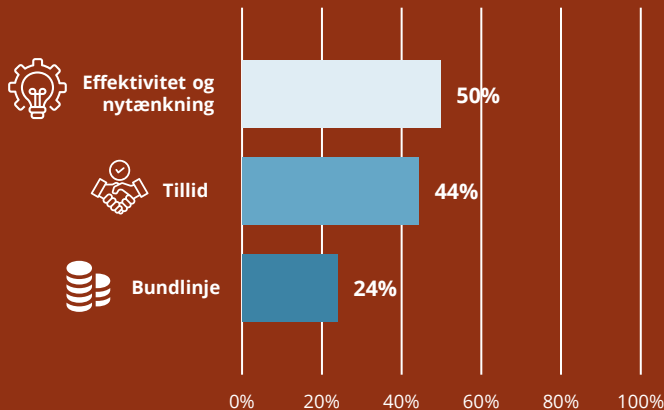
■ Har ikke bestyrelse
■ Bestyrelse primært med ejere eller direktion
■ Bestyrelse med eksterne kompetencer

Cybersikkerhed & konkurrencefordele

Antal implementerede cybersikkerhedstiltag



Andel, der oplever konkurrencefordele



ARKETYPE 3

De pligtopfyldende

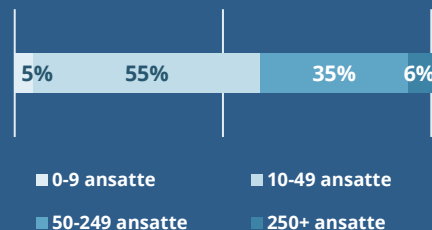
Arketypen 'De pligtopfyldende' består af virksomheder med et relativt højt niveau af cybersikkerhedstiltag, men mere moderate oplevede konkurrencefordele. De har implementeret mange tiltag, der både dækker tekniske løsninger og organisatoriske tiltag med fokus på forankring og styring samt rutiner og træning.

De pligtopfyldende er typisk lidt større virksomheder, hvor stor andel (62 pct.) har eksportaktiviteter. Der er ligeledes en høj andel af virksomhederne (72 pct.), som har en bestyrelse med eksterne kompetencer.

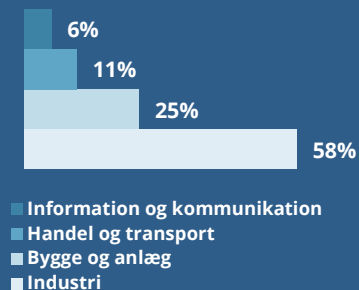
De pligtopfyldende opererer typisk på regulerede markeder, hvor en høj grad af cybersikkerhed er en nødvendighed ('licence to operate'). Det er formentlig en del af forklaringen på, at disse virksomheder ikke oplever så udtalte konkurrencefordele til trods for relativt omfattende investeringer i cybersikkerhedstiltag.

Arketypens karakteristika

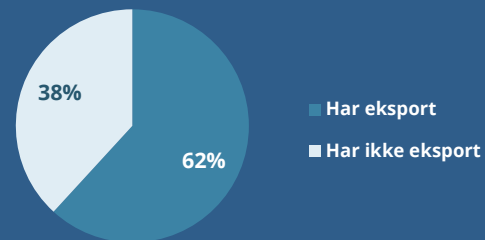
Virksomhedsstørrelse



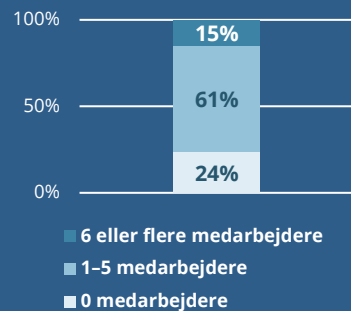
Brancher



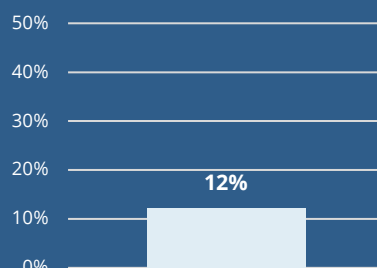
Eksport



Dedikerede medarbejdere til it-drift



Brug af standarder

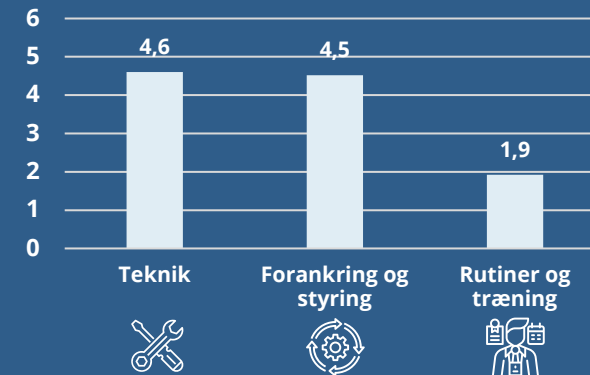


Bestyrelse med eksterne kompetencer

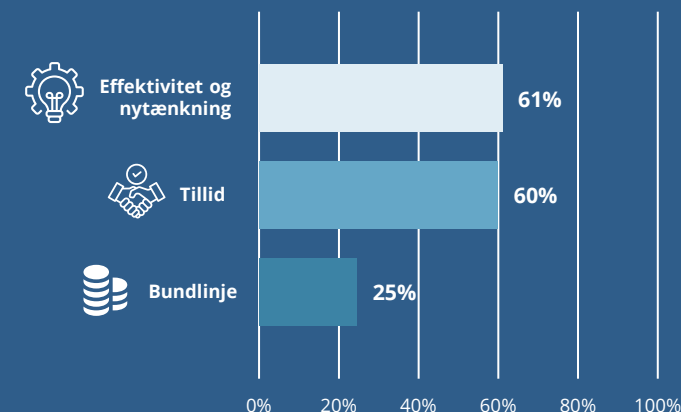


Cybersikkerhed & konkurrencefordele

Antal implementerede cybersikkerhedstiltag



Andel, der oplever konkurrencefordele



ARKETYPE 4

Frontløbere

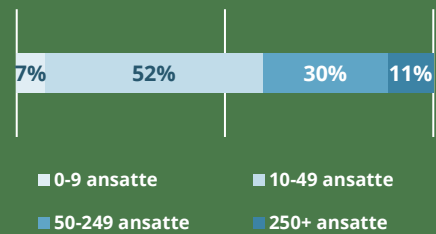
Arketypen 'Frontløbere' består af virksomheder med et højt niveau af både cybersikkerhedstiltag og oplevede konkurrencefordele. De arbejder systematisk med både teknik, forankring og styring samt rutiner og træning.

Deres motivation er en kombination af regulering og risikostyring, men de adskiller sig fra de andre arketyper ved at have en strategisk ambition om at være 'frontrunner'. De ser i højere grad cybersikkerhed som et element, der kan styrke virksomhedens drift og markedsposition.

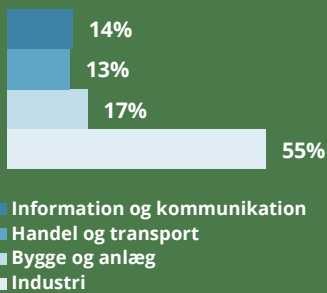
Frontløbere er kendetegnet ved at være større og modne virksomheder, der arbejder proaktivt med at omsætte styrket cybersikkerhed til konkurrencefordele. En høj andel af virksomhederne (72 pct.) har en bestyrelse med eksterne kompetencer, som understøtter en langsigtet udvikling med at gøre cybersikkerhed til en konkurrencefordel. Dertil anvender frontløbere i højere grad standarder (26 pct.), hvilket afspejler en højere organisatorisk modenhed, og at de generelt arbejder struktureret med udviklingen af flere dele af deres forretning.

Arketypens karakteristika

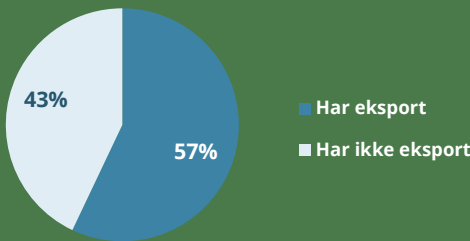
Virksomhedsstørrelse



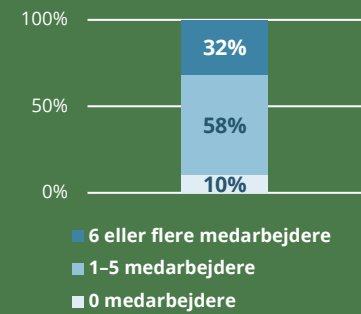
Brancher



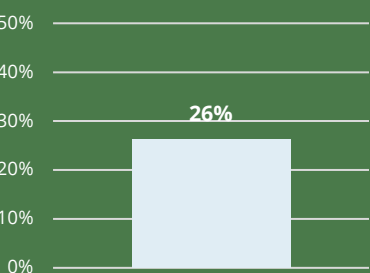
Eksport



Dedikerede medarbejdere til it-drift



Brug af standarder

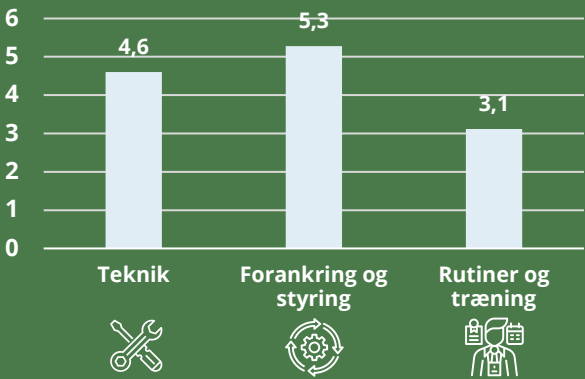


Bestyrelse med eksterne kompetencer

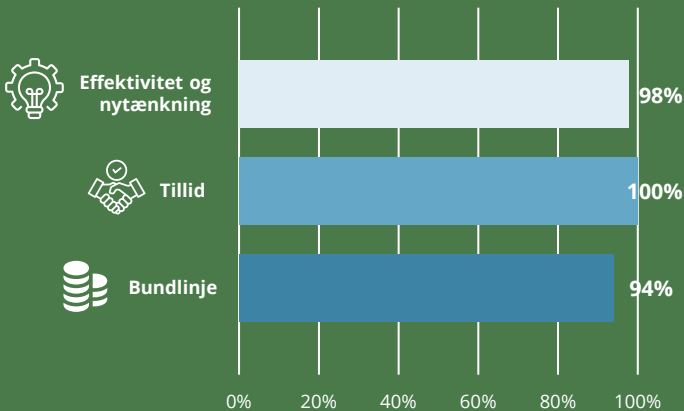


Cybersikkerhed & konkurrencefordele

Antal implementerede cybersikkerhedstiltag



Andel, der oplever konkurrencefordele



Kilde: IRIS Group på baggrund af Cyberbarometeret.
Note: N= 164 virksomheder

Alle virksomheder kan rykke sig, når de arbejder med cybersikkerhed

Flere veje mod en stærkere arketype

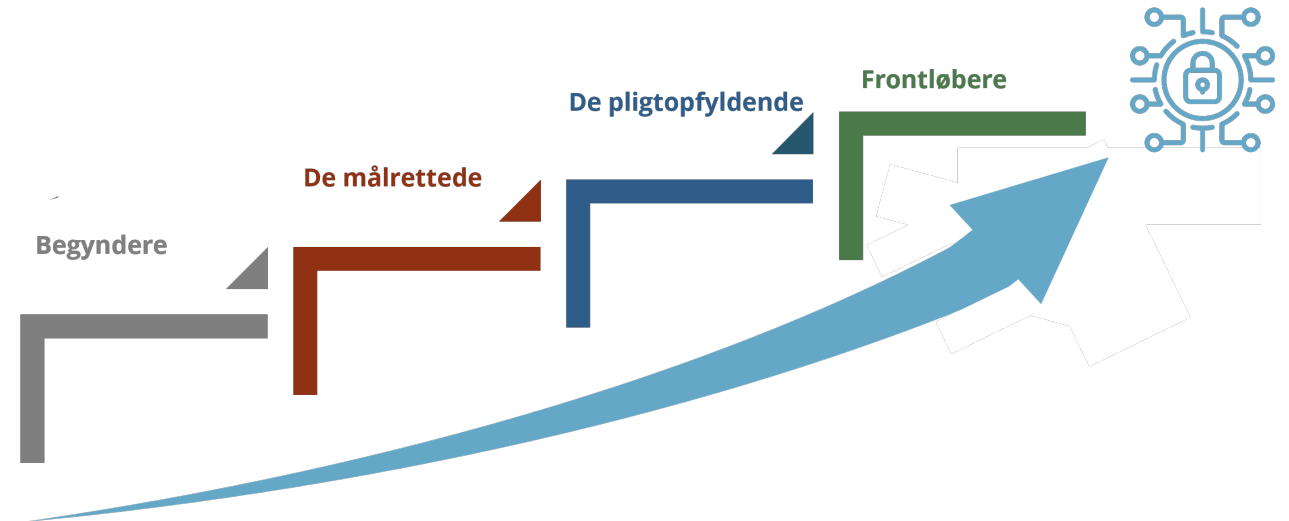
For at vurdere, om virksomheder over tid kan styrke deres arbejde med cybersikkerhed og bevæge sig mod arketyper med flere konkurrencefordele, er der gennemført en progressionsanalyse baseret på virksomheder, der har deltaget i Cyberbarometeret flere gange i perioden 2022–2024.

Analysen viser, at virksomheder ikke er fastlåst i én arketype

Virksomheder, der arbejder systematisk med cybersikkerhed, kan udvikle deres tilgang og bevæge sig mod arketyper, der i højere grad opnår konkurrencefordele i form af øget effektivitet, tillid og forbedrede forretningsmæssige resultater.

Vejene til et højt niveau af cybersikkerhed og konkurrencefordele er forskellige fra virksomhed til virksomhed. For mange er der tale om en gradvis opbygning af kompetencer, struktur og forankring i organisationen. Det indebærer, at virksomheder kan arbejde med de elementer, der er mest relevante for deres udgangspunkt, fx organisering og styring eller opbygning af kompetencer og rutiner, og derigennem styrke deres cybersikkerhedsindsats og opnå flere konkurrencefordele.

Knap en fjerdedel af virksomhederne bevæger sig mod en stærkere arketype i analysen. Analysen viser dog også, at en nogenlunde tilsvarende andel virksomheder bevæger sig i den modsatte retning og skifter til arketyper med et lavere niveau af konkurrencefordele. Det understreger, at udviklingen ikke er lineær, og at resultaterne bør fortolkes med en vis forsigtighed.



Opsamling og anbefalinger til at styrke virksomhedernes arbejde med cybersikkerhed

Analysen dokumenterer, at cybersikkerhedstiltag er en kilde til konkurrencefordele og værdiskabelse

Virksomheder, der arbejder systematisk og bredt med cybersikkerhed, opnår i højere grad gevinster i form af øget effektivitet, innovation, tillid og bedre forretningsmæssige resultater.

De største gevinster opstår ikke af tekniske tiltag alene, men når cybersikkerhed forankres bredt i organisationen og kobles til ledelse, styring, rutiner og kompetencer. Samtidig viser analysen, at virksomheder arbejder forskelligt med cybersikkerhed. De fire arketyper illustrerer, at der ikke er én entydig vej frem, men en skræddersyet og målrettet indsats kan løfte virksomheder mod højere niveauer af cybersikkerhed og stærkere konkurrencefordele.

Analysen viser samtidig, at arbejdet med cybersikkerhed i virksomheder bør ses som en løbende udviklingsproces, hvor den enkelte virksomhed gradvist bygger videre på og styrker sit cybersikkerhedsniveau. Resultaterne peger dermed på en række centrale opmærksomhedspunkter for virksomhedernes videre arbejde:

- **Udbyg indsatsen fra teknik til organisatorisk forankring**

Tekniske tiltag er et nødvendigt fundament, men de største gevinster opnås først, når cybersikkerhed integreres i ledelse, styring, rutiner og kompetencer på tværs af organisationen.

- **Arbejd systematisk på tværs af alle tre dimensioner**

Virksomheder, der kombinerer tekniske løsninger med stærk forankring og løbende træning, opnår markant større gevinster. En balanceret indsats på tværs af indsatsområder er afgørende.

- **Potentiale i at koble cybersikkerhed til forretningsmål**

De mest modne virksomheder omsætter cybersikkerhed til konkrete gevinster i form af effektivitet, tillid og bundlinje. Indsatsen bør derfor kobles til klare forretningsmæssige mål og KPI'er.

- **Arbejd aktivt med at løfte modenhedsniveauet over tid**

Analysen viser, at virksomheder kan bevæge sig mellem arketyperne og opnå flere konkurrencefordele. Det kræver, at de tager afsæt i deres nuværende niveau og løbende udvikler deres tilgang til cybersikkerhed.



IRIS GROUP

CHRISTIANS BRYGGE 28, 1. SAL | DK-1559 KØBENHAVN V

IRISGROUP@IRISGROUP.DK | WWW.IRISGROUP.DK