

Cybersikkerhed i erhvervslivet



Indhold

Nøgleresultater	2
Baggrund og formål	3
Virksomhedernes generelle krise- og it-beredskab	4
Virksomhedernes afhængighed af it-systemer	7
Bekymringsniveau	9
It-sikkerhedsforanstaltninger i praksis	11
Investeringer i cybersikkerhed	15
Motivation bag øgede investeringer	19
Barrierer og udfordringer	21
Bilag	23

Nøgleresultater

Cybersikkerhed er en integreret del af virksomheders beredskab

Over halvdelen af Dansk Erhvervs medlemmer (51 pct.) har eller er ved at udarbejde en beredskabsplan – og blandt store virksomheder er andelen oppe på 91 pct. Cybersikkerhed er det mest udbredte element i beredskabsplanerne.

Driftsforstyrrelser er virksomhedernes største bekymring ift. beredskab og sikkerhed

60 pct. af Dansk Erhvervs medlemmer peger på afbrydelser i strøm, vand, varme eller internettet som deres største bekymring ift. beredskab og sikkerhed. 40 pct. frygter ransomware og 37 pct. datalæk.

Virksomhederne har høj afhængighed af interne it-systemer

55 pct. af Dansk Erhvervs medlemmer svarer, at driften stopper eller påvirkes markant ved tab af adgang til centrale it-systemer. Kun 5 pct. kan i høj grad udføre kerneopgaver uden it-adgang.

Hver tredje virksomhed er bekymret for cyberangreb det næste år

33 pct. af virksomhederne er meget eller ret bekymrede for cyberangreb. Det gælder særligt store virksomheder (66 pct.).

Tre ud af fire virksomheder har taget stilling til mindst én it-sikkerhedsforanstaltning

Men forskellene er markante på tværs af størrelse. Mikrovirksomheder (0-9 medarbejdere) har i gennemsnit taget stilling til 2,5 foranstaltninger ud af 12, mens store virksomheder ligger på 7,7.

Halvdelen af virksomhederne har øget investeringerne i cybersikkerhed det seneste år

Blandt store virksomheder er andelen 86 pct.

47 pct. forventer at øge investeringerne i cybersikkerhed det kommende år

Det gælder især store virksomheder, virksomheder, der allerede har øget investeringerne og virksomheder med et højt bekymringsniveau for cyberangreb.

Mangel på viden, tid og overblik er største barrierer for at øge investeringer og implementere foranstaltninger

Virksomhederne peger især på usikkerhed om, hvad der virker (29 pct.), mangel på tid (24 pct.) og mangel på kompetencer (23 pct.).

Baggrund og formål

Cybersikkerhed fylder mere end nogensinde i dansk erhvervsliv. Virksomhedernes stigende afhængighed af digitale systemer betyder, at selv mindre it-hændelser kan få store driftsmæssige konsekvenser. Samtidig udvikler trusselsbilledet sig hastigt, og både cyberkriminalitet, geopolitisk ustabilitet og fysiske hændelser udfordrer virksomhedernes robusthed.

Dansk Erhvervs har derfor gennemført en medlemsundersøgelse, der giver et aktuelt indblik i:

- Hvordan vores medlemmer arbejder med cybersikkerhed
- Hvilke risici de oplever
- Hvordan de investerer i at styrke deres modstandsdygtighed
- Hvilke udfordringer de står over for

Undersøgelsen belyser både virksomhedernes it-afhængighed, deres beredskab, bekymringsniveau, investeringer og de barrierer, der står i vejen for yderligere sikkerhedsindsatser.

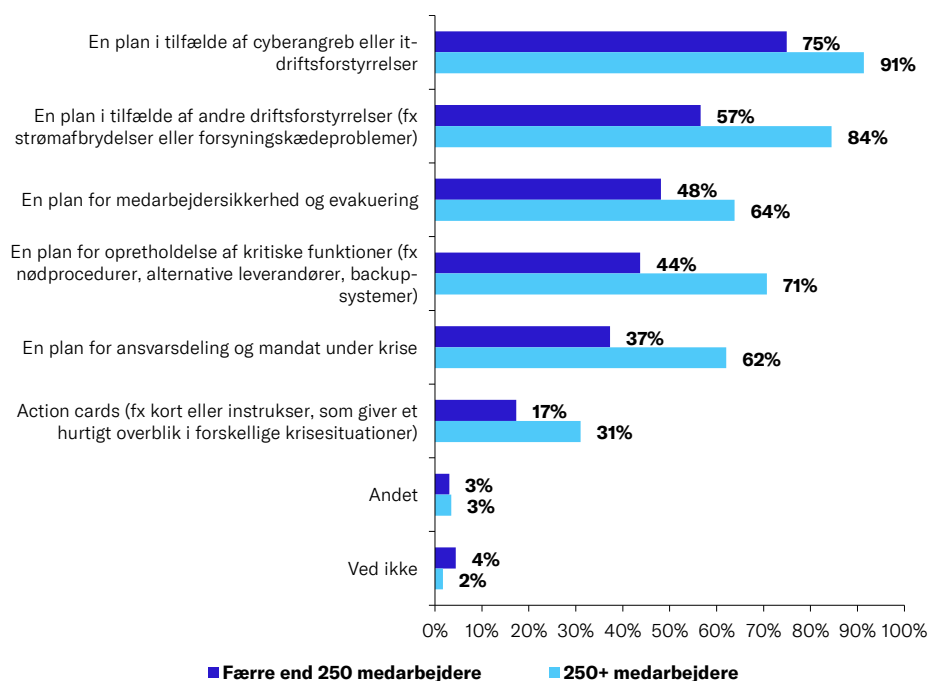
Formålet med analysen er at afdække, hvordan Dansk Erhvervs medlemmer vurderer deres egen cybersikkerhed, hvilke it-sikkerhedsforanstaltninger de arbejder med, og hvordan de prioriterer investeringer i sikkerhed i lyset af nye lovkrav og et mere komplekst trusselsbillede.

Analysen baserer sig på besvarelser fra 695 medlemsvirksomheder på tværs af de brancher og virksomhedsstørrelser, som Dansk Erhverv repræsenterer. Se fordeling i bilag på side 23.

Virksomhedernes generelle krise- og it-beredskab

Undersøgelsen viser, at 51 pct. af Dansk Erhvervs medlemmer enten har en beredskabsplan eller er i færd med at udarbejde en (ikke vist i figur). Beredskabsmodenheden stiger markant med virksomhedsstørrelsen – hele 91 pct. af de store virksomheder med 250+ medarbejdere har en formaliseret plan. Cybersikkerhed og it-drift er blandt de mest centrale elementer i beredskabsplanerne, se figur 1. Den mest udbredte del af planerne er håndtering af cyberangreb og it-driftsforstyrrelser, hvilket understreger at digitale risici vurderes som væsentlige strategiske udfordringer.

Figur 1: **Hvad består din virksomheds beredskabsplan af?**



Kilde: Dansk Erhvervs medlemsundersøgelse, november-december 2025.

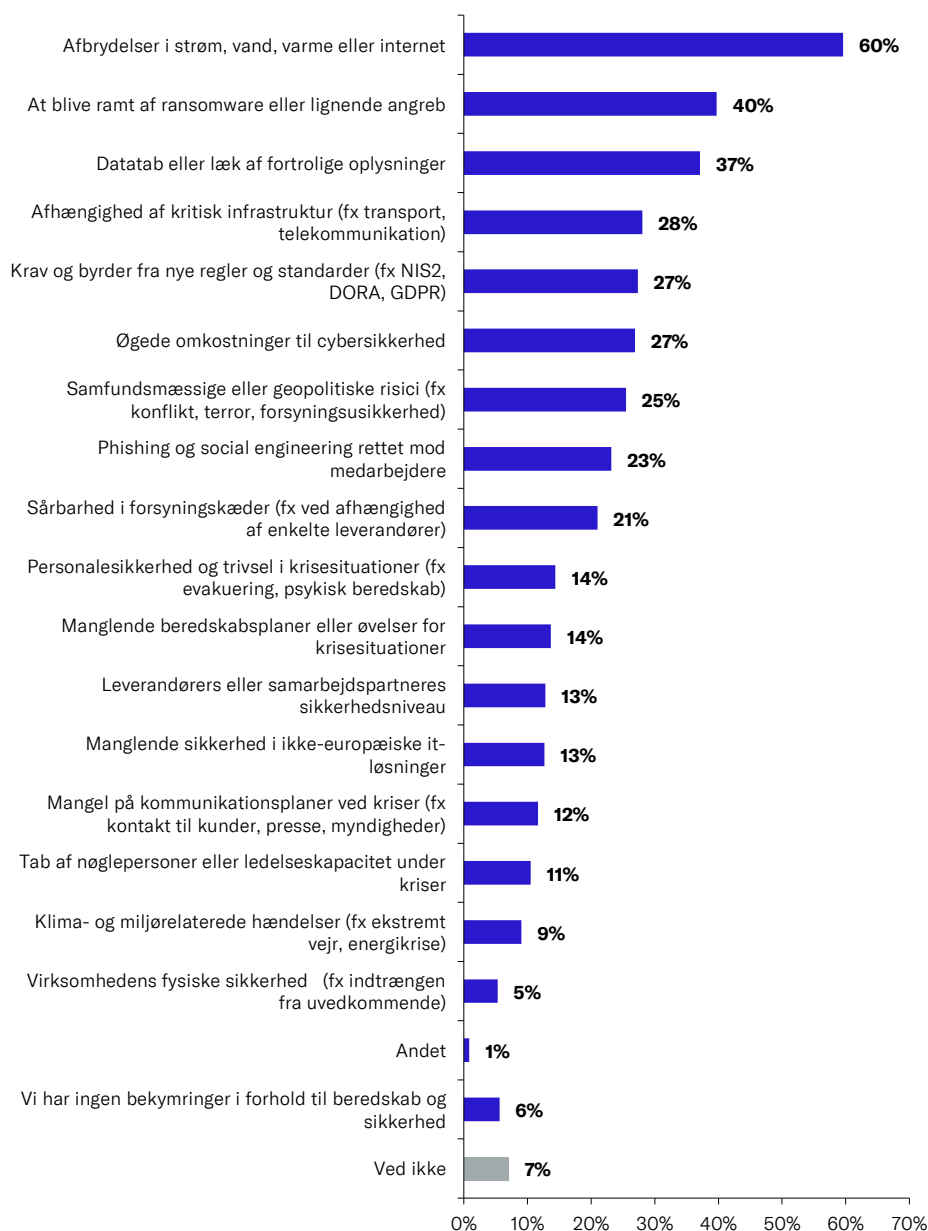
Note: n (Færre end 250 medarbejdere) = 295, n (250+ medarbejdere) = 58. Kun virksomheder, der har en beredskabsplan eller ved at udarbejde en beredskabsplan. Det var muligt for virksomhederne at angive flere svar.

Store virksomheder er generelt længere fremme end små og mellemstore virksomheder. Ni ud af ti virksomheder med 250+ medarbejdere (91 pct.) har en plan for cyberhændelser, mens det samme gælder tre ud af fire virksomheder (75 pct.) med færre end 250 medarbejdere. Det indikerer, at jo større en virksomhed er, desto større er både eksponeringen over for cyberrisici og behovet for formaliserede beredskabsprocedurer.

Når virksomhederne bliver spurgt til deres største aktuelle bekymringer ift. beredskab og sikkerhed, fremgår det, at driftsforstyrrelser generelt fylder endnu mere end cyberangreb isoleret set. 60 pct. angiver afbrydelser i strøm, vand, varme eller internet som en af deres største bekymringer, se figur 2. 40 pct. peger på ransomware og 37 pct. på datalæk. Det indikerer et komplekst trusselsbillede, hvor både cyberhændelser og fysiske infrastruktursvigt vurderes som kritiske risici.

Samlet set placerer det cybersikkerhed højt på listen over strategiske prioriteter i sikkerhedsarbejdet hos Dansk Erhvervs medlemmer.

Figur 2: **Hvad er din virksomheds største bekymringer ift. beredskab og sikkerhed lige nu?**



Kilde: Dansk Erhvervs medlemsundersøgelse, november-december 2025.

Note: 695. var muligt for virksomhederne at angive flere svar.

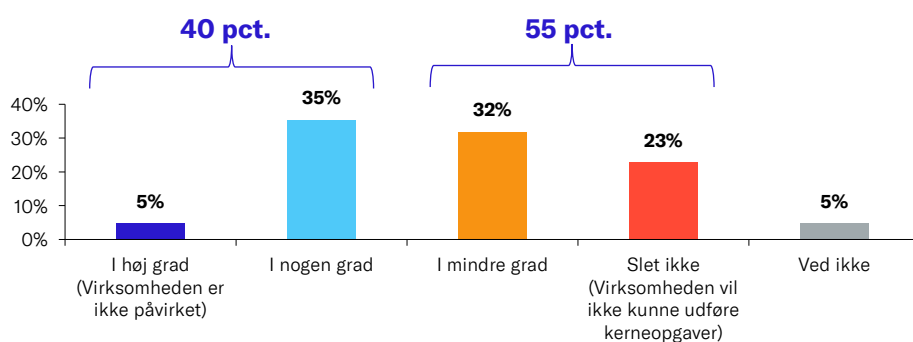
Virksomhedernes afhængighed af it-systemer

Dansk Erhverv har spurgt medlemmerne, i hvilken grad de vil være i stand til at udføre deres kerneopgaver, hvis virksomheden mister adgangen til centrale interne it-systemer. Nogle af de mest almindelige it-systemer, som virksomheder er afhængige af i deres daglige drift, er fx ordresystem, lagersystem, økonomisystem, kommunikationsmidler, kundedatabase, intranet osv.

Figur 3 viser, at langt størstedelen af virksomhederne er afhængige af deres it-systemer i en sådan grad, at driften enten stopper (23 pct.) eller påvirkes markant ved it-nedbrud (32 pct.). Kun en lille andel af virksomhederne vurderer, at de i høj grad vil kunne opretholde deres kerneopgaver uden adgang til centrale systemer (5 pct.).

Det understreger, at digitale systemer udgør fundamentet for den daglige drift i mange virksomheder, og at cybersikkerhed ikke kun handler om at undgå angreb, men om at sikre opretholdelse af it-systemer generelt.

Figur 3: **I hvilken grad vil din virksomhed være i stand til at udføre sine kerneopgaver, hvis virksomheden mister adgangen til centrale interne it-systemer?**



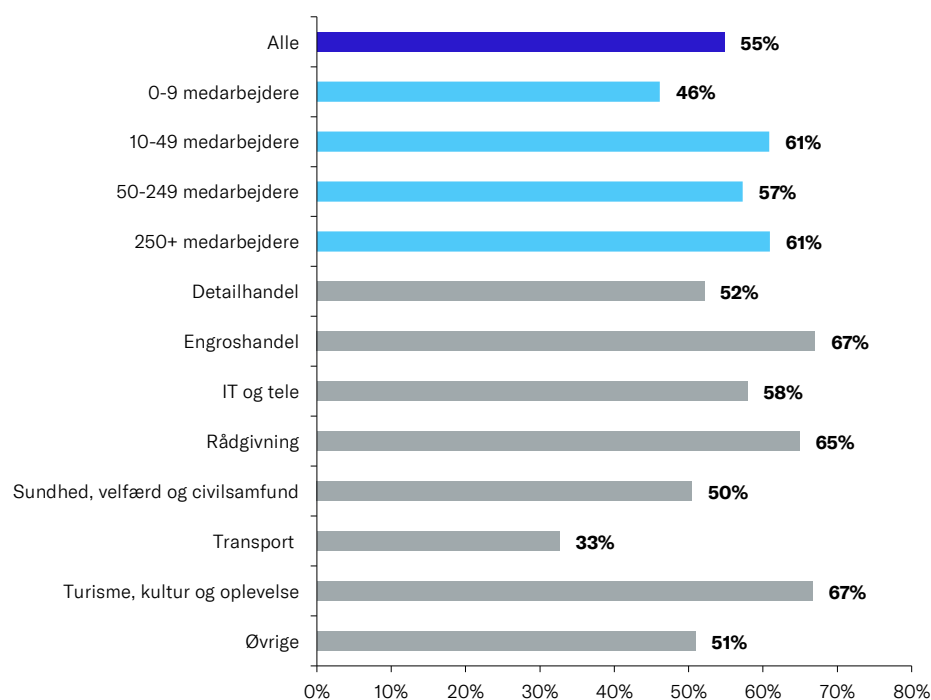
Kilde: Dansk Erhvervs medlemsundersøgelse, november-december 2025.

Note: n = 695. Nogle af de mest almindelige it-systemer, som virksomheder er afhængige af i deres daglige drift, er fx ordresystem, lagersystem, økonomisystem, kommunikationsmidler, kundedatabase, intranet osv.

På tværs af virksomhedsstørrelse er det særligt virksomheder med 10+ medarbejdere, der svarer, at de i mindre grad eller slet ikke vil kunne udføre deres kerneopgaver uden adgang til deres centrale it-systemer, se figur 4.

Branchemæssigt er it-afhængigheden særligt udtalt i engroshandlen, rådgivningsbranchen, turisme-, kultur- og oplevelse samt it- og telebranchen. Der er dog ikke signifikant forskel. Kun i transportbranchen er der signifikant færre, der svarer, at de ikke kan fortsætte deres arbejde, hvis de mister adgangen til it-systemer.

Figur 4: **Andel virksomheder, som i mindre grad eller slet ikke vil være i stand til at udføre sine kerneopgaver, hvis virksomheden mister adgangen til centrale interne it-systemer**



Kilde: Dansk Erhvervs medlemsundersøgelse, november-december 2025.

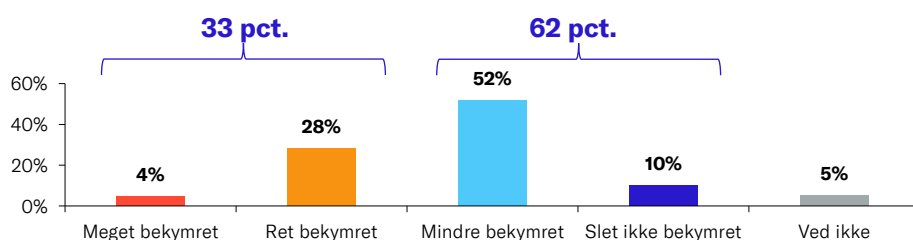
Note: n (Alle) = 695, n (0-9 medarbejdere) = 258, n (10-49 medarbejdere) = 263, n (50-249 medarbejdere) = 110, n (250+ medarbejdere) = 64, n (Detailhandel) = 96, n (Engroshandel) = 97, n (IT og tele) = 76, n (Rådgivning) = 114, n (Sundhed, velfærd og civilsamfund) = 111, n (Transport) = 98, n (Turisme, kultur og oplevelse) = 48, n (Øvrige) = 55. Nogle af de mest almindelige it-systemer, som virksomheder er afhængige af i deres daglige drift, er fx ordresystem, lagersystem, økonomisystem, kommunikationsmidler, kundedatabase, intranet osv.

Bekymringsniveau

Dansk Erhverv har spurgt medlemmerne, hvor bekymrede de er for, at virksomheden vil blive udsat for eller være genstand for forsøg på cyberangreb de næste 12 måneder.

Undersøgelsen viser, at en tredjedel af Dansk Erhvervs medlemmer (33 pct.) er meget eller ret bekymrede for at blive udsat for cyberangreb i den kommende tid, se figur 5. 52 pct. svarer, at de er mindre bekymrede, mens hver tiende virksomhed (10 pct.) slet ikke er bekymret.

Figur 5: **Hvor bekymret er du for, at din virksomhed vil blive udsat for eller være genstand for forsøg på cyberangreb inden for de næste 12 måneder?**



Kilde: Dansk Erhvervs medlemsundersøgelse, november-december 2025.

Note: n = 695.

Tallene stemmer godt overens med Dansk Erhvervs medlemsundersøgelse fra august 2025 (ikke vist i figur). Den viser, at 42 pct. af virksomhederne svarer, at sikkerhedsrisici (cybertrussel) i høj eller i nogen grad har været en udfordring eller bekymring for virksomhedens omsætning og muligheder for vækst de seneste 12 måneder. Det er den fjerde største bekymring ud af de 12, vi har nævnt for virksomhederne.¹ Den viser også, at 43 pct. forventer stigende udfordringer eller bekymringer med sikkerhedsrisici (cybertrussel) ift. virksomhedens omsætning og muligheder for vækst de kommende 12 måneder sammenlignet med de seneste 12 måneder. Det er den næststørste bekymring for virksomhederne ud af dem, vi har nævnt.

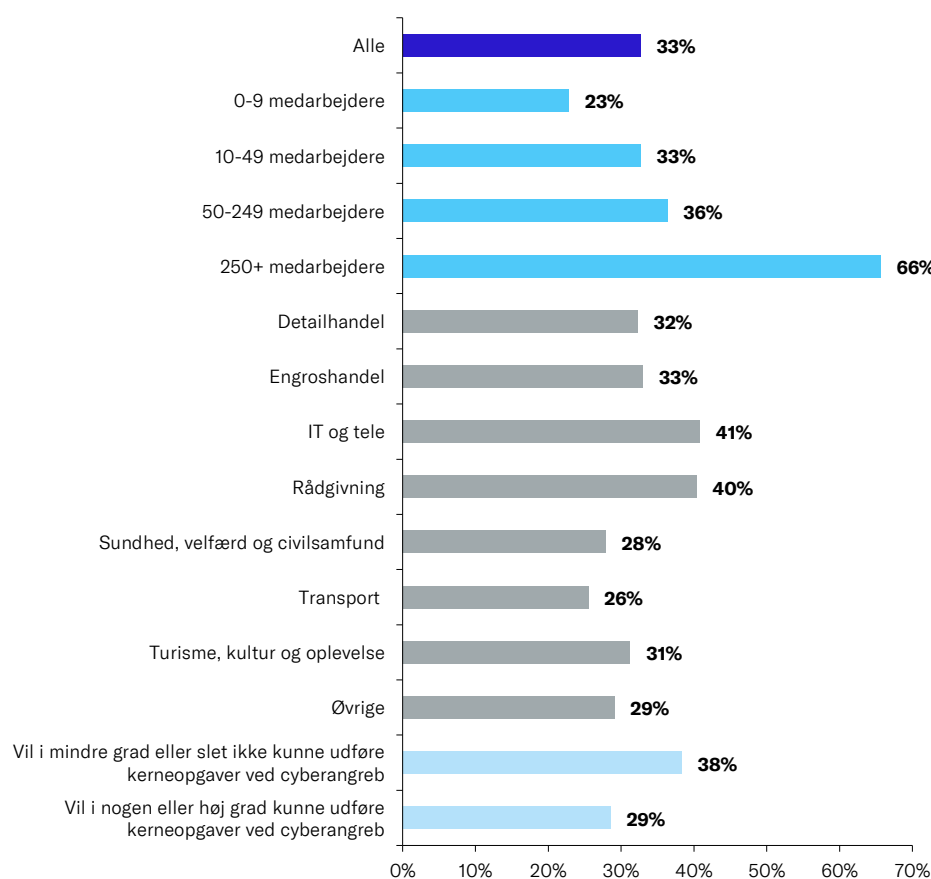
Figur 6 viser, at det særligt er store virksomheder med 250+ medarbejdere, der er bekymrede for cyberangreb (66 pct.). Branchemæssigt er bekymringen højest i it- og telebranchen samt rådgivningsbranchen, men forskellene er ikke signifikante. Virksomheder med lav robusthed

¹ Se de 12 udfordringer eller bekymringer i denne: [besvarlig-regulering-er-virksomheders-storste-vakstbarriere.pdf](#)

– dvs. virksomheder, der forventer ikke at kunne opretholde driften ved et cyberangreb – er i gennemsnit mere bekymrede end virksomheder med høj robusthed.

Bekymringsniveauet afspejler både det skærpede trusselsbillede og den stigende forståelse for, at cyberhændelser kan få direkte driftsmæssige og økonomiske konsekvenser.

Figur 6: **Andel virksomheder, der er meget eller ret bekymret for, at virksomheden vil blive udsat for eller være genstand for forsøg på cyberangreb de næste 12 måneder**



Kilde: Dansk Erhvervs medlemsundersøgelse, november-december 2025.

Note: n (Alle) = 695, n (0-9 medarbejdere) = 258, n (10-49 medarbejdere) = 263, n (50-249 medarbejdere) = 110, n (250+ medarbejdere) = 64, n (Detailhandel) = 96, n (Engroshandel) = 97, n (IT og tele) = 76, n (Rådgivning) = 114, n (Sundhed, velfærd og civilsamfund) = 111, n (Transport) = 98, n (Turisme, kultur og oplevelse) = 48, n (Øvrige) = 55, n (Vil i mindre grad eller slet ikke kunne udføre kerneopgaver ved cyberangreb) = 381, n (Vil i nogen eller høj grad kunne udføre kerneopgaver ved cyberangreb) = 280.

It-sikkerhedsforanstaltninger i praksis

Dansk Erhverv har undersøgt, hvilke it-sikkerhedsforanstaltninger virksomhederne har taget stilling til. "Taget stilling til" dækker over, at virksomheden fx har implementeret en foranstaltning, har overvejet/planlagt den, eller har vurderet den som relevant/ikke relevant. De it-sikkerhedsforanstaltninger, vi har spurgt til, relaterer sig til NIS2.²

NIS2

- NIS2-direktivet er en ny EU-lov, der stiller krav til virksomheders cybersikkerhed og håndtering af it-risici. Direktivet betyder, at flere virksomheder skal investere mere i sikkerhed, risikostyring og beredskab.
- Den danske NIS2-lov trådte i kraft den 1. juli 2025, og virksomheder, der er omfattet, skulle senest den 1. oktober 2025 registrere sig hos myndighederne.
- NIS2-direktivet gælder for mellemstore og store virksomheder i samfundsvigtige sektorer som fx energi, transport, sundhed, finans, digital infrastruktur og offentlig forvaltning.

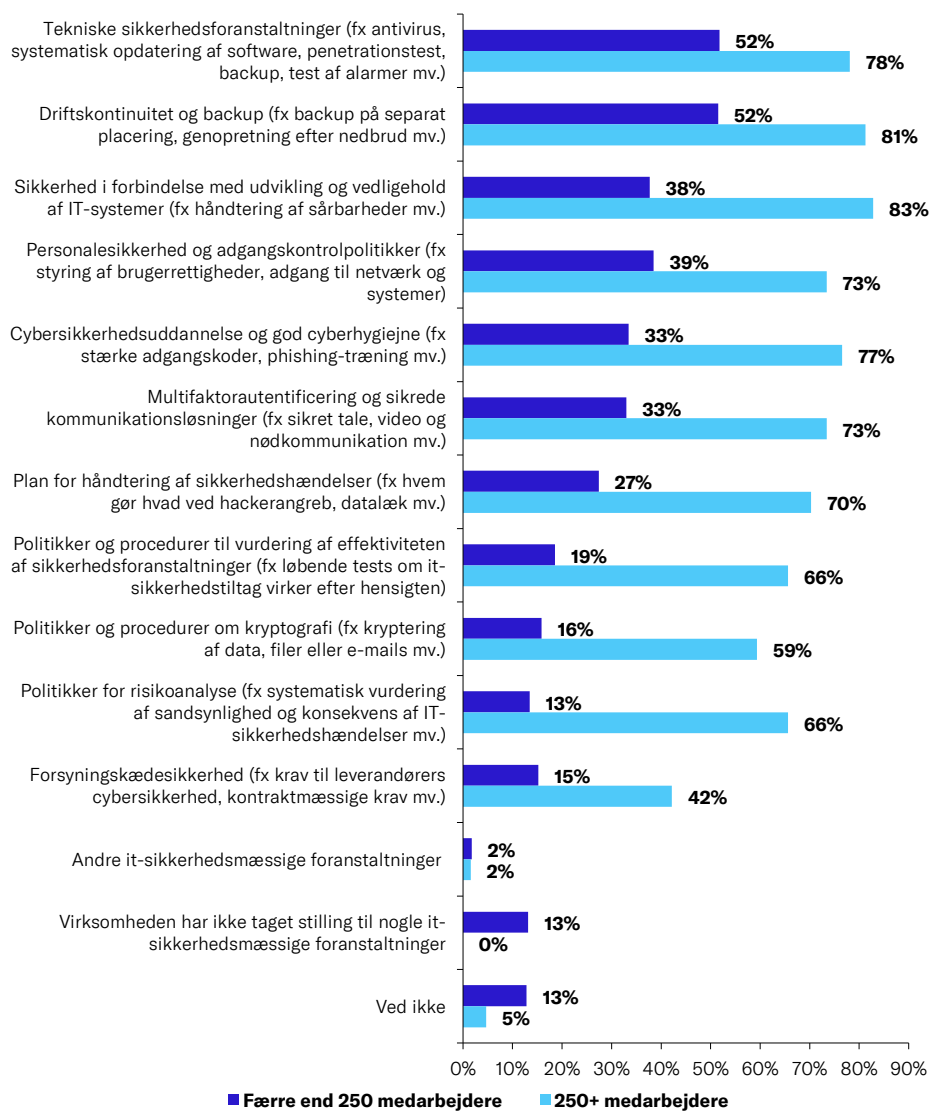
Undersøgelsen viser, at der er stor forskel på tværs af virksomhedsstørrelse, se figur 7. Store virksomheder (250+ medarbejdere) har i langt højere grad taget stilling til et bredt spektrum af sikkerhedsforanstaltninger ift. virksomheder med færre end 250 medarbejdere.

Blandt mikro- små og mellemstore virksomheder (med færre end 250 medarbejdere) har flest taget stilling til tekniske sikkerhedsforanstaltninger, som fx antivirus, systematisk opdatering af software, penetrationstest, backup, test af alarmer mv. (52 pct.), og driftskontinuitet og backup (fx backup på separat placering, genopretning efter nedbrud mv.) (52 pct.).

Blandt store virksomheder med 250+ medarbejdere har flest virksomheder taget stilling til sikkerhed i forbindelse med udvikling og vedligehold af IT-systemer, fx håndtering af sårbarheder mv. (83 pct.), og driftskontinuitet og backup (81 pct.).

² [NIS 2 | Styrelsen for Samfundssikkerhed](#)

Figur 7: **Hvilke af følgende it-sikkerhedsmæssige foranstaltninger har din virksomhed taget stilling til?**



Kilde: Dansk Erhvervs medlemsundersøgelse, november-december 2025.

Note: n (Færre end 250 medarbejdere) = 631, n (250+ medarbejdere) = 64. Det var muligt for virksomhederne at angive flere svar. "Taget stilling til" dækker over, at virksomheden fx har implementeret en foranstaltning, under overvejelse/planlagt, vurderet som relevant/ikke relevant.

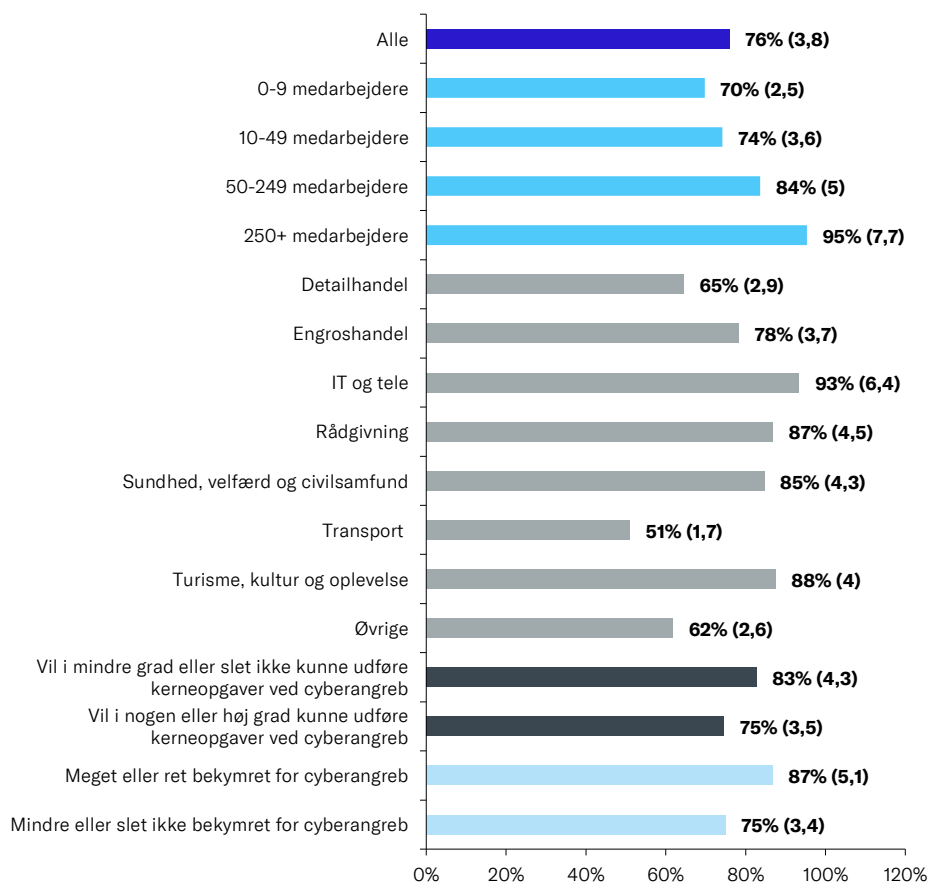
Samlet set har tre ud af fire af Dansk Erhvervs medlemmer taget stilling til mindst én it-sikkerhedsmæssig foranstaltning (76 pct.), se figur 8. Figuren sammenligner andelen af virksomheder, der har taget stilling til mindst én foranstaltning, på tværs af virksomhedsstørrelser, brancher og risikoprofiler. I parentes ses, hvor mange foranstaltninger de i gennemsnit har taget stilling til.

På tværs af **virksomhedsstørrelse** er mønsteret, at jo større virksomhed, desto flere har taget stilling til mindst én foranstaltning og desto flere foranstaltninger, har de taget stilling til. Blandt mikrovirksomheder (0–9 medarbejdere) har 70 pct. taget stilling til mindst én foranstaltning, og de har i gennemsnit taget stilling til 2,5 ud af de 12 mulige. For små virksomheder (10–49 medarbejdere) gælder det 74 pct., som i gennemsnit har taget stilling til 3,6 foranstaltninger. Blandt mellemstore virksomheder (50–249 medarbejdere) stiger andelen til 84 pct., og disse har i gennemsnit taget stilling til 5 foranstaltninger. De største virksomheder (250+ medarbejdere) ligger markant højere: Hele 95 pct. har taget stilling til mindst én foranstaltning, og i gennemsnit har de forholdt sig til 7,7 foranstaltninger.

Der er også betydelige forskelle mellem **brancher**. It- og telebranchen er den mest modne: 93 pct. har arbejdet med mindst én foranstaltning, og branchen har i gennemsnit taget stilling til 6,4. Også turisme-, kultur- og oplevelsesbranchen (88 pct., 4 foranstaltninger), rådgivningsbranchen (87 pct., 4,5) samt sundhed, velfærd og civilsamfund (85 pct., 4,3) ligger højt. I den anden ende af skalaen ligger detailhandlen og transportbranchen, hvor færrest virksomheder har taget stilling til it-sikkerhedsforanstaltninger.

Ser vi på virksomhedernes **risikoprofiler**, tegner der sig et lignende billede: Virksomheder med høj bekymring for cyberangreb eller stor afhængighed af deres it-systemer har taget stilling til flere foranstaltninger end virksomheder, der er mindre udsatte, eller har en lavere risiko-bevidsthed.

Figur 8: **Andel virksomheder, der har taget stilling til it-sikkerhedsmæssige foranstaltninger (gennemsnitlig antal it-sikkerhedsforanstaltninger i parentes)**



Kilde: Dansk Erhvervs medlemsundersøgelse, november-december 2025.

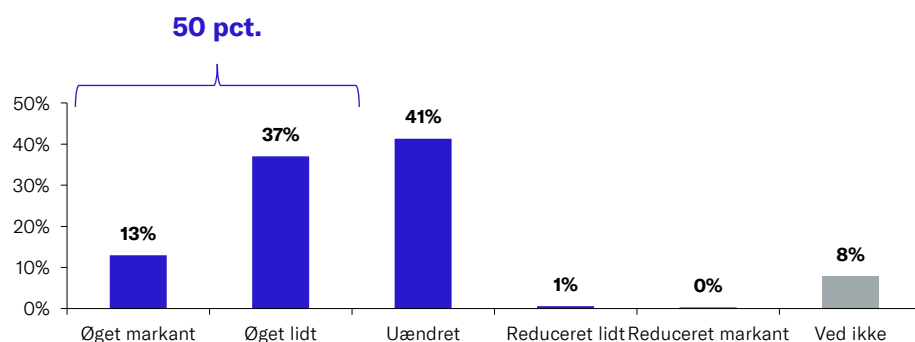
Note: n (Alle) = 695, n (0-9 medarbejdere) = 258, n (10-49 medarbejdere) = 263, n (50-249 medarbejdere) = 110, n (250+ medarbejdere) = 64, n (Detailhandel) = 96, n (Engroshandel) = 97, n (IT og tele) = 76, n (Rådgivning) = 114, n (Sundhed, velfærd og civilsamfund) = 111, n (Transport) = 98, n (Turisme, kultur og oplevelse) = 48, n (Øvrige) = 55, n (Vil i mindre grad eller slet ikke kunne udføre kerneopgaver ved cyberangreb) = 381, n (Vil i nogen eller høj grad kunne udføre kerneopgaver ved cyberangreb) = 280, n (Meget eller ret bekymret for cyberangreb) = 227, n (Mindre eller slet ikke bekymret for cyberangreb) = 431. "Taget stilling til" dækker over, at virksomheden fx har implementeret en foranstaltning, under overvejelse/planlagt, vurderet som relevant/ikke relevant. Virksomheder, der ikke har svaret "Virksomheden har ikke taget stilling til nogle it-sikkerhedsmæssige foranstaltninger" eller "Ved ikke" på spørgsmålet: "Hvilke af følgende it-sikkerhedsmæssige foranstaltninger har din virksomhed taget stilling til? Det er muligt at angive flere svar."

Investeringer i cybersikkerhed

Dansk Erhverv har undersøgt, om medlemmerne har øget eller reduceret deres investeringer i cybersikkerhed de seneste 12 måneder, og hvad de forventer at gøre i de kommende 12 måneder.

Figur 9 viser, at 50 pct. af Dansk Erhvervs medlemmer har øget deres investeringer det sidste år. Heraf har 13 pct. øget markant og 37 pct. har øget lidt. Næsten ingen virksomheder har reduceret deres investeringer.

Figur 9: **Har din virksomhed øget eller reduceret sine investeringer i cybersikkerhed de seneste 12 måneder?**



Kilde: Dansk Erhvervs medlemsundersøgelse, november-december 2025.

Note: n = 695.

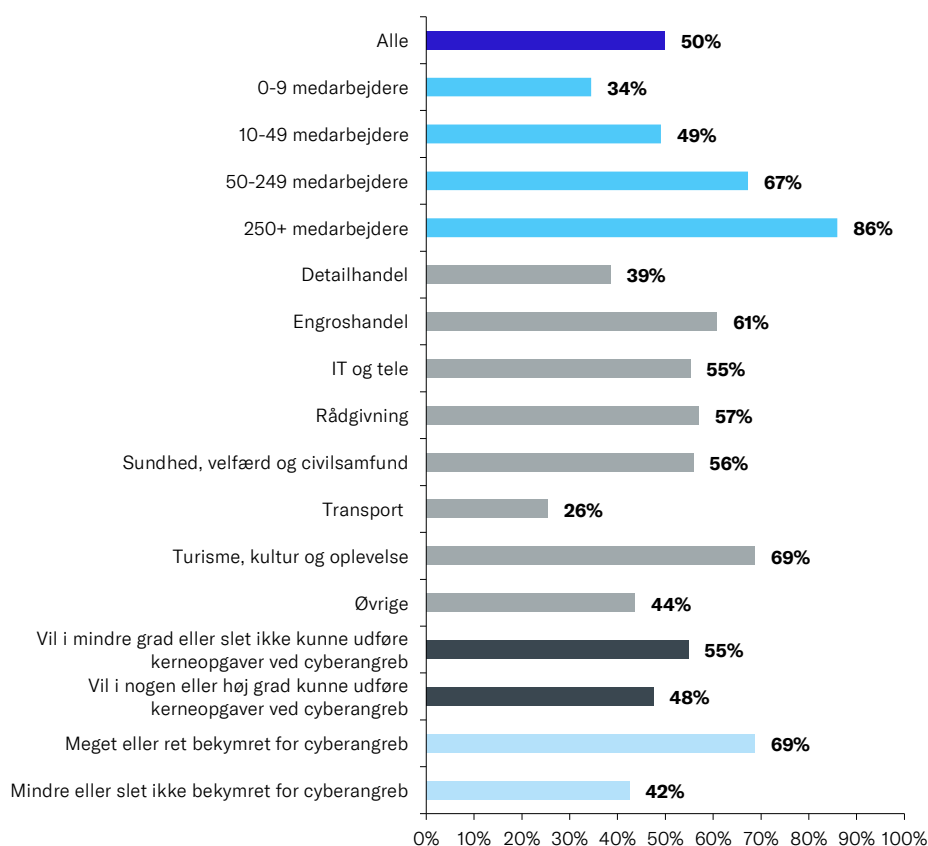
Figur 10 viser tydelige forskelle på tværs af virksomhedsstørrelse, branche og risikoprofil.

Generelt gælder, at jo større virksomheden er, desto flere har øget sine investeringer i cybersikkerhed det seneste år. Blandt mikrovirksomhederne har 34 pct. øget investeringerne, mens det samme gælder 49 pct. af de små virksomheder, 67 pct. af de mellemstore virksomheder og 86 pct. af de store virksomheder.

Turisme-, kultur og oplevelsesbranchen er den branche, hvor flest har øget deres investeringer i cybersikkerhed (69 pct.). Detailhandlen og transportbranchen ligger under flere af de øvrige brancher.

Signifikant flere virksomheder med høj bekymring for cyberangreb har øget investeringerne ift. mindre bekymrede virksomheder, ligesom flere virksomheder med lav robusthed over for cyberangreb øger investeringerne ift. dem, der i højere grad kan opretholde driften (ikke signifikant forskel).

Figur 10: **Andel virksomheder, der har øget sine investeringer i cybersikkerhed de seneste 12 måneder**

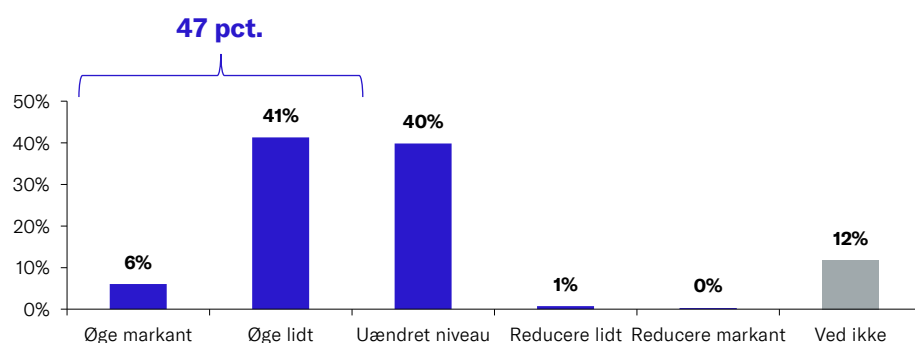


Kilde: Dansk Erhvervs medlemsundersøgelse, november-december 2025.

Note: n (Alle) = 695, n (0-9 medarbejdere) = 258, n (10-49 medarbejdere) = 263, n (50-249 medarbejdere) = 110, n (250+ medarbejdere) = 64, n (Detailhandel) = 96, n (Engroshandel) = 97, n (IT og tele) = 76, n (Rådgivning) = 114, n (Sundhed, velfærd og civilsamfund) = 111, n (Transport) = 98, n (Turisme, kultur og oplevelse) = 48, n (Øvrige) = 55, n (Vil i mindre grad eller slet ikke kunne udføre kerneopgaver ved cyberangreb) = 381, n (Vil i nogen eller høj grad kunne udføre kerneopgaver ved cyberangreb) = 280, n (Meget eller ret bekymret for cyberangreb) = 227, n (Mindre eller slet ikke bekymret for cyberangreb) = 431.

47 pct. af Dansk Erhvervs medlemmer forventer at øge sine investeringer i cybersikkerhed det kommende år. 40 pct. forventer uændrede investeringer, mens 12 pct. svarer "ved ikke".

Figur 11: **Forventer din virksomhed at øge eller reducere sine investeringer i cybersikkerhed inden for de kommende 12 måneder?**



Kilde: Dansk Erhvervs medlemsundersøgelse, november-december 2025.

Note: n = 695.

Figur 12 viser samme tendenser for de kommende investeringer i cybersikkerhed som for de foregående investeringer.

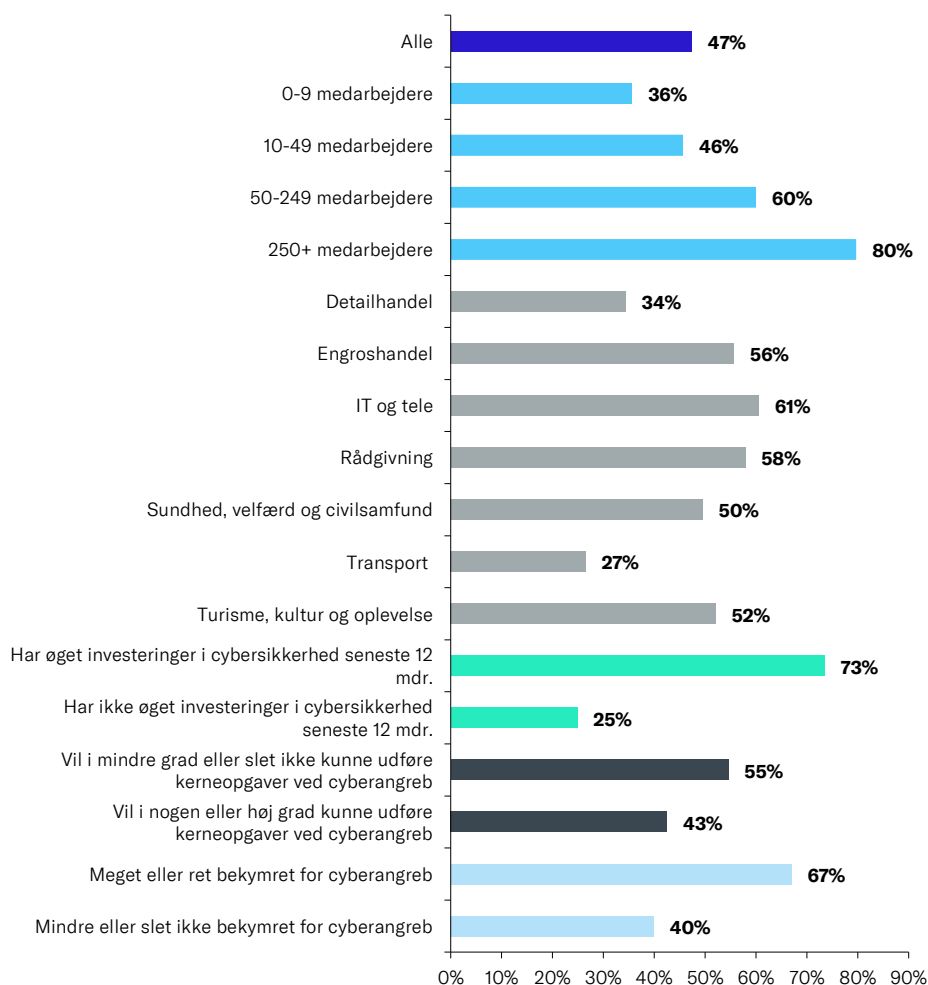
Jo større virksomhed, jo større andel forventer at øge sine investeringer i cybersikkerhed det kommende år. Det spænder fra 36 pct. blandt mikrovirksomhederne, som vil øge investeringerne til 80 pct. blandt de store virksomheder.

Detailhandlen og transportbranchen ligger også her signifikant under flere af de øvrige brancher.

Figuren viser også, at signifikant flere virksomheder, der allerede har øget sine investeringer i cybersikkerhed også forventer at gøre det fremover sammenlignet med dem, der ikke har øget deres investeringer det seneste år. Der kan derfor med tiden måske opstå et gab mellem dem, der allerede investerer og vil fortsætte med at gøre det, og dem, der ikke gør det.

Der er desuden signifikant flere virksomheder med høj bekymring for cyberangreb, der forventer at øge investeringerne end mindre bekymrede virksomheder, ligesom flere virksomheder med lav robusthed over for cyberangreb forventer at øge investeringerne ift. dem, der i højere grad kan opretholde driften.

Figur 12: **Andel virksomheder, der forventer at øge sine investeringer i cybersikkerhed de kommende 12 måneder**



Kilde: Dansk Erhvervs medlemsundersøgelse, november-december 2025.

Note: n (Alle) = 695, n (0-9 medarbejdere) = 258, n (10-49 medarbejdere) = 263, n (50-249 medarbejdere) = 110, n (250+ medarbejdere) = 64, n (Detailhandel) = 96, n (Engroshandel) = 97, n (IT og tele) = 76, n (Rådgivning) = 114, n (Sundhed, velfærd og civilsamfund) = 111, n (Transport) = 98, n (Turisme, kultur og oplevelse) = 48, n (Øvrige) = 55, n (Har øget investeringer i cybersikkerhed seneste 12 mdr.) = 347, n (Har ikke øget investeringer i cybersikkerhed seneste 12 mdr.) = 293, n (Vil i mindre grad eller slet ikke kunne udføre kerneopgaver ved cyberangreb) = 381, n (Vil i nogen eller høj grad kunne udføre kerneopgaver ved cyberangreb) = 280, n (Meget eller ret bekymret for cyberangreb) = 227, n (Mindre eller slet ikke bekymret for cyberangreb) = 431.

Motivation bag øgede investeringer

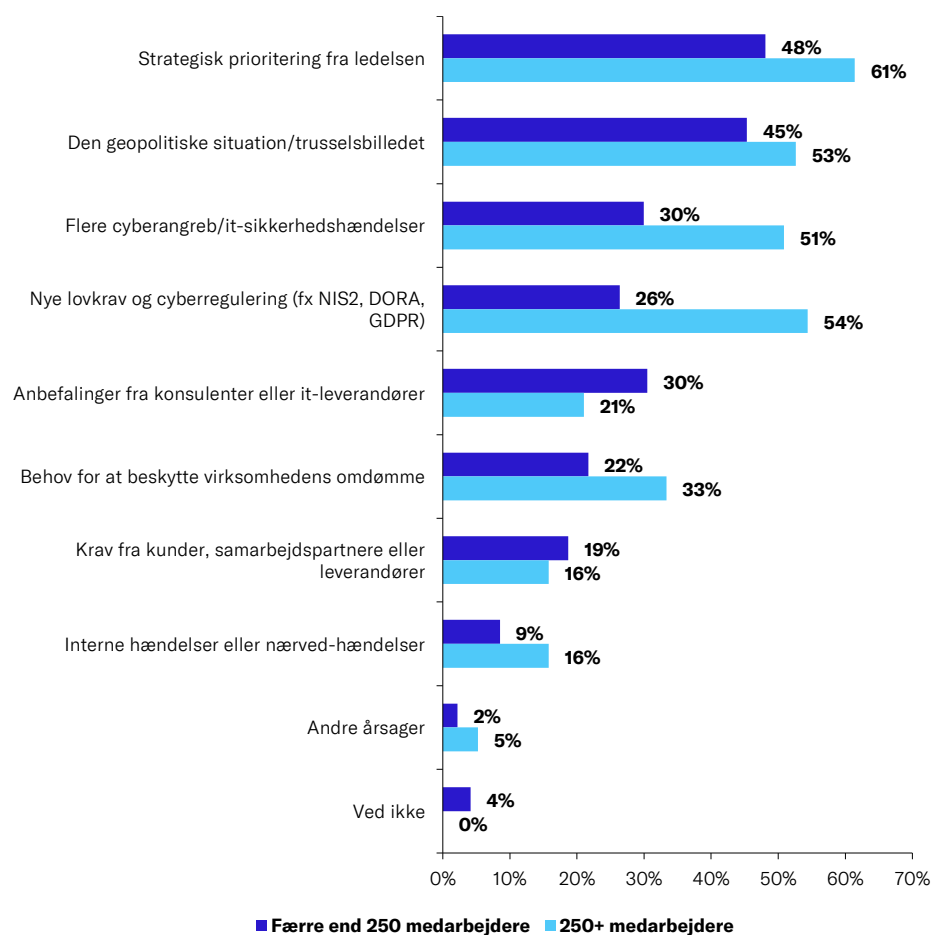
Dansk Erhverv har undersøgt årsagerne til de øgede investeringer i cybersikkerhed, både for så vidt angår de virksomheder, der allerede har øget sine investeringer det seneste år, og dem, der forventer at øge deres investeringer det kommende år.

Undersøgelsen viser, at den største årsag til øgede investeringer er strategiske prioriteringer fra ledelsen, som nævnes af 48 pct. af mikro-, små og mellemstore virksomheder (SMV'er) og 61 pct. af store virksomheder, se figur 13. Det vidner om, at cybersikkerhed i stigende grad er et ledelsesansvar og ikke længere et rent teknisk anliggende.

For SMV'erne er den geopolitiske situation/trusselsbilledet den næststørste driver (45 pct.), mens store virksomheder i høj grad drives af lovkrav og regulering – herunder NIS2, DORA og GDPR (54 pct.).

Andre væsentlige faktorer er flere cyberangreb, anbefalinger fra konsulenter og it-leverandører samt behovet for omdømmebeskyttelse.

Figur 13: **Hvorfor har din virksomhed øget eller forventer at øge investeringerne i cybersikkerhed?**



Kilde: Dansk Erhvervs medlemsundersøgelse, november-december 2025.

Note: n (Færre end 250 medarbejdere) = 364, n (250+ medarbejdere) = 57. Kun virksomheder, har øget deres investeringer i cybersikkerhed de seneste 12 måneder eller forventer at gøre det de kommende 12 måneder. Det var muligt for at angive flere svar.

Barrierer og udfordringer

Selvom mange virksomheder ønsker at styrke deres cybersikkerhed, står de over for en række barrierer. Hele 66 pct. af virksomhederne oplever barrierer og udfordringer i forhold til at investere i og implementere foranstaltninger for at styrke deres cybersikkerhed. Den største udfordring er usikkerhed om, hvilke indsatser der reelt virker (29 pct.). Hertil kommer mangel på tid (24 pct.), viden og kompetencer (23 pct.) samt manglende overblik over risici og systemer (22 pct.). Økonomi spiller også en rolle. (19 pct.), ligesom det kan være vanskeligt at måle effekt og værdi (19 pct.). Store virksomheder peger især på tid, overblik, økonomi og rekruttering af medarbejdere med de rette kompetencer som deres primære udfordringer. Det viser, at virksomhederne ikke alene har brug for tekniske løsninger, men også for vejledning, kompetenceløft og praktiske værktøjer, der gør cyberindsatser mere håndterbare og forståelige.

Figur 14: **Hvilke barrierer og udfordringer oplever din virksomhed i forhold til at investere i og implementere foranstaltninger for at styrke virksomhedens cybersikkerhed?**



Kilde: Dansk Erhvervs medlemsundersøgelse, november-december 2025.

Note: n = 695. Det var muligt at angive flere svar.

Bilag

I nedenstående tabeller ses fordelingen af virksomheder i undersøgelsen fordelt på branche og størrelse (antal medarbejdere).

Tabel 1: **Virksomhederne fordelt efter branche**

	Andel af alle virksomheder
Detailhandel	14%
Engroshandel	14%
IT og tele	11%
Rådgivning	16%
Sundhed, velfærd og civilsamfund	16%
Transport	14%
Turisme, kultur og oplevelse	7%
Øvrige	8%
n	695

Kilde: Dansk Erhvervs medlemsundersøgelse, november-december 2025.

Tabel 2: **Virksomhederne fordelt efter størrelse**

	Andel af alle virksomheder
0-9 medarbejdere	37%
10-49 medarbejdere	38%
50-249 medarbejdere	16%
250+ medarbejdere	9%
n	695

Kilde: Dansk Erhvervs medlemsundersøgelse, november-december 2025.

Om denne rapport

Arbejdet med rapporten er afsluttet i december 2025.

Om Dansk Erhvervs medlemsundersøgelse

Dansk Erhverv har foretaget en medlemsundersøgelse, som afdækker vores medlemmers afhængighed af interne it-systemer og investeringer i cybersikkerhed. 695 virksomheder har svaret på undersøgelsen. Disse virksomheder er repræsentative for Dansk Erhvervs medlemmer på størrelse, branche og region. Stikprøven er ikke nødvendigvis repræsentativ for det samlede danske erhvervsliv, da Dansk Erhverv ikke har medlemmer indenfor alle brancher. Den maksimale stikprøveusikkerhed i en undersøgelse med 695 respondenter er +- 3,7 procentpoint. Usikkerheden er naturligvis større i de figurer, som bygger på færre respondenter.

Om Dansk Erhvervs Analyser

Dansk Erhverv udarbejder løbende analyser, som samles i analysenotater eller rapporter. Ambitionen er at udgøre et kvalificeret og anvendeligt beslutningsgrundlag i forhold til væsentlige, aktuelle udfordringer på alle områder, som har betydning for dansk erhvervsliv og den samfundsøkonomiske udvikling. Det er tilladt at citere fra Dansk Erhvervs analyser med tydelig henvisning til Dansk Erhverv.

Kontakt

Henvendelser angående Dansk Erhvervs politik på området kan ske til chefkonsulent, Joen Magieres på joma@danskerhverv.dk eller på tlf. 3374 6136.

Henvendelser angående analysen kan ske til Seniorøkonom, Christine Sinkjær-Rasmussen på chsi@danskerhverv.dk eller på tlf. 3374 6156.

DANSK ERHVERV

Børsgade 4
1217 København K

www.danskerhverv.dk
info@danskerhverv.dk
T. + 45 3374 6000

Vi handler på vegne af vores medlemmer

I Dansk Erhverv handler vi hver dag på vegne af 18.000 medlemsvirksomheder og flere end 100 brancheforeninger. Vi er erhvervsorganisation og arbejdsgiverforening for et af verdens mest handlekraftige erhvervsliv.

Vi tilbyder rådgivning inden for medarbejder- og virksomhedsforhold og politisk gennemslagskraft. Vores indsatser bygger på medlemmernes aktive deltagelse i netværk og udvalg.

I Dansk Erhverv arbejder vi hver dag for, at Danmark bliver verdens bedste land at drive virksomhed i. Til gavn for arbejdspladser, velstand og Danmark i fremgang.

Vi arbejder for et Danmark med sammenhængskraft og handlekraft.