Cyberagendaen 2026

December 2025

86 %

af virksomhederne med en øget bekymring for cybertrusler relaterer denne til den geopolitiske situation.

50 %

af virksomhederne oplever, at manglende overblik over tredjeparter og leverandører er den største barriere for at leve op til de nye sikkerhedskrav i NIS 2 og DORA.

76 %

af virksomhedernes bestyrelser har cybersikkerhed som en fast del af deres årshjul.

64 %

af respondenterne forventer, at deres virksomheds cyber- og informationssikkerhedsbudget vil vokse inden for de næste 12 måneder.

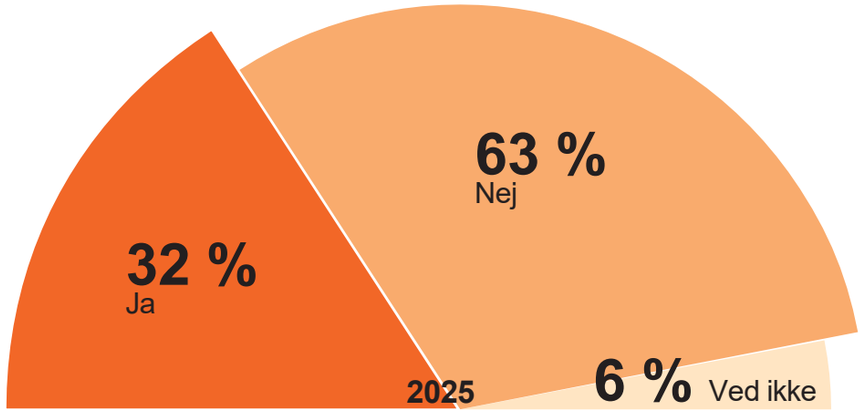
Cybersikkerhed i fokus

Danske virksomheder og offentlige organisationer opruster fortsat på cybersikkerhedsområdet.

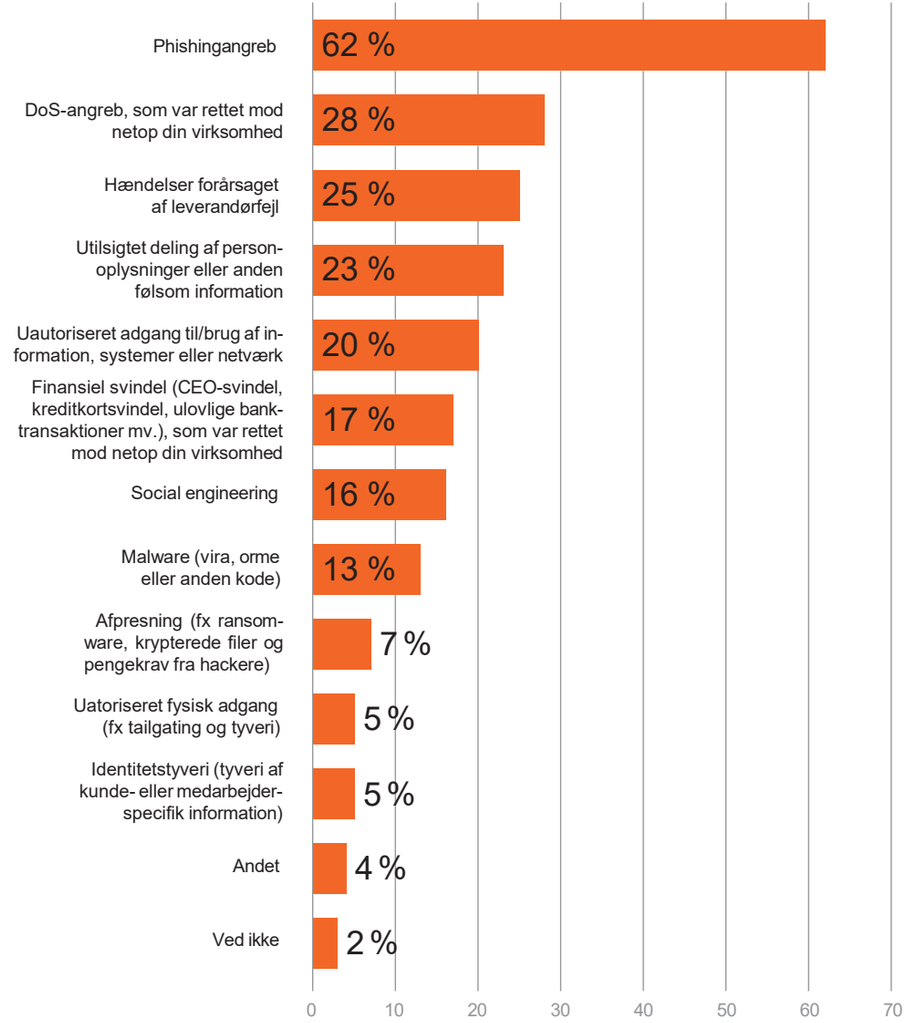
62 %

af de virksomheder, der har været ramt af sikkerhedshændelser, rapporterer, at det drejer sig om phishingangreb.

Har din virksomhed været udsat for en sikkerhedshændelse inden for de seneste 12 måneder?



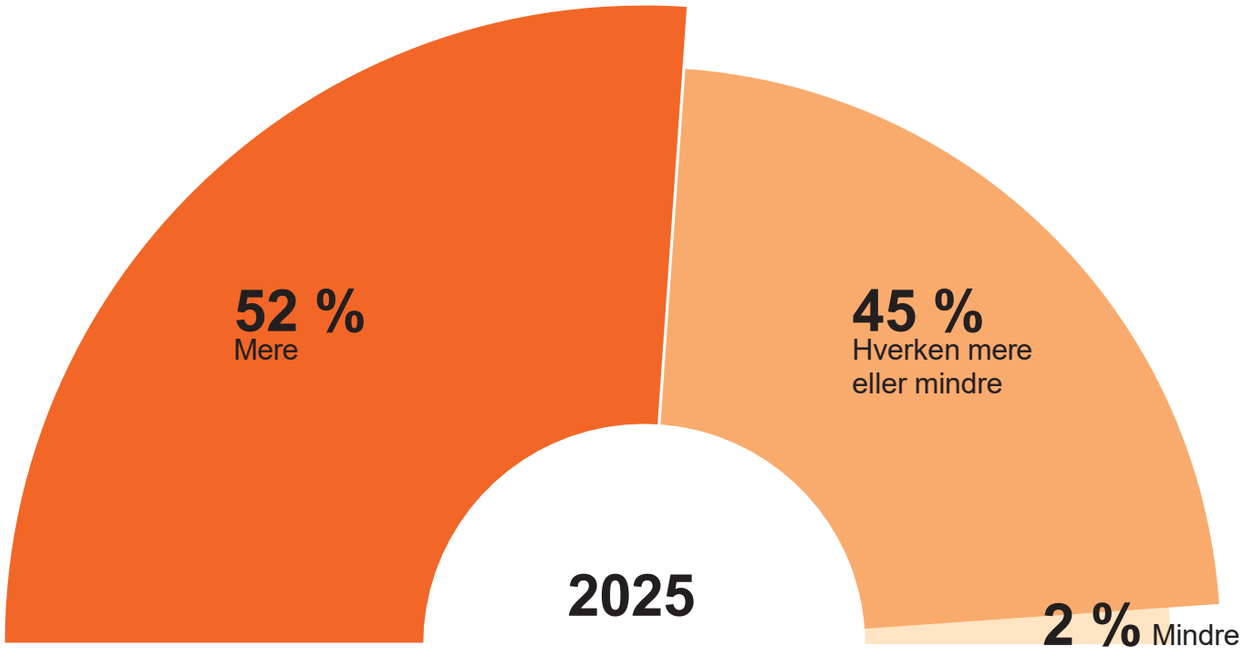
Hvilken type sikkerhedshændelse(r) var der tale om?



72 %

af respondenterne er mest bekymret for længerevarende nedbrud på kritiske systemer som en alvorlig konsekvens af cybertrusler.

Bekymrer du dig i dag mere eller mindre om de cybertrusler, din virksomhed oplever, end du gjorde for 12 måneder siden?



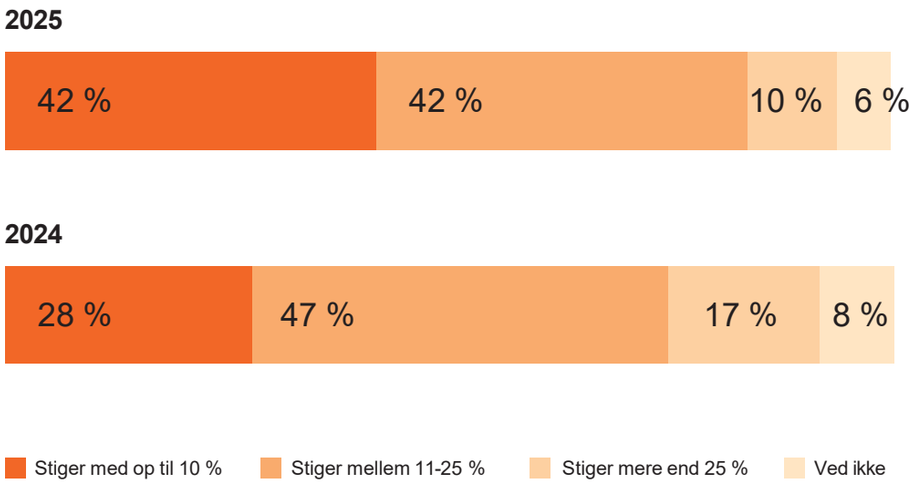
Investeringerne vokser, og det gør ambitions-niveauet også

Cybersikkerhed er ikke længere et spørgsmål om, hvorvidt man skal investere, men hvordan investeringerne skal fordeles og prioriteres.

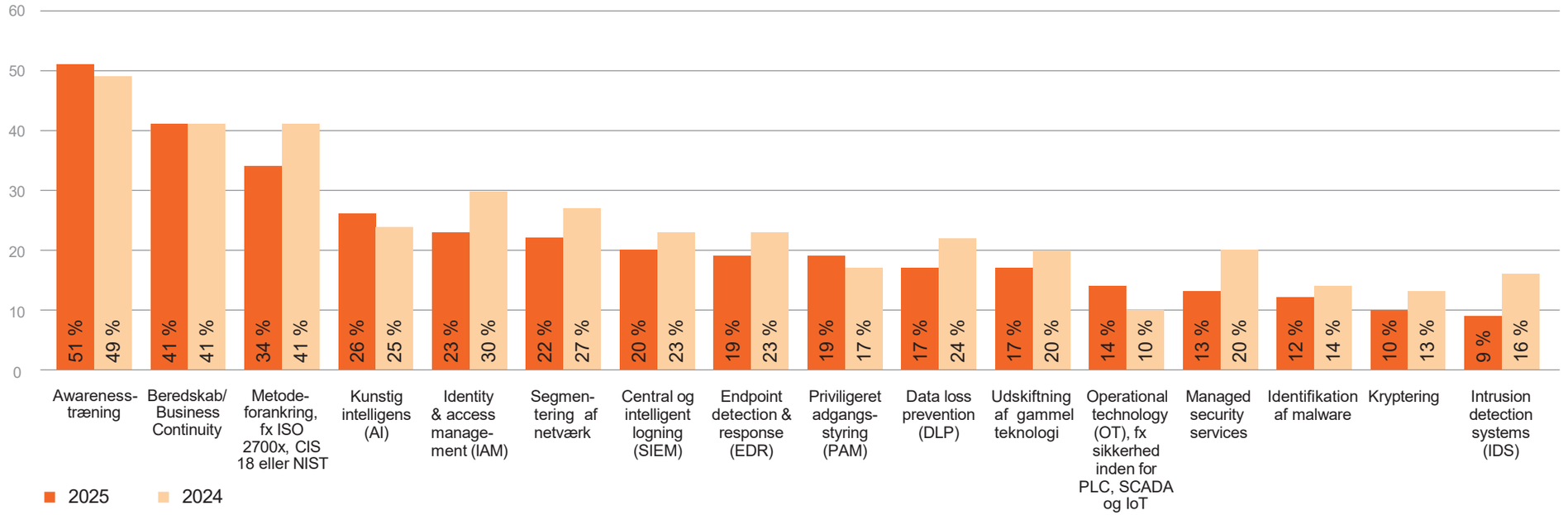
64 %

af respondenterne forventer, at deres budget til cyber- og informationssikkerhed vil vokse i løbet af de næste 12 måneder.

Hvor meget forventer du, at cyber- og informationssikkerheds-budgettet vil stige inden for de næste 12 måneder?



Hvad er din virksomheds højst prioriterede investeringer inden for cyber- og informationssikkerhed de næste 12 måneder?



41 %

af virksomhederne i undersøgelsen prioriterer investeringer i beredskab og 34 % i metodeforankring, hvilket understreger en helhedsorienteret tilgang.

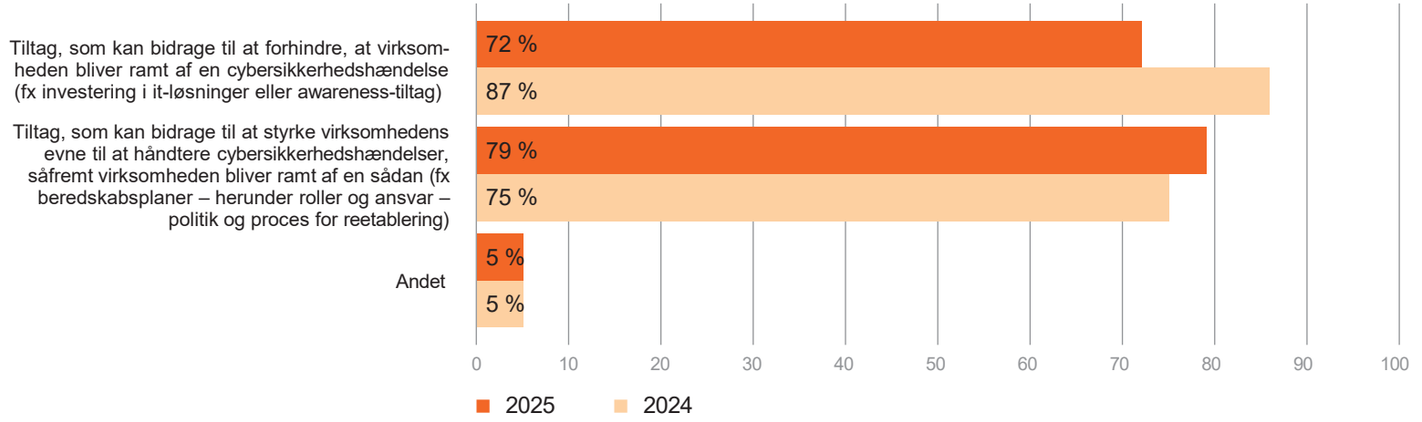
Geopolitik som drivkraft for cybersikkerhed

Den stigende bekymring for cybertrusler hænger tæt sammen med den aktuelle geopolitiske situation, hvor krigen mellem Rusland og Ukraine har intensiveret spændingerne mellem Rusland, Europa og USA.

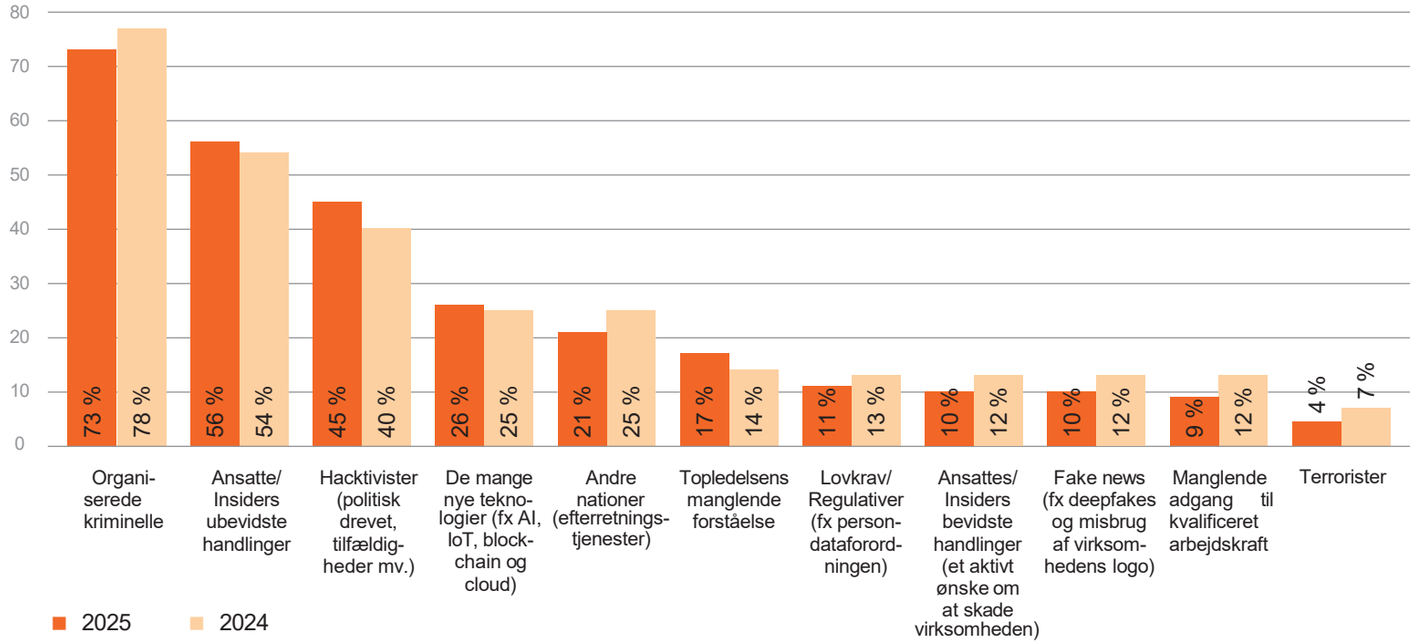
86 %

af de respondenter, der oplever øget bekymring for cybertrusler, tilskriver denne bekymring kom-pleksitet og usikkerhed på internationalt plan.

Hvilke nye cybersikkerhedstiltag har din virksomhed implementeret som følge af den øgede bekymring for cybertrusler?



Hvad udgør de største trusler for din virksomhed i relation til cyber- og informationssikkerhed?



73 %

af respondenterne angiver organiserede kriminelle som den største trussel i relation til cyber- og informationssikkerhed.

“

Resultaterne understreger, at truslerne både kommer udefra og indefra, og at medarbejdernes adfærd spiller en central rolle i virksomhedernes sikkerhedsbillede.

NIS2 og DORA fastholder momentum

Arbejdet med at imødekomme kravene i de nye EU-reguleringer, NIS2-direktivet og DORA-forordningen, fortsætter med høj intensitet blandt danske virk-somheder. Årets undersøgelse viser, at reguleringerne stadig har stor strategisk betydning, selvom de ikke længere fylder så meget i den offentlige debat.

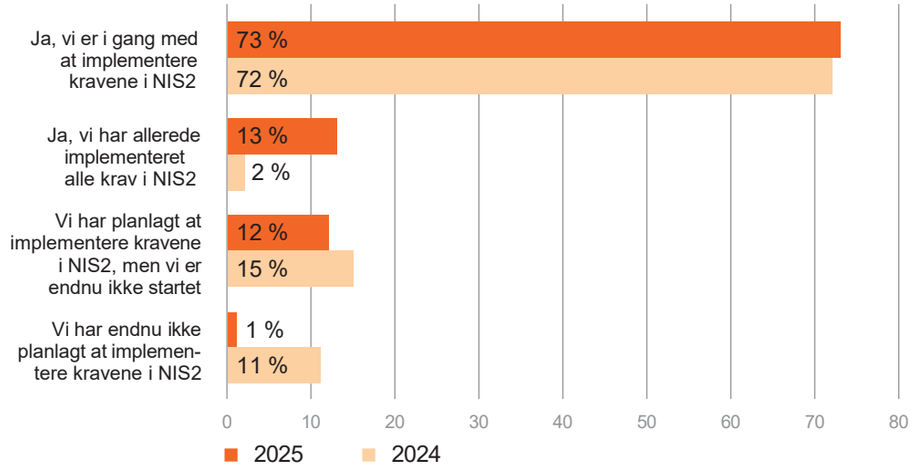
13 %

af de adspurgte virksomheder har allerede implementeret alle krav i NIS2, og 73 % er i gang.

33 %

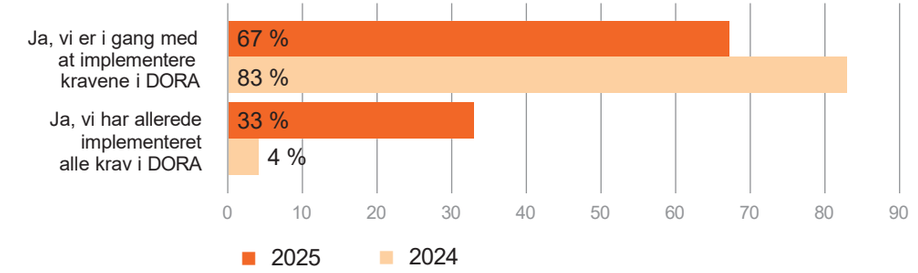
af de adspurgte virksomheder har allerede implementeret alle krav i DORA, og 67 % er i gang.

Har din virksomhed* en plan for, hvordan I vil imødekomme/implementere kravene i NIS2-direktivet?



*) Kun virksomheder, der har angivet, at de er omfattet af NIS2.

Har din virksomhed* en plan for, hvordan I vil imødekomme/implementere kravene i DORA-forordningen?



*) Kun virksomheder, der har angivet, at de er omfattet af DORA.

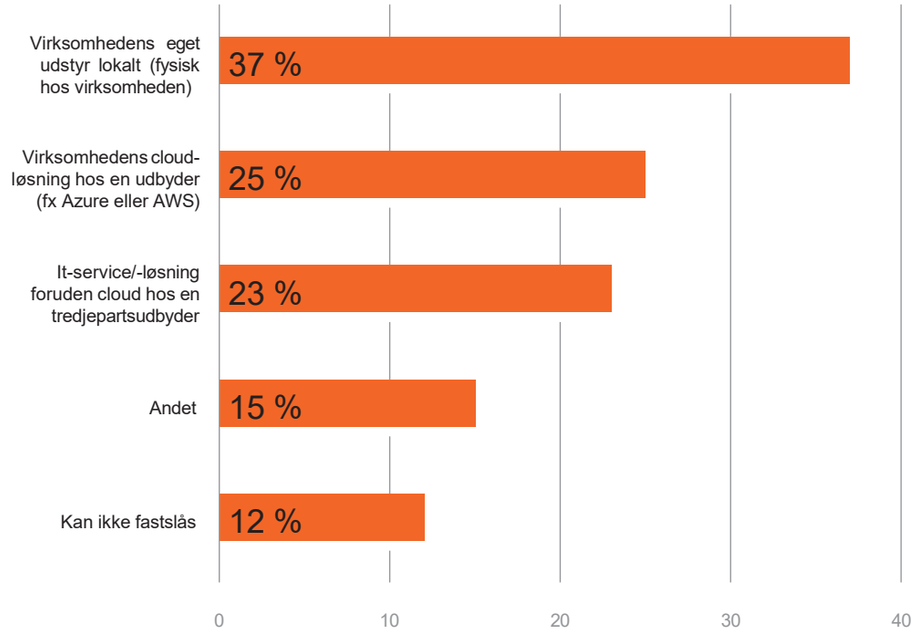
Anvender din virksomhed leverandører i forbindelse med kritiske it-systemer?

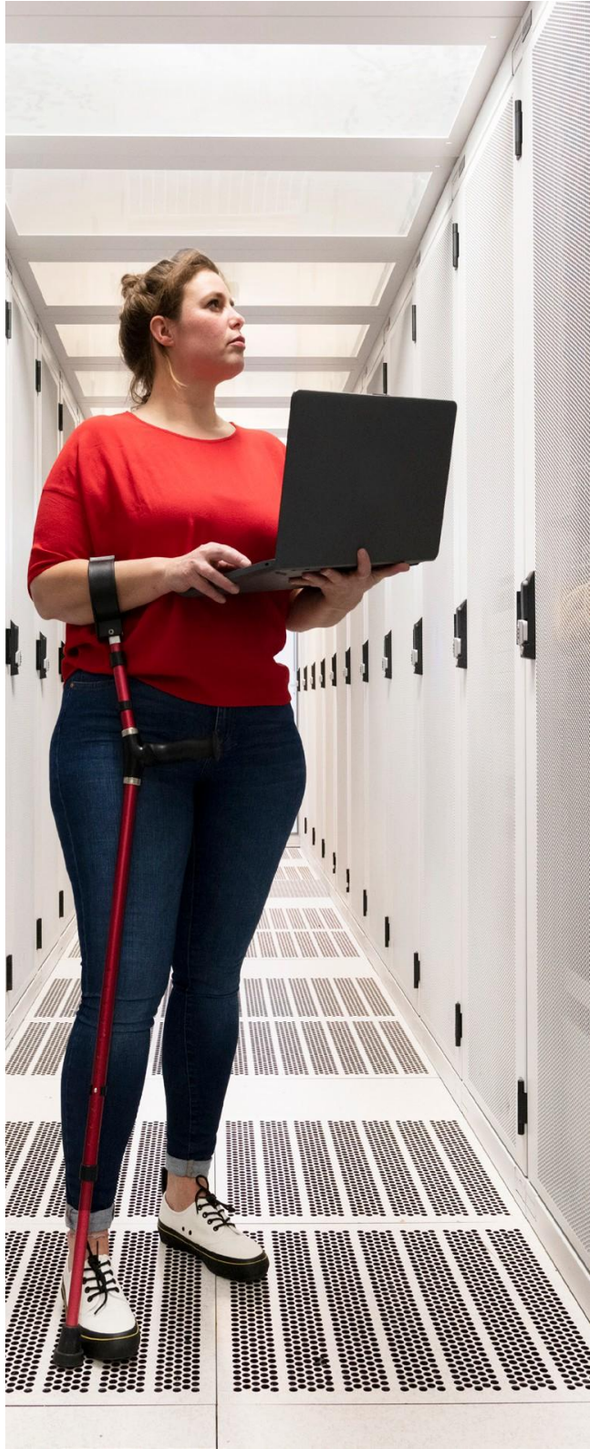
Outsourcing af en virksomheds it-infrastruktur indebærer en afgivelse af kontrol og et indskrænket ansvar for cybersikkerheden.

48 %

af respondenterne angiver, at en sikkerhedshændelse målrettet mod deres virksomhed har involveret cloud-løsninger hos en tredjepartsudbyder eller anden IT-service hos en tredjepartsudbyder.

Hvad var sikkerhedshændelsen, som var målrettet din virksomhed, relateret til?

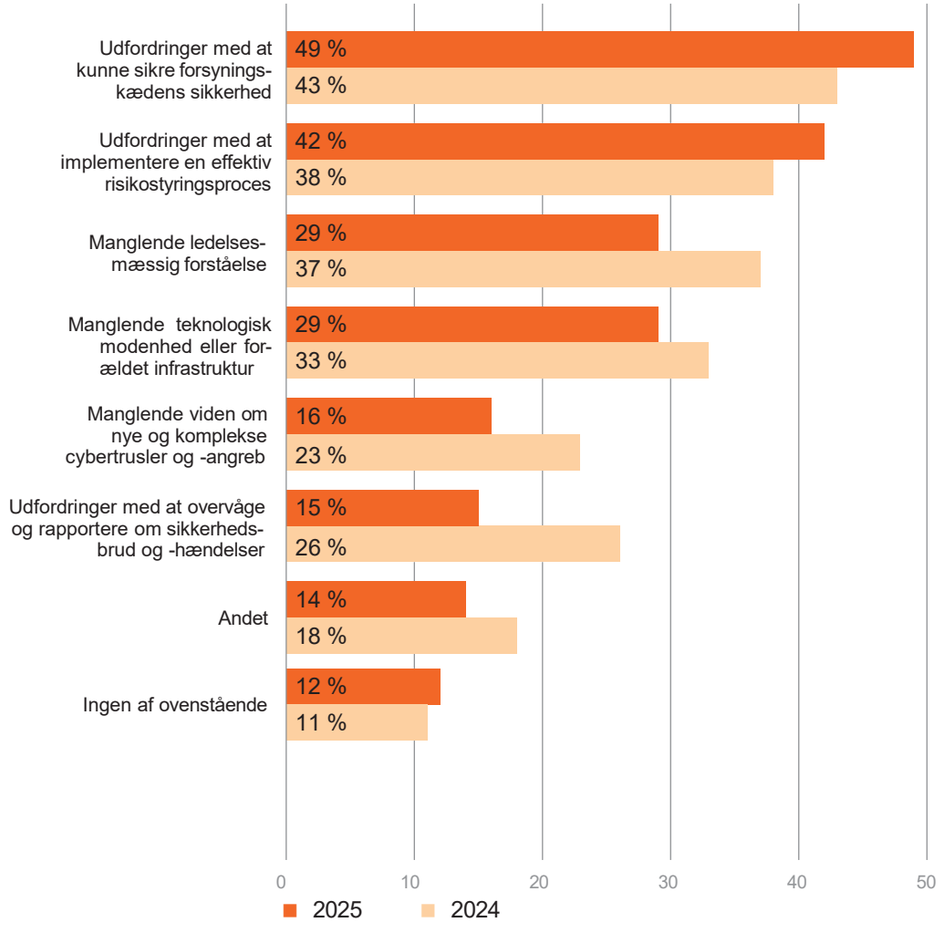




49 %

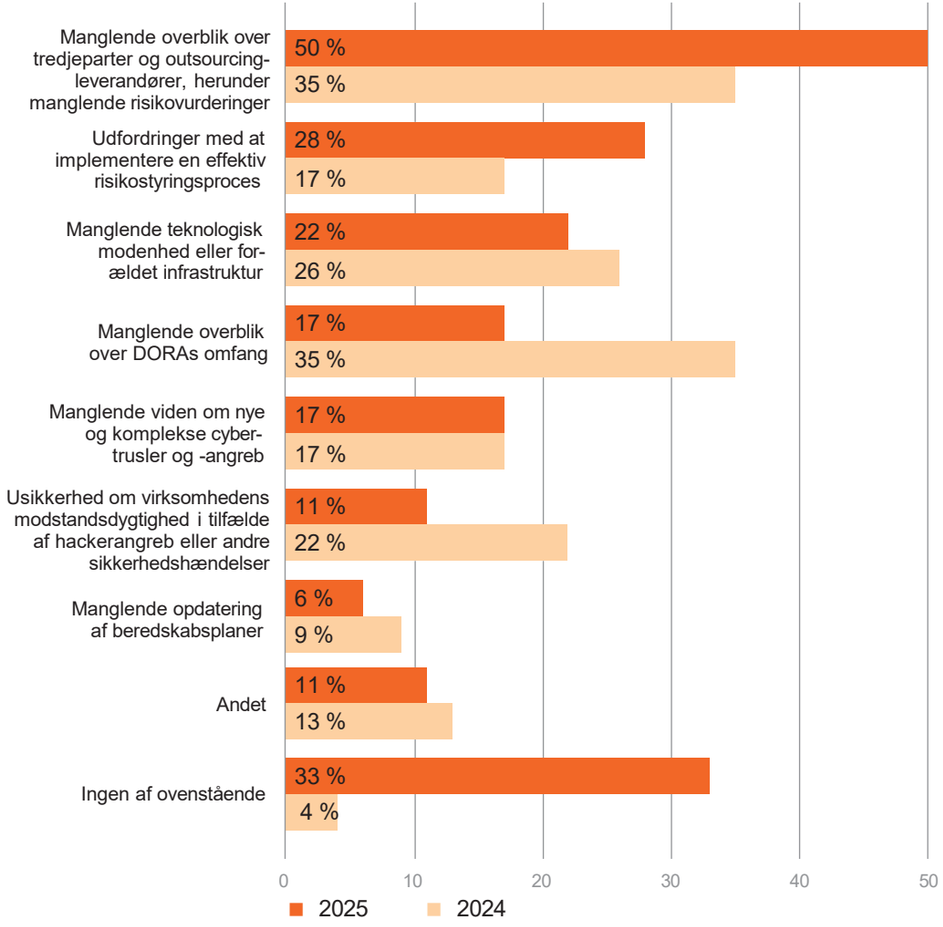
peger på udfordringer med sikkerheden i forsyningskæden som barriere for at kunne leve op til kravene i NIS2-direktivet.

Hvilke af følgende ser du som barrierer for, at din virksomhed* kan leve op til kravene i NIS2-direktivet?



*) Kun virksomheder, der har angivet, at de er omfattet af NIS2.

Hvilke af følgende ser du som barrierer for, at din virksomhed* kan leve op til kravene i DORA-forordningen?



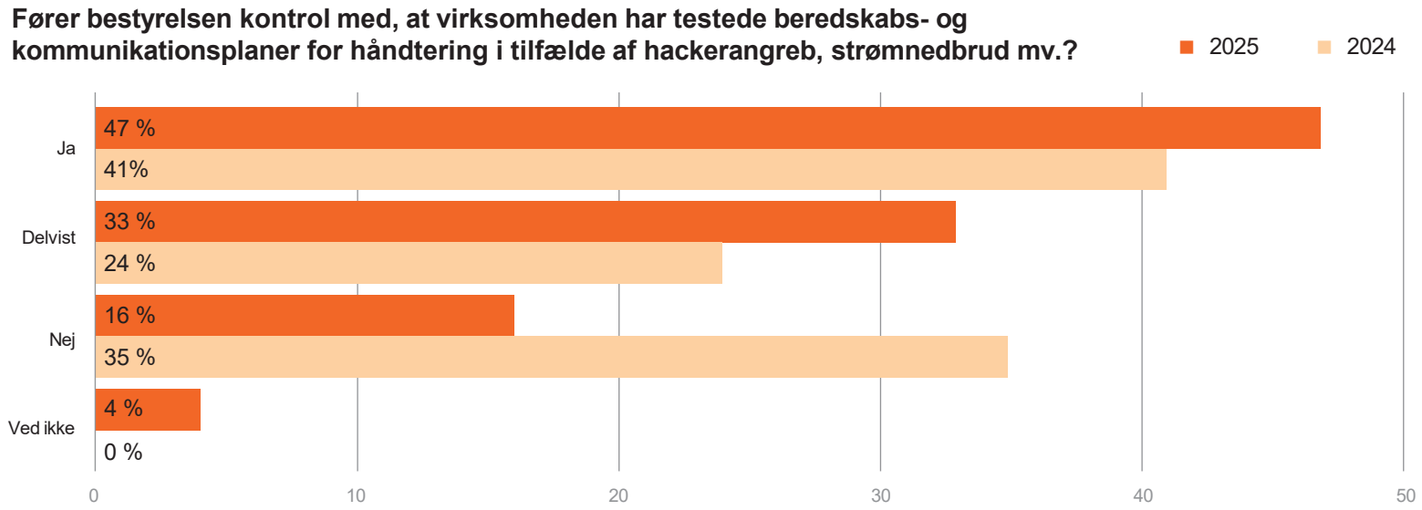
*) Kun virksomheder, der har angivet, at de er omfattet af DORA.

Cybersikkerhed på bestyrelsens dagsorden: En positiv udvikling

Cybercrime Survey 2025 viser, at cybersikkerhed i stigende grad er blevet en integreret del af bestyrelsens arbejde.

76 %

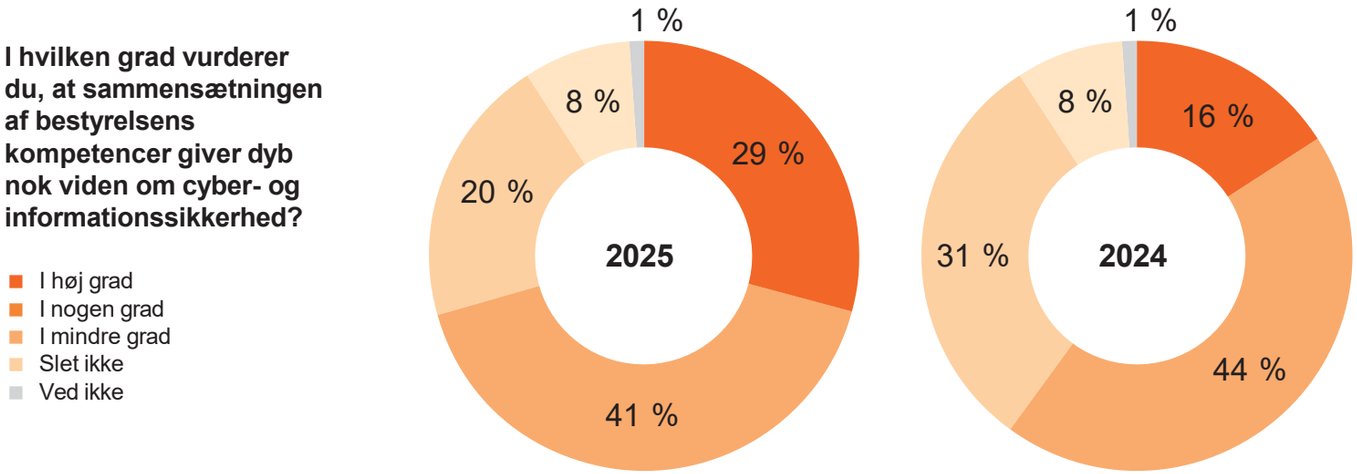
af respondenterne svarer, at cyber-sikkerhed indgår som en fast del af bestyrelsens årshjul.



29 %

af respondenterne vurderer, at bestyrelsen i høj grad har kompetencer, der giver dyb nok viden om cyber- og informationssikkerhed.

I hvilken grad vurderer du, at sammensætningen af bestyrelsens kompetencer giver dyb nok viden om cyber- og informationssikkerhed?



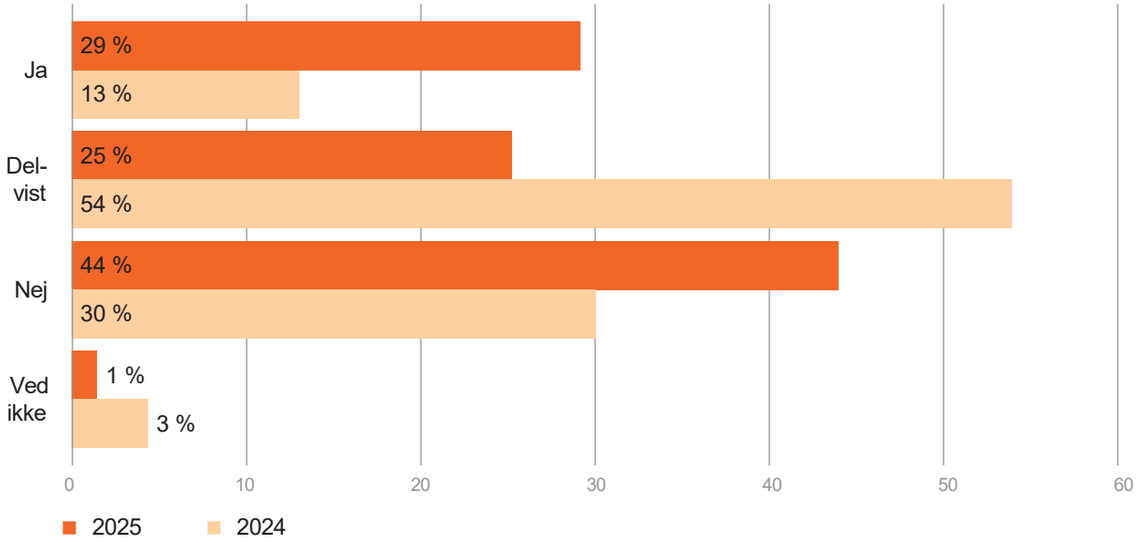
“

Andelen, der mener, at bestyrelsen kun i mindre grad besidder relevante kompetencer, er faldet fra 31 % til 20 %. Denne udvikling tyder på, at flere virksomheder har haft fokus på at styrke bestyrelsens kompetencer inden
for cybersikkerhed.

20 %

af respondenterne vurderer, at bestyrelsen i mindre grad har kompetencer, der giver dyb nok viden om cyber- og informationssikkerhed.

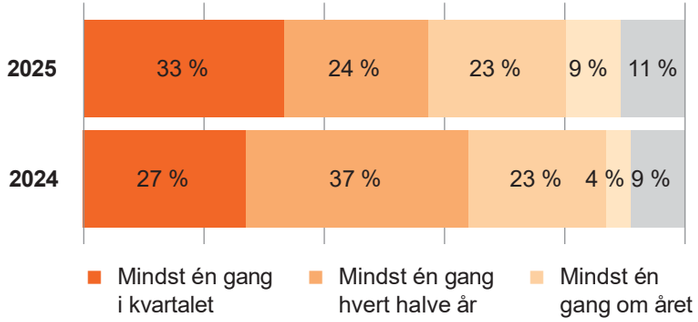
Modtager bestyrelsen træning i cyber- og informationssikkerhed?



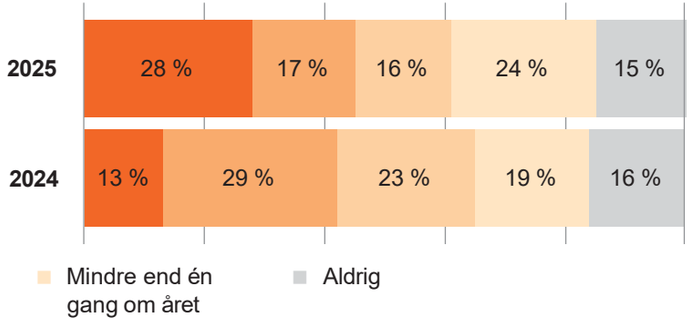
“

Indførelsen af EU-direktiverne NIS2 og DORA har øget kravene til virksomhedernes cybersikkerhed, hvor bestyrelsen nu har et direkte ansvar for at sikre tilstrækkelig styring af digitale risici og operationel robusthed.

Hvor ofte modtager og behandler bestyrelsen information vedrørende cyberrisici?



Hvor ofte behandler bestyrelsen cyberhændelser?

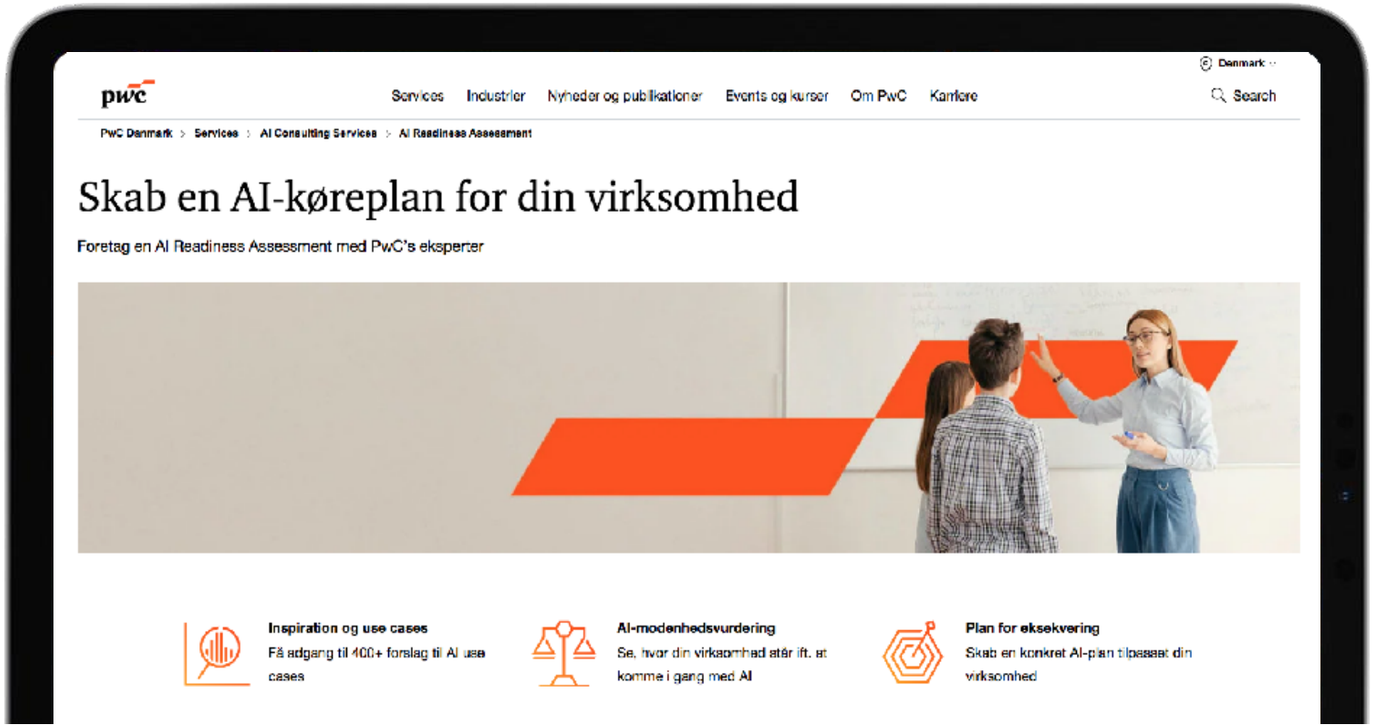


AI er fortsat en markant faktor i arbejdet med cybersikkerhed

I takt med den stigende digitalisering og kompleksiteten af cybertrusler intensiveres behovet for avancerede AI-værktøjer til at beskytte virksomheder.

72%

af virksomhederne anvender eller planlægger at bruge AI – en stigning fra 61% i 2024
Mange mangler stadig en plan for hvordan man sikrer brugen af AI i virksomheden eller har en ledelsesgodkendt praksis på området



Tak for i dag

Christian Kjær
Partner, Technology & Security,
København, PwC Denmark
E-mail: christian.kjaer@pwc.com