



Cybercrime Survey 2026

September 2026

Indhold

Cybersikkerhed i en tid med geopolitiske spændinger, digital afhængighed og AI	3
Cybersikkerhed i en verden under forandring	4
Cybersikkerhed på bestyrelsesdagsordenen	8
Investeringerne vokser, men prioriteterne skifter	12
Digital suverænitæt og afhængighed af udenlandske leverandører	16
Reguleringer i praksis: NIS2, DORA og AI Act	18
AI som både værktøj og trussel	21
OT-sikkerhed som den næste frontlinje	24
Om under-søgelsen	28
Tjekliste	29
Kontakt	30

52 %

af respondenterne er mere bekymrede for cybertrusler end for 12 måneder siden.

58 %

af virksomhederne er i høj grad afhængige af amerikanske eller andre ikke-EU-baserede cloud- og it-leverandører.

84 %

af bestyrelserne har cybersikkerhed som en fast del af årshjulet.

66 %

forventer, at cyber- og informationssikkerhedsbudgettet vokser inden for de næste 12 måneder.

Cybercrime Survey 2026 er baseret på besvarelser fra 326 ledere, sikkerhedsansvarlige og fagspecialister fra både den offentlige og den private sektor. Undersøgelsen giver et aktuelt indblik i, hvordan danske virksomheder oplever og håndterer et trusselsbillede, der i stigende grad formes af geopolitiske spændinger, teknologisk kompleksitet og en voksende afhængighed af udenlandske leverandører. Samtidig træder emner som digital suverænitæt og OT-sikkerhed frem som helt nye strategiske dagsordner.

Cybersikkerhed i en tid med geopolitiske spændinger, digital afhængighed og AI



Christian Kjær

Partner, Cyberrisikostyring,
PwC

Cybersikkerhed handler i dag om langt mere end teknologi. Det handler om, hvordan vi som samfund og virksomheder navigerer i en tid, hvor digital afhængighed, geopolitiske spændinger og accelererende teknologiudvikling smelter sammen til ét sammenhængende risikobillede. Årets undersøgelse viser, at danske virksomheder har taget dette til efterretning, men også, at der er områder, hvor modenheden endnu ikke matcher trusselsniveauet.

Bestyrelser og direktioner er i højere grad end nogensinde ansvarlige for at forstå og prioritere cybersikkerhed. Samtidig kræver nye reguleringer som NIS2, DORA og EU's AI Act, at man ikke blot forholder sig til egen organisation, men også til hele leverandørkæden. Det er ikke længere nok at have styr på egne systemer – man skal også kunne dokumentere, at man har styr på sine partners systemer.

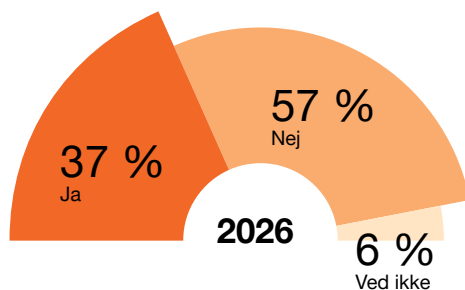
I dette års Cybercrime Survey belyser vi blandt andet, hvordan geopolitiske spændinger, stigende digital afhængighed og den hastige udvikling inden for AI er med til at ændre trusselsbilledet og stille nye krav til danske virksomheders og offentlige organisationers cybersikkerhed.



Samfund og virksomheder navigerer i en tid, hvor digital afhængighed, geopolitiske spændinger og accelererende teknologiudvikling smelter sammen til ét sammenhængende risikobillede.

Cyber-sikkerhed i en verden under forandring

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

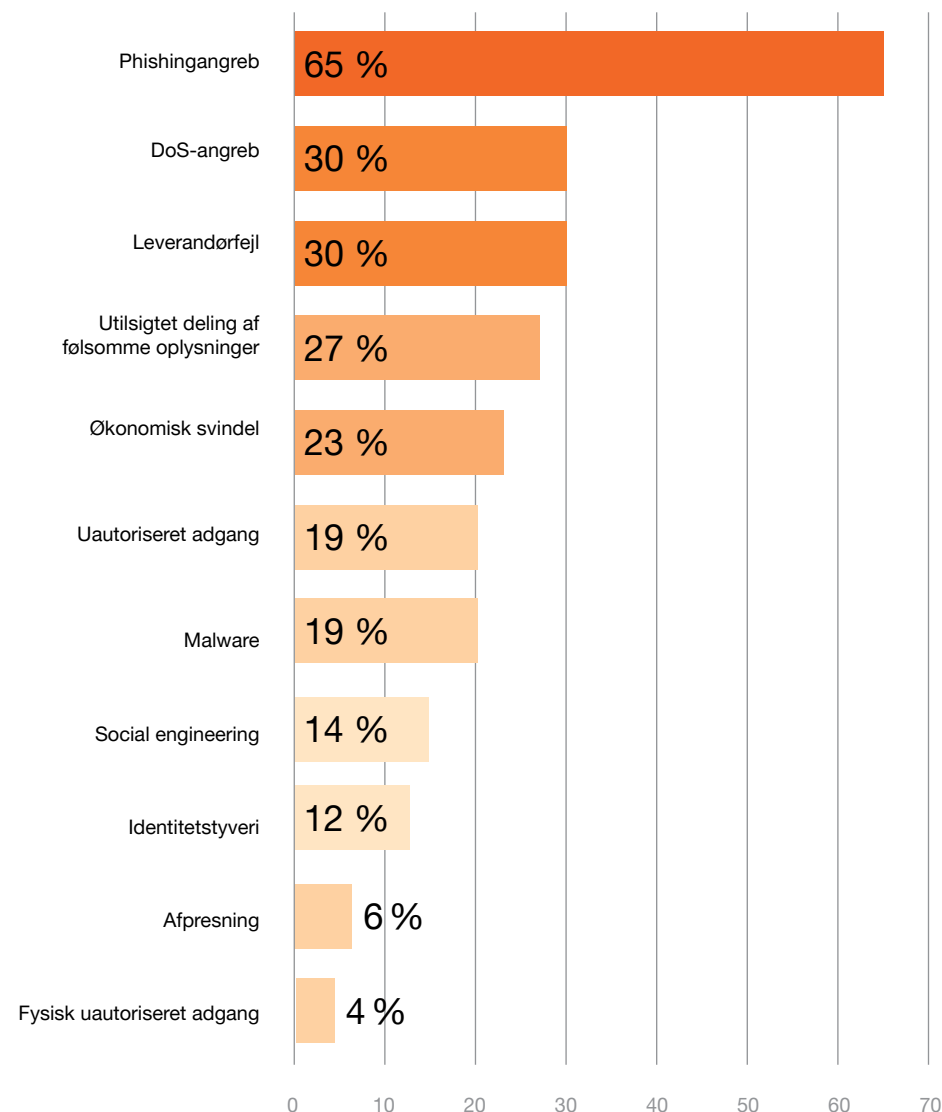


Danske virksomheder og offentlige organisationer opererer i et foranderligt trusselsbillede. Krigen i Ukraine fortsætter, spændingerne mellem USA, Kina og Europa er tiltaget, og hybridtrusler mod kritisk infrastruktur er blevet en del af den sikkerhedspolitiske virkelighed. Samtidig har fremkomsten af generative AI-værktøjer og en stigende regulering skabt en ny balance mellem muligheder og risici.

Cybercrime Survey 2026 tegner et billede af, at 37 % af virksomhederne har oplevet en sikkerhedshændelse inden for de seneste 12 måneder. Dertil kommer, at 22 % har været udsat for et målrettet angreb, hvor netop deres organisation har været genstand for en bevidst udvælgelse. Det understreger, at cybertruslen ikke kun består af tilfældige hændelser, men i stigende grad også af målrettede og strategiske angreb.

Blandt de virksomheder, der har været ramt, er phishingangreb den mest udbredte hændelsestype: hele 65 % rapporterer at have været udsat for phishing. Herefter følger DoS-angreb (30 %), leverandørfejl (30 %), utilsigtet deling af følsomme oplysninger (27 %) samt økonomisk svindel (23 %). Tallene understreger, at truslerne rammer bredt, både gennem menneskelige, tekniske og forsyningskæde-relaterede kanaler.

Hvilken type sikkerhedshændelse(r) var der tale om?

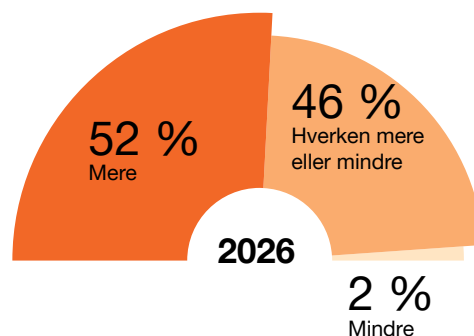


52 %

af respondenterne,
angiver at de er
mere bekymrede for
cybertrusler nu end
for 12 måneder siden.

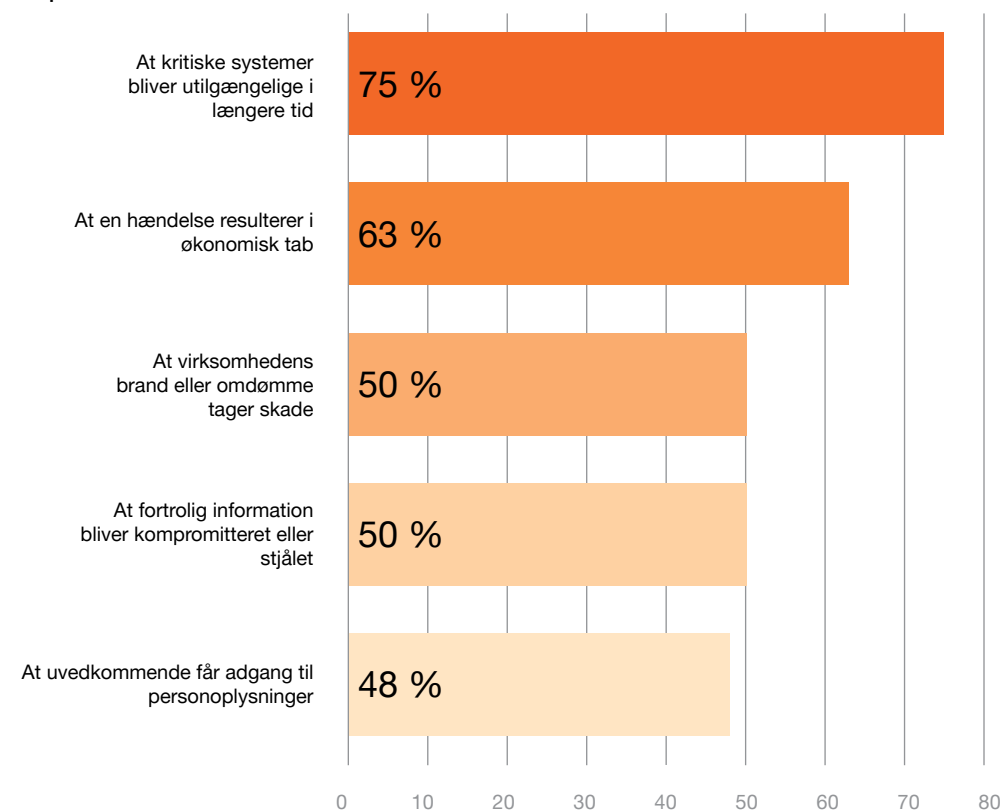
Samtidig angiver 52 % af respondenterne, at de er mere bekymrede for cybertrusler nu end for 12 måneder siden, og kun 2 % er blevet mindre bekymrede. Bekymringen retter sig først og fremmest mod driftskritiske forhold: 75 % frygter længerevarende nedbrud på kritiske systemer, 63 % peger på økonomiske tab, og 50 % bekymrer sig om skader på brand og omdømme, ligesom 50 % nævner kompromittering af fortrolige oplysninger. Bekymringen for uautoriseret adgang til persondata er også høj (48 %).

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



Hvad er din virksomheds største bekymring i relation til konsekvenserne af en cyberhændelse?

Top 5



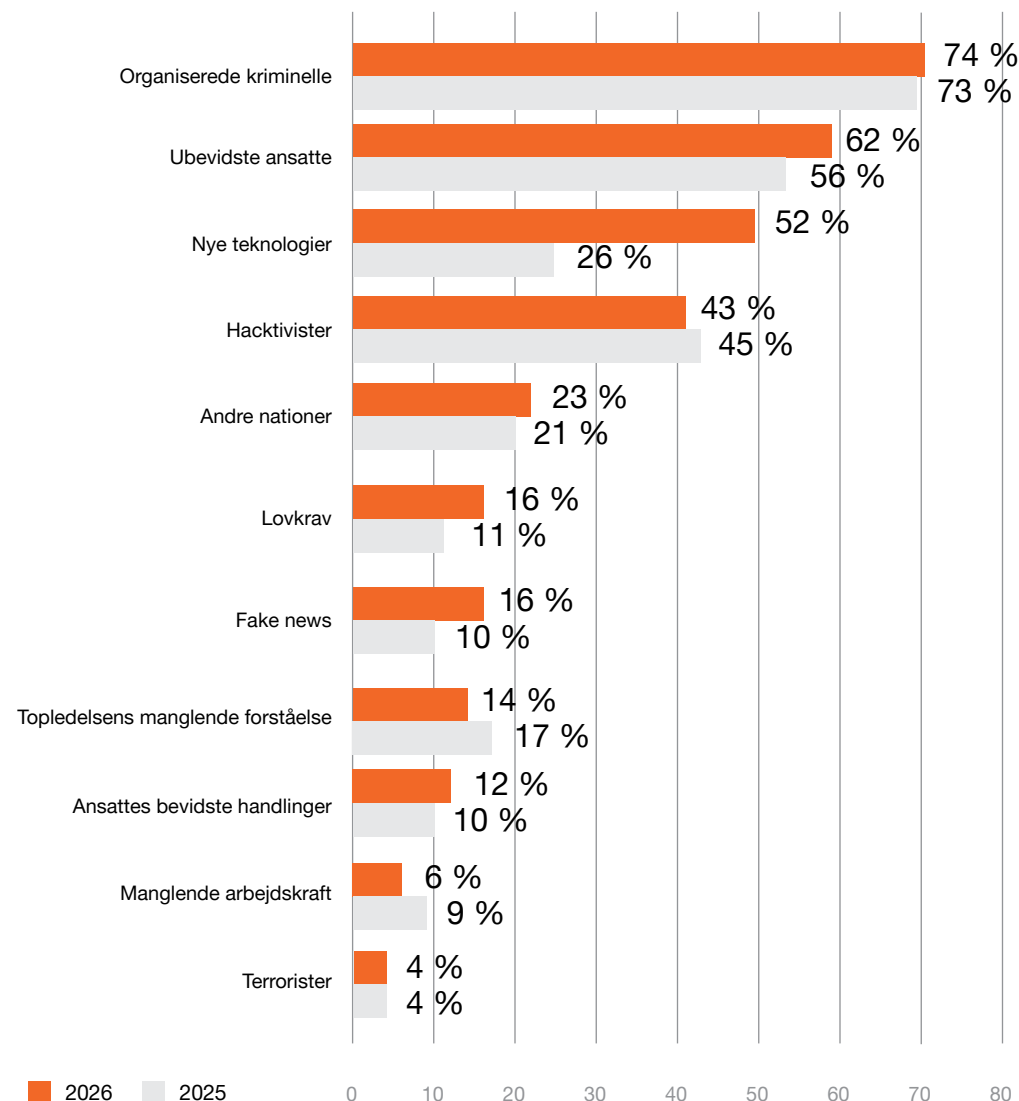


Trusselsbilledet: Fra tilfældige angreb til strategisk målrettede

Ligesom i tidligere år udgør organiserede kriminelle den største trussel mod danske virksomheders cyber- og informations-sikkerhed. Hele 74 % peger på denne gruppe. Men et andet tal fanger opmærksomheden: De mange nye teknologier (AI, IoT, blockchain, cloud) opfattes nu som en trussel af 52 % af respondenterne – en meget markant stigning fra 26 % i 2025.

Den relative fordobling afspejler, at virksomhederne har oplevet, hvordan særligt AI kan bruges til at automatisere og skalere angreb, og hvordan IoT- og cloud-miljøer udvider angrebsfladen. Samtidig følger 62 % af respondenterne op med, at medarbejdernes ubevidste handlinger fortsat udgør en central trussel, mens hacktivister (43 %) og andre nationer/efterretningstjenester (23 %) også spiller en synlig rolle i trusselsbilledet.

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





Phishing: Stadig den mest udbredte angrebsform

Phishing er en form for it-kriminalitet, hvor cyberkriminelle forsøger at narre modtageren til at afgive fortrolige oplysninger som brugernavne, adgangskoder eller betalingsdata. Angrebene sker typisk via e-mails eller sms'er, der efterligner legitime afsendere. PwC's Global Digital Trust Insights 2026 viser, at 25 % af sikkerhedsledere rangerer social engineering som en af de trusler, de er mindst forberedte på, og rapporten peger på, at AI-drevne angreb i stigende grad udfordrer virksomheders evne til at opdage og stoppe forsøgene i tide. Rapporten viser desuden, at over halvdelen af organisationerne vurderer sig som "ikke særlig kapable" til at modstå angreb, der udnytter svage autentificerings- og adgangskontroller, hvilket understreger vigtigheden af MFA. Den bedste beskyttelse er derfor en kombination af teknisk filtrering, MFA og løbende awareness-træning af medarbejderne.



Læs mere [her](#)



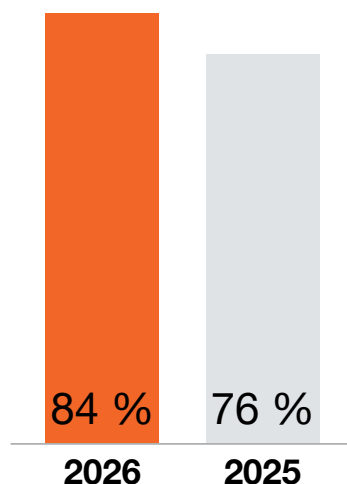
Cyber-sikkerhed på bestyrelses-dagsordenen

84 %

af respondenterne svarer, at cybersikkerhed er en fast del af bestyrelsens årshjul.

Cybersikkerhed har etableret sig som et fast punkt på bestyrelsens dagsorden. I 2026 svarer 84 % af respondenterne, at cybersikkerhed er en fast del af bestyrelsens årshjul. Det er en stigning fra 76 % i 2025 og bekræfter, at området fortsat rykker tættere på den strategiske ledelseskerne. Udviklingen afspejler både det stigende trusselsniveau og de nye regulatoriske krav, særligt fra NIS2 og DORA, der pålægger bestyrelsen et direkte ansvar for cyberrisici.

Har bestyrelsen cybersikkerhed som en fast del af sit årshjul?

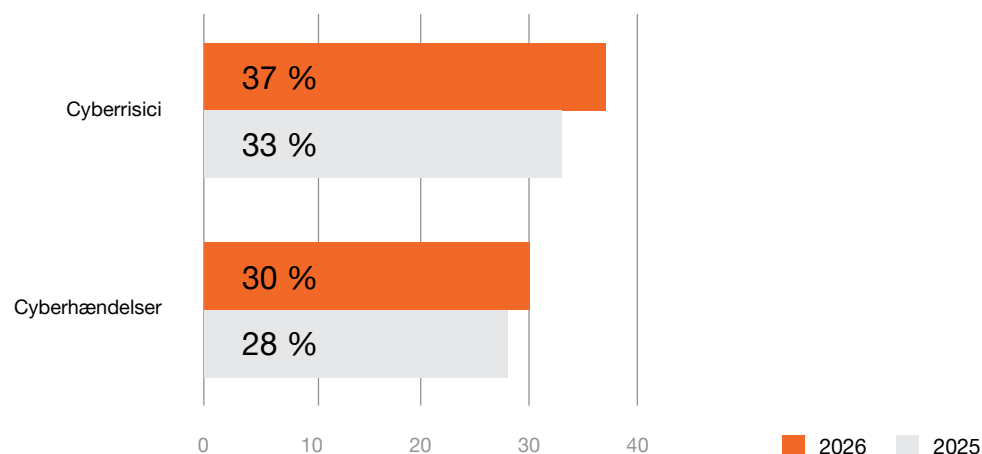


Behandlingsfrekvensen halter efter den formelle forankring

Selvom cybersikkerhed står højere på dagsordenen end nogensinde, sker den løbende behandling stadig relativt sjældent. Kun 37 % af bestyrelserne modtager og behandler information om cyberrisici mindst én gang i kvartalet – en marginalt højere andel end i 2025. Tilsvarende svarer 30 %, at bestyrelsen behandler konkrete cyberhændelser mindst kvartalsvist. Det efterlader et betydeligt gab mellem den formelle forankring og den reelle, løbende opfølgning.

Det understreger behovet for, at cybersikkerhed ikke alene håndteres som et fast punkt på årshjulet, men indgår løbende i bestyrelsens arbejde med risici og forretningskritiske forhold. Særligt i lyset af det hastigt skiftende trusselsbillede, herunder AI-drevne angreb og geopolitiske hændelser, er der god grund til at genoverveje frekvensen og formatet for bestyrelsens cyberrapportering.

Bestyrelsens behandling af cyberrisici og cyberhændelser pr. kvartal



37 %

af respondenterne angiver, at bestyrelsen fører fuld kontrol med, at der findes testede beredskabs- og kommunikationsplaner.

Bestyrelsens kontrol med beredskabet

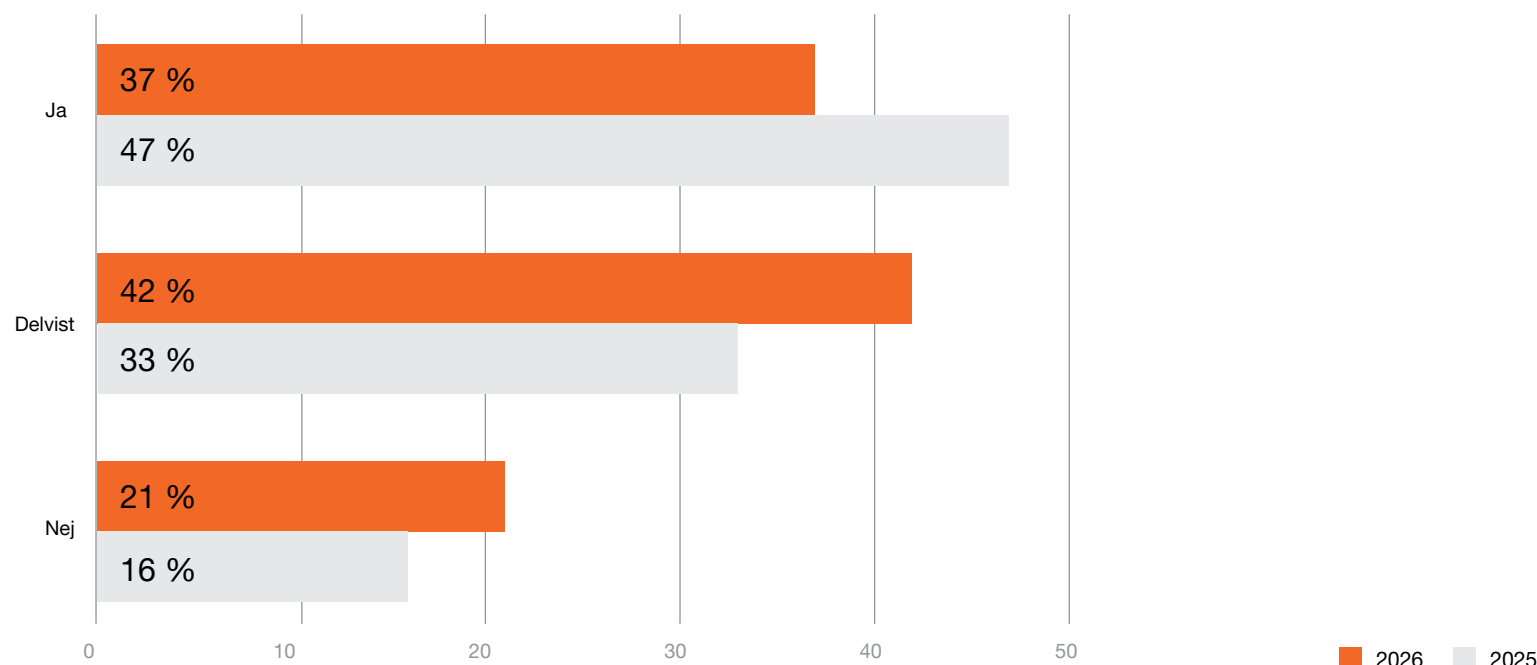
Årets resultater viser en interessant forskydning i, hvordan bestyrelsen udøver kontrol med organisationens beredskab. I 2026 angiver 37 % af respondenterne, at bestyrelsen fører fuld kontrol med, at der findes testede beredskabs- og kommunikationsplaner. Det er lavere end i

2025, hvor andelen var 47 %. Til gengæld svarer hele 42 % i 2026, at bestyrelsen delvist fører denne kontrol mod 33 % året før.

Bevægelsen kan tolkes som et udtryk for, at flere bestyrelser i praksis vurderer deres kontrol som delvis snarere end fuld, hvilket kan afspejle en mere kritisk selv vurdering

af, hvor grundigt planerne reelt er testet. Udviklingen understreger vigtigheden af, at bestyrelsen ikke blot forholder sig til, om planer eksisterer, men også validerer, at de faktisk testes og virker under pres, da det netop er denne dybde, der afgør, hvor hurtigt en organisation kan komme sig efter et alvorligt angreb.

Fører bestyrelsen kontrol med, at virksomheden har testede beredskabs- og kommunikationsplaner for håndtering i tilfælde af hackerangreb, strømnedbrud mv.?





Bestyrelsens rolle under NIS2 og DORA

Med NIS2 og DORA har bestyrelsen fået et direkte, personligt ansvar for at sikre tilstrækkelig cyberrobusthed. Det betyder, at bestyrelsen ikke længere kan nøjes med at delegeres ansvaret, den skal aktivt kunne dokumentere, at den forstår risikoen, godkender risikoappetit og følger op på implementeringen. I praksis kræver det både rapportering på et strategisk niveau og en løbende dialog med direktionen. PwC anbefaler, at bestyrelsen fastlægger en fast kadence for rapportering om cybersikkerhed med mindst kvartalsvise opdateringer fra direktionen, suppleret af en årlig, dybere gennemgang af risikovurderinger og ekstern validering af effekten af igangsatte tiltag.

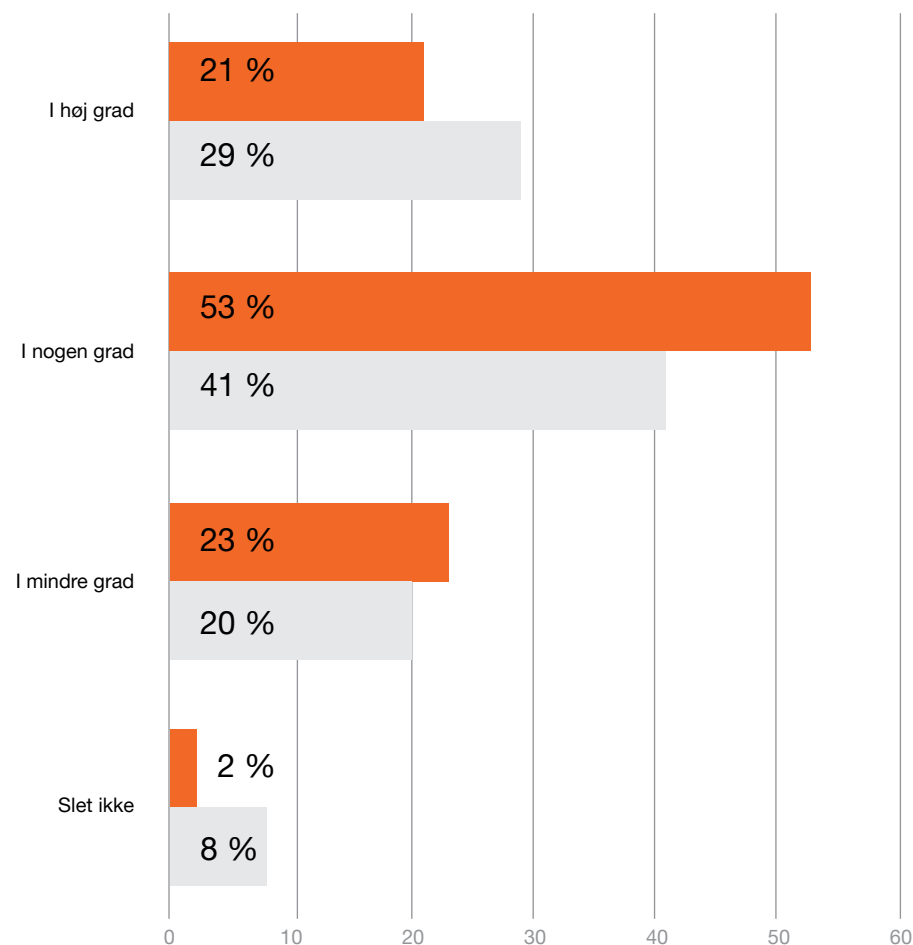


Læs mere [her](#)

Bestyrelsens cybersikkerhedskompetencer kræver fortsat opmærksomhed

Et af de mest bemærkelsesværdige resultater i årets undersøgelse handler om bestyrelsens kompetencer. Kun 21 % af respondenterne vurderer, at bestyrelsen i høj grad har eller sikrer kompetencer, der giver dyb nok viden om cyber- og informationssikkerhed. Det er et fald fra 29 % i 2025. Samtidig angiver 23 %, at bestyrelsen kun i mindre grad besidder tilstrækkelige kompetencer, mod 20 % året før. Hele 53 % svarer "i nogen grad", hvilket peger på, at mange bestyrelser har en vis indsigt, men uden at kompetenceniveauet opleves som tilstrækkeligt dybt i lyset af de nye udviklede reguleringer inden for cybersikkerhed. Tilbagegangen viser, at der fortsat er behov for at styrke bestyrelsernes viden om cybersikkerhed, i takt med at kravene og trusselsbilledet udvikler sig. Med stigende krav til personligt ansvar, rapportering og løbende risikostyring får bestyrelserne et større ansvar for at forstå og følge udviklingen i cybersikkerheden. Det stiller nye krav til rekruttering, uddannelse og vidensdeling mellem CISO'en, direktionen og bestyrelsen.

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



2026 2025



PwC erfarer

PwC oplever, at de virksomheder, der lykkes bedst med at forankre cybersikkerhed på bestyrelsesniveau, arbejder med tre tiltag: For det første oversætter de tekniske risici til forretningskonsekvenser, fx tabt omsætning, mistede kunder eller regulatoriske sanktioner. For det andet etablerer de en fast rapporteringsstruktur med tydelige KPI'er og modenhedsindikatorer, så udviklingen kan følges over tid. Og for det tredje investerer de i decideret cyberuddannelse af bestyrelsen, ofte i form af workshops, simuleringsøvelser og adgang til uafhængige eksperter. Denne kombination sikrer, at bestyrelsen ikke blot "afkrydser" et compliance-punkt, men reelt fungerer som strategisk sparringspartner for CISO og direktionen.



Læs mere [her](#)



Investeringerne vokser, men prioriteterne skifter

66 %

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

Cybersikkerhed er ikke længere et spørgsmål om, hvorvidt der skal investeres, men hvordan investeringerne skal fordeles og prioriteres. I 2026 forventer 66 % af respondenterne, at deres cyber- og informationssikkerhedsbudget vil vokse inden for de næste 12 måneder. Det er en fortsat stigning i investeringsmomentum, men billedet er mere afdæmpet end tidligere.

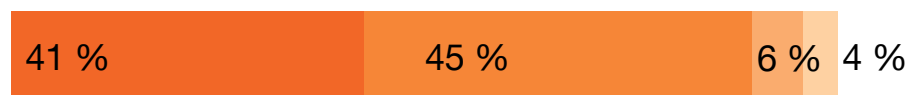
Sammenlignet med 2025 er der to markante udviklinger. For det første er andelen, der forventer moderate stigninger på 11-25 %, steget til 45 % (mod 42 % i 2025). For det andet er andelen, der overhovedet forventer budgetvækst, steget fra 64 % til 66 %. Det tegner et billede af en investeringsstrategi, der er ved at stabilisere sig efter de store NIS2- og DORA-relaterede investeringer i 2024 og 2025, men hvor cybersikkerhed nu opfattes som en fast og voksende driftsomkostning.

Forventer eller tror du, at din virksomheds cyber- og informations-sikkerhedsbudget vil vokse inden for de næste 12 måneder?

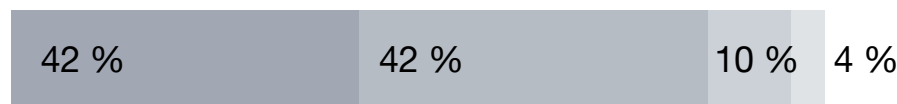


■ 2026 ■ 2025

Hvor meget forventer du, at cyber- og informations-sikkerhedsbudgettet vil vokse med inden for de næste 12 måneder?



■ 1-10 % ■ 11-25 % ■ 26-50 % ■ > 50 %



■ 1-10 % ■ 11-25 % ■ 26-50 % ■ > 50 %



PwC erfarer

PwC anbefaler, at virksomheder styrker deres beredskab ud fra et hybridtrussel-perspektiv, hvor man ikke kun over isolerede cyberscenerier, men også kombinerede forløb, hvor cyberangreb sammenfalder med fysiske hændelser eller andre forstyrrelser. PwC's Global Digital Trust Insights 2026 anbefaler konkret, at direktion og bestyrelse deltager i scenarieøvelser, der simulerer såkaldte "hybrid threat operations", og at cybersikkerhed gøres til et fælles ansvar fra bestyrelseslokalet til driftsorganisationen. Det indebærer regelmæssigt at stressteste beslutningsveje og eskalering samt en løbende gennemgang af leverandørkæder for at identificere geopolitiske sårbarheder, fx afhængighed af enkelte teknologier eller lande

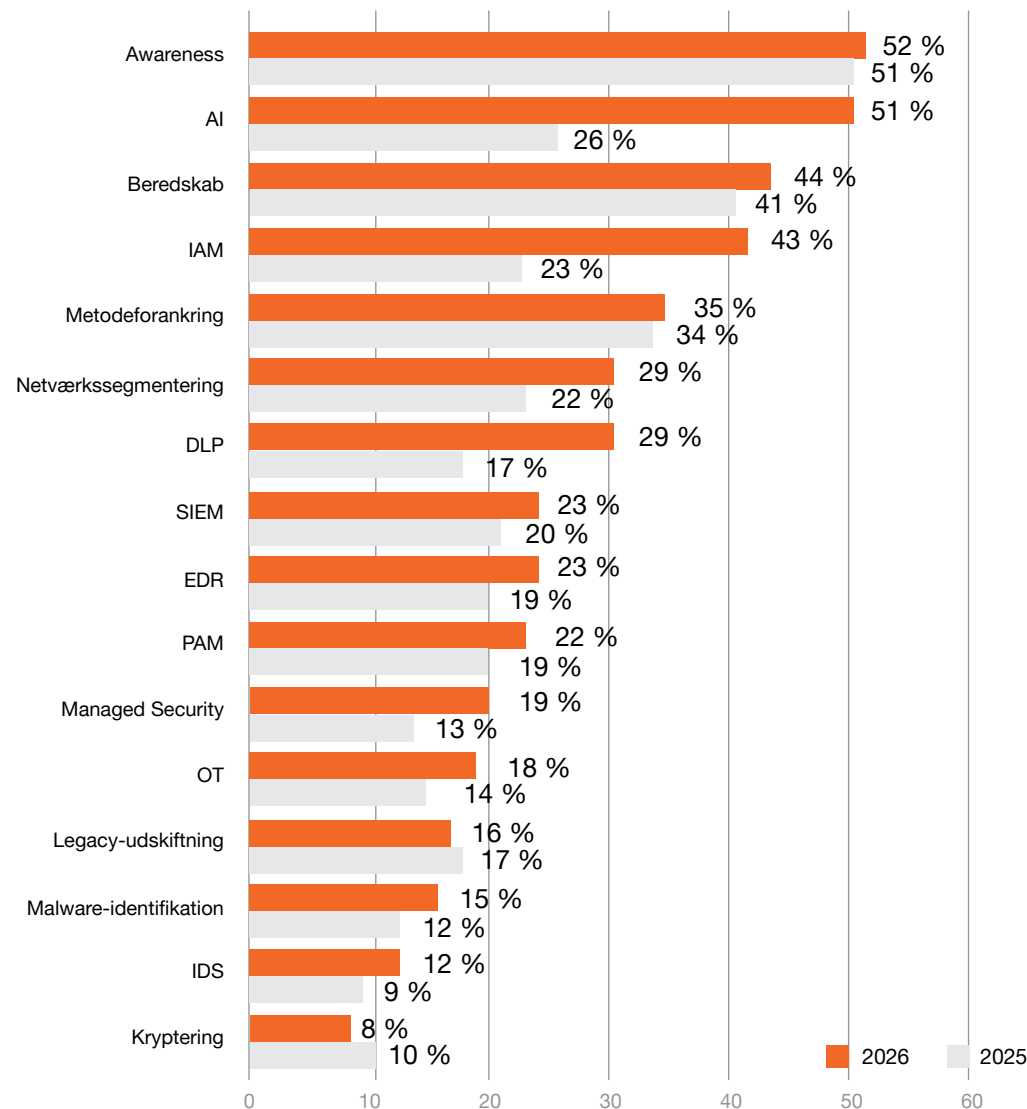


Læs mere [her](#)

Hvor placeres investeringerne i 2026?

Årets undersøgelse afslører en forskydning i, hvad virksomhederne prioriterer. Awareness-træning topper stadig listen med 52 %, men følges tæt af kunstig intelligens (AI), som hele 51 % af virksomhederne fremhæver som en af de højst prioriterede investeringer. Det er en markant stigning fra 26 % i 2025 og en tydelig indikation af, at AI er i færd med at blive et centralt element i danske virksomheders sikkerhedsstrategi. Beredskab og business continuity (44 %) samt Identity and Access Management, IAM, (43 %) placerer sig ligeledes højt, mens metodeforankring (ISO 2700x, CIS 18, NIST) med 35 % afspejler et fortsat behov for at systematisere og dokumentere sikkerhedsindsatsen, ikke mindst i lyset af NIS2 og DORA. Netværkssegmentering og Data Loss Prevention (DLP) prioriteres begge af 29 % af virksomhederne, mens SIEM (23 %), EDR (23 %), PAM (22 %) og OT-sikkerhed (18 %) tilsammen tegner et billede af en helhedsorienteret tilgang, hvor teknisk beskyttelse, identitetsstyring og organisatorisk forankring vægtes højt. Geopolitik og hybridtrusler ændrer risikobilledet

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

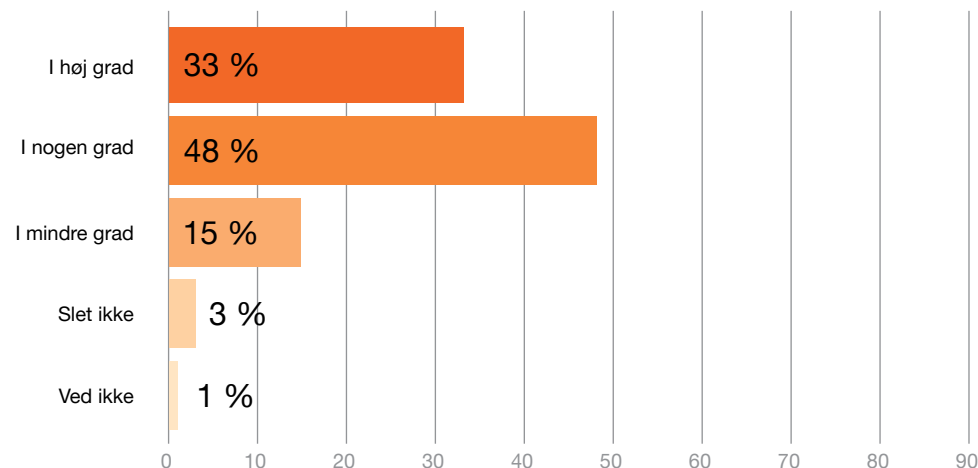




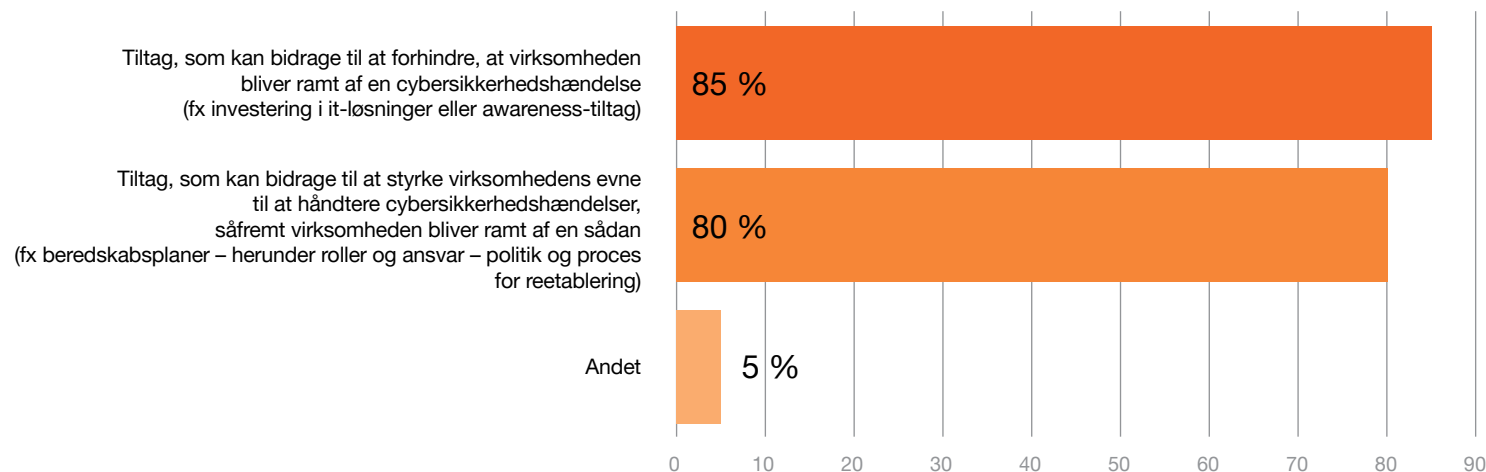
Geopolitik og hybridtrusler ændrer risikobilledet

Sjældent har det geopolitiske landskab spillet så tydeligt ind på danske virksomheders cybersikkerhedsagenda. Krigen i Ukraine fortsætter, forholdet mellem USA og Europa er præget af øgede spændinger, og Kinas stigende teknologiske selvstændighed påvirker globale markeder og forsyningskæder. Samtidig ser vi en stigning i hybridtrusler, hvor cyberangreb, misinformation og fysiske sabotagehændelser vikles sammen til én sammenhængende trusselsform.

I hvilken grad hænger bekymringen sammen med den geopolitiske situation?



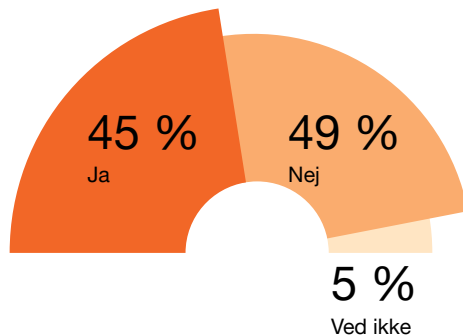
Hvilke nye cybersikkerhedstiltag har din virksomhed implementeret som følge af den øgede bekymring for cybertrusler?



52 %

af respondenterne er mere bekymrede for cybertrusler i dag end for 12 måneder siden.

Har din virksomhed planlagt eller implementeret nye cybersikkerhedstiltag som følge af den geopolitiske situation?



Undersøgelsen viser, at 52 % af respondenterne er mere bekymrede for cybertrusler i dag end for 12 måneder siden. Blandt de bekymrede peger 33 % på, at bekymringen i høj grad hænger sammen med den geopolitiske situation, og yderligere 48 % oplever, at det er tilfældet i nogen grad. Tilsammen kobler dermed 81 % af de bekymrede virksomheder deres uro direkte til den internationale situation.

45 % af virksomhederne har allerede iværksat eller planlagt nye cybersikkerhedstiltag som direkte respons på den geopolitiske situation. Blandt disse fokuserer 85 % på forebyggende tiltag (fx investeringer i tekniske løsninger og awareness), mens 80 % arbejder med responskapacitet (fx business continuity-planer, roller og ansvar). Det vidner om en helhedsorienteret tilgang, hvor virksomhederne både forsøger at reducere sandsynligheden for et angreb og styrke evnen til at komme sig, hvis uheldet er ude.



Hybridtrusler: Når cyber, misinformation og fysisk sabotage smelter sammen

Hybridtrusler beskriver situationer, hvor statslige eller statssponserede aktører kombinerer forskellige virkemidler for at destabilisere modstandere. Det kan være cyberangreb på kritisk infrastruktur, spredning af misinformation via sociale medier og målrettede fysiske aktioner. For danske virksomheder, særligt inden for energi, transport, finans og forsyning, betyder det, at cybersikkerhed må tænkes sammen med fysisk sikkerhed, forretningsberedskab og kommunikationsberedskab i én samlet ramme.

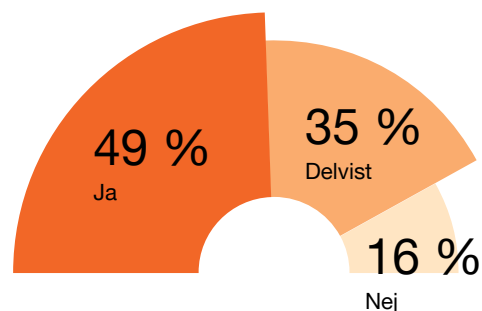


Læs mere [her](#)



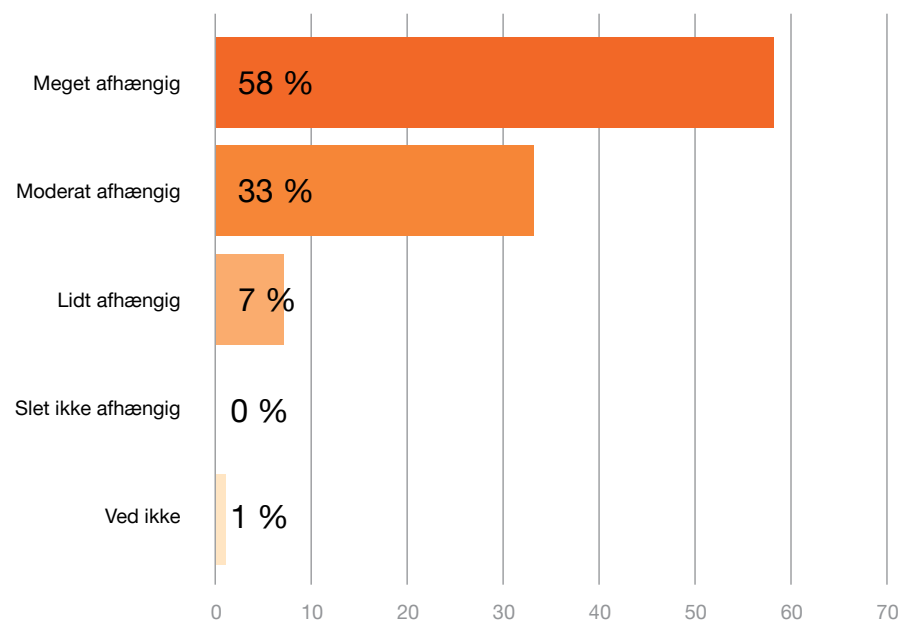
Digital suverænitet og afhæn- gighed af udenlandske leverandører

Er digital suverænitet
et emne, der behandles
på ledelses- eller
bestyrelsesniveau?



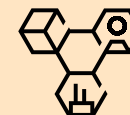
Digital suverænitet, dvs. evnen til selv at kontrollere sine data, sin infrastruktur og sin teknologi, har på blot ét år bevæget sig fra at være et akademisk begreb til at være en konkret diskussion i mange danske organisationer. Årets undersøgelse viser, at 49 % af respondenterne allerede har digital suverænitet på dagsordenen i ledelse eller bestyrelse. Yderligere 35 % arbejder delvist med det, mens kun 16 % endnu ikke har taget emnet op.

Hvor afhængig er jeres virksomhed af amerikanske eller andre ikke-EU-baserede cloud- og it-leverandører?



Afhængigheden af amerikanske og ikke-EU-baserede leverandører

Blandt de virksomheder, der anvender leverandører til kritiske it-systemer, angiver 58 %, at de i høj grad er afhængige af amerikanske eller andre ikke-EU-baserede cloud- og it-leverandører. Yderligere 33 % er moderat afhængige, og kun 7 % vurderer, at afhængigheden er beskeden.



Hvad er digital suverænitet i praksis?

Digital suverænitet handler ikke om at afskaffe amerikanske eller globale leverandører, men om at have et bevidst, dokumenteret og robust forhold til dem. I praksis betyder det for det første, at man kender og klassificerer sine data og forstår, hvor de opbevares og behandles. Derudover at man har exit-strategier for kritiske leverandører, og at man overvejer europæiske eller danske alternativer for de mest kritiske funktioner. Det indebærer også, at man sikrer kontraktuelle garantier for dataadgang og -portabilitet, og at man tester beredskabet for et scenarie, hvor adgangen til en central udenlandsk platform ophører eller begrænses.

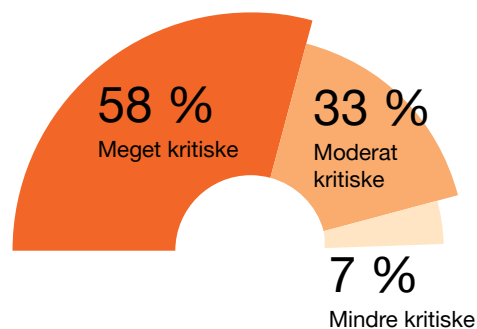


Læs mere [her](#)

73 %

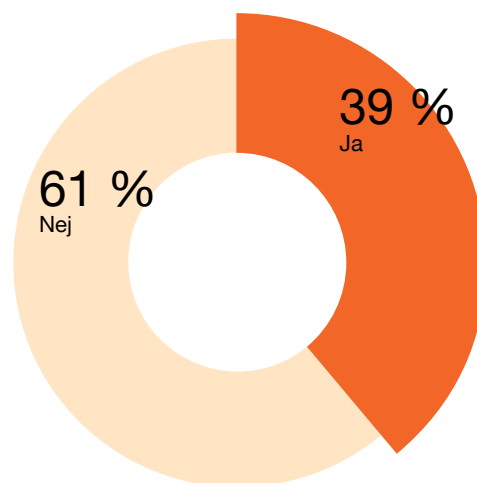
af respondenterne
peger på manglen på
reelle alternativer som
den største hindring
for at reducere deres
afhængighed af
specifikke leverandører.

Hvor kritiske er disse
systemer for forretningen?



Denne afhængighed vurderes samtidig som forretningskritisk: Virksomhederne oplyser, at de systemer, hvor afhængigheden er størst, er dybt integreret i den daglige drift. En eventuel afbrydelse, uanset om den skyldes et cyberangreb, en handelspolitisk beslutning eller en kommerciel konflikt, vil derfor have direkte konsekvenser for både omsætning, kundeoplevelse og regelefterlevelse.

Har I igangsat tiltag for at
reducere afhængigheden af
specifikke leverandører?

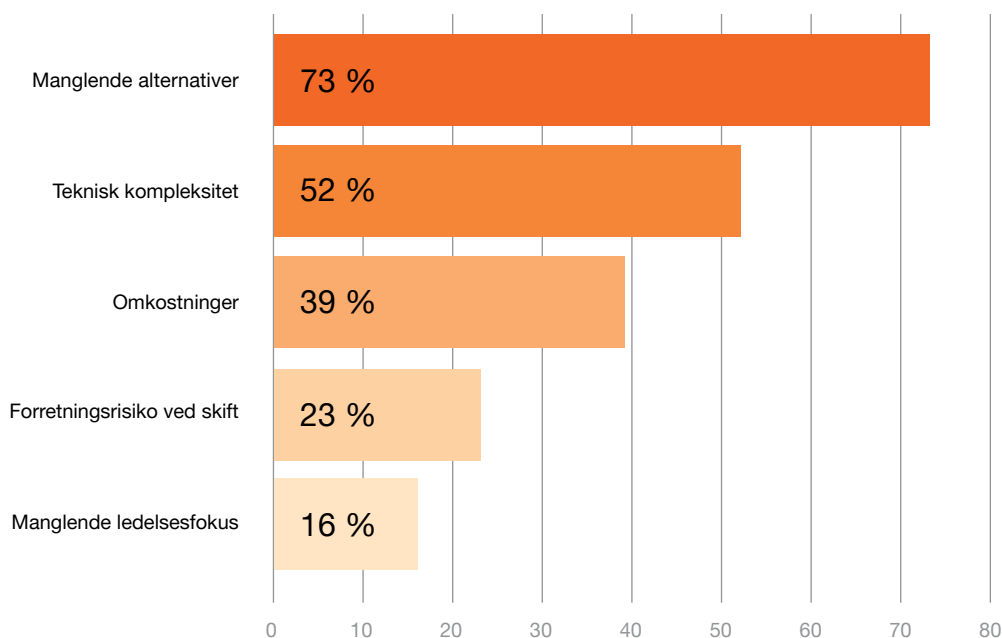


Tiltag for at reducere afhængigheden

39 % af virksomhederne har iværksat konkrete tiltag for at reducere deres afhængighed af specifikke leverandører, fx multi-cloud-strategier, dataklassifikation, exit-planer eller etablering af europæiske alternativer. Der er dog store barrierer: Hele 73 % peger på manglen på reelle alternativer som den største hindring,

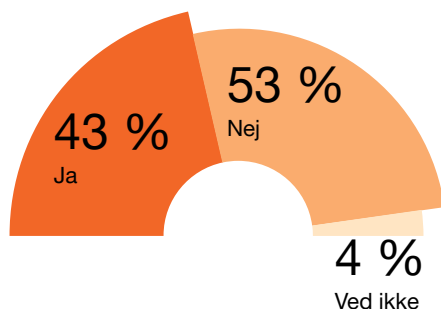
52 % fremhæver teknisk kompleksitet, 39 % peger på omkostningerne, og 23 % nævner forretningsrisikoen forbundet med at skifte leverandør. 16 % peger desuden på manglende ledelsesfokus som en barriere.

Hvad er de største barrierer for at reducere afhængigheden?
(vælg op til 3)



Reguleringer i praksis: NIS2, DORA og AI Act

Er din virksomhed omfattet af NIS2-direktivet?



2026 er året, hvor de store europæiske cyberreguleringer for alvor bliver hverdag. NIS2 er trådt i kraft, DORA gælder for finanssektoren, og AI Act begynder at få direkte betydning for de virksomheder, der udvikler eller anvender AI-systemer i risikofyldte områder. Undersøgelsen viser, at reguleringerne stadig sætter dagsordenen, men også at implementeringen er længere fremme nogle steder end andre.

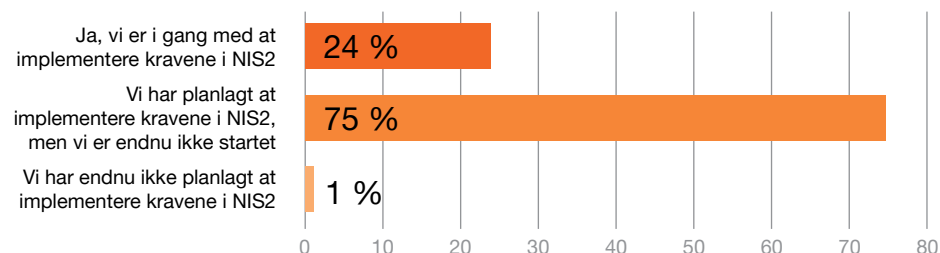
NIS2: Fra kendskab til implementering

43 % af respondenterne angiver, at deres organisation er omfattet af NIS2-direktivet. Blandt disse er 24 % helt færdige med implementeringen af kravene, mens hele 75 % stadig er i gang. Kun 1 % har endnu ikke påbegyndt arbejdet. Det tyder på, at NIS2-processerne er godt i gang, men at implementeringen fortsat udgør en udfordring for mange organisationer.

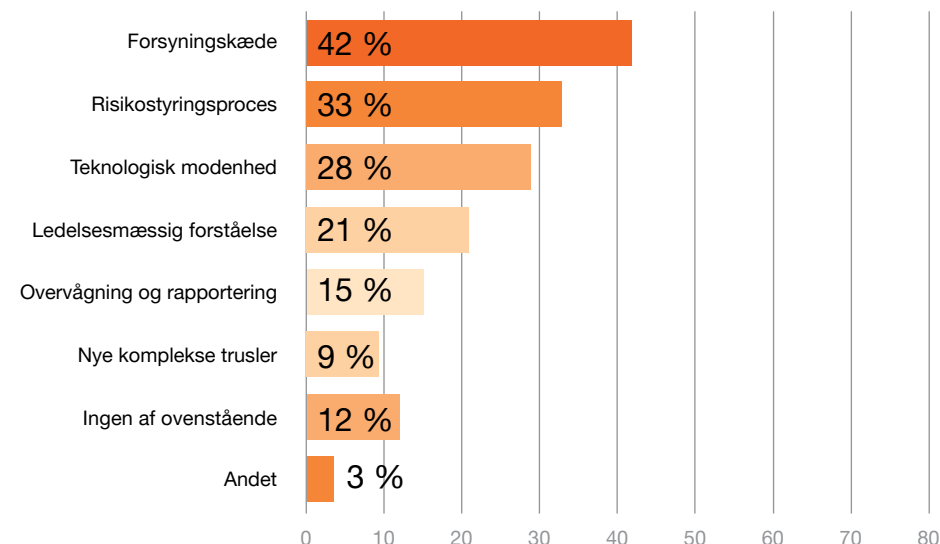
Blandt de virksomheder, der er omfattet af NIS2, angiver 42 % udfordringer med at sikre forsyningskædens sikkerhed som den største barriere for at leve op til kravene. 33 % peger på implementering af en effektiv risikostyringsproces, 28 % på manglende teknologisk modenhed eller forældet infrastruktur og 21 % på manglende ledelses-

mæssig forståelse. Tallene understreger, at NIS2 ikke blot er et teknisk projekt, men at det er lige så meget et governance-, kultur- og leverandørprojekt.

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



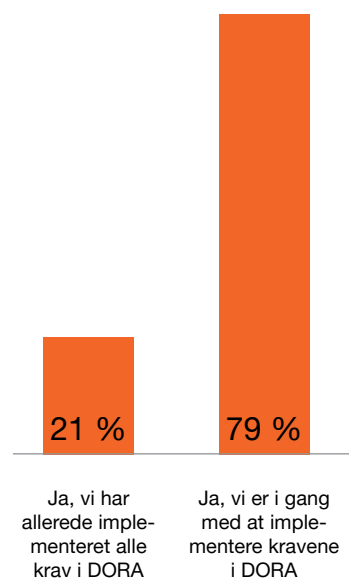
Hvilke af følgende aspekter ser du som barrierer for, at din virksomhed kan leve op til kravene i NIS2-direktivet?



DORA: Højt kendskab, fortsat implementeringsarbejde

Blandt de finansielle virksomheder, der har besvaret spørgsmålene om DORA, er kendskabet meget højt: 89 % er fuldt bekendt med forordningens krav. 70 % er omfattet af DORA, og blandt disse er 79 % i gang med at implementere kravene, mens 21 % allerede har implementeret alle krav.

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



70 %

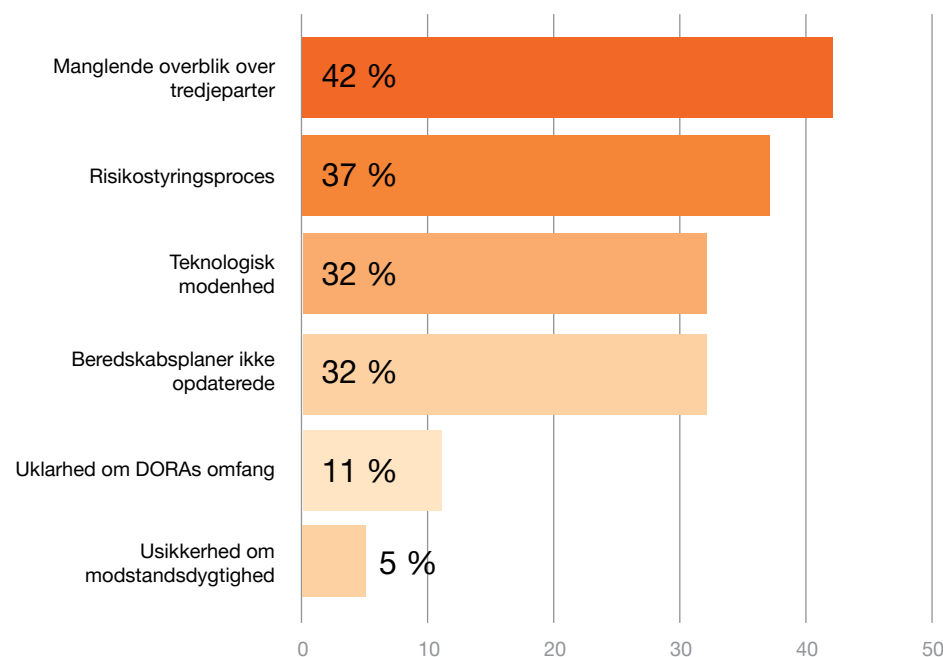
af de finansielle virksomheder, der har besvaret spørgsmålene om DORA, er omfattet af forordningen.

Der er dermed reelt ingen virksomheder blandt respondenterne, som er omfattet af DORA uden at have en plan i gang.

De største barrierer for at leve op til DORA er ifølge respondenterne manglende overblik over tredjeparter og outsourcing-leverandører (42 %), udfordringer med at implementere en effektiv risikostyrings-

proces (37 %), manglende teknologisk modenhed (32 %) og manglende opdatering af beredskabsplaner (32 %). Særligt tredjepartsstyringen er en central udfordring – hvilket flugter med den generelle observation i NIS2-arbejdet: Forsyningskæden er blevet den største compliance-udfordring i 2026.

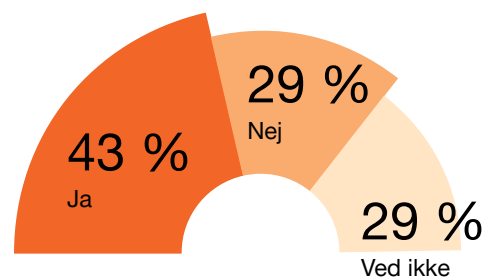
Hvilke af følgende aspekter ser du som barrierer for, at din virksomhed kan leve op til kravene i DORA-forordningen?



29 %

af respondenterne ved ikke om de er omfattet af AI Act.

Er din virksomhed omfattet af EU AI Act?



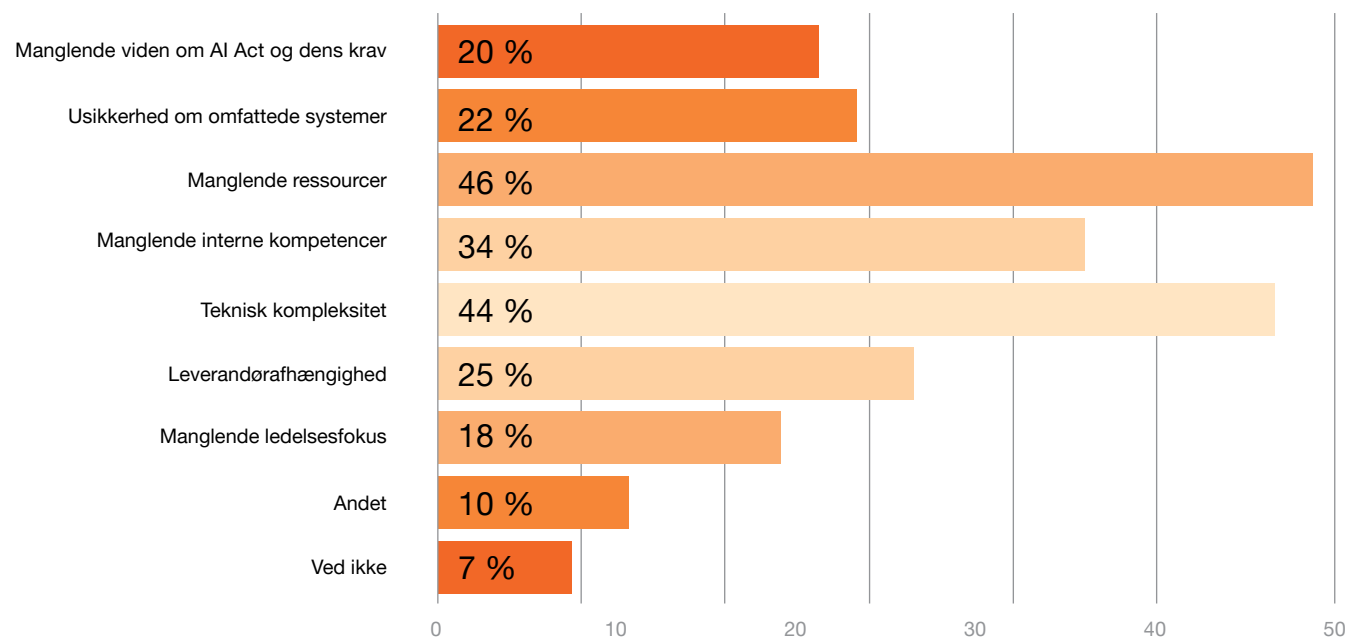
AI Act: nyt regulatorisk lag på vej

AI Act er 2026-årets nye regulatoriske dagsorden, og undersøgelsen viser et blandet billede. Blandt respondenterne svarer 43 %, at de er omfattet af AI Act, mens 29 % ikke er omfattet og 29 % ved ikke, om de er omfattet. Kendskabet er fortsat begrænset. Kun en mindre del oplyser at være fuldt bekendt med kravene, mens langt de fleste "har hørt om reguleringen" og kender nogle af kravene, men ikke dem alle.

De største barrierer for at leve op til AI Act er manglende viden om reguleringen og dens krav, usikkerhed om, hvilke AI-systemer der er omfattet, mangel på ressourcer (tid, budget, kompetencer) samt teknisk kompleksitet i at dokumentere og overvåge AI-modeller. Særligt mangel på ressourcer (46 %) og teknisk kompleksitet i at dokumentere og overvåge AI-modeller (44 %) skiller sig ud som de mest udbredte barrierer. Dette peger på, at de praktiske

og operationelle udfordringer ved compliance vejer tungere end den grundlæggende forståelse af reguleringen. Virksomhederne kender med andre ord i høj grad til AI Act, men mangler de tekniske og organisatoriske kapaciteter til reelt at omsætte kravene til praksis, hvilket kan tyde på et betydeligt behov for målrettet kompetenceopbygning og investering i compliance-værktøjer.

Hvilke af følgende aspekter ser du som barrierer for, at din virksomhed kan leve op til kravene i EU AI Act-forordningen?



AI som både værktøj og trussel

AI er blevet et paradoks i 2026-udgaven af Cybercrime Survey. På den ene side er 52 % af respondenterne enige om, at nye teknologier, herunder AI, er blandt de største trusler mod deres cyber- og informationssikkerhed. Det er en meget markant stigning fra 26 % i 2025. På den anden side står AI øverst på investeringslisten hos hele 51 % af virksomhederne.

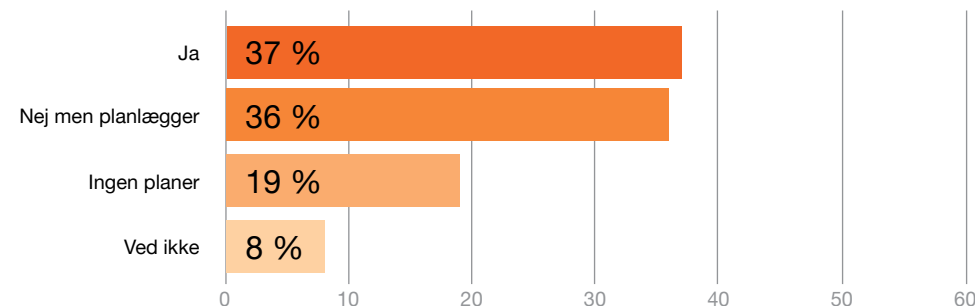
Anvendelse af AI i cybersikkerhedsarbejdet

37 % af virksomhederne anvender allerede AI aktivt i deres arbejde med cybersikkerhed. Yderligere 36 % planlægger at gøre det, mens 19 % endnu ikke har planer i den retning. Tilsammen betyder det, at 73 % af respondenterne enten anvender eller planlægger at anvende AI i deres cyberforsvar, en tydelig indikation af, at AI nu er blevet en integreret del af sikkerhedsdisciplinen.

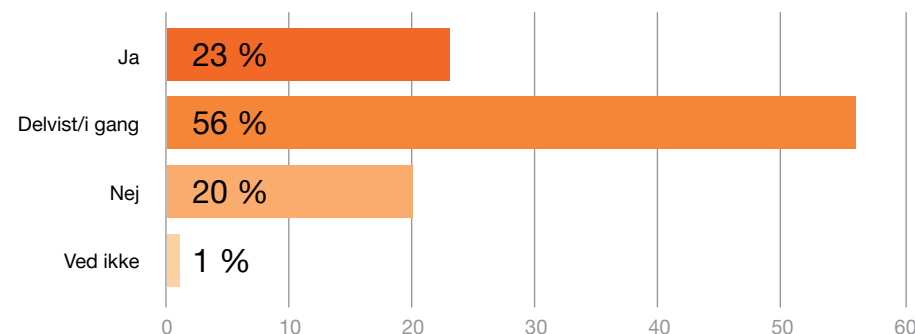
Governance omkring AI: fortsat under opbygning

Undersøgelsen viser, at 39 % af virksomhederne arbejder med risikovurderinger af deres AI-løsninger, mens 38 % gør det delvist, og 22 % gør det slet ikke. En formel AI-governance-struktur er ligeledes under opbygning: Mange virksomheder er

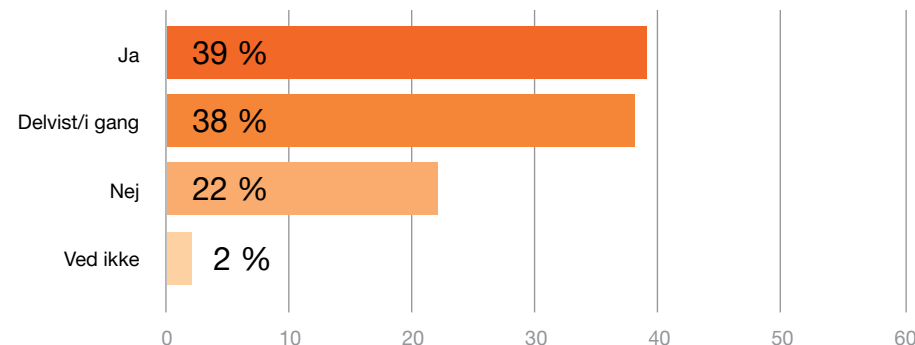
Anvender din organisation AI i arbejdet med cybersikkerhed?



Har jeres organisation etableret en formel AI-governance-struktur?



Arbejder I med risikovurdering af AI-løsninger?



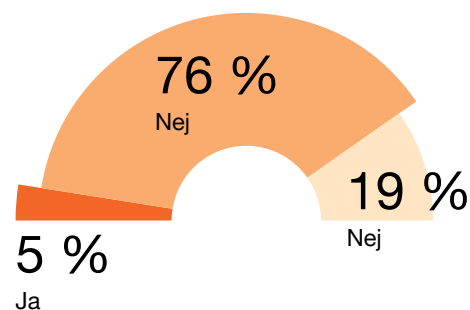
28 %

af respondenterne har implementeret specifikke sikkerhedsforanstaltninger for AI-systemer.

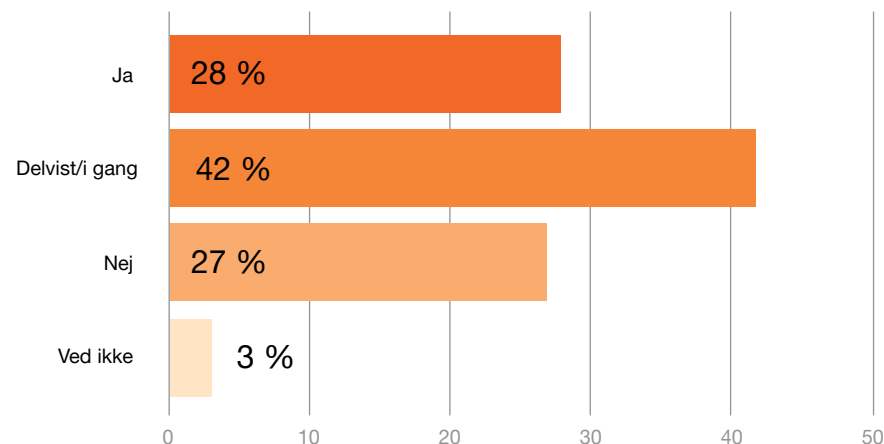
kun delvist på plads med både politikker, roller og løbende overvågning af deres AI-systemer. Det er en påmindelse om, at AI-adoptionen i praksis ofte går hurtigere end den tilhørende governance, og at netop dét åbner nye risikoflader.

5 % af virksomhederne rapporterer, at de har oplevet en sikkerhedshændelse, hvor AI enten er blevet misbrugt af angribere eller utilsigtet har bidraget til hændelsen. Selvom procentandelen fortsat er lav, er tendensen tydelig: AI-drevne angreb, alt fra hyperrealistiske deepfakes til automatiseret sårbarhedsudnyttelse, vokser i hyppighed og kompleksitet.

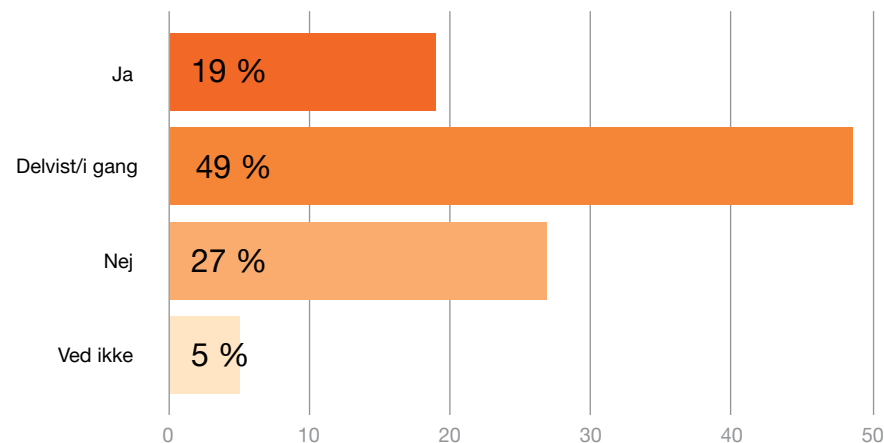
Har organisationen oplevet sikkerhedshændelser, hvor AI blev misbrugt eller utilsigtet bidrog?



Har I implementeret specifikke sikkerhedsforanstaltninger for AI-systemer?



Moniterer I løbende jeres AI-systemer?





Deepfakes og AI-drevne phishingangreb

AI-drevne angreb er ikke længere fremtidsscenarier – de er en del af hverdagen. Generative AI-modeller bruges til at skabe overbevisende phishing-e-mails på flydende dansk, syntetiske stemmer, der efterligner ledelsen, og deepfake-videoer, der kan misbruges til bedrageri eller omdømmeskade. Beskyttelsen mod disse angreb kræver en kombination af teknisk detektion (fx AI-baserede filtre), procesbaserede kontroller og løbende træning af medarbejderne, så mistanke og verifikation bliver en refleks.



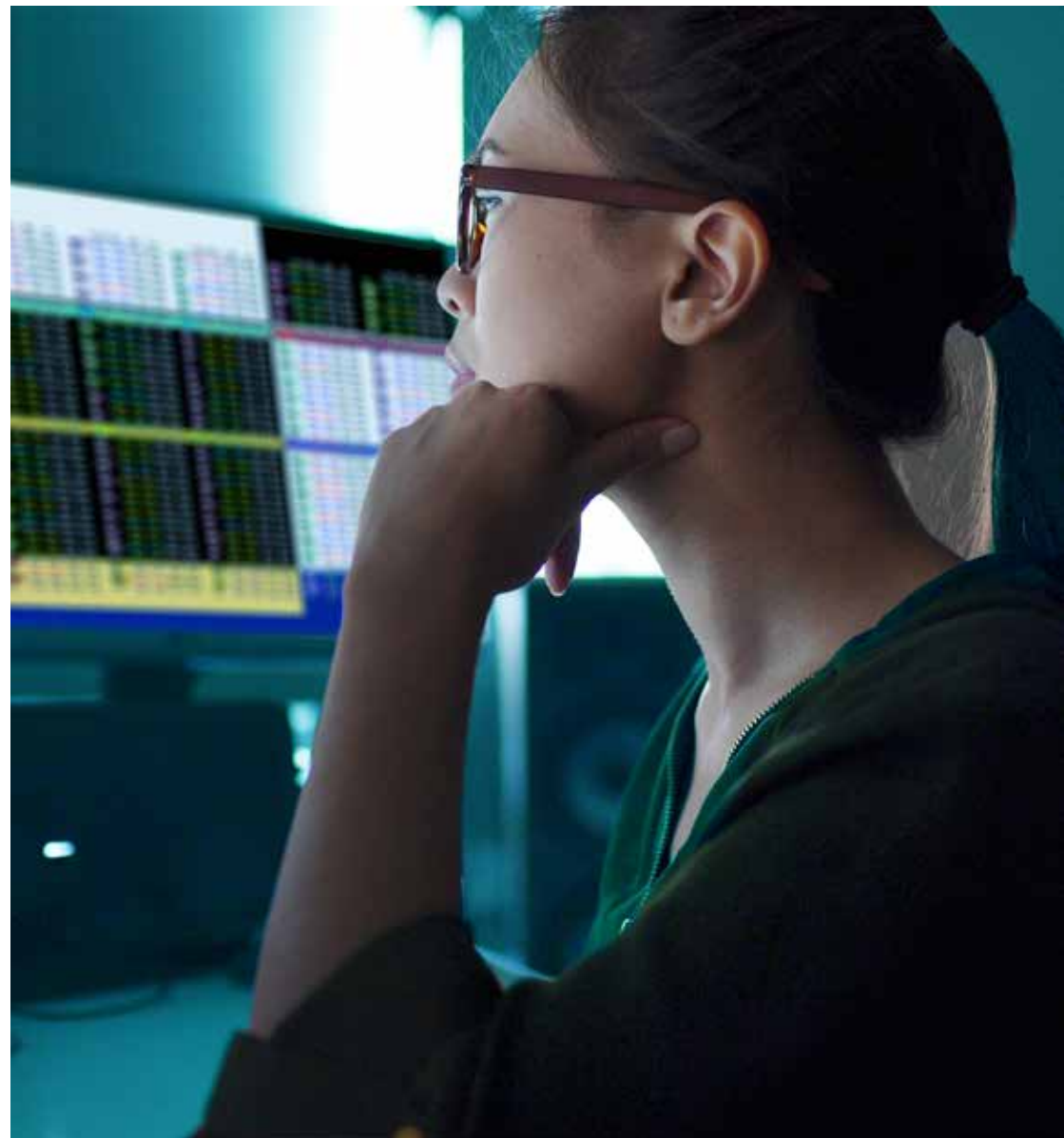
Læs mere [her](#)

PwC erfarer

PwC anbefaler, at virksomheder arbejder med AI ud fra to spor samtidigt: AI til forsvar og sikring af AI som ny risiko. På forsvarssiden ser vi stor effekt af AI-baseret automatisering af trusseldetektion, sårbarhedsvurderinger og Incident Response, særligt i SOC-miljøer, hvor AI kan analysere store mængder sikkerhedsdata og identificere afvigelser, som ellers ville overvælde menneskelige analytikere. AI bør ikke bruges som et isoleret værktøj, men som en samlet kapacitet, der understøtter og koordinerer indsatser på tværs af hele cyberforsvaret. På risikosiden anbefaler vi, at man arbejder struktureret med sikring af AI ved at vurdere eksisterende kontroller og identificere, hvor der er behov for nye tekniske tiltag og tydelig menneskelig styring, både i udviklingen og anvendelsen af AI-løsninger.



Læs mere [her](#)



OT-sikkerhed som den næste frontlinje

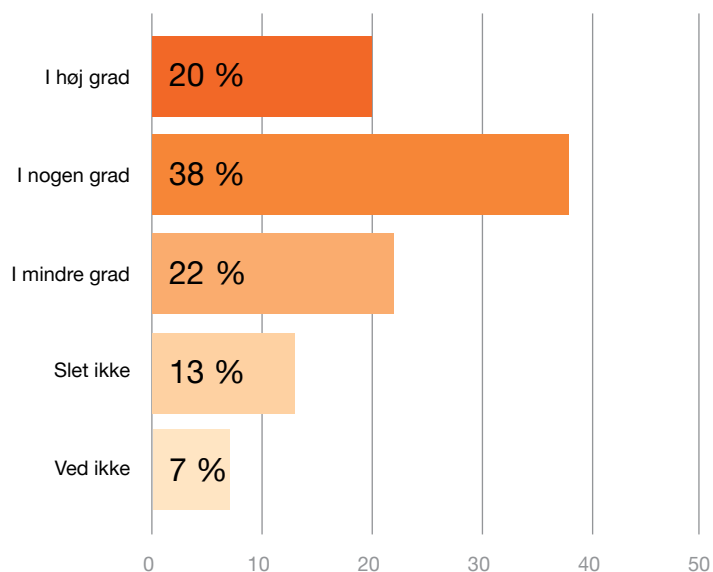
Operational Technology (OT) er de industrielle kontrolsystemer og fysiske produktionsmiljøer, der driver alt fra fjernvarme og vandforsyning til fødevareproduktion og transport, og de er blevet en stadig mere central del af cyberdagsordenen. NIS2 har for alvor sat OT-sikkerhed på ledelsens bord, og det stigende trusselsniveau mod kritisk infrastruktur gør emnet uhyggeligt aktuelt.

Blandt de virksomheder, der arbejder med OT, angiver et flertal, at de har fokus på OT-sikkerhed, men også at der er betydelige udfordringer med at skabe det nødvendige overblik og modenhedsniveau. 20 % oplever, at ældre OT-systemer (legacy-systemer) i høj grad udgør en udfordring for OT-sikkerheden, og yderligere 38 % oplever det i nogen grad. Kun 13 % siger, at legacy-systemer slet ikke er en udfordring.

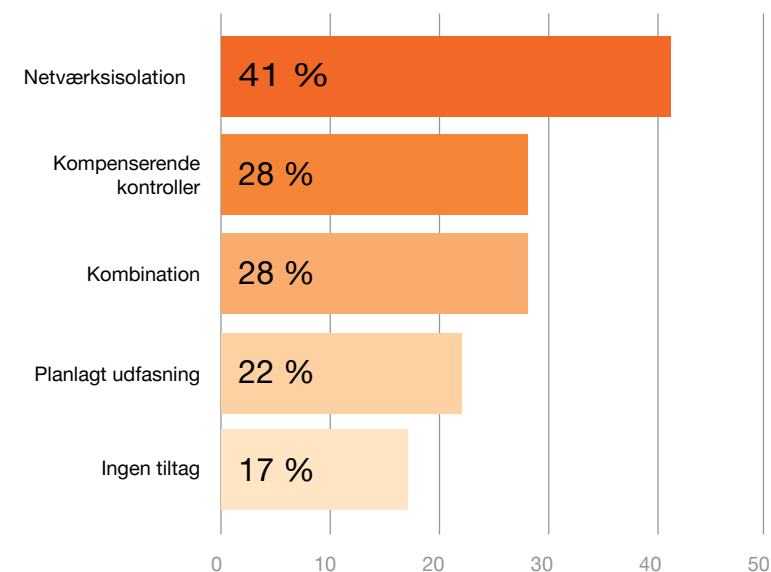
Håndtering af risici i legacy OT

Virksomhederne håndterer risici fra legacy OT-systemer med en bred vifte af tiltag: 41 % anvender netværksisolation, hvor legacy-systemer segmenteres i separate netværkszoner med dedikerede firewall-regler. 28 % arbejder med kompenserende sikkerhedskontroller, ligeledes 28 % med en kombination af flere metoder, mens 22 % har en konkret plan for udfasning eller migration. 17 % har ikke iværksat særlige tiltag.

I hvilken grad udgør ældre OT-systemer en udfordring?



Hvordan håndterer I risici ved ældre OT-systemer, som ikke kan opdateres?



64 %

af virksomhederne har et fuldt opdateret og dokumenteret overblik over OT-aktiver.

Ansvarsfordeling og modenhed

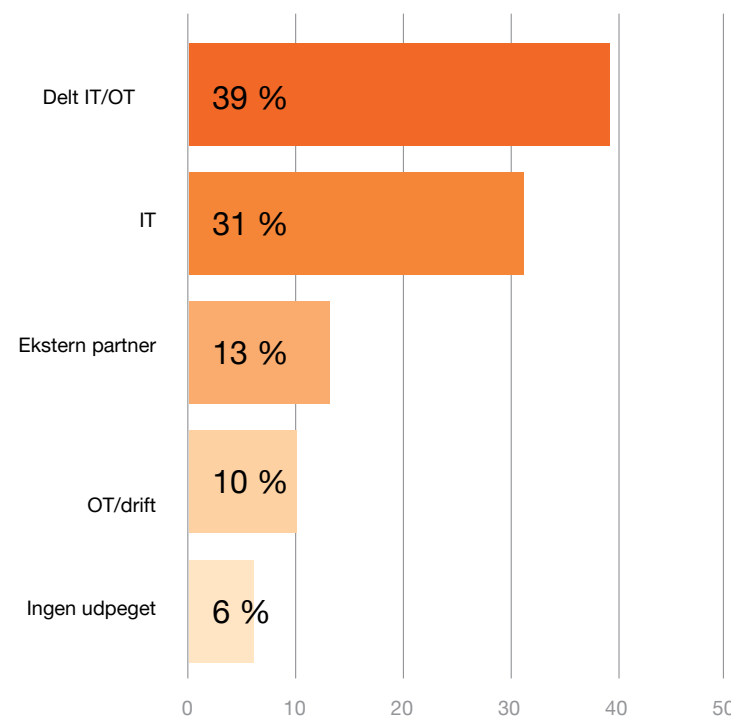
Ansvaret for OT-sikkerhed er delt: I 39 % af virksomhederne er det et delt ansvar mellem it-afdelingen og OT/drift, mens 31 % placerer ansvaret entydigt i it-afdelingen. 10 % lægger ansvaret i OT/drifts-afdelingen, og 13 % benytter en ekstern partner. 6 % har ikke udpeget en ansvar-

lig. Fordelingen afspejler, at OT-sikkerhed er en tværfaglig disciplin, hvor et tæt samarbejde mellem it og drift er afgørende for at sikre en effektiv beskyttelse af OT-miljøerne.

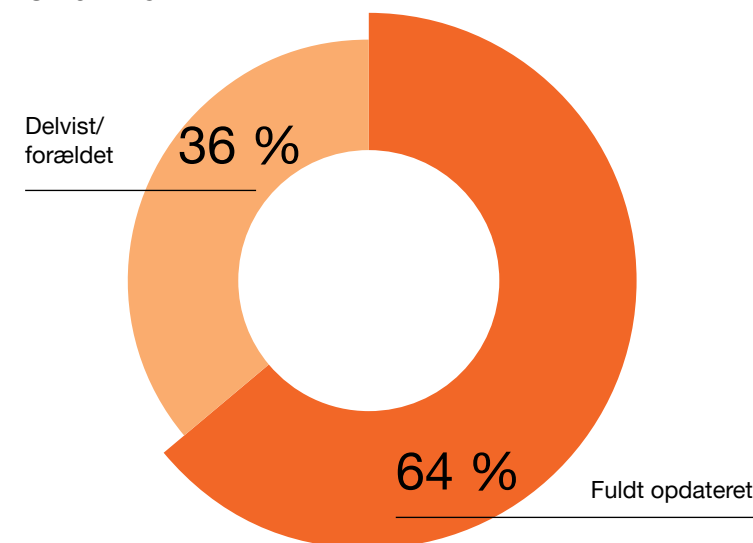
På trods af det store fokus har kun 64 % af virksomhederne et fuldt opdateret og

dokumenteret overblik over aktiverne i deres OT-miljø. 36 % har ikke et sådant overblik, hvilket er en kritisk mangel, når man skal kunne risikovurdere, overvåge og beskytte ens OT-miljø effektivt. Et opdateret asset inventory er en af de mest fundamentale forudsætninger for både OT-sikkerhed og NIS2-compliance.

Hvem har det primære ansvar for OT-sikkerhed?



Har du et dokumenteret overblik over alle OT-aktiver?



82 %

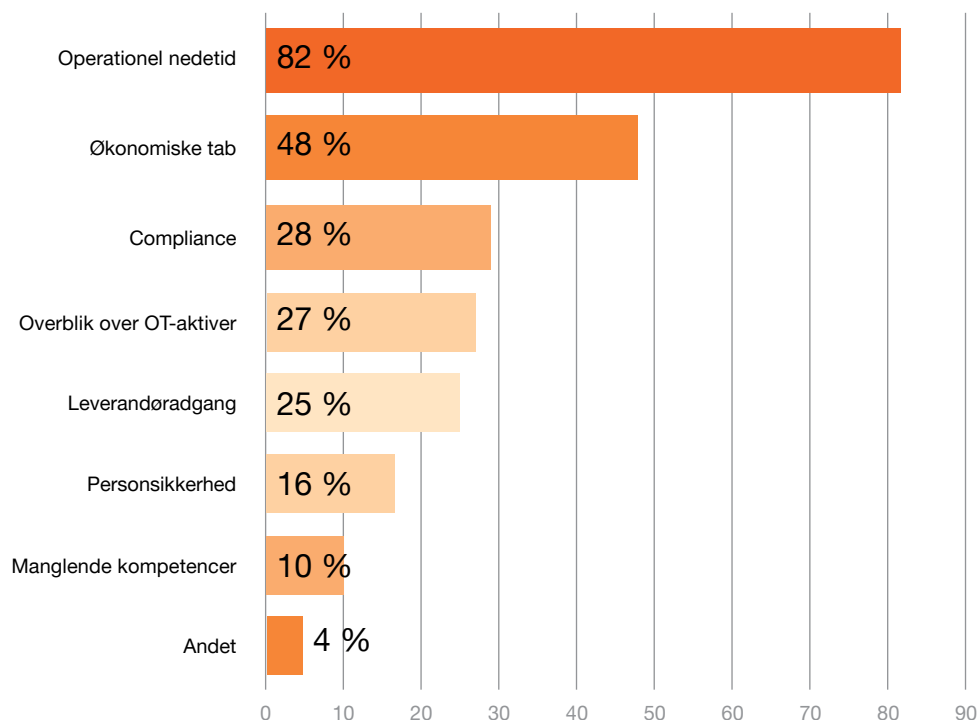
af respondenterne
nævner operationel
nedetid som den mest
kritiske.

De største bekymringer i OT-miljøet

Når virksomhederne bliver bedt om at pege på de største bekymringer i deres OT-miljø, nævner hele 82 % operationel nedetid som den mest kritiske. Det understreger, at OT-sikkerhed først og fremmest handler om at holde produktionen kørende.

Derefter følger økonomiske tab (48 %), compliance- og regulatoriske krav (28 %), manglende overblik over OT-aktiver (27 %) og trusler fra leverandørangang (25 %). Manglende interne kompetencer (10 %) og personsikkerhed (16 %) fylder også i billedet.

Hvad er jeres største bekymring i forhold til OT-sikkerhed? (Vælg op til 3)



Hvorfor er OT-sikkerhed anderledes end it-sikkerhed?

OT-miljøer er designet til at prioritere tilgængelighed og sikkerhed for mennesker og udstyr, ikke fortrolighed, som er hovedfokus i traditionel it-sikkerhed. Det betyder, at klassiske it-sikkerhedspraksisser (fx hyppige opdateringer og genstart af systemer) kan være direkte skadelige i OT-sammenhæng, hvor selv sekundlange afbrydelser kan koste dyrt eller udgøre en sikkerhedsrisiko. OT-sikkerhed kræver derfor en dedikeret tilgang med segmentering, kompenserende kontroller, tæt monitorering og et modent samarbejde mellem it, drift og eksterne leverandører.



Læs mere [her](#)



PwC erfarer

PwC oplever, at de virksomheder, der lykkes bedst med OT-sikkerhed, starter med det mest grundlæggende: at skabe overblik og forstå risikoen ved at kortlægge infrastruktur, processer og sårbarheder og arbejde procesorienteret med risikovurdering af de systemer, der er mest kritiske for driften. Herfra anbefaler vi at lægge en realistisk plan, opdelt i faser over måneder og år, med klare minimumskrav til sikkerhedsniveauet og løbende evaluering. Det kræver et tværfagligt projekt-team med projektleder, OT-ansvarlig, cybersikkerhedsspecialist, forretningsrepræsentant og HR-repræsentant, der kan sikre fremdrift og forankring. Under implementeringen er det afgørende at prioritere synlighed og transparens samt gradvist etablere en driftsorganisation, der tager ejerskab efter projektets afslutning. Endelig bør man sikre løbende overvågning, evaluering og automatisering af processer som patching og hændelseshåndtering, så sikkerheden forbliver håndterbar og løbende styrkes i takt med, at trusselsbilledet udvikler sig



PwC's trin-for-trin guide: Sådan skaber du robust OT-sikkerhed – fra sårbarhed til sikker drift.
Download [her](#)



Om undersøgelsen

326 danske topledere, sikkerhedschefer og fagspecialister har deltaget i PwC's Cybercrime Survey 2026. Denne rapport sætter fokus på cybersikkerhed i dansk erhvervsliv og hos offentlige institutioner.

Undersøgelsen er igen i år gennemført med opbakning fra Finans Danmark, It-branchen, Dansk Erhverv, Styrelsen for Samfundssikkerhed, KITA, Rådet for Digital Sikkerhed, ISACA, Dansk IT, Bestyrelsesforeningen, Punktum DK og Computerworld.

Analysen bygger på onlinebesvarelser. Respondenterne er blevet stillet en række spørgsmål inden for cyber- og informationssikkerhed. Målingens spørgsmål og svarmuligheder er udarbejdet af PwC, og online

326

danske topledere, sikkerhedschefer og fagspecialister har deltaget i PwC's Cybercrime Survey 2026.

Få flere tips til cyberberedskabet

Er du CFO eller en del af ledelsen? CFO'ens Cyberguide tager dig igennem de trin, der ligger i at opbygge et strategisk cyberberedskab i din virksomhed. Læs mere i CFO'ens Cyberguide.

Læs mere i CFO'ens Cyberguide [her](#).

Se alle kapitler i CFO'ens CyberGuide



Sådan håndterer I bedst en cyberhændelse



Få styr på beredskabet, inden uheldet sker



Sådan forbereder du organisationen til NIS2



Cybersikkerhed og GDPR - der er en sammenhæng



Cyberforsikring - overførsel af risiko til tredjepart



Vigtig viden om CFO'ens samspil med bestyrelsen



Få styr på virksomhedens vigtigste aktiver



Teknologivag - inhouse og eksternt



Håndtering af brugere og adgang



Adfærd og awareness



Tjekliste

I PwC vil vi gerne hjælpe virksomheder med at sikre sig bedst muligt mod cybertrusler – både før, under og efter et angreb. Da løsningerne kan være mange og ofte komplekse, har PwC udarbejdet denne liste, der kan hjælpe virksomheder med at tage stilling til nogle af de vigtigste indsatsområder inden for cyber- og informationssikkerhed.



Governance, risk og compliance

	Har I etableret et formelt sikkerhedsudvalg med repræsentanter fra virksomhedens topledelse?
	Er øvrige roller for cyber- og informationssikkerhed defineret, allokeret og kommunikeret?
	Arbejder I struktureret med risikovurdering ud fra sikkerhedstrusler, sårbarheder og konsekvens for forretningen?
	Rapporteres virksomhedens sikkerhedsstatus jævnligt/løbende til virksomhedens direktion/bestyrelse?
	Omfatter arbejdet med sikkerhed både informationssikkerhed og cybersikkerhed? Læs mere om ISO 27001 og NIS2 her .
	Har I implementeret relevante foranstaltninger til overholdelse af GDPR (persondataforordningen)?
	Arbejder I proaktivt med henblik på fortsat overholdelse af kravene i GDPR?

Processer

	Har I foretaget en vurdering af jeres robusthed mod cybertruslerne (cyber assessment)?
	Har I dokumenteret og kommunikeret processer for alle områder af sikkerhed?

Adfærd

	Er der etableret et program for løbende uddannelse og oplysning af medarbejderne om sikkerhed? Læs mere her .
--	---

Validering

	Gennemfører I løbende test i forhold til identifikation af sårbarheder i jeres infrastruktur og systemer?
	Har I fastlagt og afprøvet en Incident Response-proces? Læs mere her .
	Har I testet jeres beredskabsplaner for cyberhændelser? Læs mere her .

Arkitektur

	Har I udarbejdet en plan for implementering af hensigtsmæssig sikkerhedsteknologi?
	Har I fastlagt en proces for privacy by design, herunder adgang til persondata? Læs mere her og her .

Kontakt

Vi vil meget gerne i dialog med dig om resultaterne fra årets Cybercrime Survey. Kontakt en af PwC's eksperter for en uforpligtende snak om dine konkrete udfordringer og behov.

Læs mere om vores ydelser inden for cyber- og informationssikkerhed på pwc.dk/cyber, eller scan QR-koden.



Mads Nørgaard Madsen

Partner,
Leder af Cyber Excellence
T: 2811 1592
E: mads.norgaard.madsen@pwc.com



Marc Jerner

Partner,
Security Technology
T: 4099 4698
E: marc.jerner@pwc.com



Jørgen Sørensen

Partner,
Digital Tvilling & Responsible AI
T: 2494 5254
E: jorgen.jgs.sorensen@pwc.com



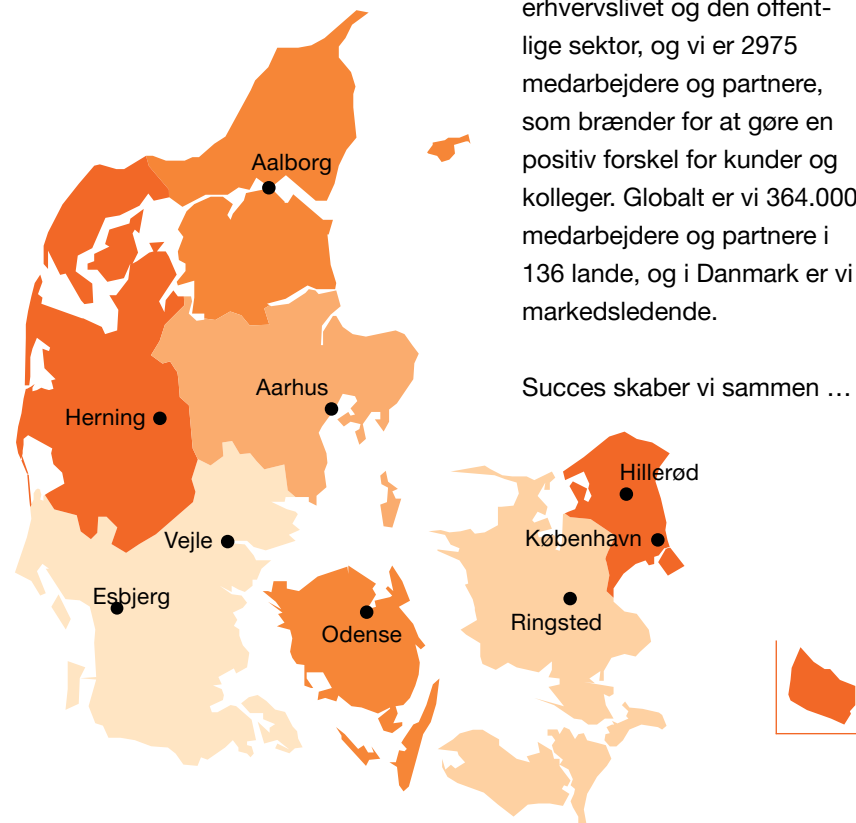
Christian Kjær

Partner,
Cyberrisikostyring
T: 5132 1270
E: christian.kjaer@pwc.com



Malene Fagerberg

Partner,
Cyberrisk & Regulation
T: 2567 9447
E: malene.fagerberg@pwc.com



Om PwC

I PwC arbejder vi for at styrke tilliden i samfundet og være med til at løse væsentlige problemstillinger. Det gør vi med udgangspunkt i vores viden inden for revision, skat og rådgivning. Vores kunder kommer fra alle dele af erhvervslivet og den offentlige sektor, og vi er 2975 medarbejdere og partnere, som brænder for at gøre en positiv forskel for kunder og kolleger. Globalt er vi 364.000 medarbejdere og partnere i 136 lande, og i Danmark er vi markedsledende.

Succes skaber vi sammen ...

Cyber Incident Response-team

PwC hjælper kunder med at forebygge og håndtere cybersikkerhedshændelser

Vi har etableret en central cyberhotline for kunder, så du har mulighed for at få akut hjælp. PwC's team af eksperter hjælper med at skabe overblik over indsatsområder i forhold til den konkrete trussel, og vores cyberforensics-specialister identificerer angrebets art og de udnyttede sårbarheder. Derefter implementerer vi forbedringer af sikkerheden og udarbejder en rapport til brug for bl.a. ledelsen, forsikringen, Datatilsynet og politiet.



PwC's cyberhotline

70 222 444

Læs mere: [pwc.dk/response](https://www.pwc.dk/response)





[pwc.dk/cyber](https://www.pwc.dk/cyber)

Denne publikation er udarbejdet alene som en generel orientering om forhold, som måtte være af interesse, og udgør ikke professionel rådgivning. Du bør ikke disponere på baggrund af de oplysninger, der er indeholdt i publikationen, uden at indhente specifik professionel rådgivning. Vi afgiver ingen erklæringer eller garantier (udtrykkeligt eller underforstået), hvad angår nøjagtigheden og fuldstændigheden af de oplysninger, der findes i denne publikation, og i det omfang loven tillader, accepterer eller påtager PwC, dets partnere, medarbejdere og repræsentanter sig ikke nogen forpligtelse eller noget ansvar for eventuelle konsekvenser, som følger af, at du eller andre handler eller undlader at handle i tillid til de oplysninger, der findes i denne publikation, eller for eventuelle beslutninger truffet på baggrund af publikationen.

© 2026 PricewaterhouseCoopers Statsautoriseret Revisionspartnerselskab. Alle rettigheder forbeholdes. I dette dokument refererer "PwC" til PricewaterhouseCoopers Statsautoriseret Revisionspartnerselskab, som er et medlemsfirma af PricewaterhouseCoopers International Limited, hvor hver enkelt virksomhed er en særskilt juridisk enhed.