

# Cybercrime Survey 2022

73 %

af CXO'er og it-fagfolk angiver, at deres øgede bekymring for cybertrusler i nogen eller i høj grad skyldes konflikten mellem Rusland og Vesten.

47 %

regner hacktivister blandt de største trusler. Det er 11 %-point flere end sidste år og den største andel nogensinde.

51 %

angiver, at deres virksomhed har været utsat for mindst én sikkerhedshændelse inden for det seneste regnskabsår. Det er fjerde år i træk, at mere end hver anden virksomhed har været ramt.



# Indhold

Leder: Det er på tide at tage næste skridt inden for cybersikkerhed	4
Flere end halvdelen af danske virksomheder har været utsat for en cyberhændelse	5
Phishingangreb toppe fortsat listen over hændelser	8
Konflikten mellem Rusland og Vesten øger bekymringen for cybertrusler	12
Truslen fra hacktivister er steget væsentligt	16
Virksomheder indfører nye sikkerhedstiltag som følge af konflikten med Rusland	18
Plads til forbedring i virksomhedernes GDPR-compliance	20
Plads til forbedring i virksomhedernes tillid til håndtering af GDPR og cybersikkerhed	23
Behov for øget ledelsesfokus på cybersikkerhed	26
Bestyrelsens styrerammer og håndtering bør forbedres	28
Syv ud af ti større virksomheder forventer at øge investeringerne i cybersikkerhed	32
Et norsk perspektiv	38
Om undersøgelsen	39
PwC's sikkerhedskoncept PAVA	40
Tjekliste	41
Kontakt	42
Cyber Incident Response-team	43

518 virksomhedsledere, it-chefer og specialister fra danske virksomheder har deltaget i PwC's Cybercrime Survey 2022, hvor de har delt deres syn på forskellige udviklinger og udfordringer i relation til cyberkriminalitet i Danmark. De har således taget stilling til trusselsbilledet og har rapporteret, hvordan og i hvilket omfang de arbejder med udfordringerne.



“

CXO'er og it-fagfolk er i dag mere bekymrede for cyberangreb end for blot et år siden. Et stort flertal af disse peger på konflikten med Rusland som årsag til den stigende bekymring.

Mads Nørgaard Madsen, Partner, Technology & Security

# Det er på tide at tage næste skridt inden for cybersikkerhed



## Leder

Vi ser et fortsat stort antal cyberhændelser i dansk erhvervsliv og i den offentlige sektor. 51 % af de danske CXO'er og it-fagfolk fortæller i dette års Cybercrime Survey, at deres virksomhed eller organisation har været utsat for mindst én sikkerhedshændelse inden for det seneste regnskabsår. Det er fjerde år i træk, at mere end hver anden virksomhed har været ramt.

Krigen i Ukraine præger naturligvis trusselsbilledet, og selvom Danmark ikke har været utsat for større angreb relateret til konflikten, er 63 % af CXO'er og it-fagfolk mere bekymrede for cyberangreb end for blot et år siden. Et stort flertal af disse peger på konflikten mellem Rusland og Vesten som årsag til den stigende bekymring. Ifølge Center for Cybersikkerheds trusselsvurdering fra 2022 er det da også muligt, at fx pro-russiske hackere vil gå efter mål i Danmark. Dette er en ændring fra de seneste år, hvor kun få forventede, at cyberaktivister ville have til hensigt at gå efter danske mål.

Der er dog også andre grunde til bekymring i dansk erhvervsliv, når det kommer til cyber- og informationssikkerhed. Virksomhederne er under pres i lyset af den hastige digitale udvikling og den konstante fremvækst af ny software. Cybersikkerhed er derfor ikke længere bare et spørgsmål om at undgå at blive ramt af cyberangreb. Det er et spørgsmål om, hvordan man mitigerer risici og minimerer implikationerne af de hændelser, virksomheden med stor sandsynlighed vil stå over for. Det kunne fx være de såkaldte zero day-hændelser, hvor sårbarheder i kernesoftware åbner døren for de cyberkriminelle til virksomhedens kritiske systemer. Her er det helt afgørende, at den udsatte virksomhed formår at isolere og begrænse hændelserne,

så virksomhedens forretningskritiske systemer ikke falder som dominobrikker med uoverskuelige forretningsmæssige tab til følge. Man bør som virksomhed iværksætte zero trust-modeller, hvor hele virksomhedens it-arkitektur er baseret på, at enhver medarbejder er en potentiel kilde til sikkerhedshændelser, hvorfor alle brugeres adgang til netværk, systemer og data bør være skarpt afgrænset.

Det kræver imidlertid ressourcer, kompetencer og løbende opfølgning at arbejde helhedsorienteret med cyber- og it-sikkerhed. Det er derfor positivt, at området har en stadigt højere prioritet i virksomhederne. 59 % af CXO'er og it-fagfolk forventer således, at deres virksomheds cyber- og informationssikkerhedsbudget vil vokse inden for de næste 12 måneder. Dette er en fortsættelse af de senere års tendens med øgede investeringer i cybersikkerhed, som også er et nødvendigt skridt for at imødegå de mange risici, virksomhederne står over for. Ud over nye risici skal virksomhederne leve op til ny regulering, der også kræver ressourcer. Fx har EU-medlemslandene vedtaget NIS2-direktivet, der udvider kravene til cybersikkerhed og sanktionerne ved manglende overholdelse af disse for at harmonisere og strømline sikkerhedsniveauet på tværs af medlemslandene. Det medfører

skærpede krav til flere sektorer og betyder, at virksomhederne skal forholde sig til bl.a. risikostyring, kontrol og tilsyn.

Vi ser også, at flere virksomheder ønsker at arbejde mere helhedsorienteret med cybersikkerhed. Men det er samtidig vores erfaring, at en væsentlig andel af virksomhederne ikke får implementeret vedvarende programmer for håndtering af sikkerhed. Et tilstrækkeligt videngrundlag er en forudsætning for, at fx en bestyrelse kan håndtere virksomhedens cybersikkerhed hensigtsmæssigt. På trods af det angiver blot 51 % af bestyrelsesmedlemmerne i PwC's Cybercrime Survey 2022, at de mindst én gang om året modtager en anvendelig rapport vedrørende virksomhedens cybersikkerhed.

Det kan derfor være en overvejelse værd for mange virksomheder at tage endnu flere skridt, som sikrer, at både organisationens bestyrelse og topledelse har indgående indsigt i trusselsbilledet og de kritiske aktiver, og at de prioriterer sikkerhedsområdet i et langsigtet perspektiv. Til dette arbejde har vi tilvejebragt en række anbefalinger, som knytter sig til årets resultater i Cybercrime Survey 2022.

Rigtig god læselyst.



**Mads  
Nørgaard Madsen**  
Partner  
Technology & Security

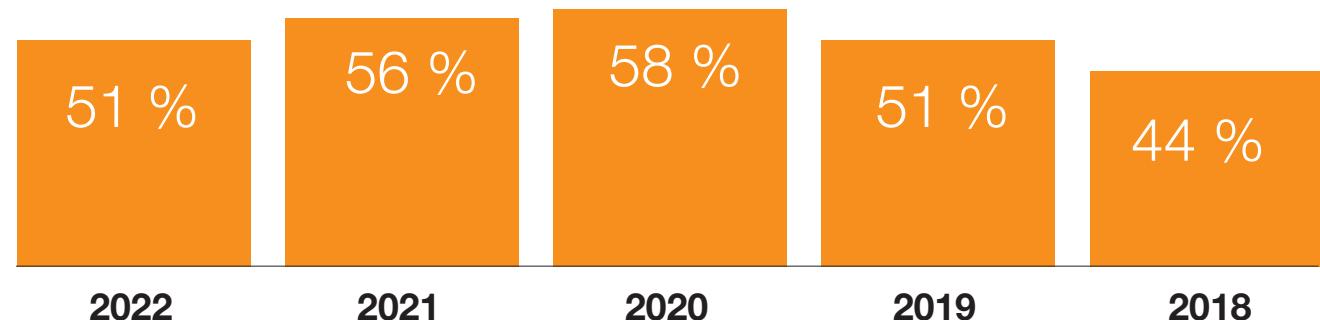


## Flere end halvdelen af danske virksomheder har været utsat for en cyberhændelse

Der er et fortsat højt niveau af cybersikkerhedshændelser i dansk erhvervsliv og i den offentlige sektor. 51 % af de danske CXO'er og it-fagfolk svarer således i undersøgelsen, at deres virksomhed eller organisation har været utsat for mindst én sikkerhedshændelse inden for det seneste regnskabsår. Trods et mindre fald er det fjerde år i træk, at mere end hver anden har været ramt.



### Andel, der har været utsat for mindst én sikkerhedshændelse.



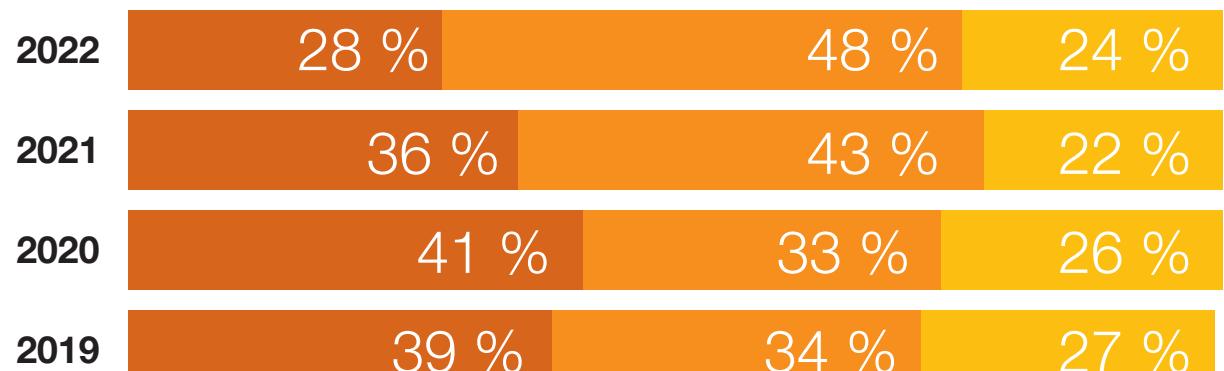


Knap tre ud af ti (28 %) vurderer, at sikkerhedshændelsen var målrettet deres organisation, hvilket er lidt færre end i de foregående år. Det er væsentligt at understrege, at der sandsynligvis er flere sikkerhedshændelser, end undersøgelsen viser. Det skyldes, at en del sikkerhedshændelser ikke nødvendigvis bliver opdaget, og andre kan være svære at fastslå som egentlige hackerangreb. Således angiver 24 % af CXO'erne og it-fagfolkene, at de ikke kan fastslå, om de har været utsat for hændelser, der var målrettet netop deres virksomhed.



---

**Spørgsmål: Har din virksomhed oplevet en eller flere sikkerhedshændelser, der var målrettet din virksomhed?**



■ Ja ■ Nej ■ Kan ikke fastslå

---

Note: Evt. sumafvigelser skyldes afrunding.

# 24 %

af CXO'erne og it-fagfolkene kan ikke fastslå, om de har været utsat for en hændelse.

---



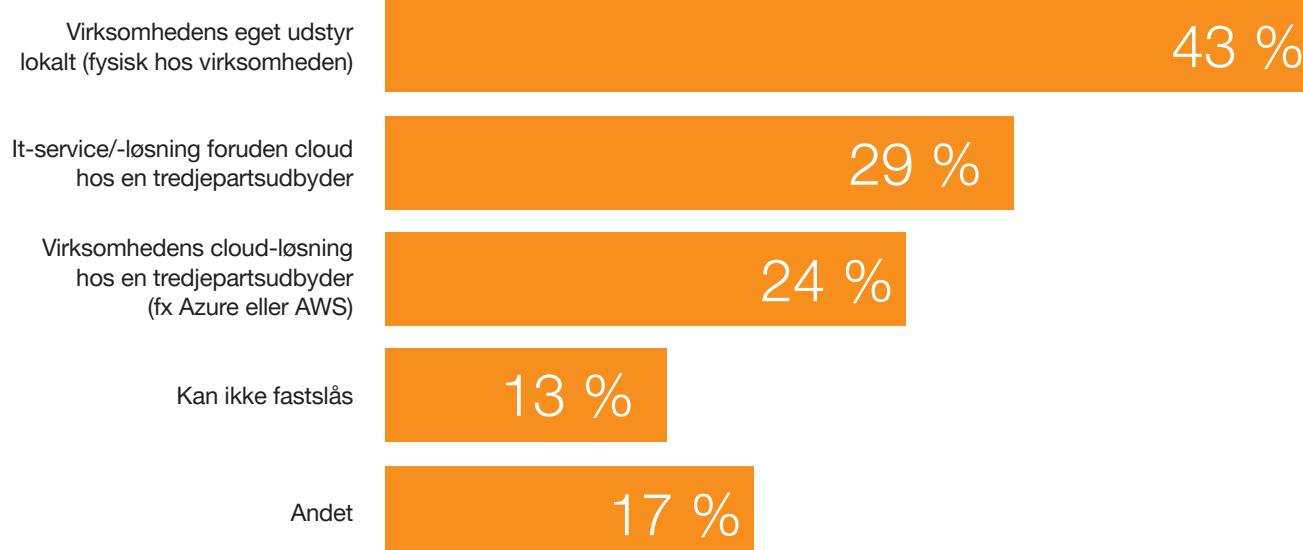
Hvis virksomhederne skal lykkes med at sikre sig effektivt mod målrettede hackerangreb, er der behov for viden om, hvilke svagheder hackerne typisk udnytter, så man som virksomhed nemmere kan sikre sig mod kendte angrebstyper.

43 % af dem, der ved, de har været ramt af en sikkerheds-

hændelse, svarer, at hændelsen var relateret til udstyr, der fysisk er placeret hos virksomheden. Til sammenligning har henholdsvis 24 og 29 % været utsat for hændelser, der var relateret til henholdsvis en cloud-løsning hos en tredjepartsudbyder og en it-service-/løsning hos en tredjepartsudbyder.



## Spørgsmål: Hvad var hændelserne relateret til?



### PwC anbefaler:

Det er vigtigt at være opmærksom på, at man som virksomhed ikke kan fraskrive sig risikoen ved at anvende tredjepartsleverandører. Hvis man har valgt en tredjepartsleverandør til it-drift, anbefaler PwC, at man vælger en anden part på sikkerhedsområdet, med henblik på at sikre funktionsadskillelse og det rette niveau af specialisering.

# Phishingangreb toppe fortsat listen over hændelser

Phishing er ifølge undersøgelsen den mest udbredte type angreb. Det hænger sammen med, at det er en form for angreb, der er nemme at udføre for cyberkriminelle sammenlignet med andre angrebstyper, da phishing ikke nødvendigvis stiller store krav til de cyberkriminelles kompetencer og ressourcer.

Undersøgelsen viser således, at langt størstedelen af dem, der har været ramt af en sikkerhedshændelse i løbet af de seneste 12 måneder, har været utsat for et phishingangreb. Det gælder i alle tre sektorer: I den private sektor og den finansielle sektor har hele 78 % af CXO'erne og it-fagfolkene oplevet et phishingangreb, mens det gælder 69 % i den offentlige sektor.

Dernæst er malware og hændelser forårsaget af leverandørfejl de hyppigst oplevede hændelser i det seneste år på tværs af alle tre sektorer. Knap en tredjedel (30 %) i den private sektor har desuden oplevet finansiel svindel rettet mod netop deres virksomhed. Det placerer finansiel svindel som

den tredje mest oplevede hændelse for den private sektor, mens den type svindel ikke optræder i de to andre sektors top 5.

DoS-angreb<sup>1</sup> målrettet en virksomhed er mest udbredt i den finansielle sektor, hvor knap en tredjedel (30 %) har oplevet denne hændelse i løbet af det seneste år.

I den offentlige sektor er trusselsbilledet generelt mere spredt. Således har over halvdelen af CXO'erne og it-fagfolkene oplevet de tre hyppigste trusler – phishing, hændelser forårsaget af leverandørfejl og utilsigtet deling af personoplysninger, mens de øvrige trusler er oplevet af 17 % eller færre.

1 Denial of Service (DoS) er en angrebstype, som hackere benytter, når formålet er at gøre en enhed utilgængelig, fx gøre en hjemmeside utilgængelig for brugerne.

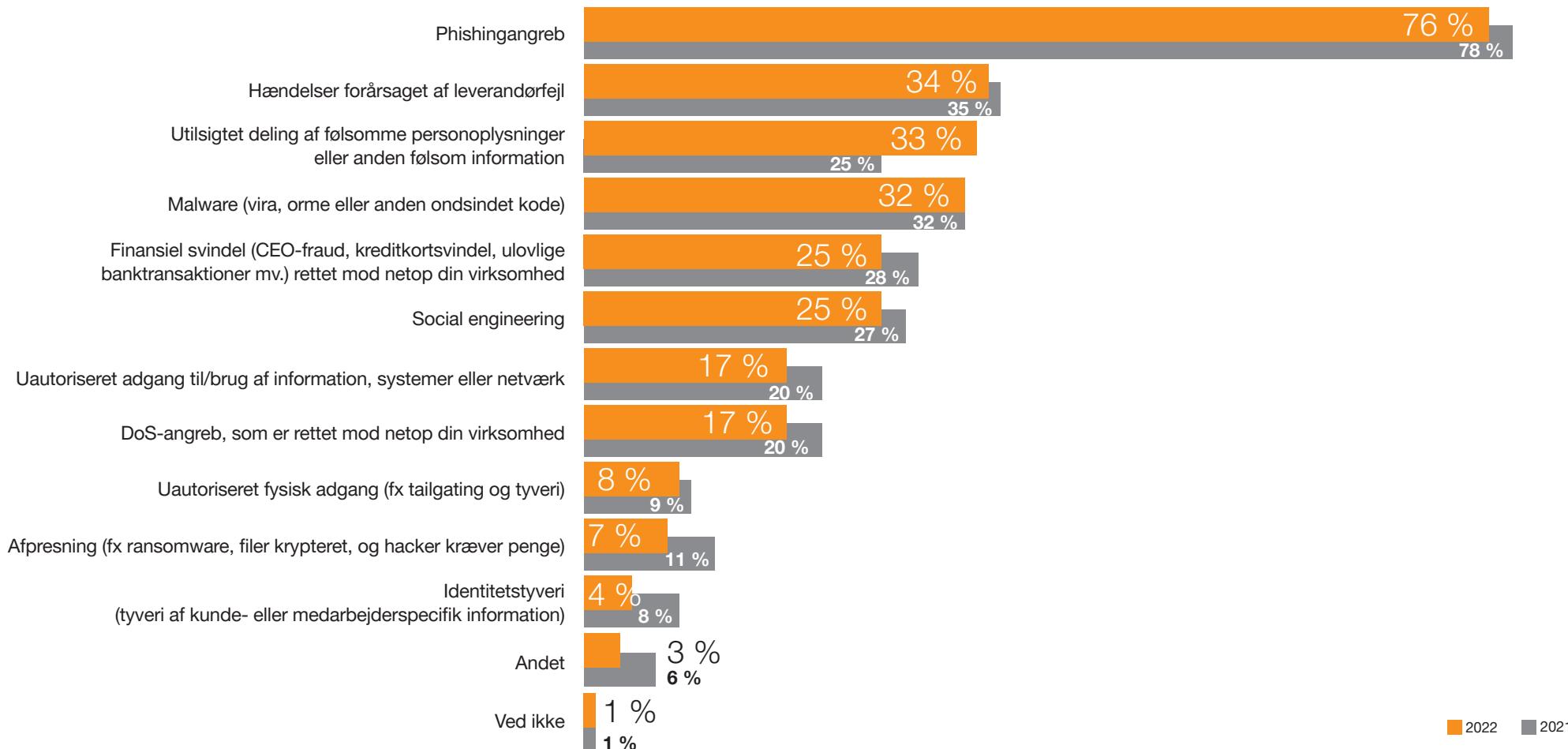
2 Domain-based Message Authentication, Reporting, and Conformance (DMARC) er en godkendelsesprocedure for e-mails, der beskytter mod misbrug af et domæne til fx CEO fraud og phishing.

## PwC anbefaler:

Hændelser som phishing kan få alvorlige konsekvenser for de ramte virksomheder, og derfor anbefaler PwC, at virksomhederne gør deres medarbejdere mere bevidste om denne type hændelser og gør dem klogere på, hvad de skal være opmærksomme på (awareness-træning). Tekniske tiltag kan være endpointbeskyttelse, som er en sikkerhedsløsning på virksomhedens enheder/aktiver, der kan forhindre cyberangreb, DMARC<sup>2</sup> på mailservere mv. Afpresning er heldigvis mindre udbredt (privat sektor: 5 %, finansiel sektor: 9 %, offentlig sektor: 14 %) end de fleste andre former for cyberangreb, men det kan få større konsekvenser for de virksomheder, der rammes. Virksomhederne kan derfor med fordel arbejde arbejde ud fra en risikobaseret tilgang og prioritere at beskytte sig mod hændelser ud fra balancen mellem, hvor ofte de finder sted, og hvor store konsekvenser de medfører.



## Hvilke hændelser har din virksomhed oplevet i de seneste 12 måneder som resultat af cyberkriminalitet eller informationssikkerhedshændelser?



2022 2021

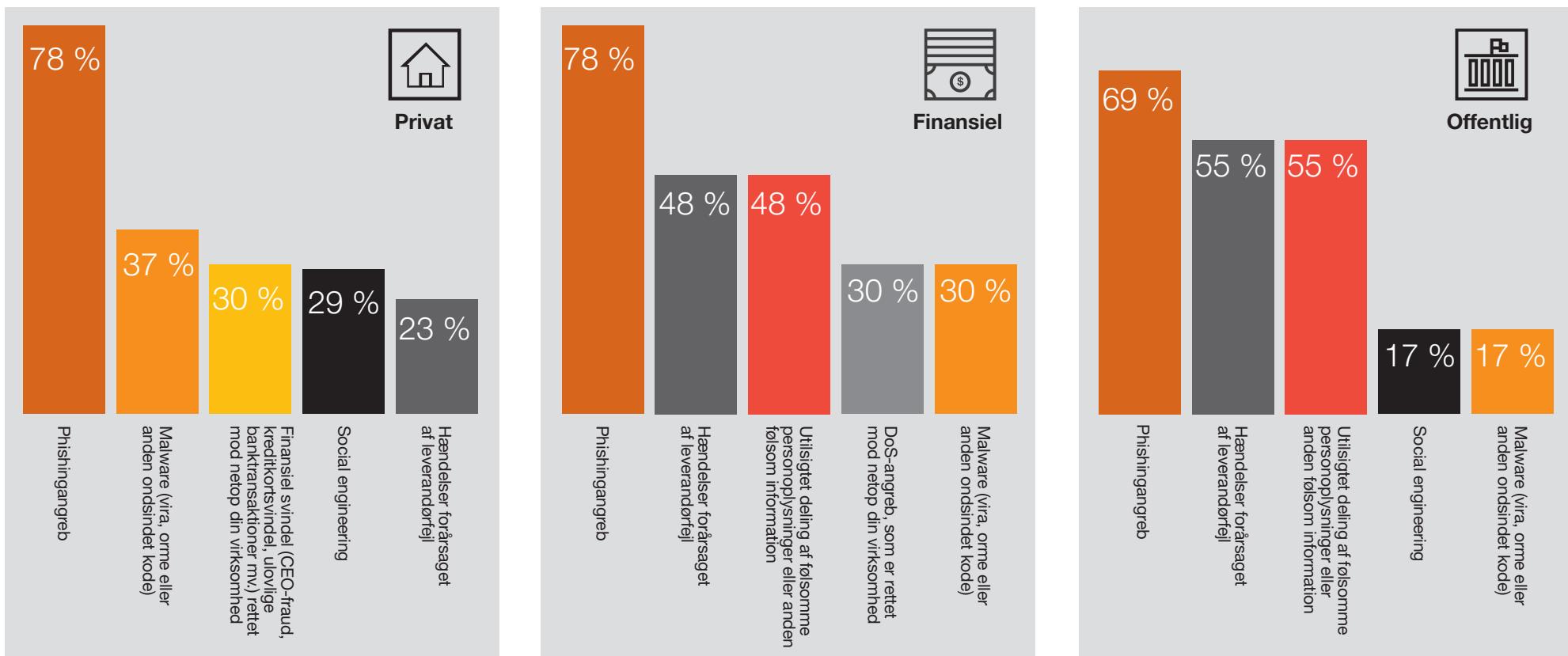


**78 %**

af CXO'erne og it-fagfolkene i den private sektor og den finansielle sektor har oplevet et phishingangreb

## TOP 5

### Top 5 hændelser fordelt på sektorer

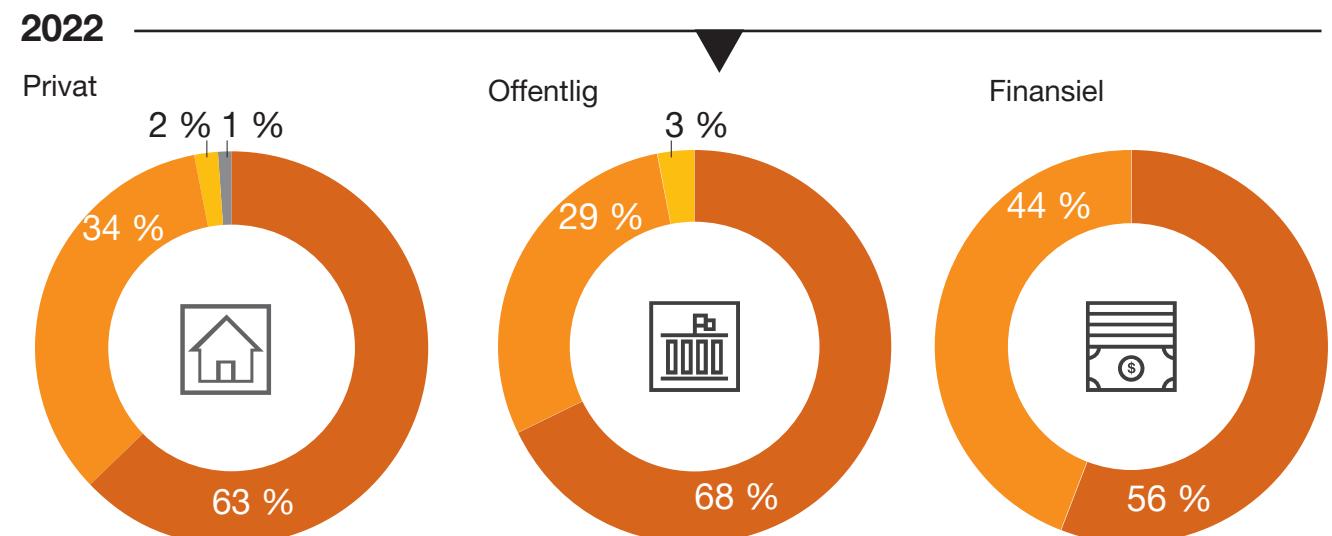


# Konflikten mellem Rusland og Vesten øger bekymringen for cybertrusler

Ruslands invasion af Ukraine har skabt et fornyet trusselsbillede i Vesten, og Center for Cybersikkerhed (CFCS) har i 2022 hævet trusselsniveauet for cyberaktivisme som følge af krigen. Trusselsbilledet kan løbende ændre sig i takt med en stigende uro og usikkerhed i verden, og virksomheder og offentlige organisationer bør derfor løbende holde øje med nye risici og ruste sig bedst muligt mod cyberangreb.

Det øgede trusselsniveau afspejler sig i CXO'ernes og it-fagfolkenes bekymring for cyberkriminalitet. PwC's Cybercrime Survey 2022 viser således, at 63 % af CXO'erne og it-fagfolkene i det private erhvervsliv er mere bekymrede for cybertruslen, end de var for 12 måneder siden. I de offentlige virksomheder er andelen af bekymrede endnu højere (68 %), mens den er lavest i den finansielle sektor (56 %).

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



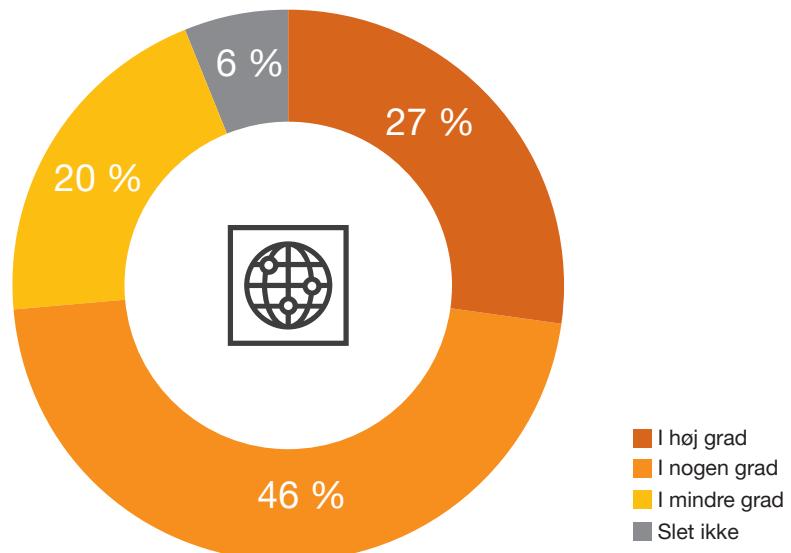


Stigningen i andelen af CXO'er og it-fagfolk, der bekymrer sig om cybertruslen, skyldes i overvejende grad konflikten mellem Rusland og Vesten. Således svarer hele 73 %, at

deres bekymring i nogen eller i høj grad er relateret til den vserende konflikt.



### Spørgsmål: I hvilken grad er denne bekymring relateret til konflikten mellem Rusland og Vesten?

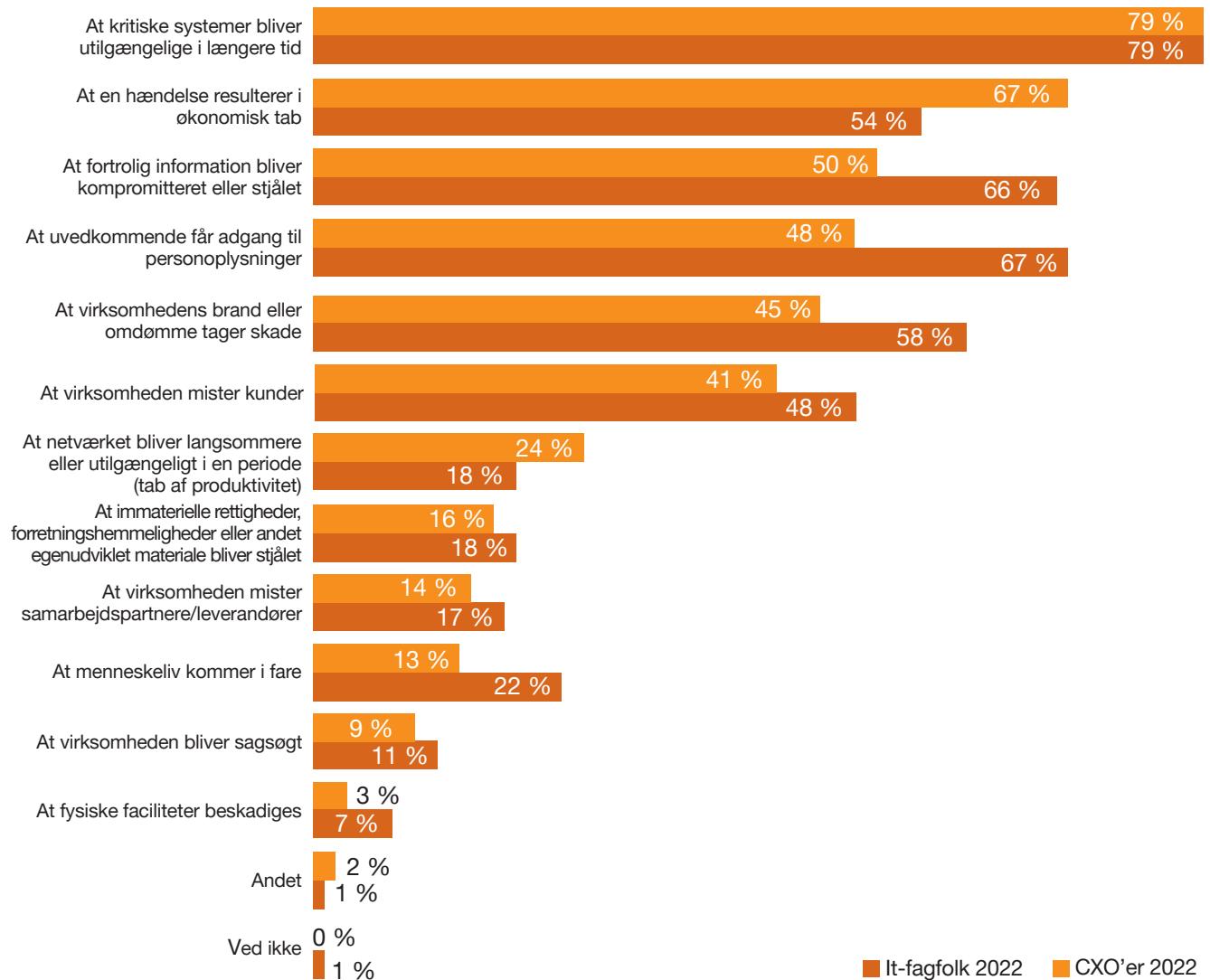




## Spørgsmål: Hvad er din virksomheds største bekymring i relation til konsekvenserne af en cyberhændelse?

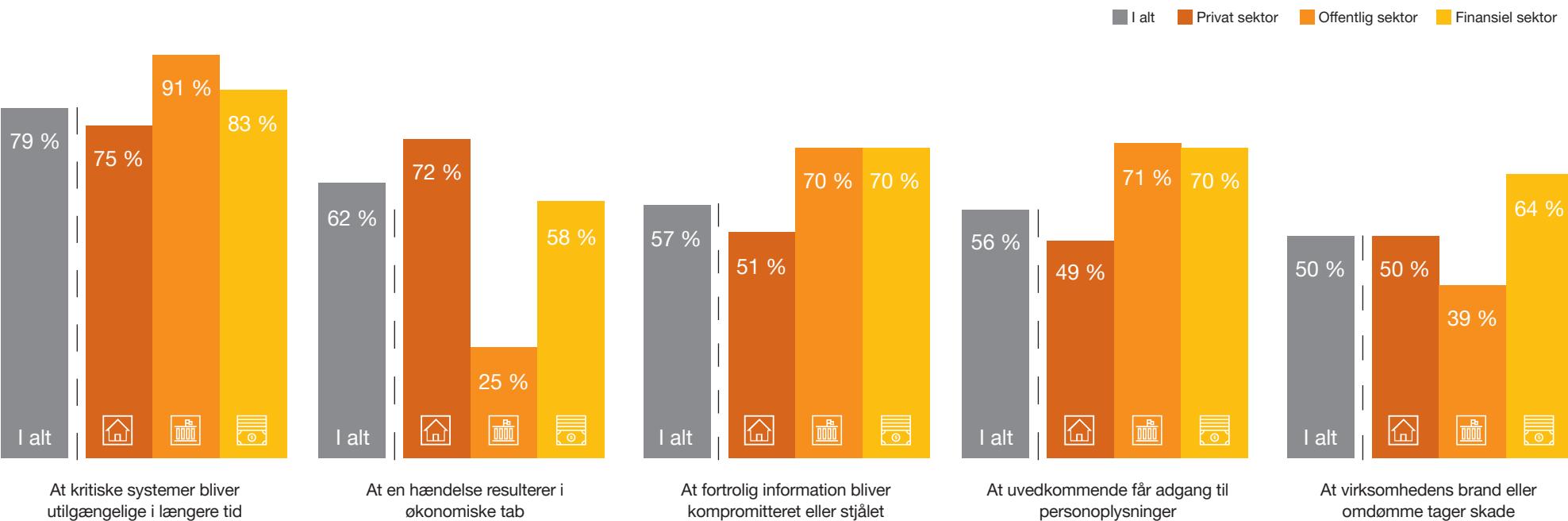
Otte ud af ti CXO'er og it-fagfolk udtrykker i undersøgelsen, at de er bekymrede for, at kritiske systemer bliver utilgængelige i længere tid som konsekvens af en cyberhændelse. Dernæst er både CXO'er og it-fagfolk bekymrede for, at fortrolig information kompromitteres eller stjåles, at uvedkommende får adgang til personoplysninger, og at virksomhedens brand eller omdømme tager skade.

Undersøgelsen viser desuden, at der er forskel på, hvilke følgevirkninger af et cyberangreb man er mest bekymret for i de tre sektorer (henholdsvis den private, den finansielle og den offentlige sektor). I den offentlige og i den finansielle sektor er man mere bekymret for, at fortrolig information bliver kompromitteret eller stjålet, og at uvedkommende får adgang til personoplysninger, end man er i den private sektor. Syv ud af ti i den offentlige og i den finansielle sektor udtrykker således bekymring for dette mod fem ud af ti i den private sektor. I den private og i den finansielle sektor er man til gengæld mere bekymret for, at brandet tager skade (henholdsvis 50 % og 64 %) end i den offentlige (39 %).





## Spørgsmål: Hvad er din virksomheds største bekymring i relation til konsekvenserne af en cyberhændelse? Fordelt på sektorer



# Truslen fra hacktivister er steget væsentligt

Ser man på virksomhedernes egne vurderinger af de største trusler i relation til cybersikkerhed, er der sket ændringer i forhold til sidste år. Det er fortsat organiserede kriminelle, der toppe listen over virksomhedernes største trusler mod cybersikkerheden. I år er der væsentligt flere danske virksomheder end sidste år, der regner hacktivismus blandt de største trusler. I 2022 vurderer 47 % af CXO'erne og it-fagfolkene, at

## Fakta:

Hacktivismus eller cyberaktivisme kan dække over forskellige typer af cyberangreb og angrebsvektorer. Fælles for dem alle er, at de oftest er en reaktion på en specifik begivenhed med et ideologisk eller politisk grundlag som motivation.



hacktivistere udgør en af de største trusler, mod 36 % i 2021. Udviklingen stemmer overens med CFCS' opjustering<sup>3</sup> af truslen fra cyberaktivisme mod danske virksomheder fra lav til middel i sommeren 2022. Ifølge CFCS' trusselsvurdering er det muligt, at fx pro-russiske hackere vil gå efter mål i Danmark. Dette er en ændring sammenlignet med de seneste år, hvor man ikke har vurderet, at cyberaktivister kunne have til hensigt at ramme danske mål.

Den trussel, der er steget mest i forhold til 2021 (12 %), er introduktionen af "de mange nye teknologier, herunder kunstig intelligens, IoT<sup>4</sup>, blockchain<sup>5</sup> og cloud-baserede værktøjer", som de cyberkriminelle kan drage nytte af. Virksomhederne anvender i stigende grad disse fremadstormende teknologier – oftest med henblik på innovation og effektivisering, men de udgør samtidig en øget risiko for cyberangreb. De nye teknologier åbner for nye sårbarheder og angrebsflader, som kan udnyttes af cyberkriminelle, hvis de ikke er implementeret eller konfigureret sikkert.

## PwC anbefaler:

En struktureret tilgang til cybersikkerhed giver organisationer bedre mulighed for effektivt at imødegå sofistikerede cyberangreb fra både cyberkriminelle og statsstøttede aktører. Det er essentielt, at organisationens topledelse har en god forståelse af trusselsbilledet og organisationens kritiske aktiver, og at de prioriterer sikkerhedsområdet. Der bør udvikles en flerårig, fleksibel og dynamisk sikkerhedsplan, så organisationen løbende kan tilpasse sig det omskiftelige cybertrusselsbillede. Denne tilgang bør omfatte alle områder i sikkerhedskonceptet PAVA (se side 40) og således være forankret både teknisk, organisatorisk og kulturelt.

3 <https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/cfcs-haver-trusselsniveauet-for-cyberaktivisme/>

4 Internet of Things dækker over genstande, som er forbundet til internettet – fx biler, hvidevarer eller legetøj.

5 En decentraliseret database. Det er bl.a. denne teknologi, som kryptovaluta mv. er bygget på, herunder bitcoin.



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



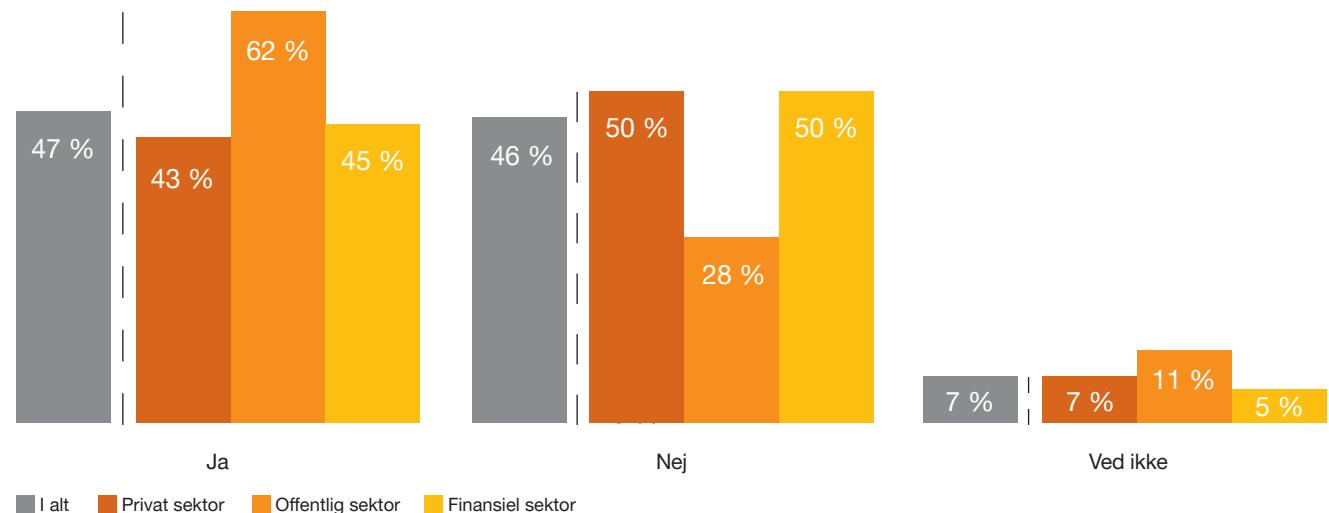
# Virksomheder indfører nye sikkerhedstiltag som følge af konflikten med Rusland

Krigen i Ukraine og konflikten mellem Rusland og Vesten giver anledning til en fornyet risikovurdering i virksomhederne. Det kan fx være nødvendigt at øge indsatsen for at lukke en backlog af sårbarheder, som er rettet mod de mest forretningskritiske processer og aktiver i virksomheden.

Ifølge undersøgelsen har knap halvdelen (47 %) af CXO'erne og it-fagfolkene planlagt eller implementeret nye sikkerhedstiltag som følge af konflikten. Der er væsentligt flere i den offentlige sektor, der har implementeret eller planlagt nye tiltag (62 %), end i den private sektor (43 %).

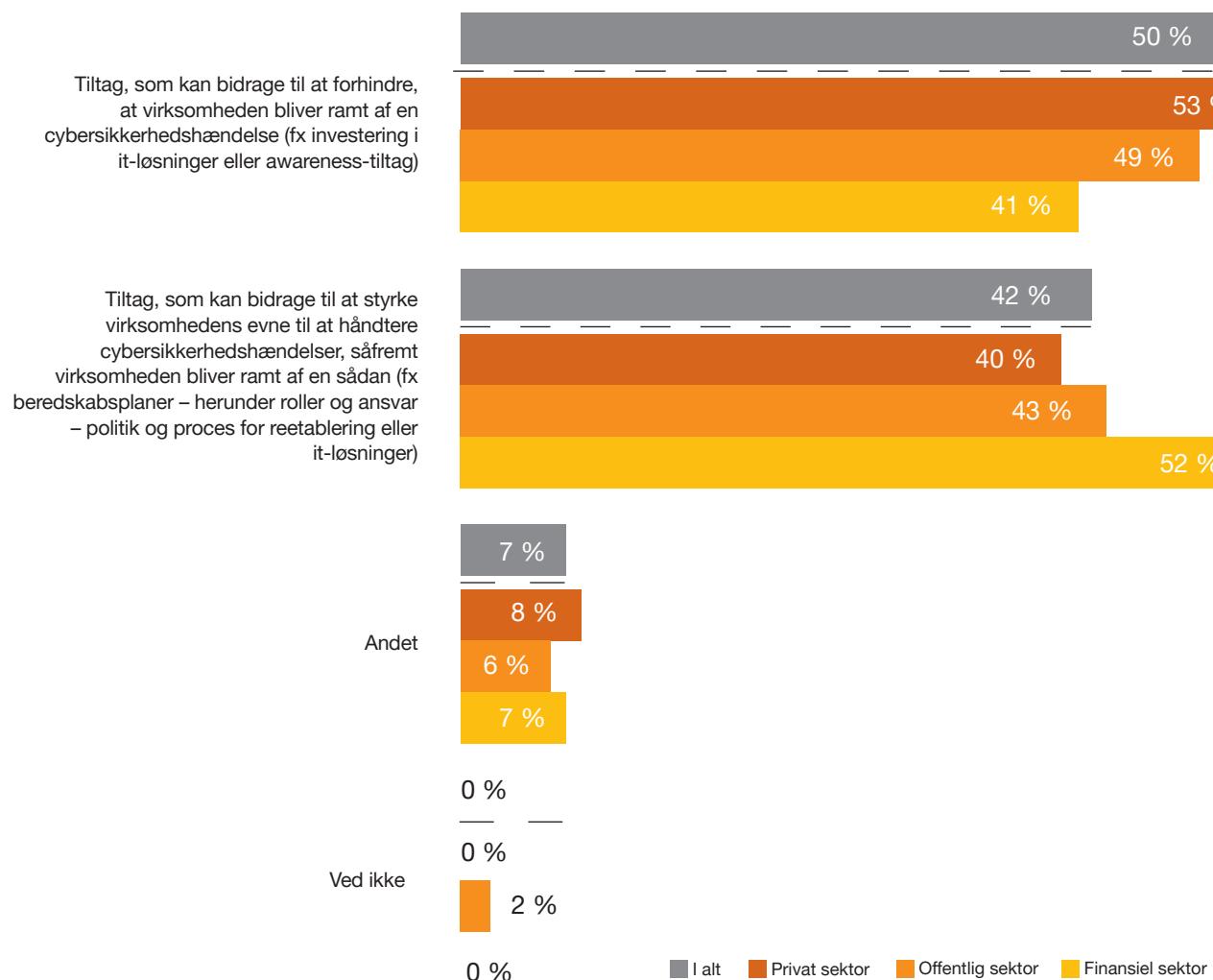


**Spørgsmål:** Har din virksomhed planlagt eller implementeret nye cybersikkerhedstiltag som følge af konflikten mellem Rusland og Vesten?





## Spørgsmål: Hvilke af følgende tiltag drejer dette sig om?



Undersøgelsen viser desuden, at halvdelen af CXO'erne og it-fagfolkene, som har angivet, at de har planlagt eller implementeret nye tiltag, fokuserer på tiltag, som kan bidrage til at forhindre, at virksomheden bliver ramt af en cybersikkerhedshændelse. Lidt færre (42 %) har planlagt tiltag, som kan styrke virksomhedens evne til at håndtere cybersikkerheds-hændelser. I den finansielle sektor er der flere virksomheder (52 %), der har implementeret eller planlægger dette.

PwC's cybersikkerhedsteam erfarer, at flere og flere virksomheder efterspørger bistand i forbindelse med beredskabsplanlægning – især med fokus på forretningsberedskab (business continuity) – hvilket delvist skyldes invasionen af Ukraine.

### PwC anbefaler:

Virksomheder og organisationer bør arbejde med at blive mere modstandsdygtige over for en given hændelse. Man kan med fordel tænke på cybertruslen som et spørgsmål om, hvornår man bliver ramt, og ikke hvorvidt man bliver ramt. Det kan være med til at skærpe virksomhedens fokus på aktiviteter, der kan genoprette virksomhedens systemer og netværk effektivt eller holde kritiske forretningsprocesser kørende gennem velafprøvede beredskabsplaner, som regelmæssigt justeres og tilpasses det nuværende trusselsbillede og virksomhedens udvikling.



## Plads til forbedring i virksomhedernes GDPR-compliance

56 % af CXO'erne og it-fagfolkene angiver, at deres største bekymringer i relation til konsekvenserne af en cyberhændelse er, "at uvedkommende får adgang til personoplysninger" (se side 15). GDPR og databeskyttelse er derfor fortsat områder, der kræver stor bevågenhed og høj prioritering.

Der er imidlertid fortsat potentiale for forbedring i en del virksomheder, når det kommer til niveauet af GDPR-compliance. Når PwC assisterer virksomhederne med at vurdere deres niveau af GDPR-compliance, anvender vores GDPR-eksperter en skala fra 0 til 5, hvor 5 er bedst. På denne skala giver 30 % af CXO'erne og it-fagfolkene deres virksomhed en

score på 2 eller derunder, hvilket er utilstrækkelige niveauer inden for GDPR-compliance. Det er positivt, at syv ud af ti responderer vurderer, at deres GDPR-compliance-niveau er "Defineret", "Kvantitativt styrende" eller "Optimeret" (hendesvis niveau 3, 4 og 5), og i den finansielle sektor er det hele 84 %, der angiver dette.

### PwC anbefaler:

GDPR-compliance-niveauet bør vurderes og gennemgås af uafhængige eksterne parter mindst én gang årligt, så man har større sikkerhed for, at man får et retvisende billede af organisationens modenhed. GDPR indebærer en lang række lovpligtige dokumenter, men "papirskjoldet" er ikke tilstrækkeligt til at efterleve GDPR. Et højt compliance-niveau kræver, at alle procedurerne bliver forankret i forretningen og indarbejdet som en del af de faste forretningsprocesser.

# 56 %

af CXO'erne og if-fagfolkene angiver, at deres største bekymringer er, at uvedkommende får adgang til personoplysninger

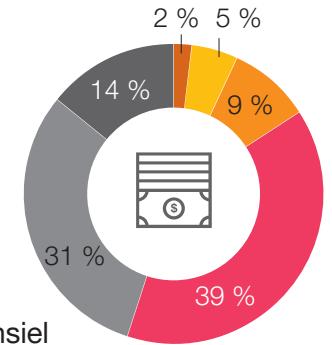
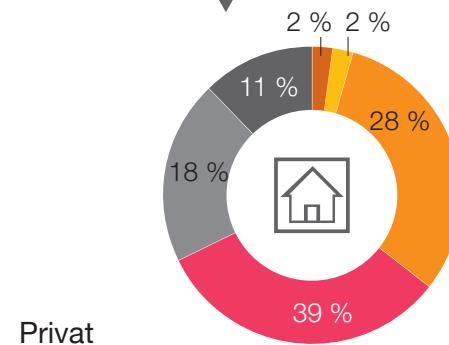
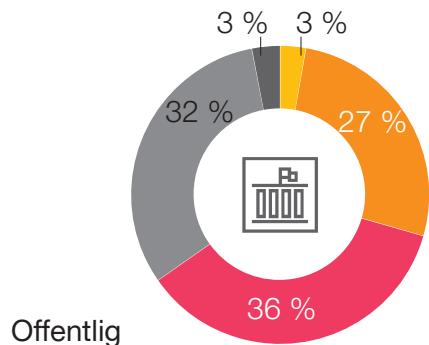


## Spørgsmål: Hvordan vurderer du din virksomheds GDPR-compliance-niveau?

OBS: Bemærk, at alle forhold i de forudgående niveauer skal være opfyldt, før organisationen kan egenvurdere sig til et højere niveau. Dvs. at for at vurdere sig som værende på niveau 4, skal alle krav til niveau 1-3 være opfyldt.



2022

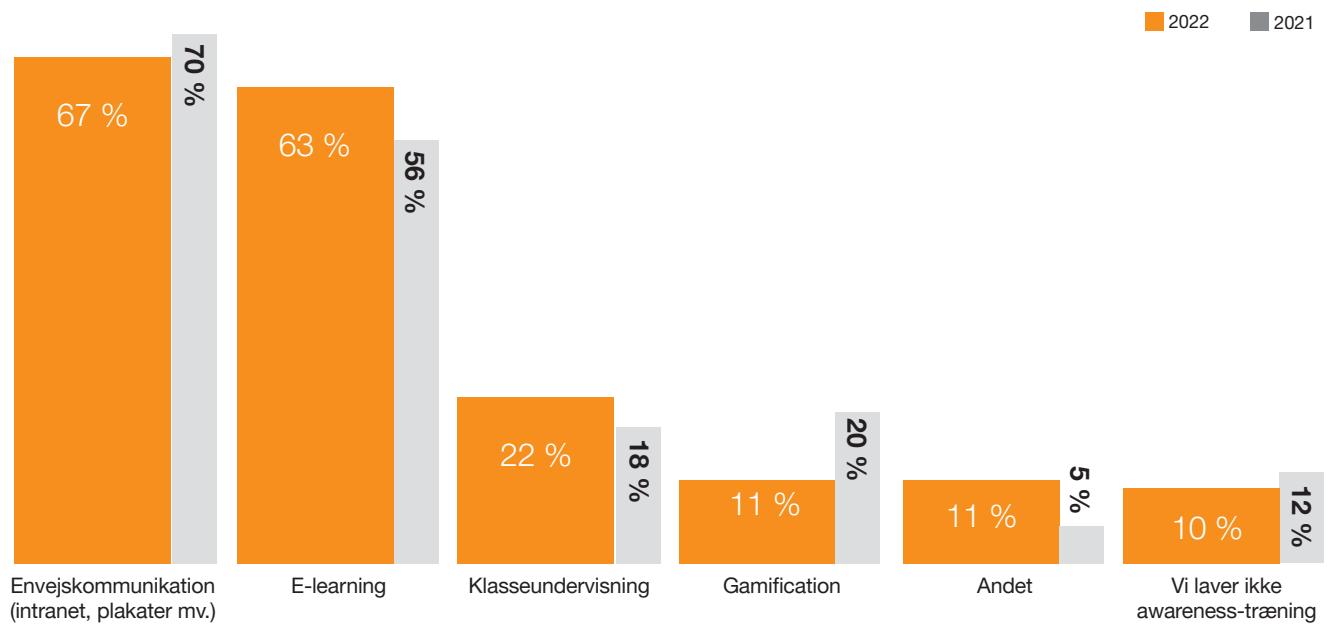




Ser man på, hvilke tiltag virksomhederne anvender til at øge medarbejdernes awareness – herunder på GDPR-området – er det ligesom i de forrige år envejskommunikation i form af fx plakater (67 %) og e-learning (63 %), der oftest anvendes. Dette er der ikke nødvendigvis noget i vejen med, så længe træningen er effektiv. Dog er der en tendens til, at awareness-træning kan have en for generel karakter, og at den dermed ikke er tilpas konkret og målrettet en medarbejders hverdag. Mange kan derfor med fordel i højere grad tilpasse e-learningen til målgrupper og/eller supplere med fx en anden type af undervisning, såsom klasseundervisning.



**Spørgsmål:** Hvilke af følgende tiltag har din virksomhed benyttet i forbindelse med GDPR og cyber- og informationssikkerheds-awareness inden for de seneste 12 måneder?  
Sæt gerne flere krydser.



### Game of Threats™

PwC's Game of Threats er specielt designet til at give ledelseslaget interaktiv undervisning i de risici, som er forbundet med cyberkriminalitet, og i vigtigheden af at investere i cyber- og informationssikkerhed.

Læs mere på [www.pwc.dk/cyberaware](http://www.pwc.dk/cyberaware)

# Plads til forbedring i virksomhedernes tillid til håndtering af GDPR og cybersikkerhed

Det er vigtigt for tilliden i vores samfund, at den enkelte borgere kan være tryg ved, at såvel den offentlige som den private sektor håndterer data sikkert og i overensstemmelse med gældende lovkrav og regler.

Med hensyn til tilliden til GDPR-compliance i sektorerne viser PwC's Cybercrime Survey 2022, at der stadig er en høj grad af tillid til den finansielle sektors GDPR-compliance-niveau. Således angiver knap ni ud af ti (88 %), at de i nogen eller i høj grad har tillid til denne sektors GDPR-compliance, hvilket er på niveau med 2021.

67 % svarer, at de i nogen eller i høj grad har tillid til statens håndtering af GDPR-compliance, hvilket ligeledes er på niveau med 2021 (69 %).

Når vi betragter tilliden til kommunernes GDPR-compliance, er der ligesom i de forgangne år plads til forbedring. I 2022 har 51 % angivet, at de har tillid til kommunernes håndtering, hvilket er en lille stigning i forhold til 2021 (47 %). Dog er det værd at bemærke, at hele 30 % angiver, at de i mindre grad har tillid til denne sektors niveau af GDPR-compliance, og at 16 % ingen tillid har til kommunernes håndtering af GDPR.

Angående den private sektor er der også plads til forbedring, idet 45 % angiver, at de i nogen eller i høj grad har tillid til denne sektors GDPR-håndtering, mens 42 % svarer "i mindre grad".

For så vidt angår tilliden til cybersikkerhed, er billedet ligeledes stort set uændret i forhold til 2021. Der er fortsat størst tillid til cybersikkerheden i den finansielle sektor, hvor hele 89 % angiver, at de i nogen eller i høj grad har tillid til cybersikkerheden (90 % i 2021). Tilliden til kommunernes niveau af cybersikkerhed er ligesom i de forgangne år lavest sammenlignet med øvrige sektorer, idet 31 % angiver, at de i nogen eller i høj grad har tillid til denne sektors niveau af cybersikkerhed (30 % i 2021). Næsten halvdelen (46 %) angiver, at de i mindre grad har tillid til kommunernes niveau af cybersikkerhed, mens en femtedel ingen tillid har til denne sektors cybersikkerhed.

Scan koderne, og læs mere om NIS2 og DORA

NIS2



DORA



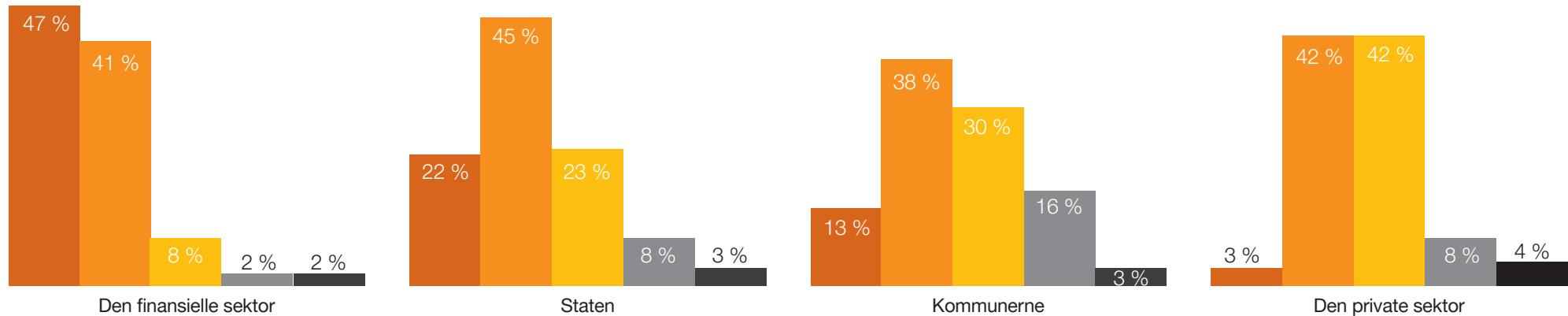
## PwC anbefaler:

Tillid spiller en væsentlig rolle som fundamentet i en enhver forsyningsskæde og ethvert samfund. De seneste års sikkerhedshændelser understreger netop vigtigheden af at validere samarbejdspartners praksis for at kunne skabe tillid på tværs af virksomheder, organisationer og samfundets borgere. Flere af de love og regulativer, der er på vej (NIS2 og DORA), adresserer netop det at skabe tillid til de samfundskritiske institutioner. PwC's sikkerhedskoncept, PAVA, beskæftiger sig netop med validering gennem en tilgang, der skal sikre opdagelse og verificering af svagheder i virksomhedens tekniske og organisatoriske kontroller. Tillid bør således anses som et værdiskabende koncept – ikke alene internt i organisationen, men også som en mulighed for at skabe en konkurrencemæssig fordel udadtil for kunder/borgere, relationer og samarbejdspartnere.

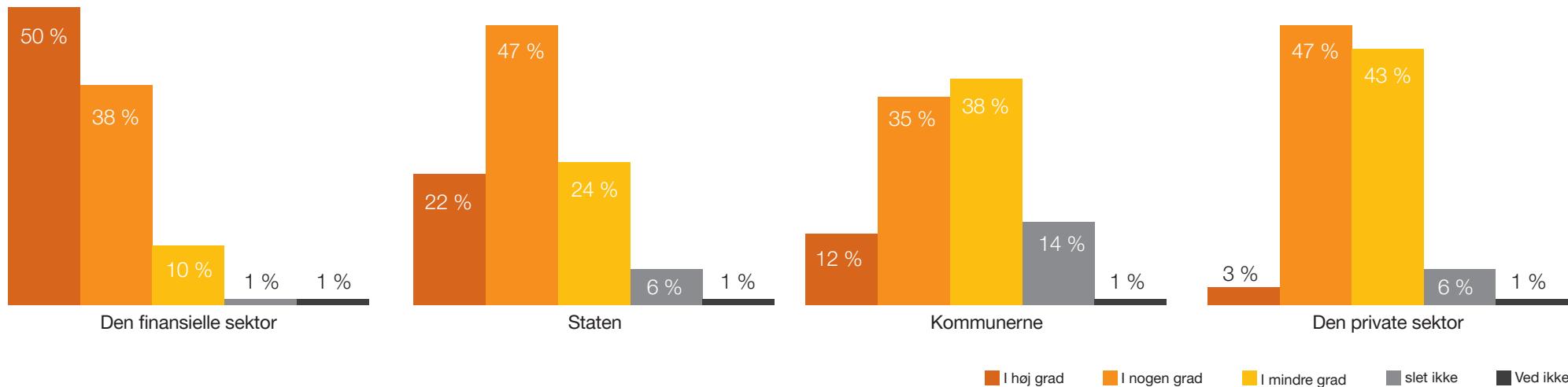


## Spørgsmål: I hvilken grad har du tillid til GDPR-compliance-niveauet i?

2022



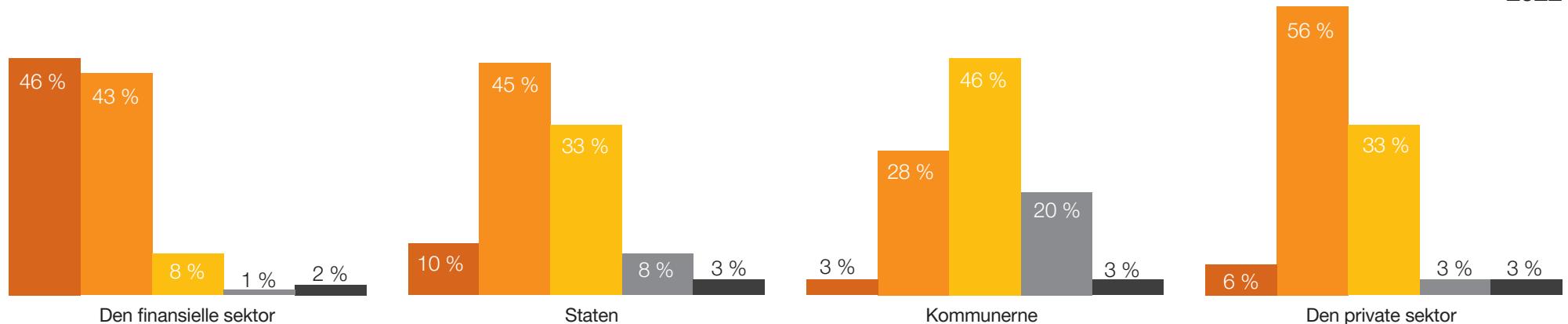
2021



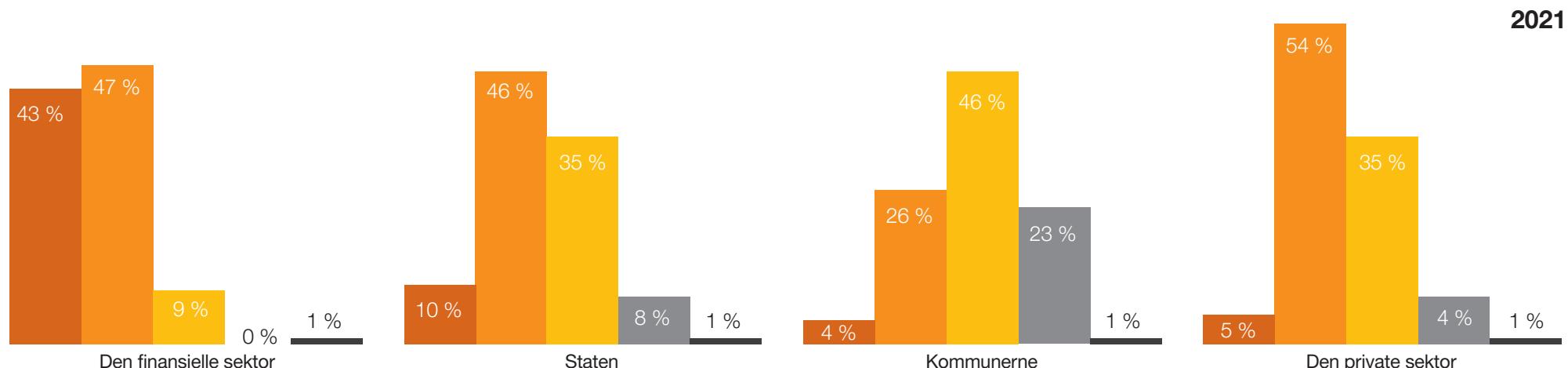


## Spørgsmål: I hvilken grad har du tillid til cybersikkerheden?

2022



2021



■ I høj grad ■ I nogen grad ■ I mindre grad ■ slet ikke ■ Ved ikke

# Behov for øget ledelsesfokus på cybersikkerhed

Topledelsen i en virksomhed skal prioritere cybersikkerhed og sørge for, at virksomheden har de rette sikkerhedstiltag, så den er i stand til at beskytte sig bedst muligt mod cybertruslen.

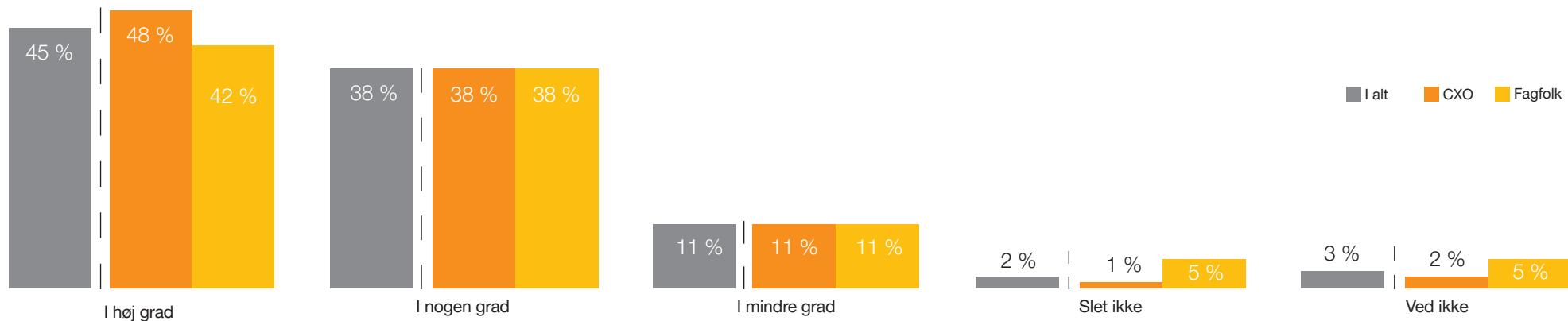
Undersøgelsen viser, at rekordmange CXO'er og it-fagfolk (45 %) vurderer, at direktionen/ledelsen i høj grad har fokus på at opnå den rette balance mellem de cybertrusler, virksomheden står over for, risikoen for virksomheden og deres

investeringer i cybersikkerhed. Lidt over halvdelen angiver dog, at der kun i nogen grad, i mindre grad eller slet ikke er balance mellem cybertruslen på den ene side og investeringer i cybersikkerhed på den anden. Der er således plads

til, at direktionen/ledelsen i lidt over halvdelen af virksomhederne øger deres fokus på at opnå en bedre balance på området og dermed i højere grad beskytter virksomheden mod cyberangreb.



**Spørgsmål:** I hvilken grad har direktionen/ledelsen i din virksomhed – efter din opfattelse – fokus på at opnå den rette balance mellem de cybertrusler, I står over for, og investeringer i cybersikkerhed?

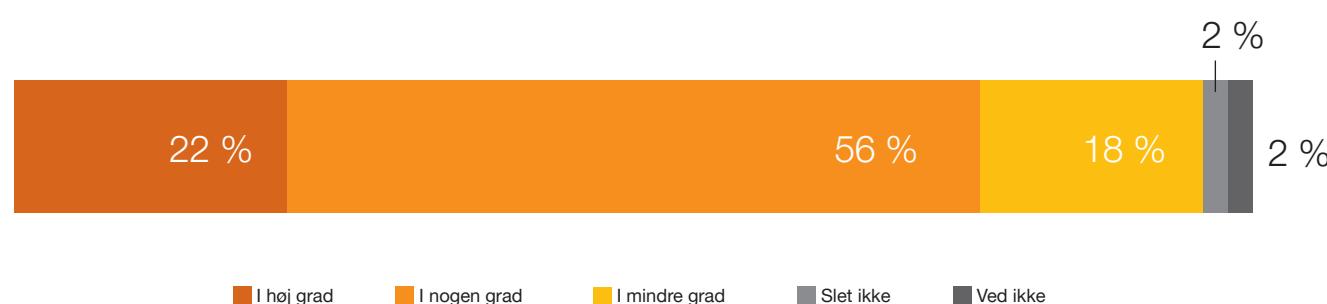




Ud over topledelsens fokus har virksomhedens generelle cyberkompetencer betydning for muligheden for at håndtere cybertrusler. Ifølge undersøgelsen mener kun godt en femtedel af CXO'erne og it-fagfolkene (22 %), at virksomheden i høj grad besidder tilstrækkelige cyberkompetencer til at ruste den mod aktuelle cybertrusler. Desuden svarer en femtedel (20 %), at virksomheden kun i mindre grad eller slet ikke har de rette kompetencer.



**Spørgsmål:** I hvilken grad vurderer du, at din virksomhed besidder tilstrækkelige cyberkompetencer til at ruste virksomheden mod aktuelle cybertrusler?



**PwC anbefaler:**

Det kan være vanskeligt for en direktion/ledelse selv at vurdere virksomhedens cybersikkerhedsniveau og trusselsbillede. Vi anbefaler derfor, at virksomhedens cybersikkerhedsniveau vurderes og gennemgås af uafhængige, eksterne partnere mindst hvert år, og at virksomheden løbende foretager intern kontrol af egne kompetencer. Et højt cyberkompetenceniveau kræver løbende validering, da der sker konstante ændringer på området. Vi anbefaler desuden, at de benchmark og standarde, virksomheden anvender til at vurdere dens modenhed, kan sammenlignes, så man har mulighed for løbende at følge udviklingen.

# Bestyrelsens styrerammer og håndtering bør forbedres

Cybersikkerhed er et anliggende for virksomhedens bestyrelse, som har ansvaret for at vurdere virksomhedens risici og beslutte, på hvilket niveau virksomheden skal beskytte sig mod cybertruslen.

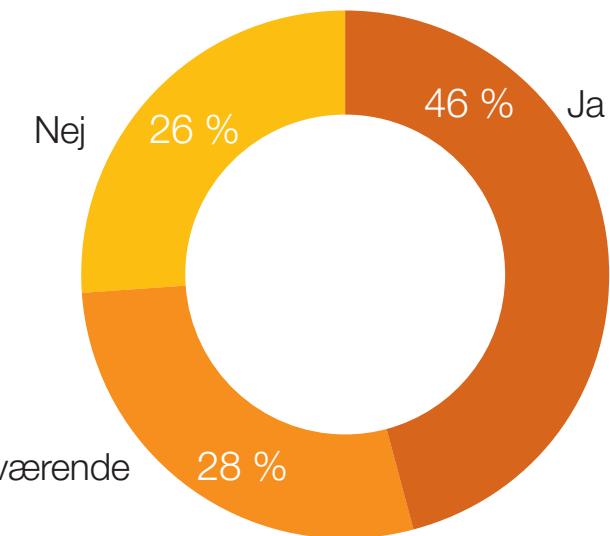
Det er bestyrelsens ansvar at sikre værdiskabelse og konkurrenceevne samt at beskytte virksomhedens værdier, både på kort og langt sigt (jf. selskabslovens § 115). Bestyrelsen er ansvarlig for virksomhedens strategi og opfølging på gennemførelse af strategien. Dette gælder også, når det kommer til cybersikkerhed, da en cyberhændelse i værste fald kan påvirke såvel virksomhedens bundlinje som evnen til at nå de strategiske mål.

Denne del af undersøgelsen er derfor målrettet bestyrelsen.

Ifølge undersøgelsen er cybersikkerhed i stigende grad en tilbagevendende del af bestyrelsesarbejdet. Men selvom der er fremgang at spore, er der fortsat mange virksomheder, hvor der ikke er tilstrækkelig styring. Næsten halvdelen (46 %) af bestyrelsesmedlemmerne angiver, at deres virksomhed har etableret en længerevarende handlingsplan/et program for cyberområdet, mens 28% er i gang med at etablere dette. 26 % har ikke en længerevarende handlingsplan/et program for cyberområdet og er ikke gået i gang med dette. En handlingsplan/et program består af et sæt dokumenterede aktiviteter og skal bidrage til at bringe virksomhedens cybersikkerhed op på et acceptabelt niveau over en periode.



**Spørgsmål:** Har din virksomhed etableret en længerevarende handlingsplan/et program for cyberområdet\*?



\* Definition: En længerevarende handlingsplan/et program for cyberområdet defineres som et sæt af dokumenterede aktiviteter, der over en periode bringer virksomhedens cybersikkerhed op på et acceptabelt niveau.



Desuden svarer 39 % af bestyrelsesmedlemmerne, at de ikke har cybersikkerhed som en fast del af årshjulet, som skal sikre, at cybersikkerhed prioriteres og er på virksomhedens agenda, mens 61 % angiver, at dette er tilfældet.

Herudover angiver 23 % af bestyrelsesmedlemmerne, at de mindre end én gang om året eller aldrig behandler information om cyberrisici. 54 % af bestyrelsesmedlemmerne angi-

ver, at de ikke/kun delvist fører kontrol med, at virksomheden har testede beredskabsplaner i tilfælde af hændelser. Både behandling af information om cyberrisici og kontrol med, at beredskabsplaner er testede, skal bidrage til, at bestyrelsen kan tage stilling til virksomhedens risikoappetit og evne til at håndtere cyberhændelser.



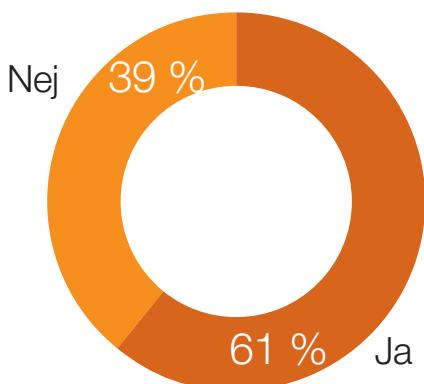
### Spørgsmål:

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



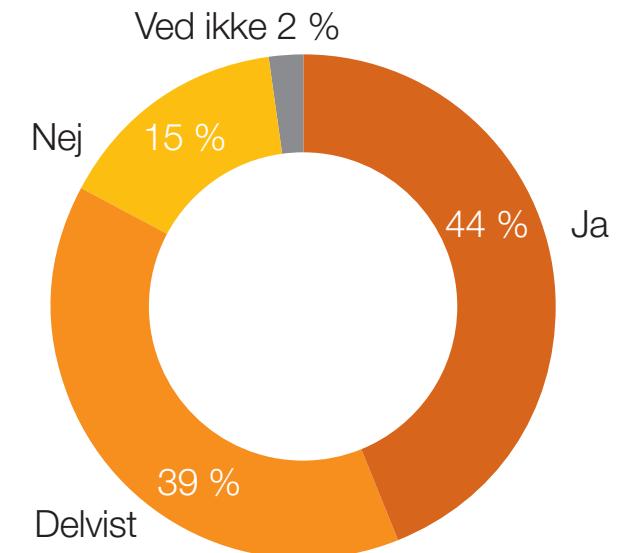
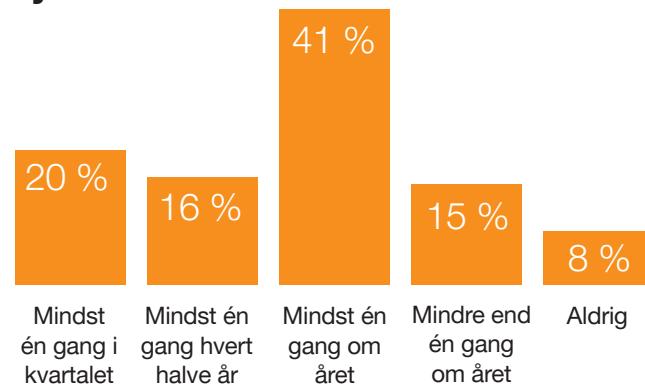
### Spørgsmål:

**Har bestyrelsen cybersikkerhed som en fast del af sit årshjul?**



### Spørgsmål:

**Hvor ofte modtager og behandler bestyrelsen information om cyberrisici?**





Et tilstrækkeligt videngrundlag er forudsætningen for, at bestyrelsen kan håndtere virksomhedens cybersikkerhed hensigtsmæssigt. Alligevel er det kun halvdelen (51 %) af bestyrelsesmedlemmerne, som angiver, at de mindst én gang om året modtager en anvendelig rapport vedrørende cybersikkerhed.

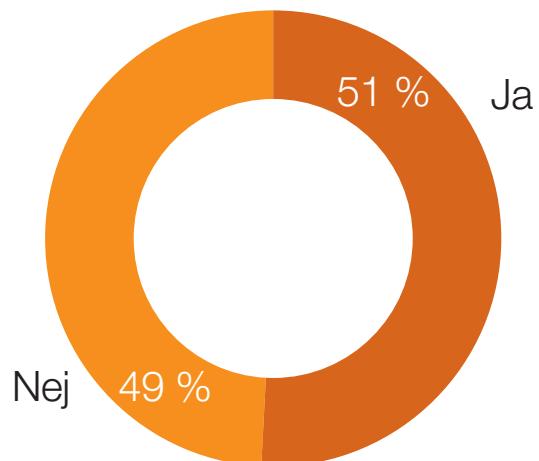
Undersøgelsen viser desuden, at kun 10 % af bestyrelsesmedlemmerne modtager træning i cyber- og informationssikkerhed. Dertil kommer, at hele 39 % af bestyrelsesmedlemmerne ikke vurderer, at sammensætningen af bestyrelsens kompetencer giver dyb nok viden om cyber- og

informationssikkerhed. Bestyrelsesmedlemmers viden om cyber- og informationssikkerhed kan forbedres ved at sætte cyber- og informationssikkerhed højere på agendaen og ved at få inspiration fra eksterne parter.



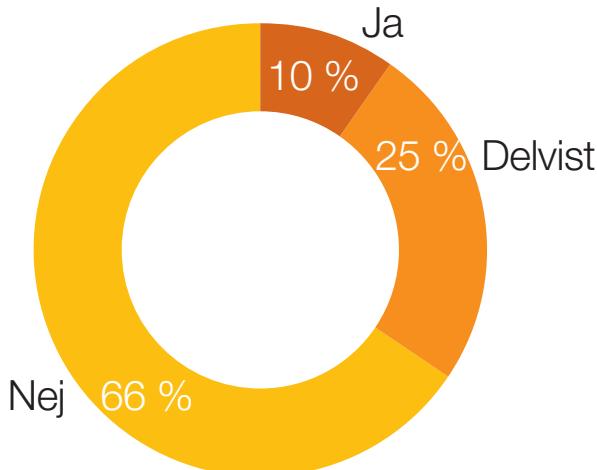
#### Spørgsmål:

**Modtager bestyrelsen mindst én gang årligt en anvendelig rapport vedrørende cybersikkerhed?**



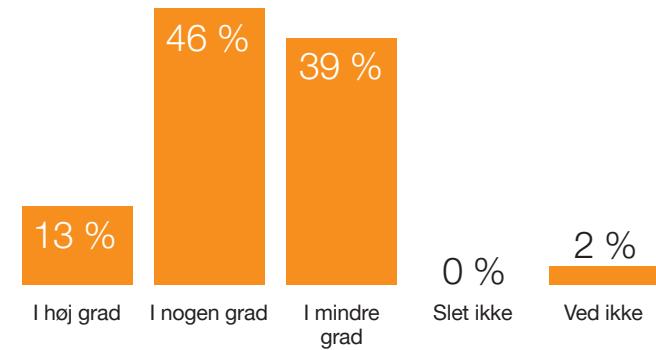
#### Spørgsmål:

**Modtager bestyrelsen træning i cyber- og informationssikkerhed?**



#### Spørgsmål:

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





### PwC anbefaler:

Bestyrelsen bør minimum årligt modtage en risiko- og sårbarhedsvurdering af virksomheden fra direktionen. Desuden bør bestyrelsen minimum årligt tage stilling til virksomhedens risikoappetit, hvor bestyrelsen godkender den samlede risikostrategi – inklusive de specifikke aktiviteter, som virksomheden ønsker at igangsætte for at forbedre processer, styrke arkitekturen, øge god adfærd, forbedre beredskabet og dermed reducere det samlede risikobillede. Det anbefales desuden, at cybersikkerhed er en fast del af bestyrelsens årshjul, og at det er på agendaen på bestyrelsesmøder. For at opretholde virksomhedens evne til at håndtere konkrete hændelser, bør bestyrelsen yderligere mindst én gang om året kontrollere, at virksomhedens beredskabsplaner er opdaterede. Der bør jævnligt gennemføres træningsforløb med fokus på cyber- og informationssikkerhed, som er målrettet bestyrelsesmedlemmer, og som kan styrke deres viden om og kompetencer i relation til cybersikkerhed.





## Syv ud af ti større virksomheder forventer at øge investeringerne i cybersikkerhed

Undersøgelsen viser, at størstedelen af virksomhederne forventer at øge investeringerne inden for cyber- og informationssikkerhed. Således svarer 59 %, at virksomhedens cyber- og informationssikkerhedsbudget forventes at vokse inden for de næste 12 måneder. Dette tal var sidste år 62 %.

Særligt i de større private virksomheder (virksomheder med mindst 200 ansatte) forventer man at øge sikkerhedsbudgettet. Her forventer syv ud af ti (72 %) af CXO'erne og it-fagfolkene, at virksomhedens cybersikkerhedsbudget vil vokse inden for de næste 12 måneder. Til sammenligning

forventer knap seks ud af ti fra de større finansielle virksomheder en stigning, mens det kun er fem ud af ti fra større offentlige virksomheder.

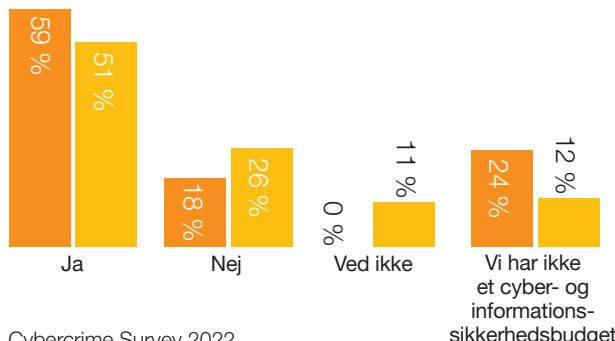


**Spørgsmål:** Forventer/Tror du, at virksomhedens cyber- og informationssikkerhedsbudget vil vokse inden for de næste 12 måneder?

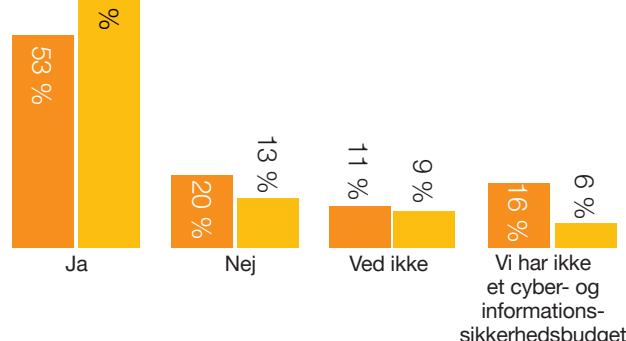


### Sektorer

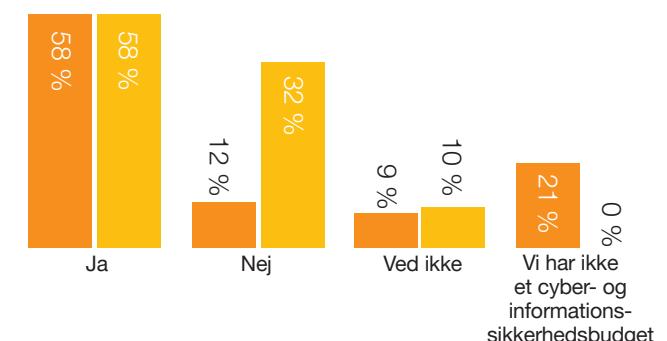
#### Offentlig



#### Privat



#### Finansiel



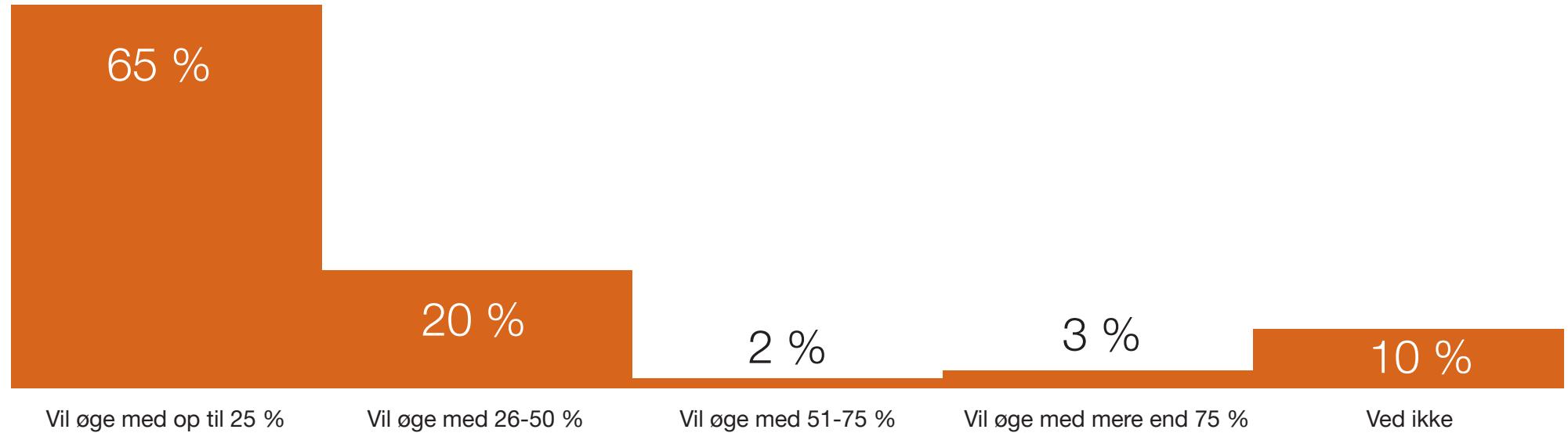


Heraf forventer 65 %, at budgettet vil stige med op til 25 %, mens dette tal var 59 % sidste år. En fjerdedel forventer en budgetstigning på over 25 %.



### Spørgsmål:

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





Ledelsen i en virksomhed har en forpligtelse over for alle sine interesser – medarbejdere, kunder, leverandører og samarbejdspartnere – til at beskytte virksomheden mod digitale trusler. Dette kræver løbende investeringer inden for cybersikkerhed.

Undersøgelsen viser, at hele 56 % af CXO'erne og it-fagfolkene peger på, at awareness-træning er virksomhedens højst prioriterede investering de næste 12 måneder. Investering i awareness-træning har ligget højt på listen i flere år, da det er en løbende proces at træne sine medarbejdere, idet cybertruslen konstant udvikler sig. Den høje placering hænger tæt sammen med, at 59 % af CXO'erne og it-fagfolkene vurderer, at de ansattes ubevidste handlinger er blandt de største trusler (se side 17).

På en andenplads over prioriterede investeringer findes "segmentering af netværk", som lå på en femteplads sidste år. Til gengæld falder investeringer i "identity and access management" (IAM), "privilegeret adgangsstyring" (PAM) og "central og intelligent logning (SIEM) i prioritering i forhold til 2021. Det kan hænge sammen med, at der typisk er tale om engangsinvesteringer, som virksomhederne kan have foretaget i tidligere år.

I den finansielle sektor er det særligt investeringer i segmentering af netværk og "endpoint detection and response (EDR)", der ligger højt på listen. Det samme gælder for den private sektor, hvor lidt færre planlægger at investere i disse områder end i den finansielle sektor. I den offentlige sektor ligger investeringer i metodeforankring og SIEM højt.

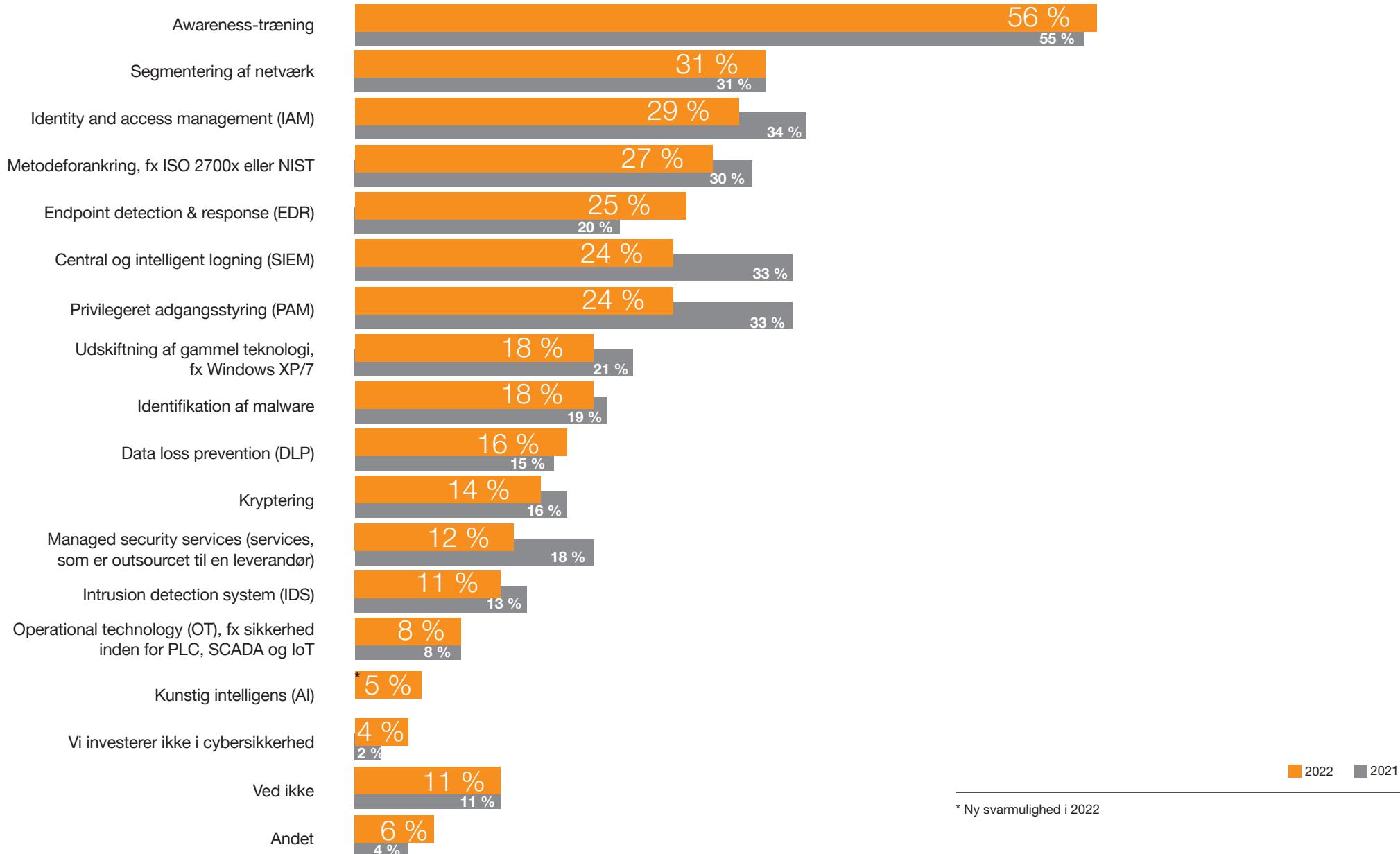
Mange sikkerhedstiltag, foruden awareness-træning, har det til fælles, at når systemerne først er implementeret, er der ikke behov for yderligere investeringer, og virksomheden kan prioritere andre sikkerhedsområder højere. Fx er det PwC's erfaring, at den finansielle sektor bredt set allerede har implementeret IAM, PAM og SIEM, hvorfor disse områder ligger relativt lavt på listen over prioriterede investeringer i sektoren.

## Awareness-træning

har ligget højt på listen i flere år, da det er en løbende proces at træne sine medarbejdere, idet cybertruslen konstant udvikler sig



## Spørgsmål: Hvad er din virksomheds højst prioriterede investeringer inden for it-sikkerhed de næste 12 måneder?



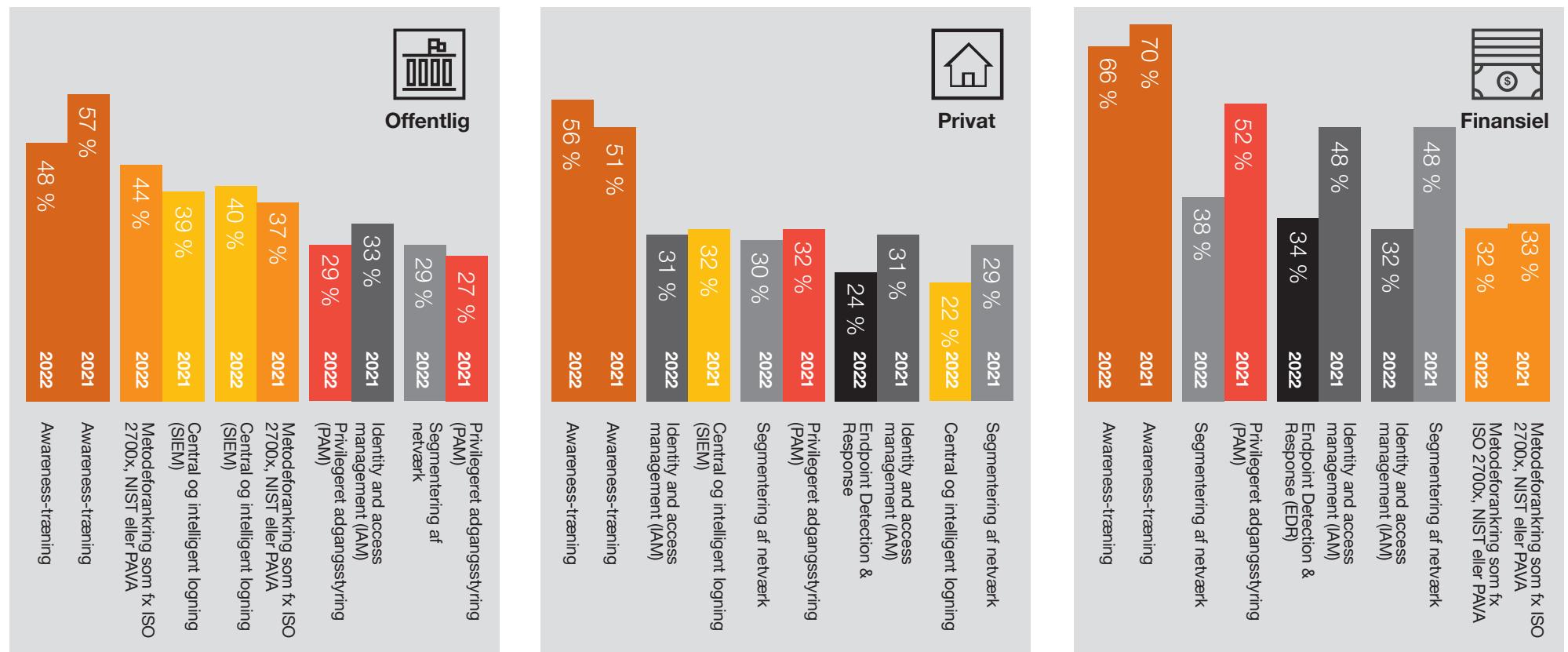


**56 %**

peger på, at awareness-træning er virksomhedens højest prioriterede investering

## TOP

### Virksomhedernes top 5 prioriterede investeringer indenfor it-sikkerhed de næste 12 måneder



# Et norsk perspektiv

101 norske virksomhedsledere, it-chefer og it-sikkerhedsspecialister har gennem PwC's Cybercrime Survey 2022 delt deres syn på en række spørgsmål relateret til cybersikkerhed.

Generelt er bekymringen for cybertrusler stigende, og over halvdelen af responderne (Danmark: 63 %, Norge: 64 %) angiver, at de er mere bekymret for cybertrusler i dag, end de var for et år siden.

Det, at kritiske systemer bliver utilgængelige i længere tid, er fortsat den største bekymring – både i Danmark og i Norge (Danmark: 79 % og Norge: 77 %, hvilket for Norge er en stigning på 9 % fra sidste år (Danmark: 77 %, Norge: 68 %)).

Respondenter, som er mere bekymrede for cybertrusler sammenlignet med for 12 måneder siden



Respondenter, som er bekymrede for at kritiske systemer bliver utilgængelige i længere tid



■ Danmark ■ Norge

På spørgsmålet om, hvorvidt virksomhederne har planlagt eller implementeret nye sikkerhedstiltag som følge af konflikten mellem Rusland og Vesten, har over halvdelen af de norske responderne svaret, at de har planlagt eller implementeret nye cybersikkerhedstiltag som følge heraf (Danmark: 47 %, Norge: 57 %).

Der ses afvigelser mellem de danske og norske besvarelser, i forhold til hvilke sikkerhedstiltag der er blevet implementeret.

Over halvdelen af de norske besvarelser nævner, at de har indført eller planlagt tiltag, der kan bidrage til at styrke virksomhedens evne til at håndtere cybersikkerhedshændelser, fx beredskabsplaner (Danmark: 42 % Norge: 54 %). Derimod fokuserer halvdelen af de danske besvarelser på tiltag, som kan bidrage til at forhindre, at virksomheden bliver ramt af en cybersikkerhedshændelse, fx investering i it-løsninger eller awareness-tiltag (Danmark: 50 %, Norge: 32 %).

Derudover er der forskel på, hvor virksomhedernes højest prioriterede investering i it-sikkerhed ligger. I Norge er identity and access management (IAM) den højest prioriterede investering i de kommende 12 måneder (Danmark 29 %, Norge: 51 %), mens den højest prioriterede investering i Danmark er awareness-træning (Danmark 56 %, Norge: 38 %).

Virksomheder, der har planlagt eller implementeret nye sikkerhedstiltag som følge af konflikten mellem Rusland og Vesten



Hvilke af følgende tiltag drejer dette sig om?

Danmark

■ Tiltag, der kan bidrage til at styrke virksomhedens evne til at håndtere cybersikkerhedshændelser, såfremt virksomheden bliver ramt af en sådan (fx beredskabsplaner – herunder roller og ansvar – politik og proces for reetablering eller it-løsninger)

Norge

■ Tiltag, der kan bidrage til forhindre, at virksomheden bliver ramt af en cybersikkerhedshændelse (fx investering i it-løsninger eller awareness-tiltag)

■ Andet



## Om undersøgelsen

518 danske og 101 norske virksomhedsledere, it-chefer og it-sikkerhedsspecialister har deltaget i PwC's Cybercrime Survey 2022.

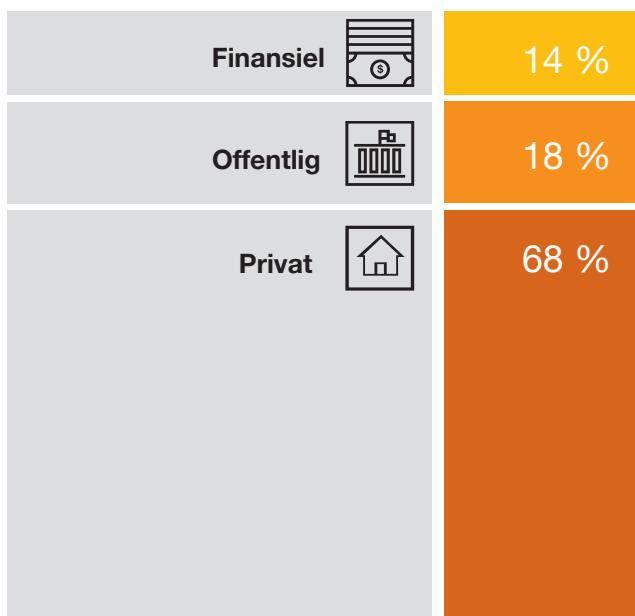
Undersøgelsen er igen i år gennemført med opbakning fra Center for Cybersikkerhed, DI Digital, Finans Danmark, Dansk Erhverv, IT-Branchen, Dansk It, KITA, Rådet for Digital Sikkerhed, ISACA, Microsoft, DK Hostmaster og Bestyrelsesforeningen. Analysen bygger på onlinebesvarelser.

Respondenterne er blevet stillet en række spørgsmål inden for cyber- og informationssikkerhed, fx om de er blevet ramt af et cyberangreb; om de forventer, at deres cyber- og informationssikkerhedsbudget vil stige; og hvad der er deres højest prioriterede investeringer.

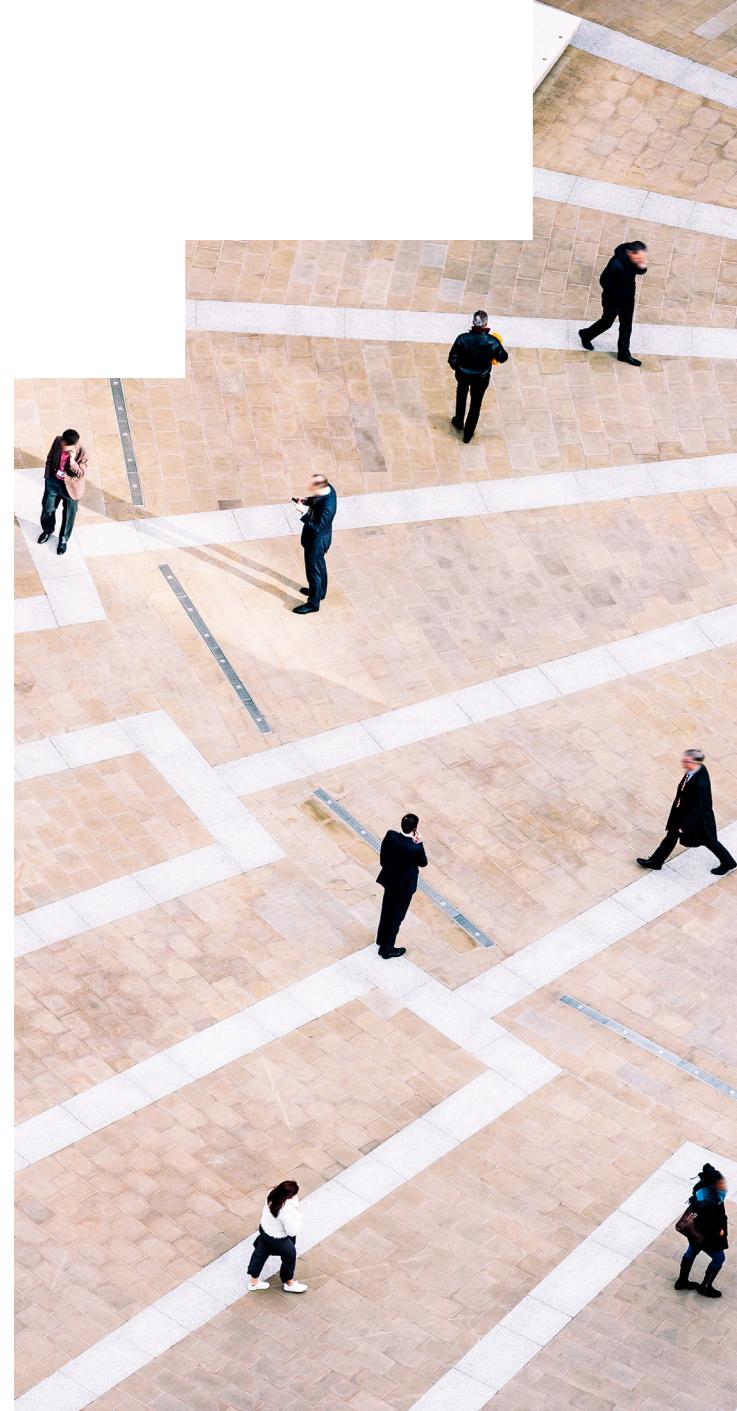
Målingens spørgsmål og svarmuligheder er udarbejdet af PwC, og onlinespørgeskemaet er udsendt i samarbejde med fornævnte organisationer.



### Undersøgelsens respondenter fordelt på sektorer:



Større virksomheder er defineret som  $\geq 200$  medarbejdere.  
Mindre virksomheder er defineret som  $\leq 199$  medarbejdere.

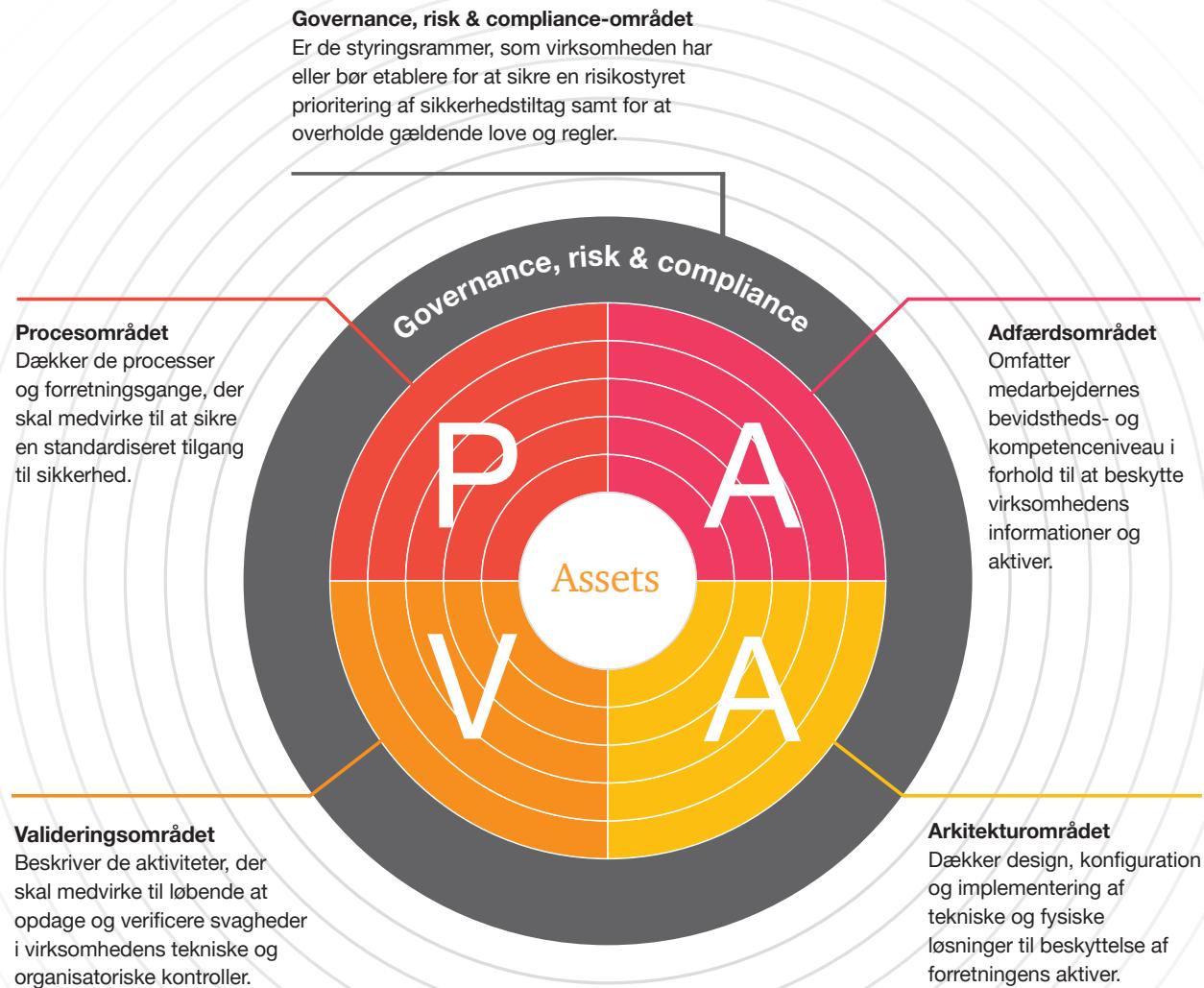


# PwC's sikkerhedskoncept PAVA

Kort fortalt er PAVA et koncept, der kan medvirke til at skabe en fælles forståelse mellem topledelsen og de fagfolk, der arbejder med sikkerhed. PAVA-konceptet er et generisk kommunikations-, vurderings- og rapporteringskoncept, som virksomheder bør bruge til bl.a. at vurdere og rapportere deres parathed og robusthed over for forskellige typer af cyberrisici og -trusler.

Konceptet kan anvendes på tværs af de mange forskellige sikkerhedsstandarder og frameworks og kan derfor rumme kompleksitet, samtidig med at der kan skabes klare fokusområder til sammenligning med andre virksomheder. På den måde giver PAVA et fælles grundlag for konkrete og prioriterede løsninger inden for specifikke sikkerhedsområder i virksomheden til brug i en bredere kontekst og til løbende effektmåling.

PAVA dækker over fem hovedområder – fra governance, risk & compliance til proces, adfærd, validering og arkitektur. Afhængig af den enkelte virksomheds modenheds- og sikkerhedsniveau er der behov for en indsats inden for alle områder, hvis man skal opnå en langsigtet og robust cyber- og informationssikkerhed. Denne struktur følger også de fleste virksomheders måde at fordele ansvar og roller for sikkerhedsarbejdet på, ligesom det er muligt at fokusere på enkelte områder efter behov uden at miste overblikket.



# Tjekliste

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



## Governance, risk & 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/lobende til virksomhedens direktion/bestyrelse?
- Omfatter arbejdet med sikkerhed både informationssikkerhed og cybersikkerhed? Læs mere om ISO27001 og NIS2 på [pwc.dk](#)
- 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 på [www.pwc.dk/cyberaware](#)

## 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 på [pwc.dk/response](#)
- Har I testet jeres beredskabsplaner for cyberhændelser? Læs mere på [pwc.dk/beredskab](#)

## 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 på [pwc.dk/iam](#) og [pwc.dk/pam](#)

## 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 på [www.pwc.dk/cfocyberguide](#)



# 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. Du kan også læse mere om vores ydelser inden for cyber- og informationssikkerhed på [www.pwc.dk/cyber](http://www.pwc.dk/cyber).



**Mads Nørgaard Madsen**  
Partner  
Leder af Technology & Security  
Technology & Security  
T: 2811 1592  
E: [mads.norgaard.madsen@pwc.com](mailto:mads.norgaard.madsen@pwc.com)



**Peter Brock Madsen**  
Partner  
Cyberrisikostyring  
Technology & Security  
T: 2056 8505  
E: [peter.brock.madsen@pwc.com](mailto:peter.brock.madsen@pwc.com)



**William Sharp**  
Partner  
Cyber Operationel Technology  
Technology & Security  
T: 4040 1074  
E: [william.sharp@pwc.com](mailto:william.sharp@pwc.com)



**Christian Kjær**  
Partner  
Cyberberedskab  
Technology & Security  
T: 5132 1270  
E: [christian.kjaer@pwc.com](mailto:christian.kjaer@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 ca. 2.600 medarbejdere og partnere, som brænder for at gøre en positiv forskel for kunder og kolleger. Vi arbejder med samfundsansvar med fokus på mennesker, mindset og miljø, hvor vi har en ambition om at være net zero senest i 2030. Globalt er vi 328.000 PwC'ere i 152 lande, og i Danmark er vi markedsledende. Mød os over hele landet. Vi er der, hvor du er.

**Succes skaber vi sammen ...**

Denne publikation udgør ikke og kan ikke erstatte professionel rådgivning. PricewaterhouseCoopers Statsautoriseret Revisionspartnerselskab påtager sig intet ansvar for tab, nogen måtte lide som følge af handlinger eller undladelser baseret på publikationens indhold, ligesom PricewaterhouseCoopers Statsautoriseret Revisionspartnerselskab ikke påtager sig ansvar for indholdsmæssige fejl og mangler.

© 2022 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.

## 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 cyber-forensics-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**

Du kan også læse mere på [www.pwc.dk/response](http://www.pwc.dk/response)



ISSN: 2597-193X

Revision. Skat. Rådgivning.



Succes skaber vi sammen ...