

Cybercrime Survey 2023

54 %

bekymrer sig mere for cybertruslen i dag end for 12 måneder siden

67 %

forventer, at virksomhedens cyber- og informationssikkerhedsbudget vil vokse inden for de næste 12 måneder

49 %

af dem, der de seneste 12 måneder har forsøgt at rekruttere medarbejdere inden for cybersikkerhed, har haft udfordringer med dette

31 %

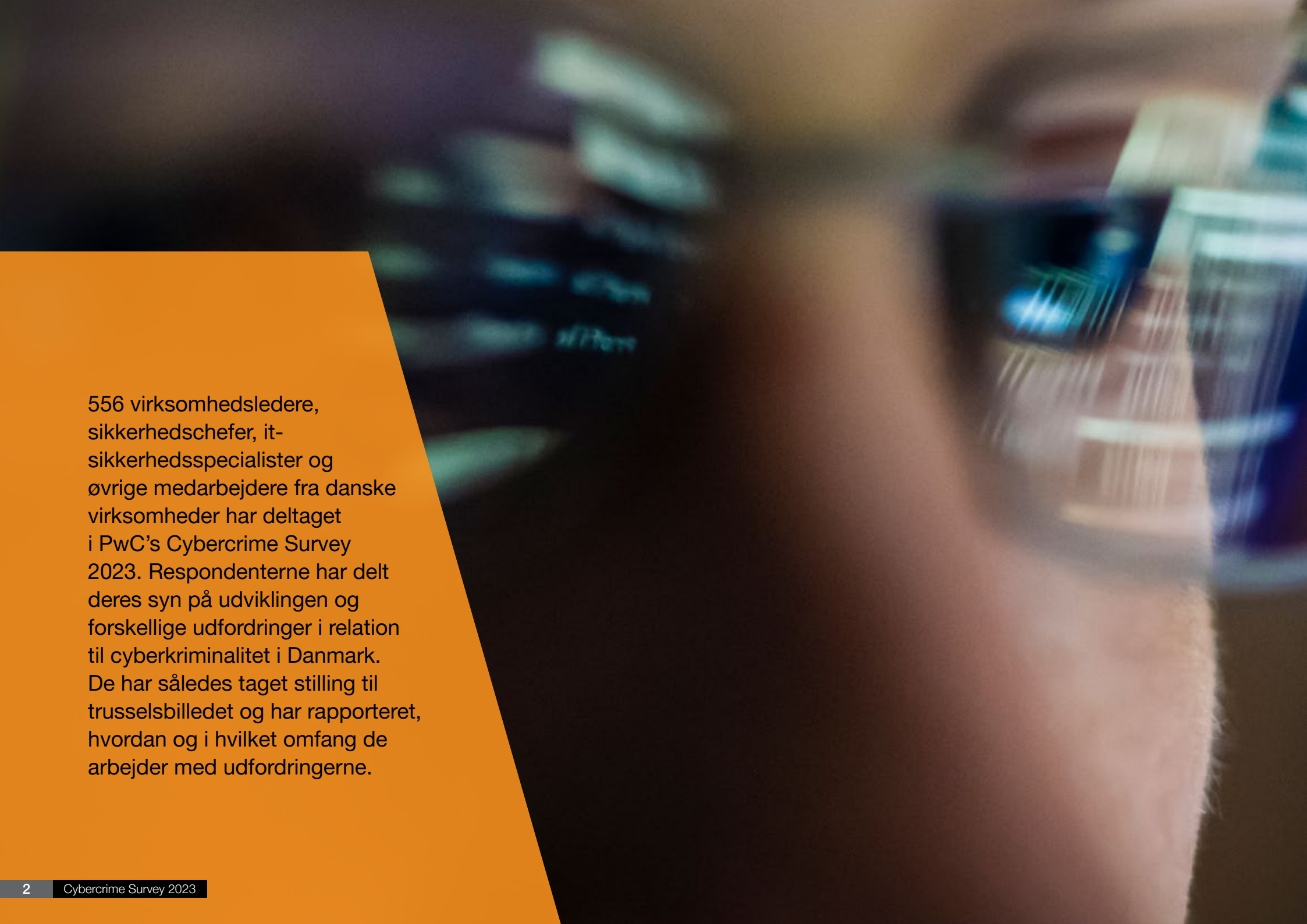
af de større virksomheder har planer om at anvende AI i arbejdet med cybersikkerhed i fremtiden



pwc

Revision. Skat. Rådgivning.

Succes skaber vi sammen ...



556 virksomhedsledere, sikkerhedschefer, it-sikkerhedsspecialister og øvrige medarbejdere fra danske virksomheder har deltaget i PwC's Cybercrime Survey 2023. Respondenterne har delt deres syn på udviklingen og forskellige 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.

Indhold

Leder: Nye udfordringer kræver nyt fokus i arbejdet med cybersikkerhed	4
Mere end hver anden større virksomhed har været ramt af sikkerhedshændelser	5
Phishing toppe listen over oplevede hændelser	8
Virksomhederne bekymrer sig mere for cyberkriminalitet i dag end for 12 måneder siden	10
CXO'erne er især bekymrede for nedbrud på kritiske systemer	12
De ansattes ubevidste handlinger udgør den største trussel	14
Virksomhederne prioriterer især awareness-træning	16
Tu af tre virksomheder forventer at øge investeringerne i cybersikkerhed	17
Flere virksomheder prioriterer AI i arbejdet med cybersikkerhed	19
Ny lovgivning inden for cybersikkerhed kræver fokus hos virksomhederne	22
Knap hver anden virksomhed har svært ved at rekruttere medarbejdere inden for cybersikkerhed	30
Bestyrelsens fokus på cyberkriminalitet stiger, men der er stadig plads til forbedringer	32
Om undersøgelsen	35
Tjekliste	36
Kontakt	38
Cyber Incident Response-team	40



Flere sætter ind over for cybertruslen i de kommende 12 måneder.

Christian Kjær
Partner

Nye udfordringer kræver nyt fokus i arbejdet med cybersikkerhed

Knap syv ud af ti danske virksomheder skruer op for budgettet inden for cyber- og informationssikkerhed over de kommende 12 måneder og ruster sig dermed mod det aktuelt høje trusselsniveau fra cyberkriminalitet.

Flere sætter ind over for cybertruslen

Cybersikkerhed har høj prioritet i danske private og offentlige virksomheder, og stadig flere sætter ind over for cybertruslen. Over de kommende 12 måneder forventer 67 % af virksomhederne således at øge budgettet til cyber- og informationssikkerhed, hvoraf godt halvdelen vil øge budgettet med mere end 10 %. De lovgivnings- og sikkerhedsmæssige forandringer stiller nye krav til virksomhedernes kapabiliteter og kompetencer. Cybercrime Survey 2023, der for niende år i træk har taget temperaturen på arbejdet med cybersikkerhed i Danmark, viser imidlertid, at det for knap hver anden rekrutterende virksomhed er svært at ansætte de rette medarbejdere.

Phishingangreb topper listen

Det fortsat voksende fokus på cybersikkerhed skal ses i lyset af det aktuelle trusselsniveau. Center for Cybersikkerhed har i maj 2023 vurderet, at truslen mod danske virksomheder og myndigheder fra cyberkriminalitet er meget høj, og Cybercrime Survey 2023 bekræfter, at antallet af hændelser i dansk erhvervsliv fortsat er på et relativt højt niveau. Mere end hver anden større virksomhed fortæller således, at de inden for det seneste regnskabsår har været ramt af mindst én sikkerhedshændelse, der har påvirket virksomheden negativt. Der ses en stor variation i hændelsestyperne, men phishingangreb topper listen over hyppigst oplevede hændelser i virksomhederne.

Der er fra virksomhedernes side øget opmærksomhed på mulige indgange for cyberkriminelle, og 67 % peger i år på "ansattes ubevidste handlinger" som en trussel mod virksomheden (mod 59 % i 2022). Det er derfor positivt, at 51 % af virksomhederne har awareness-træning som højest prioriterede investering i relation til cybersikkerhed de kommende 12 måneder.

Bekymring for nedbrud på kritiske systemer

Den geopolitiske situation påvirker virksomhedernes arbejde med cybersikkerhed. 54 % fortæller, at de i dag er mere bekymrede for cybertrusler end for kun 12 måneder siden, mens blot 2 % er mindre bekymrede. For tre ud af fire vedkommende er den øgede bekymring i nogen eller høj grad relateret til Ruslands konflikt med Vesten. Samtidig ser vi, at ledelsens fokus er på at beskytte virksomhedens kritiske systemer. 83 % af CXO'erne fortæller således, at længerevarende nedbrud på kritiske systemer udgør den største bekymring i forhold til cyberangreb.

Skærpede krav til cybersikkerhed

I oktober 2024 træder EU's NIS 2-direktiv i kraft. Direktivet udvider kravene og sanktioneringen i forhold til cybersikkerhed. De skærpede krav for flere sektorer betyder, at mange organisationer skal forholde sig mere indgående til risikostyring, beredskab, leverandørstyring og ledelses-

ansvar. Det kræver nyt fokus, og ca. halvdelen af de omfattede virksomheder fortæller i Cybercrime Survey 2023, at de er i gang med at implementere/imødekomme de nye krav. En del oplever dog udfordringer med at implementere en effektiv risikostyringsproces, og flere end hver tredje er ikke fuldt ud bekendt med omfanget af direktivet. Dette gør sig også gældende for DORA-forordningen, som er rettet mod den finansielle sektor og træder i kraft i januar 2025. Af dem, der er omfattet af direktivet, fortæller 46 %, at de mangler overblik over DORAs omfang.

Der ligger således stadig et større arbejde forude for mange virksomheder, der skal tilpasse sig de stigende krav til cybersikkerhed.



Christian Kjær
Partner
Cyber & Privacy

Mere end hver anden større virksomhed har været ramt af sikkerhedshændelser

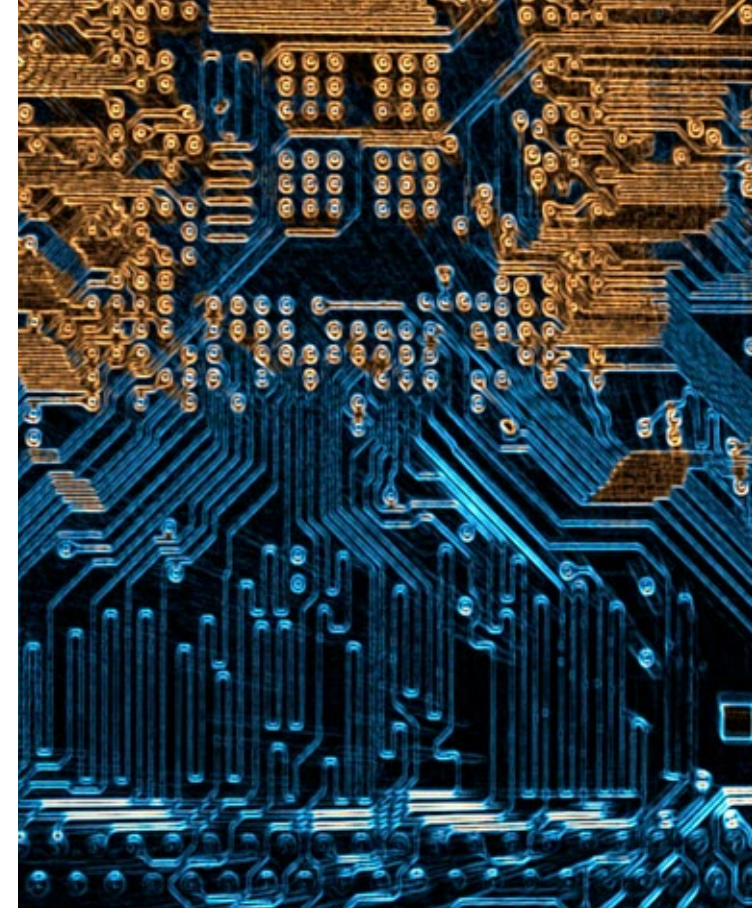
Cybercrime Survey har igen i år bedt dansk erhvervsliv om at vurdere hændelsesniveauet i deres organisation. Knap 45 % fortæller, at deres organisation har oplevet mindst én sikkerhedshændelse i løbet af de seneste 12 måneder. Niveauet er fortsat højt, men er i år lidt lavere end i 2022 (51 %).

Det er særligt større virksomheder med mindst 200 ansatte, der har været udsat for hændelser. Blandt de større virksomheder fortæller 54 % således, at deres virksomhed har været ramt af mindst én sikkerhedshændelse i løbet af de seneste 12 måneder, mens det gælder 35 % af virksomhederne med færre end 200 ansatte.

31 % fortæller endvidere, at de har været udsat for hændelser, som var målrettet deres virksomhed, hvilket er på niveau med 2022 (28 %). Af dem, der har oplevet en hændelse målrettet deres virksomhed, siger omtrent hver tredje, at hændelsen var relateret til virksomhedens eget udstyr lokalt. 48 % angiver, at hændelsen var relateret til deres eksterne leverandører, hvor 27 % var mod cloud-løsningen, og 21 % var mod it-servicen.

Det er væsentligt at understrege, at der sandsynligvis er flere sikkerhedshændelser, end undersøgelsen viser. En tredjedel angiver, at de ikke kan fastslå, om de har været udsat for hændelser, der var målrettet netop deres virksomhed. Det skyldes, at en del sikkerhedshændelser ikke nødvendigvis bliver opdaget, og andre kan være svære at fastslå som egentlige hackerangreb.

¹ En sikkerhedshændelse defineres som en hændelse, der negativt påvirker eller vurderes at ville kunne påvirke forretningens datatilgængelighed, integritet eller fortrolighed, informationssystemer, digitale netværk eller digitale tjenester.

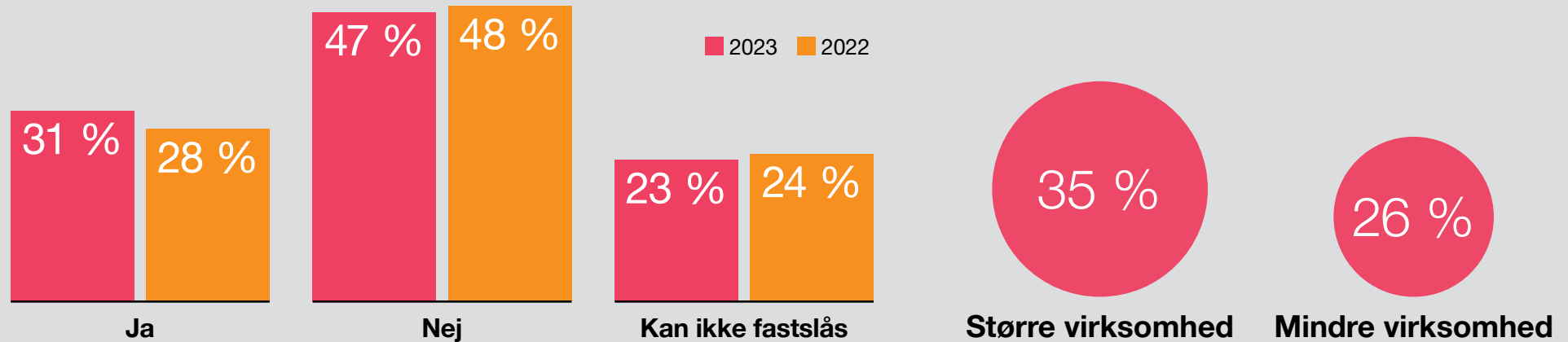


45 %

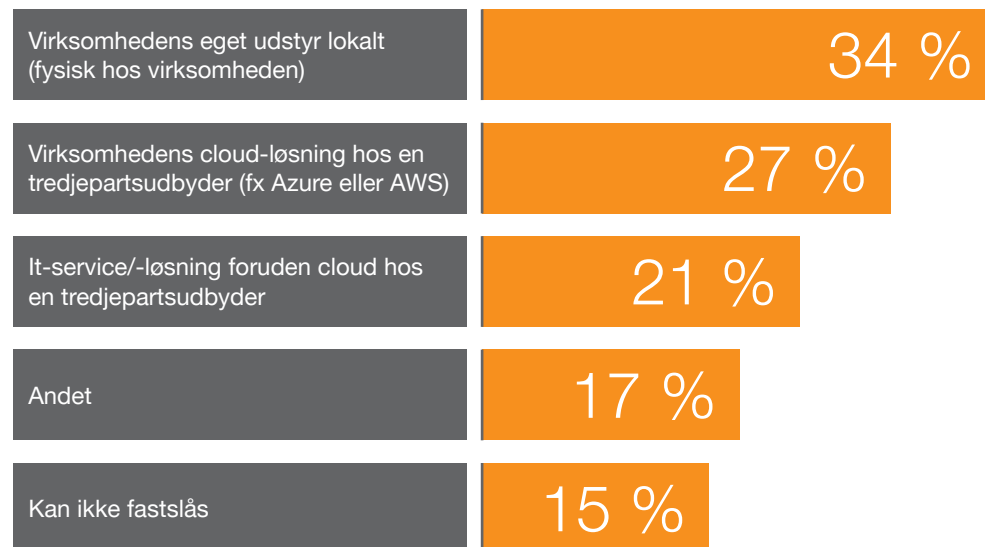
fortæller, at deres virksomhed har været udsat for mindst én sikkerhedshændelse i løbet af de seneste 12 måneder

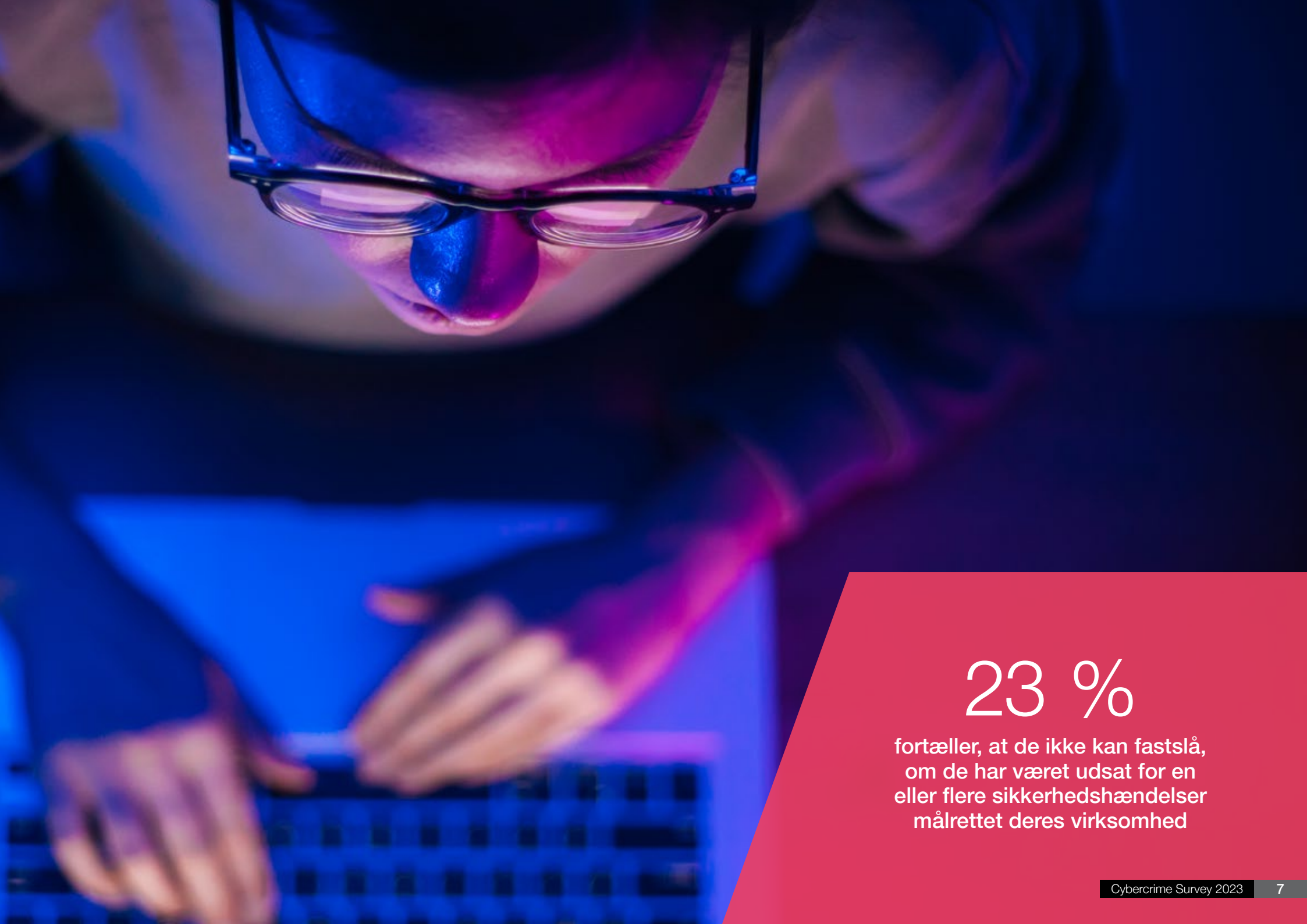


Spørgsmål: Har din virksomhed oplevet en eller flere sikkerhedshændelser, der var målrettet din virksomhed?



Spørgsmål: Hvad var hændelserne relateret til?





23 %

fortæller, at de ikke kan fastslå,
om de har været udsat for en
eller flere sikkerhedshændelser
målrettet deres virksomhed

Phishing topper listen over oplevede hændelser

Phishingangreb står øverst på listen over de typer af sikkerhedshændelser, virksomhederne udsættes for. Det hænger sammen med, at phishing er nemmere at udføre for cyberkriminelle sammenlignet med andre angrebstyper. Phishing stiller fx ikke nødvendigvis store krav til de cyberkriminelles kompetencer eller ressourcer.

Årets Cybercrime Survey fortæller, at størstedelen af de virksomheder, der har været ramt af en sikkerhedshændelse i løbet af de seneste 12 måneder, har oplevet et phishingangreb (72 %). 38 % har oplevet malware (mod 32 % i 2022), som derfor rangerer nummer to på årets liste over hyppigste typer af hændelser.. Samtidig går utilsigtet deling af følsomme oplysninger samt hændelser relateret til leverandørfejl tilbage og rykker dermed ud af dette års top tre over de hyppigste typer af hændelser, sammenlignet med sidste år.

Phishing er en af de mest brugte angrebsformer blandt cyberkriminelle. Ved et phishingangreb forsøger hackere at lokke medarbejdere til at foretage en handling, der øger sandsynligheden for succes for den cyberkriminelle. Det kan være at klikke på et link til en hjemmeside eller åbne en fil, som til forveksling ligner en tjeneste, medarbejderen kender på forhånd. Når først en medarbejder interagerer med linket eller filen, kan det resultere i, at de cyberkriminelle får adgang til fortrolige oplysninger, eller at der bliver åbnet en digital bagdør ind til virksomheden.

Phishing foregår primært gennem e-mails, men kan også forekomme via beskeder på sociale medier. Man skal derfor altid være opmærksom, uanset hvad, før man klikker på noget eller indtaster personlige eller fortrolige oplysninger.

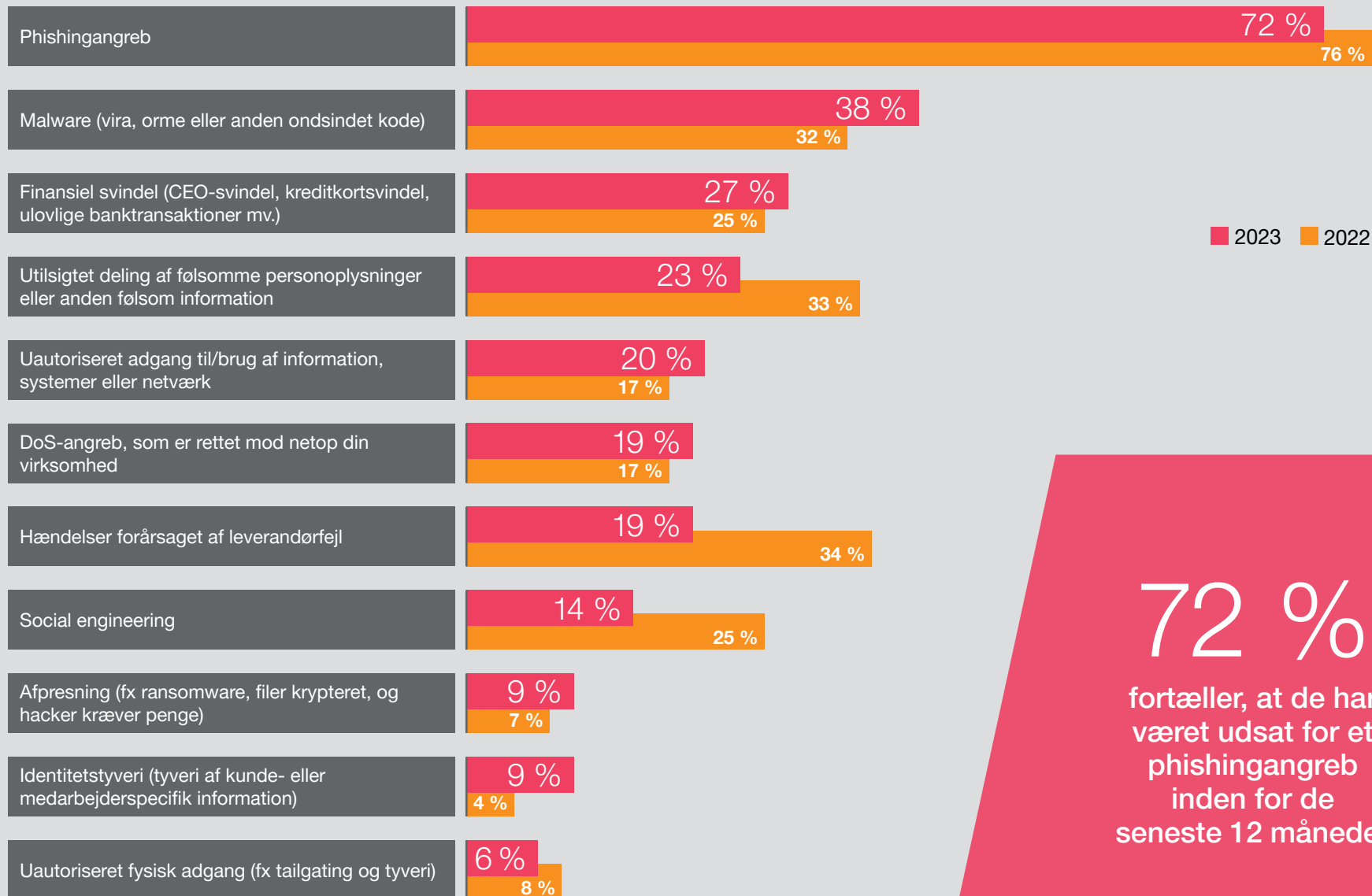
PwC erfarer

Phishing kan få alvorlige konsekvenser for de ramte virksomheder, og angrebene sker hyppigere og hyppigere og bliver mere og mere avancerede. Den bedste metode til at håndtere phishing og minimere eventuelle risici er gennem awareness-træning af virksomhedens medarbejdere. Træningen bør bestå af flere elementer, som samlet set øger modstandsdygtigheden i forhold til denne type angreb. E-learning eller phishingsimulationer og -kampagner kan medvirke til at træne medarbejderne i at spotte mistænksomme e-mails eller henvendelser samt forstå konsekvenserne af eventuelle phishingangreb.

Samtidig bør virksomhederne fokusere på de tekniske kontroller, der kan reducere konsekvensen ved et angreb. Dette gælder bl.a. en styrket beskyttelse af de enkelte enheder (endpoint protection) såvel som en højere grad af netværkssegmentering, der kan modvirke, at et angreb spreder sig fra én enhed til hele virksomheden.



Spørgsmål: Hvilke hændelser har din virksomhed oplevet inden for i de seneste 12 måneder som resultat af cyberkriminalitet eller informationssikkerhedshændelser?



■ 2023 ■ 2022

72 %
fortæller, at de har været udsat for et phishingangreb inden for de seneste 12 måneder

Virksomhederne bekymrer sig mere for cyberkriminalitet i dag end for 12 måneder siden

Vi befinder os fortsat i en usikker tid med uro og store globale udfordringer. Det smitter igen i år af på trusselsbilledet.

Der er generelt tiltagende bekymring for cyberkriminalitet i de danske virksomheder. På tværs af sektorer og roller er 54 % således mere bekymrede for cyberkriminalitet i dag end for 12 måneder siden. Kun 2 % er mindre bekymrede, mens de resterende 44 % har samme bekymringsniveau som for et år siden. Den geopolitiske situation er med til at hæve bekymringsniveauet i dansk erhvervsliv, og for flere end tre ud af fire er den øgede bekymring i nogen eller høj grad relateret til konflikten mellem Rusland og Vesten.

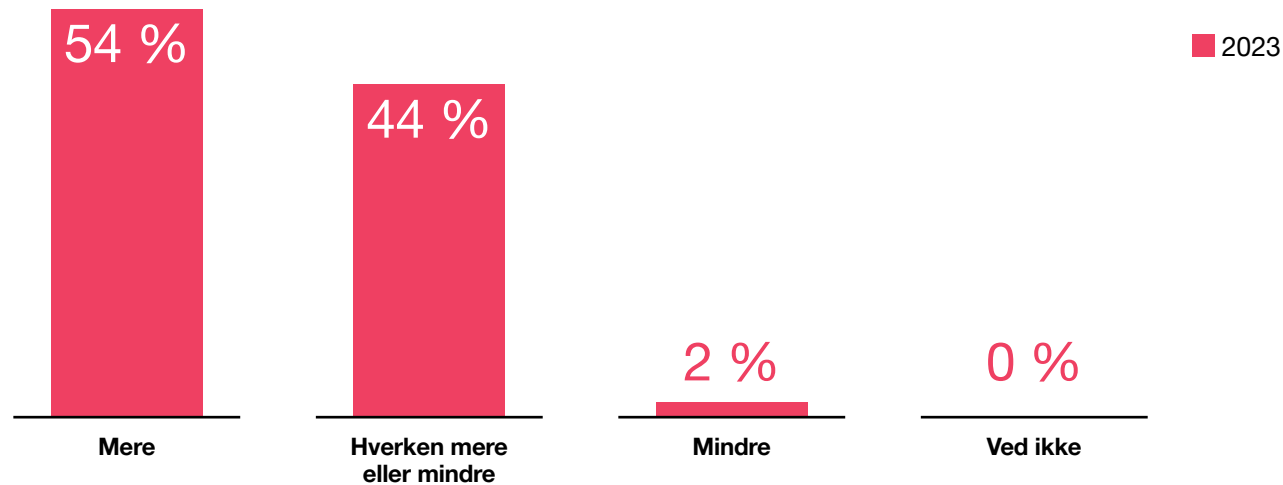
3 ud af 4

fortæller, at deres øgede bekymring for cyberkriminalitet i nogen eller høj grad er relateret til konflikten mellem Rusland og Vesten

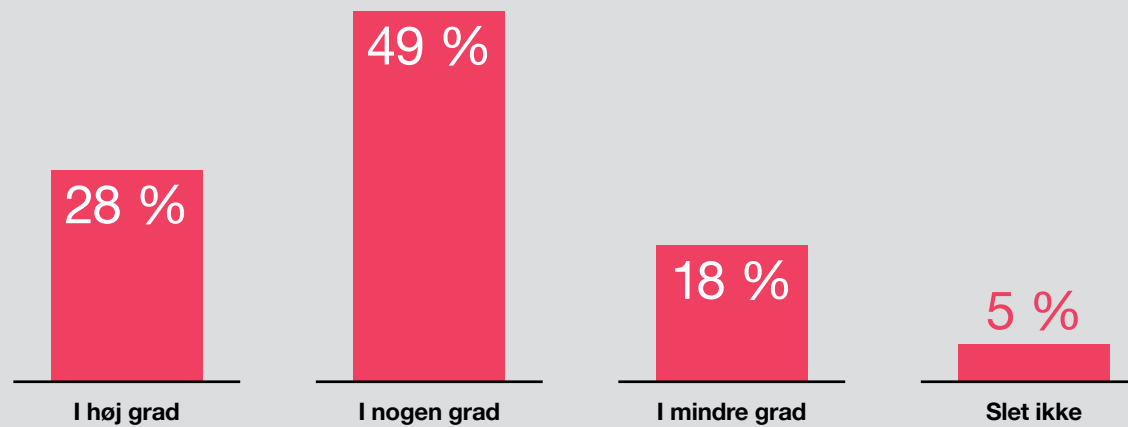




Spørgsmål: Bekymrer du dig i dag mere eller mindre om de cybertrusler, din virksomhed oplever, end du gjorde for 12 måneder siden?



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

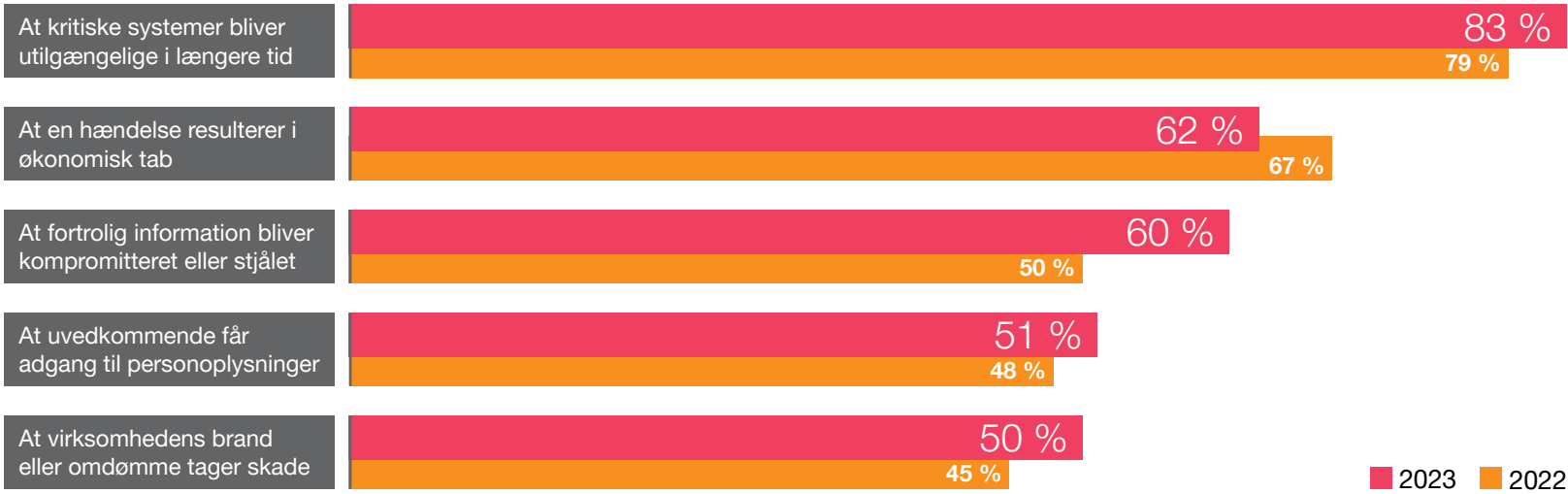


CXO'erne er især bekymrede for nedbrud på kritiske systemer

83 % af CXO'erne fortæller, at en af deres største bekymringer i forhold til konsekvenserne af en cyberhændelse er, at kritiske systemer bliver utilgængelige i længere tid. Det er lidt flere end i 2022 (79 %). Ligeledes er der en stigende bekymring for, at fortrolig information bliver stjålet eller kompromitteret. I årets survey er andelen på 60 % mod 50 % i 2022. Det skal ses i lyset af, at phishingangreb igen i år topper listen over oplevede sikkerhedshændelser, og at stjålne informationer kan have alvorlige konsekvenser for både enkeltpersoner og virksomheder. CXO'ernes bekymringer for økonomisk tab er faldet en smule siden sidste år.

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

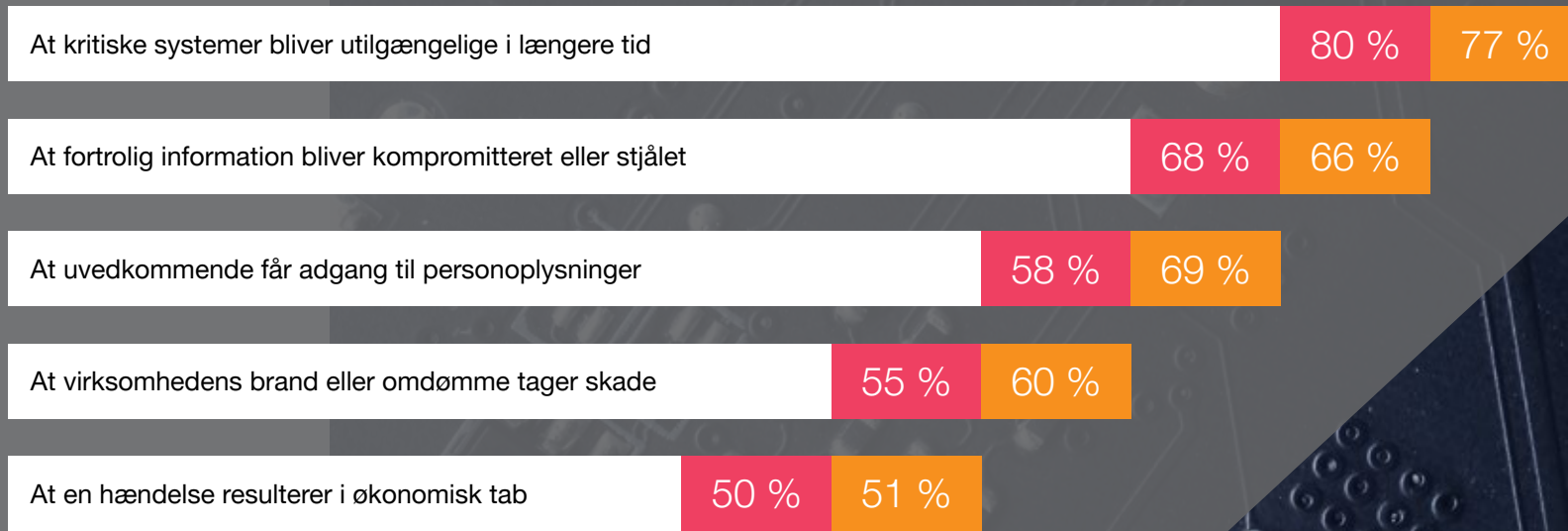
CXO'ernes Top 5



■ 2023 ■ 2022

CISO'ernes og it-sikkerhedsspecialisternes

Top 5



■ 2023 ■ 2022

De ansattes ubevidste handlinger udgør den største trussel

Medarbejderne udgør i stigende grad en sikkerhedsrisiko, vurderer virksomhederne i Cybercrime Survey 2023. Således peger 67 % (mod 59 % i 2022) på, at de ansattes ubevidste handlinger ses som den største trussel mod virksomhedens cyber- og informationssikkerhed. I den offentlige sektor ser hele 72 % medarbejdernes ubevidste handlinger som den største trussel. Truslen skal ses i lyset af det fortsat høje

antal phishingangreb, idet succesene ved denne type angreb bl.a. afhænger af ansattes ubevidste handlinger.

Organiserede kriminelle ligger fortsat højt på virksomhedernes liste over de største trusler inden for cyber- og it-sikkerhed, dog i mindre grad end sidste år (65 % i 2023 mod 74 % i 2022).



Top 3 Trusler fordelt på sektor

Privat sektor



Ansattes ubevidste handlinger	67 %
Organiserede kriminelle	66 %
Hacktivist	44 %

Finansiel sektor



Organiserede kriminelle	79 %
Ansattes ubevidste handlinger	64 %
Hacktivist	47 %

Offentlig sektor

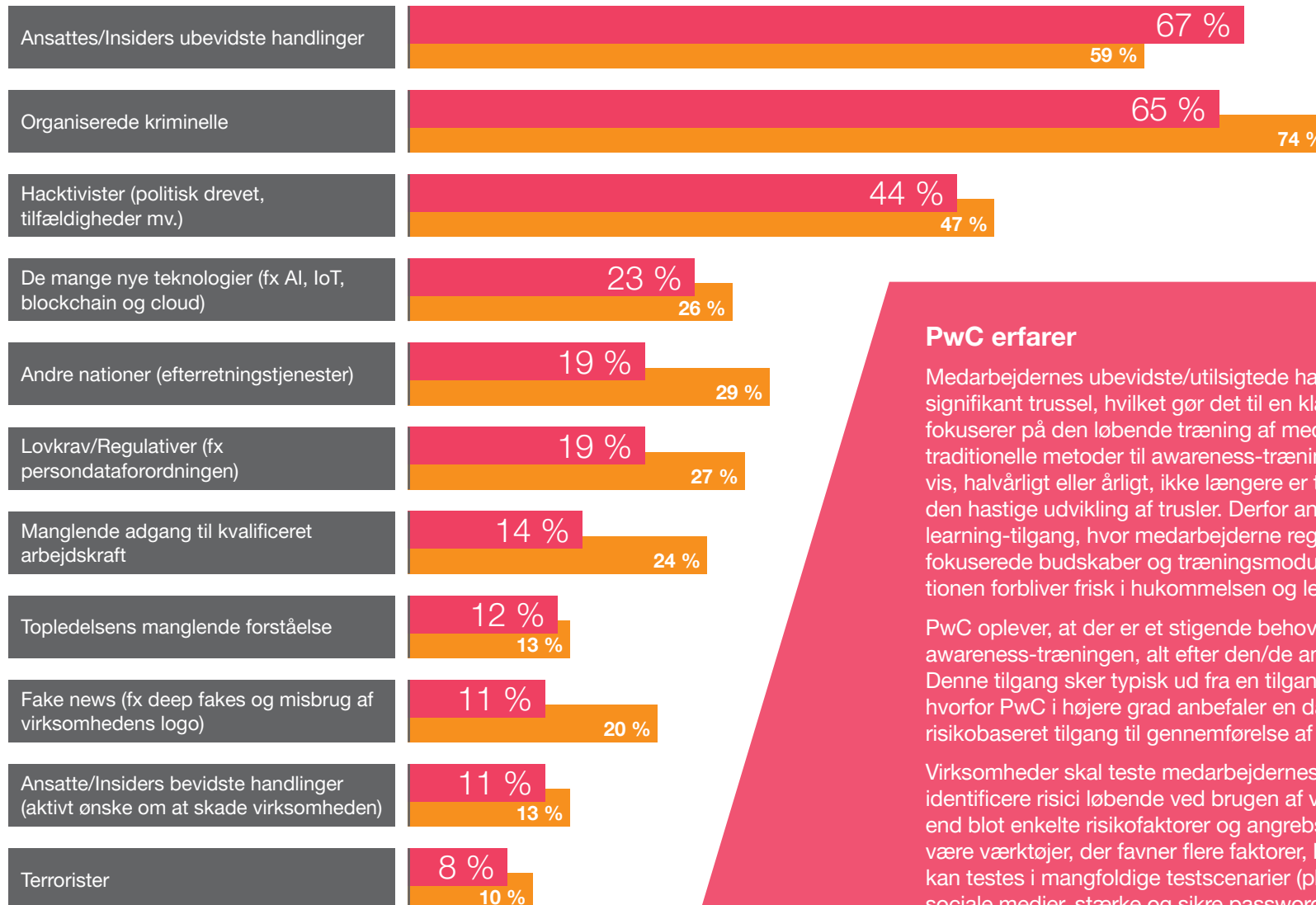


Ansattes ubevidste handlinger	72 %
Organiserede kriminelle	42 %
Hacktivist	38 %



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

2023 2022



PwC erfarer

Medarbejdernes ubevidste/utillsigtede handlinger repræsenterer en signifikant trussel, hvilket gør det til en klar topprioritet, at virksomheder fokuserer på den løbende træning af medarbejderne. PwC erfarer, at traditionelle metoder til awareness-træning, som typisk udføres kvartalsvis, halvårligt eller årligt, ikke længere er tilstrækkelige til at imødegå den hastige udvikling af trusler. Derfor anbefaler PwC en micro-/nano-learning-tilgang, hvor medarbejderne regelmæssigt modtager korte, fokuserede budskaber og træningsmoduler. Dette skal sikre, at informationen forbliver frisk i hukommelsen og lettere kan anvendes i praksis.

PwC oplever, at der er et stigende behov for at kunne differentiere awareness-træningen, alt efter den/de ansattes funktion og behov. Denne tilgang sker typisk ud fra en tilgang, der ikke er evidensbaseret, hvorfor PwC i højere grad anbefaler en datadrevet udvælgelse og reel risikobaseret tilgang til gennemførelse af træningen.

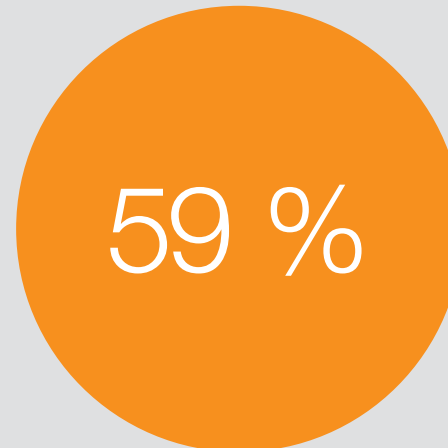
Virksomheder skal teste medarbejdernes viden om og evner til at kunne identificere risici løbende ved brugen af værktøjer, som rummer mere end blot enkelte risikofaktorer og angrebsformer. Dette skal således være værktøjer, der favner flere faktorer, hvor medarbejderne løbende kan testes i mangfoldige testscenarier (phishing, tailgating, adfærd på sociale medier, stærke og sikre passwords mv.).

Virksomhederne prioriterer især awareness-træning

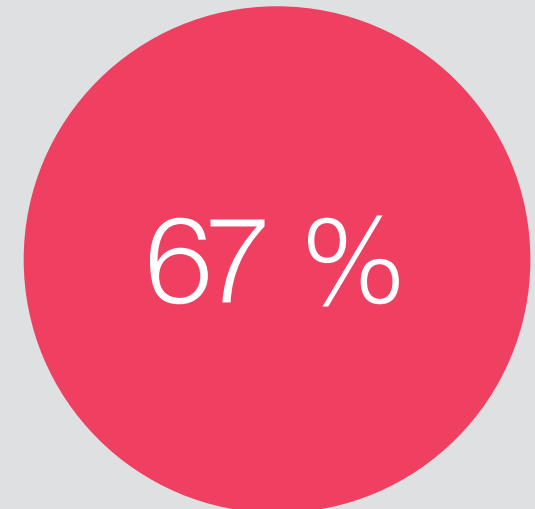
Der er fokus på at skærpe medarbejdernes forståelse og håndtering af cybersikkerhedsrisici. Således er awareness-træning den højest prioriterede investering hos 51 % af virksomhederne, og aktiviteten er prioriteret i både større (53 %) og mindre virksomheder (48 %). Segmentering af netværk er særligt på listen i de større virksomheder, hvor 41 % har denne investering som en høj prioritet, mens den blot er en prioritet hos 17 % af de mindre virksomheder.

12 % har desuden AI som en prioriteret investering på sikkerhedsområdet de næste 12 måneder, som er mere end en fordobling sammenlignet med 2022 (5 %).

Andel, der forventer, at virksomhedens cyber- og informationssikkerhedsbudget vil vokse inden for de næste 12 måneder



2022

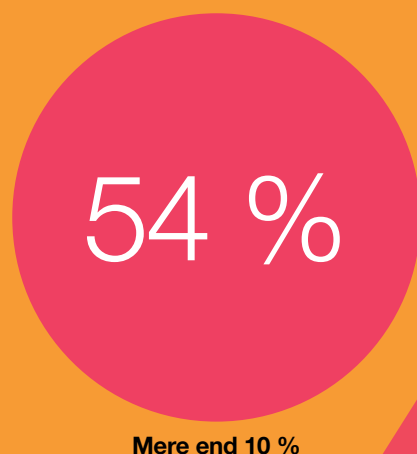


2023

En af de mest omkostningseffektive måder at styrke it-sikkerheden på er at investere i awareness-træning. Awareness-træning er en træningsform, som lærer medarbejdere at identificere og spotte tegn på cyberangreb eller -hændelser, hvilket kan spare virksomheden for store tab af tid, penge og data. Awareness-træning er ikke kun en engangsaktivitet, men en løbende proces, som kræver opfølgning og opdatering. Det er vigtigt at holde sig ajour med de nyeste trusler og tendenser.

51 %
af virksomhederne fortæller, at awareness-træning er deres højest prioriterede investering de næste 12 måneder

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



To ud af tre virksomheder forventer at øge investeringerne i cybersikkerhed

Stadig flere virksomheder forventer at øge investeringerne i cyber- og informationssikkerhed, og årets **Cybercrime Survey** tydeliggør, at cybersikkerhed fortsat er i hastig udvikling og står højt på virksomhedernes liste over prioriteringer.

Ovenstående hænger sammen med, at 54 % er mere bekymrede for cyberkriminalitet, og at næsten halvdelen oplever sikkerhedshændelser rettet mod virksomheden. Således svarer 67 % af virksomhederne, at de forventer, at virksomhedens cybersikkerhedsbudget vil vokse i de kommende 12 måneder. Det er en stigning i forhold til 2022, hvor tallet lå på 59 %. I virksomheder med mindst 200 ansatte forventer 74 % at øge investeringerne, hvilket er en stigning fra 64 % i 2022.

23 % af virksomhederne angiver derudover at udskiftning af gammel teknologi er deres højst prioriterede investering inden for it-sikkerhed de næste 12 måneder. Ældre it-systemer kan have store udfordringer i virksomheders it-landskaber, og kan være dyre i drift og svære at integrere med.

PwC erfarer

Cybersikkerhed er ikke længere blot "et ben" i it-afdelingen. Det er et indsatsområde, der kræver forretningsmæssig investering, forankring og fokus, og som bliver en stadigt mere central og nødvendig del af virksomheders daglige processer og forretningsgange. Effektiv cybersikkerhed og -strategier er med til at øge den sikkerhed, der skal understøtte den digitale udvikling for både virksomheder, brugere og samfundet generelt.

Mange virksomheder oplever at "sidde fast" i situationer, der er sikkerhedsmæssigt og teknisk uholdbar grundet forældede legacy it-systemer.² For at imødegå dette er der behov for at forbedre og påbegynde en modernisering og eventuelt en udskiftning af systemerne. Det indebærer bl.a. en proces, hvor virksomhederne skal tage stilling til, hvad der skal ske med de gamle it-systemer.

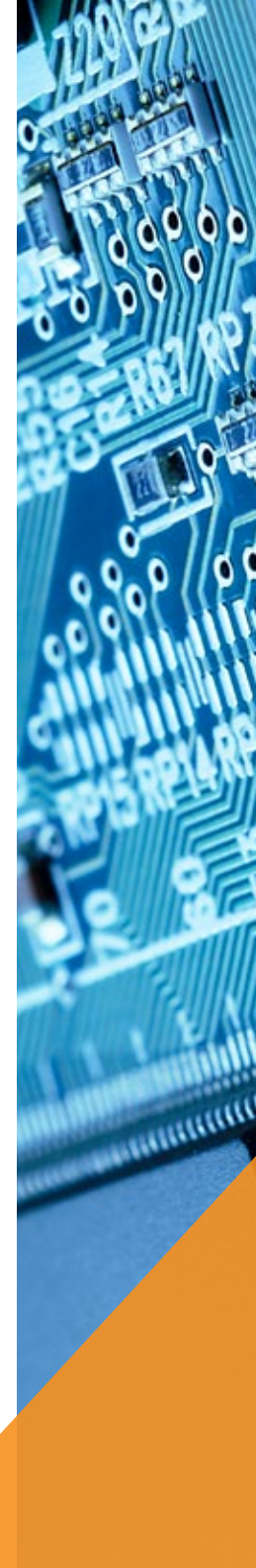
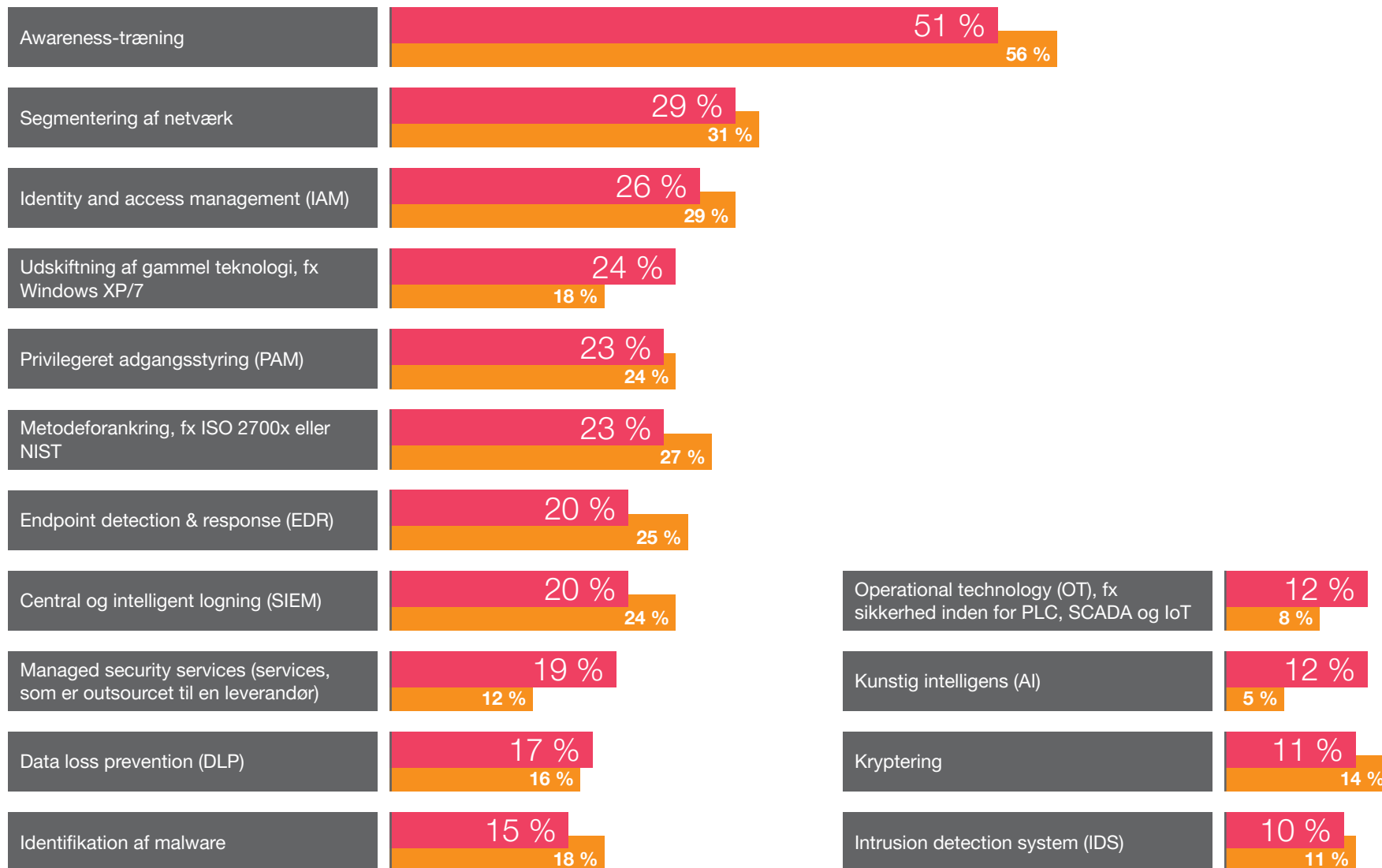
Læs mere om, hvordan PwC kan hjælpe virksomheder med udskiftning af forældede legacy it-systemer [her](#).

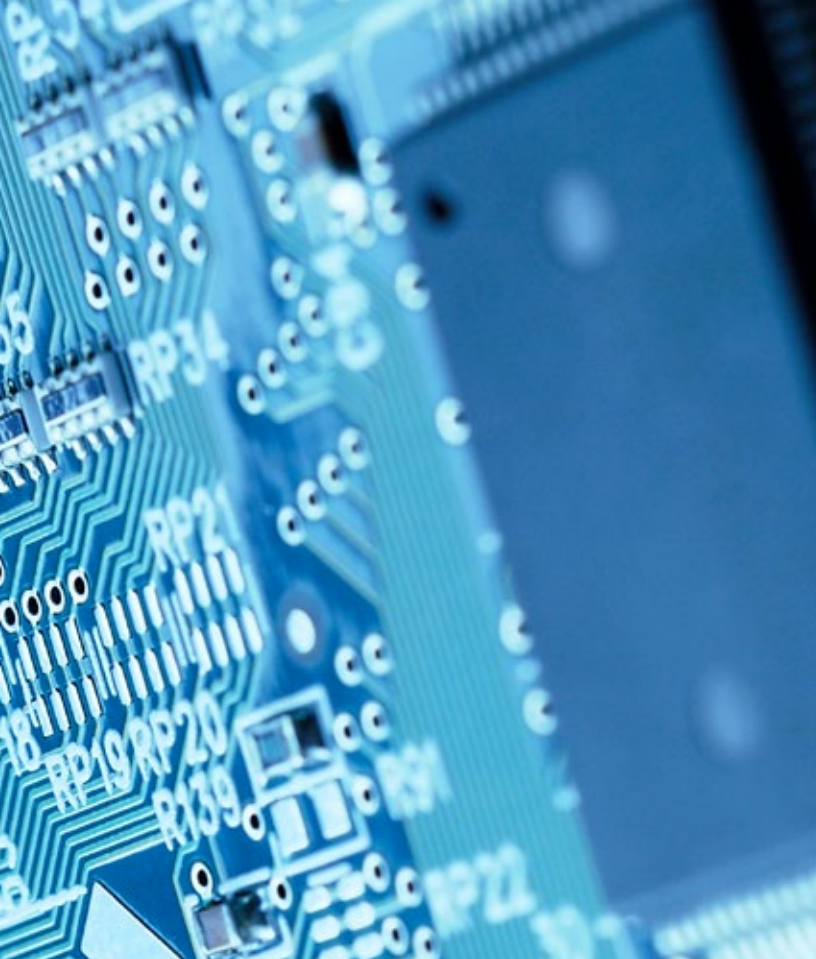
² Legacy it-systemer er ældre it-systemer baseret på gammel it-arkitektur og/eller teknologi.



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

2023 2022





Flere virksomheder prioriterer AI i arbejdet med cybersikkerhed

Udviklingen inden for AI åbner nye muligheder i arbejdet med cyber- og informationssikkerhed. Det optager især de større virksomheder.

23 % af de større virksomheder fortæller, at de i dag anvender AI i arbejdet med cybersikkerhed, og yderligere 31 % har planer om at anvende AI i fremtiden. I de mindre virksomheder svarer færre end hver tiende, at AI i dag indgår i virksomhedens arbejde med cybersikkerhed. Vi ser ligeledes en forskel, når det kommer til de højst prioriterede investeringer i de kommende 12 måneder i relation til cyber- og it-sikkerhed. AI er på listen hos 18 %

af de større virksomheder, mens det blot er tilfældet for 8 % af de mindre virksomheder.

De virksomheder, der anvender eller vil anvende AI, ser særligt et potentiale i AI i forhold til at opdage og identificere mulige hændelser og trusler samt med henblik på at beskytte virksomhedens aktiver, fx ved automatisk at blokere angreb.

PwC erfarer

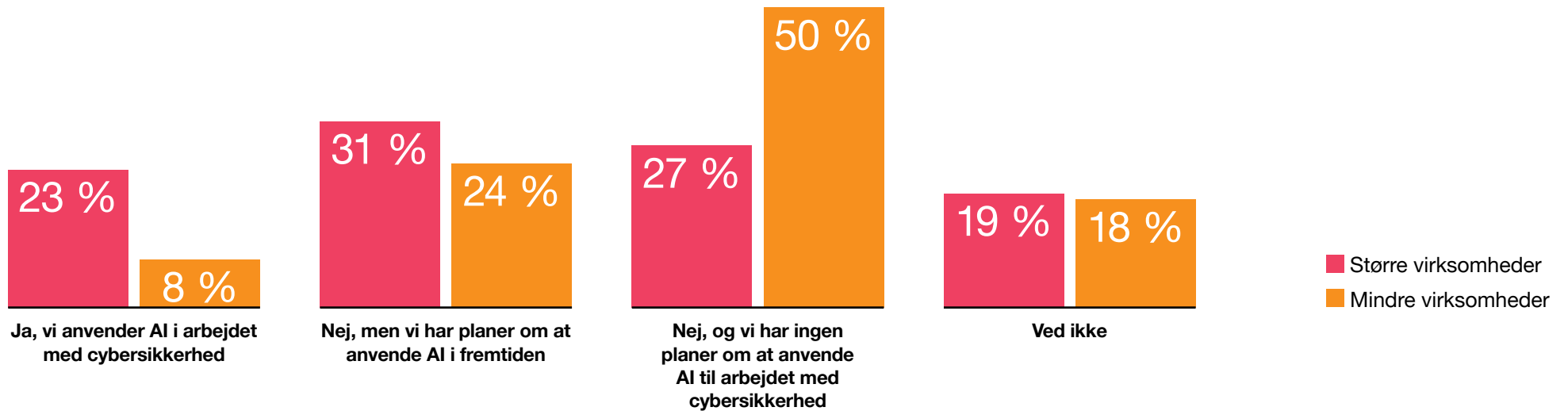
Kunstig intelligens (på engelsk: artificial intelligence, forkortet "AI") er en teknologi, som muliggør en højere grad af automatisering af opgaver, der normalt kræver menneskelig interaktion.

Når det gælder sikkerhedshændelser, kan AI ses som en stor trussel for virksomheder. Sammenlignet med en konventionel angriber, der anvender manuelle processer, standardværktøjer og egen ekspertviden, kan en "AI-støttet angriber" anvende AI til at automatisere opgaver samt forbedre og sammenkøre værktøjer. Dette kan føre til en højere succesrate for den cyberkriminelle ved fx at minimere eller kamuflere netværkstrafik, styrke og koordinere angreb eller identificere mulige mål for målrettede phishingangreb.

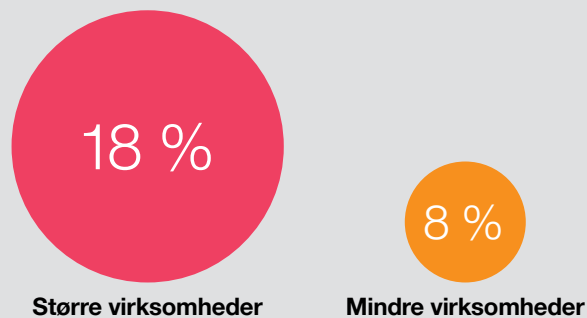
AI kan samtidig anvendes til den defensive del af cybersikkerhed i relation til virksomheder, fx til at identificere mulige trusler gennem avancerede phishingfiltre eller at overvåge slutbrugeres enheder for at registrere, hvis deres aktiviteter afviger fra normalen. Overordnet kan AI bruges til at effektivisere manuelle processer som scanninger og konfigurationer. PwC erfarer, at det er vigtigt, at virksomheder også fokuserer på begrænsningerne ved brugen af AI. I sidste ende bør det altid være en cybersikkerhedseksperter, der tager beslutningerne eller bedømmer, om resultaterne er påvirkede af falske positive mv.



Spørgsmål: Anvender din virksomhed AI i arbejdet med cybersikkerhed?

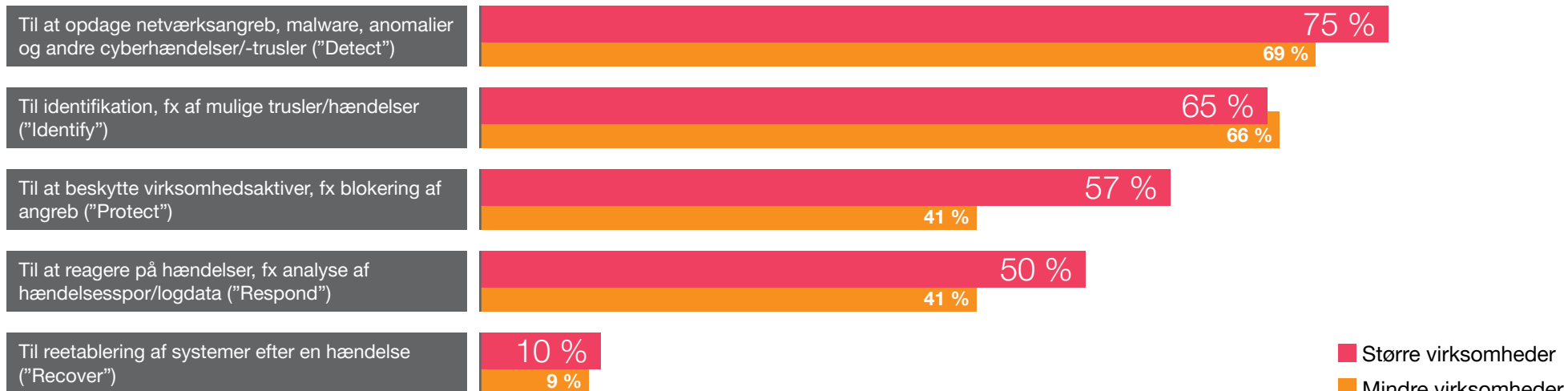


Spørgsmål: Andel af virksomheder, der har AI som en af de højst prioriterede investeringer de næste 12 måneder





Spørgsmål: Inden for hvilke områder anvender eller planlægger din virksomhed at anvende AI?



Ny lovgivning inden for cybersikkerhed kræver fokus hos virksomhederne

NIS 2-direktivet

Denne del af undersøgelsen indbefatter kun ikke-finansielle virksomheder, som er omfattet af direktivet.

Ifølge Cybercrime Survey er de danske virksomheder, der er omfattet af NIS 2-direktivet, generelt godt informerede om direktivets indhold. Af de virksomheder, der angiver, at de er omfattet af direktivet, er det 97 %, der enten er fuldt bekendt med direktivet eller har hørt om nogle af kravene deri. Der er dog næsten ingen af disse virksomheder, der er i mål med implementeringen af alle kravene. Næsten halvdelen (49 %) er i gang med processen, mens 36 % endnu ikke har planlagt implementeringen af kravene.

Virksomhederne angiver, at barriererne for implementeringen bl.a. er udfordringer med at implementere en effektiv risikostyringsproces og at sikre forsyningskædens sikkerhed.

Det er væsentligt at påpege, at 23 % af CXO'erne, CISO'erne og it-sikkerhedsspecialisterne ikke kan angive, hvorvidt de er omfattet af NIS 2. Det kan skyldes, at anvendelsesområdet for NIS 2 er udvidet betydeligt siden NIS, og at NIS 2 ikke vil være en bindende del af dansk lovgivning før oktober 2024. Ligeledes kan det potentielt være svært for virksomheder, der ikke tidligere var omfattet af NIS, at navigere i det nye direktiv.

For at sikre et højt fælles niveau af cybersikkerhed i EU har EU vedtaget et nyt cybersikkerhedsdirektiv, som erstatter NIS fra 2016. Det nye direktiv kaldes NIS 2 og er gældende i dansk lovgivning fra den 18. oktober 2024. NIS 2-direktivet omfatter net- og informationssystemer og stiller en række krav til både offentlige og private aktører, som leverer vigtige eller væsentlige tjenester inden for forskellige sektorer såsom energi, transport, sundhed, finans, digital infrastruktur, vandforsyning, affaldshåndtering og offentlig forvaltning.

NIS 2-direktivet har til formål at øge kravene til håndhævelse af reglerne og ensrette sanktionerne i hele EU. Det betyder, at de berørte aktører skal efterleve en række forpligtelser, som bliver udmøntet i nationale bekendtgørelser og fungerer som bindende lovgivning. Ydermere stiller NIS 2 krav til ledelse, risikostyring, forretningskontinuitet og kontrol samt tilsyn med de berørte aktører.

23 %

af CXO'erne, CISO'erne og it-sikkerhedsspecialisterne fortæller, at de ikke kan fastslå, om de er omfattet af NIS 2



PwC erfarer

Arbejdet med det oprindelige NIS-direktiv viste, at det var en både omfattende og tidskrævende opgave at implementere. Virksomhederne står efter PwC's vurdering over for et tilsvarende omfattende arbejde med implementeringen af det 150 sider lange NIS 2-direktiv, og det forberedende arbejde bør iværksættes i god tid. Men hvor starter man? Og hvordan får man kravene implementeret, så de rent faktisk efterleveres i praksis? I PwC har vi lavet en trin-for-trin-guide, som hjælper din organisation i gang med implementeringen af NIS 2-kravene.

Læs mere og hent guiden **her**.



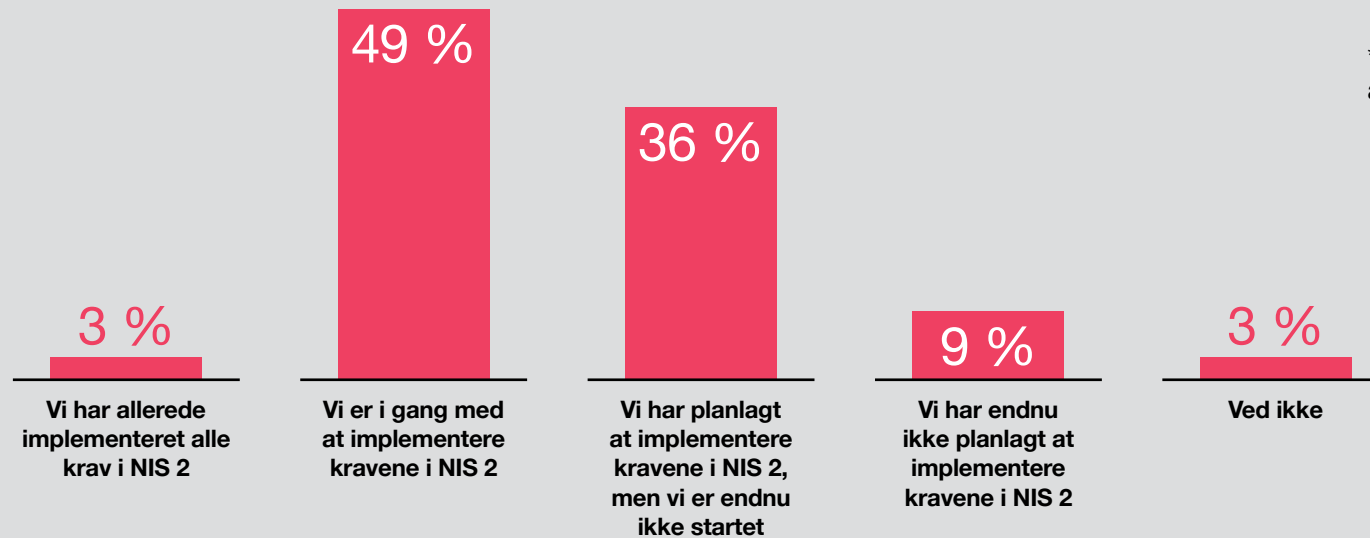
Spørgsmål: Er din virksomhed* bekendt med EU's NIS 2-direktiv og dets krav til beskyttelse mod cyberangreb og af kritisk infrastruktur?



*) Kun virksomheder, der har angivet, at de er omfattet af NIS 2



Spørgsmål: Hvor langt er I* med at implementere/imødekomme kravene i NIS 2?



*) Kun virksomheder, der har angivet, at de er omfattet af NIS 2



Hvilke af følgende ser du som barrierer for, at din virksomhed* kan leve op til kravene i NIS 2?

Top 5

Udfordringer med at implementere en effektiv risikostyringsproces

38 %

Udfordringer med at kunne sikre forsyningskædens sikkerhed

35 %

Udfordringer med at overvåge og rapportere om sikkerhedsbrud og -hændelser

22 %

Manglende ledelsesmæssig forståelse

22 %

Manglende teknologisk modenhed eller forældet infrastruktur

20 %

*) Kun virksomheder, der har angivet, at de er omfattet af NIS 2

DORA-forordningen

Denne del af undersøgelsen indbefatter kun de finansielle virksomheder, som er omfattet af forordningen.

De fleste virksomheder har et godt kendskab til DORA og de tilhørende krav. Ud af de virksomheder, der har angivet, at de er omfattet af DORA, er 44 % fuldt bekendt med den nye forordning, mens 54 % kun er bekendt med nogle af kravene. Kendskabet er dog ikke ensbetydende med handling. Ingen af virksomhederne er i mål med implementeringen, mens 39 % er i gang med processen. Næsten halvdelen (46 %) angiver, at de har planlagt at skulle implementere kravene, mens 10 % endnu ikke har planlagt implementeringen. Det kan således være svært for virksomhederne at påbegynde implementeringen, når de ikke er bekendt med alle kravene i forordningen.

Den mest udbredte grund til, at virksomhederne endnu ikke har implementeret eller har planlagt at implementere DORA, er det manglende overblik. Det gælder både overblikket over DORAs omfang og over tredjeparter samt outsourcingleverandører, herunder manglende risikovurderinger.

Hele 12 % af CXO'erne, CISO'erne og it-sikkerhedspécialisterne kan ikke fortælle, om deres virksomhed er omfattet af forordningen. Det kan skyldes, at der ligesom for andre finansielle reguleringer gælder et proportionalitetsprincip, hvorfor mindre finansielle aktører kan være usikre på, i hvilken grad de er omfattet.



DORA er en del af et nyt og bredere europæisk rammeværk rettet mod den finansielle sektor.

DORA træder i kraft den 17. januar 2025 og er en ny EU-forordning, der har til formål at styrke den finansielle sektors digitale operationelle modstandsdygtighed over for såvel cyber- som informations- og kommunikationsteknologi (IKT)-risici. DORA gælder for alle finansielle virksomheder og deres IKT-tjenesteudbydere, som leverer kritiske funktioner – fx cloud-tjenester, datacentre og softwareudvikling.

DORA indeholder en række forpligtelser for de berørte aktører og omfatter bl.a. ledelse, risikovurdering, test, rapportering og overvågning af deres digitale operationelle modstandsdygtighed. DORA giver også de nationale tilsynsmyndigheder beføjelser til at føre tilsyn med – og sanktionere – de berørte aktører i tilfælde af manglende overholdelse af reglerne. DORA bidrager således til at fremme et ensartet og højt niveau af cybersikkerhed i den finansielle sektor i hele EU.



Spørgsmål: Er din virksomhed* bekendt med EU's DORA-forordning og dens krav til beskyttelse mod cyberangreb og af kritisk infrastruktur?

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

Ja, vi er fuldt ud bekendt med forordningen og kravene deri

44 %

Vi har hørt om forordningen og kender nogle af kravene deri, men ikke alle

54 %

Vi har hørt om forordningen, men kender ikke til kravene deri

2 %



Spørgsmål: Hvor langt er I* med at implementere/imødekomme kravene i DORA?

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

0 %

Vi har allerede implementeret alle krav i DORA

39 %

Vi er i gang med at implementere kravene i DORA

46 %

Vi har planlagt at implementere kravene i DORA, men vi er endnu ikke startet

10 %

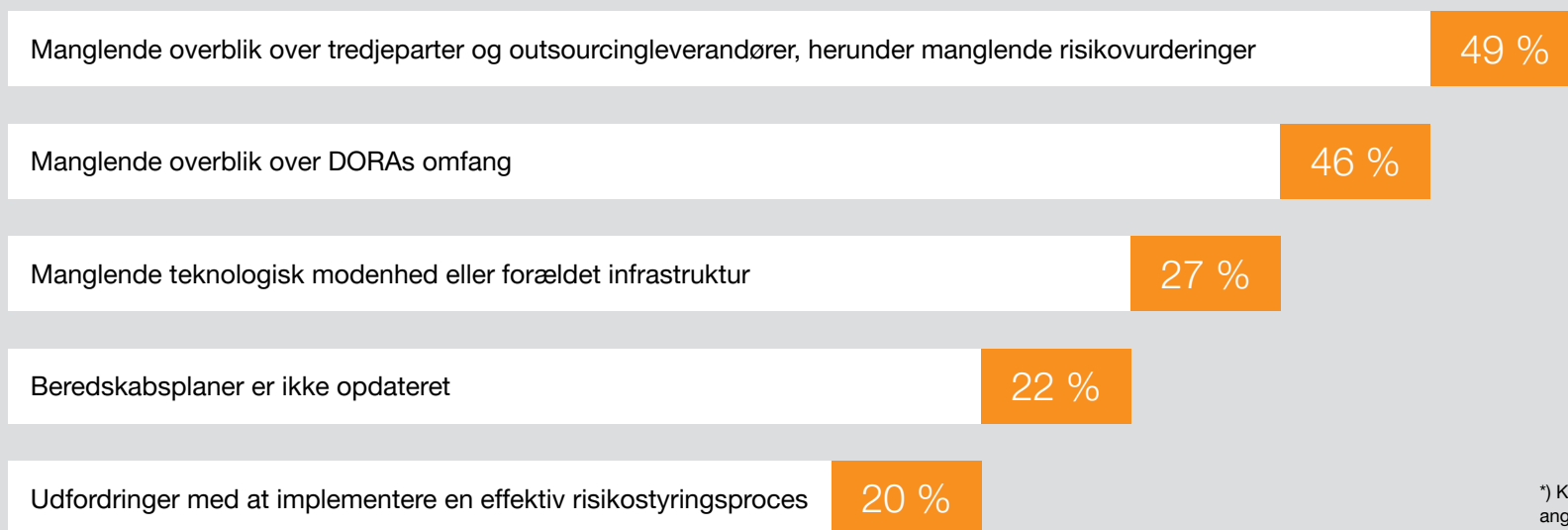
Vi har endnu ikke planlagt at implementere kravene i DORA

5 %

Ved ikke

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

Top 5



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

PwC erfarer

Der er generelt et godt kendskab blandt de berørte virksomheder i forhold til DORA-forordningen og kravene heri, men der er fortsat betydelige udfordringer i forhold til implementering og overholdelse af kravene. Barrierer såsom manglende overblik over tredjeparter, teknologisk modenhed og beredskabsplaner udgør betydelige udfordringer for virksomheder, der skal opfylde DORA-kravene. PwC erfarer, at virksomheder opfatter DORA som værende kompleks, grundet sin størrelse og påvirkning mange steder i den operationelle organisation. Selvom forordningen først træder i kraft i januar 2025, anbefaler PwC, at finansielle virksomheder og IKT-tjenesteudbydere allerede nu begynder at tilpasse sig de nye krav, da en implementering kan være både tids- og ressourcekrævende. PwC's erfaring viser, at en struktureret tilgang med nedbrydning af reguleringspunkterne på alle indsatsområder gør det let for virksomhederne at overskue forordningen og dermed vurdere, hvordan de kommer videre.

Læs mere om DORA og om, hvem der er omfattet, [her](#).

En utilstrækkelig forståelse af kravene i NIS 2 og DORA samt af kravenes kompleksitet, og hvordan de skal implementeres, kan medføre, at mange virksomheder ikke når at blive compliant med lovgivningen. Derfor bør virksomhederne prioritere at overholde NIS 2-direktivet og DORA-forordningen samt søge vejledning og støtte fra relevante aktører.

12 %

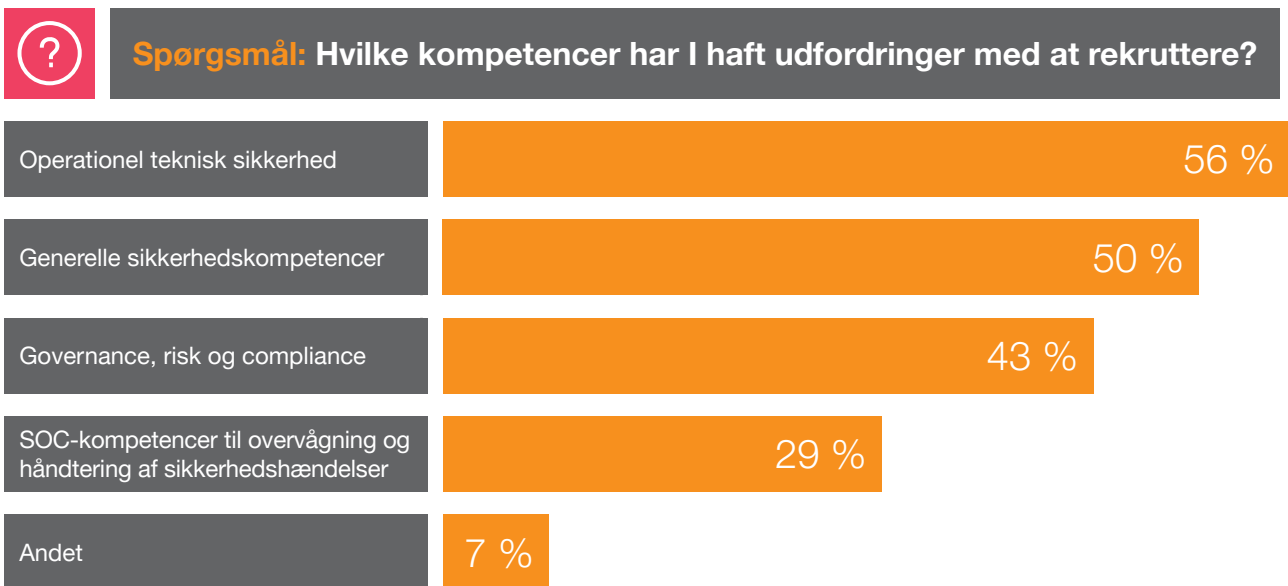
af CXO'erne, CISO'erne og it-sikkerhedsspecialisterne fortæller, at de ikke kan fastslå, om de er omfattet af DORA



Knap hver anden virksomhed har svært ved at rekruttere medarbejdere inden for cybersikkerhed

Der er stor mangel på kvalificeret arbejdskraft i Danmark, hvilket også har betydning for virksomhedernes muligheder for at ruste sig på cybersikkerhedsområdet.

Omtrent halvdelen af de virksomheder (49 %), der har haft behov for nye medarbejdere inden for cyber- og informationssikkerhed i de seneste 12 måneder, har haft svært ved at rekruttere de rette medarbejdere. Blandt de større virksomheder er det 56 %. Udfordringerne med at rekruttere nye medarbejdere er især centreret om kompetencer inden for operationel teknisk sikkerhed, generelle sikkerhedskompetencer samt governance, risk og compliance.





PwC erfarer

Kun 29 % af virksomhederne angiver, at de har haft udfordringer med at rekruttere medarbejdere med Security Operations Centre (SOC)-kompetencer, hvis opgave er at overvåge, om der er sikkerhedsrelaterede hændelser i it-systemer og netværk. PwC vurderer, at grunden hertil kan være, at det oftest kun er de større virksomheder, der har deres egen SOC-funktion. De mindre virksomheder outsourcer ofte SOC-tjenesten til eksterne parter.

Hvad oplever din virksomhed som de vigtigste motiverende faktorer for jobkandidater inden for cyber- og informationssikkerhed?

Top 3

Arbejdsopgaver

51 %

Lønvedtægter

46 %

Muligheden for udvikling/Karrieremuligheder

43 %

Bestyrelsens fokus på cyberkriminalitet stiger, men der er stadig plads til forbedringer

Bestyrelsesmedlemmer i danske virksomheder er mere opmærksomme på cybersikkerhed end nogensinde før, men cyberangreb er fortsat blandt de største trusler og koster danske virksomheder på bundlinjen.

Cybersikkerhed er et anliggende for virksomhedens bestyrelse, der har ansvaret for at vurdere og håndtere risici i virksomheden. Bestyrelsens opgave er at beskytte ikke kun virksomhedens økonomi, men også dens værdier, konkurrenceevne og strategiske mål på kort og lang sigt. Samtidig skal bestyrelsen beslutte, hvor omfattende beskyttelsen mod cybertrusler skal være, hvilket er et afgørende element, da et cyberangreb kan have konsekvenser for både virksomhedens resultater og dens evne til at nå strategiske mål.

Denne del af undersøgelsen er målrettet bestyrelsen og dens rolle i at styrke virksomhedens cybersikkerhed.

72 % af bestyrelsesmedlemmerne har cybersikkerhed som en fast del af deres årshjul. Det er en forbedring sammenlignet med 2022 (61 %), men bør for alle være en fast bestanddel af årshjulet og en naturlig del af bestyrelsens arbejde. Over halvdelen (58 %) af bestyrelsesmedlemmerne angiver, at deres virksomhed har etableret en længerevarende handlingsplan eller et program³ på cybersikkerhedsområdet, mens 24 % endnu ikke har en handlingsplan på plads.

³ 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.

Et tilstrækkeligt videngrundlag er forudsætningen for, at bestyrelsen kan håndtere virksomhedens cybersikkerhed hensigtsmæssigt. Alligevel er det kun 33 %, der modtager og behandler information om cyberrisici mindst én gang i kvartalet, mens det for 38 % er mindst én gang om året, sjældnere eller aldrig. 37 % af bestyrelsesmedlemmerne modtager derudover ikke en årlig rapport om cybersikkerhed, og 47 % trænes ikke i området. Det er en kritisk mangel, da regelmæssig træning i cybersikkerhed er afgørende for håndteringen og forståelsen af cyberrisici.

Overordnet er der udfordringer med at sikre, at bestyrelsesmedlemmerne har tilstrækkelig viden om cyber- og informationssikkerhed. Cybercrime Survey indikerer, at 79 % kun i nogen eller mindre grad mener, at sammensætningen af bestyrelsens kompetencer giver dyb nok viden om cyber- og informationssikkerhed.

PwC erfarer

For at forbedre bestyrelsens viden om cyber- og informationssikkerhed bør bestyrelsen sætte sikkerhed højere på agendaen. Således skal bestyrelsen gå forrest og understøtte en stærk og bevidst cybersikkerhedskultur. Bestyrelsen skal overveje at gøre brug af eksterne eksperter samt søge inspiration fra andre organisationer og brancher.

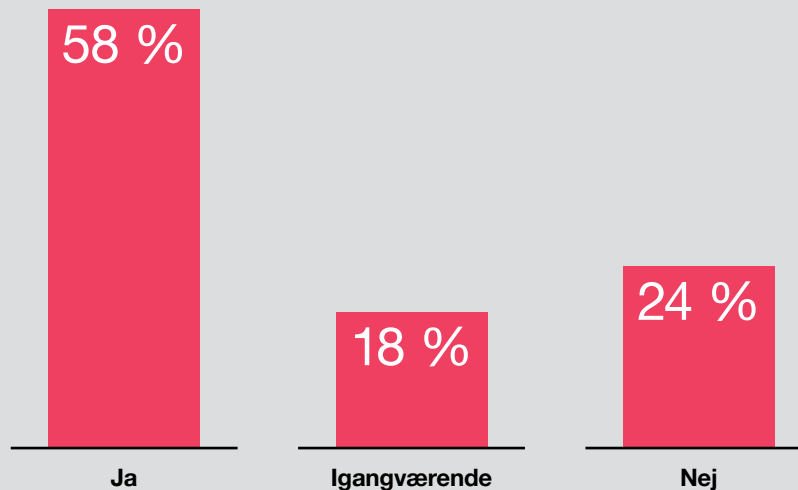
Læs mere i CFO'ens Cyberguide [her](#).

47 %

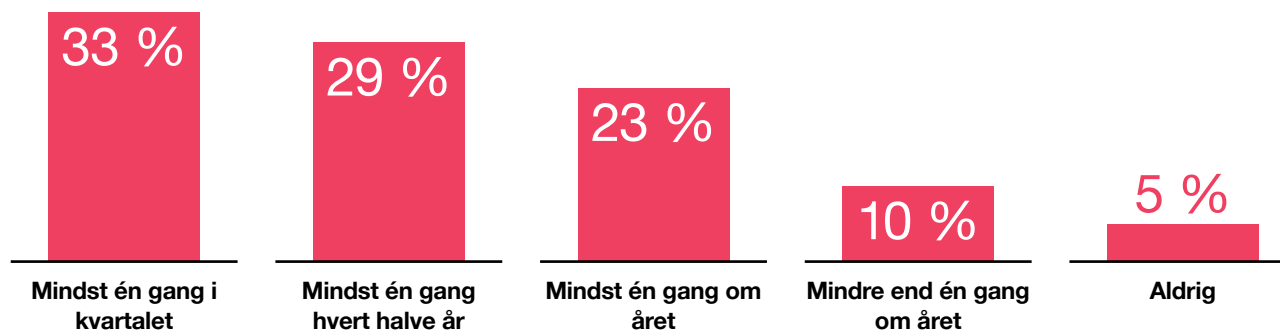
af bestyrelsesmedlemmerne
modtager ikke
træning i cyber- og
informationssikkerhed



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

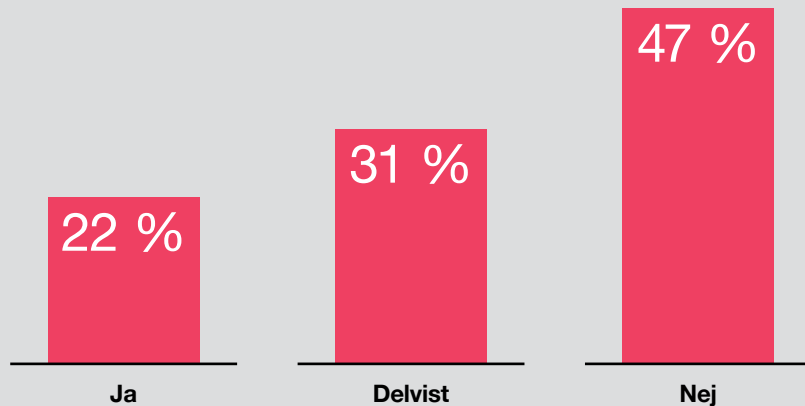


Spørgsmål: Hvor ofte modtager og behandler bestyrelsen information om cyberrisici?

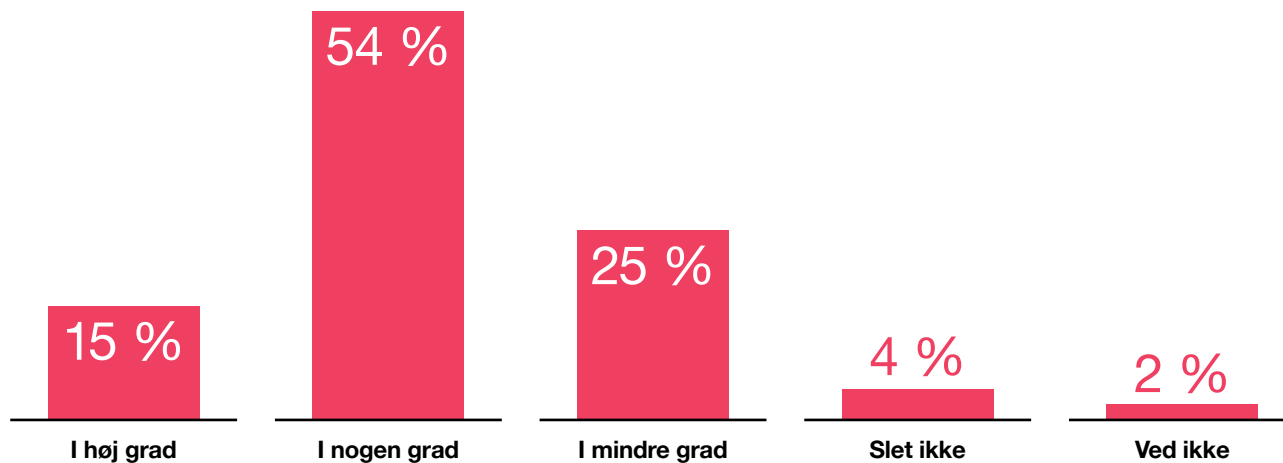




Spørgsmål: Modtager bestyrelsen træning i cyber- og informationssikkerhed?



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





Om undersøgelsen

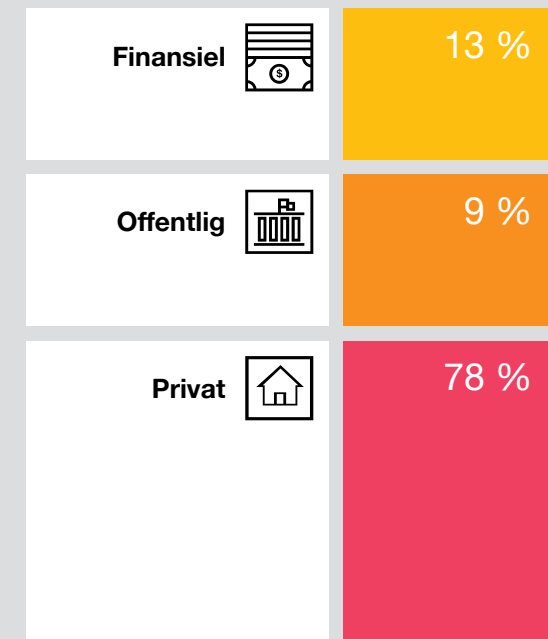
556 danske og 106 norske virksomhedsledere, it-chefer og it-sikkerhedsspecialister har deltaget i PwC's Cybercrime Survey 2023. Denne rapport sætter fokus på cybersikkerhed i dansk erhvervsliv og hos offentlige institutioner.

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, Punktum dk 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 førnævnte organisationer.

Undersøgelsens respondenter fordelt på sektorer i Danmark



Større virksomheder er defineret som ≥ 200 medarbejdere.
Mindre virksomheder er defineret som ≤ 199 medarbejdere.

Tjekliste

I PwC vil vi gerne hjælpe virksomheder 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 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 NIS 2 på [pwc.dk](https://www.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 [pwc.dk/cyberaware](https://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](https://www.pwc.dk/response)

Har I testet jeres beredskabsplaner for cyberhændelser? Læs mere på [pwc.dk/beredskab](https://www.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](https://www.pwc.dk/iam) og [pwc.dk/pam](https://www.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 [pwc.dk/cfocyberguide](https://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 pwc.dk/cyber.



Mads Nørgaard Madsen
Partner
Leder af Consulting

T: 2811 1592
E: mads.norgaard.madsen@pwc.com



Peter Brock Madsen
Partner
Cyberrisikostyring

T: 2056 8505
E: peter.brock.madsen@pwc.com



William Sharp
Partner
Cyber Operationel
Technology

T: 4040 1074
E: william.sharp@pwc.com



Christian Kjær
Partner
Cyberrisikostyring

T: 5132 1270
E: christian.kjaer@pwc.com

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.

© 2023 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.



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 næsten 2.800 medarbejdere og partnere, som brænder for at gøre en positiv forskel for kunder og kolleger. Globalt er vi 328.000 PwC'ere i 152 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 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

ISSN: 2597-1948

ISBN 978-87-94274-17-3