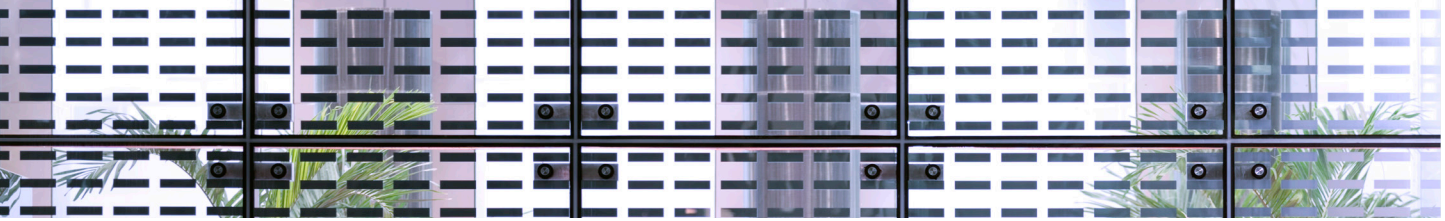
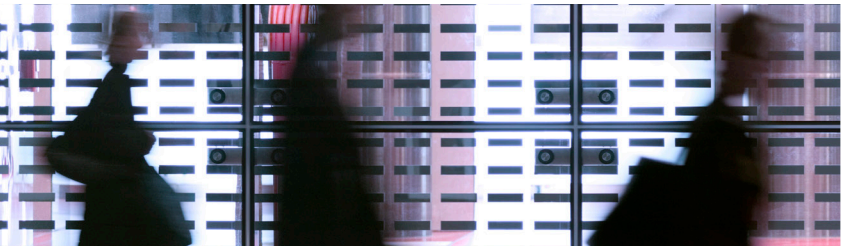


61 %

anvender eller planlægger at anvende AI i arbejdet med cybersikkerhed

60 %

er mere bekymrede for cybertrusler i dag end for 12 måneder siden



Cybercrime Survey 2024

41 %

af virksomhederne har beredskab som højest prioriterede investering

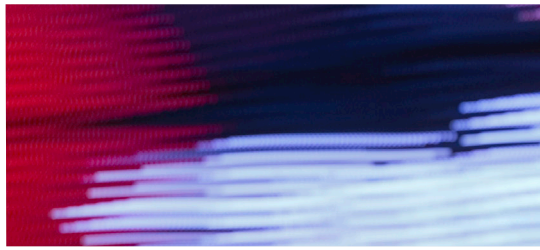
pwc

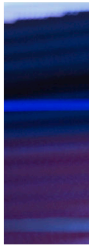
Revision. Skat. Rådgivning.

Succes skaber vi sammen ...

For 10. år i træk har PwC taget temperaturen på arbejdet med cybersikkerhed i Danmark. 463 topledere, sikkerhedschefer og fagspecialister fra den private og offentlige sektor har deltaget i undersøgelsen. Respondenterne har bidraget med deres indsigter i bl.a. investeringer, udfordringer og muligheder i arbejdet med cybersikkerhed. De har desuden vurderet det aktuelle trusselsbillede og rapporteret, hvordan og i hvilket omfang de arbejder med cyber- og informationssikkerhed.

Indhold





Øget fokus på cybersikkerhed: Virksomheder skruer op for AI og beredskab

Beredskab som prioritet i Danmark

For 10. år i træk har PwC taget temperaturen på arbejdet med cybersikkerhed i dansk erhvervsliv og den offentlige sektor. Undersøgelsen viser, at temaet kun har fået højere prioritet I de danske organisationer. I 2015 svarede blot hver tredje virksomhed, at de havde øget cybersikkerhedsbudgettet i seneste regnskabsperiode. I 2024 svarer 66 % af virksomhederne, at de forventer at øge deres sikkerhedsbudget inden for de næste 12 måneder.

Det skal naturligvis ses i lyset af, at der generelt i Danmark er et stadig større fokus på beredskab og modstandskraft mod krisesituationer såsom cyberangreb.

I sommer udsendte Beredskabsstyrelsen nye anbefalinger for at forberede befolkningen på krisesituationer, og derudover er der for nylig oprettet et nyt ministerie for at styrke indsatsen på beredskabsområdet. Ny lovgivning som NIS 2, CER og DORA sætter desuden fokus på virksomhedernes evne til at opretholde samfundskritiske forretningsprocesser. Disse forhold afspejler, at arbejdet med beredskab og cybersikkerhed er et endnu mere centralt strategisk tema for enhver organisation i den offentlige sektor, i de samfundsbærende institutioner og i det private erhvervsliv.

Stigende bekymring for cybertrusler

I årets Cybercrime Survey rapporterer 60 % af virksomhederne, at de er mere bekymrede for cybertrusler nu end for 12 måneder siden. Den stigende bekymring er for de flestes vedkommende relateret til konflikten mellem Rusland og Vesten. Denne bekymring har direkte indflydelse på virksomheders prioriteringer, hvor beredskab er blevet den næsthøjest prioriterede investering. 41 % af virksomhederne har således som topprioritet at styrke deres beredskab for at reducere konsekvenserne af en cyberrelateret hændelse.

Investeringer i teknologi og AI

Virksomhederne investerer også i ny teknologi: 61 % angiver, at de anvender eller planlægger at anvende AI som led i deres cybersikkerhed. Denne teknologi er afgørende for hurtigt at opdage og reagere på trusler. På tre år er der sket en femdobling i andelen af virksomheder, som har AI blandt de højest prioriterede investeringer inden for cybersikkerhed.

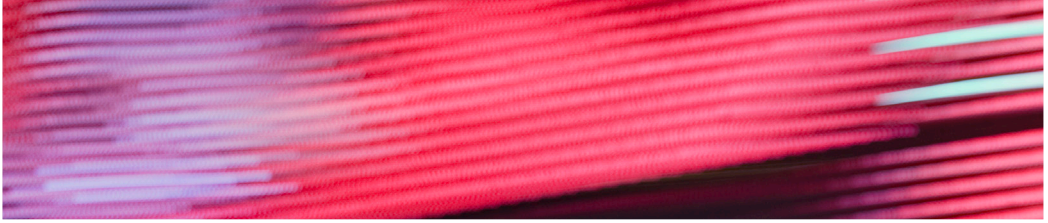
Regulering og tilpasning til NIS 2

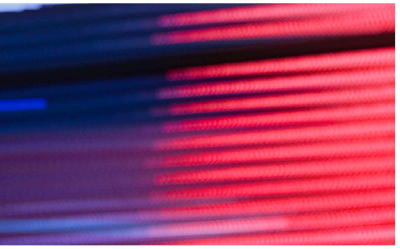
I disse måneder er virksomhederne desuden fokuseret på at tilpasse sig NIS 2-direktivet, hvor 80 % af de omfattede virksomheder nu har et godt kendskab til kravene, og 72 % fortæller, at de er i gang med implementeringen. Dette viser en klar fremgang i kendskabet, hvilket er nødvendigt for at sikre overholdelse af de nye krav i et stadig mere reguleret landskab.

En klar, fremadskuende strategi

Årets undersøgelse viser, at beredskab, investeringer i cybersikkerhed og tilpasning til regulering fylder mere end tidligere. Det er afgørende, at virksomhederne fortsætter med at prioritere disse områder for at sikre deres modstandskraft i fremtiden.

Christian Kjær
Partner
Cyber & Privacy

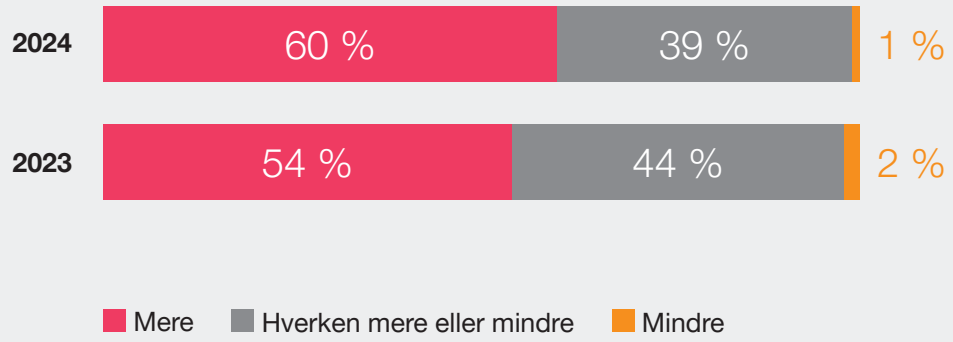




Øget bekymring for cyberangreb i dansk erhvervsliv og den offentlige sektor

Bekymringen for cybertrusler fortsætter med at vokse i det danske erhvervsliv og den offentlige sektor. Hele 60 % af de adspurgte virksomheder angiver, at de er mere bekymrede for de cybertrusler, de står over for i dag, sammenlignet med for 12 måneder siden. 39 % vurderer, at deres bekymringsniveau er uændret, mens blot 1 % føler sig mindre bekymrede end for et år siden.

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

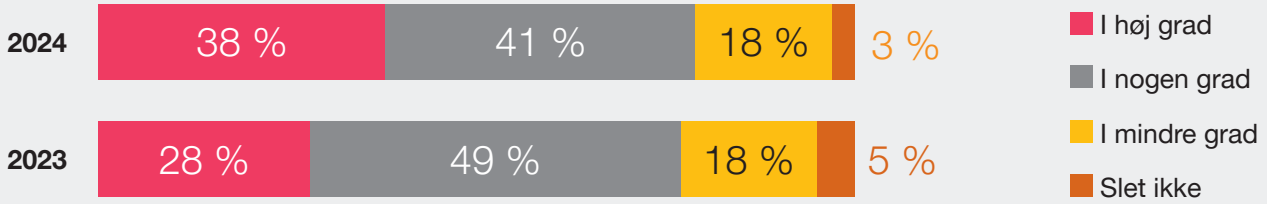


> På tre år er der sket en femdobling i andelen af virksomheder, der har AI som højt prioriteret investering inden for cybersikkerhed.

Christian Kjær
Partner

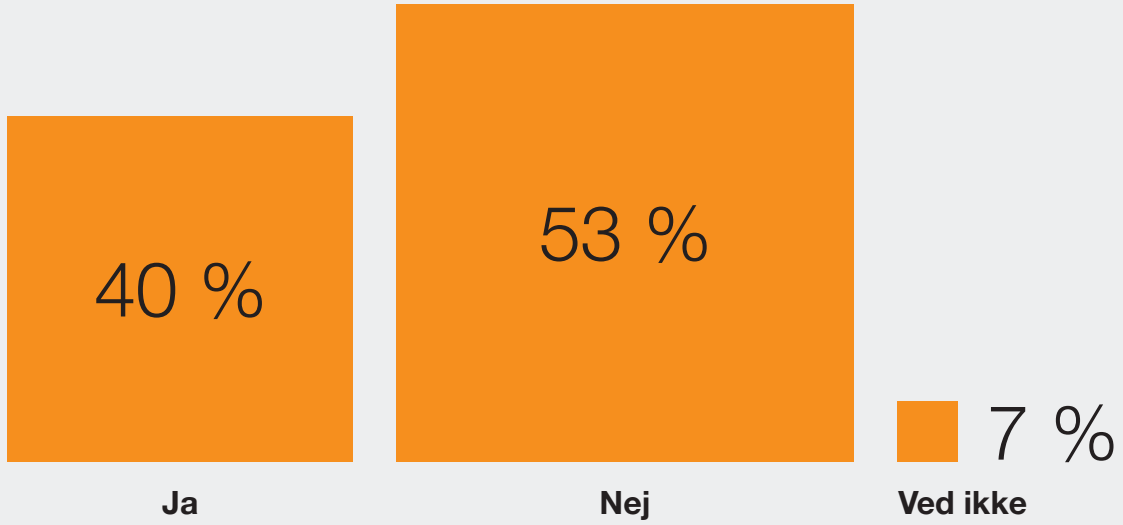
Denne stigende bekymring knytter sig til den geopolitiske situation. Blandt de virksomheder, der udtrykker øget bekymring, angiver 79 % således, at konflikten mellem Rusland og Vesten i nogen eller høj grad fortsat har indflydelse på deres bekymringsniveau. Desuden stiger andelen af dem, der i høj grad knytter den øgede bekymring til konflikten.

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



Som reaktion på den forøgede trussel har 40 % af virksomhederne implementeret nye cybersikkerhedstiltag. Disse omfatter både forebyggende foranstaltninger til at forhindre hændelser og beredskabsforanstaltninger, der styrker virksomhedernes evne til hurtigt og effektivt at reagere, hvis de bliver ramt af et cyberangreb.

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



Spørgsmål: Hvilke tiltag drejer det sig om?

PwC erfarer

For at imødekomme den stigende bekymring om cyberangreb anbefaler PwC, at organisationer investerer i grundlæggende sikkerhedsforanstaltninger såsom stærke adgangskoder, regelmæssige opdateringer og backup af data. PwC understreger ligeledes vigtigheden af at uddanne medarbejdere i sikkerhedspraksis og have et beredskab klar i tilfælde af et cyberangreb. Organisationer bør også overveje at få en professionel sikkerhedsvurdering for at identificere sårbarheder.

Læs mere om PwC's anbefalinger **her**.

PwC anbefaler ligeledes, at virksomheder løbende øver deres beredskab, for at sikre at de er klar til at håndtere en kompleks it-hændelse og minimere de forretningsmæssige konsekvenser – herunder ved at evaluere situationen, prioritere tiltag og kommunikere effektivt.

Læs mere om it-beredskabsplaner **her**.

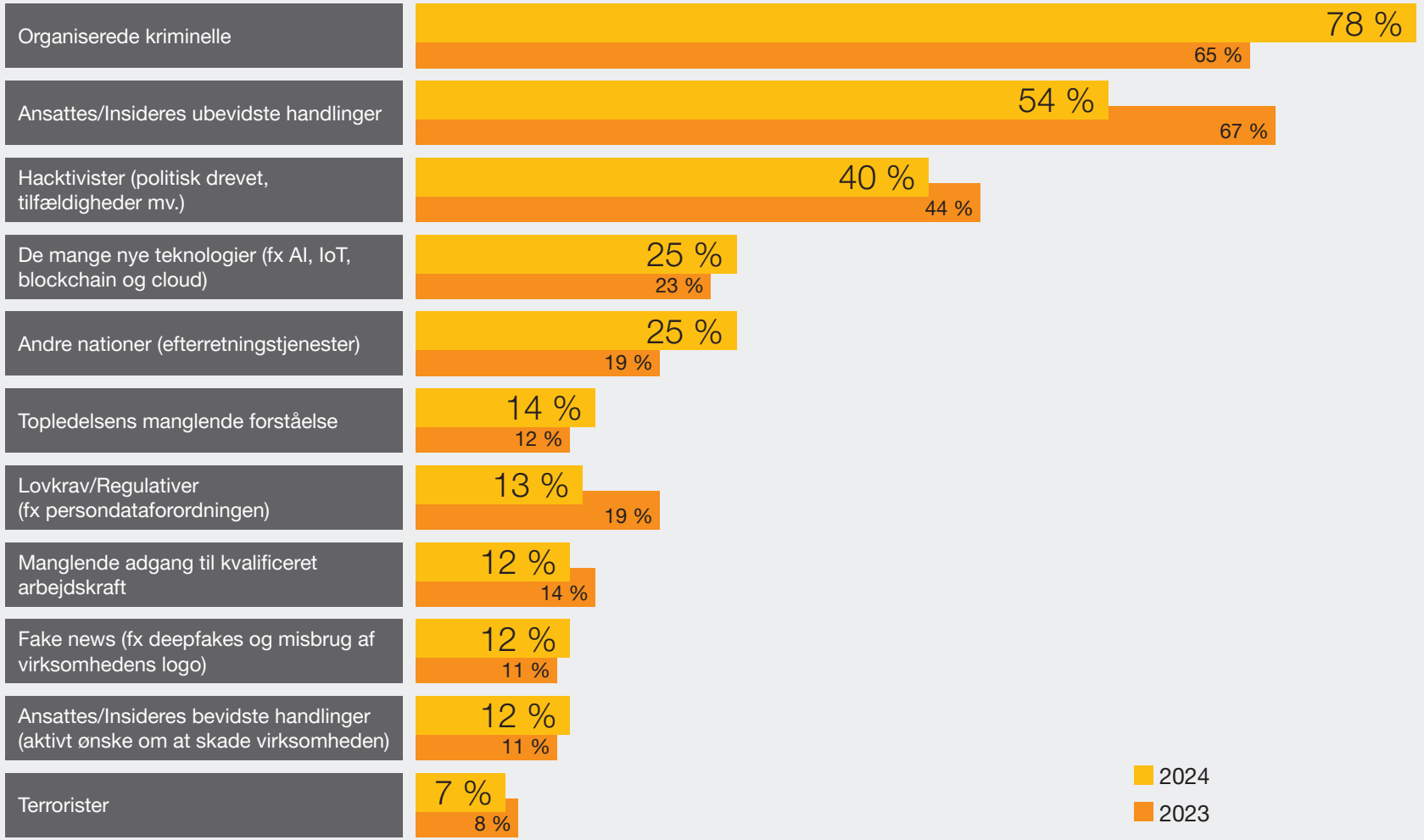
Fakta

Med stigende digitalisering og fjernarbejde er angrebsfladen for potentielle angreb vokset, hvilket betyder, at det er afgørende for organisationer at have en proaktiv tilgang til cybersikkerhed. Samtidig bliver cyberangreb mere sofistikerede og hyppige, hvilket har ført til en betydeligt stigende bekymring blandt virksomhederne.

Organiserede kriminelle topper listen over trusler

Virksomhederne anser i år organiserede kriminelle for en større trussel end tidligere, når det kommer til cyber- og informationssikkerhed. Således svarer hele 78 % af respondenterne, at organiserede kriminelle er blandt de største trusler mod deres virksomhed. Samtidig er truslen fra ansattes/insideres ubevidste handlinger aftaget i forhold til de seneste år.

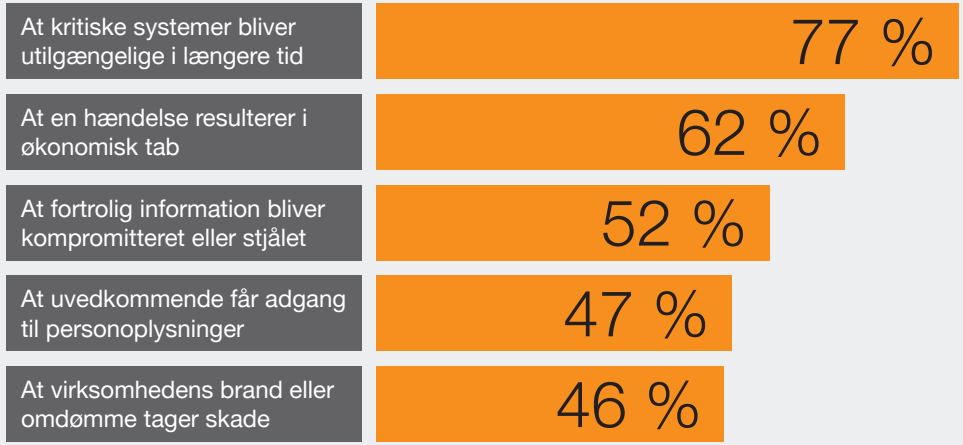
Spørgsmål: Hvad udgør de største trusler for din virksomhed i relation til cyber- og informationssikkerhed?



Det er phishingangreb, der udgør langt størstedelen af de hændelser, som virksomhederne rapporterer om. I årets undersøgelse svarer 64 % af dem, der har oplevet en cyberhændelse, at der var tale om phishingangreb, hvilket er betydeligt flere end øvrige typer af hændelser.

Når det kommer til de potentielle konsekvenser af en cyberhændelse, er den største bekymring udsigten til længerevarende nedbrud på kritiske it-systemer. Hele 77 % angiver, at nedbrud på kritiske systemer er deres største bekymring, mens 62 % peger på de direkte økonomiske konsekvenser af et cyberangreb.

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



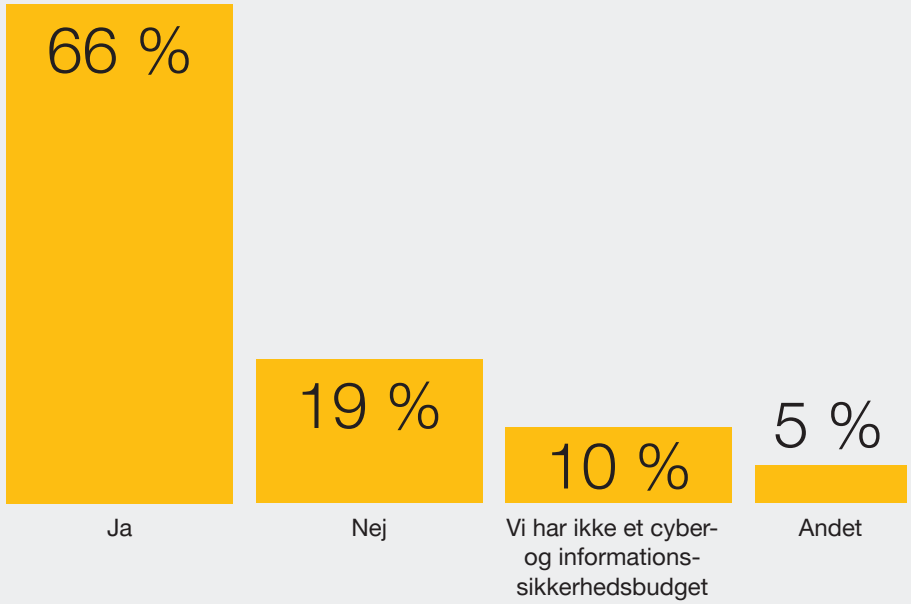
Fakta

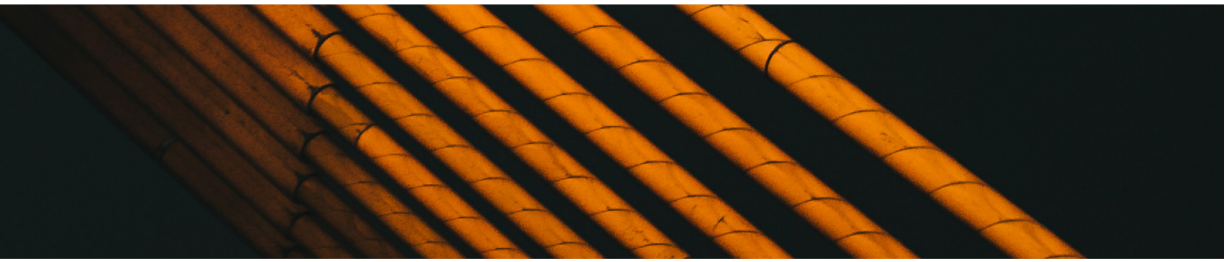
Cybertrusler er ikke længere begrænset til hackere. Truslerne kan opstå internt i organisationen på grund af medarbejdernes ubevidste handlinger, fx ved at en medarbejder klikker på et link i en phishingmail eller kommer til at dele følsomme oplysninger med uautoriserede personer. Medarbejdernes ubevidste/utilsigtede handlinger repræsenterer en signifikant trussel, hvorfor menneskelige risici bør prioriteres højt på sikkerhedsagendaen, da selv den bedste teknologiske sikkerhed kan blive undermineret af menneskelige fejl.

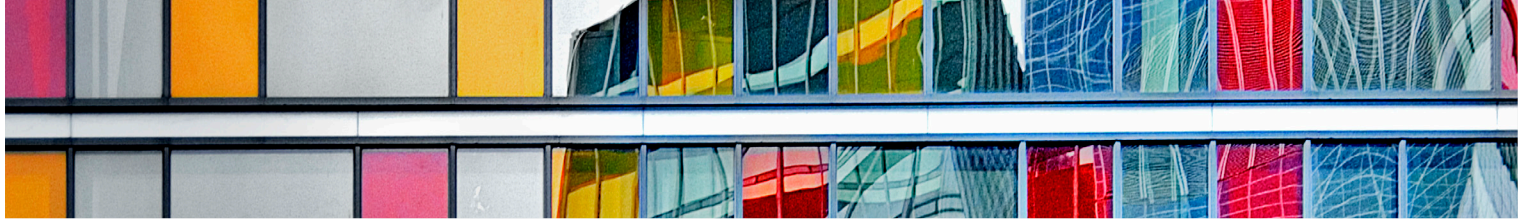
66 % forventer at øge cybersikkerhedsbudgettet de næste 12 måneder

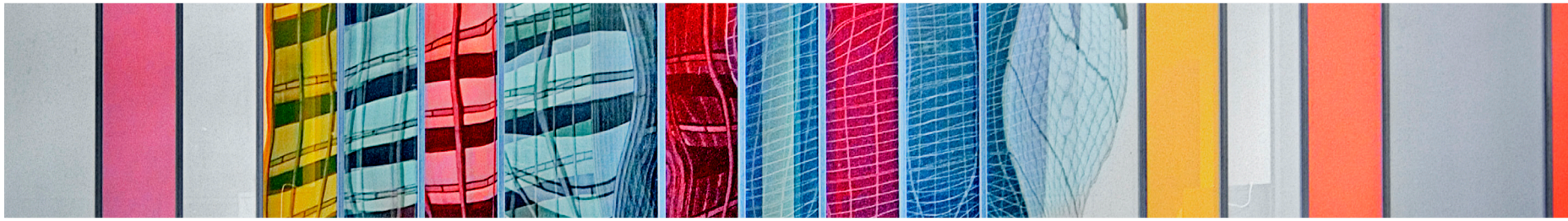
De danske virksomheder fortsætter med at øge budgetterne inden for cyber- og informationssikkerhed. Således forventer 66 % af virksomhederne at bruge endnu flere midler på bekæmpelse af cyberangreb. Blandt dem, der forventer at øge budgettet, svarer 64 %, at de forventer at øge det med mere end 10 % over de kommende 12 måneder.

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



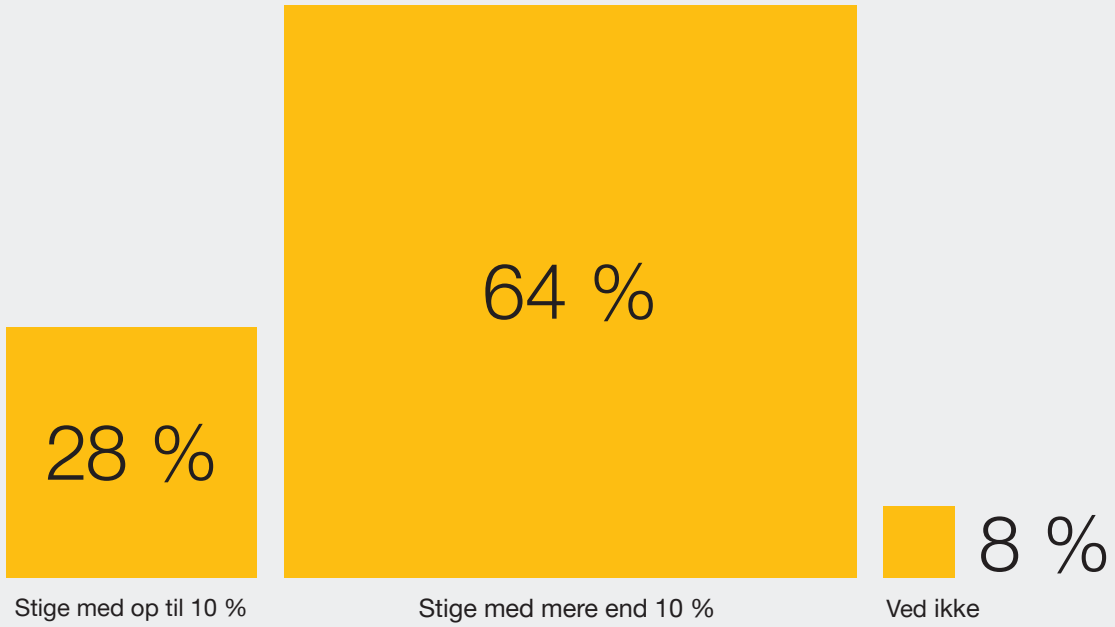




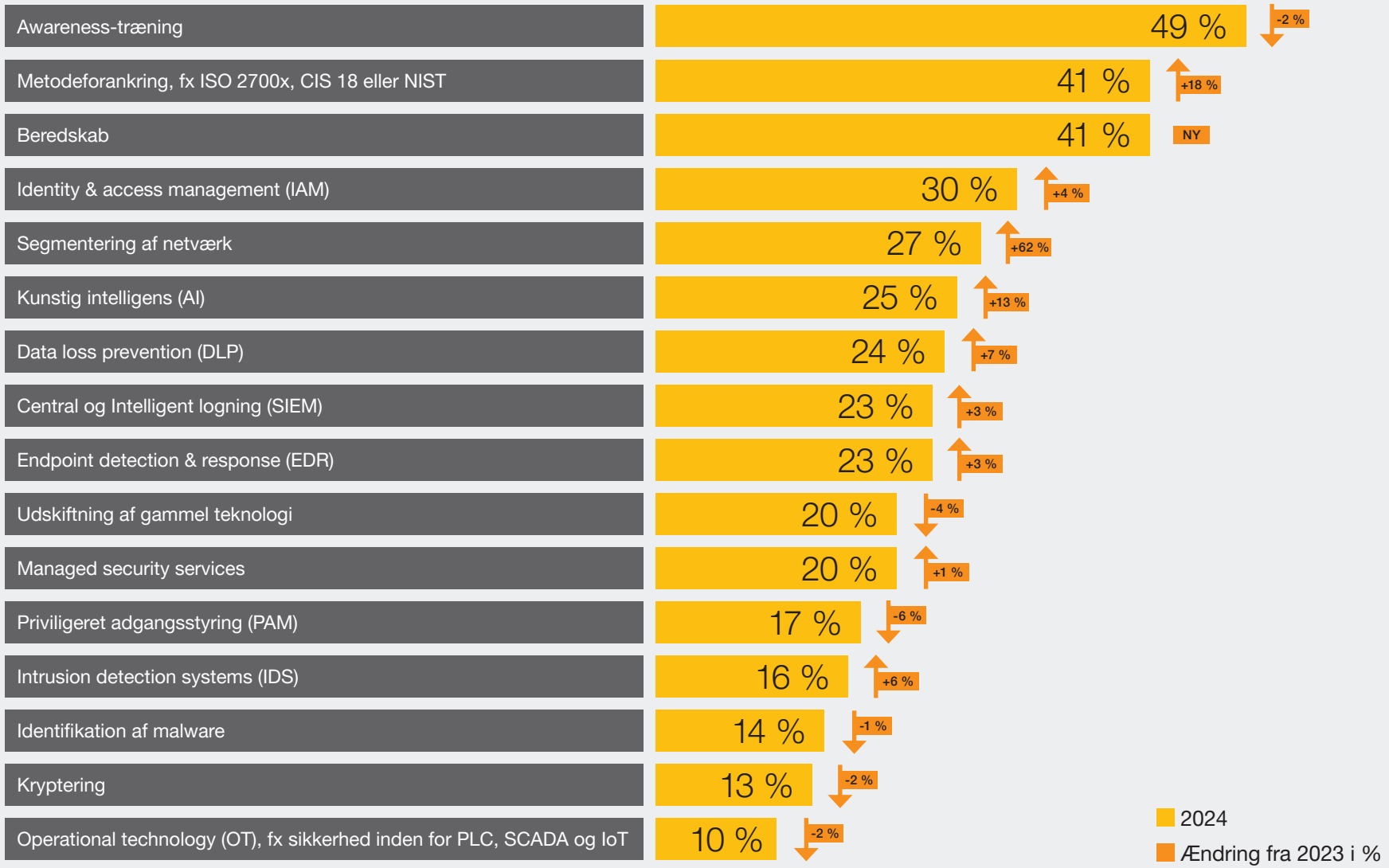


Awareness-træning topper virksomhedernes liste over prioriterede investeringer. I årets undersøgelse har man som noget nyt kunnet vælge beredskab, og denne kategori går direkte ind på en delt andenplads over de mest prioriterede investeringer. På en delt andenplads finder vi også metodeforankring, som går fra 23 % i 2023 til 41 % i 2024. Det skyldes bl.a., at flere virksomheder i stigende grad læner sig op ad diverse metoder til at strukturere deres sikkerhedsarbejde for at imødekomme kravene fra ny lovgivning, fx NIS 2 og DORA.

Spørgsmål: Hvor meget forventer du, at cyber- og informations-sikkerhedsbudgettet vil stige inden for de næste 12 måneder?



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



PwC erfarer

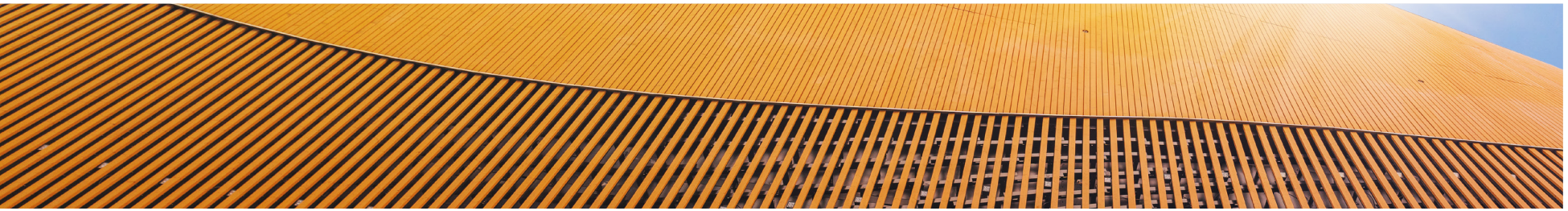
For at styrke organisationens forsvar mod cybertrusler anbefaler PwC, at awareness-træning bliver en integreret del af virksomhedens sikkerhedsstrategi.

PwC har erfaret, at en micro-/nanolearning-tilgang, hvor medarbejdere kontinuerligt modtager korte, målrettede budskaber og træningssessioner, ikke kun reducerer mængden af ressourcer, der er nødvendige for træning i cybersikkerhed, men også sikrer, at centrale budskaber forbliver aktuelle i medarbejdernes bevidsthed og nemmere kan omsættes til handling – og dermed er lettere at anvende i praksis. Ligeledes bør træningen være tilpasset organisationens specifikke risici med fokus på personlig og adaptiv læring, hvor indhold skræddersys til individuelle funktioner og behov. Løbende awareness-træning vil være med til at opbygge en kultur, hvor sikkerhed prioriteres af alle ansatte. Awareness-træning er ikke kun en engangsaktivitet, men en løbende proces, som kræver opfølgning og opdatering.

Læs mere om PwC's skræddersyede awareness-træning og e-learning-platform **her**.

Fakta

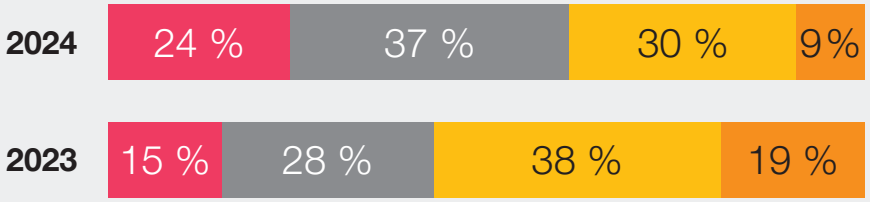
Awareness-træning er en metode til at øge medarbejdernes bevidsthed om cybersikkerhed og databeskyttelse gennem regelmæssige, målrettede træningssessioner. Awareness-træning kan reducere risikoen for cyberangreb betydeligt og samtidig forbedre medarbejdernes reaktionstid og evne til at identificere potentielle trusler i deres daglige arbejde.



AI er blevet en langt større faktor i arbejdet med cybersikkerhed

På listen over de højest prioriterede investeringer inden for cybersikkerhed stiger AI fra 12 % i 2023 til hele 25 % i 2024. Set over en treårig periode er der sket en femdobling, hvilket vidner om, hvilken hastighed teknologien udvikler sig med. Ifølge undersøgelsen angiver 61 % af virksomhederne, at de enten anvender eller planlægger at implementere AI i deres cybersikkerhedsstrategier – en stigning fra 43 % i 2023.

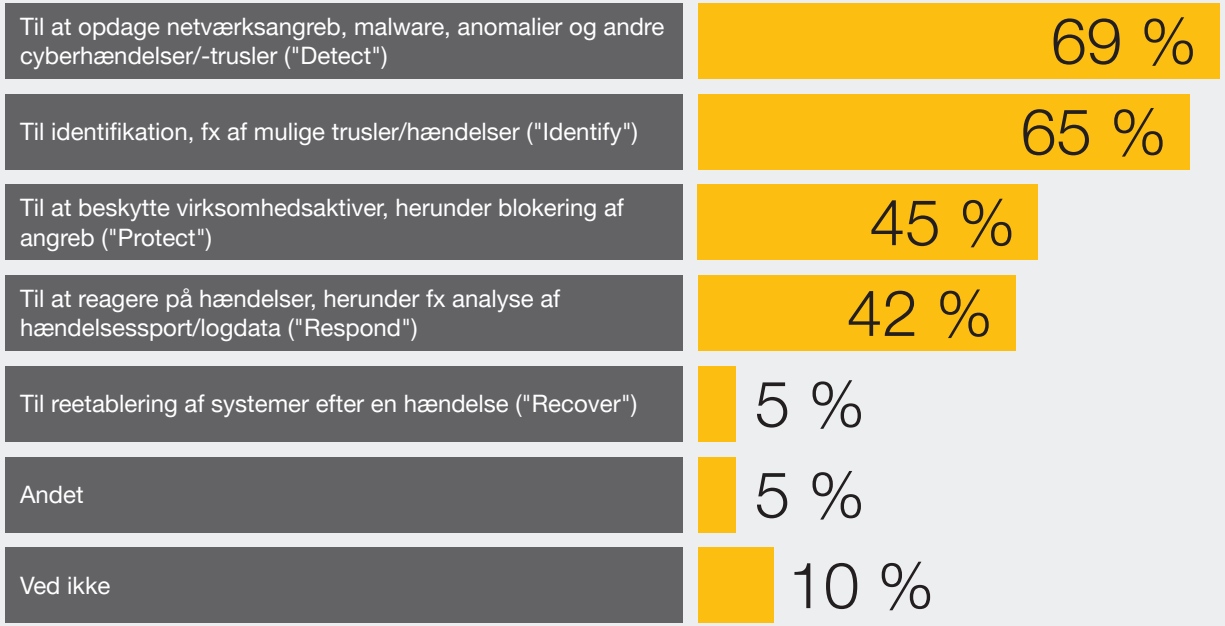
Spørgsmål: Anvender din virksomhed AI i arbejdet med cybersikkerhed?



- Ja, vi anvender AI i arbejdet med cybersikkerhed
- Nej, men vi har planer om at anvende AI i arbejde med cybersikkerhed i fremtiden
- Vi har ingen planer om at anvende AI i arbejdet med cybersikkerhed
- Ved ikke

Virksomhederne ser især AI som et værktøj til at effektivisere opdagelse af cyberangreb og identificering af trusler, men mange betragter også AI som en hjælp til at beskytte virksomhedens aktiver og reagere på hændelser. Kun 5 % af respondenterne anser AI som nyttig til reetablering af systemer efter en hændelse.

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



Fakta

Udviklingen inden for AI har haft en betydelig indflydelse på cybersikkerhed. AI kan både skabe nye sikkerhedstrusler og tilbyde avancerede løsninger til at imødegå dem. 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 samkøre værktøjer. Dette kan føre til en højere succesrate for den cyberkriminelle. Eksempler på AI-baserede trusler inkluderer deepfakes og AI-manipulerede cyberangreb. Samtidig kan AI i den defensive del af cybersikkerhed anvendes til at forbedre sikkerhedsforanstaltninger såsom detektion af phishing og netværksindtrængning samt til kryptering. AI's evne til at analysere store datamængder og identificere mønstre gør teknologien til et uundværligt værktøj i moderne cybersikkerhed, men det kræver også omhyggelig styring af de medfølgende risici.

PwC erfarer

PwC anbefaler, at virksomheder integrerer AI som en central komponent i deres cybersikkerhedsstrategi. AI kan hjælpe med at opdage trusler hurtigere, identificere mønstre (der ellers ville blive overset) og reagere automatisk på potentielle sikkerhedsbrud. Især de mange avancerede tekniske løsninger, som virksomhederne benytter i deres cyberforsvar, anvender AI til at effektivisere dataanalyse, detektion mv. Virksomhederne køber løsninger, der anvender AI, hvilket kommer dem til gode. Dog er det vigtigt at kombinere AI med menneskelig overvågning, for at sikre at systemerne fungerer optimalt og tilpasser sig nye trusler.

Som med enhver ny teknologi medfører AI også potentielle risici og nye lovgivningskrav, der skal overholdes. For at hjælpe virksomheder med at udnytte generativ AI's store potentiale samt med effektiv håndtering af risici og lovgivningsmæssige krav har PwC udviklet rammeværket "Responsible AI". PwC tilbyder således værktøjer og rådgivning til at hjælpe virksomheder med at opbygge og styre AI på en ansvarlig måde, der understøtter langsigtet tillid og bæredygtighed.

Læs mere om, hvordan PwC's arbejder med "Responsible AI" **her**.

PwC tilbyder en "AI Readiness Assessment", der kan hjælpe virksomheder med at evaluere deres parathed til at implementere AI. Vurderingen fokuserer på at identificere styrker og svagheder i virksomhedens nuværende teknologi, datahåndtering, medarbejdere og ledelsesstruktur. Målet er at udvikle en klar plan for at forbedre AI-paratheden og sikre en vellykket implementering af AI-løsninger.

Læs mere om PwC's AI Readiness Assessment **her**.

Arbejdet med at tilpasse sig ny regulering har prioritet

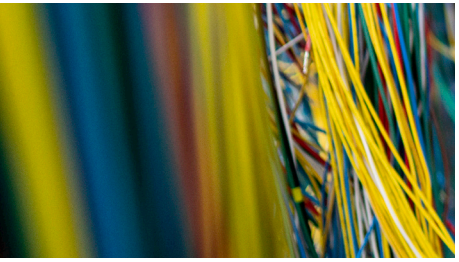
NIS 2-direktivet

Øget kendskab til NIS 2-direktivet

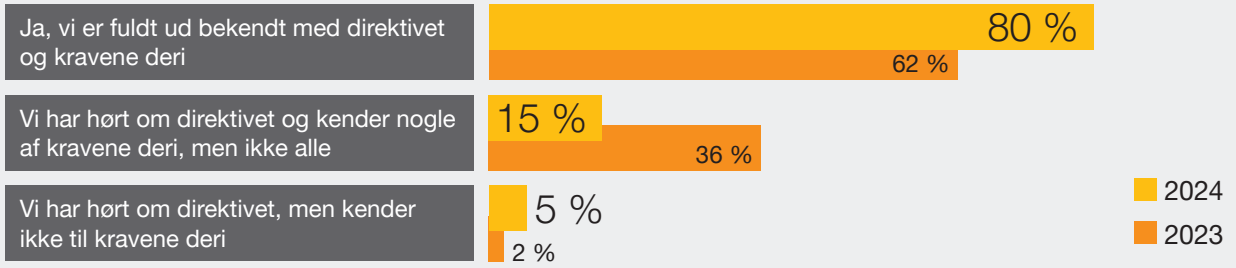
Resultaterne fra årets undersøgelse viser en markant stigning i virksomhedernes kendskab til NIS 2-direktivet. 80 % af de omfattede virksomheder angiver, at de nu er fuldt bekendt med direktivet og de tilhørende krav. Dette er en stigning på hele 18 % i forhold til sidste år, hvor blot 62 % havde samme niveau af kendskab.

Fremgang i implementering af NIS 2-krav

Undersøgelsen viser også en betydelig fremgang i implementeringen af NIS 2-direktivets krav. I år oplyser 72 % af virksomhederne, at de er i gang med at implementere NIS 2, hvilket er en markant stigning fra sidste år, hvor kun 49 % havde igangsat processen.

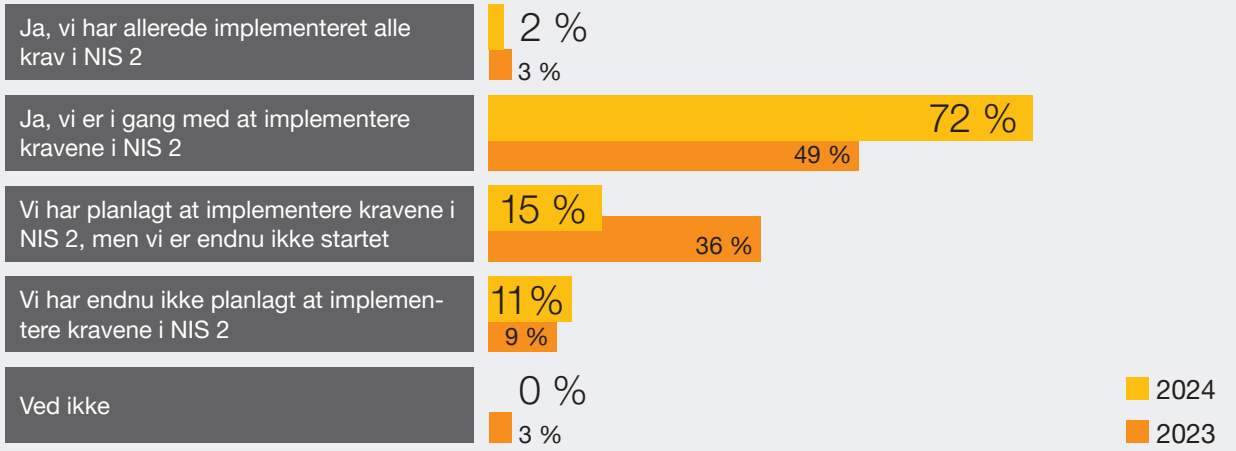


Spørgsmål: Er din virksomhed* bekendt med EU's NIS 2-direktiv og dets krav til beskyttelse mod cyberangreb og af kritisk infrastruktur?



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

Spørgsmål: Har din virksomhed* en plan for, hvordan I vil imødekomme/ implementere kravene i NIS 2-direktivet?

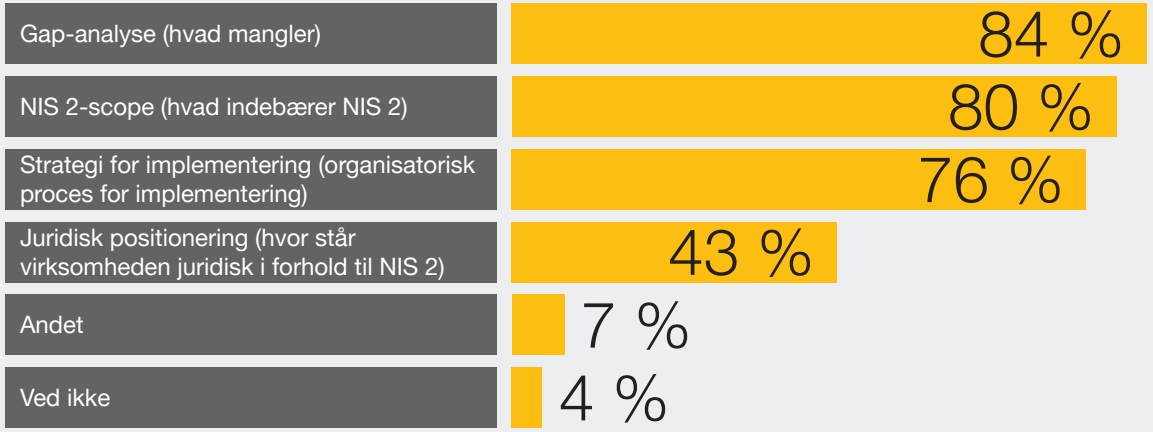


*) Kun virksomheder, der har angivet, at de er omfattet af NIS 2.

Planlægning og fokusområder i implementeringsprocessen

I år har vi for første gang spurgt ind til de konkrete elementer i virksomhedernes implementeringsplaner. Her angiver 84 %, at deres plan indeholder en gap-analyse, mens 80 % har udarbejdet et NIS 2-scope. 76 % har en strategi for implementeringen, og 43 % har vurderet deres juridiske position i forhold til NIS 2. Dette giver et indblik i, hvilke områder virksomhederne har prioriteret i deres forberedelser.

Spørgsmål: Hvad indeholder din virksomheds* plan for implementeringen af NIS 2?

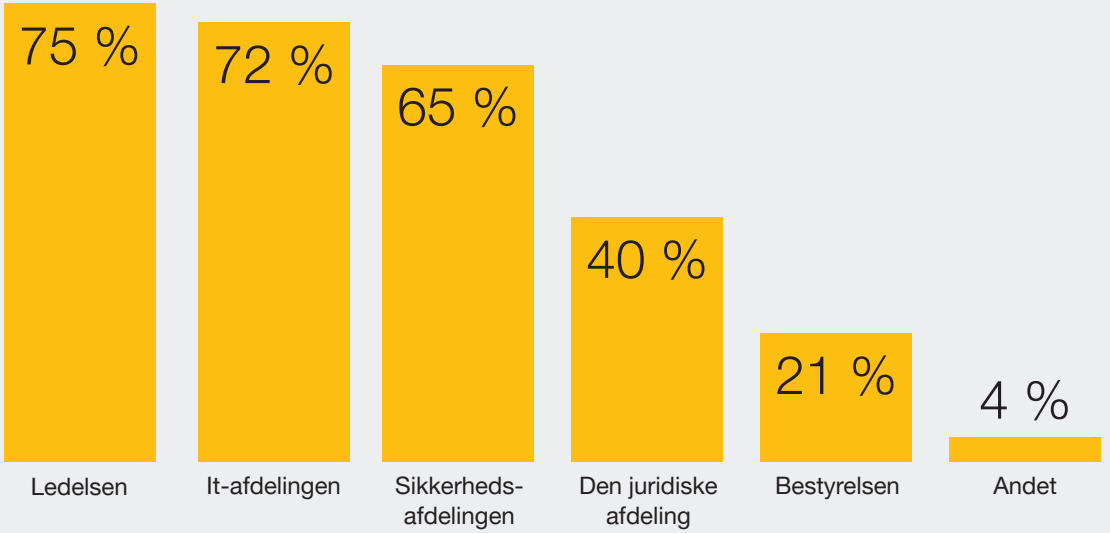


* Kun virksomheder, der har angivet, at de er omfattet af NIS 2.

Ledelsens engagement i NIS 2-implementeringen

Når det kommer til organiseringen af NIS 2-planen, viser undersøgelsen, at ledelsen spiller en central rolle. Hele 75 % af virksomhederne angiver, at deres ledelse aktivt har deltaget i organiseringen af NIS 2-planen. It-afdelingen er også tæt involveret (72 %), mens 40 % af virksomhederne har involveret deres juridiske afdeling i processen.

Spørgsmål: Hvem har været med til at organisere denne plan for implementeringen af NIS 2-direktivet i din virksomhed*?

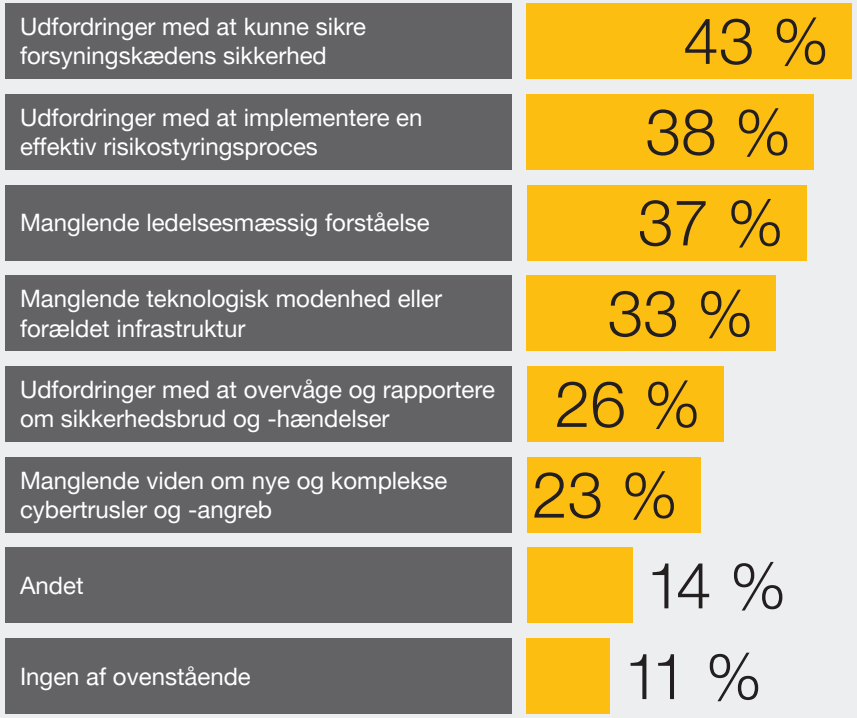


*) Kun virksomheder, der har angivet, at de er omfattet af NIS 2.

Barrierer for implementeringen af NIS 2

På trods af den positive udvikling er der stadig udfordringer. Ifølge 43 % af virksomhederne er den største barriere for implementeringen af NIS 2-kravene at sikre forsyningskædens sikkerhed. Andre udfordringer omfatter implementeringen af en effektiv risikostyringsproces samt manglende forståelse hos ledelsen, som er et problem i mere end hver tredje virksomhed.

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



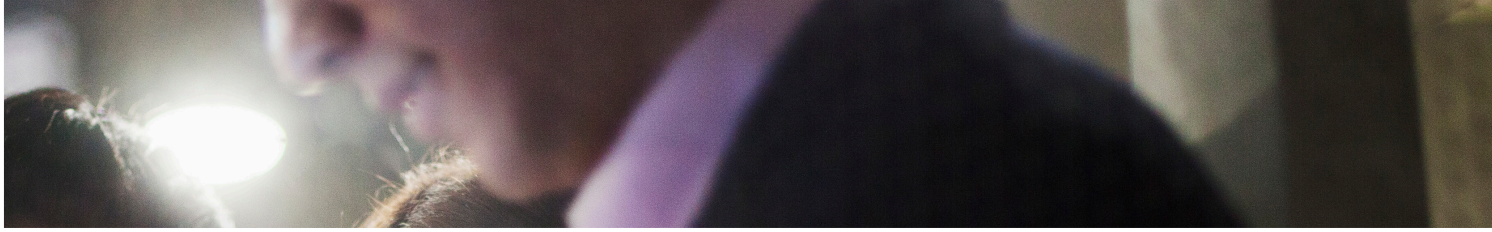
*) Kun virksomheder, der har angivet, at de er omfattet af NIS 2.

Fakta

NIS 2-direktivet har udvidet de tidligere krav fra NIS-direktivet og har til formål at styrke cybersikkerheden i hele EU for både offentlige og private aktører, der leverer vigtige eller væsentlige tjenester inden for sektorer såsom energi, transport, sundhed, finans, digital infrastruktur, vandforsyning, affaldshåndtering eller offentlig forvaltning.

Direktivet stiller højere krav til risikostyring, incident response og informationsdeling og kræver, at virksomheder implementere mere robuste sikkerhedsforanstaltninger, der sammen har til formål at styrke håndteringen af cyberrisici. Ydermere stiller NIS 2 krav til ledelse, risikostyring, forretningskontinuitet og kontrol samt tilsyn med de berørte aktører. Virksomheder, der ikke overholder NIS 2, kan risikere betydelige bøder og andre sanktioner. Derfor er det afgørende, at virksomheder på tværs af Europa forbereder sig på de nye krav.

Vær opmærksom på, at NIS 2 fastsætter nogle minimumsgrænser, der betyder, at det kun er virksomheder med flere end 50 ansatte og en årlig omsætning på mere end 10 mio. euro eller en årlig balance på over 43 mio. euro, der skal efterleve kravene.



PwC erfarer

PwC erfarer, at det er både omfattende og tidskrævende at implementere NIS 2. For at opfylde kravene i NIS 2-direktivet anbefaler PwC, at virksomheder gennemgår deres nuværende cybersikkerhedsstrategier og identificerer eventuelle mangler i forhold til de nye krav. Det er essentielt at etablere robuste processer for risikostyring, incident response og løbende overvågning af netværk. Ligeledes er det vigtigt at involvere ledelsen og bestyrelsen i sikkerhedsstrategien, da disse er personligt ansvarlige for manglende overholdelse af NIS 2-direktivet. Ydermere skal virksomheden sørge for, at alle relevante medarbejdere er trænet i de nye retningslinjer.

Er du i tvivl om, hvorvidt du er omfattet af NIS 2? Prøv PwC's scoping-værktøj **her**.

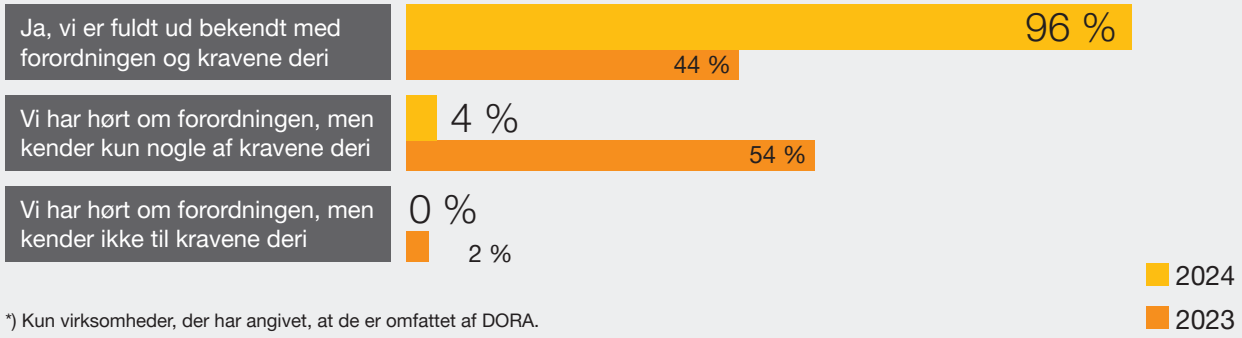
Læs mere, og hent trin-for-trin-guiden til implementering af kravene i NIS 2 **her**.

DORA-forordningen

Øget kendskab til DORA-forordningen

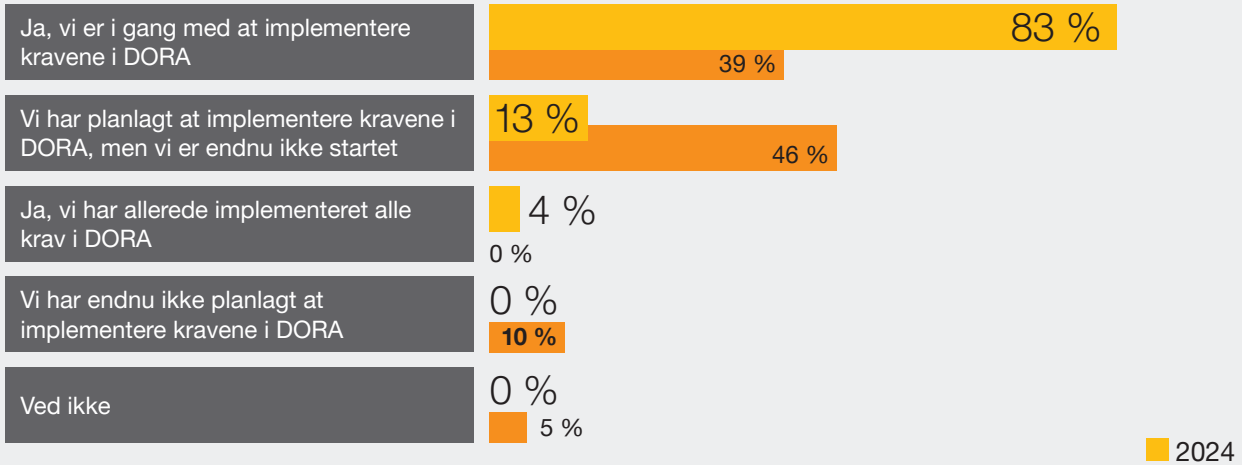
Kendskabet til Digital Operational Resilience Act (DORA) er steget markant blandt de omfattede virksomheder. Ifølge årets Cybercrime Survey angiver 96 % af virksomhederne, at de er fuldt bekendt med forordningen og dens krav. Dette er mere end en fordobling i forhold til sidste år, hvor tallet lå væsentligt lavere (44 %). Ud over det øgede kendskab til DORA viser undersøgelsen, at 83 % af virksomhederne er i gang med at implementere forordningens krav, hvilket er en betydelig stigning fra 39 % i 2023. Implementeringsarbejdet organiseres i langt de fleste virksomheder på tværs af organisationen med inddragelse af ledelsen og compliance-funktioner samt it- og sikkerhedsafdelingerne.

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.

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

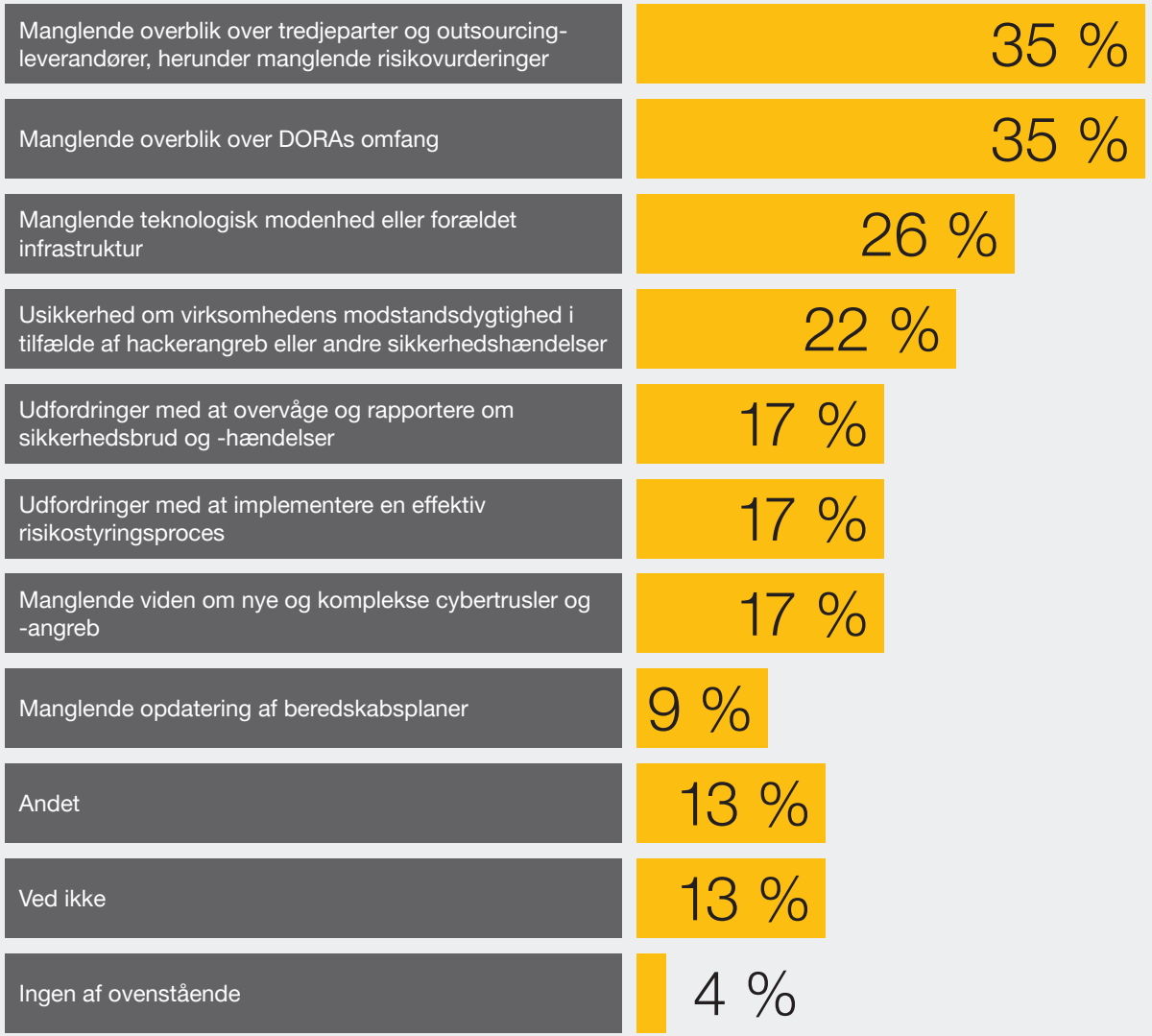


*) Kun virksomheder, der har angivet, at de er omfattet af DORA.

Barrierer for implementeringen

Selvom mange virksomheder har taget konkrete skridt i retning af implementering, oplever en tredjedel udfordringer med at få overblik over omfanget af kravene i DORA. Manglende viden om, hvad forordningen præcis kræver, nævnes som en barriere for fuld implementering. Ligeledes angiver ca. hver tredje virksomhed, at de mangler overblik over deres tredjeparter og outsourcing-leverandører, hvilket kan skabe yderligere vanskeligheder i implementeringsprocessen.

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



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

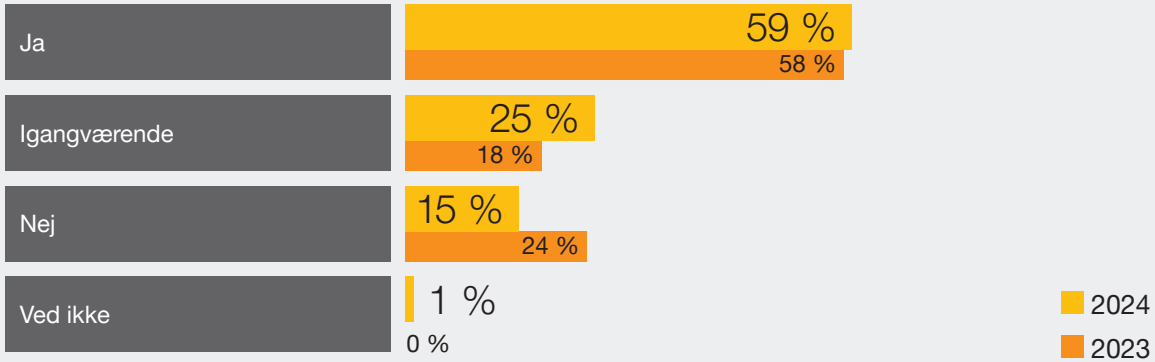
Cybersikkerhed på bestyrelsesdagsordenen: Fremskridt, men plads til forbedring

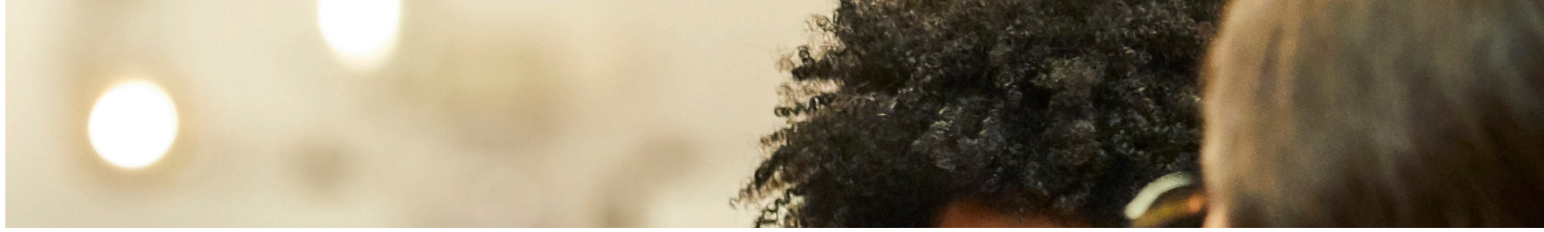
Strategisk fokus på cybersikkerhed vokser

Cybersikkerhed har opnået en central placering på bestyrelsesniveau i dansk erhvervsliv. Cybercrime Survey 2024 viser, at 84 % af bestyrelsesmedlemmerne enten har etableret eller er i færd med at udarbejde en langsigtet handlingsplan for cybersikkerhed. Dette markerer en stigning fra 76 % i 2023 og understreger en voksende erkendelse af behovet for at arbejde mere strategisk med cybersikkerhed. Syv ud af ti bestyrelsesmedlemmer har nu cybersikkerhed som en fast del af deres årshjul, hvilket viser et positivt fremskridt mod en mere struktureret håndtering af risici.

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.

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



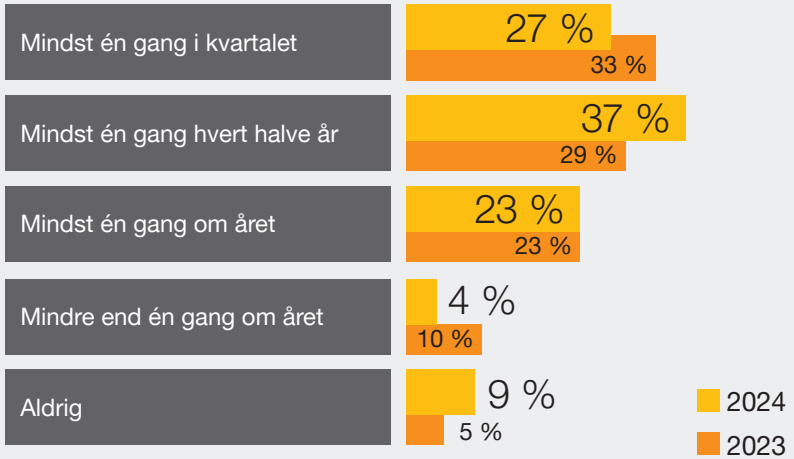


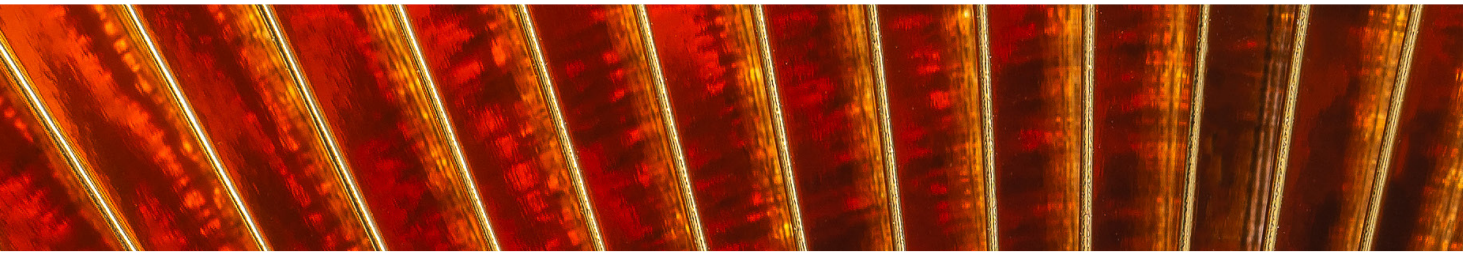
7 ud af 10

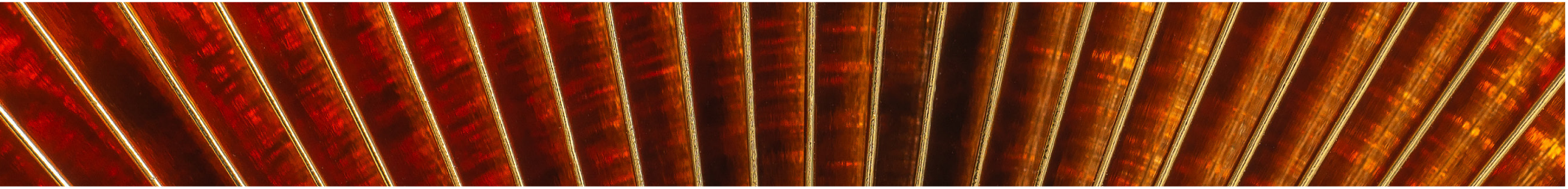
bestyrelsesmedlemmer har cybersikkerhed som en fast del af deres årshjul

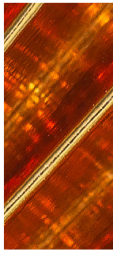
Trods dette strategiske fokus viser undersøgelsen, at der er områder, hvor udviklingen stagnerer. Løbende opfølgning på cyberrisici og behandling af hændelser drøftes eksempelvis ikke oftere i bestyrelserne end tidligere. Derudover fortæller færre bestyrelsesmedlemmer, at de modtager træning i cyber- og informationssikkerhed sammenlignet med tidligere år, hvilket kan pege på en udfordring, i forhold til at sikre at bestyrelsen har de nødvendige kompetencer til at håndtere de stigende trusler. Flere medlemmer end tidligere fortæller også, at bestyrelsens samlede kompetencer på dette område ikke er tilstrækkeligt dybdegående.

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



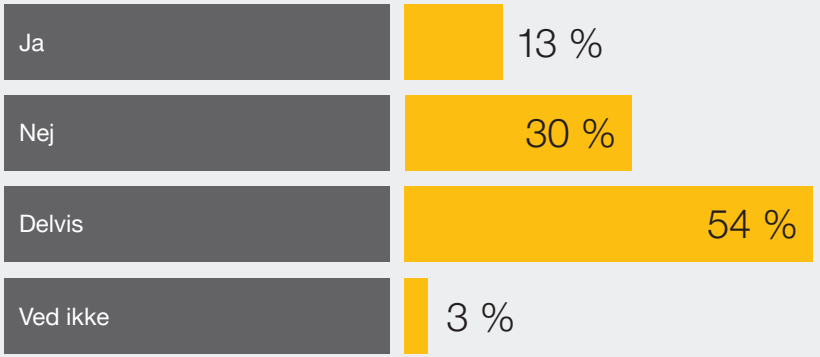


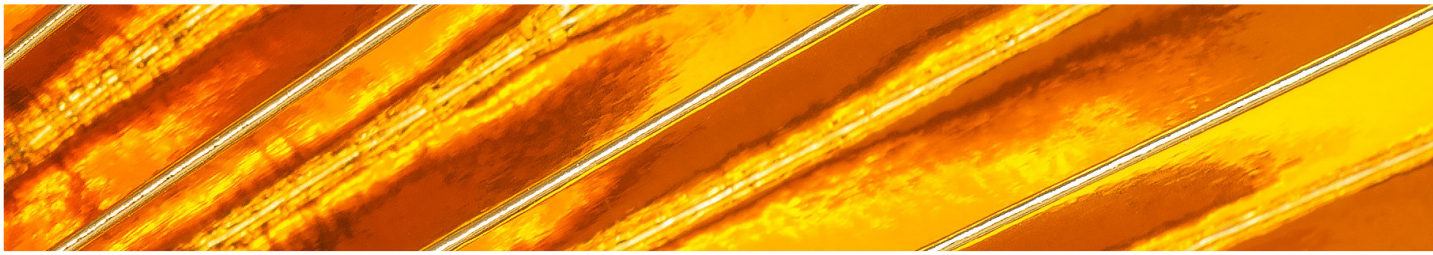


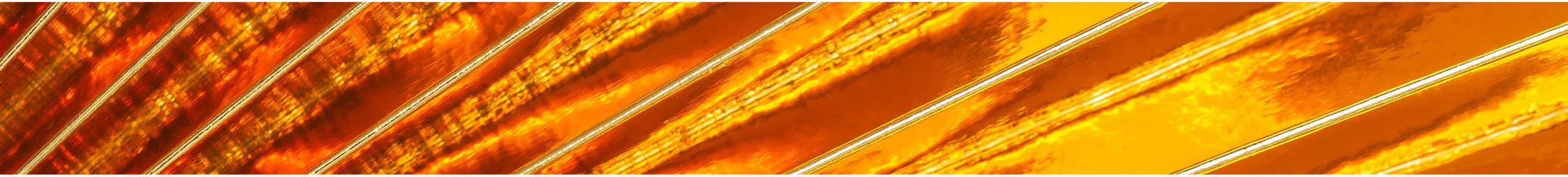


Spørgsmål: Hvor ofte behandler bestyrelsen cyberhændelser?

Spørgsmål: Modtager bestyrelsen træning i cyber- og informationssikkerhed?





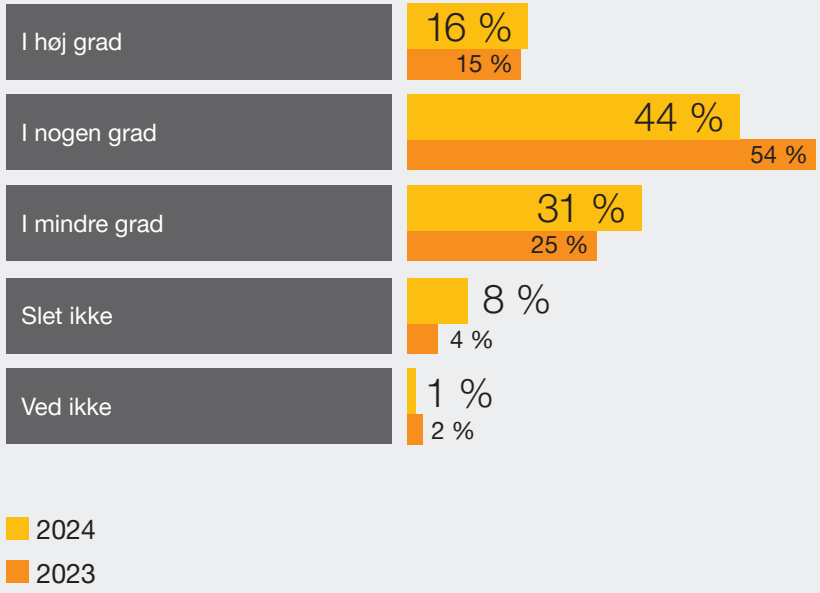


Beredskab er en af de højest prioriterede investeringer i forbindelse med cyber- og informationssikkerhed, da bekymringen for cybertrusler er stigende. Alligevel viser undersøgelsen, at ét ud af fire bestyrelsesmedlemmer ikke har overblik over, om virksomheden har testede beredskabs- og kommunikationsplaner på plads til at håndtere potentielle hændelser såsom hackerangreb eller it-nedbrud. Dette udgør en risiko, da manglende forberedelse i sådanne situationer kan få alvorlige konsekvenser.

På trods af betydelige fremskridt er der tydelige områder, hvor der stadig er plads til forbedring. Bedre opfølgning på cyberrisici, øget træning af bestyrelsesmedlemmer og en mere systematisk tilgang til beredskab er afgørende for, at bestyrelsen kan styrke virksomhedens modstandsdygtighed over for cybertrusler. Med den stigende opmærksomhed på cybersikkerhed er der et stærkt fundament at bygge videre på, men også et behov for handling for at lukke de huller, som stadig eksisterer.

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

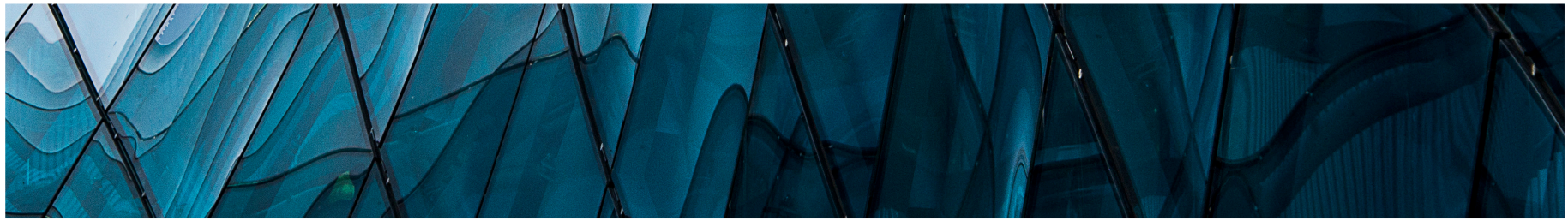
Spørgsmål: I hvilken grad vurderer du, at sammensætningen af bestyrelsens kompetencer giver dyb nok viden om cyber- og informationssikkerhed?

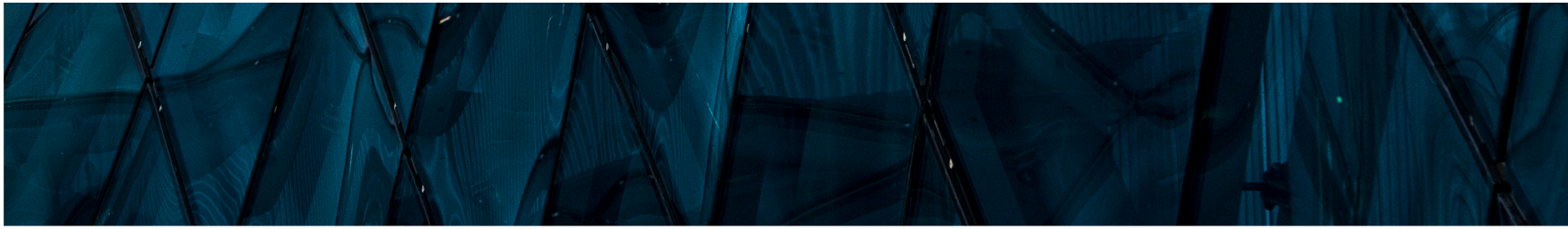


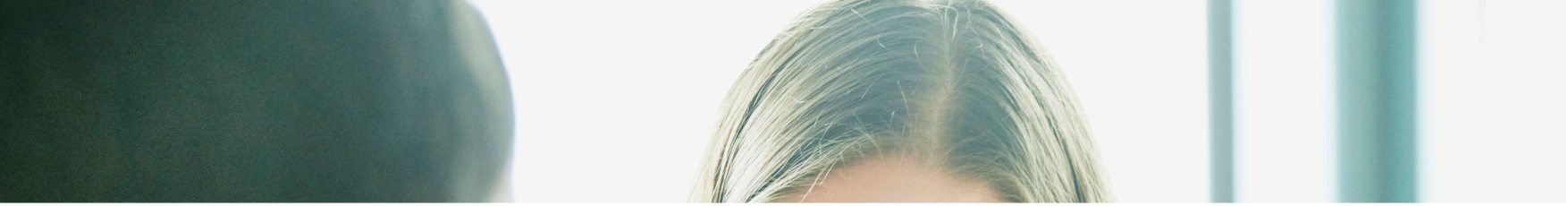
Om undersøgelsen

463 danske topledere, sikkerhedschefer og fagspecialister har deltaget i PwC's Cybercrime Survey 2024. 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.







Få flere tips til cyberberedskabet

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

Læs mere i CFO'ens Cyberguide **her**.

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 denne liste, der kan hjælpe virksomheder med at tage stilling til nogle af de vigtigste indsatsområder inden for cyber- og informationssikkerhed.

Governance, risk og compliance

	Har I etableret et formelt sikkerhedsudvalg med repræsentanter fra virksomhedens topledelse?
	Er øvrige roller for cyber- og informationssikkerhed defineret, allokeret og kommunikeret?
	Arbejder I struktureret med risikovurdering ud fra sikkerhedstrusler, sårbarheder og konsekvens for forretningen?
	Rapporteres virksomhedens sikkerhedsstatus jævnligt/løbende til virksomhedens direktion/bestyrelse?
	Omfatter arbejdet med sikkerhed både informationssikkerhed og cybersikkerhed? Læs mere om ISO 27001 og NIS 2 her.
	Har I implementeret relevante foranstaltninger til overholdelse af GDPR (persondataforordningen)?
	Arbejder I proaktivt med henblik på fortsat overholdelse af kravene i GDPR?

Processer

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

Adfærd

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

Validering

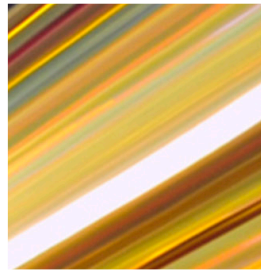
	Gennemfører I løbende test i forhold til identifikation af sårbarheder i jeres infrastruktur og systemer?
	Har I fastlagt og afprøvet en Incident Response-proces? Læs mere her.
	Har I testet jeres beredskabsplaner for cyberhændelser? Læs mere her.

Arkitektur

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

Kontakt

Vi vil meget gerne i dialog med dig om resultaterne fra årets Cybercrime Survey. Kontakt en af PwC's eksperter for en uforpligtende snak om dine konkrete udfordringer og behov. Du kan også læse mere om vores ydelser inden for cyber- og informationssikkerhed her.



Mads Nørgaard Madsen

Partner
Leder af Consulting
T: 2811 1592
E: mads.norgaard.madsen@pwc.com

Christian Kjær

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

Peter Brock Madsen

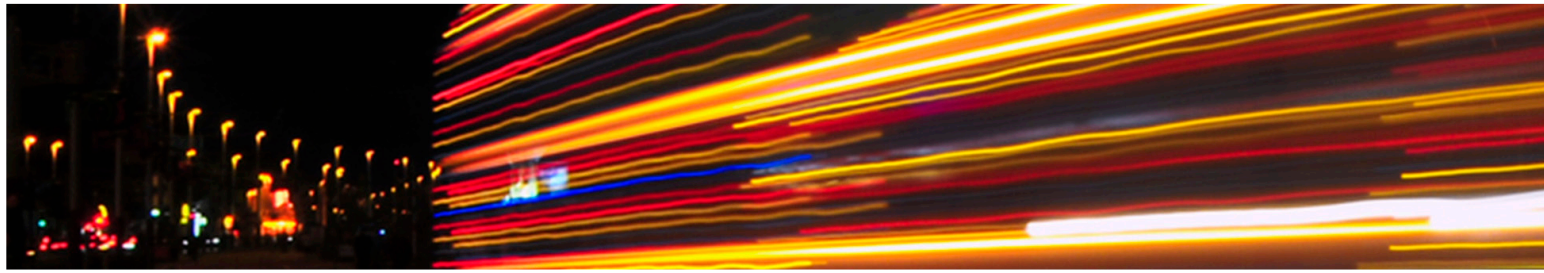
Partner
Cyberrisikostyring
T: 2056 8505
E: peter.brock.madsen@pwc.com

William Sharp

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

Kenneth Studsgaard Pedersen

Partner
Cyberrisikostyring
T: 3136 1073
E: kenneth.studsgaard.pedersen@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 over 3.000 medarbejdere og partnere, som brænder for at gøre en positiv forskel for kunder og kolleger. Globalt er vi 370.000 PwC'ere i 149 lande, og i Danmark er vi markedsledende.

Succes skaber vi sammen …

Cyber Incident Response-team

PwC's cyberhotline

70 222 444

Du kan også læse mere **her**.

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.