Cybercrime Survey 2021

62 %

forventer en stigning i deres cyber- og informationssikkerhedsbudget inden for de næste 12 måneder.

78 %

angiver, at organiserede kriminelle udgør den største trussel i relation til cyber- og informationssikkerhed.

81 %

af CXO'erne er bekymrede for, at kritiske systemer bliver utilgængelige i længere tid, hvilket er rekordhøjt.

pwc

Revision. Skat. Rådgivning.

Succes skaber vi sammen ...

402 virksomhedsledere, it-chefer og specialister fra danske virksomheder har deltaget i PwC's Cybercrime Survey 2021, 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.

Indhold

Bekymringen for organiserede cyberkriminelle er rekordstor

Cybercrime Survey 2021 viser, at organiserede kriminelle nu udgør den største trussel i relation til cyber- og informationssikkerhed. Hele 78 % af de adspurgte anser således organiserede kriminelle for at være blandt de største cybertrusler, hvilket er den højeste andel nogensinde i Cybercrime Surveyens historie (siden 2015). Center for Cybersikkerhed vurderer da også, at truslen fra cyberkriminalitet er "meget høj" i Danmark, og konstaterer, at de cyberkriminelle udvikler deres kompetencer og begynder at tage nye angrebsmetoder i brug.[1] Det gælder eksempelvis bagmændene bag ransomware-angreb, der i stigende grad anvender avancerede angrebsteknikker. De kriminelle hackere udfører ikke alene "klassiske" ransomware-angreb med kryptering af virksomheders data, men er derudover begyndt at stjæle data, hvorefter de kan true virksomheder og personer yderligere med at lække de stjålne følsomme oplysninger, såfremt en løsesum ikke bliver betalt.

Avancerede cyberangreb, du ikke vil udsættes for

Der er i de seneste år set eksempler på nogle af historiens mest avancerede angreb. I 2020 blev en amerikansk it-sikkerhedsvirksomhed således udsat for et angreb i forsyningskæden (supply chain attack), hvor cyberkriminelle implementerede ondartet kode (malware) i en opdatering til et kundevendt softwaresystem. Dette gav hackerne mulighed for at spionere mod en lang række samfundskritiske virksomheder og organisationer, hvor alle virksomheder, som havde kørt softwareopdateringen, var sårbare. I 2021 fandt endnu et avanceret angreb sted. Også denne gang var det mod en stor virksomhed, at en hackergruppe udnyttede et sikkerhedshul i et kundevendt mailsystem. Virksomheden var ikke bekendt med dette sikkerhedshul, før angrebet fandt sted – en ægte såkaldt zero-day vulnerability. Dette angreb åbnede ligeledes en bagdør for adgang til følsomme oplysninger fx alle mails og kalenderoplysninger. Disse nye avancerede former for angreb sætter såvel erhvervslivet som samfundet under pres, når tusinder, hvis ikke millioner, af virksomheder er sårbare på samme tid. PwC erfarer da også, at markant flere virksomheder er bekymrede for at blive udsat for et sådant angreb. Dette understøttes af, at PwC's incident response-team flere gange har måttet etablere et decideret beredskab for at kunne kontakte mere end 1.000 sårbare danske virksomheder inden for meget kort tid.

Det er tidligere set, at medieomtale af cyberhændelser eller selvoplevede angreb har medført større investeringer i cybersikkerhed, fordi virksomhederne er blevet bekendt med de fatale konsekvenser heraf, fx negativ indvirkning på omdømmet eller økonomien. Nu ser vi i højere grad, at virksomheder selv begynder at investere i sikkerhedsforanstaltninger, før angreb finder sted. PwC erfarer desuden, at flere og flere virksomheder – for at mitigere cybertruslen – begynder at investere i flerårige transformationssikkerhedsprogrammer og etablere sikkerhedsteknologier, der giver reel sikring af virksomhedens kritiske aktiver.

Cybersikkerhed har et skærpet fokus i topledelsen

Det er en forudsætning, at der er en fokuseret og prioriteret indsats fra ledelsen, før virksomheden kan implementere de rette effektive sikkerhedstiltag. Derfor er det positivt, at hele 8 ud af 10 (80 %) af de adspurgte vurderer, at direktionen/ledelsen fokuserer på at opnå den rette balance mellem cybertrusler og investeringer i cybersikkerhed.

Vi ser dog samtidig, at der er plads til forbedring, når det kommer til kommunikation og/eller sikkerhedsrapportering på tværs af ledelseslag fra den ansvarlige sikkerhedsafdeling til direktion og bestyrelse. Denne kommunikationsudfordring vanskeliggør en effektiv og tilstrækkelig forståelse af sikkerhedsudfordringerne i ledelserne, og dermed kan der være en risiko for, at den nødvendige indsats ikke prioriteres på korrekt vis.

Det er derfor afgørende, at topledelse og bestyrelse i arbejdet med cyberstrategien får implementeret en fast praksis for rapportering og kommunikation om det aktuelle trusselsbillede, hændelser, prioriterede tiltag mv. Dette er med til at skabe en helhedsorienteret cyberstrategi, hvor man både internt og eksternt kan være tryg ved sikkerhedshåndteringen. For cybersikkerhed handler blandt andet om at skabe tillid til, at omverdenen trygt kan handle og indgå i relationer med virksomheden. Denne tillid er et aktiv, som virksomhederne bør værne omhyggeligt om.

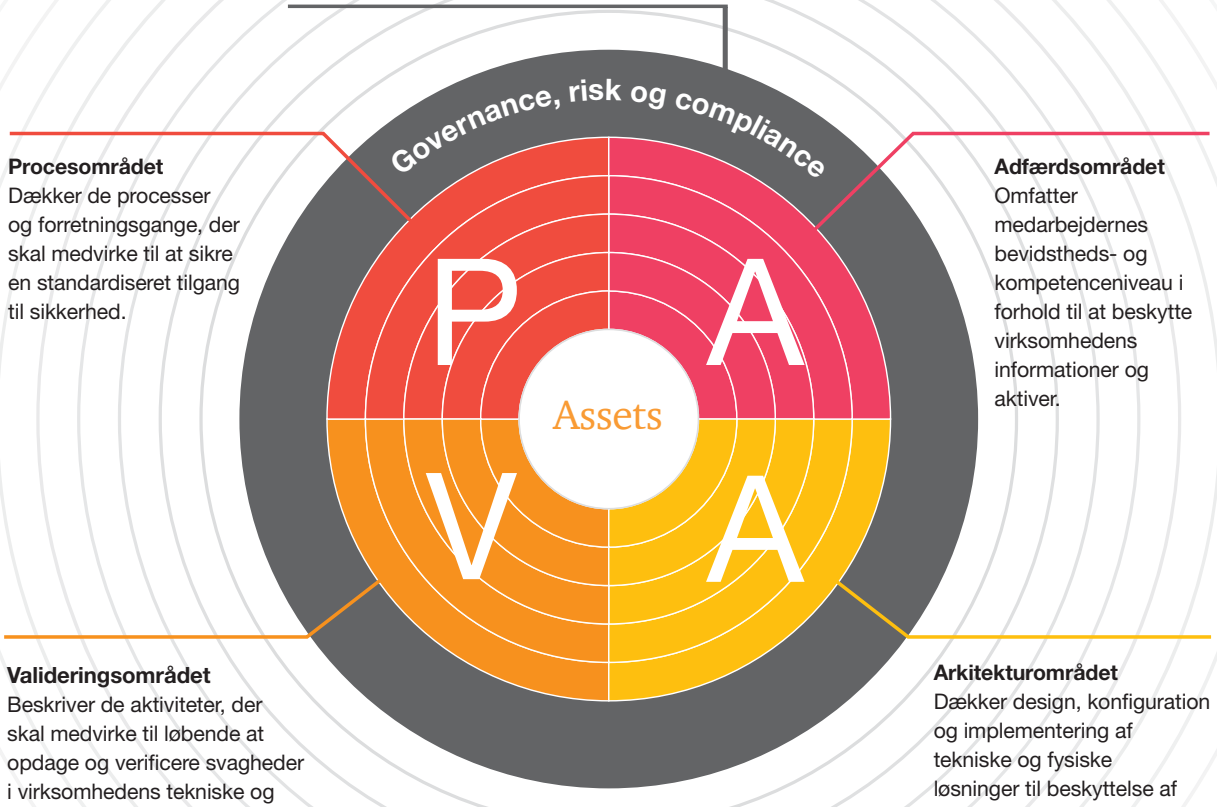
Mads Nørgaard Madsen
Partner
Technology & Security

1) https://cfcs.dk/da/cybertruslen/trusselsvurderinger/cybertruslen-mod-danmark/

PAVA
– et forståeligt sikkerhedskoncept

Undersøgelsesresultatet er igen i år struktureret ud fra PwC's PAVA-koncept. Vi har erfaring med, at dette koncept 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 kan 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 denne kompleksitet, samtidig med at der kan skabes klare fokusområder til brug for 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 og 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.

Governance, risk og compliance-området
Er de styringsrammer, som virksomheden har eller bør etablere for at sikre en risikostyret prioritering af sikkerhedstiltag samt for at overholde gældende love og regler.



Procesområdet
Dækker de processer og forretningsgange, der skal medvirke til at sikre en standardiseret tilgang til sikkerhed.

Adfærdsområdet
Omfatter medarbejdernes bevidstheds- og kompetenceniveau i forhold til at beskytte virksomhedens informationer og aktiver.

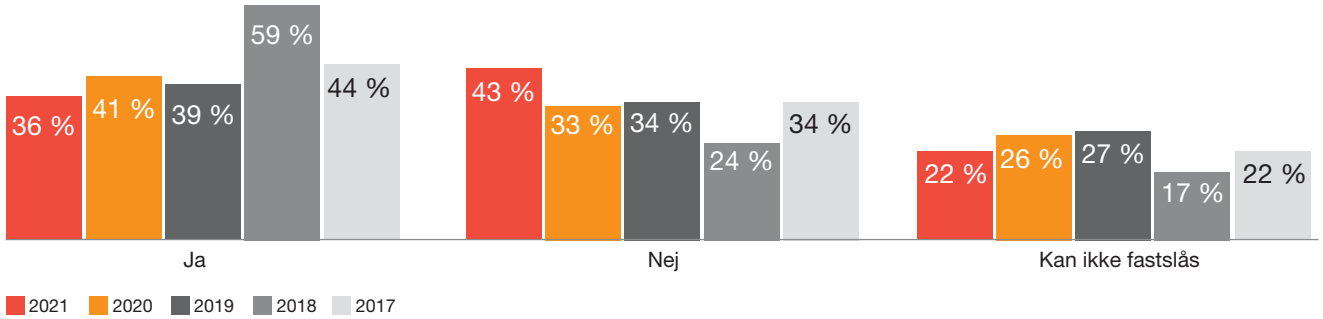
Valideringsområdet
Beskriver de aktiviteter, der skal medvirke til løbende at opdage og verificere svagheder i virksomhedens tekniske og organisatoriske kontroller.

Arkitekturområdet
Dækker design, konfiguration og implementering af tekniske og fysiske løsninger til beskyttelse af forretningens aktiver.

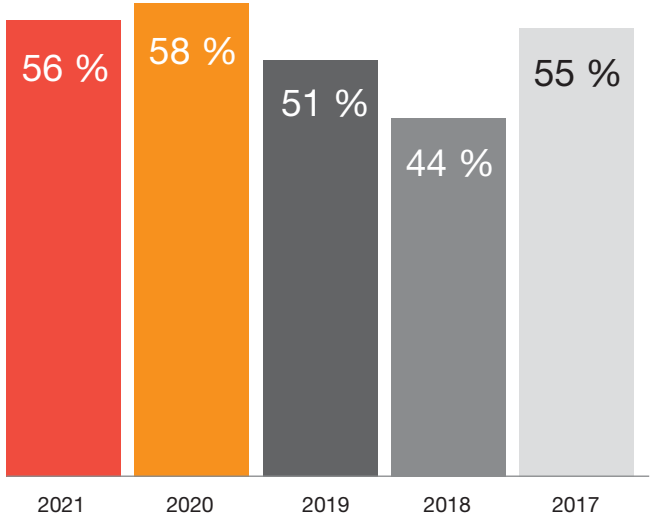
Hver anden virksomhed har oplevet mindst én sikkerhedshændelse

Cybercrime Survey 2021 svarer mere end hver anden (56 %), at deres virksomhed har været udsat for mindst én sikkerhedshændelse inden for den seneste regnskabsperiode. Dette er nogenlunde på niveau med 2020 (58 %). Undersøgelsen viser desuden, at mere end hver tredje i 2021 (36 %) har oplevet én eller flere sikkerhedshændelser, der var målrettet deres virksomhed, hvilket er et lille fald i forhold til 2020 (41 %). Virksomhederne er fortsat bekymrede for cybertruslen, og mere end hver anden (54 %) svarer i 2021, at de er mere bekymrede for cybertruslen i dag, end de var for 12 måneder siden.

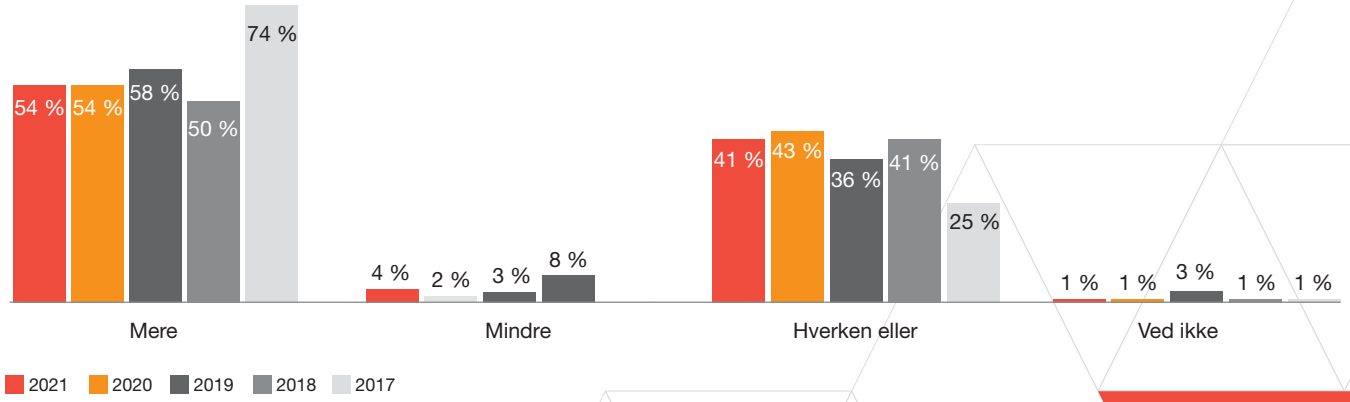
Har I i din virksomhed oplevet en eller flere sikkerhedshændelser, der var målrettet din virksomhed?



Har været udsat for mindst én hændelse



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



Fortsat stor tillid til den finansielle sektors data- og cybersikkerhed

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

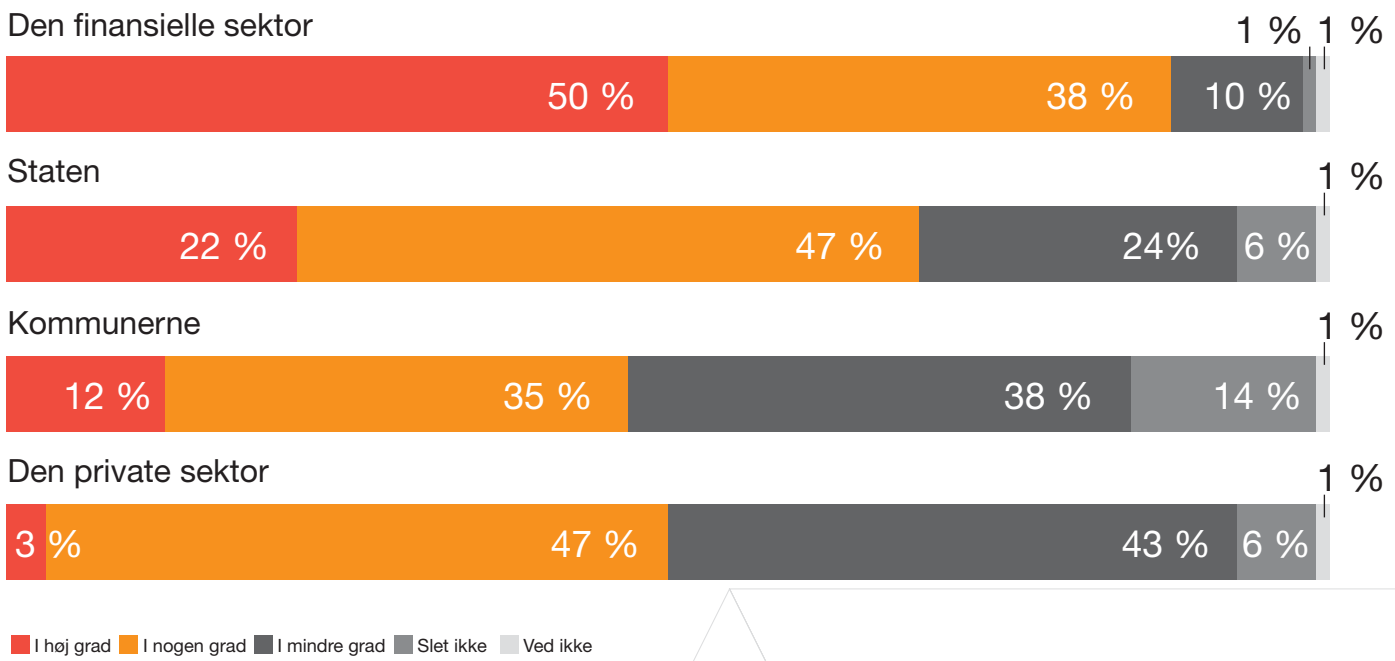
Cybercrime Survey 2021 viser, at tilliden til den finansielle sektors GDPR-compliance fortsat er den største, når vi sammenligner på tværs af sektorer. Således svarer næsten 9 ud af 10 (88 %) af de adspurgte, at de i nogen eller i høj grad har tillid til GDPR-compliance-niveauet i den finansielle sektor, hvilket er på højde med året før.

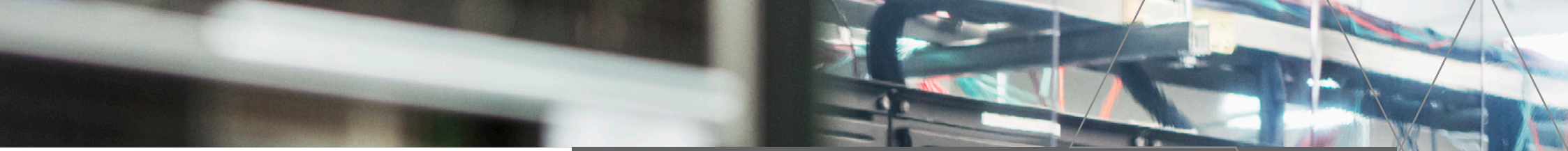
Ca. 7 ud af 10 (69 %) svarer, at de i nogen eller høj grad har tillid til statens håndtering af GDPR-compliance, hvilket er en stigning i forhold til 2020 (64 %).

Når vi ser på tilliden til kommunernes GDPR-compliance, er der fortsat et pænt potentiale for forbedring. I 2021 har 47 % således i nogen eller i høj grad tillid til GDPR-compliance-niveauet i kommunerne, hvilket er en lille fremgang i forhold til 2020 (42 %). Dog er det værd at fremhæve, at hele 38 % i mindre grad har tillid til kommunernes GDPR-compliance-niveau, og at 14 % ingen tillid har til denne sektors håndtering af GDPR-compliance.

For den private sektor er der ligeledes plads til forbedring, idet 50 % svarer, at de i nogen eller i høj grad har tillid til denne sektors GDPR-håndtering, mens hele 43 % svarer "i mindre grad".

I hvilken grad har du tillid til GDPR-compliance-niveauet i

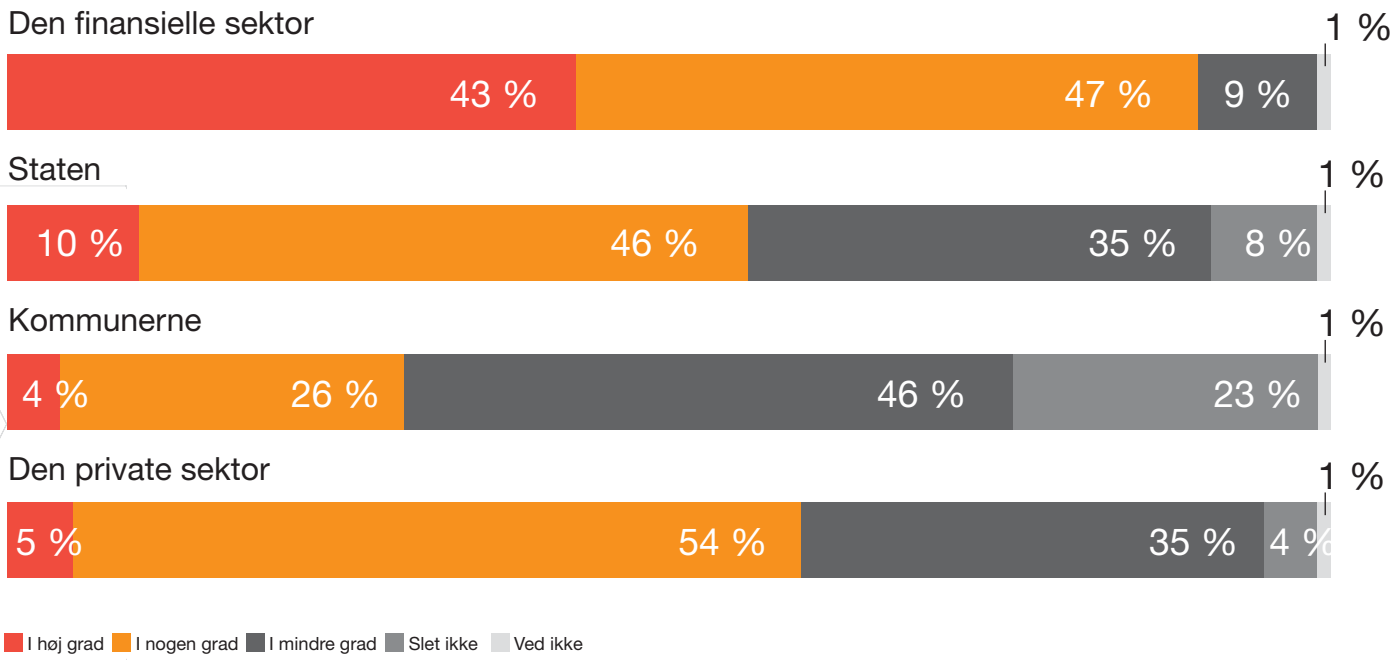




For så vidt angår tilliden til cybersikkerhed, er billedet på tværs af sektorerne stort set uændret i forhold til 2020. Der er fortsat størst tillid til cybersikkerheden i den finansielle sektor, da hele 90 % af de adspurgte svarer, at de i nogen eller i høj grad har tillid til cybersikkerheden i den finansielle sektor (89 % i 2020). Tilliden til kommunernes cybersikkerhed er fortsat mindst. Kun 30 % svarer således, at de i nogen eller i høj grad har tillid til cybersikkerheden i kommunerne (31 % i 2020).

PwC anbefaler: Tillid er vigtig for både mennesker, organisationer og virksomheder for at kunne udvikle sig og skabe relationer. En organisation eller virksomhed, der vækker tillid, vil alt andet lige være bedre til at skabe relationer med kunder, medarbejdere og sin omverden end en organisation eller virksomhed, der ikke vækker tillid. Cybersikkerhed kan medvirke til at skabe tillid til virksomhedens håndtering af data. PwC anbefaler derfor, at virksomheder sikrer en korrekt og sikker datahåndtering.

I hvilken grad har du tillid til cybersikkerheden i



PAVA

Governance, risk og compliance

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

Bestyrelse

Cybercrime Survey 2021 viser, at kun 15 % af de bestyrelsesmedlemmer, der har besvaret surveyen, angiver, at sammensætningen af bestyrelsens kompetencer i høj grad giver dyb nok viden om cyber- og informationssikkerhed. Yderligere angiver 61 % at bestyrelsen ikke modtager træning i cyber- og informationssikkerhed. Dette er dog en klar forbedring i forhold til 2020, hvor hele 89 % angav, at der ikke var etableret et cybertrænings- og uddannelsesprogram for bestyrelsen.

Topledelsen er mere bekymrede for konsekvenserne af cyberhændelser

Cybersikkerhed kræver forståelse og prioritering i virksomhedens topledelse, så virksomheden er i stand til at implementere de rette effektive sikkerhedstiltag på baggrund af en risikovurdering.

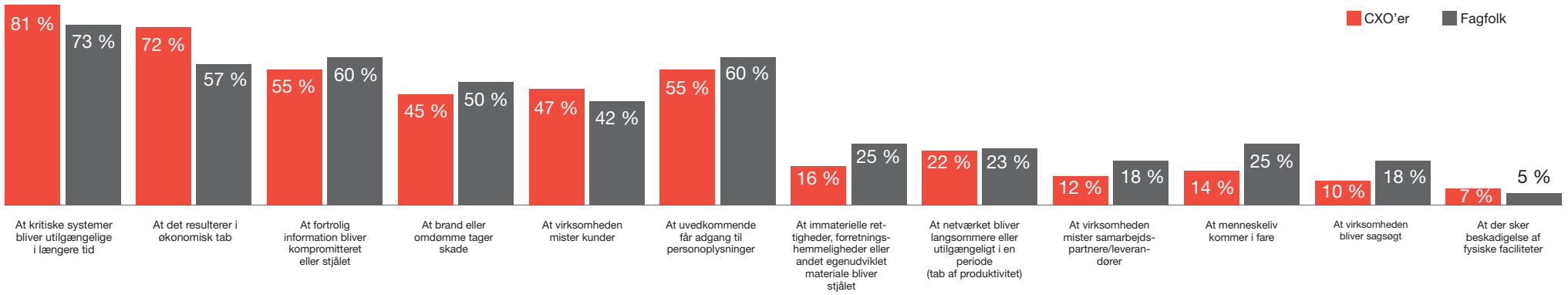
I dette års undersøgelse peger flere CXO'er[2] på, at de er bekymrede for konsekvenserne ved en sikkerhedshændelse. Den primære bekymring i år – både blandt CXO'er og fagfolk[3] – er, at kritiske systemer bliver utilgængelige i længere tid. Dette var også tilfældet i 2020. I år angiver hele 81 % af CXO'erne, at de er bekymrede for, at kritiske systemer bliver utilgængelige i længere tid, hvilket er en stigning på 11 %-point i forhold til 2020.

Der er ligeledes sket en stigning fra sidste år i andelen af CXO'er, der er bekymrede for sikkerhedshændelser, som fx resulterer i, at virksomheden lider et økonomisk tab, at fortrolig information bliver kompromitteret eller stjålet, eller at uvedkommende får adgang til personoplysninger. Disse emner ligger også højest på fagfolkenes liste over bekymringer.

2) Inkluderer stillingsbetegnelserne CEO, CFO, CIO, CCO, CTO mv.
3) Inkluderer stillingsbetegnelserne CISO, sikkerhedsmedarbejdere, sikkerhedsspecialister og øvrige medarbejdere.

PwC anbefaler: Ledelsens opmærksomhed vil fortsat være nødvendig i arbejdet med at prioritere, motivere og sponsorere bekæmpelsen af cyberkriminaliteten således, at virksomhedens kritiske aktiver ikke mistes eller bliver utilgængelige i længere tid. Der er stadig behov for, at virksomhederne lægger en flerårig plan for styrkelse af cybersikkerheden.

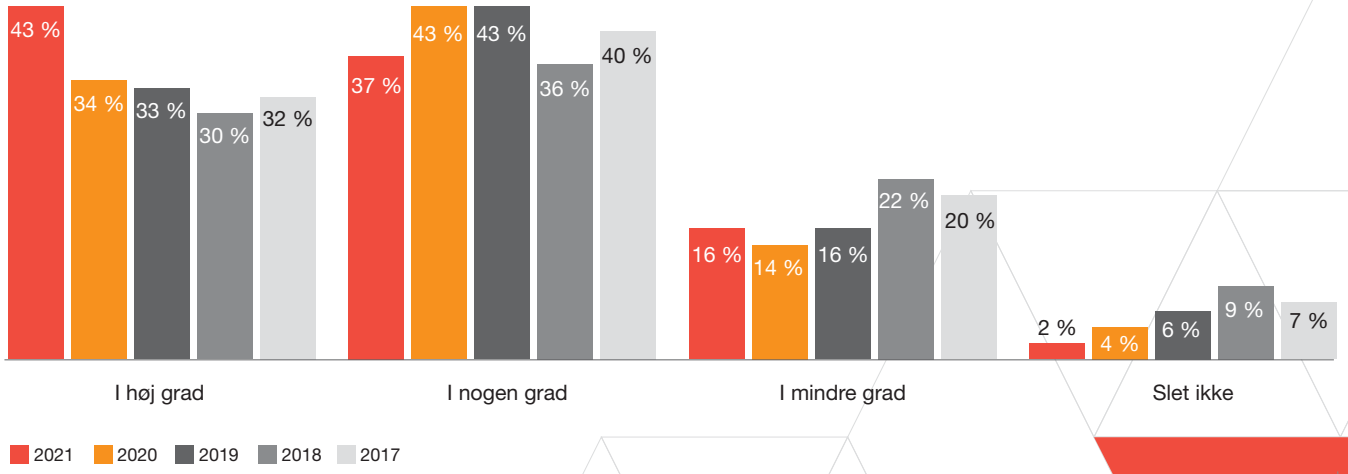
Hvad er din virksomheds største bekymring i relation til konsekvenserne af en cyberhændelse?



Hver fjerde (24 %) af de adspurgte mente i 2020, at topledelsens manglende forståelse udgjorde en trussel for virksomheden. At topledelsen i år er mere bekymrede for og bevidste om konsekvenserne ved cyberhændelser, kan have ændret dette billede. Således svarer kun 16 % i 2021, at topledelsens manglende forståelse udgør en trussel for virksomheden (se graf på side 18).

80 % mener i 2021, at direktionen/ledelsen i nogen eller i høj grad har fokus på at opnå den rette balance mellem cybertrusler og investeringer i cybersikkerhed (77 % i 2020). Den positive udvikling bliver endnu mere tydelig, når vi kun ser på andelen, der besvarer spørgsmålet med "i høj grad". Hele 43 % vurderer således i 2021, at deres ledelse i høj grad har fokus på at opnå den rette balance, hvilket er en fremgang på 9 %-point i forhold til 2020.

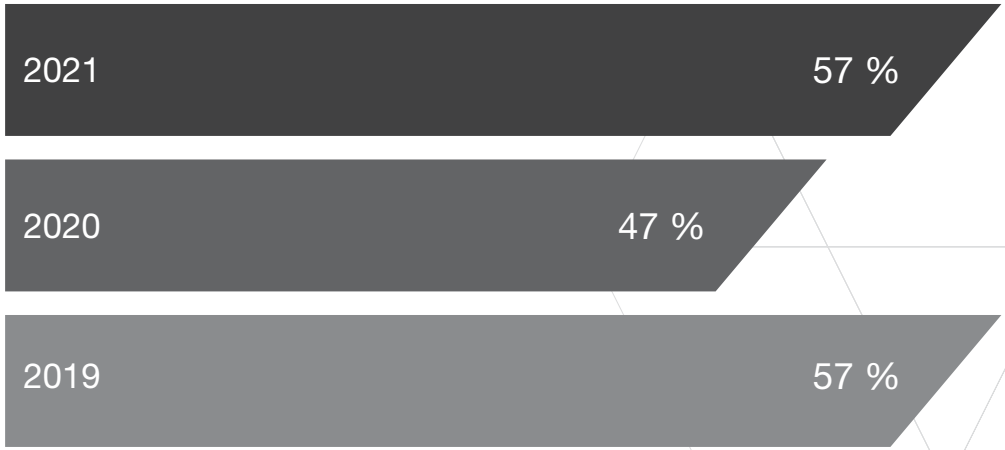
I hvilken grad har direktionen/ledelsen i din virksomhed, efter din opfattelse, fokus på at opnå den rette balance mellem de cybertrusler, I står over for, og investeringer i cybersikkerhed?



Fokus på beskyttelse af personoplysninger er øget markant

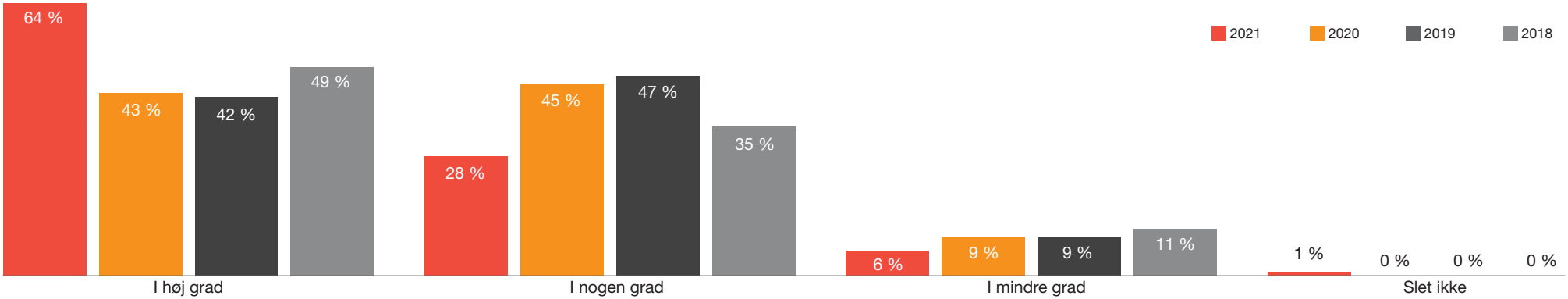
Over halvdelen (57 %) af respondenterne angiver i år, at en af deres store bekymringer i relation til konsekvenserne af en cyberhændelse er, "at uvedkommende får adgang til personoplysninger". Der er således sket en betydelig stigning fra 47 % i 2020.

Andel, der har angivet en bekymring for, at uvedkommende får adgang til personoplysninger:

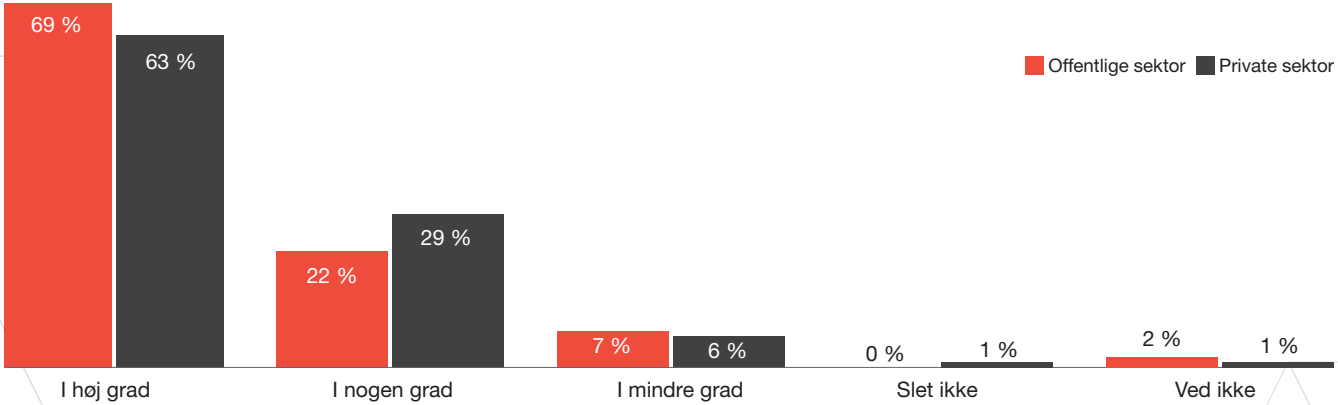


Vi ser yderligere, at virksomhederne har et øget fokus på at beskytte personoplysninger i henhold til GDPR. Således svarer 9 ud af 10 (92 %) af de adspurgte, at deres virksomhed i nogen eller i høj grad beskytter personoplysninger i henhold til GDPR. Andelen, der svarer "i høj grad", er steget fra 43 % i 2020 til hele 64 % i år, hvilket er rekordhøjt.

I hvilken grad beskytter din virksomhed personoplysninger i henhold til persondataforordningen (GDPR)?



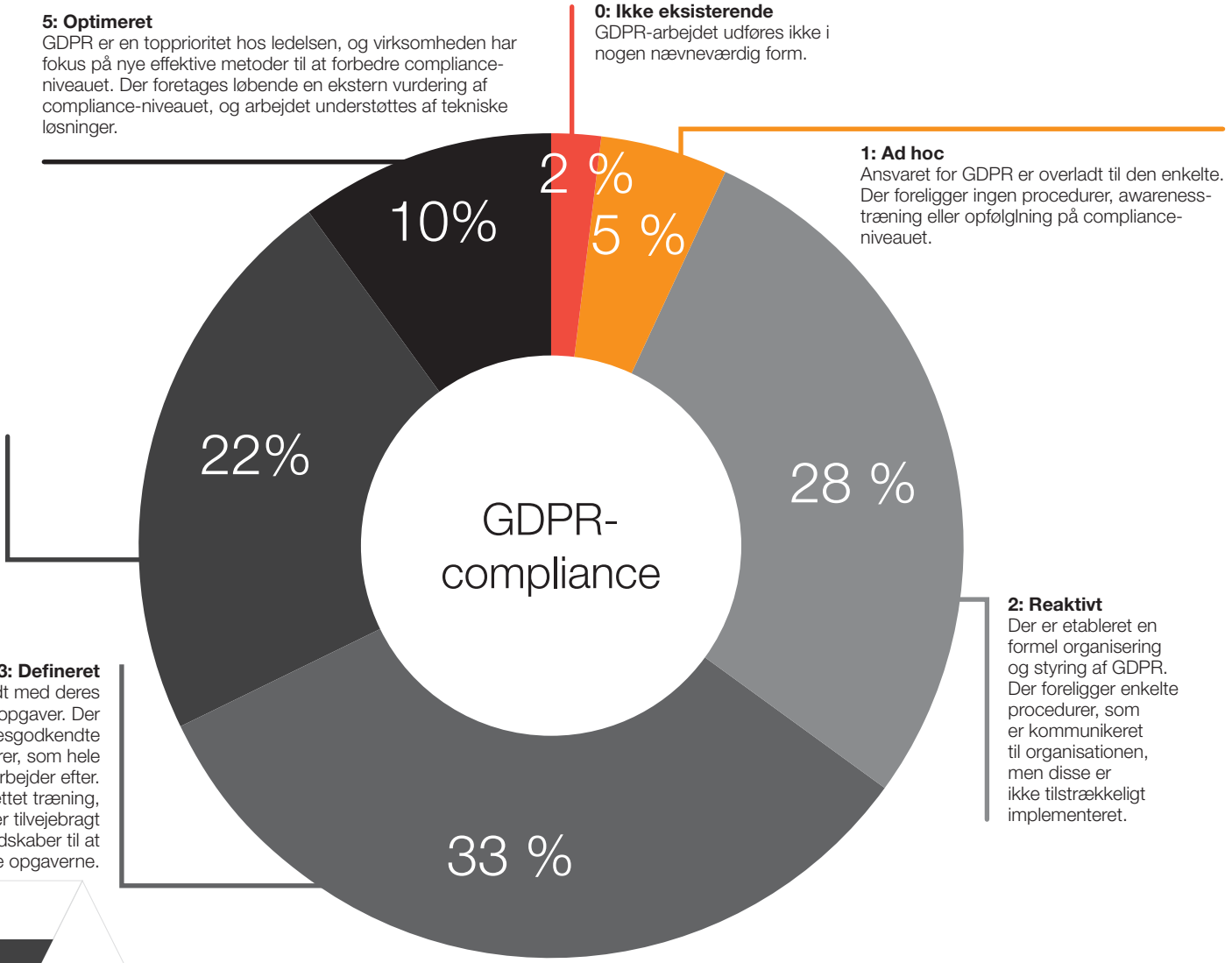
Der er både i den offentlige og private sektor en vurdering af, at man beskytter personoplysninger i henhold til GDPR. Den offentlige sektor vurderer sig dog en anelse bedre sammenlignet med den private sektor. Således mener 69 % af respondenterne fra den offentlige sektor, at deres organisation i høj grad beskytter personoplysninger i henhold til GDPR, mens det for den private sektors vedkommende er 63 %.



Når PwC assisterer virksomhederne med at vurdere deres niveau af GDPR-compliance, anvender PwC's GDPR-eksperter en skala fra 0-5, hvor 5 er bedst (se figur).

28 % af respondenterne angiver, at virksomhedens GDPR-compliance-niveau er reaktivt (niveau 2). Positivt set angiver over halvdelen (55 %) af de adspurgte, at deres GDPR-compliance-niveau er "Defineret" eller "Kvantitativt styrende" (henholdsvis niveau 3 og 4).

Hvordan vurderer du din virksomheds GDPR-compliance-niveau?



Det er PwC's erfaring, at de fleste organisationer er reaktive (niveau 2) og vurderer compliance-niveauet højere, end det reelt er. PwC anbefaler derfor, at det reelle GDPR-compliance-niveau vurderes og gennemgås af uafhængige eksterne parter mindst én gang årligt. GDPR indebærer en lang række lovpligtige dokumenter, men "papirskjoldet" er ikke tilstrækkeligt for at efterleve GDPR. Et højt compliance-niveau kræver, at alle procedurerne bliver implementeret i forretningen og indarbejdet som en del af de faste forretningsprocesser.

PwC vurderer, at den øgede indsats vedrørende beskyttelse af personoplysninger særligt skyldes to forhold. Dels er kunder og borgere blevet mere opmærksomme på databeskyttelse og deres rettigheder, og dels har Datatilsynet offentliggjort en række indstillinger til politianmeldelser, hvor især brud på persondatasikkerheden, som skal anmeldes til Datatilsynet, ofte medfører en større granskning af virksomhedernes behandlingssikkerhed, som kan føre til alvorlige sager hos tilsynet.

PAVA

Proces

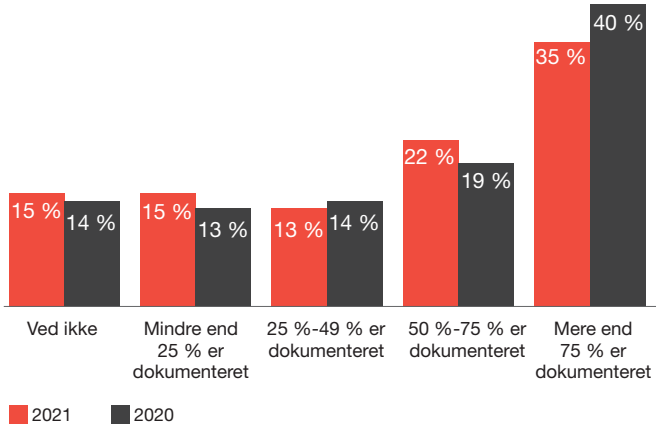
Virksomhederne arbejder fortsat med at dokumentere sikkerheds- og lovgivningskrav

Ligesom sidste års Cybercrime Survey viser dette års undersøgelse, at virksomhederne fortsat arbejder med at dokumentere sikkerheds- og lovgivningskrav. Dette arbejde skal bidrage til, dels at interne procedurer og retningslinjer bliver forankret og efterlevet i virksomheden, og dels at virksomheder kan dokumentere, at de efterlever gældende krav fra myndigheder og kunder.

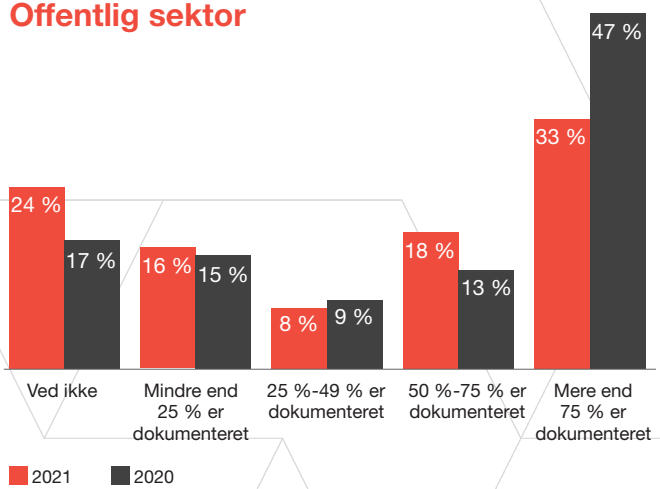
Lidt over halvdelen (57 %) af de adspurgte angiver i år, at mere end 50 % af deres processer er dokumenteret, hvilket er omtrent på niveau med 2020 (59 %). Sammenlignet med sidste år er der sket et lille fald i andelen, der angiver, at "mere end 75 % er dokumenteret".

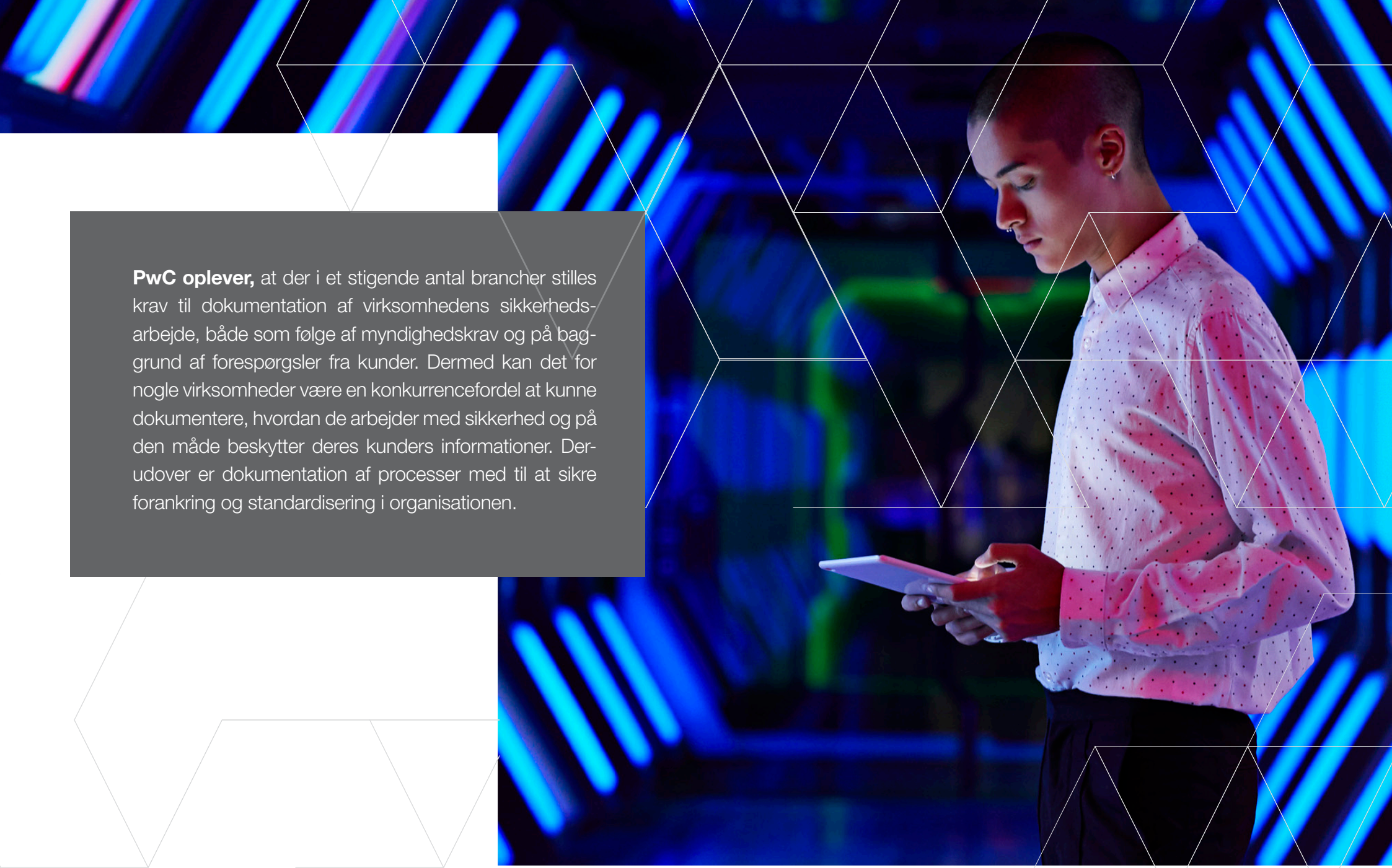
Faldet skyldes bl.a., at færre i den offentlige sektor i 2021 vurderer, at mere end 75 % af deres processer er dokumenteret. Således svarede knap halvdelen (47 %) af de adspurgte i den offentlige sektor i 2020, at mere end 75 % var dokumenteret. I 2021 er det blot hver tredje.

I hvilket omfang er sikkerheds- og lovgivningskrav dokumenterede i jeres virksomheds interne retningslinjer, procedurer og/eller vejledninger?



Offentlig sektor





PwC oplever, at der i et stigende antal brancher stilles krav til dokumentation af virksomhedens sikkerheds-arbejde, både som følge af myndighedskrav og på bag-grund af forespørgsler fra kunder. Dermed kan det for nogle virksomheder være en konkurrencefordel at kunne dokumentere, hvordan de arbejder med sikkerhed og på den måde beskytter deres kunders informationer. Der-udover er dokumentation af processer med til at sikre forankring og standardisering i organisationen.

PAVA

Adfærd

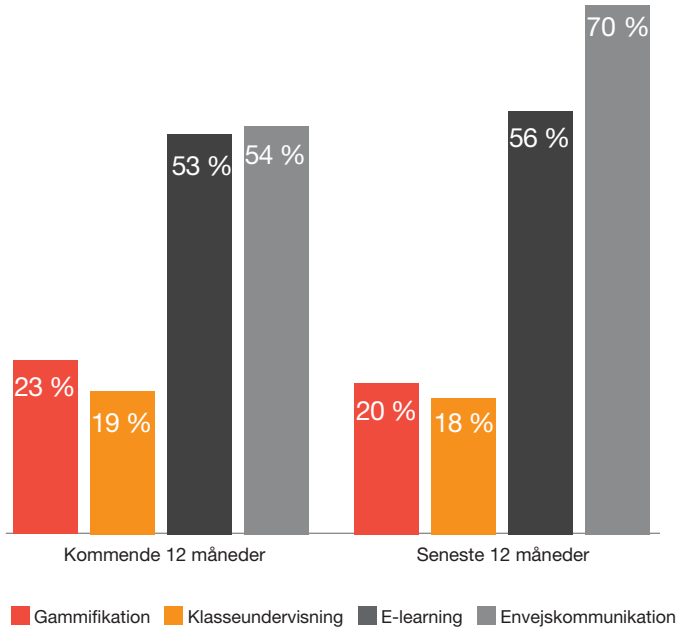
Virksomheder har fokus på træning af medarbejdere

Awareness-træning skal bidrage til at gøre virksomhedens medarbejdere opmærksomme på de digitale trusler og risici, som kan have konsekvenser for enten virksomheden, kunder eller borgere.

I årets survey svarer 7 ud af 10 af de adspurgte, at de i de seneste 12 måneder har benyttet sig af envejskommunikation for at skabe awareness inden for cyber- og informationssikkerhed. I de kommende 12 måneder er det dog kun 54%, som forventer at benytte envejskommunikation.

Et tiltag, som har stigende interesse hos virksomhederne, er gamification. 23 % af de adspurgte svarer, at de i de kommende 12 måneder vil benytte sig af dette tiltag, hvor det i 2020 var 15 %. I løbet af de seneste 12 måneder har 20 % benyttet sig af gamification, hvilket er 5 %-point højere end forventningen i 2020.

Hvilke af følgende tiltag gør din virksomhed brug af i forbindelse med GDPR-, cyber- og informationssikkerheds-awareness?



PwC anbefaler, at virksomheder fortsat prioriterer at træne og uddanne deres medarbejdere i cyber- og informationssikkerhed, så medarbejderne er i stand til at forebygge og opdage, hvis virksomheden er udsat for cyberkriminalitet. Træningen kan fx foregå via e-learnings, hvor medarbejderne bliver aktiveret og får en øget forståelse af cybersikkerhed.

E-learnings fra PwC

PwC har udviklet en række e-learnings om EU's persondataforordning og cybersikkerhed, som på en effektiv og lettilgængelig måde kan træne medarbejdere.

Læs mere på www.pwc.dk/cyberaware

PAVA

Validering

Truslen fra organiserede kriminelle er rekordstor

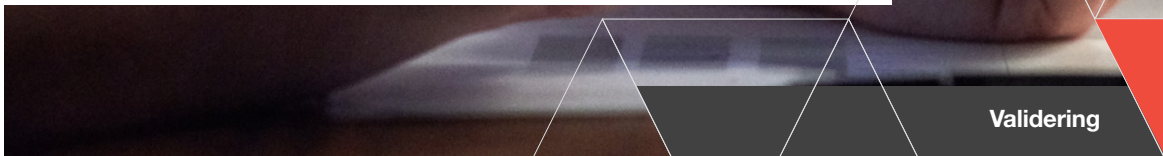
2021 udgør organiserede kriminelle fortsat den største trussel for dansk erhvervsliv.

Hele 78 % af de adspurgte anser nu organiserede kriminelle for at være blandt de største cybertrusler, hvilket er den hidtil største andel i PwC's Cybercrime Survey. Til sammenligning var det i 2020 72 %, og vi har set en støt stigning i andelen de seneste år (fra 55 % i 2017).

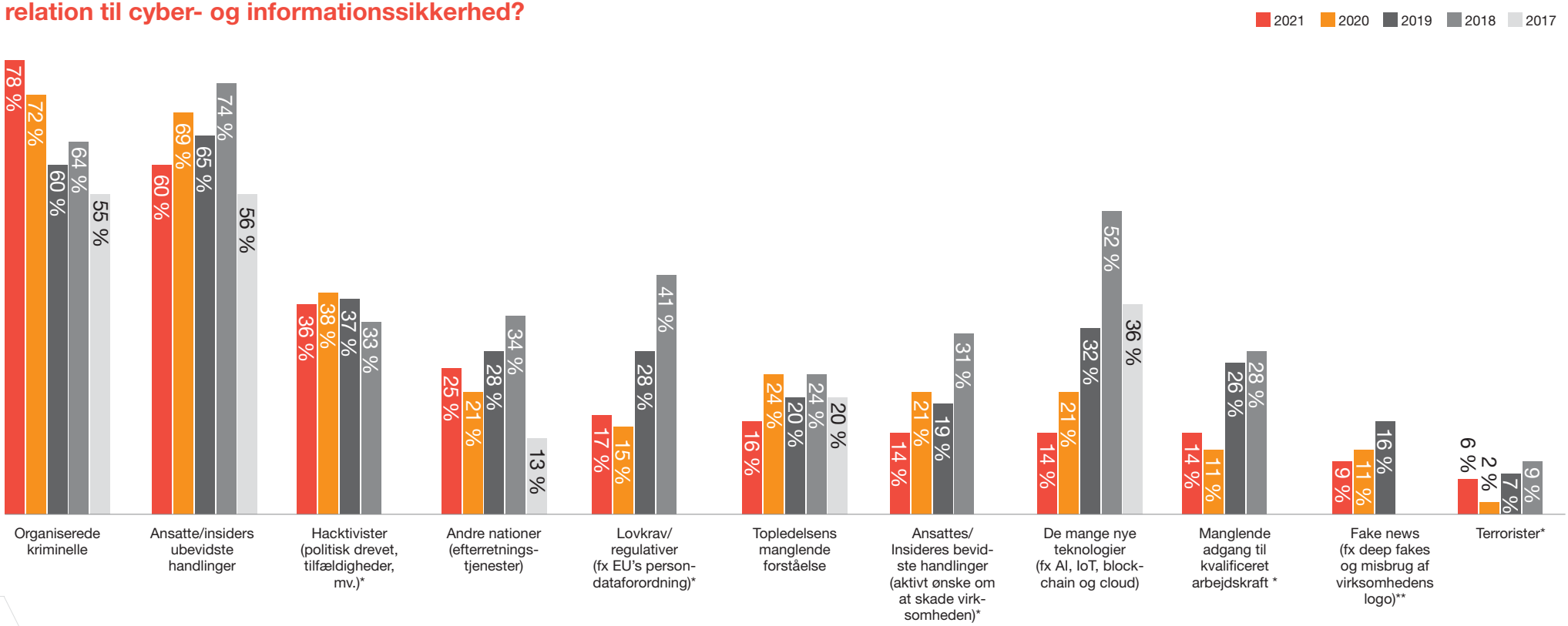
Til gengæld er vurderingen af truslen fra ansattes/insideres ubevidste handlinger faldet med 9 %-point fra 2020 til 2021, hvilket er positivt, set i lyset af at virksomhederne nu for tredje år i træk har awareness-træning som investeringsmæssig topprioritet.

Truslen fra ansattes/insideres ubevidste handlinger er dog stadig reel, hvilket understreges af, at undersøgelsen igen i år viser, at virksomhederne i høj grad bliver udsat for phishingangreb. I 2021 fortæller 78 % af de adspurgte således, at deres virksomhed har oplevet et phishingangreb inden for de seneste 12 måneder.

Det er værd at fremhæve, at færre (fra 38 % i 2020 til 25 % i 2021) angiver, at de har været udsat for en hændelse, hvor følsomme personoplysninger eller anden følsom information utilsigtet er blevet delt. Det kan ligeledes hænge sammen med virksomhedernes kontinuerlige ønske om at prioritere awareness-træning.

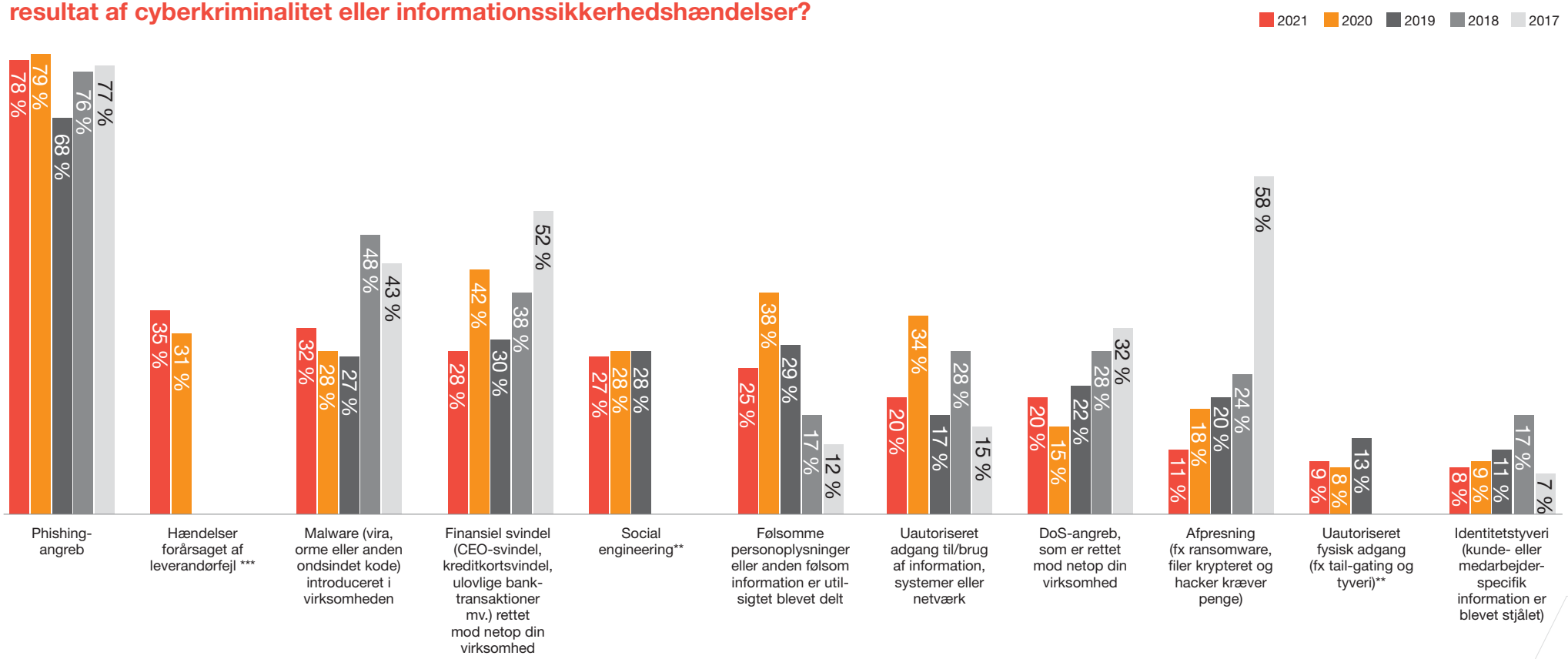


Hvad udgør de største trusler for din virksomhed i relation til cyber- og informationssikkerhed?



*Denne svarmulighed blev tilføjet i 2018.
**Denne svarmulighed blev tilføjet i 2019.

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



**Denne svarmulighed blev tilføjet i 2019.
***Denne svarmulighed blev tilføjet i 2020.

PwC erfarer, at cyberangreb bærer præg af, at de cyberkriminelle agerer stadigt mere professionelt. I hackergrupperne specialiserer de sig og videreudvikler deres angrebsteknikker. Nogle cyberkriminelle er specialiserede i phishingangreb med det mål at skaffe sig adgang til en identitet. Andre er specialiserede i at udføre ransomware-angreb, og hvis de via phishingangrebet kan skaffe sig tilstrækkeligt gode adgangsrettigheder, kan de tilgå kritiske data og systemer.

PAVA

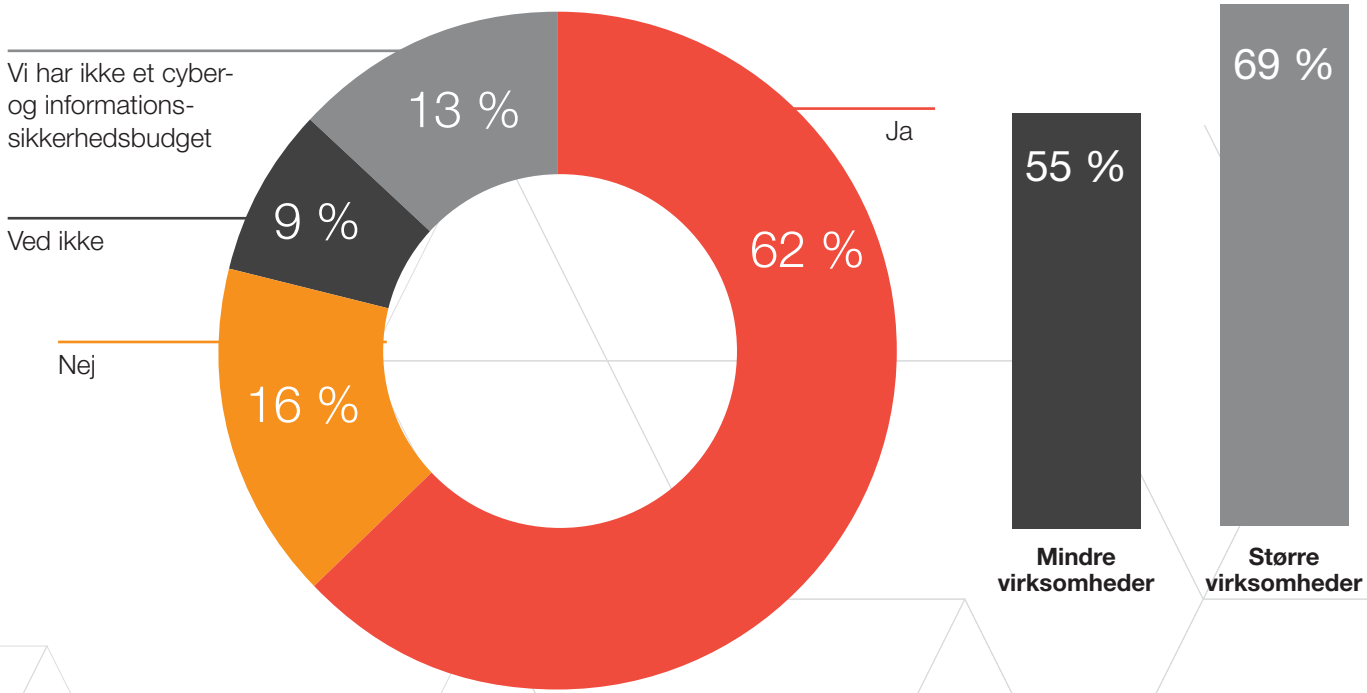
Arkitektur

2 ud af 3 forventer, at deres cybersikkerheds-budget vil stige i løbet af de næste 12 måneder

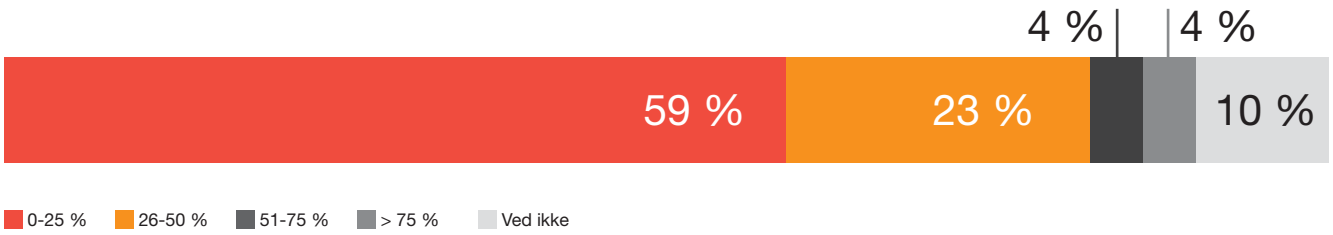
I dette års Cybercrime Survey er der spurgt til virksomhedernes forventninger til fremtidigt cyber- og informationssikkerhedsbudget.

Hele 62 % af de adspurgte svarer, at de i deres virksomhed forventer en stigning i cyber- og informationssikkerhedsbudgettet inden for de næste 12 måneder. 69 % af de større virksomheder forventer, at budgettet vil stige, mens 55 % af de mindre virksomheder ligeledes forventer en stigning i cybersikkerhedsbudgettet.

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



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



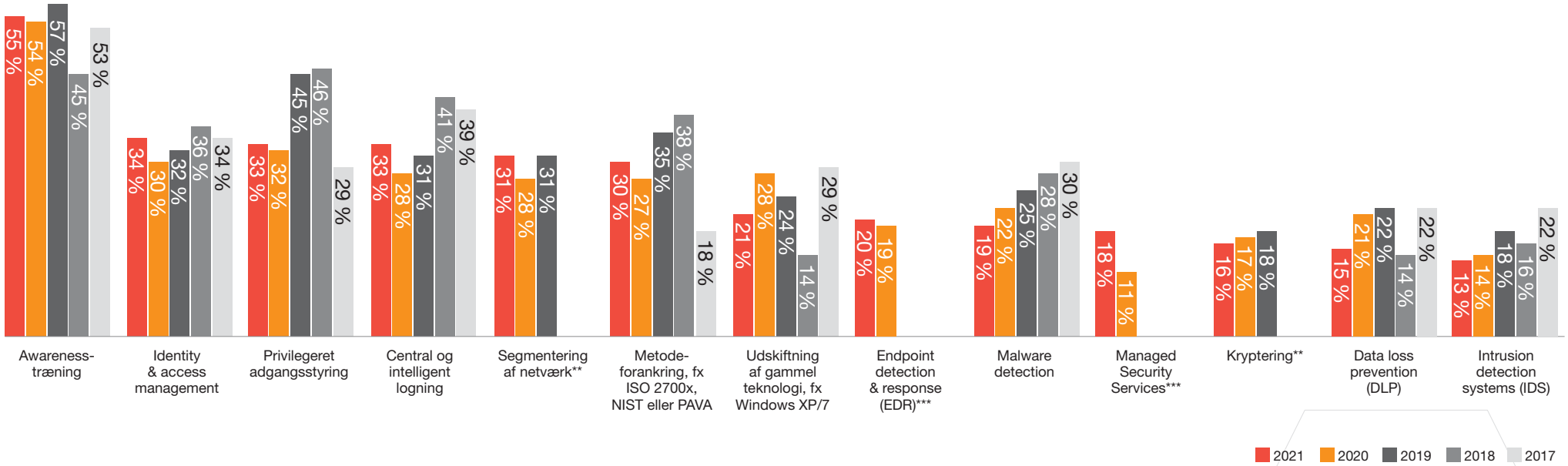
Heraf forventer 6 ud af 10, at budgettet vil stige med op til 25 %, mens 3 ud af 10 forventer en budgetstigning på over 25 %.

Når der spørges nærmere ind til respondenternes prioriterede investeringer inden for cyber- og informationssikkerhed de næste 12 måneder, viser undersøgelsen, at årets højdespringer er awareness-træning (55 %), hvilket ligeledes gjorde sig gældende i de foregående år.

Efter awareness-træning ligger identity & access management[4] (34 %), privilegeret adgangsstyring[5] (33 %) og central og intelligent logning[6] (33 %) på henholdsvis en anden- og en delt tredjeplads, hvilket er meget lig billedet i 2020. Det bemærkes, at disse top-3 investeringer alle er steget siden 2020.

4) Identity & access management (IAM) handler om at strukturere og automatisere alle identiteter i virksomheden, herunder rettidigt at sikre korrekt rettighedstildeling og -fratagelse.
5) Priviligeret adgangsstyring (PAM) handler om at få styr på de privilegerede rettigheder i virksomhedens infrastruktur.
6) Central og intelligent logning handler om, at logs indsamles til en central platform, som efterfølgende bliver analyseret af et automatisk system (fx SIEM).

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



**Denne svarmulighed blev tilføjet i 2019.
***Denne svarmulighed blev tilføjet i 2020.

PwC har gennem de seneste år erfaret, at danske ledelser og bestyrelser i højere grad end tidligere er opmærksomme på risici, som følger af cyberkriminalitet. Det gælder ikke kun større virksomheder, men også mellemstore virksomheder i alle brancher. Opmærksomheden medfører, at der sker en øget investering i dedikerede tiltag, som skal medvirke til at reducere risiciene fra cyberkriminalitet. Desuden etableres der deciderede cyberprogrammer med nøje afstemte og godkendte budgettal.

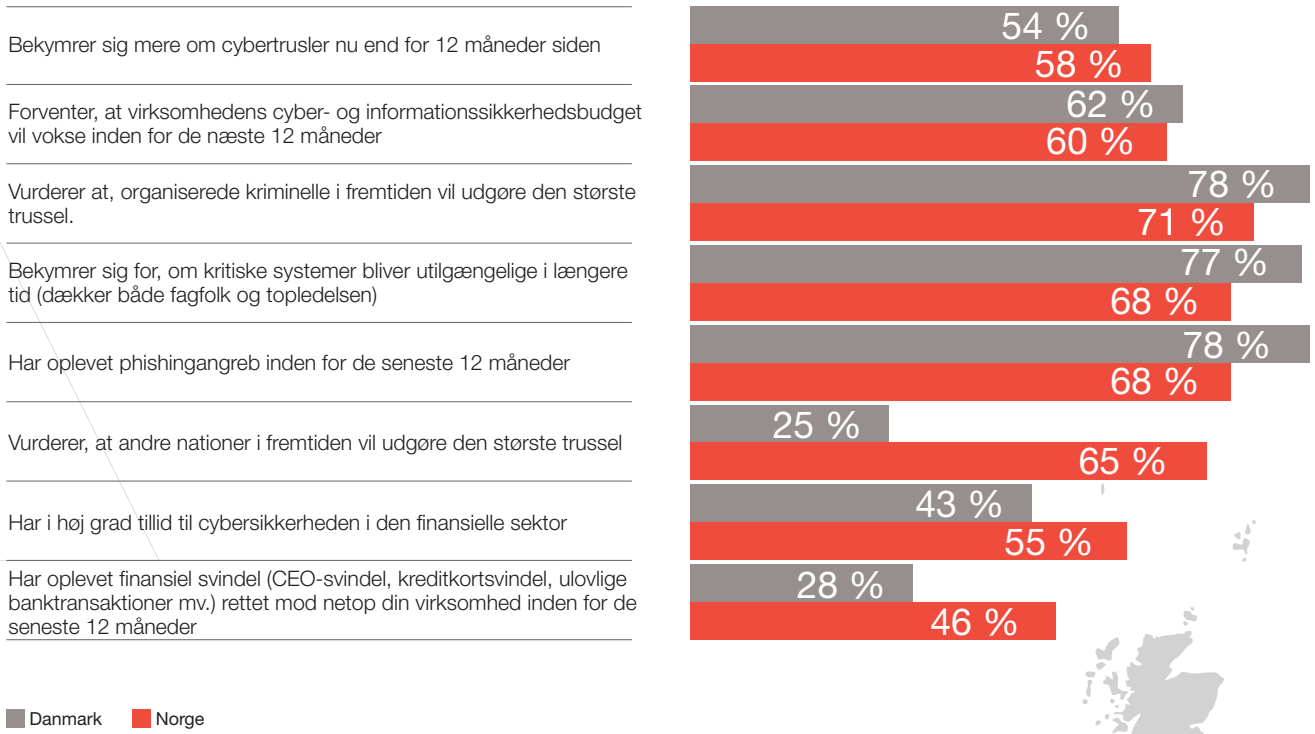
Et norsk perspektiv

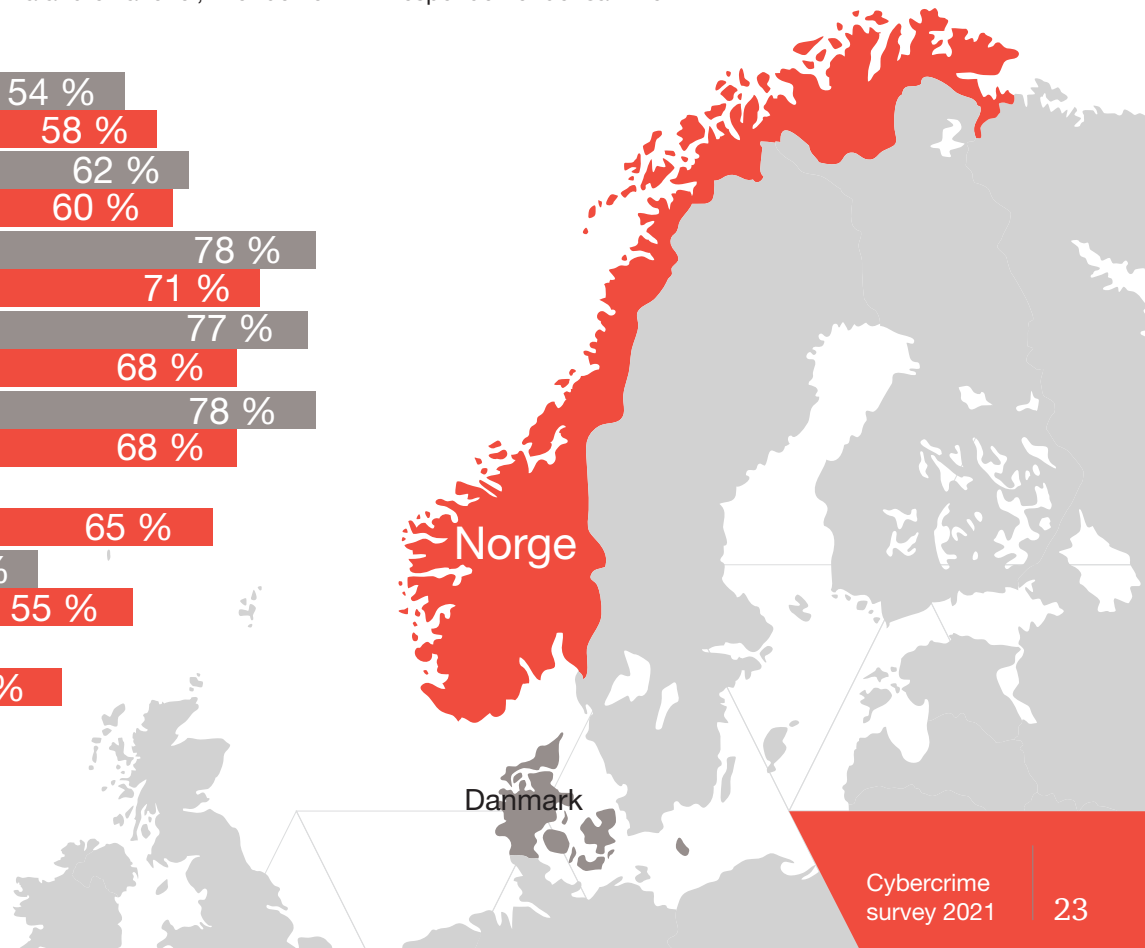
119 norske it-chefer og sikkerhedsspecialister har gennem PwC's Cybercrime Survey 2021 delt deres syn på en række spørgsmål relateret til cybersikkerhed.

Generelt er bekymringen for cybertrusler stigende, og over halvdelen af respondenterne (Danmark: 54 %, Norge: 58 %) angiver, at de er mere bekymrede for cybertrusler i dag, end de var for et år siden – ligesom størstedelen af respondenterne i begge lande forventer en stigning i cybersikkerhedsbudgettet inden for det næste år (Danmark: 62 %, Norge: 60 %). I lighed med trusselsbilledet i Danmark vurderes organiserede kriminelle at udgøre den største trussel i Norge (Danmark: 78 %, Norge: 71 %). Den største bekymring som konsekvens af en cyberhændelse er – ligesom i Danmark – at kritiske systemer bliver utilgængelige i længere tid (Danmark: 77 %, Norge: 68 %).

De danske og norske besvarelser afviger fra hinanden, hvad angår den vurderede trussel fra andre nationer, hvor de norske respondenter angiver denne trussel over 2,5 gang oftere end de danske respondenter (Danmark: 25 %, Norge: 65 %).

Derudover er der forskel på, hvor stor en andel af virksomhederne der har været udsat for finansiel svindel. Knap halvdelen (46 %) af de norske respondenter har været ramt af enten CEO-svindel, kreditkortsvindel, ulovlige banktransaktioner mv. Til sammenligning angiver 28 % af de danske respondenter det samme.





Om undersøgelsen

En stor tak til årets samarbejdspartnere og de virksomhedsledere, it-chefer og sikkerhedsspecialister, der har bidraget til dette års PwC Cybercrime Survey, og som derved er med til at sætte fokus på cybersikkerhed i dansk erhvervsliv og hos offentlige institutioner.

Hele 402 danske og 119 norske virksomhedsledere, it-chefer og sikkerhedsspecialister har deltaget i PwC's Cybercrime Survey 2021. 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, som relaterer til cyberområdet, 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.

Større virksomheder er defineret som ≥ **200** medarbejdere.

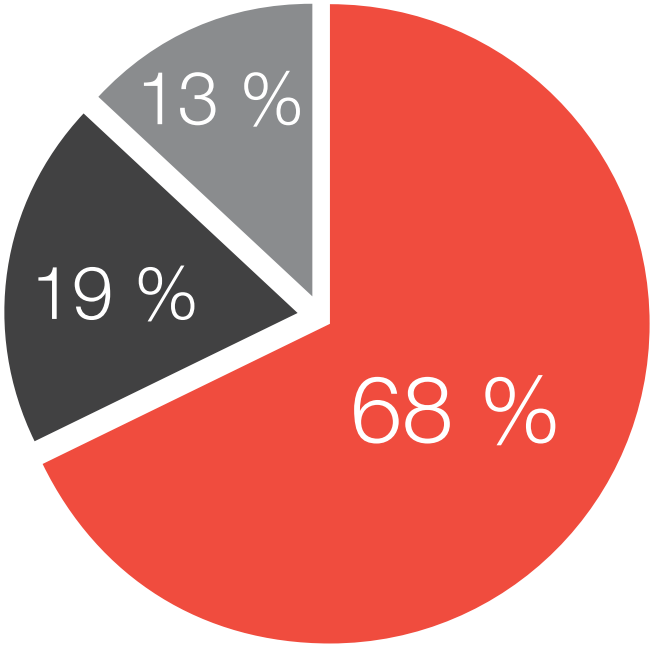
Mindre virksomheder er defineret som ≤ **199** medarbejdere.

Undersøgelsens respondenter fordelt på sektorer:

Den private sektor

Den offentlige sektor

Den finansielle sektor



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 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 løbende til virksomhedens direktion/bestyrelse?
- [ ] Omfatter arbejdet med sikkerhed både informationssikkerhed (ISO 27001) og cybersikkerhed? Læs mere på pwc.dk/iso27001
- [ ] Har I implementeret persondataforordningen?
- [ ] Er der etableret en driftsorganisation for fortsat sikring af compliance med persondataforordningen?

Processer

- [ ] Har I foretaget en måling 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 til identifikation af sårbarheder i jeres infrastruktur og systemer?
- [ ] Har I en defineret og afprøvet incident response-proces? Læs mere på www.pwc.dk/response
- [ ] Har I testet jeres beredskabsplaner for cyberhændelser? Læs mere på pwc.dk/beredskab

Arkitektur

- [ ] Har I en plan for implementering af sikkerhedsteknologi?
- [ ] Har I en proces og plan for efterlevelse af privacy by design, herunder implementering af en sikkerhedsarkitektur? 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

Om PwC

PwC arbejder 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 flere end 2.500 medarbejdere og partnere, som brænder for at gøre en positiv forskel for kunder og kolleger. Globalt er vi over 276.000 PwC'ere i 157 lande, og i Danmark er vi markedsledende. Mød os over hele landet. Vi er der, hvor du er.

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

Mads Nørgaard Madsen
Partner
Leder af Technology & Security

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

Peter Brock Madsen
Partner
Cyber Risikostyring

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

William Sharp
Partner
Cyber Operationel Technology

Technology & Security
T: 4040 1074
E: william.sharp@pwc.com

Christian Kjær
Partner
Cyber beredskab

Technology & Security
T: 5132 1270
E: christian.kjaer@pwc.com

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

Revision. Skat. Rådgivning.

Succes skaber vi sammen ...