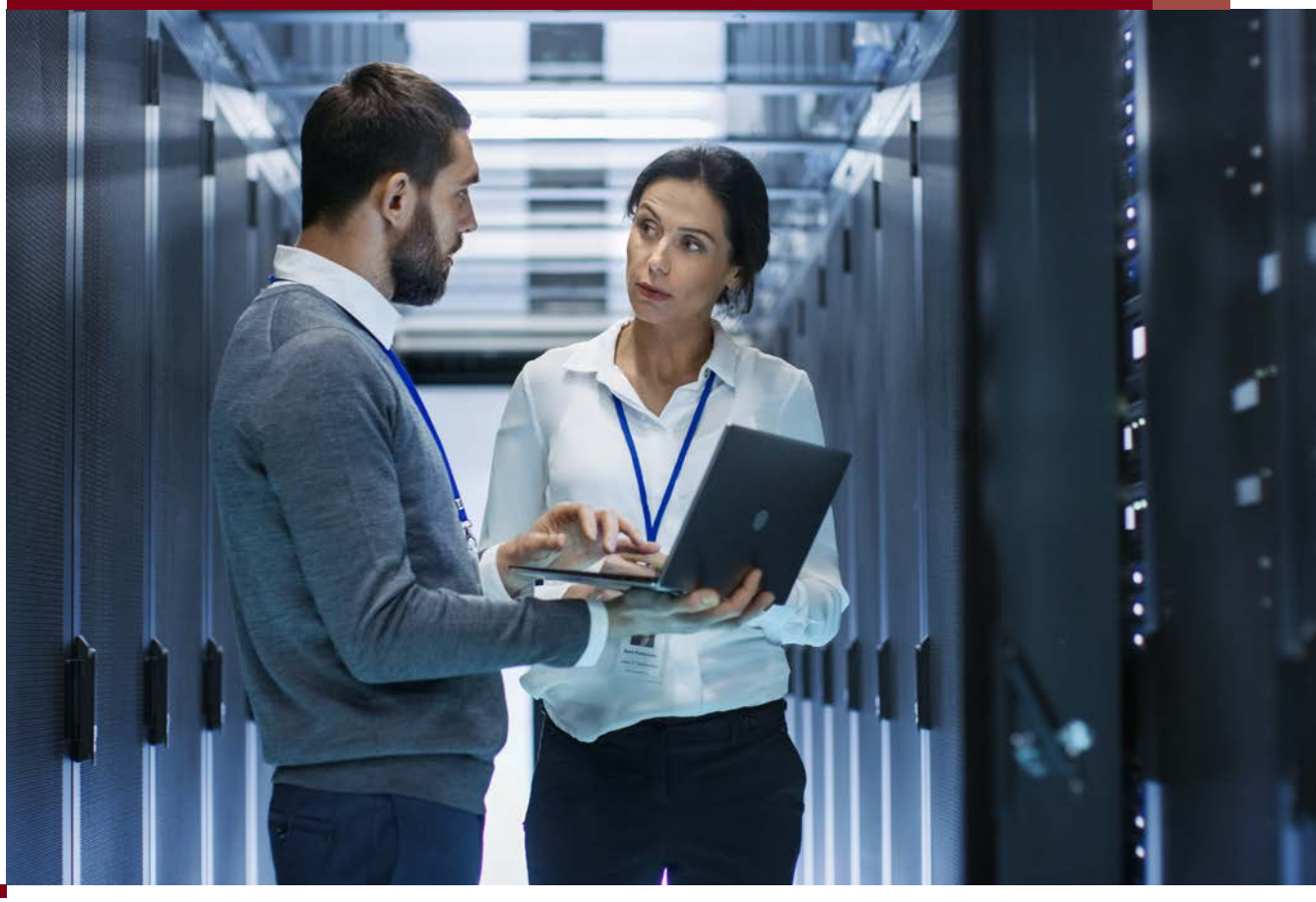
Der er kommet fokus på cybersikkerhed i Danmark

Cybercrime Survey 2018



pwc

Flere end 250 danske og 100 norske virksomhedsledere, it-chefer og specialister har deltaget i PwC's Cybercrime Survey 2018, hvor de har delt deres syn på forskellige forhold i relation til cyberkriminalitet i Danmark. De har således taget stilling til udviklingen i trusselsbilledet og har rapporteret, hvordan og i hvilket omfang de arbejder med udfordringerne.

20%

af de adspurgte i den private sektor har et informations-/ cybersikkerhedsbudget på over 7 millioner kr.

46%

angiver, at virksomhedens personoplysninger i nogen eller mindre grad er beskyttet i henhold til EU-persondataforordningen

21%

har ansat en CISO inden for det seneste år

Revision. Skat. Rådgivning.

Indhold

Færre, men mere alvorlige hændelser

Den teknologiske og digitale udvikling er i konstant forandring – nye teknologier opstår hele tiden, og digitale data bliver en stadig mere central og nødvendig del af virksomhedens daglige processer og forretningsgange. Det giver helt nye muligheder for virksomheder og organisationer, men samtidig gør den hastige udvikling det muligt for kriminelle at gennemføre mere ødelæggende og avancerede cyberangreb end hidtil.

PwC's Cybercrime Survey 2018 viser, at selvom færre virksomheder er blevet ramt af cyberangreb sammenlignet med sidste år, så har flere virksomheder været ramt af alvorlige hændelser. Ifølge PwC's Cybercrime Survey 2018 er de økonomiske omkostninger som følge af cyberangreb steget, hvilket bl.a. skyldes, at angrebene er mere målrettede end tidligere. 49 % angiver i 2018 (mod 41 % i 2017), at de har haft øgede udgifter til udbedring og efterforskning af sikkerhedshændelser i forhold til sidste år. Cyberhændelser er derfor i fokus som aldrig før – hver femte virksomhed har i dag et sikkerhedsbudget på over 7 millioner kroner årligt.

Mangel på talent er fortsat en udfordring

Cybercrime Survey 2018 viser en stigende bekymring for manglende adgang til kandidater med de rette sikkerhedskompetencer, hvilket også ses i PwC's CEO Survey 2018 og CXO Survey 2018. I PwC oplever vi også en stigning i antallet af virksomheder, der efterspørger rådgivning inden for håndtering af komplekse sikkerhedshændelser.

Nogle af de angreb, som flest rammes af, er phishing-angreb[1], som hele 76 % af respondenterne i undersøgelsen har været ramt af. Et vigtigt skridt for at afværge truslen handler om, at man skal beskytte sine konti bedre end blot med et password, da dette nemt kan tilegnes, især når mange benytter det samme password til flere konti. Virksomheder såvel som privatpersoner bør derfor hæve sikkerhedsbaren, fx ved at benytte to-faktor-autentifikation[2]. Der bør yderligere fokuseres på at beskytte privilegerede brugere, som har administrator-adgange til systemerne.

En fokuseret indsats fra ledelseslaget er nødvendig

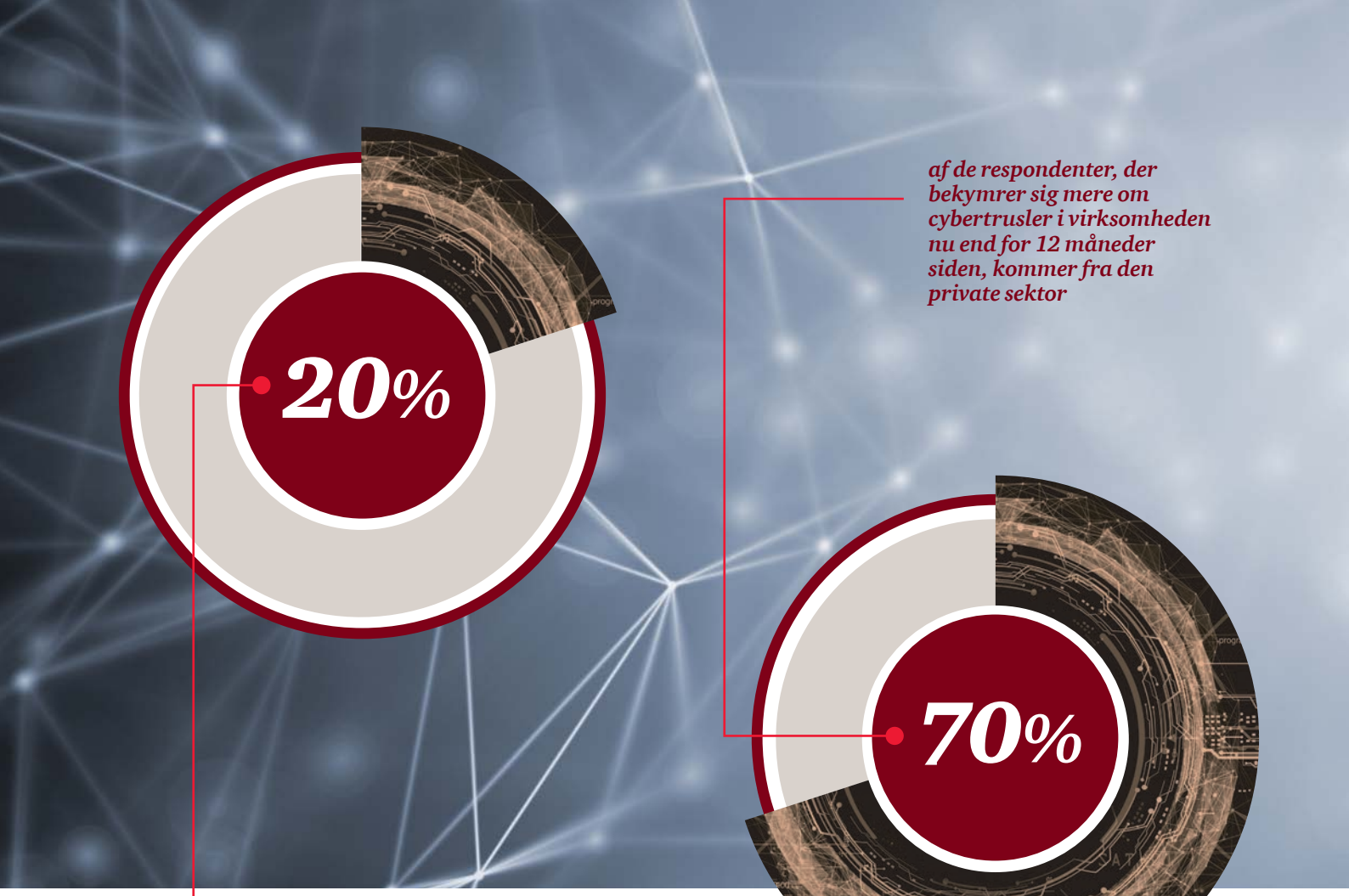
Cybercrime Survey 2018 viser, at topledelsens manglende forståelse for cybertruslen fortsat er en bekymring blandt respondenterne. Regeringens Nationale Strategi for Cyber og Informationssikkerhed er således et kærkomment tiltag, der blandt andet har fokus på ledelsesopgaver og uddannelse[3].

At være i stand til at håndtere et cyberangreb bliver mere og mere centralt, men det kan for mange virksomheder være en lang og sej rejse at komme i gang med sikkerhed. Arbejdet med sikkerhed kræver en pragmatisk tilgang og en anerkendelse af, at standarder og politikker ikke kan stå alene i beskyttelsesfasen. Frem for alt kræver det en fokuseret indsats fra ledelseslaget. Mange virksomheder har et it-setup, som bygger på en it-platform, der kan være 10-15 år gammel, og her er det vigtigt, at ledelsen tager teten med at opdatere sikkerheden. Dette tager tid og kræver store investeringer i form af især teknologi og awareness-træning, men det er en nødvendig rejse, hvis forretningen skal kunne fortsætte, i tilfælde af at virksomheden rammes af en sikkerhedshændelse. Sikkerhedsrejsen er desuden blevet yderligere kompliceret af, at der efter EU's persondataforordning i visse tilfælde skal indrapporteres til Datatilsynet, såfremt personoplysninger er involveret i en hændelse. Netop dette har skabt stor bekymring hos mange virksomheder, hvilket vi kan mærke i de henvendelser vi i PwC får gennem vores incident response-team.

At være en førende digital nation kræver, at erhvervslivet og offentlige institutioner har sikkerhed og beskyttelse af data som højeste prioritet. Det vil vi i PwC gerne være med til at sætte på agendaen, og med vores Cybercrime Survey vil vi gerne bidrage med viden inden for cyber- og informationssikkerhed.
En stor tak til alle, der har delt deres indsigt og erfaringer i dette års survey. Vi vil gerne opfordre alle til at blive ved med at være åbne omkring hændelser i det omfang, det nu engang er muligt. Således vil vi i fællesskab kunne være i stand til at belyse et område af stigende væsentlighed.

Mads Nørgaard Madsen
Partner
Security & Technology

[1] Phishing er ofte en mail, der er forsøgt kamufleret som en reel henvendelse. Den har til formål at få brugeren til at klikke på et link i mailen og få dem til at indtaste personoplysninger på et falsk site, som angriberen kan misbruge. Alternativt planter e-mailen malware i systemet, når der klikkes på linket.
[2] To-faktor-autentifikation er en metode til at identificere en bruger på, der kræver minimum to trin. I tillæg til brugernavn og password kan man fx tilføje et ekstra sikkerhedslag ved at skulle angive en kode, der bliver tilsendt på SMS.
[3] Regeringen, maj 2018. *National Strategi for Cyber- og Informationssikkerhed – 2018-2021.*



af de respondenter, der bekymrer sig mere om cybertrusler i virksomheden nu end for 12 måneder siden, kommer fra den private sektor

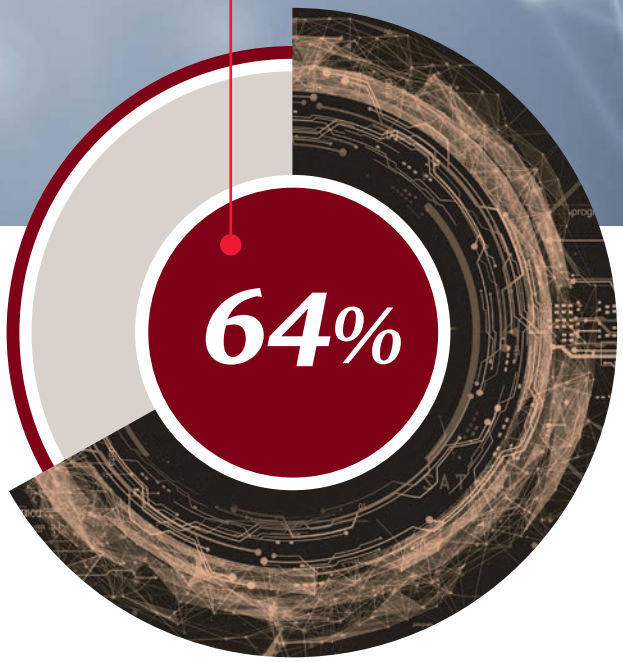
færre respondenter sammenlignet med sidste år angiver, at de har været udsat for en hændelse de seneste 12 måneder sammenlignet med 2017

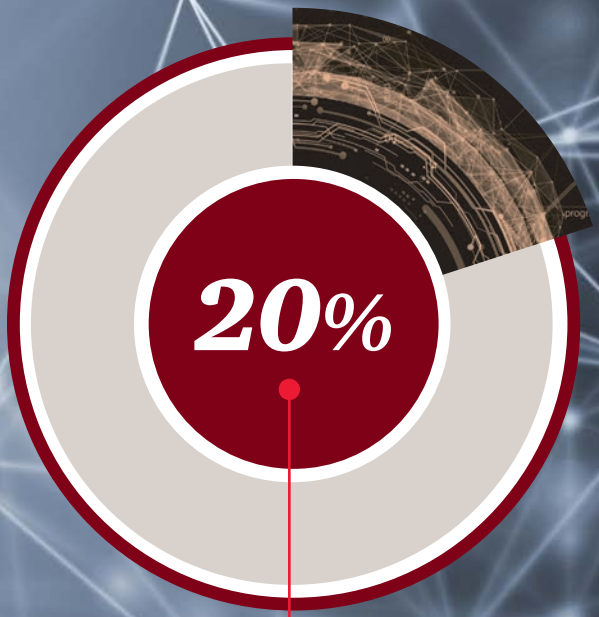
Cybertruslen bekymrer især den private sektor

PwC's Cybercrime Survey 2018 viser, at der er sket en positiv udvikling fra 2017 til 2018 i antallet af virksomheder, der angiver, at de har været udsat for en sikkerhedshændelse. Således er der sket et fald på 20 % (fra 55 % i 2017 til 44 % i 2018) i andelen af virksomheder, der angiver, at de har været udsat for en hændelse. Undersøgelsen viser dog samtidig, at flere har haft øgede udgifter til udbedring og efterforskning af sikkerhedshændelser. 49 % har haft øgede udgifter i forhold til sidste år. I 2017 svarede 41 % det samme, hvilket svarer til en stigning på 8 procentpoint. 50 % af respondenterne (mod 74 % i 2017) angiver, at de bekymrer sig mere for cybertruslen i dag end for 12 måneder siden. Der er dermed sket et fald, hvad angår antallet af hændelser, men der tegner sig samtidig et billede af, at bekymringsniveauet for cybertrusler fortsat er højt, på trods af et fald sammenlignet med 2017. Af de 50 %, der svarer, at de bekymrer sig mere for cybertruslen i dag end for 12 måneder siden, tilhører hele 70 % den private sektor[4]. Ser man bekymringen fordelt på virksomhedsstørrelser, kommer 59 % fra større virksomheder.

[4] De resterende tilhører enten den offentlige sektor eller har ikke angivet branche.

af de virksomheder, der har været udsat for en sikkerheds-hændelse de seneste 12 måneder, kommer fra den private sektor

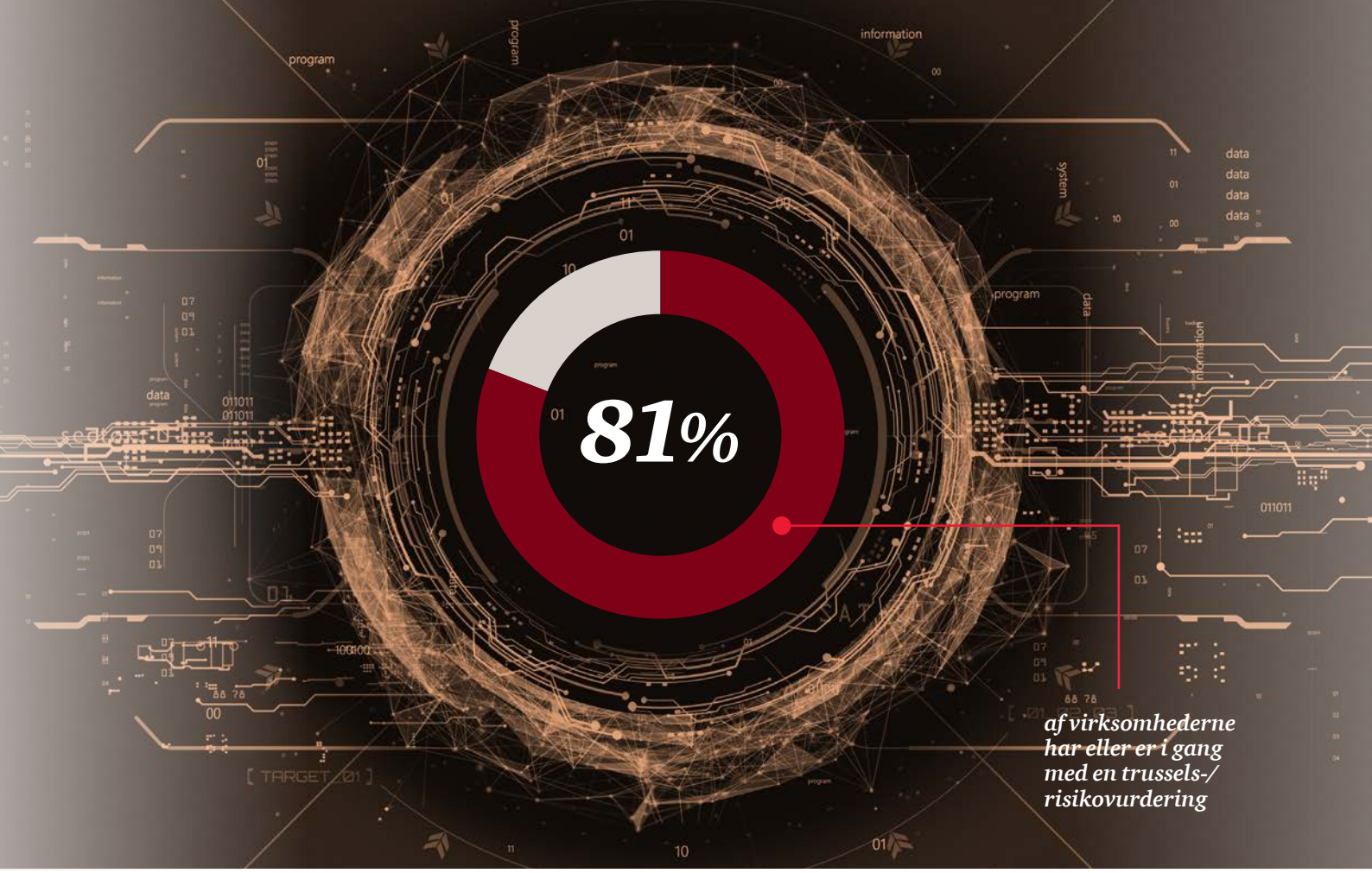




af de adspurgte i den private sektor har et informations-/cybersikkerheds-budget på over 7 millioner kr.

Det er ikke uden grund, at bekymringen er så høj i den private sektor. PwC's Cybercrime Survey 2018 viser, at 64 % af de respondenter, der rapporterer, at de har været udsat for en sikkerhedshændelse de seneste 12 måneder, kommer fra den private sektor. Samtidig kan det ses, at 48 % af de private virksomheder, der bekymrer sig mere om cybertruslen i dag end for 12 måneder siden, har haft øgede udgifter til udbedring og efterforskning af sikkerhedshændelser i det seneste regnskabsår.

At der generelt er en fortsat høj bekymring for cybertruslen, samt at der ses en stigning i andelen af respondenter, der angiver, at de har haft øgede udgifter til udbedring og efterforskning af sikkerhedshændelser, kan være med til at forklare, at der også ses en stigning i andelen af respondenter, der angiver, at deres virksomhed har afsat ressourcer til et informations-/cybersikkerhedsbudget. Således svarer 73 % af respondenterne i 2018 (mod 64 % i 2017), at de har afsat ressourcer til et informations-/cybersikkerhedsbudget. Undersøgelsen viser samtidig, at 20 % af de adspurgte i den private sektor har et samlet informations-/cybersikkerhedsbudget på over 7 millioner kroner. Til sammenligning var det 17 % i 2017.

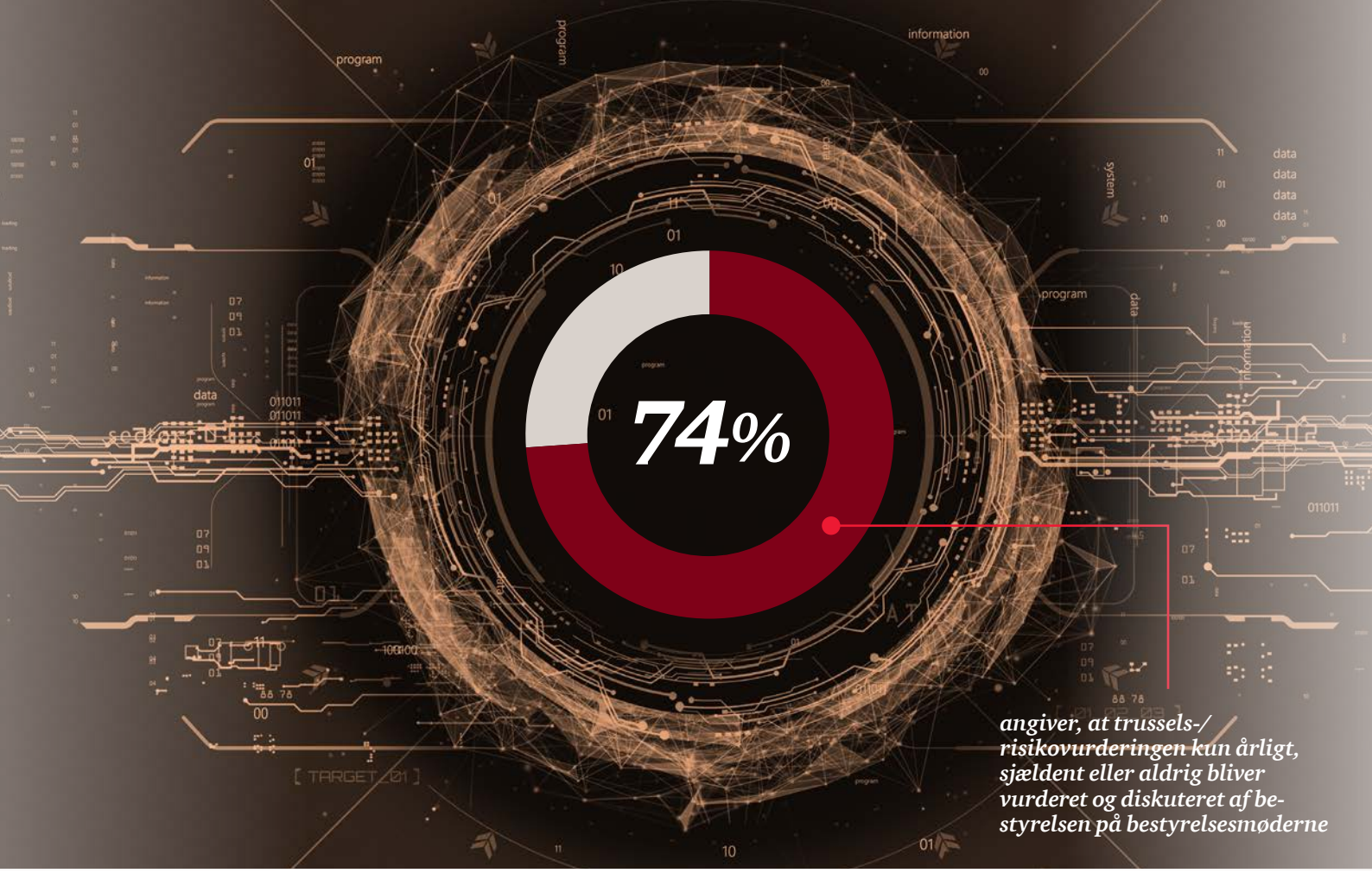


Topledelsens manglende forståelse for cybertruslen bekymrer fortsat

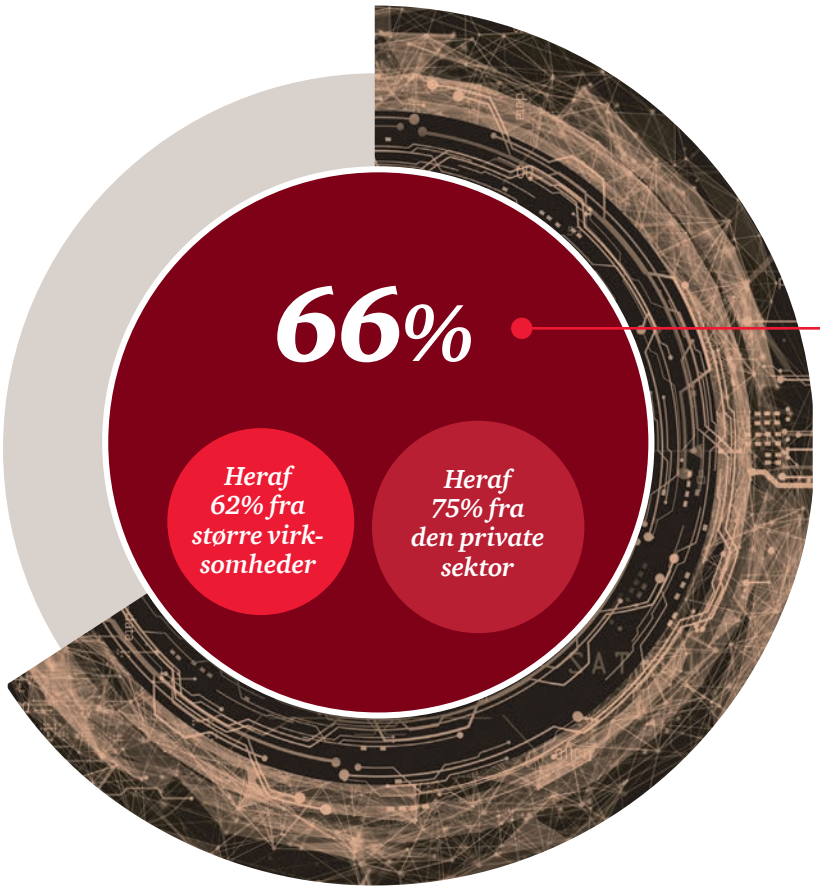
PwC's Cybercrime Survey 2018 viser et fald i antallet af respondenter, der angiver, at topledelsen i nogen eller i høj grad har fokus på balancen mellem cybertrusler og investeringer i cybersikkerhed. Dette fald er undersøgt på tværs af brancher og virksomhedsstørrelser, og der ses en tendens til, at det primært er i de større, private virksomheder, at respondenterne mener, at der mangler fokus fra topledelsen.

I 2017 angav 72 % af respondenterne, at topledelsen i nogen eller i høj grad havde fokus på balancen mellem cybertrusler og investeringer i cybersikkerhed. I 2018 er tallet faldet til 66 %, hvoraf 75 % tilhører den private sektor, og 62 % kommer fra større virksomheder. Respondenternes fortsat høje bekymring giver god mening set i lyset af, at 81 % af respondenterne oplyser, at virksomheden har eller er i gang med en trussels-/risikovurdering, men at den i hele 74 % af tilfældene kun årligt, sjældent eller aldrig diskuteres af bestyrelsen/topledelsen. Vejen fra det indledende kortlægningsarbejde til kontinuerlig opfølgning kan for mange virksomheder være en udfordring og kræver løbende dialog mellem ledelsen og den sikkerhedsansvarlige. Denne dialog er ikke etableret i alle virksomheder, da ca. 1 ud af 3 angiver, at virksomhedens sikkerhedsansvarlige kun årligt eller aldrig briefer virksomhedens ledelse om risikoen ved cybertrusler.

> *" De virksomheder, vi ser, som håndterer cybertrusler bedst, har involveret ledelsen i at få risikovurderet virksomhedens aktiver som grundlag for en prioritering af de nødvendige sikkerhedstiltag. Vi vil anbefale, at dette sker løbende – og mere end én gang årligt – og at der følges op på implementeringen af de nødvendige sikkerhedstiltag. Specielt i forebyggelsen mod cyberhændelser er der behov for tæt og kontinuerlig dialog samt prioritering fra ledelsen, hvis man ikke vil blive negativt overrasket over konsekvenserne ved cyberhændelser, som løbende udvikler sig og bliver mere avancerede og målrettede.*
>
> ***– PwC***



angiver, at trussels-/ risikovurderingen kun årligt, sjældent eller aldrig bliver vurderet og diskuteret af bestyrelsen på bestyrelsesmøderne



mener, at ledelsen i nogen eller i høj grad har fokus på balancen mellem cybertrusler og investeringer i cybersikkerhed[5]

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 samt vigtigheden i at investere i cyber-og informationssikkerhed.

Læs mere på www.pwc.dk/got

[5] Ved de 75 % fra den private sektor og 62 % fra større virksomheder kan de samme respondenter gå igen to gange, eftersom de kan tilhøre begge grupper – derfor ender den samlede procentandel på over 100.

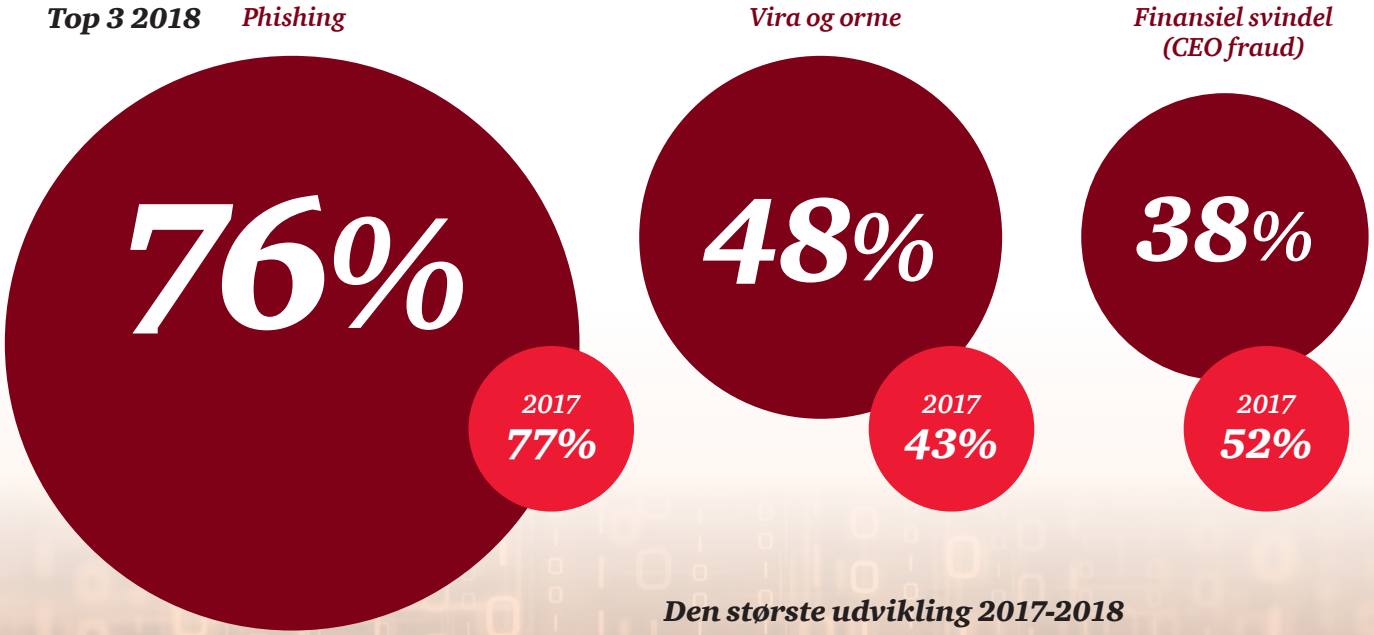
Antallet af ransomware-angreb er dalet

Selvom antallet af sikkerhedshændelser i år er faldet 20 % siden 2017 (fra 55 % til 44 %), viser undersøgelsen, at der er sket en ændring i selve sikkerhedshændelserne, som er blevet mere målrettede. 59 % af respondenterne har således oplevet en eller flere sikkerhedshændelser, der var målrettet deres virksomhed. Til sammenligning var dette tal 44 % i 2017.

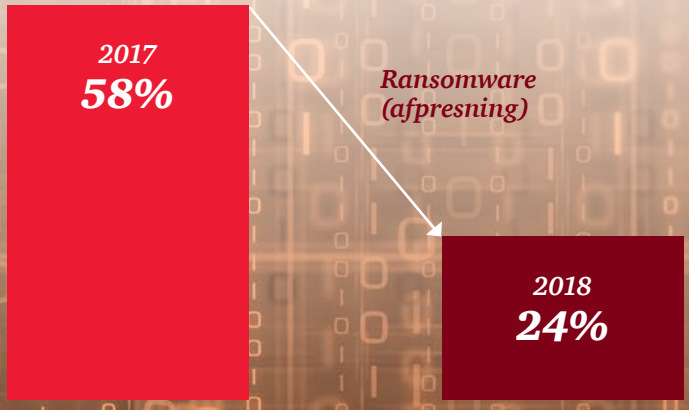
Undersøgelsen viser også et skift i de angrebstyper, som respondenterne tilkendegiver, at virksomhederne har oplevet. Ransomware eller afpresning, der tidligere har været en af de hyppigst oplevede angrebstyper med hele 58 % i 2017, har taget et markant dyk og har i 2018 ramt 24 %, hvilket er et fald på hele 34 procentpoint. Denne type cyberangreb er finansielt motiveret, da angriberen tager virksomhedens data som gidsel ved at kryptere virksomhedens data og efterfølgende afpresse virksomheden ved at tilbyde krypteringsnøglen mod betaling. Årsagen til faldet kan skyldes, at virksomhederne er blevet bedre sikret mod denne type angreb. Dette kan underbygges ved at kigge nærmere på antallet af phishing-angreb, der med sine 76 % i 2018 er oplevet over tre gange så ofte som ransomware-angreb. Da phishing-metoden er den primære angrebsmetode for et ransomware-angreb, kan en mulig forklaring derfor være, at virksomhederne har registreret et phishing-angreb, men samtidig har været i stand til at forhindre et potentielt ransomware-angreb. Derfor er antallet af phishing-angreb højere end antallet af ransomware-angreb. Selvom antallet af ransomware-angreb er dalet, vurderer Center for Cybersikkerhed i deres trusselsvurdering for maj 2018, at truslen stadig er

Hændelser som virksomheden har oplevet de seneste 12 måneder som resultat af cyberkriminalitet eller informationssikkerhedshændelser

Top 3 2018



Den største udvikling 2017-2018



betydelig[6]. Det er derfor vigtigt, at virksomhederne ikke undervurderer truslen fra ransomware, men forbereder sig på nye typer af ransomware-angreb.

I årets top tre over de hændelser, som virksomhederne har oplevet de seneste 12 måneder, finder vi – ud over phishing – malware, vira og orme, hvor hele 48 % af respondenterne angiver, at de har oplevet denne angrebstype i 2018. Konsekvenserne af denne angrebstype kan være store, siden malware automatisk kan korruptere systemer og ødelægge data på en måde, der oftest er svært at opdage, før det er for sent.

Sidst i årets top tre er finansiel svindel (CEO fraud)[7], hvor 38 % af respondenterne angiver, at de har været udsat for denne type angreb. Dette er et stort dyk i forhold til sidste års 52 %. Angrebene bliver dog stadig mere avancerede, fx ved at de kriminelle nu i højere grad vælger at stjæle identiteter frem for som tidligere at forfalske e-mails fra virksomhedens CEO. Førstenævnte sker i stigende omfang, fordi mange virksomheder har skiftet til cloud uden at sikre sig med mere end blot brugernavn og password.

> *" I forlængelse af den oplevede udviklingstendens vedrørende CEO fraud, som netop bygger på identitetstyveri, oplever vi i PwC gennem et stigende antal henvendelser, at identitetstyveri, der ikke kun kan spores tilbage til CEO fraud, generelt bliver mere og mere udbredt. Denne type angreb rammer enkeltpersoner og har i mange år været et kendt problem i udlandet, hvor vi i Danmark tidligere kun har haft få tilfælde. Vigtigheden i, at vi nu også i Danmark bliver nødt til at forholde os til identitetstyveri, er blevet forstærket, efter at EU-persondataforordningen (GDPR) er trådt i kraft, da denne type cyberkriminalitet har afgørende konsekvenser for den registreredes privatlivsrettigheder og handlemuligheder. Det forholder sig fx lige nu således, at man på det sorte marked kan finde priser på stjålne identiteter, der står i langt højere kurs end eksempelvis kreditkort."*
>
> ***– PwC***

PwC anbefaler

Phishing

PwC anbefaler, at medarbejderne i organisationen løbende gennemgår awareness-træning, da phishing-forsøg oftest sker ved, at en medarbejder modtager en inficeret e-mail. Dette kan kobles med selv at teste organisationen uden konsekvenser ved at benytte såkaldt "positive phishing".

Ransomware

PwC anbefaler, at man ved ransomware-sager sidestiller angreb med en sikkerhedshændelse. Det vil sige, at man straks bør kontakte sin sikkerhedsafdeling, hvis man har mistanke om et angreb, så man kan håndtere sagen med mindst mulig skade for forretningen.

CEO Fraud

PwC's incident team har fået mange henvendelser i 2018 omhandlende cloud-mail tyveri, hvor formålet for de kriminelle har været at svindle med betalinger. PwC anbefaler derfor at aktivere to-faktor-autentifikation på alle eksternt vendte services og især på e-mail. Dette gælder også private konti til cloud, sociale medier, m.m.

[6] Trusselsvurderingsenheden ved Center for Cybersikkerhed, maj 2018. *Cybertruslen mod Danmark.*

[7] Ved denne angrebstype udgiver angriberen sig for at være et højtstående medlem af organisationen og anmoder om overførsler af virksomhedens midler til angriberens konti.

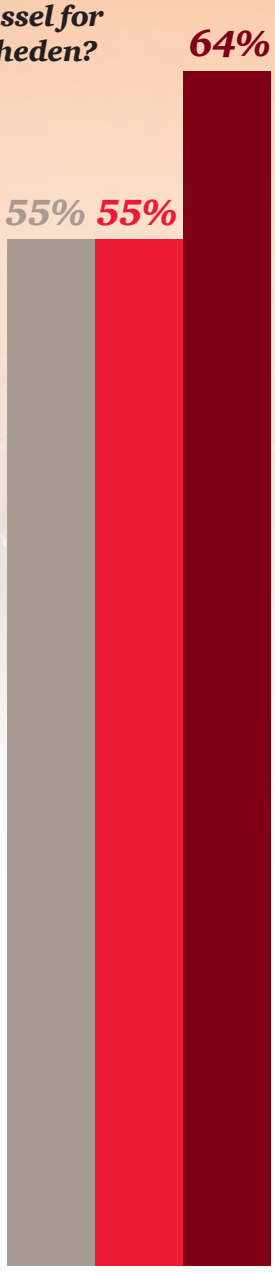
Den største bekymring er ansattes/insideres ubevidste handlinger og organiserede kriminelle

PwC's Cybercrime Survey 2018 viser, at cybertruslen er under konstant forandring. Undersøgelsen viser, at ansattes/insideres ubevidste handlinger med hele 74 % i 2018 udgør den største cybertrussel, tæt fulgt af organiserede kriminelle med 64 %. Til sammenligning var den største cybertrussel i 2017 ansattes/insideres ubevidste handlinger med 56 %, og i 2016 var det organiserede kriminelle med 55 %. Udviklingen stemmer overens med den store andel, der er ramt af phishing-angreb (76 % i 2018), da succesen for de kriminelle af denne type angreb afhænger af ansattes/insideres ubevidste handlinger.

En anden markant ændring i respondenternes tilkendegivelse af markante cybertrusler fra 2017 til 2018 er cybertruslen knyttet til nye teknologier, som er steget fra 32 % i 2017 til 52 % i 2018. Også truslen fra andre nationer er steget betragteligt til 34 %, hvilket er tæt på en tredobling, sammenlignet med sidste års 13 %. Center for Cybersikkerhed vurderer blandt andet i deres trusselsvurdering for maj 2018[8], at truslen fra cyberspionage mod Danmark er meget høj – specielt for danske myndigheder, men også for danske forskningstunge virksomheder. På listen over, hvad der i fremtiden vil udgøre den største cybertrussel for virksomhederne, findes også topledelsens manglende forståelse, der med 24 % har vist sig at være en stabil trussel for danske virksomheder gennem de forgangne år. At denne trussel er steget en anelse siden sidste år (fra 20 % til 24 %) kan hænge sammen med, at også færre i år mener, at topledelsen i nogen eller i høj grad har fokus på balancen mellem cybertrusler og investeringer i cybersikkerhed.

> *" Mange virksomheder opsøger hjælp til at sikre klar kommunikation til topledelsen. Når vi hjælper virksomheder før, under eller efter et angreb, er der nu også et særligt fokus på at skabe forståelse i topledelsen for nødvendige investeringer, der sikrer virksomheden bedre mod cybertruslerne i fremtiden. Den nye persondataforordning (GDPR) har medvirket til at sætte mere fokus på sikkerheden, selvom det endnu ikke er alle virksomheder, der lever op til kravene, jævnfør PwC's Cybercrime Survey 2018.*
> ***– PwC***

Hvad vil i fremtiden udgøre den største cybertrussel for virksomheden?



2016 2017 2018

[8] Trusselsvurderingsenheden ved Center for Cybersikkerhed, maj 2018. *Cybertruslen mod Danmark.*

PwC anbefaler

Organiserede kriminelle

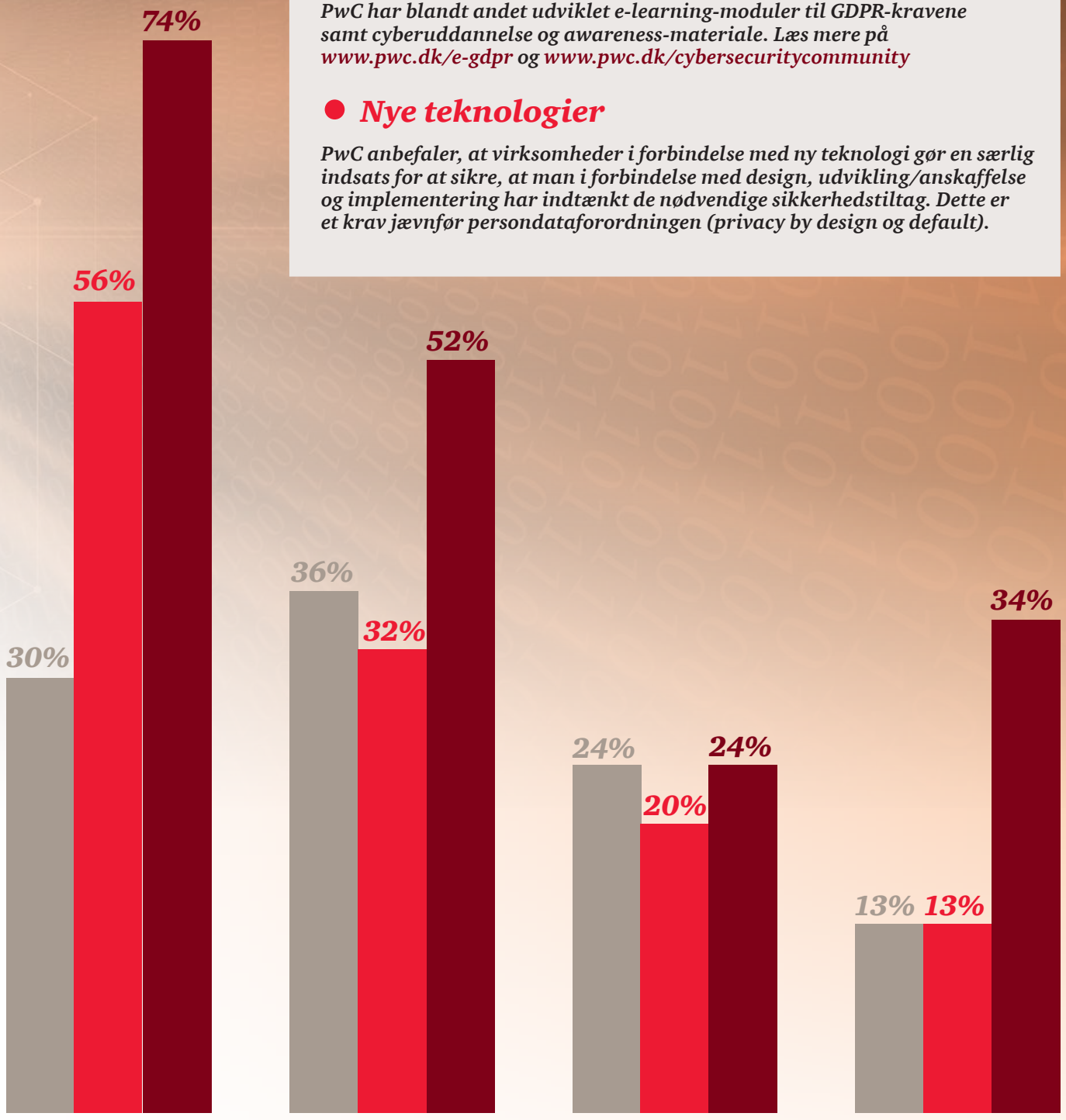
PwC anbefaler, at man i kampen mod den organiserede kriminalitet etablerer et homogent og dækkende sikkerhedsprogram, så alle kritiske dele af virksomhedens systemer og infrastruktur sikres på en tilstrækkelig effektiv måde, og således at det er afstemt med virksomhedens risikovillighed. Her tænkes specielt på de sikkerhedstiltag, der imødegår truslen fra cyberkriminelle.

Ansattes/insideres ubevidste handlinger

PwC anbefaler, at medarbejdere løbende gennemgår awareness-træning. PwC har blandt andet udviklet e-learning-moduler til GDPR-kravene samt cyberuddannelse og awareness-materiale. Læs mere på www.pwc.dk/e-gdpr og www.pwc.dk/cybersecuritycommunity

Nye teknologier

PwC anbefaler, at virksomheder i forbindelse med ny teknologi gør en særlig indsats for at sikre, at man i forbindelse med design, udvikling/anskaffelse og implementering har indtænkt de nødvendige sikkerhedstiltag. Dette er et krav jævnfør persondataforordningen (privacy by design og default).

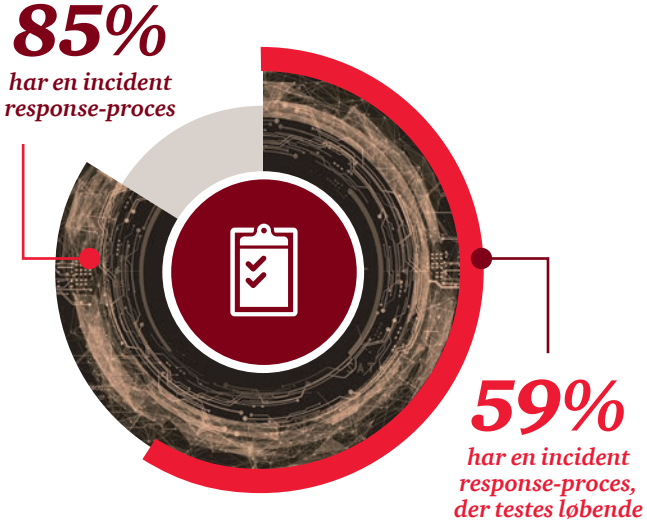


De fleste virksomheder har en incident response-proces – 2 ud af 3 tester den løbende

Der er sket en markant positiv udvikling i antallet af virksomheder, der i 2018 har en incident response-proces. Således viser PwC's Cybercrime Survey 2018, at en langt større andel af respondenter i 2018, sammenlignet med 2017, har angivet, at deres virksomhed har en incident response-proces[9], da 85 % af de adspurgte virksomheder angiver, at de har en incident response-proces i 2018, mod 55 % i 2017. 59 % ud af de 85 % af respondenterne angiver, at virksomheden tester deres incident response-proces løbende – denne andel var på 34 % i 2017.

> *" De seneste års cyberhændelser har vist værdien og behovet for en incident response-proces. Vi oplever, at flere og flere har fokus på at få etableret en incident response-proces, men at der stadig er en del, der mangler af få den forankret gennem løbende tests af processens aktivitet, så de er forberedt, når der sker en alvorlig sikkerhedshændelse.*
> ***– PwC***

Undersøgelsen viser desuden, at ud af de respondenter, der angiver, at de er mere bekymrede for cybertruslen i dag end for 12 måneder siden, har 90 % en incident response-proces. Det ses også, at 100 % af de respondenter, der har været udsat for en målrettet sikkerhedshændelse, har en incident response-proces. Undersøgelsen peger dermed på, at det særligt er de virksomheder, der har været ramt af målrettede sikkerhedshændelser, der afsætter ressourcer til en incident response-proces.



[9] En incident response-proces er en proces, der definerer, hvordan man håndterer hændelser, der kan kompromittere fortroligheden, integriteten og/eller tilgængeligheden af data eller digitale services og dermed have indvirkning på virksomhedens image, omtale og processer. En incident response-proces identificerer og beskriver derfor blandt andet de forskellige roller og ansvarsområder hos en virksomheds incident response-team.

Virksomhederne er i mindre grad end forventet i stand til at beskytte deres person-oplysninger i henhold til GDPR

I 2018 peger 49 % af respondenterne på, at deres data i høj grad er beskyttet i henhold til GDPR. I 2017 svarede 60 % af respondenterne, at de i høj grad forventede at være i stand til at beskytte virksomhedens personoplysninger i henhold til GDPR. Undersøgelsen viser således en difference på 11 procentpoint i forhold til virksomhedernes forventninger i 2017, og hvad de lever op til i 2018. 46 % angiver samtidig, at deres data i nogen eller i mindre grad er beskyttet i henhold til GDPR, hvilket betyder, at lidt under halvdelen af respondenterne ikke anser virksomhederne som tilstrækkelig compliant på nuværende tidspunkt.

Behovet for omlægninger af arbejdsprocesser og opgaver afspejles i respondenternes svar. 64 % af respondenterne oplyser, at de har omlagt virksomhedens processer i større eller mindre grad som følge af GDPR, mod 11 %, der ikke kan kvantificere nogle omlægninger. Selvom den nye lovgivning har sat krav til virksomhederne, er de overvejende positivt indstillede over for dens effekt – 42 % angiver, at persondataforordningen har skabt bedre datakvalitet/brug af personoplysninger i virksomheden, og 20 % mener, at det har skabt nye muligheder og værdi for virksomheden.

> *" Undersøgelsen viser således, at en stor andel af danske virksomheder med fordel kan gøre en større indsats på GDPR-området. Dette er ikke blot i forhold til at blive compliant, men også i forhold til at fastholde det nødvendige compliance-niveau. Dette kræver omlægning af arbejdsprocesser og opgaver samt en investering i teknologi, der kan sikre en overholdelse af kravene, men også medvirke til at beskytte mod de stigende cybertrusler.*
> ***– PwC***

> *" Det er positivt at se, at så mange virksomheder har en god indstilling til den nye lovgivning, trods det store arbejde, som mange virksomheder har lagt i det. Vi har oplevet, at virksomheder også har fået fordele ud af det, blandt andet styr på interne processer, oprydning i data og øget sikkerhed.*
> ***– PwC***

angiver, at deres data i nogen eller i mindre grad er beskyttet i henhold til GDPR

oplyser, at deres data i høj grad er beskyttet i henhold til GDPR

svarer, at GDPR har krævet mindre eller større omlægninger af virksomheden

Dansk erhvervslivs top 5-investeringer inden for cybersikkerhed

EU-persondataforordningen har for alvor sat sit præg på danske virksomheder i 2018, når man ser på deres planlagte investeringer. Undersøgelsen viser, at 46 % af respondenterne angiver, at deres virksomhed planlægger at investere i privilegeret adgangsstyring[10], 45 % planlægger investeringer i awareness-træning, 41 % i central og intelligent logning[11] og 38 % i metodeforankring[12]. Antallet af respondenter, der peger på awareness-træning, er faldet fra 53 % i 2017, hvilket står i kontrast til den stigende bekymring omkring ansattes/insideres ubevidste handlinger, der aldrig har været højere. Vi bad også respondenterne forholde sig til, hvor mange af de ovennævnte investeringer, der er drevet af persondataforordningen. Her peger 56 % på awareness-træning, 37 % på privilegeret adgangsstyring, 33 % på metodeforankring samt 26 % på central og intelligent logning.

PwC's Cybercrime Survey 2017 viste, at persondataforordningen fyldte meget på virksomhedernes agenda, da 70 % af respondenterne havde GDPR-compliance øverst på listen over investeringsprioriteringer i 2017. I forlængelse af dette viser dette års undersøgelse, at omkring hver femte virksomhed (18 %) har brugt over 10 millioner kroner på aktiviteter, der relaterer sig til GDPR.

> *" Der er stadig mange virksomheder, der mangler at få forankret GDPR i deres daglige processer, så de bliver ved med at være compliant i fremtiden. En af de vigtigste dele af forankringsprocessen handler om at skabe en klar rolle- og ansvarsfordeling samt definere en egentlig GDPR-driftsansvarlig, således at den enkelte medarbejder ved, hvor man kan søge råd og vejledning i forbindelse med de mange daglige udfordringer, som forordningen giver.*
>
> ***– PwC***

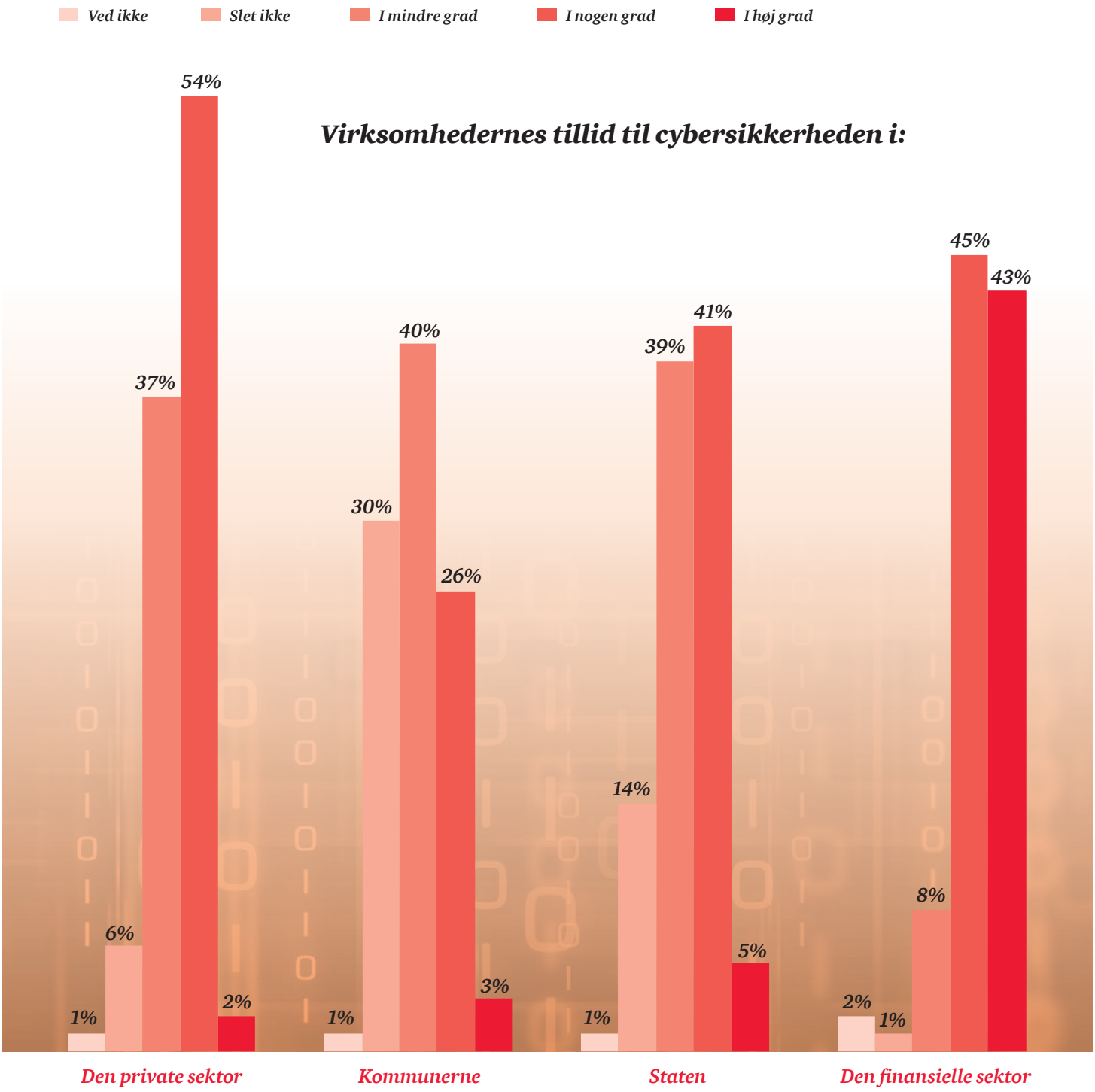
[10] Privilegeret adgangsstyring handler om at få styr på de privilegerede rettigheder i en virksomheds it-infrastruktur.
[11] Ved central og intelligent logning sender alle systemer logdata til ét centralt system. Systemet er intelligent i den forstand, at det leder efter mønstre eller anormaliteter i logdataene.
[12] Metodeforankring omfatter, at man arbejder systematisk og struktureret efter en anerkendt metode.


Virksomhedernes højst prioriterede investeringer inden for cybersikkerhed de næste 12 måneder
2017
2018
Privilligeret adgangsstyring
46%
2017
29%
Awareness-træning
45%
2017
53%
Central og intelligent logning
41%
2017
39%
Metode-forankring
38%
2017
18%
Identity management
36%
2017
34%

Tilliden til cybersikkerhed og GDPR-compliance-niveauet i kommunerne er lav

En af de væsentligste forudsætninger for at opnå succes med digitalisering i såvel virksomheder som i samfundet er, at kunder og borgere har tillid til, at deres data behandles sikkert og fortroligt.

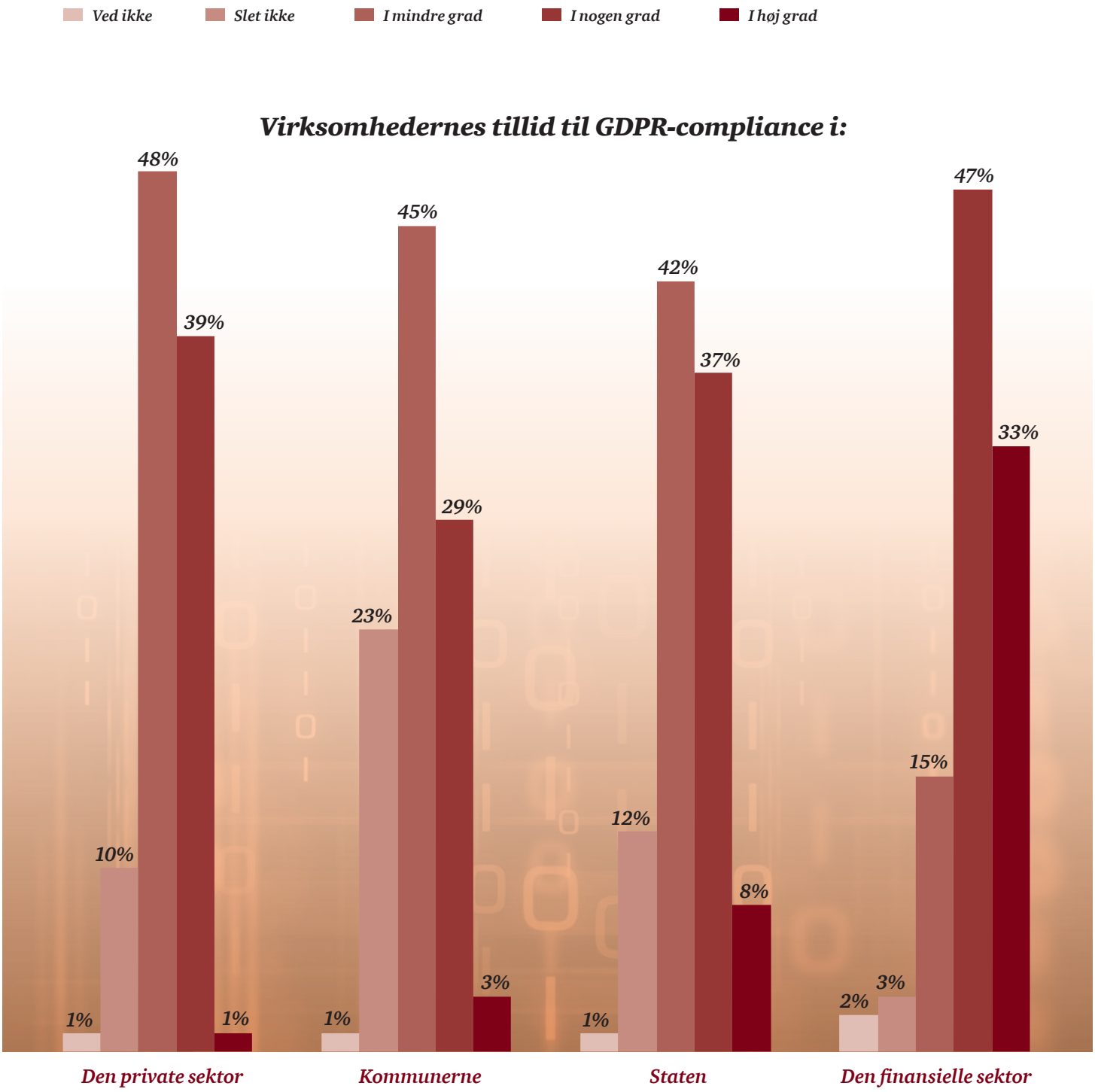
Dette er også den primære baggrund for EU's persondataforordning (GDPR) og en af de grundlæggende målsætninger med den danske nationale cyberstrategi:



"Tilliden til sikkerheden i digitale løsninger er afgørende for den fortsatte digitale udvikling af vores samfund." [13]

Derfor har vi i dette års cybercrime survey spurgt ind til respondenternes tillidsniveau til de forskellige sektorer i forhold til cybersikkerhed og GDPR-compliance. PwC's Cybercrime Survey 2018 viser, at tilliden til cybersikkerheden i kommunerne er lavest, da hele 70 % har angivet, at de i mindre grad eller slet ikke har tillid til cybersikkerheden i kommunerne. Den finansielle sektor skiller sig imidlertid markant ud fra resten, da kun 9 % i mindre grad eller slet ikke har tillid til cybersikkerheden i den finansielle sektor. De samme tendenser ses ved tilliden til GDPR-compliance, hvor 68 % af de adspurgte respondenter svarer, at de i mindre grad eller slet ikke har tillid til GDPR-compliance i kommunerne. Også her skiller den finansielle sektor sig ud, da kun 18 % i mindre grad eller slet ikke har tillid til GDPR-compliance i den finansielle sektor.

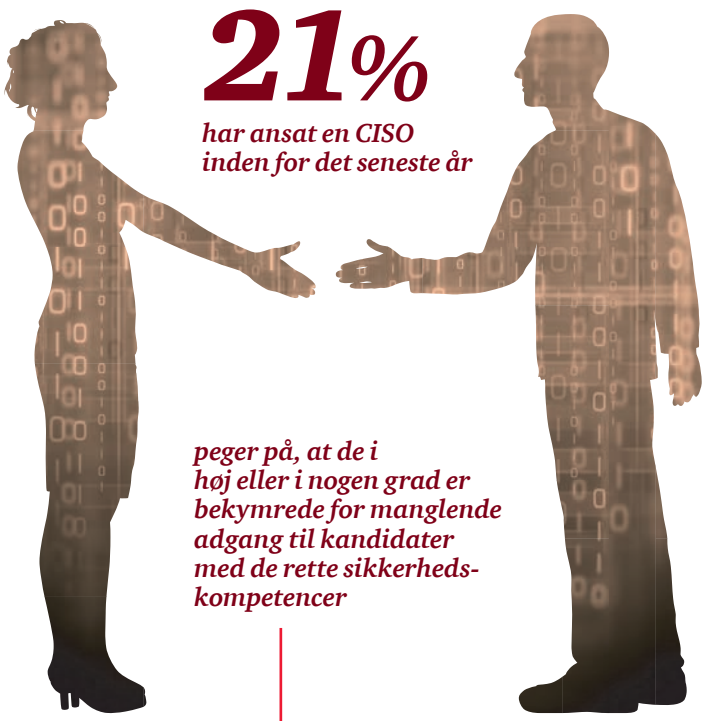
[13] Regeringen, maj 2018. *National Strategi for Cyber- og Informationssikkerhed – 2018-2021.*



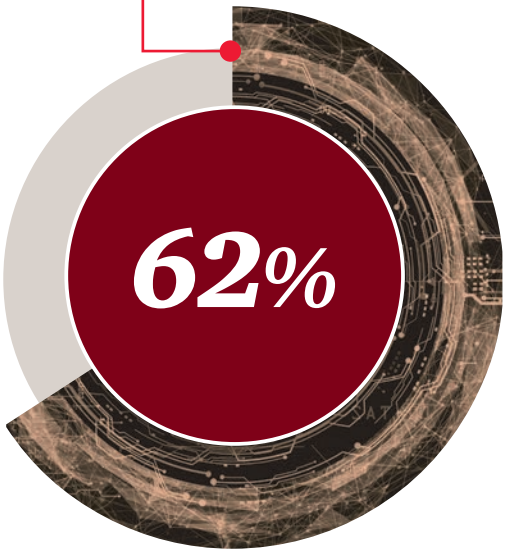
Stigende bekymring for manglende kandidater med de rette sikkerheds-kompetencer

I takt med at trusselsbilledet ændrer sig, stiger også efterspørgslen på erfarne specialister inden for cybersikkerhed. PwC's Cybercrime Survey 2018 viser, at over halvdelen af de adspurgte respondenter er bekymrede for manglende adgang til kandidater med de rette sikkerhedskompetencer. 62 % af respondenterne har således svaret, at de i høj eller i nogen grad er bekymrede for manglende adgang til kandidater med de rette sikkerhedskompetencer. Denne tendens har vi i år set på tværs af flere af PwC's andre undersøgelser. Fx viser PwC's CEO Survey 2018, at 38 % af topledere angiver, at manglen på kvalificeret arbejdskraft i høj grad er en forretningsmæssig bekymring i forhold til virksomhedernes vækstforventninger. Og PwC's CXO Survey 2018 viser, at 46 % angiver, at den største barriere for, at virksomhederne kan investere i og anvende ny teknologi de kommende 3-5 år, er "manglende adgang til kompetencer, som har forståelse for den digitale og teknologiske udvikling koblet med forretningsforståelse". Bekymringen for manglende adgang til de rette kandidater kom også til udtryk i sidste års Cybercrime Survey, hvor 37 % af respondenterne vurderede, at de slet ikke eller i mindre grad havde adgang til de talenter og kompetencer, de havde brug for inden for informations- og cybersikkerhed.

Bekymringen for manglende kvalificeret arbejdskraft i PwC's Cybercrime Survey 2018 er suverænt størst i den private sektor, eftersom 85 % af de respondenter, der har angivet, at de i høj grad er bekymrede for manglende adgang til kandidater med de rette sikkerhedskompetencer, kommer fra den private sektor.



peger på, at de i høj eller i nogen grad er bekymrede for manglende adgang til kandidater med de rette sikkerheds-kompetencer



CISO-services

PwC's CISO-as-a-service-gruppe, der hjælper med optimering, transformering og varetagelse af virksomhedernes sikkerhedsfunktion, oplever, at virksomhederne mangler ressourcer med de rette kompetencer. Det medfører blandt andet et behov for assistance til at etablere deres sikkerhedsorganisation, restrukturere enheden eller finde de rette profiler til organisationens sikkerhedsfunktion. Derfor arbejder vi sammen med organisationer om at etablere et koncept, hvor virksomheder kan få support, værktøjer og uddannelse af deres medarbejdere inden for de forskellige sikkerhedsdiscipliner, hvad enten det er sikkerhedsfunktionen, systemejere eller ledende medarbejdere, der har behov for viden om og erfaring med sikkerhed.

www.pwc.dk/ciso

Norge – dobbelt så bekymrede for truslen fra andre nationer

Ligesom i de forrige år har norske erhvervsfolk givet deres bidrag til PwC's Cybercrime Survey 2018. 111 norske virksomhedsledere, it-chefer og specialister har deltaget i undersøgelsen, og når vi sammenligner henholdsvis de norske og de danske svar, så afviger billedet især ved trusselsaktører og hændelser. Dét, der specielt skiller sig ud, er truslen fra andre nationer, som de norske respondenter har angivet næsten dobbelt så ofte som de danske (NO: 67 %, DK: 34 %).

Den store bekymring i Norge for cybertrusler fra andre nationer er ikke ubegrundet. I den norske efterretningstjenestes risikovurdering "Fokus 2018"[14] beskrives det, at Norge i januar 2018 blev udsat for cyberspionage i sundhedssektoren. Her blev det offentliggjort, at hackere var trængt ind i et it-system på et sygehus i Helse Sør-Øst. I risikovurderingen beskrives det samtidig, at de alvorligste trusler mod Norge anses for at være digital efterretningsaktivitet fra aktører, der forsøger at indhente oplysninger om politiske og militære mål, samt industriel spionage, hvilket er afspejlet i de norske respondenters svar i PwC's Cybercrime Survey 2018. Også det norske politis sikkerhedstjeneste (PST) nævner i deres årlige trusselsvurdering[15], at virksomheder inden for den norske forsvars- og beredskabssektor, statsforvaltning, forskning og udvikling samt virksomheder med en kritisk infrastruktur betragtes som særligt udsatte mål for udenlandske efterretningstjenester. Politiets trusselsvurdering nævner desuden, at det forventes, at udenlandske efterretningstjenester vil forsøge at rekruttere norske enkeltpersoner som kilder og agenter for at få adgang til værdier inden for de mest sårbare norske virksomheder. Det norske trusselsbillede afviger således ikke betydeligt fra det danske, da også Center for Cybersikkerhed i deres trusselsvurdering for maj 2018[16] vurderer truslen fra cyberspionage til at være meget høj. Forskellen kan dog ligge i, at Norge har været udsat for flere hændelser, hvilket kan medføre, at flere af de norske respondenter i PwC's Cybercrime Survey 2018 har peget på truslen.

[14] Etterretningstjenesten, 2018. *Fokus 2018. Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer.*
[15] Politiets Sikkerhetstjeneste, januar 2018. *Trusselsvurdering.*
[16] Trusselsvurderingsenheden ved Center for Cybersikkerhed, maj 2018. *Cybertruslen mod Danmark.*

Har i mindre grad eller slet ikke tillid til cybersikkerheden i kommunerne

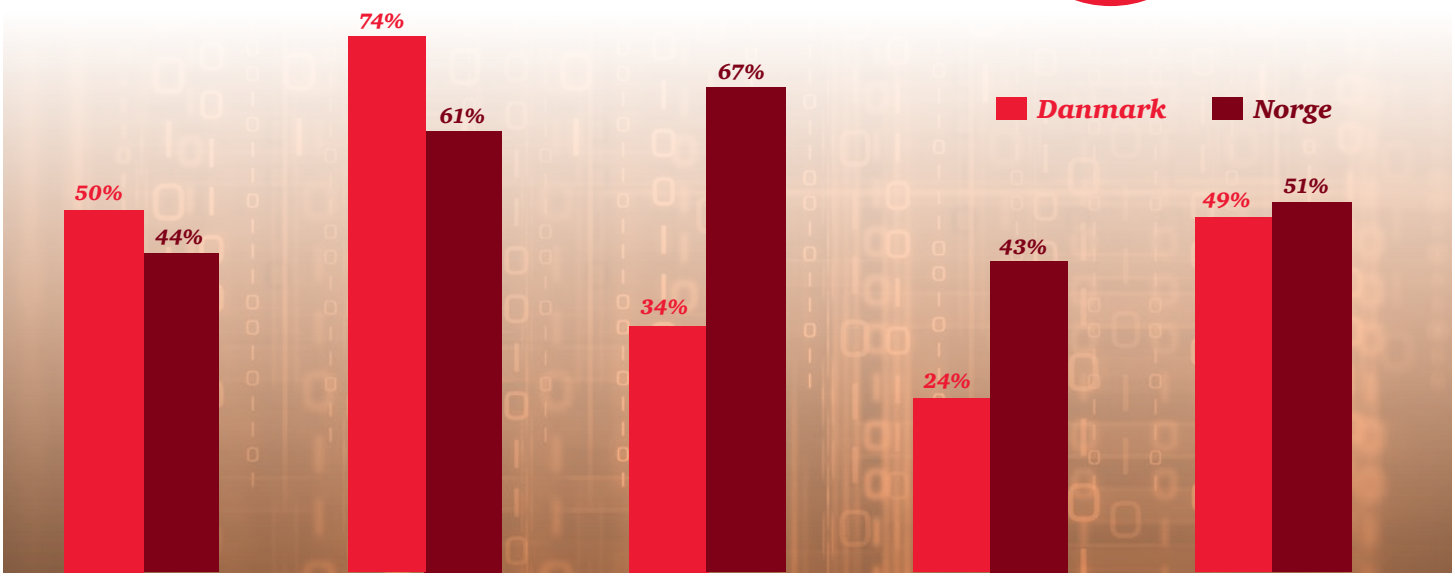
Danmark **70%**

Norge **65%**

Har i mindre grad eller slet ikke tillid til GDPR-compliance-niveauet i kommunerne

Danmark **68%**

Norge **44%**



Bekymrer sig mere om cybertrusler nu, end for 12 måneder siden

Vurderer, at ansattes/insideres ubevidste handlinger i fremtiden vil udgøre den største trussel

Vurderer, at andre nationer i fremtiden vil udgøre den største trussel

Har oplevet et ransomwareangreb inden for de seneste 12 måneder

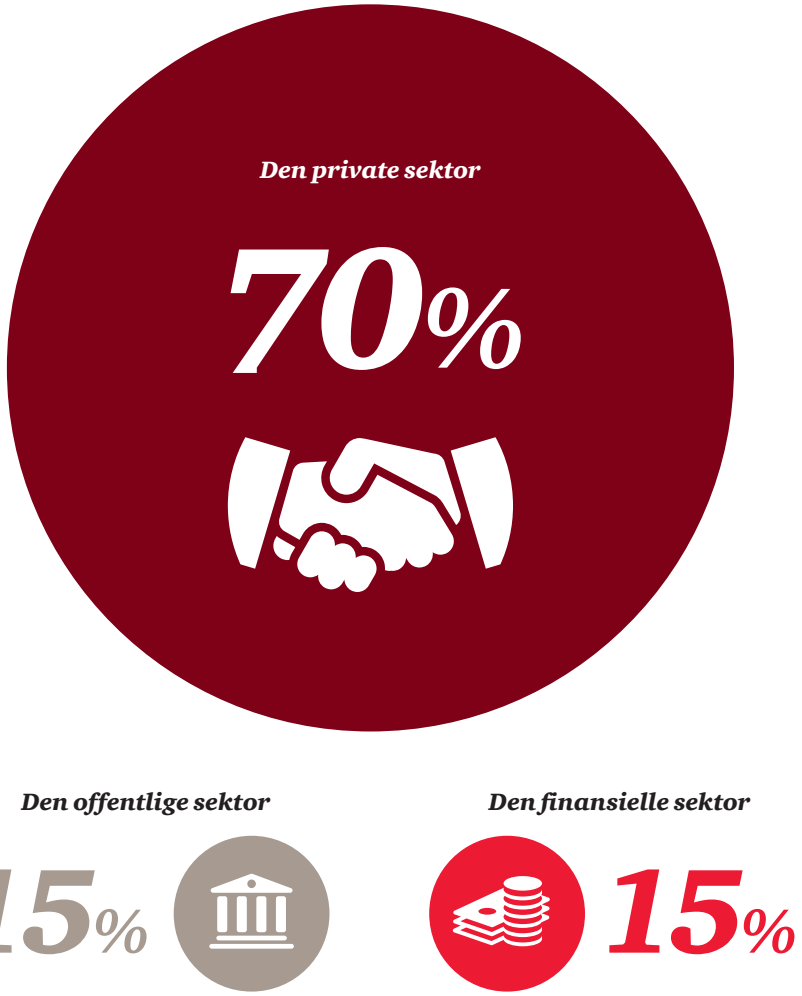
Oplyser, at virksomhedens data i høj grad er beskyttet i henhold til GDPR

Om undersøgelsen

251 danske og 111 norske virksomhedsledere, it-chefer eller sikkerhedsspecialister har deltaget i PwC's Cybercrime Survey 2018. Blandt de danske respondenter kommer 22 fra den offentlige sektor, der dækker et bredt udsnit i landet i form af flere kommuner samt andre offentlige myndigheder. Undersøgelsen er i år gennemført med opbakning fra Center for Cybersikkerhed, DI Digital, Finans Danmark, Dansk Erhverv, IT-Branchen, KITA, Rigspolitiet NC3, Microsoft, Rådet for Digital Sikkerhed og ISACA. Analysen bygger på online-besvarelser. Respondenterne er blevet stillet en række spørgsmål, som relaterer sig til cyber-området, fx om de er blevet ramt af et cyberangreb, om de er bekymrede for truslen fra cybercrime, om de har et dedikeret informations-/cybersikkerhedsbudget, i hvor høj grad virksomhedens personoplysninger er tilstrækkeligt beskyttet i henhold til EU-persondataforordningen mv. Virksomhederne kommer fra et bredt udsnit af brancher/industrier/sektorer, herunder handel, den finansielle sektor, professionelle services og rådgivning, teknologi, industrielle virksomheder, offentlige institutioner, energi og forsyning, transport, pharma mv.

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

Undersøgelsens respondenter fordelt på sektorer [17]



Større virksomheder er defineret ved >200 medarbejdere

Mindre virksomheder er defineret ved <199 medarbejdere

Den offentlige sektor

Den finansielle sektor

[17] Sektorfordelingen af surveyets respondenter er udelukkende beregnet på baggrund af de respondenter, der har angivet, hvilken sektor de tilhører. Ikke alle respondenter har angivet sektor, og disse er derfor ikke medregnet i visualiseringen ovenfor.

Cyber incident response-team

Da et fortsat stort antal af virksomheder bliver udsat for cyberangreb, har PwC fokus på at hjælpe kunder med at forebygge og håndtere cybersikkerhedshændelser.

Vi har etableret en central cyberhotline for kunder, så de 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 kan der implementeres forbedringer af sikkerheden og udarbejdes en rapport til brug for blandt andet ledelsen, forsikringen, Datatilsynet og politiet.

PwC's Cyberhotline

70 222 444

Du kan også læse mere på www.pwc.dk/response

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 vi udarbejdet nedenstående liste, der kan hjælpe virksomheder med at tage stilling til nogle af de vigtigste indsatsområder inden for cyber- og informationssikkerhed. Danske virksomheder har i de senere år arbejdet målrettet med implementering af ISO 27001-standarden som en referenceramme for et basissikkerhedsniveau. Dette har betydet, at der er kommet et øget fokus på en formalisering af processer og styring, og det har medført, at nogle af de nødvendige sikkerhedstiltag af mere teknisk karakter ikke har fået samme fokus, hvilket kan være en af årsagerne til, at virksomhederne er mere sårbare over for de mere målrettede og komplekse cyberangreb.

- ☐ *Har I etableret et formelt sikkerhedsudvalg, med repræsentanter fra virksomhedens topledelse?*
- ☐ *Arbejder I struktureret med risikovurdering ud fra sikkerhedstrusler og sårbarheder?*
- ☐ *Rapporteres virksomhedens sikkerhedsstatus løbende til virksomhedens direktion/bestyrelse?*
- ☐ *Har din virksomhed en CISO/sikkerhedsansvarlig?*
- ☐ *Omfatter arbejdet med sikkerhed både informationssikkerhed (ISO 27001) og cybersikkerhed?*
- ☐ *Har I foretaget en måling på jeres robusthed mod cybertruslerne (cyber assessment)?*
- ☐ *Har I dokumenteret og kommunikeret processer for alle områder af sikkerhed?*
- ☐ *Er der etableret et program for uddannelse og oplysning af medarbejderne omkring sikkerhed?*
- ☐ *Gennemfører I løbende test til identifikation af sårbarheder i jeres infrastruktur og systemer?*
- ☐ *Har I en defineret og afprøvet incident response-proces?*
- ☐ *Har I testet beredskabsplanen for cyberhændelser?*
- ☐ *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?*
- ☐ *Har I implementeret persondataforordningen?*
- ☐ *Er der etableret en driftsorganisation for fortsat sikring af compliance med persondataforordningen?*

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 it-sikkerhed på www.pwc.dk/cybersecurity

Mads Nørgaard Madsen
Partner
Security & Technology
2811 1592
mads.norgaard.madsen@pwc.com

Jørgen Sørensen
Partner
Security & Technology
2494 5254
jorgen.jgs.sorensen@pwc.com

Christian Kjær
Partner
Digital Trust
3945 3282
christian.kjaer@pwc.com

PwC's Incident Response team
70 222 444

Vi har kontorer i 16 byer – også en tæt på dig.

www.pwc.dk

Succes skaber vi sammen ...