Analyse af virksomheders modenhed ift. NIS2-direktivets krav

Udarbejdet for Industriens Fond
april 2023

IRISgroup

Indhold

IRIS GROUP

CHRISTIANS BRYGGE 28, 1. SAL

DK-1559 KØBENHAVN V

IRISGROUP@IRISGROUP.DK

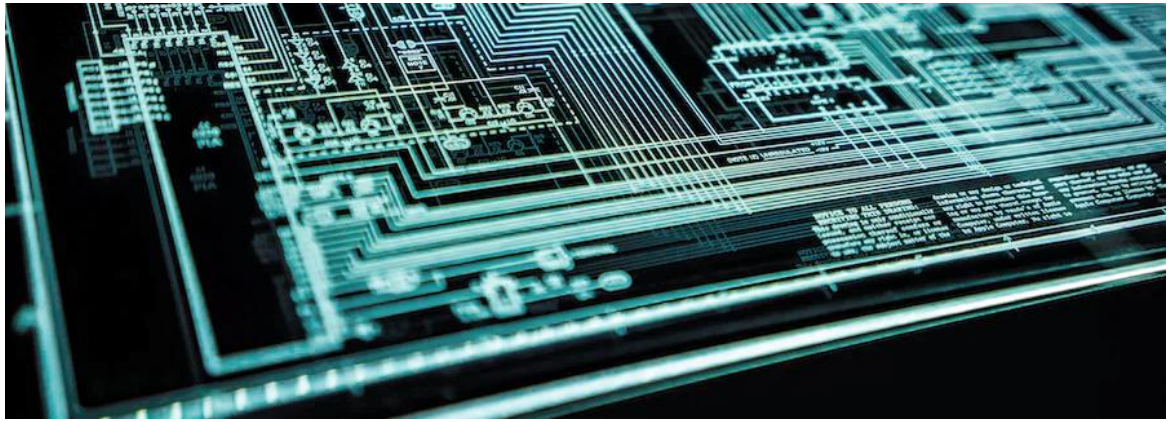
WWW.IRISGROUP.DK

Baggrund og hovedkonklusioner

Hovedkonklusioner

Analysen viser at over 70 pct. af virksomhederne i mindre grad eller slet ikke lever op til samtlige af NIS2-direktivets krav. Derudover er virksomhedernes modenhed ift. at imødekomme direktivet karakteriseret ved følgende:

- Mere end hver femte virksomhed er fortsat i tvivl om, hvorvidt de vil blive berørt af direktivet.
- Hver femte virksomhed, der har sat sig ind i direktivet og som vurderer, at de er omfattet heraf, har i mindre grad eller slet ikke en plan for at leve op til dets krav.
- Mere end hver fjerde SMV har slet ikke sat sig ind i direktivets indhold. For større virksomheder er det kun hver tiende.
- Det er særligt kravene vedrørende politikker for forsyningskædesikkerhed og for vurdering af effektiviteten af IT-sikkerhedsforanstaltninger, som færre virksomheder er rustet til at leve op til.
- Mere end halvdelen af virksomhederne kender ikke til værktøjer, der kan hjælpe dem med at øge deres IT- og informationssikkerhed.
- Virksomhederne efterspørger bl.a. styrket information og vejledning om eksisterende og ny regulering, adgang til best practice cases, kurser og rådgiverhjælp.



Baggrund

Baggrunden for denne analyse er et projekt igangsat af Industriens Fond, der skal belyse danske virksomheders modenhed i forhold til at imødekomme kravene i det kommende NIS2-direktiv fra EU (Direktiv 2022/2555). Analysen skal skabe grundlag for at branche-organisationer, erhvervsfremmeaktører m.fl. kan bistå de berørte virksomheder med relevant information, vejledning og andre relevante tiltag, der sikrer, at virksomhederne kommer i mål og kan opfylde de kommende krav til tiden.

Direktivet forventes fuldt implementeret i oktober 2024 og berører virksomheder i Europa, der vurderes at være af samfundskritisk betydning. Direktivet finder primært anvendelse på mellemstore virksomheder defineret som havende minimum 50 ansatte og en årlig omsætning eller samlet årlig balance på minimum 10 mio. euro. Dog er virksomheder inden for bestemte sektorer omfattet uagtet deres størrelse, fx hvis de udgør særlig kritisk infrastruktur i form af at være fx internetudbydere eller hvis virksomheden er den eneste udbyder af en tjeneste.

IRIS Group har i samarbejde med Industriens Fond og en følgegruppe bestående af en række brancheorganisationer og myndigheder kortlagt de danske virksomheder, der forventes at blive berørt af direktivet. I kortlægningen har IRIS Group identificeret over 1.000 virksomheder inden for 12 sektorer, der forventes berørt af NIS2-direktivet. Enkelte sektorer er ikke inkluderet i kortlægningen jf. bilag 2. Derudover knytter der sig en række udfordringer til kortlægningen af de berørte virksomheder, herunder:

1. Uklarhed om hvordan nogle af sektorerne skal defineres og afgrænses, eftersom dette først lægges endeligt fast i den danske implementeringslovgivning. Denne skal dog først være vedtaget medio oktober 2024 jf. direktivet.
2. Uklarhed om hvilke virksomheder, der er kritiske nok til at omfattes af direktivet, selvom de ikke lever op til størrelseskriterierne.
3. Uklarhed om hvilken sektor visse virksomheder bør tilhøre i tilfælde af, at de har flere aktiviteter.
4. Uklarhed om hvilke underleverandører, der berøres af direktivet. Direktivet stiller bl.a. krav til forsyningskæde- og leverandørsikkerhed, hvorfor flere virksomheder potentielt er omfattet af direktivet end de kortlagte.

Denne analyse bygger på en spørgeskemaundersøgelse foretaget blandt de kortlagte virksomheder, der vurderes at blive omfattet af NIS2-direktivet.

1. Repræsentation

Alle sektorer er fint repræsenteret

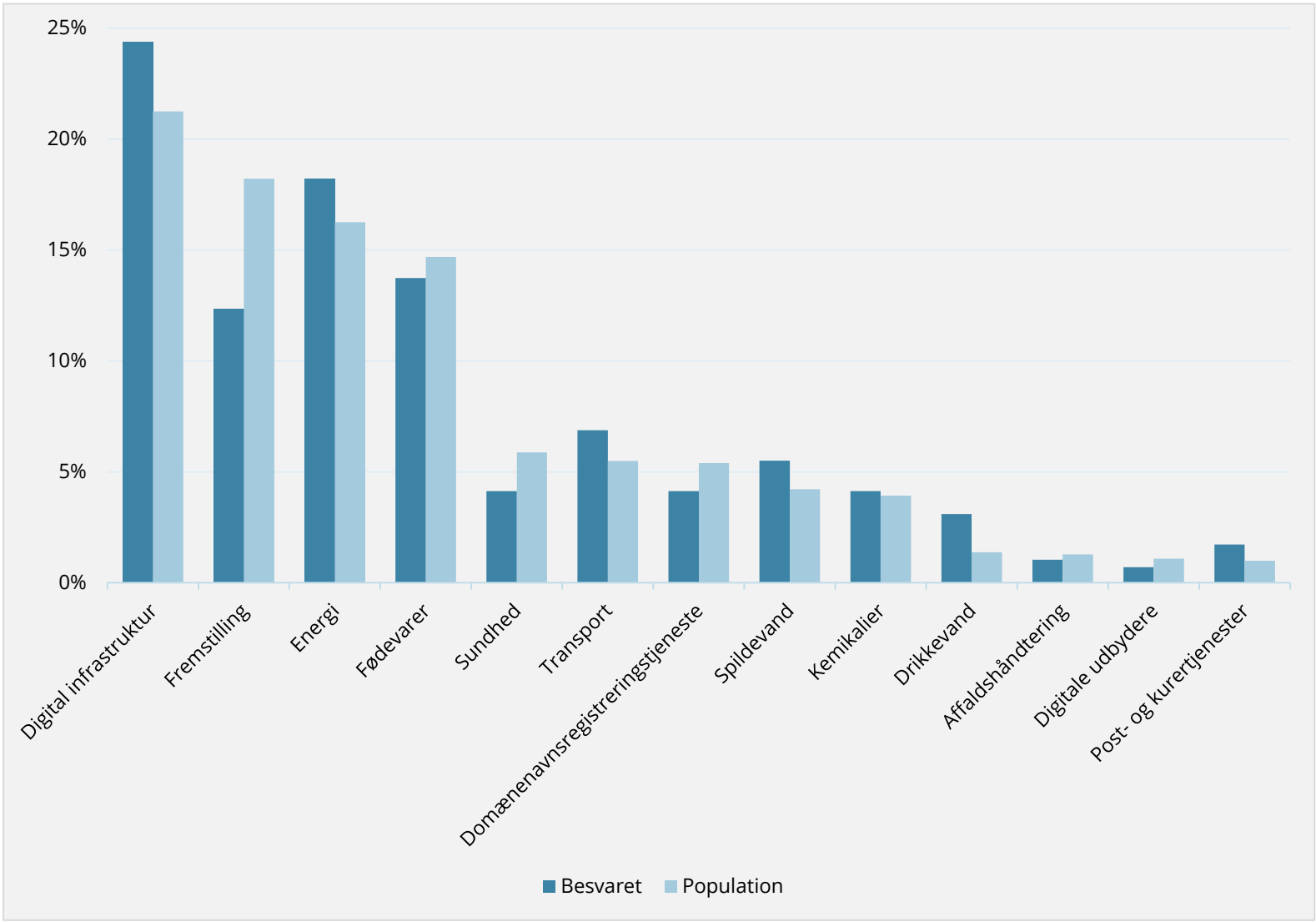
Der blev sendt et spørgeskema ud til de 1.021 virksomheder, som enten havde angivet en e-mailadresse i CVR-registret eller på deres hjemmeside. Det svarer til en dækningsgrad på 94,6 pct. af de virksomheder, der blev identificeret i første fase af analysen som værende potentielt omfattet af direktivet.

IRIS Group blev bistået af en række branche-organisationer i distributionen af spørgeskemaet. Brancheorganisationerne har været behjælpelige med at kontakte deres medlemmer og opfordre dem til at deltage i undersøgelsen. Dette har bidraget til, at den samlede svarprocent er 27,6 pct.

Ved svarfristens udløb kunne det konstateres, at særligt sektorerne "Fremstilling", "Domænenavnsregistrerings-tjenester" og "Digitale udbydere" var underrepræsen-teret i forhold til deres andel i populationen. IRIS Group valgte derfor at sende en ekstra påmindelse ud til disse, hvilket bidrog til at mindske underrepræsentationen.

Figur 1.1 viser repræsentationen af sektorer ved at sammenligne, hvordan besvarelserne og den samlede populationen, er fordelt på sektorer. Figuren viser, at størstedelen af sektorerne er fint repræsenteret i de indsamlede besvarelser. "Fremstilling" er dog underrepræsenteret.

Figur 1.1 Repræsentation af sektorer



Note: N = 291. Søjlerne angiver andele af virksomheder inden for hver sektor, der hhv. har besvaret spørgeskemaet og den andel, de udgør af populationen.

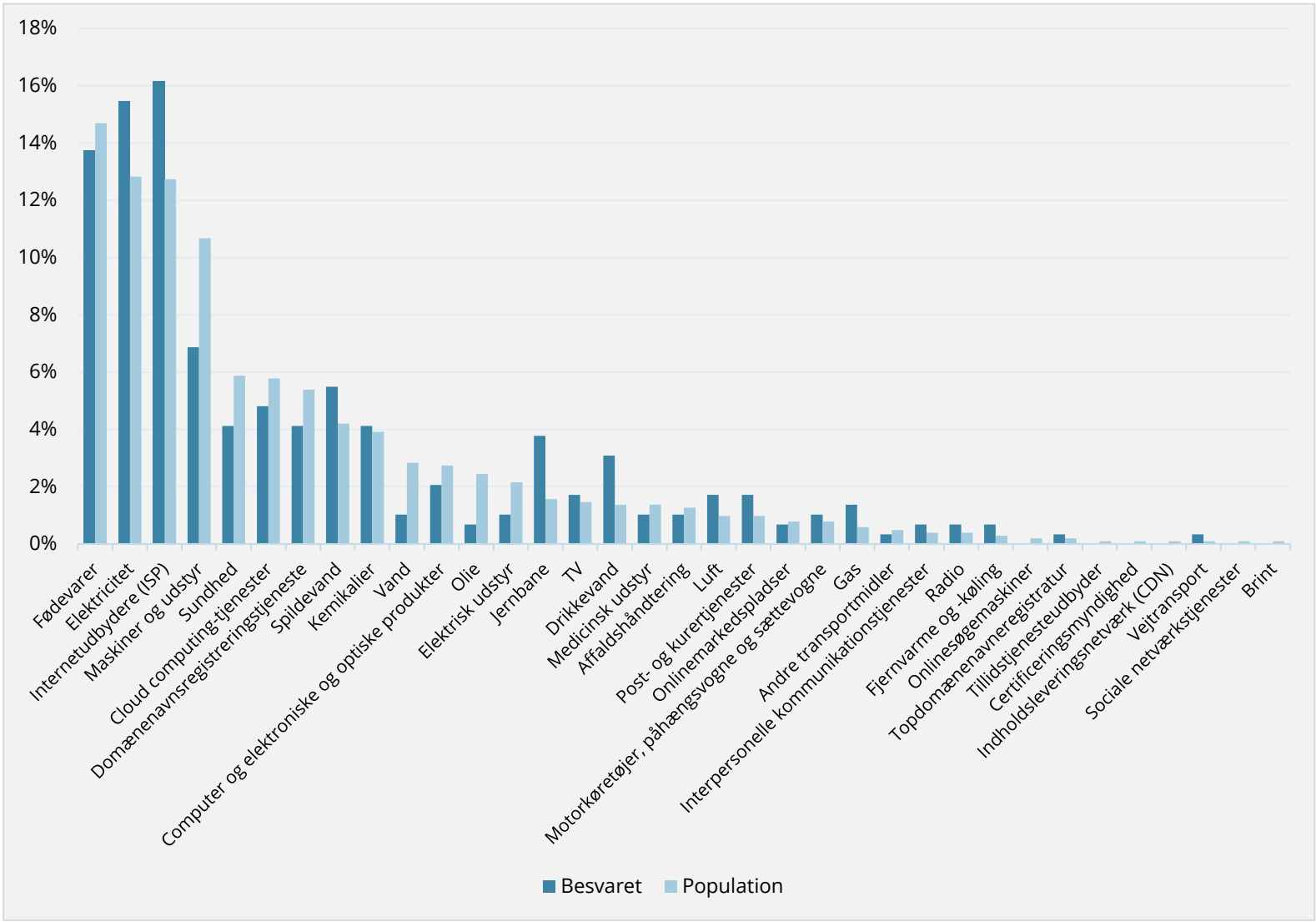
De fleste delsektorer er fint repræsenteret

Figur 1.2 viser hvordan besvarelserne og den samlede population fordeler sig på delsektorer. Figuren viser, at de fleste delsektorer er fint repræsenteret i de indsamlede besvarelser.

Delsektorerne "Elektricitet", "Internetudbydere", "Spildevand", "Jernbane" og "Drikkevand" er lidt overrepræsenteret sammenlignet med deres andel i populationen, mens delsektorerne "Maskiner og udstyr", "Vand", "Olie" og "Elektrisk udstyr" er under-repræsenteret.

Særligt små sektorer, hvor der findes to eller færre virksomheder i populationen, er ikke repræsenteret i undersøgelsen. Det kan både skyldes, at det ikke har været muligt at identificere en e-mailadresse på virksomheden eller fordi denne har valgt ikke at svare på undersøgelsen.

Figur 1.2 Repræsentation af delsektorer



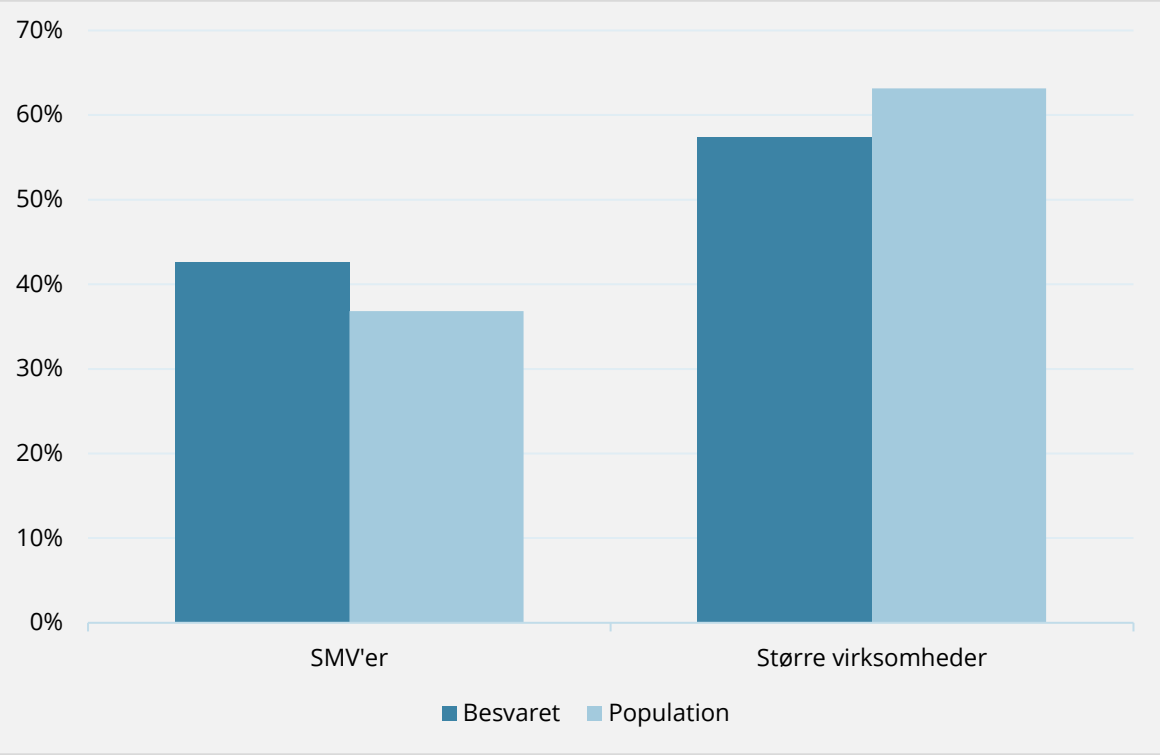
Note: N = 291. Søjlerne angiver andele af virksomheder inden for hver delsektor, der hhv. har besvaret spørgeskemaet og den andel, de udgør af populationen.

SMV'er er marginalt overrepræsenteret i besvarelserne

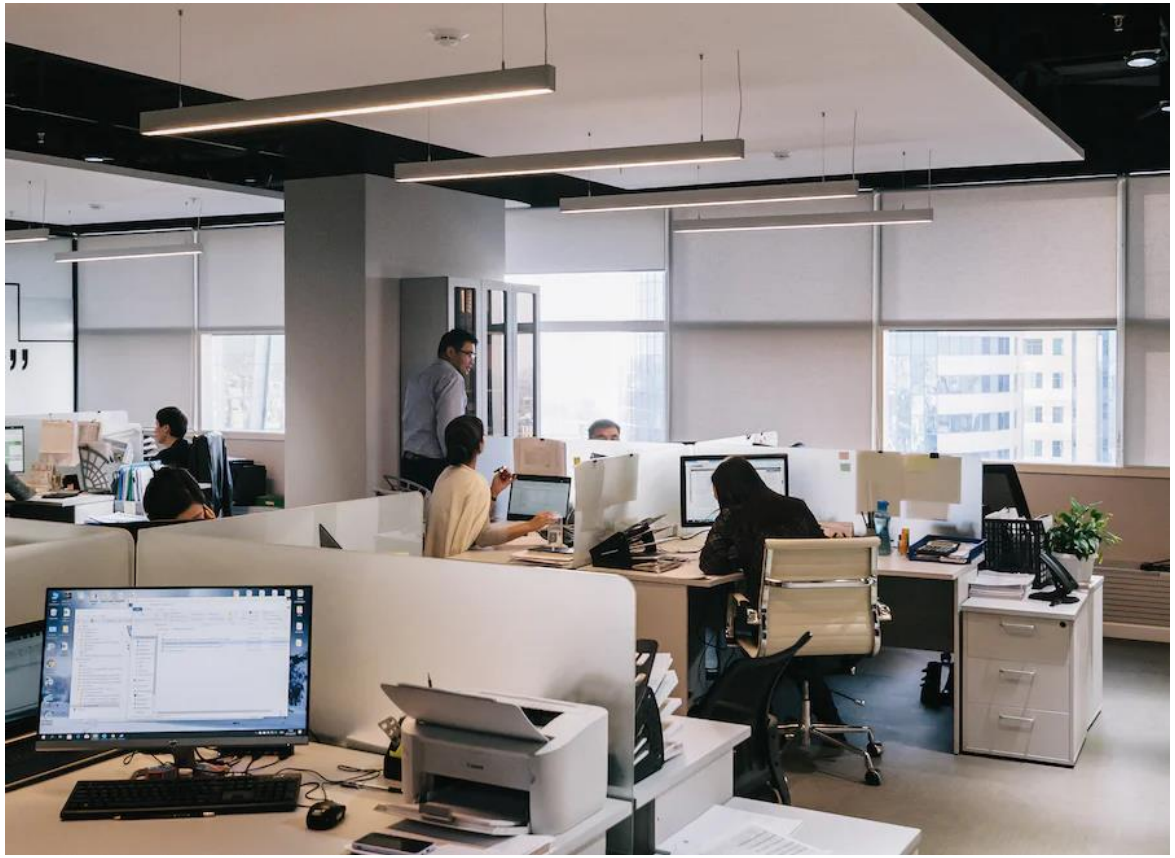
Figur 1.3 andelen af hhv. SMV'er og større virksomheder i populationen og blandt de virksomheder som har besvaret skemaet. Størrelseskategoriseringen følger definitionen i NIS2-direktivets artikel 2, jf. bilag 1.

Figuren viser, at SMV'er er en smule overrepræsenteret i de indsamlede besvarelser, mens større virksomheder er marginalt underrepræsenterede. Dette kan delvist tilskrives distributionen af spørgeskemaet, eftersom det i højere grad var muligt at identificere personlige mails på direktører og ansatte i SMV'er sammenlignet med større virksomheder. Større virksomheder anvender i højere grad info- og service-mails eller kontaktformularer på deres hjemmesider, hvilket gør det sværere for os at rette henvendelse til den rette person. Dette har resulteret i en lavere svarprocent.

Figur 1.3 Repræsentation af virksomhedsstørrelse



Note: N = 291. Søjlerne angiver den procentvise andel, som SMV'er og større virksomheder udgør af de indsamlede besvarelser og den samlede population.



De fleste besvarelser kommer fra IT-ansvarlige eller direktører i virksomhederne

I spørgeskemaet har vi spurgt ind til stillingsbetegnelsen for den person, der har besvaret skemaet på vegne af den pågældende virksomhed.

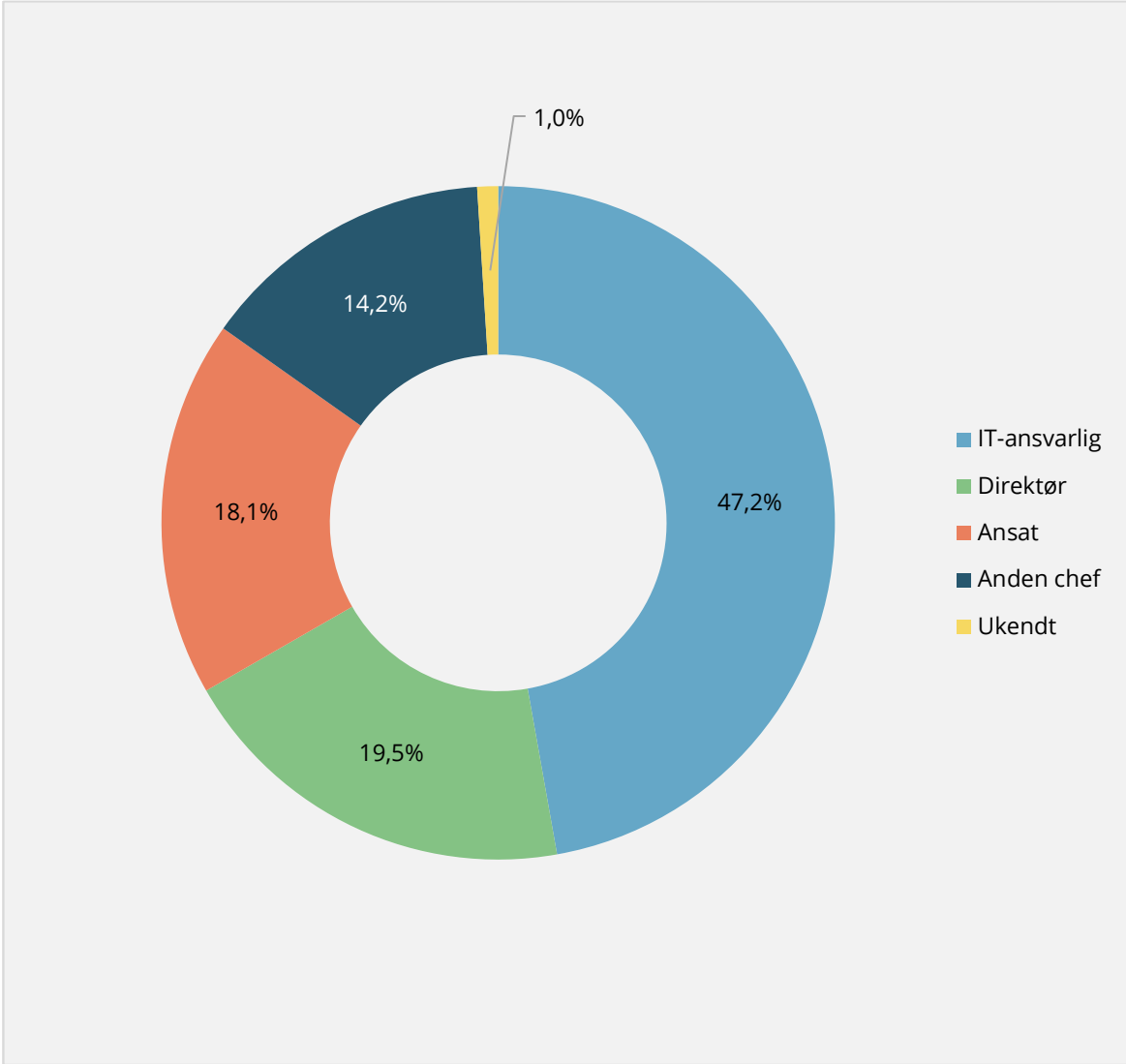
To ud af tre af virksomhedernes besvarelser er afgivet af deres IT-ansvarlige eller direktør. Det styrker validiteten af besvarelserne da disse personer forventes at have et solidt indblik i virksomhedens politikker og procedurer.

Næsten halvdelen af besvarelserne kommer fra IT- og systemansvarlige i virksomhederne. Andelen af af besvarelser, der er indtastet af IT-medarbejdere er højere end 50 pct., hvis man også tæller almindelige IT-ansatte med.

Kategorien "Anden chef" dækker fx over CFO, COO, mv.

Det var ikke muligt at fastslå stillingsbetegnelsen for 3 besvarelser (svarende til 1 pct.).

Figur 1.5 Respondenternes stillingsbetegnelser



Note: N = 282. Virksomhederne havde mulighed for selv at skrive deres stillingsbetegnelse i et frit tekstfelt. Opsummeringen er derfor baseret på tekstanalyse.

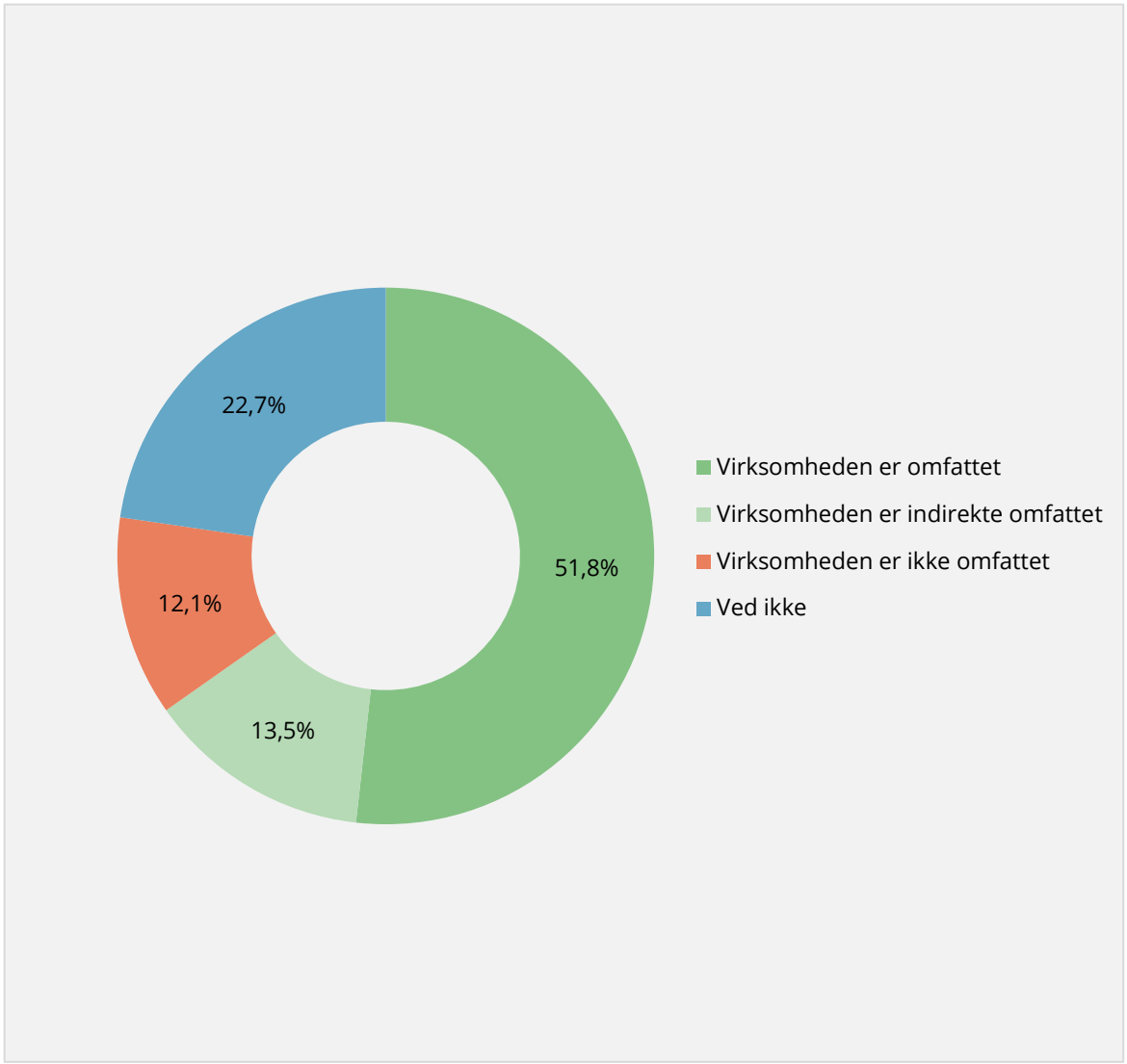
2. Samlede resultater

Mange virksomheder ved ikke, om de er omfattet af NIS2

Virksomhederne er blevet bedt om at angive, om de selv forventer at blive omfattet af NIS2.

Figur 2.2 viser, at næsten to tredjedele af virksomhederne forventer, at de vil blive omfattet af NIS2 enten direkte eller indirekte. Derudover er over hver femte virksomhed i tvivl om, hvorvidt de vil blive berørt af NIS2. Dette kan delvist forklares af, at der på udvalgte områder udestår et arbejde med nærmere at afgrænse hvilke virksomheder, der er omfattet. Dette skal afklares forud for vedtagelse af implementeringslovgivingen, der skal være endeligt på plads i oktober 2024 jf. direktivet.

Figur 2.2 Virksomheder der vurderer sig omfattet af NIS2



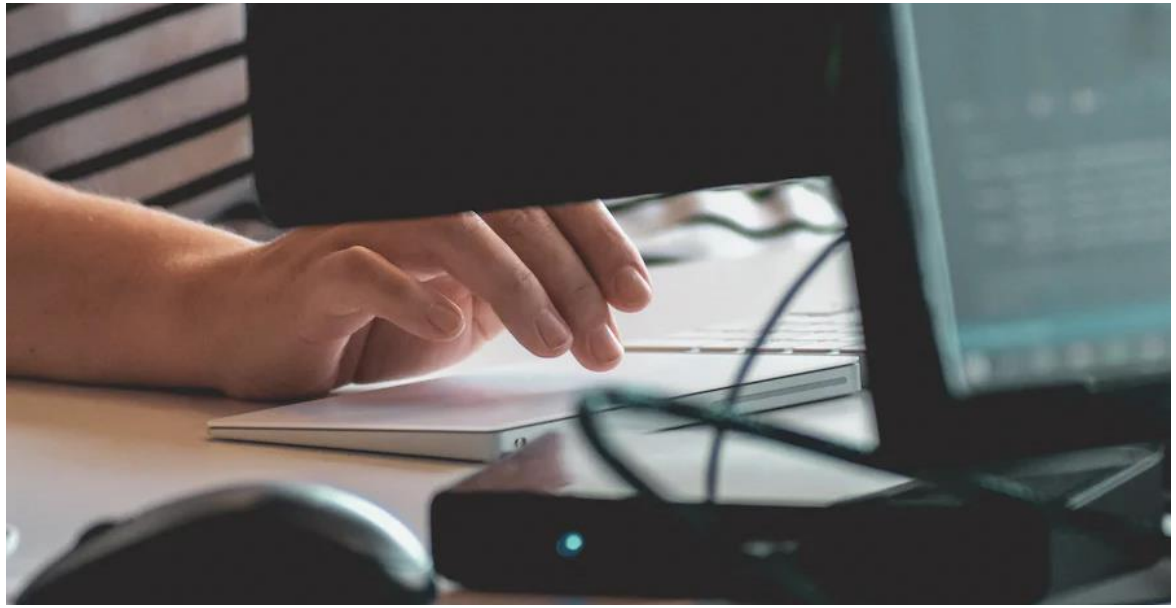
Note: N = 282. Der er her spurgt ind til, om virksomhederne selv vurderer, at de vil blive omfattet af NIS2. Alle adspurgte virksomheder har vi vurderet sandsynligvis vil blive omfattet af NIS2.

IT-ansvaret er hovedsageligt placeret hos en person ansat i virksomhederne

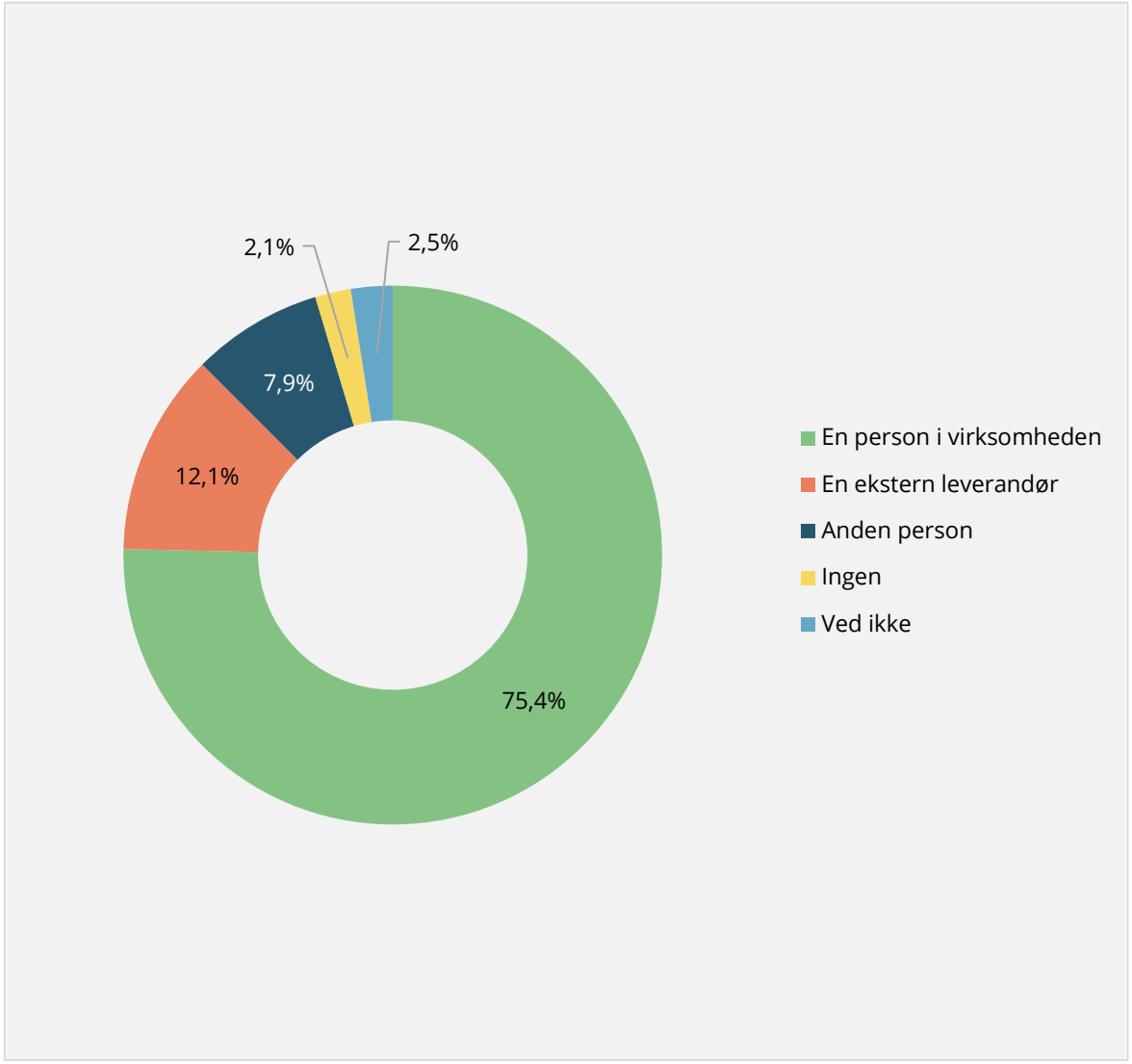
Figuren til højre viser, at tre fjerdedele af virksomhederne angiver, at det er en person ansat i virksomheden, der står for IT- og informationssikkerheden. Dette kan både være en direktør, IT-ansvarlig og almindeligt ansat.

En femtedel af virksomhederne angiver, at det er en ekstern leverandør eller en anden person uden for virksomheden, der er IT-ansvarlig. Det typiske svar ved "anden person" er en person ansat i virksomhedens moderselskab eller udenlandske afdeling.

Eksterne leverandører dækker fx over leverandører af systemer, ydelser og rådgivning.



Figur 2.3 Personer med ansvar for virksomhedernes IT- og informationssikkerhed



Note: N = 280.

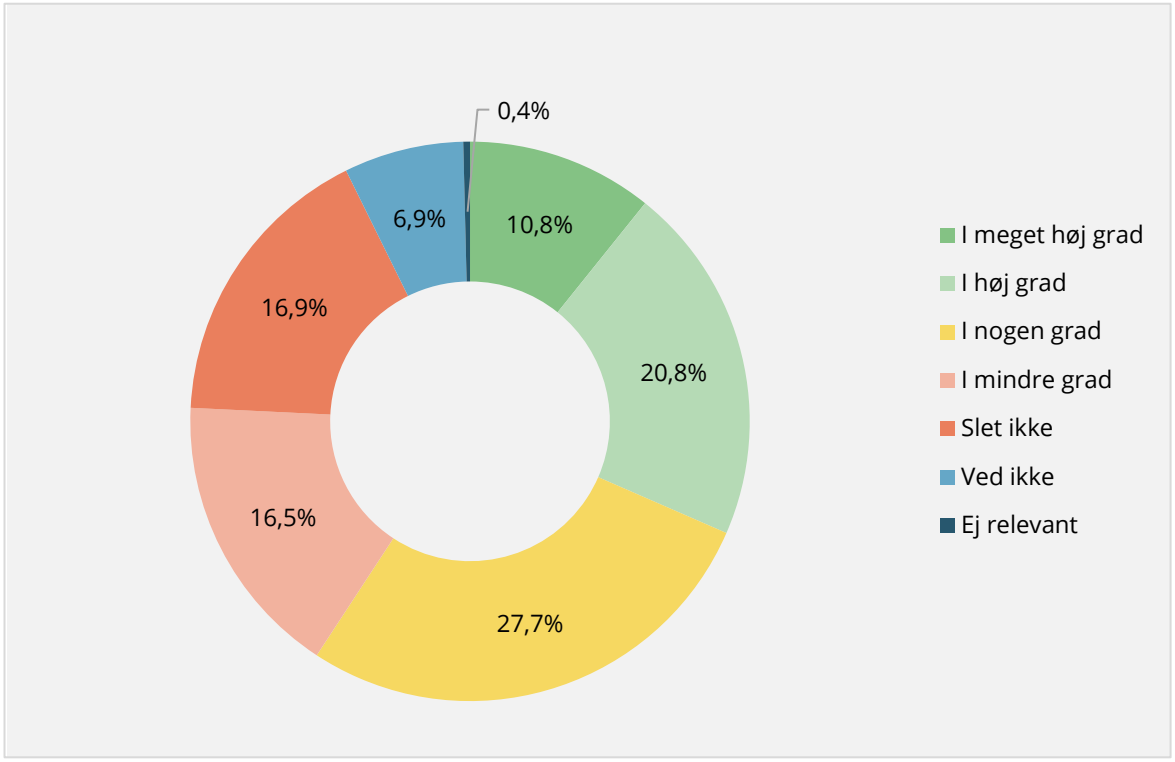
En stor del af virksomhederne har ikke sat sig ind i direktivets indhold og har ikke en plan

Figurerne neden for viser andelen af virksomheder, der angiver at have sat sig ind i NIS2-direktivet samt i hvilken grad de har en plan for at leve op til direktivet.

Figur 2.4 viser, at næsten 60 pct. af virksomhederne angiver, at de i minimum nogen grad sat sig ind i direktivet, mens over en tredjedel i mindre grad eller slet ikke har. Derudover viser figur 2.5, at lidt over halvdelen af virksomhederne svarer, at de som minimum i nogen grad har en plan for at leve op til direktivets krav – mens næsten 40 pct. svarer, at de i mindre grad eller slet ikke har en plan herfor. Det er kun godt 25 pct. af virksomhederne der svarer i høj grad eller meget høj grad på spørgsmålet om de har en plan. Dette kan delvist forklares af, at den danske implementeringslovgivning endnu ikke ligger fast, hvorfor det er uklart præcist hvordan virksomhederne skal leve op til direktivets krav samt hvordan disse skal oversættes til konkrete initiativer.

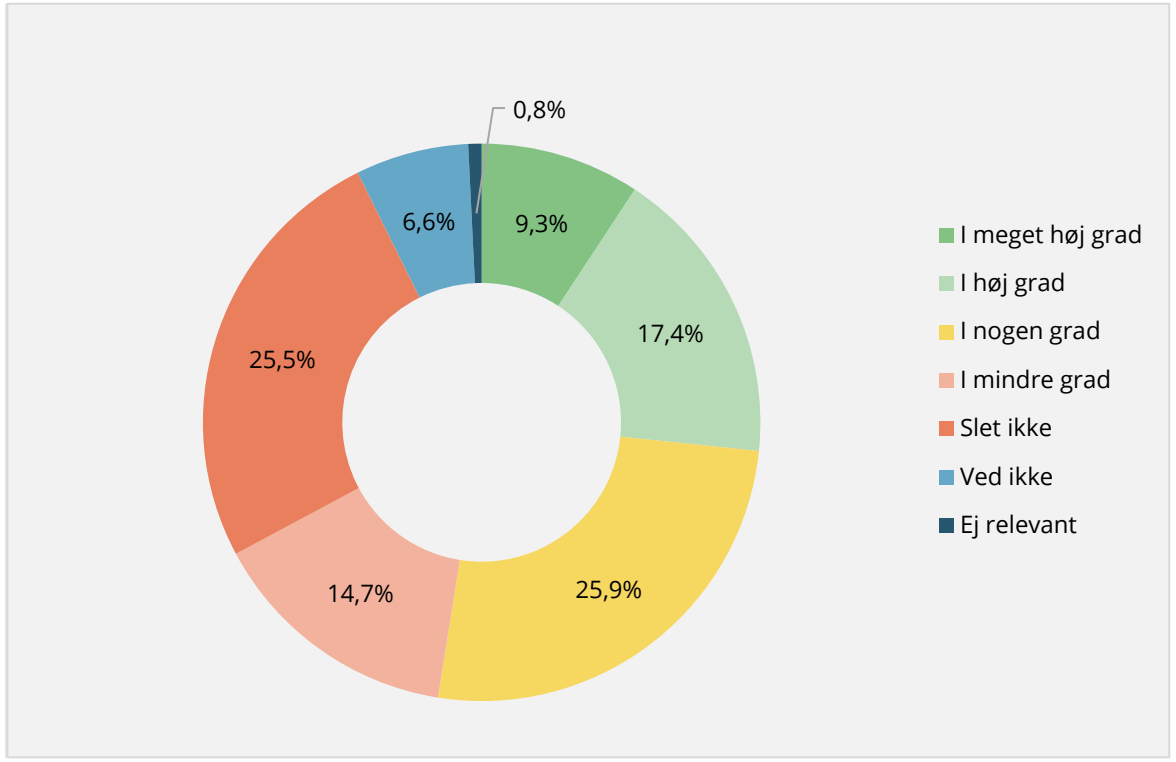
Af de virksomheder, som i minimum nogen grad har sat sig ind i direktivet, mener 85 pct. at de vil blive omfattet af NIS2.

Figur 2.4 Virksomheder fordelt på om de har sat sig ind i direktivet



Note: N = 260.

Figur 2.5 Virksomheder fordelt efter i hvilken grad de har en plan



Note: N = 259.

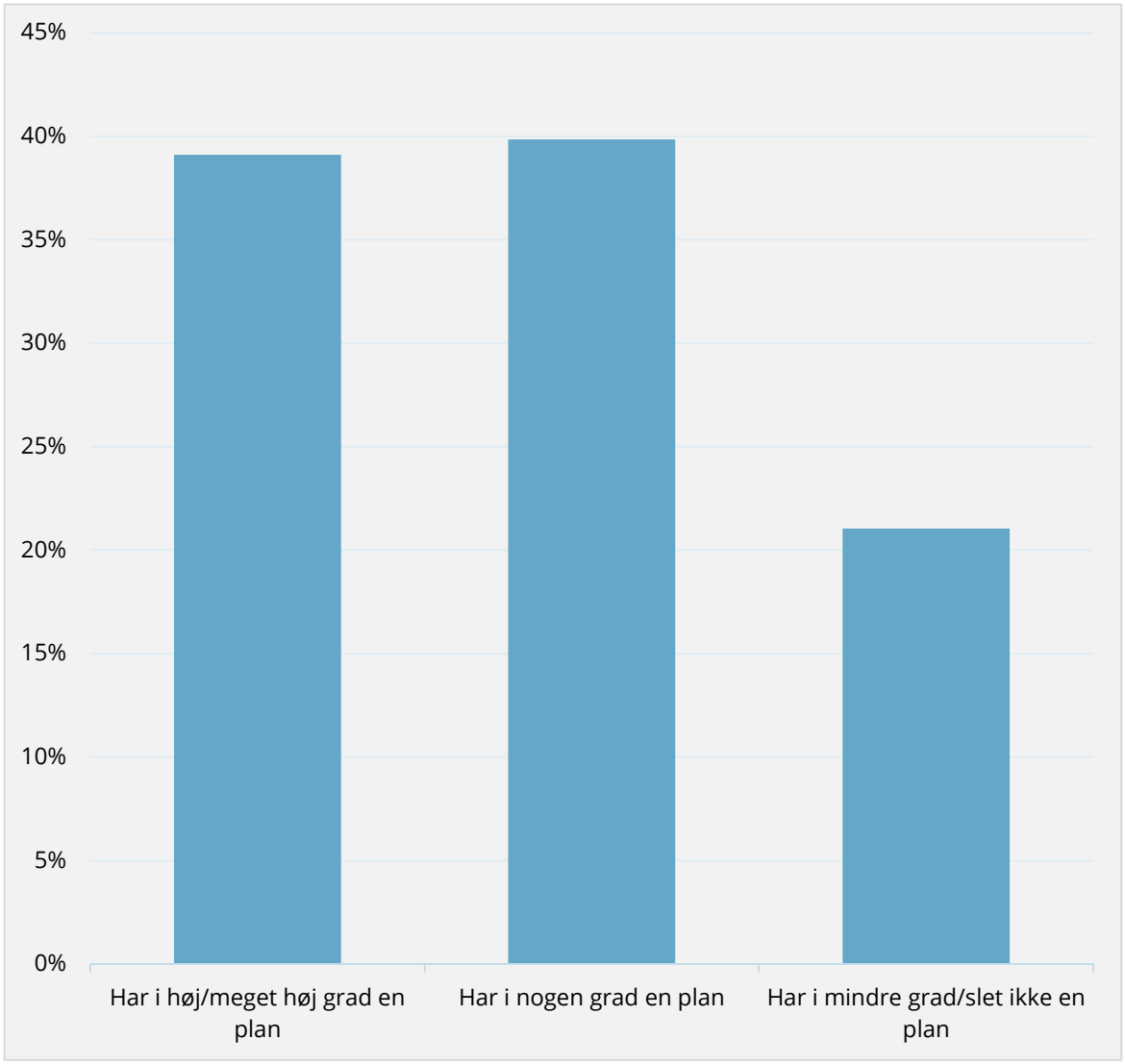
Mere end hver femte virksomhed har i mindre grad eller slet ikke plan

Figur 2.6 viser i hvilken grad de virksomheder, der har sat sig ind i direktivet og vurderer, at de er omfattet, har en plan for at leve op til direktivets krav.

Figuren viser, at ud af de virksomheder, der har sat sig ind i direktivet og som mener, at de er omfattet, har 39 pct. i høj/meget høj grad en plan for at leve op til direktivets krav.

Ca. en femtedel af de virksomheder, der har sat sig ind i direktivet og som mener, at de er omfattet, har i mindre grad eller slet ikke en plan.

Figur 2.6 Virksomheder der har sat sig ind i direktivet fordelt på om de har en plan



Note: N = 133. Der er her filtreret for de virksomheder, der i minimum nogen grad har sat sig ind i direktivet, og som vurderer, at de vil blive omfattet af NIS2.

Virksomhederne planlægger en række forskellige tiltag for at leve op til direktivets krav

Figurerne til højre viser i hvilken grad de virksomheder, der har en plan for at leve op til direktivets krav, vil anvende forskellige ressourcer hertil. De virksomheder, der i mindre grad eller slet ikke har en plan, er ikke inkluderet.

Virksomhederne planlægger en række forskellige tiltag for at leve op til direktivet. De virksomheder, der i høj eller meget høj grad har en plan, planlægger i gennemsnit at iværksætte to ud af de fire forskellige tilgange angivet til højre. Den hyppigste kombination er at afsætte økonomiske ressourcer og anvende interne medarbejderressourcer*.

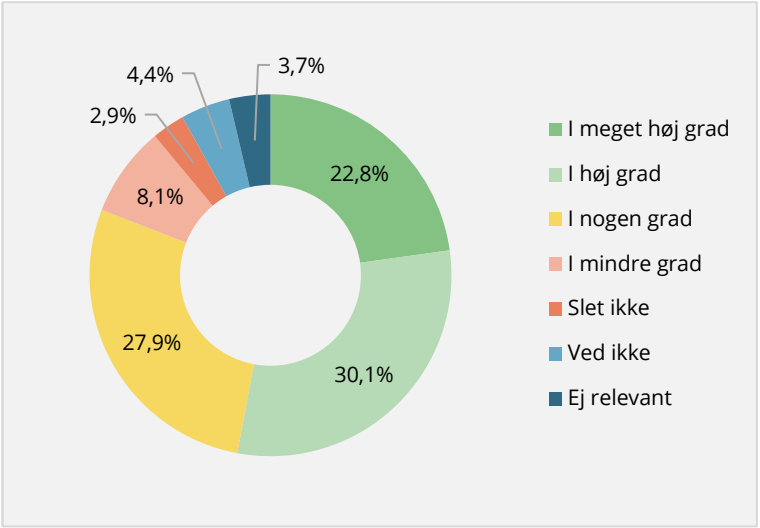
Den største andel af virksomhederne vil anvende interne ressourcer for at leve op til kravene. Omkring otte ud af ti virksomheder planlægger i minimum nogen grad at afsætte økonomiske ressourcer eller anvende interne medarbejderressourcer og mere end halvdelen angiver at de i høj eller meget høj grad vil afsætte økonomiske ressourcer med henblik på at leve op til kravene.

Tre fjerdedele af virksomhederne planlægger i minimum nogen grad at benytte eksterne rådgivere eller leverandører, mens to tredjedele angiver at de vil benytte en standard eller certificering.

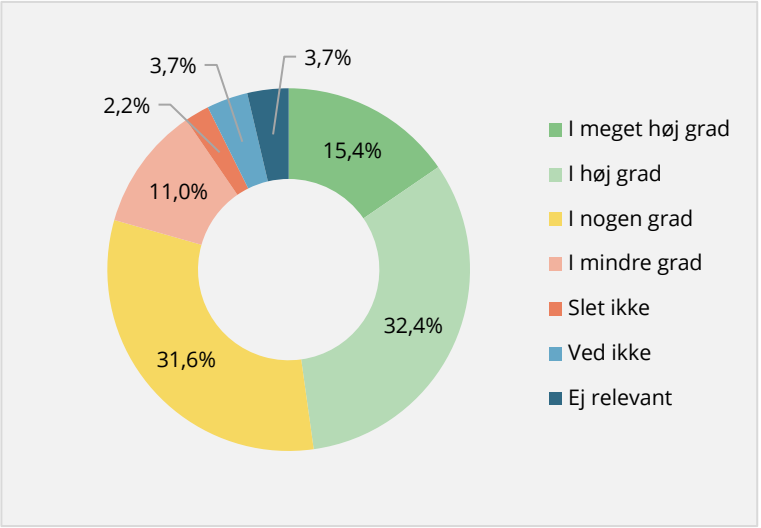
Mere end hver fjerde virksomhed angiver, at de i mindre grad eller slet ikke planlægger at benytte standarder eller certificeringer og ca. 20 pct. af virksomhederne forventer ikke at benytte eksterne rådgivere eller leverandører.

** Disse har en positiv korrelation på 0,74. Det betyder, at virksomheder der i højere grad afsætter økonomiske ressourcer også i høj grad anvender interne medarbejder-ressourcer.*

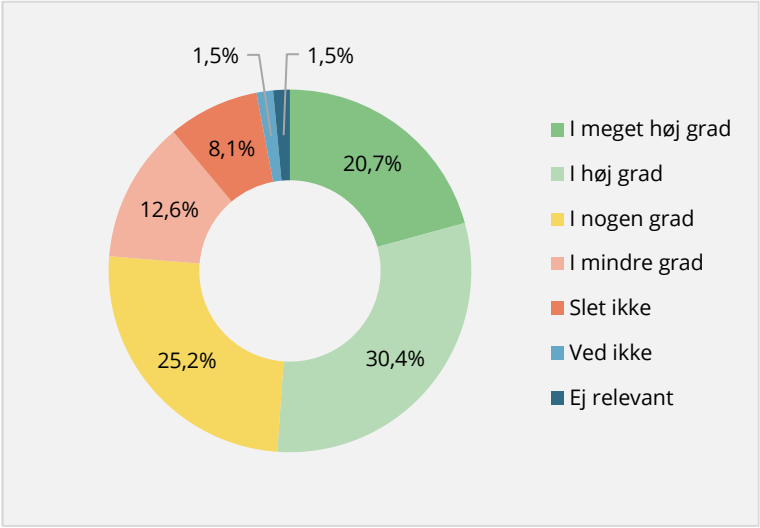
Figur 2.7 Vil afsætte økonomiske ressourcer



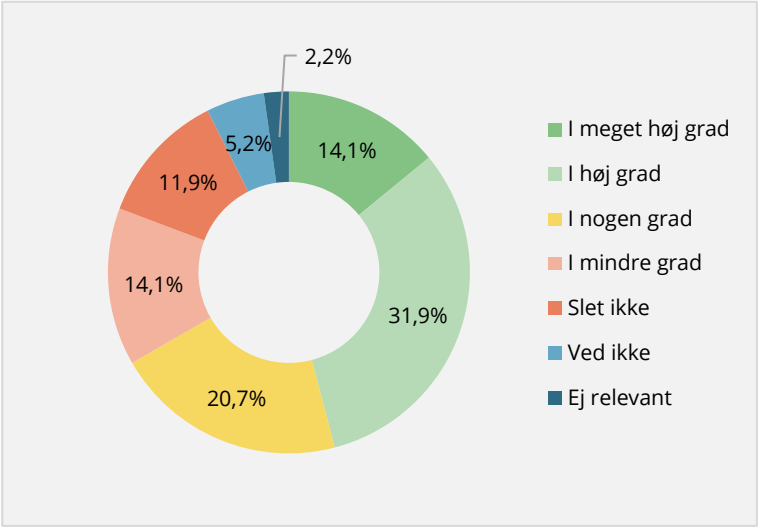
Figur 2.8 Vil anvende interne medarbejderressourcer



Figur 2.9 Vil benytte eksterne rådgivere/leverandører



Figur 2.10 Vil benytte en standard/certificering



Kun 29,2 pct. af virksomhederne lever op til direktivets 10 krav

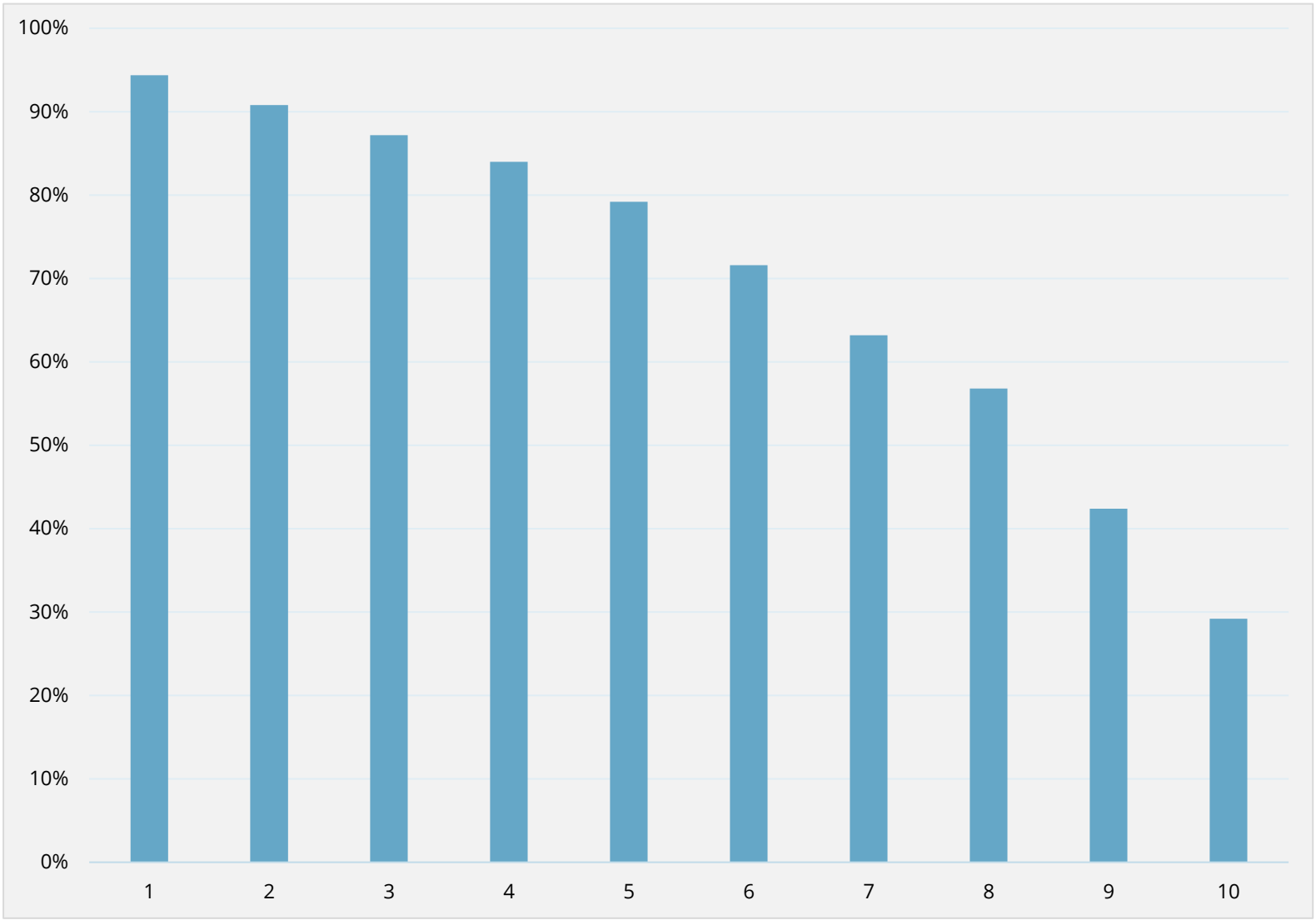
Figuren til højre viser hvor mange af direktivets krav, som virksomhederne i minimum nogen grad lever op til.

Figuren viser, at 94,4 pct. af virksomhederne lever op til mindst ét af direktivets 10 krav, mens kun 29,2 pct. lever op til samtlige af direktivets ti krav. Det betyder, at over 70 pct. af virksomhederne ikke er klar til at efterleve alle direktivets krav på nuværende tidspunkt.

Figuren viser også, at ca. otte ud af ti virksomheder lever op til 5 eller færre af direktivets krav, mens lidt over halvdelen lever op til 8 eller færre krav.

Der er således stor spredning i, hvor mange af direktivets 10 krav, som virksomhederne lever op til på nuværende tidspunkt.

Figur 2.11 Virksomheder fordelt på hvor mange af direktivets krav de lever op til



Note: Figuren illustrerer andelen af virksomheder, der lever op til hhv. 1, 2, 3, mv. af direktivets 10 krav. Virksomhederne kan således gå igen i flere søjler, hvis de opfylder mere end ét krav.

Færre virksomheder lever op til kravene om forsyningskædesikkerhed og test af effektivitet

Figuren til højre illustrerer andelen af virksomheder, der lever op til hvert af direktivets 10 krav til IT- og informationssikkerhed.

Som det fremgår af figuren, lever ni ud af ti virksomheder op til kravet om adgangskontrolpolitikker, mens det er under halvdelen, der lever op til kravet om forsyningskædesikkerhed.

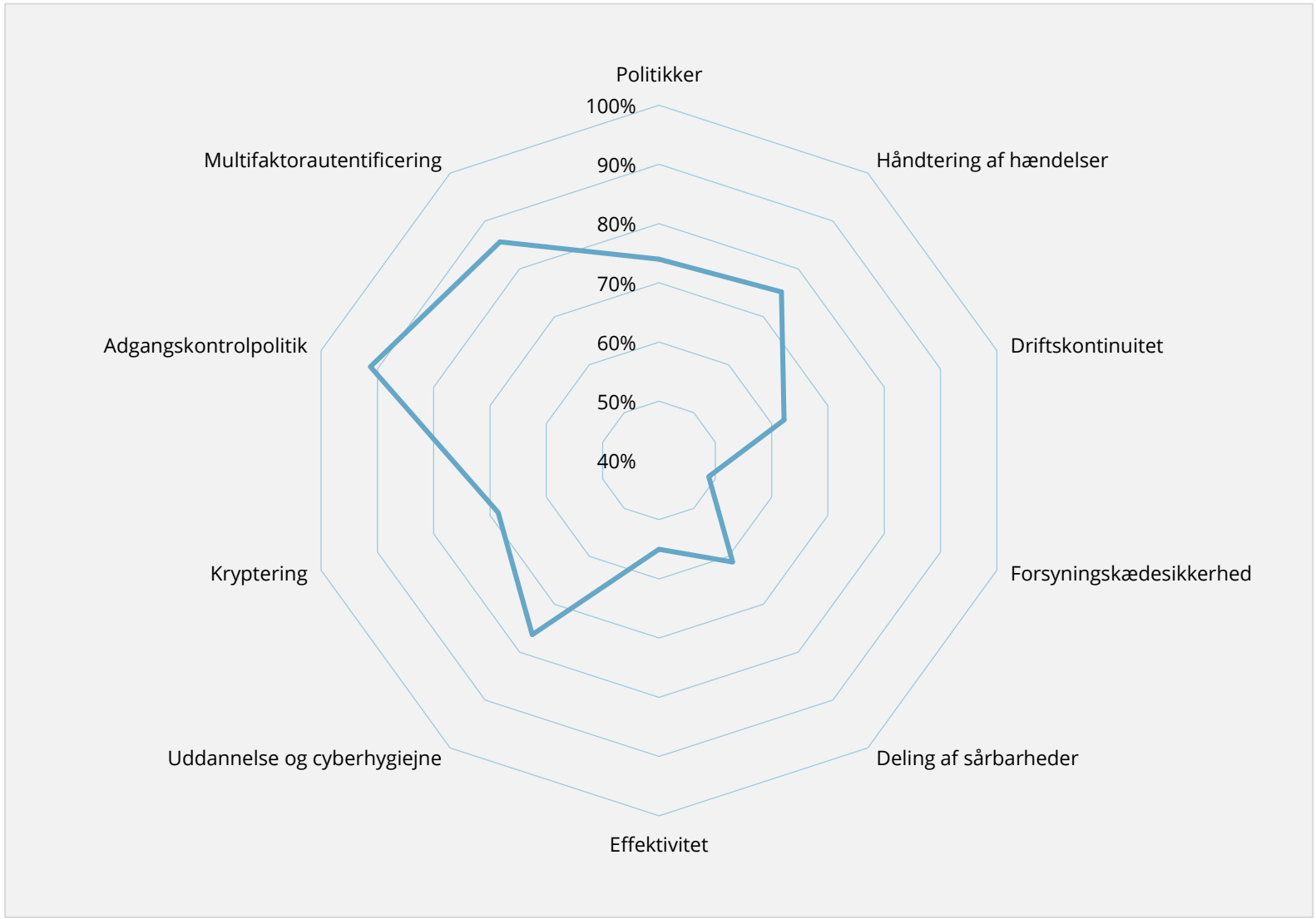
Som vist på forrige side, angiver 29,2 pct. af virksomhederne, at de som minimum i nogen grad lever op til samtlige krav i direktivet. Det betyder, at over 70 pct. ikke er klar til at efterleve direktivets krav. Det er særligt kravet om forsyningskædesikkerhed og vurdering af foranstaltningers effektivitet, der reducerer andelen.

Ca. 75 pct. af virksomhederne har procedurer for håndteringen af sikkerhedshændelser, mens ca. 62 pct. har procedurer for at opretholde virksomhedens drift under en sikkerhedshændelse.

Tallene tegner et billede af, at en større del af virksomhederne har politikker og procedurer til at sikre deres IT- og informationssikkerhed, men at virksomhederne i mindre grad har procedurer til løbende at vurdere effektiviteten af deres foranstaltninger.

Derudover har relativt få virksomheder politikker og procedurer til sikring sikkerheden i forsyningskæden blandt samarbejdspartnere, leverandører og kunder.

Figur 2.12 Andel af virksomheder der lever op til direktivets 10 krav



Note: N = 250. Virksomhederne skal som minimum have svaret "i nogen grad" på spørgsmålene for at blive kategoriseret som at leve op til kravene. Nogle indikatorer er udregnet som indeks over flere spørgsmål. Se bilag 1 for et overblik over hvilke spørgsmål, der afspejler hvilke indikatorer og bilag 2 for en beskrivelse af udregningsmetoden.

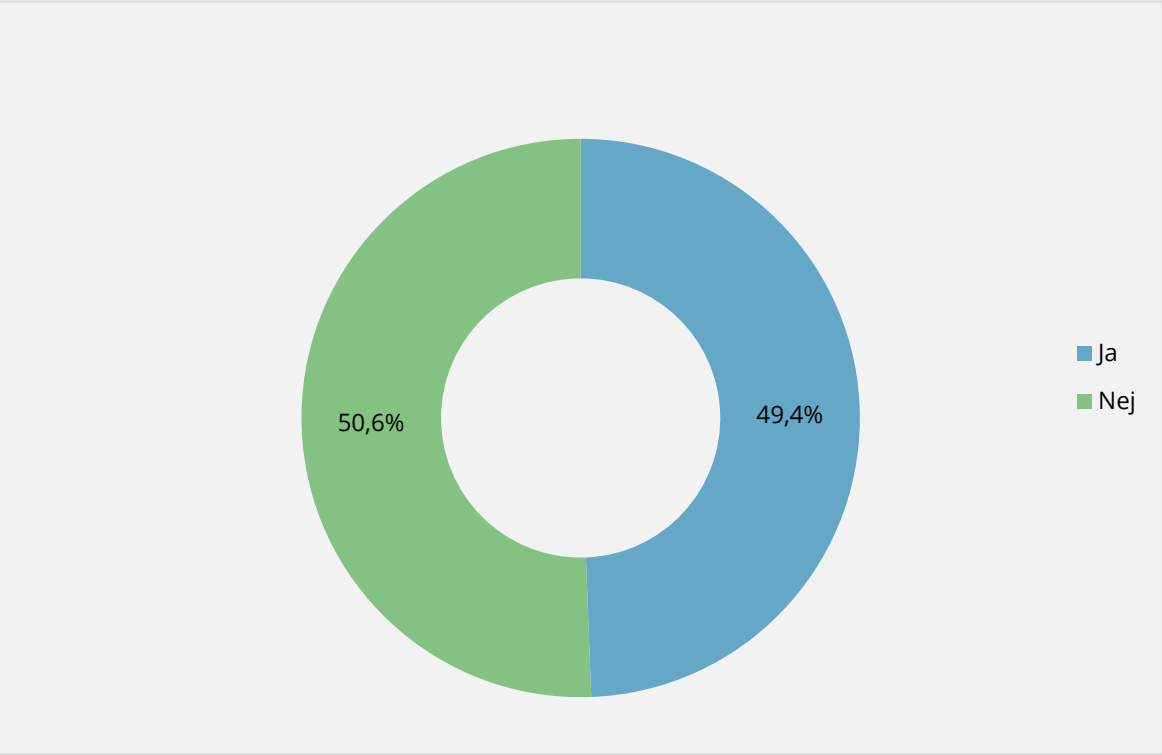
Over halvdelen af virksomhederne kender ikke til hjælpeværktøjer

Figur 2.13 illustrerer andelen af virksomheder, der angiver at kende til værktøjer, der kan hjælpe dem med at øge deres IT- og informationssikkerhed. Ca. halvdelen kender til hjælpeværktøjer.

Figur 2.14 viser de værktøjer, der er hyppigst angivet af de virksomheder, der har angivet at kende til hjælpeværktøjer. Ca. en femtedel af virksomhederne angiver at kende til sikkerdigital, mens 14,6 pct. har skrevet én eller flere standarder og 13,8 pct. har skrevet D-mærket.

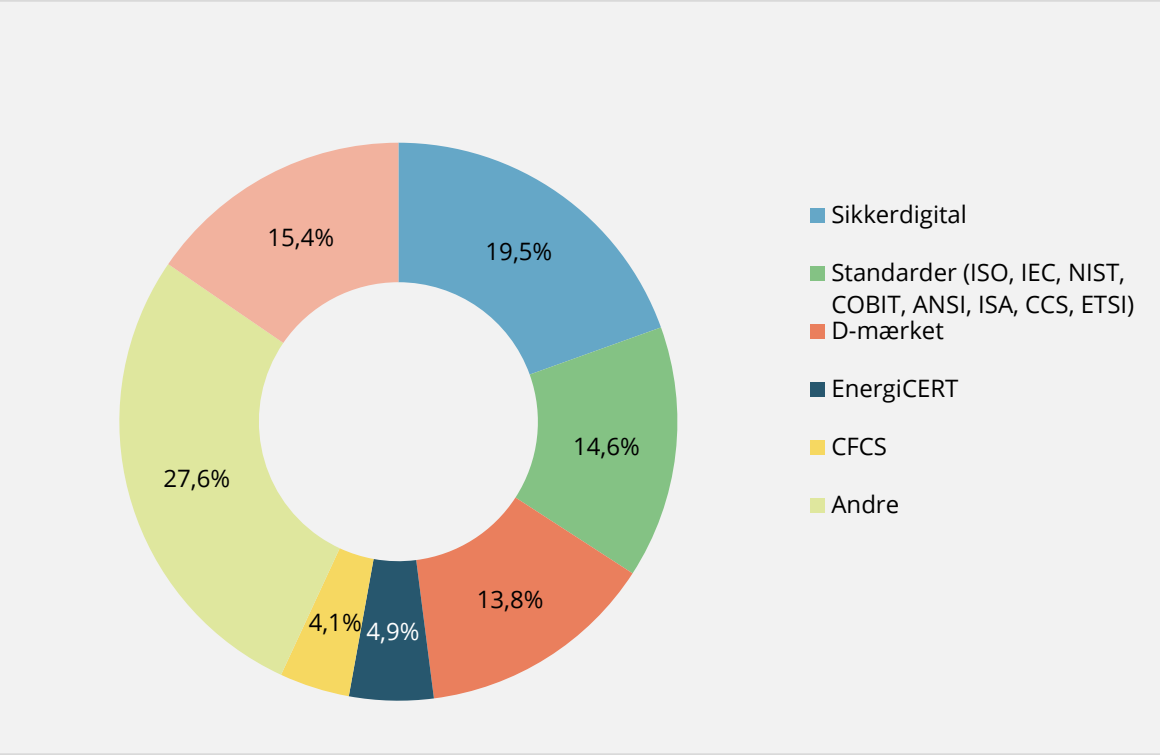
"Andre" dækker fx over specifikke løsninger som Crowdstrike, Darktrace, mv.

Figur 2.13 Virksomheder fordelt på om de kender til hjælpeværktøjer



Note: N = 249.

Figur 2.14 Virksomhedernes kendskab til hjælpeværktøjer



Note: N = 123 Virksomhederne havde mulighed for selv at skrive deres svar i et frit tekstfelt. Opsummeringen er derfor baseret på tekstanalyse. Fordi spørgsmålet var frivilligt, var det muligt for virksomhederne at vælge ikke at besvare det, hvilket 15,4% har valgt ikke at gøre.

Virksomhederne efterspørger i høj grad styrket information og vejledning

Figuren til højre viser andelen af virksomheder, der efterspørger udvalgte tiltag, der kan hjælpe dem med at øge deres IT- og informationssikkerhed.

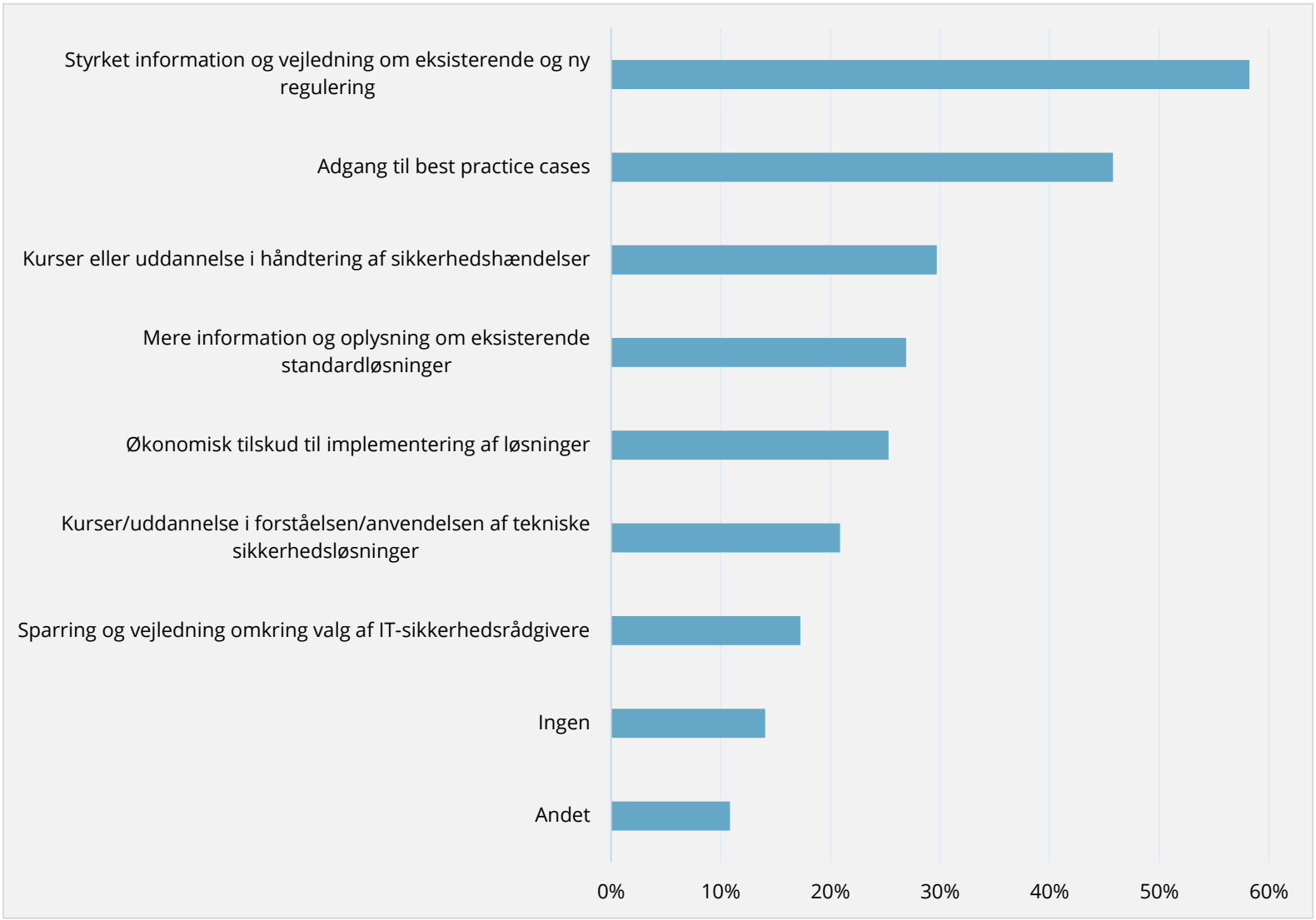
58,2 pct. af virksomhederne efterspørger styrket information og vejledning om eksisterende og ny regulering. Dette kan delvist tilskrives, at det på nuværende tidspunkt endnu ikke er helt klart, hvilke virksomheder der endeligt bliver omfattet af NIS2, eftersom den danske implementeringslovgivning ikke er vedtaget. Det er således forventeligt, at disse efterspørger mere information.

Derudover efterspørger 45,8 pct. af virksomhederne adgang til best practice cases, der fx kan anvendes til at vurdere egne foranstaltninger og praksisser.

En væsentlig andel af virksomhederne ønsker ligeledes kurser eller uddannelse i håndtering af sikkerhedshændelser, mere information om standardløsninger og økonomisk tilskud til implementering af løsninger. Ca. 17 pct. efterspørger sparring og vejledning omkring valg af IT-sikkerhedsrådgivere.

14 pct. angiver, at de ikke efterspørger nogen tiltag, mens ca. 11 pct. angiver andre tiltag end de nævnte. "Andet" dækker fx over afklaring af national implementeringslovgivning, styrkelse af awareness i virksomhederne, mv.

Figur 2.15 Tiltag efterspurgt af virksomhederne, som de mener, kan hjælpe dem med at øge deres IT-sikkerhed



Note: N = 249. Virksomhederne havde mulighed for at vælge mere end én svarmulighed, hvorfor figuren ikke summerer til 100%.

3. Sektorspecifikke resultater

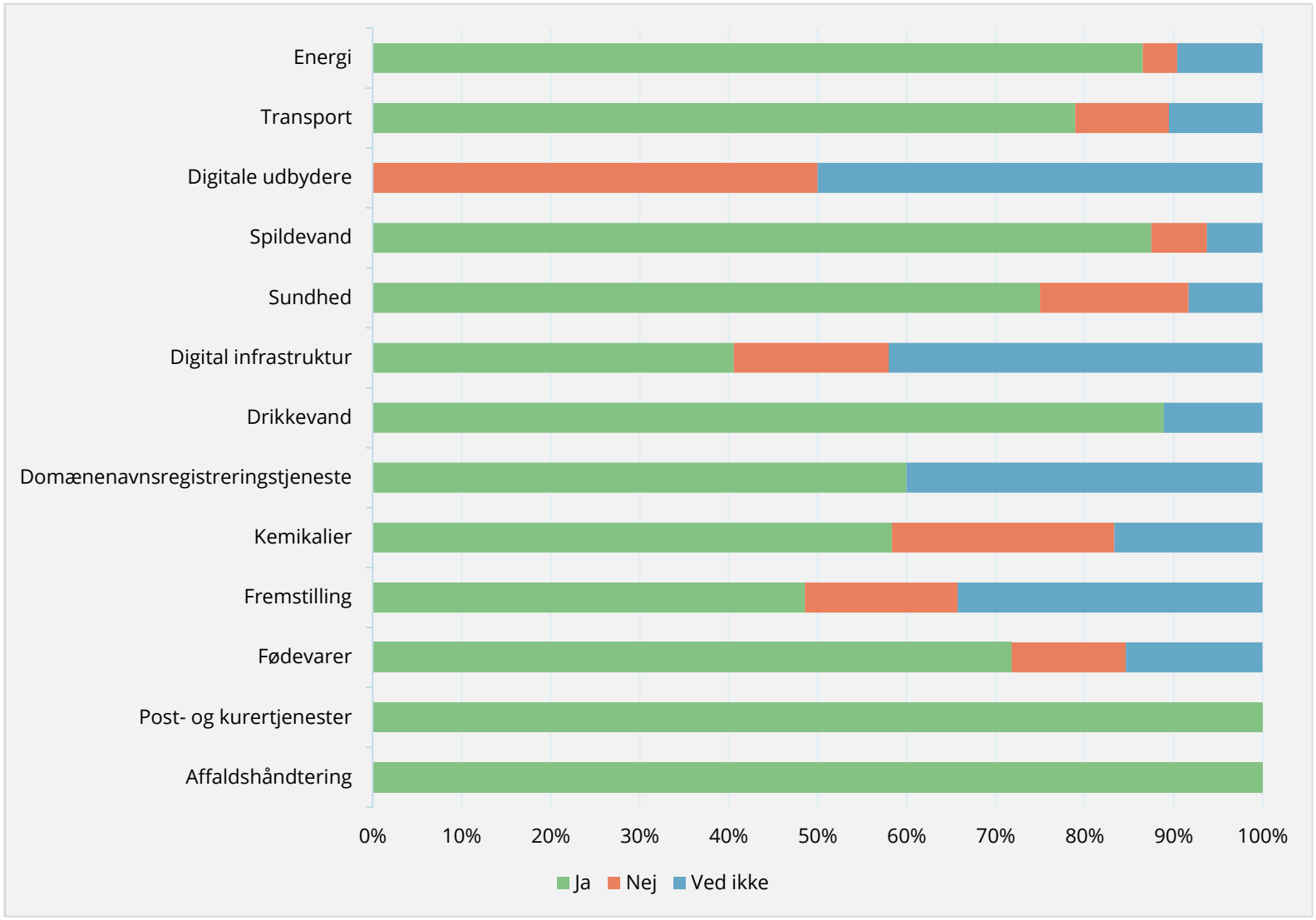
Særligt den digitale sektor og fremstillingsvirksomheder er i tvivl om de er omfattet af NIS2

Figurerne viser andelen af virksomheder, der vurderer, at de er omfattet af NIS1 og vil blive omfattet af NIS2, fordelt på sektorer.

Som figuren til højre viser, vurderer over halvdelen af virksomhederne i de fleste sektorer, at de vil blive omfattet af NIS2 enten direkte eller indirekte.

Særligt de digitale virksomheder er i tvivl om, hvorvidt de vil blive omfattet af NIS2-direktivet. Ca. 40 pct. af virksomhederne i sektorerne "Digital infrastruktur" og "Domænenavnsregistrerings-tjeneste" ved ikke, om de er omfattet.

Figur 3.1 Virksomheder der vurderer sig omfattet af NIS2 fordelt på sektorer



Note: N = 282. Kategorien "Ja" dækker over de virksomheder, der har sagt at de enten direkte eller indirekte vil blive omfattet af NIS2. Sektorerne "Digitale udbydere", "Post- og kurertjenester" og "Affaldshåndtering" har alle færre end 5 besvarelser.

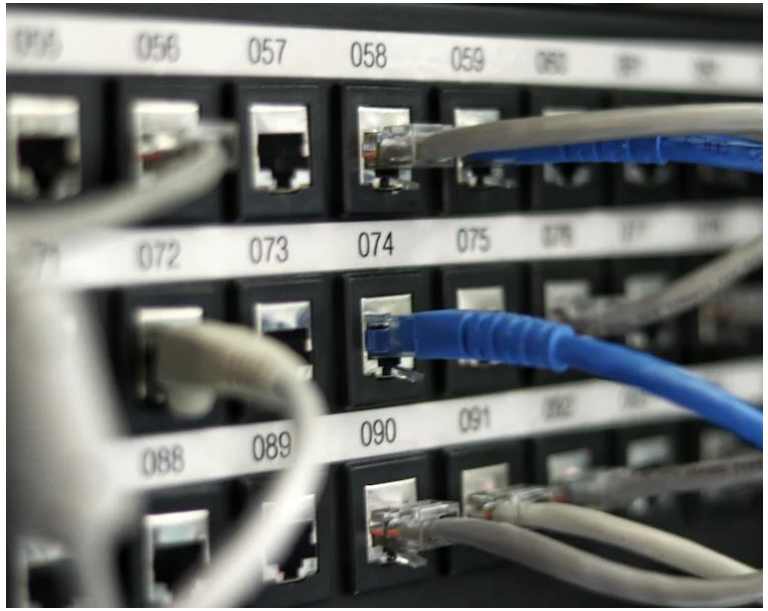
IT-ansvaret er på tværs af sektorer i høj grad placeret internt i virksomhederne

Figuren til højre illustrerer virksomhedernes placering af IT-ansvar opgjort for de berørte sektorer.

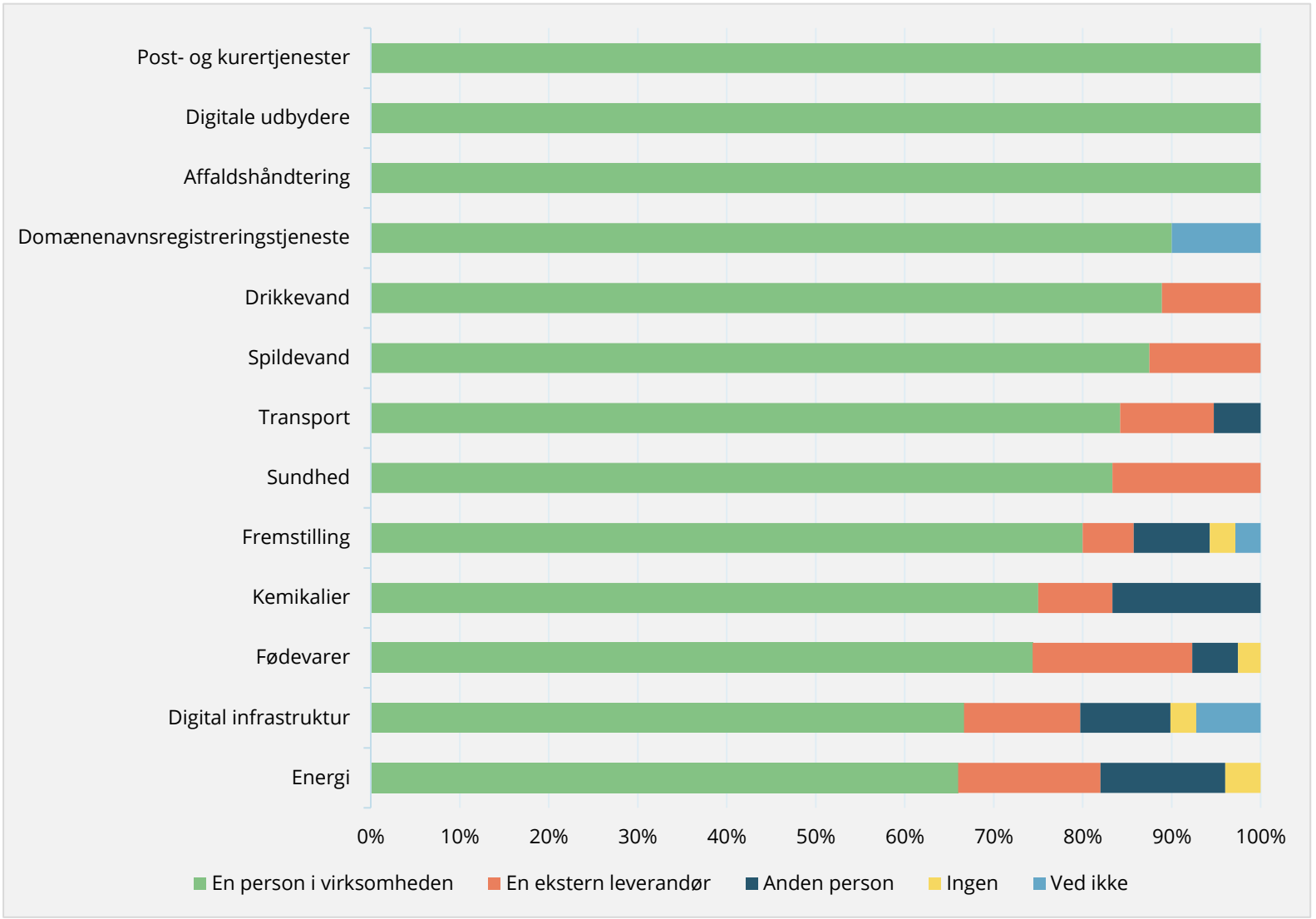
Figuren viser, at næsten alle virksomheder har en IT- og informationssikkerhedsansvarlig. Kun 6 virksomheder, svarende til ca. 2 pct., angiver at ingen har ansvaret herfor.

Figuren viser også, at to tredjedele af virksomhederne i alle sektorer angiver, at det er en intern person i virksomheden, der har ansvaret for IT- og informationssikkerheden.

Ca. en ud af seks virksomheder inden for sektorerne "Sundhed", "Fødevarer" og "Energi" angiver, at en ekstern leverandør har ansvaret for virksomhedens IT og informationssikkerhed.



Figur 3.2 Personer med ansvar for virksomhedernes IT- og informationssikkerhed fordelt på sektorer



Note: N = 280. Sektorerne "Digitale udbydere", "Post- og kurertjenester" og "Affaldshåndtering" har alle færre end 5 besvarelser.

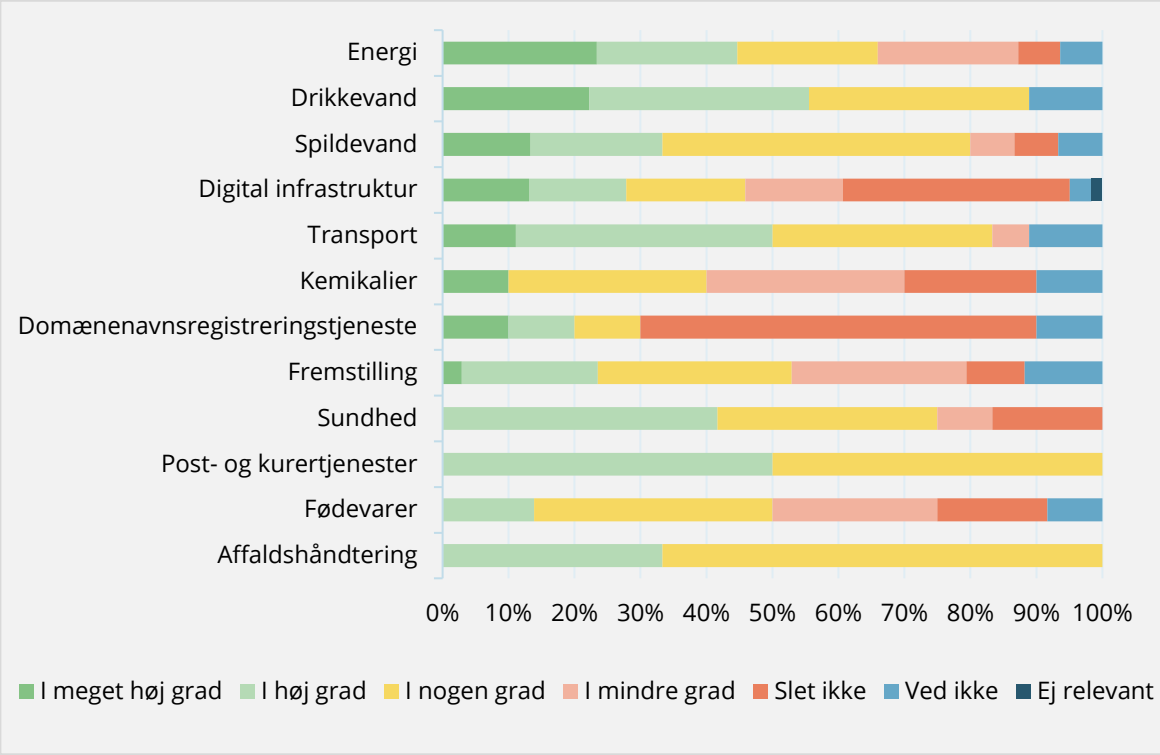
En høj andel af virksomheder inden for alle sektorer har ikke en plan for at leve op til NIS2

Figurerne neden for viser andelen af virksomheder inden for hver sektor, der har sat sig ind i NIS2-direktivet og dets betydning for virksomhederne samt i hvilken grad de har en plan for at leve op til direktivet.

Figur 3.3 viser, at andelen af virksomheder, der har sat sig grundigt ind i NIS2-direktivets indhold, er lav. Dog har en væsentlig del af virksomhederne i minimum nogen grad sat sig ind i direktivet. Inden for de digitale sektorer er der imidlertid en markant del af virksomhederne, der slet ikke har sat sig ind i direktivet. Dette kan bunde i, at de muligvis vurderer, at de ikke vil blive berørt af direktivet.

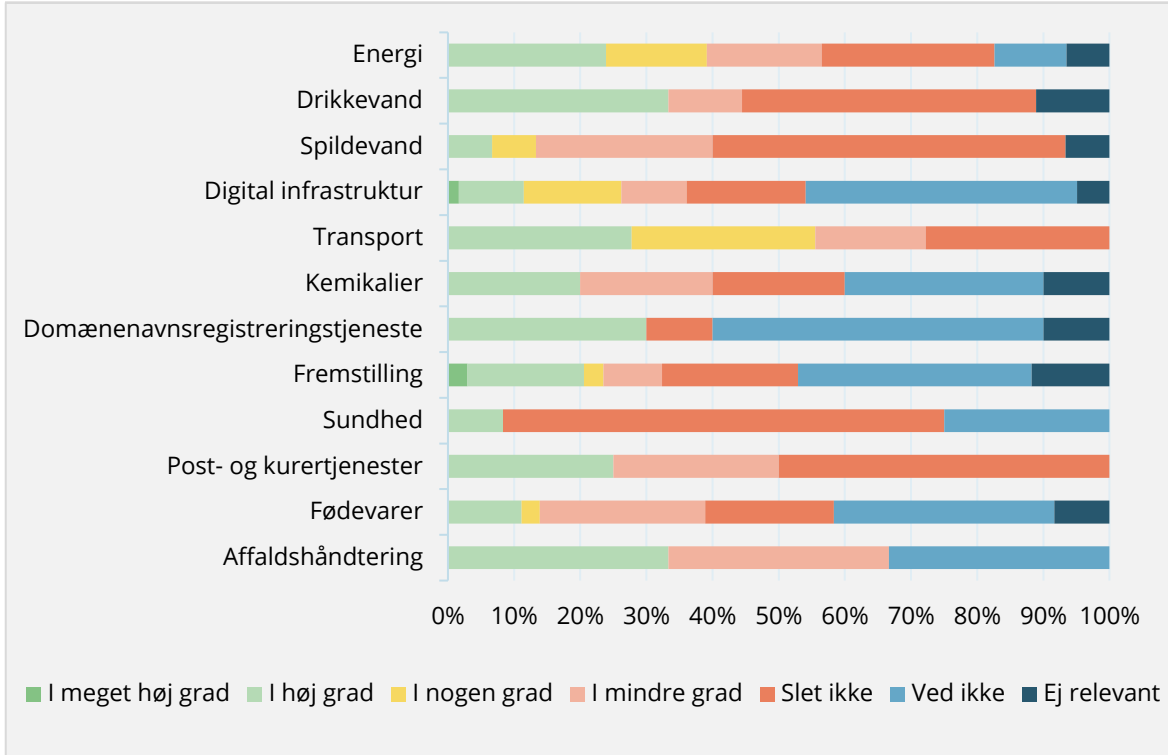
Figur 3.4 viser, at en meget lille del af virksomhederne på tværs af sektorerne har en plan for at leve op til direktivet, og at en markant del slet ikke har/ikke ved om de har en plan herfor.

Figur 3.3 Virksomhederne fordelt på sektorer efter om de har sat sig ind i direktivet



Note: N = 260. Sektoren "Digitale udbydere" er ikke inkluderet i figuren, eftersom kun én virksomhed har besvaret spørgsmålene. Sektorerne "Digitale udbydere", "Post- og kurertjenester" og "Affaldshåndtering" har alle færre end 5 besvarelser.

Figur 3.4 Virksomhederne fordelt på sektorer efter om de har en plan



Note: N = 259. Sektoren "Digitale udbydere" er ikke inkluderet i figuren, eftersom kun én virksomhed har besvaret spørgsmålene. Sektorerne "Digitale udbydere", "Post- og kurertjenester" og "Affaldshåndtering" har alle færre end 5 besvarelser.

Sektorerne planlægger at anvende alle ressourcer, men i forskelligt omfang

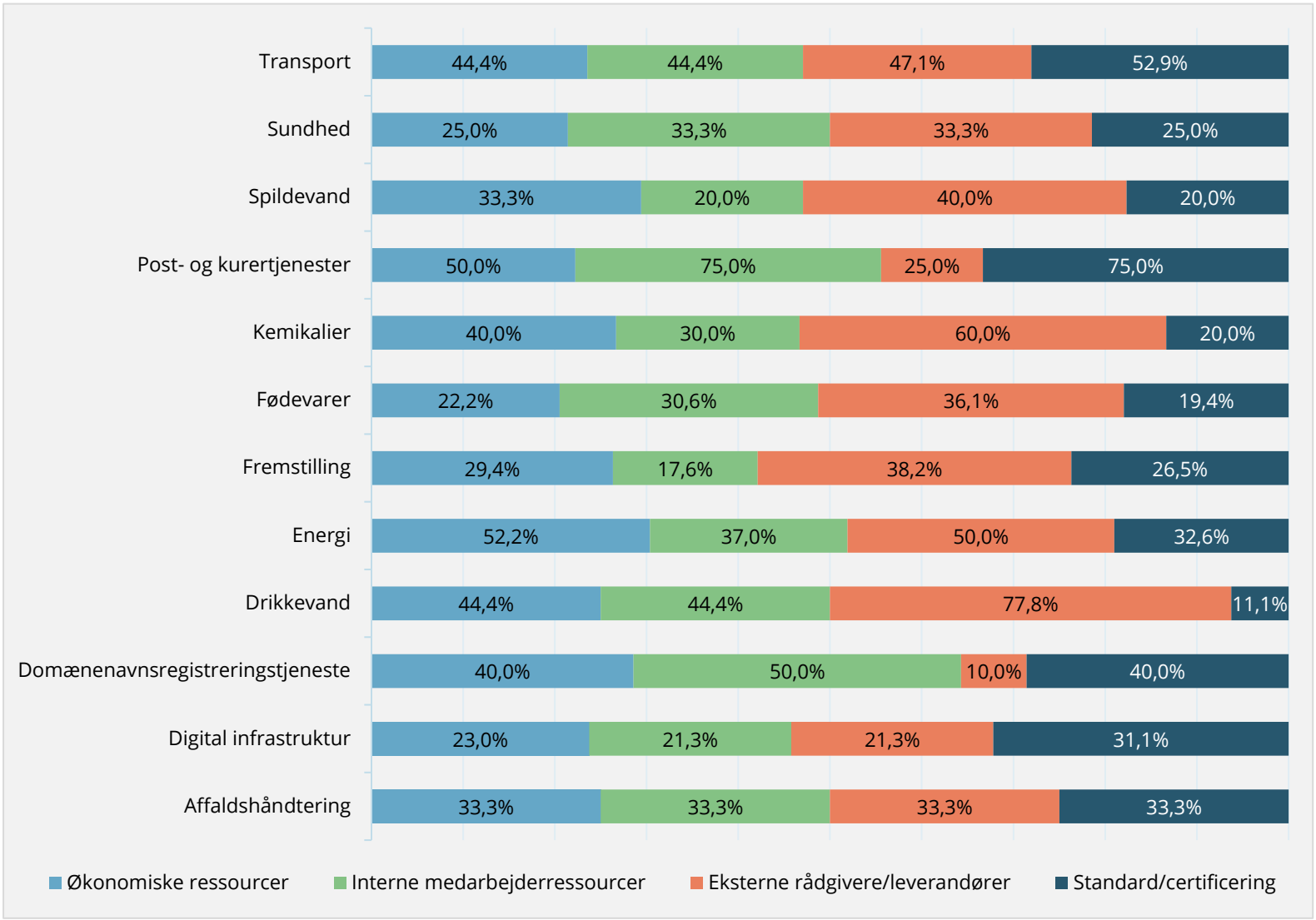
Figuren til højre viser i hvilken grad de virksomheder, der har en plan for at leve op til direktivets krav, i høj eller meget høj grad planlægger at anvende forskellige ressourcer hertil, fordelt på sektorer. De virksomheder, der i mindre grad eller slet ikke har en plan, er ikke inkluderet. Virksomhederne havde mulighed for at angive mere end ét svar.

Fælles for alle sektorer er, at mange virksomheder planlægger at benytte mere end én metode til at leve op til direktivets krav. Særligt sektorerne "Digital infrastruktur" og "Transport" har planer om at kombinere metoderne, eftersom de planlægger i gennemsnit at benytte hhv. 3 og 4 af metoderne angivet i figuren. "Fremstilling" planlægger til sammenligning blot at bruge én metode i gennemsnit.

Virksomhederne planlægger i vid udstrækning at anvende økonomiske ressourcer og eksterne rådgivere eller leverandører for at leve op til direktivets krav.

Særligt sektorerne "Post- og kurertjenester" og "Domænenavnsregistreringstjeneste" planlægger at anvende interne medarbejderresourcer for at leve op til direktivets krav, mens sektorerne "Kemikalier" og "Drikkevand" i højere grad planlægger at benytte eksterne rådgivere eller leverandører. Derudover vil sektorerne "Transport" og "Post- og kurertjenester" i højere grad benytte standarder eller certificeringer.

Figur 3.5 Indholdet af virksomhedernes plan for at leve op til direktivet fordelt på sektorer



Note: N = 259. Sektoren "Digitale udbydere" er ikke inkluderet i figuren, eftersom kun én virksomhed har besvaret spørgsmålene. Virksomhederne har mulighed for at benytte mere end én metode til at leve op til direktivet, hvorfor figuren ikke summerer til 100% inden for hver sektor. Sektorerne "Digitale udbydere", "Post- og kurertjenester" og "Affaldshåndtering" har alle færre end 5 besvarelser.

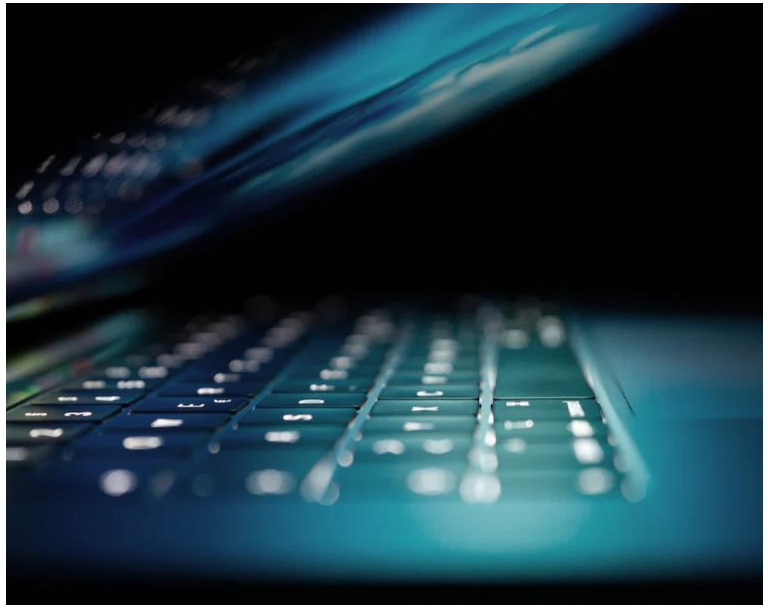
Stor variation i andelen af virksomheder, der lever op til direktivets krav, på tværs af sektorer

Figuren til højre viser andelen af virksomheder inden for hver sektor, der i minimum nogen grad lever op til alle kravene i direktivet.

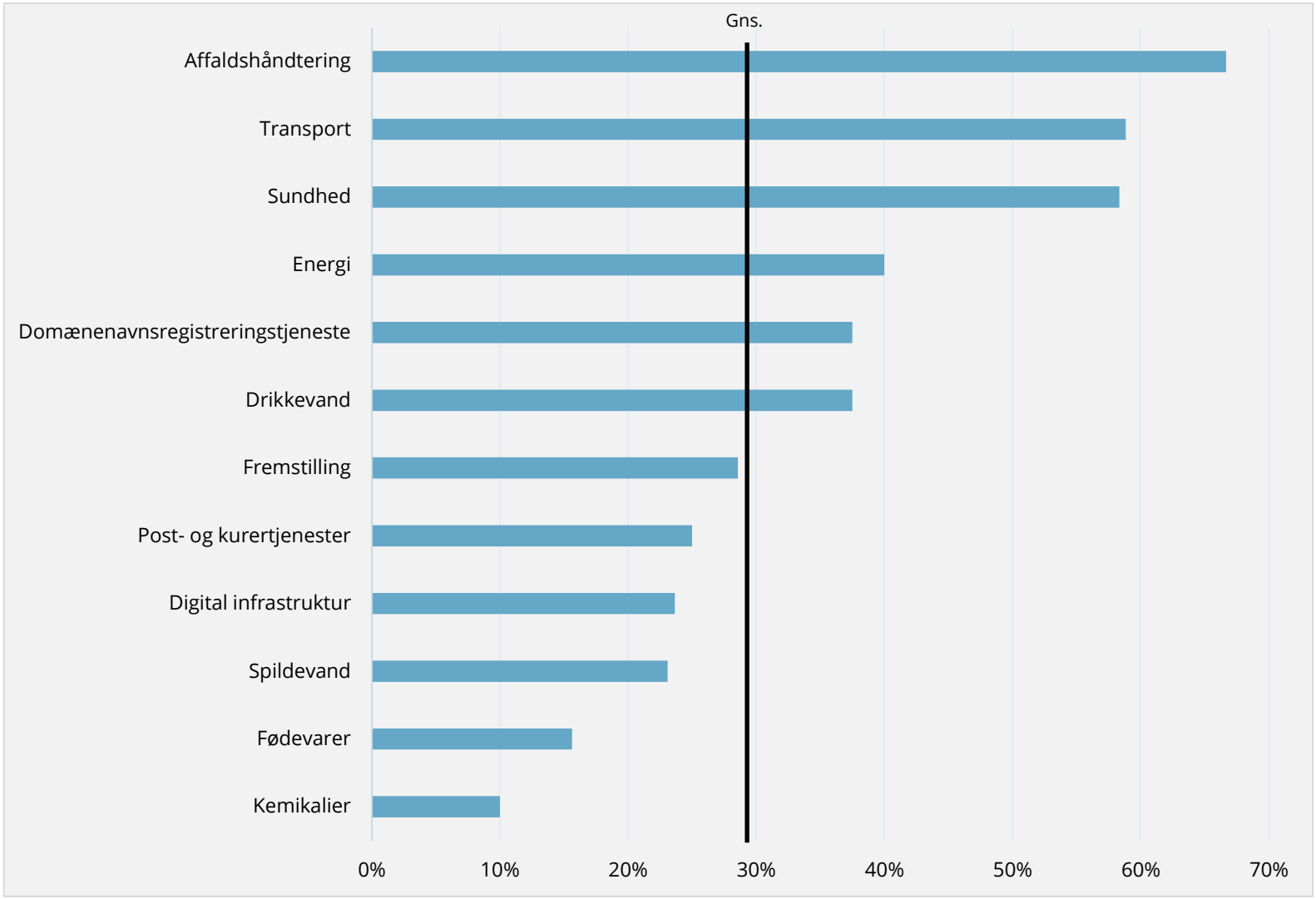
Figur 3.6 viser, at to tredjedele af virksomhederne inden for sektoren "Affaldshåndtering" lever op til direktivets krav, mens det for "Kemikalier" blot gælder en ud af ti virksomheder.

Der er kun inden for tre sektorer mere end 50 pct. af virksomhederne, der lever op til direktivets krav: "Affaldshåndtering", "Transport" og "Sundhed".

Inden for fem sektorer lever under en fjerdedel af virksomhederne op til direktivets krav.



Figur 3.6 Andele af virksomheder der lever op til samtlige krav fordelt på sektorer



Note: N = 249. Sektoren "Digitale udbydere" er ikke inkluderet i figuren, eftersom kun én virksomhed har besvaret spørgsmålene. Sektorerne "Affaldshåndtering" og "Post- og kurertjenester" har begge under 5 besvarelser. Andelen af virksomheder, der lever op til alle kravene, er udregnet på baggrund af et indeks over flere spørgsmål. Se bilag 1 for et overblik over hvilke spørgsmål, der afspejler hvilke indikatorer og bilag 2 for en beskrivelse af udregningsmetoden.

Flere sektorer halter efter ift. kravene om driftskontinuitet og forsyningskædesikkerhed

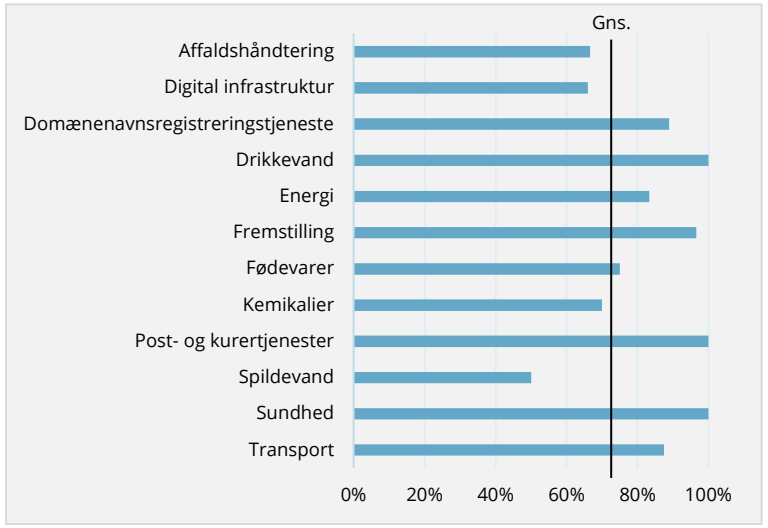
Figurerne til højre og på de næste to sider viser andelen af virksomheder inden for hver sektor, der i minimum nogen grad lever op til de forskellige krav i direktivet. På denne side gennemgås de fire første krav: Politikker for analyse og sikkerhed, håndtering af hændelser, politikker og procedurer for driftskontinuitet og forsyningskædesikkerhed. Sidstnævnte dækker over sikkerhedsrelaterede aspekter mellem virksomheden og dens leverandører eller udbydere.

Som figurerne til højre viser, er andelen af virksomheder, der lever op til kravene, forskellige fra sektor til sektor – men også fra krav til krav. Et eksempel herpå er sektoren "Spildevand", hvoraf ca. 50 pct. lever op til kravet om politikker, mens det for kravet vedrørende håndteringen af hændelser gælder ca. 80 pct.

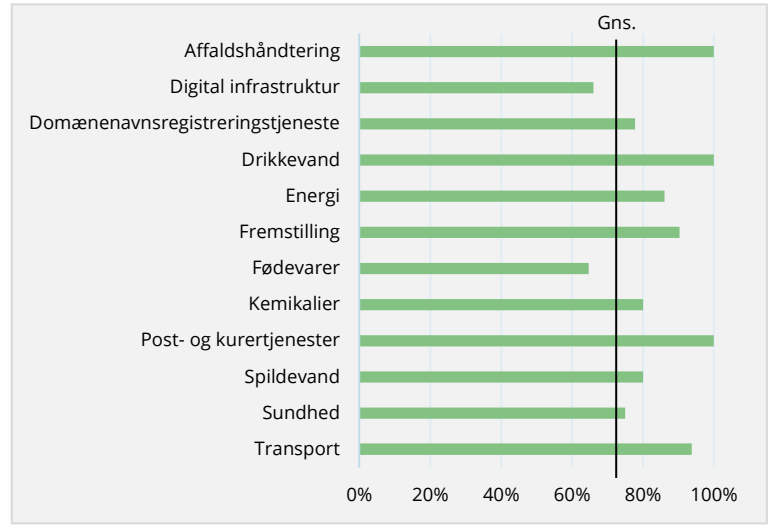
Fælles for de fleste sektorer er, at under tre fjerdedele af virksomhederne lever op til kravene for driftskontinuitet og forsyningskædesikkerhed. Samtidigt lever alle virksomhederne i enkelte sektorer op til kravene om generelle sikkerhedspolitikker og håndtering af hændelser.

Inden for sektorerne "Transport", "Drikkevand", "Energi" og "Sundhed" lever en større andel end gennemsnittet op til de fire krav illustreret til højre. Minimum seks ud af ti virksomheder inden for disse sektorer lever op til kravene.

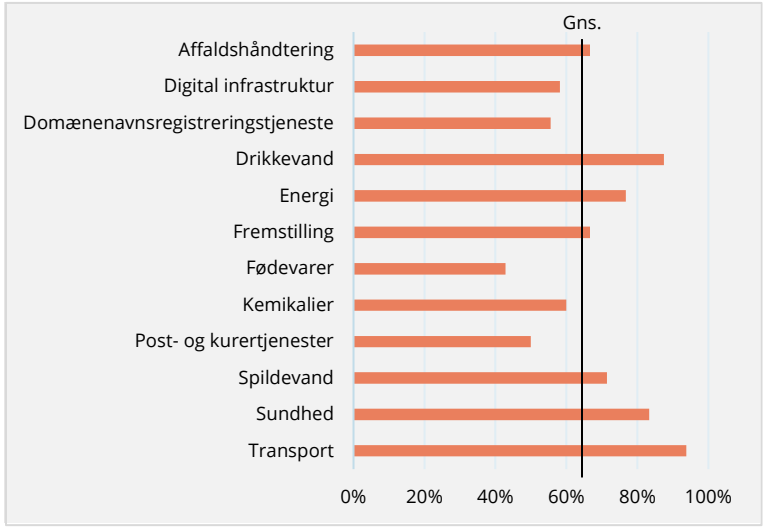
Figur 3.7 Politikker



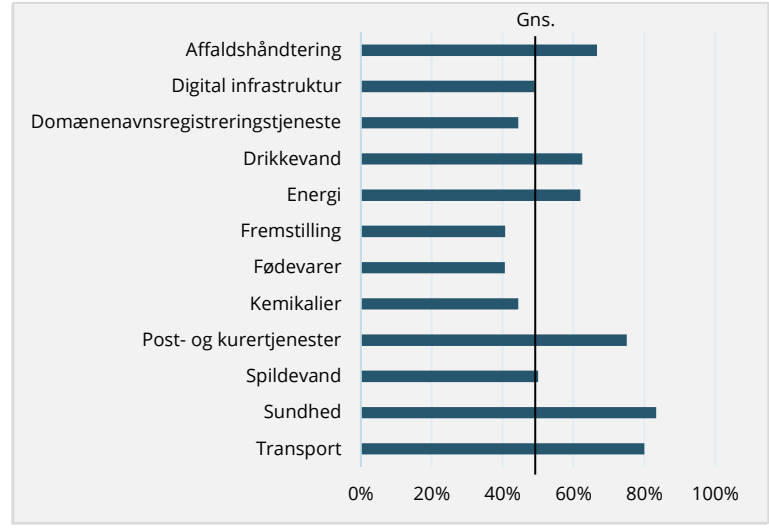
Figur 3.8 Håndtering af hændelser



Figur 3.9 Driftskontinuitet



Figur 3.10 Forsyningskædesikkerhed



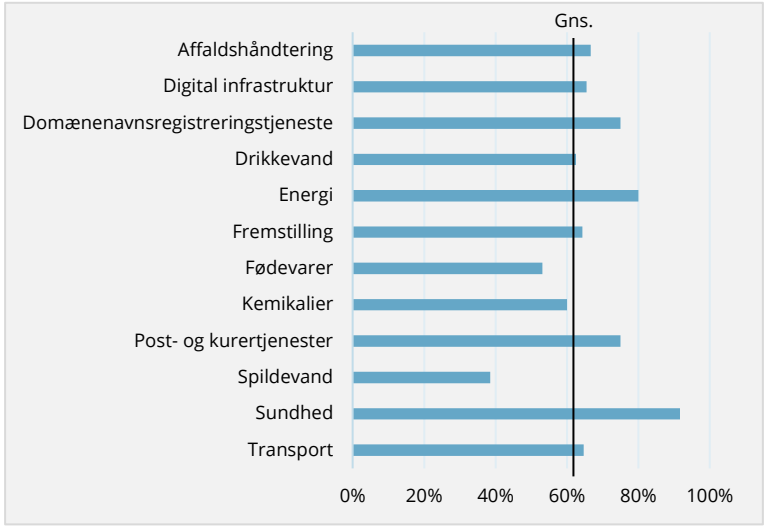
Mange opfylder krav om uddannelse og cyberhygiejne, mens få møder krav om test af effektivitet

På denne side gennemgås yderligere fire af direktivets krav: Håndtering og offentliggørelse af sårbarheder, politikker og procedurer til vurdering af effektiviteten af foranstaltninger, cybersikkerhedsuddannelse og grundlæggende cyberhygiejne samt anvendelsen af kryptografi/kryptering.

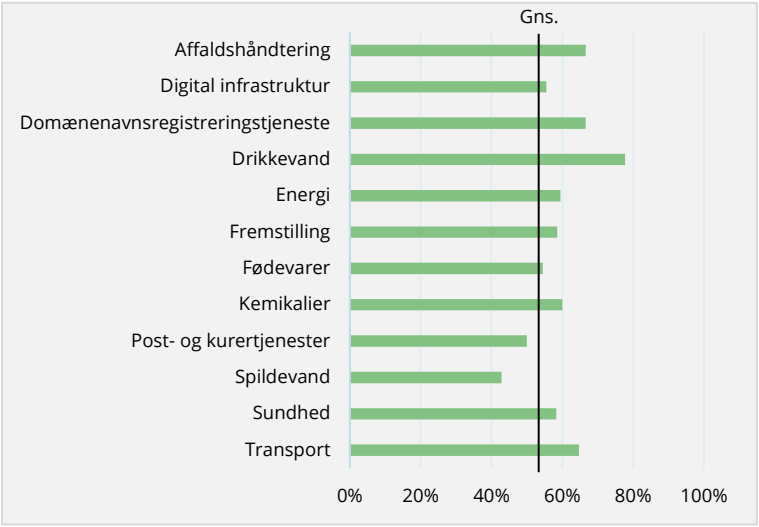
Heriblandt findes der også en stor spredning i andelen af virksomheder, der lever op til kravene, på tværs af sektorer og krav.

I flere sektorer lever alle virksomhederne op til kravene om uddannelse og cyberhygiejne samt brugen af kryptering. Dog er det under to tredjedele af virksomhederne i de fleste sektorer, der lever op til kravet om vurdering af effektiviteten af IT-foranstaltninger.

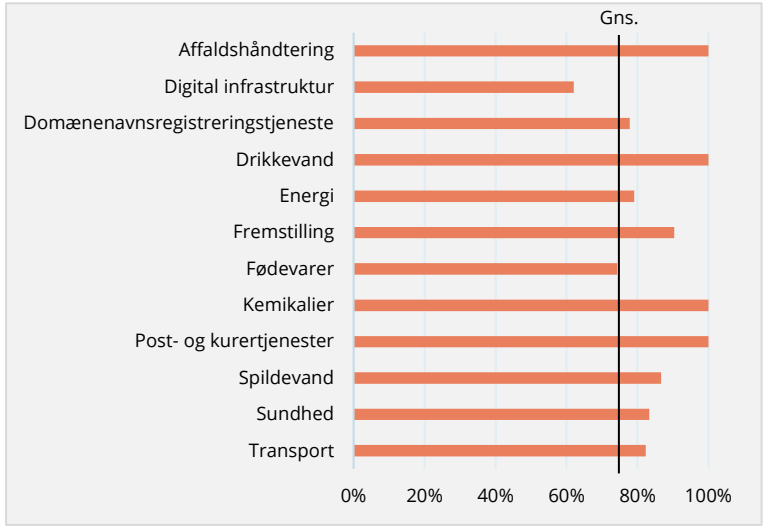
Figur 3.11 Deling af sårbarheder



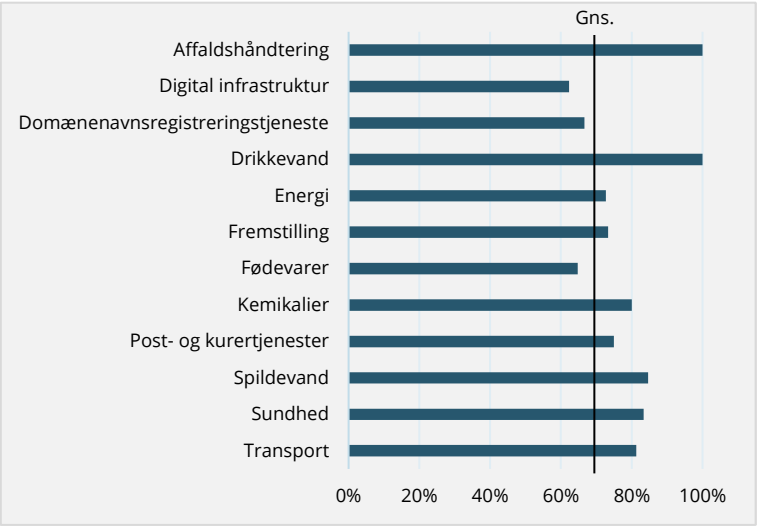
Figur 3.12 Effektivitet



Figur 3.13 Uddannelse og cyberhygiejne



Figur 3.14 Kryptering



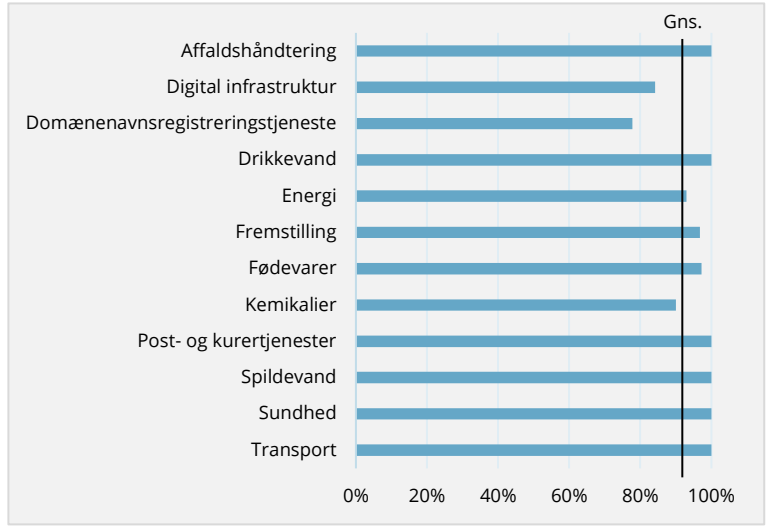
Alle sektorer er godt forberedte til at møde kravene om adgangskontrol og multifaktor-login

På denne side gennemgås de to sidste af direktivets krav: Adgangskontrolpolitikker og brugen af løsninger med multifaktorautentificering.

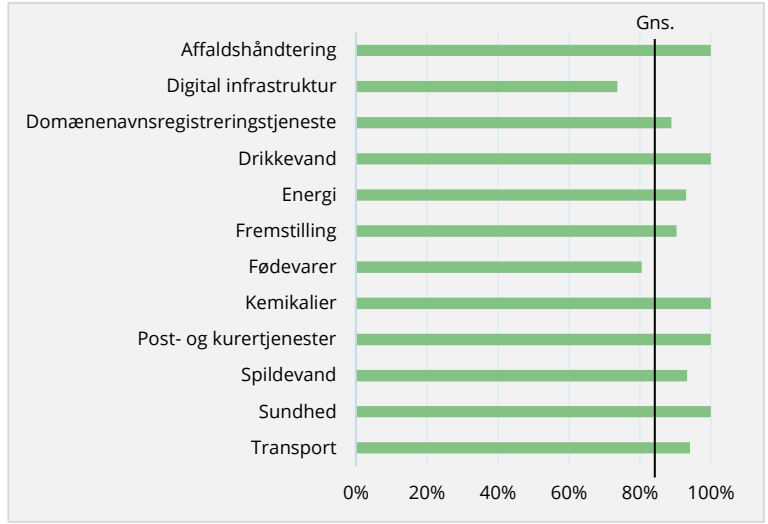
På tværs af sektorerne lever en markant andel af virksomhederne op til de to krav. Ca. ni ud af ti virksomheder lever op til disse krav, hvilket muligvis kan tilskrives udviklingen i brugen af online løsninger. Fx er adgangsbegrænsning i højere grad blevet en del af den generelle IT-politik, mens multifaktorautentificering er blevet mere udbredt i standardløsninger.

Andelen af virksomheder inden for "Digital infrastruktur", der lever op til kravene, ligger under gennemsnittet. Selvom dette er imod forventningerne, kan det delvist forklares af, at en stor del af disse er mindre internetudbydere.

Figur 3.15 Adgangskontrolpolitikker



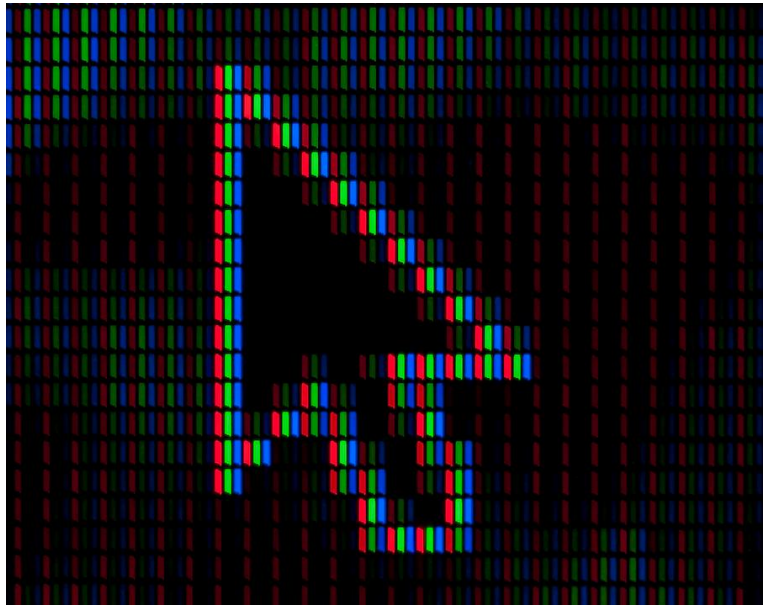
Figur 3.16 Multifaktorautentificering



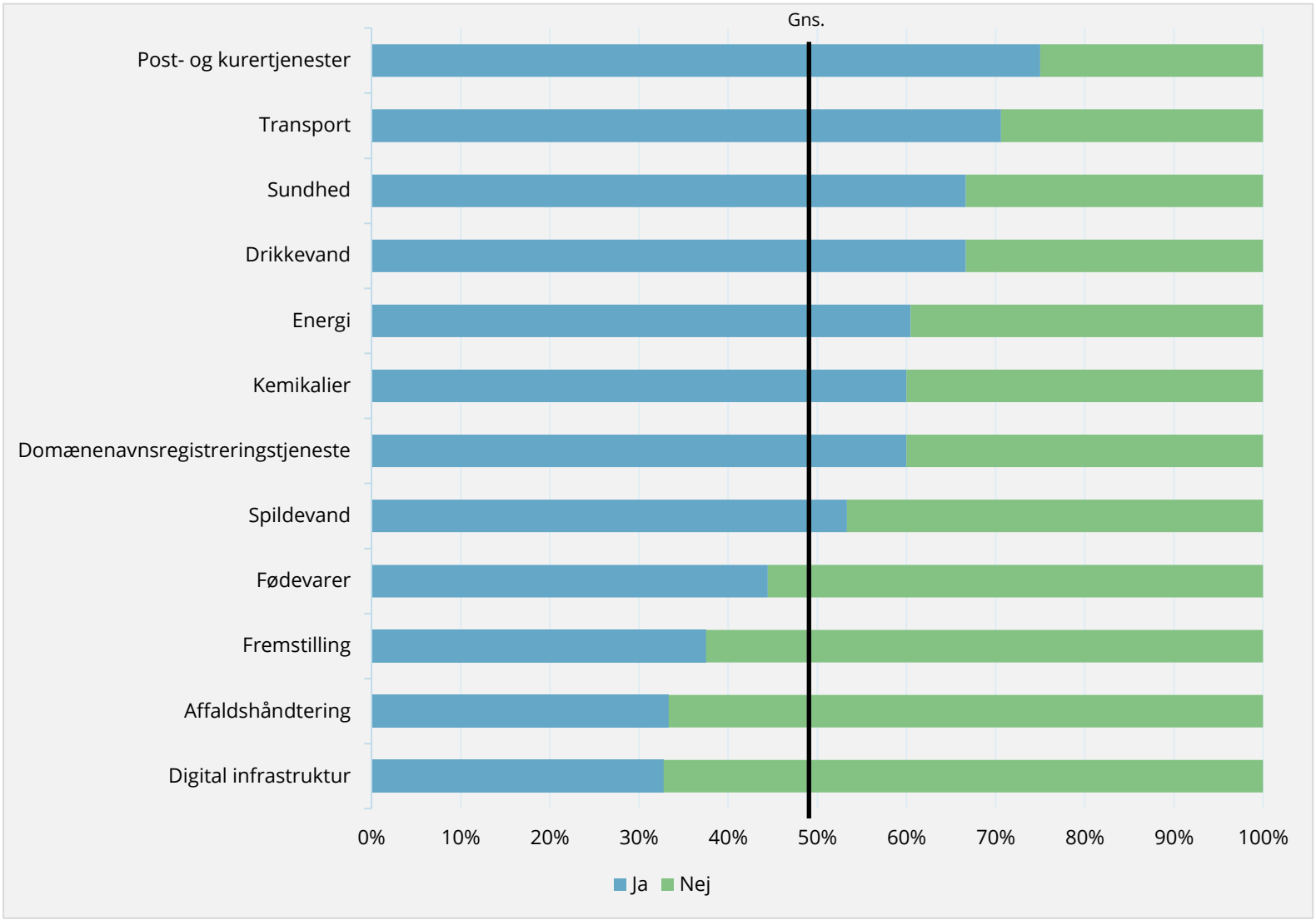
Kendskabet til hjælpeværktøjer er større inden for nogle sektorer end andre

Figuren til højre illustrerer andelen af virksomheder inden for hver sektor, der kender til værktøjer, der kan hjælpe dem med at øge deres IT- og informationssikkerhed.

I gennemsnit kender ca. halvdelen af virksomhederne til hjælpeværktøjer. Inden for sektorerne "Post- og kurertjenester", "Transport", "Sundhed" og "Drikkevand" er det imidlertid to ud af tre virksomheder, der kender til hjælpeværktøjer, mens det inden for sektorerne "Affaldshåndtering" og "Digital infrastruktur" blot gælder en ud af tre virksomheder.



Figur 3.17 Virksomheder fordelt på sektorer samt om de kender til hjælpeværktøjer



Note: N = 249. Sektoren "Digitale udbydere" er ikke inkluderet i figuren, eftersom kun én virksomhed har besvaret spørgsmålet. Sektorerne "Affaldshåndtering" og "Post- og kurertjenester" har begge under 5 besvarelser.

Alle sektorer efterspørger i høj grad styrket information og adgang til best practice cases

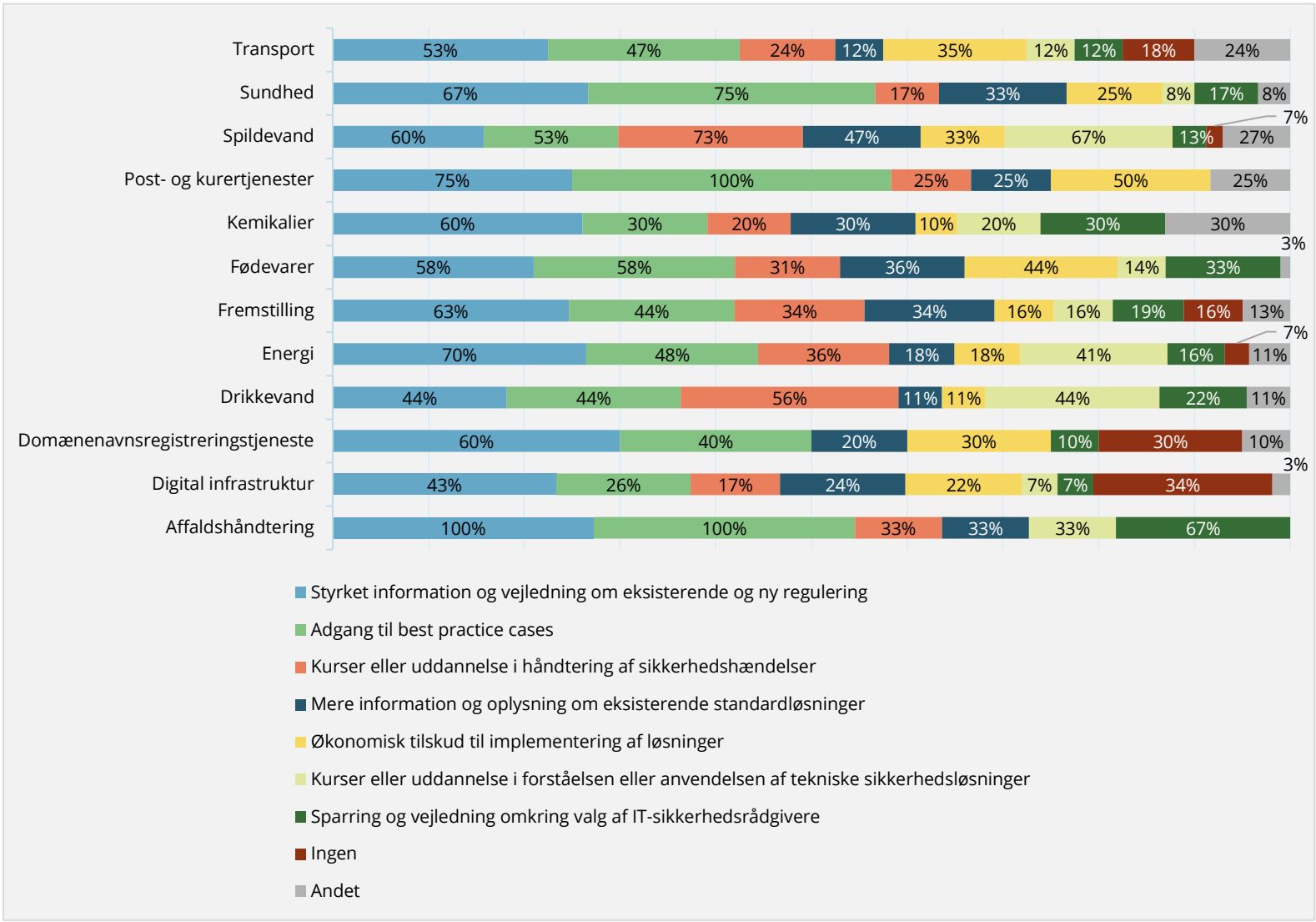
Figuren til højre viser andelen af virksomheder inden for hver sektor, der efterspørger udvalgte tiltag, der kan hjælpe dem med at øge deres IT- og informationssikkerhed.

Inden for de fleste sektorer efterspørger over halvdelen af virksomhederne styrket information og vejledning om eksisterende og ny regulering.

Særligt virksomheder i sektorerne "Sundhed", "Post- og kurertjenester" og "Affaldshåndtering" efterspørger adgang til best practice cases, mens virksomheder i sektorerne "Spildevand", "Drikkevand" og til dels "Energi" efterspørger uddannelse i håndteringen af sikkerhedshændelser samt uddannelse i forståelsen eller anvendelsen af tekniske sikkerhedsløsninger.

Derudover efterspørger virksomheder i sektorerne "Transport", "Post- og kurertjenester", "Fødevarer" og "Domænenavnsregistreringstjenester" i særlig grad økonomisk tilskud til implementering af løsninger, mens en væsentlig andel af virksomheder i de digitale sektorer ikke efterspørger nogen tiltag.

Figur 3.18 Tiltag efterspurgt af virksomhederne fordelt på sektorer



Note: N = 249. Virksomhederne havde mulighed for at vælge mere end én svarmulighed, hvorfor figuren ikke summerer til 100%. Sektoren "Digitale udbydere" er ikke inkluderet i figuren, eftersom kun én virksomhed har besvaret spørgsmålene. Sektorerne "Affaldshåndtering" og "Post- og kurertjenester" har begge under 5 besvarelser.

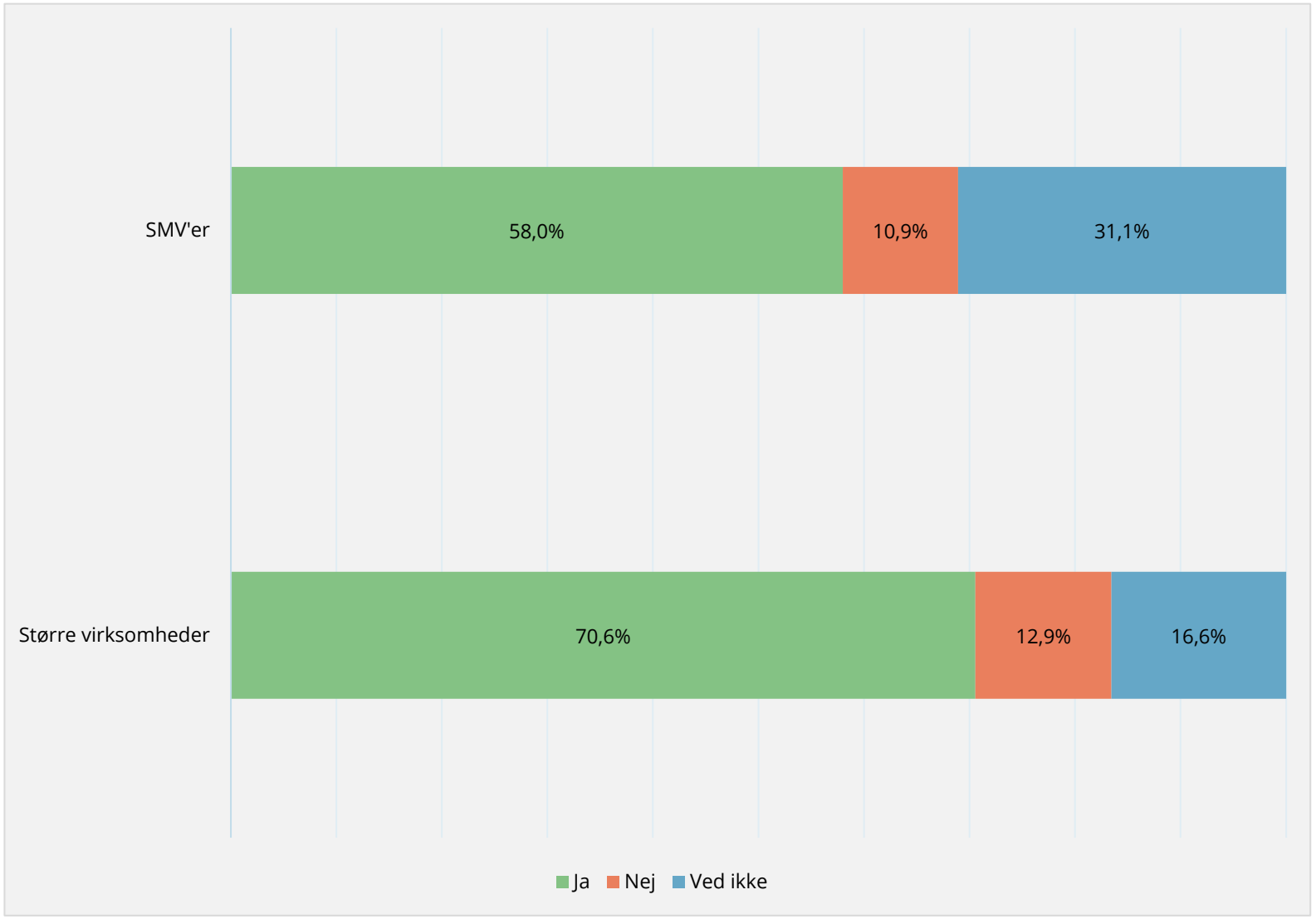
4. Størrelsesspecifikke resultater

Særligt SMV'er er i tvivl om, hvorvidt de bliver omfattet af NIS2

Figurerne viser andelen af virksomheder, der vurderer, at de vil blive omfattet af NIS2, fordelt på størrelse. Der skelnes her mellem SMV'er og større virksomheder ud fra direktivets definition herpå i artikel 2.

Figur 4.1 viser, at syv ud af ti større virksomheder vurderer, at de vil blive berørt af NIS2, mens det gælder for knap seks ud af ti SMV'er. Dog er 16,6 pct. af de større virksomheder og 31,1 pct. af SMV'erne fortsat i tvivl om, hvorvidt de er omfattet af direktivet.

Figur 4.1 Virksomheder der vurderer sig omfattet af NIS2 fordelt på størrelse



Note: N = 282. Kategorien "Ja" dækker over de virksomheder, der har sagt at de enten direkte eller indirekte vil blive omfattet af NIS2.

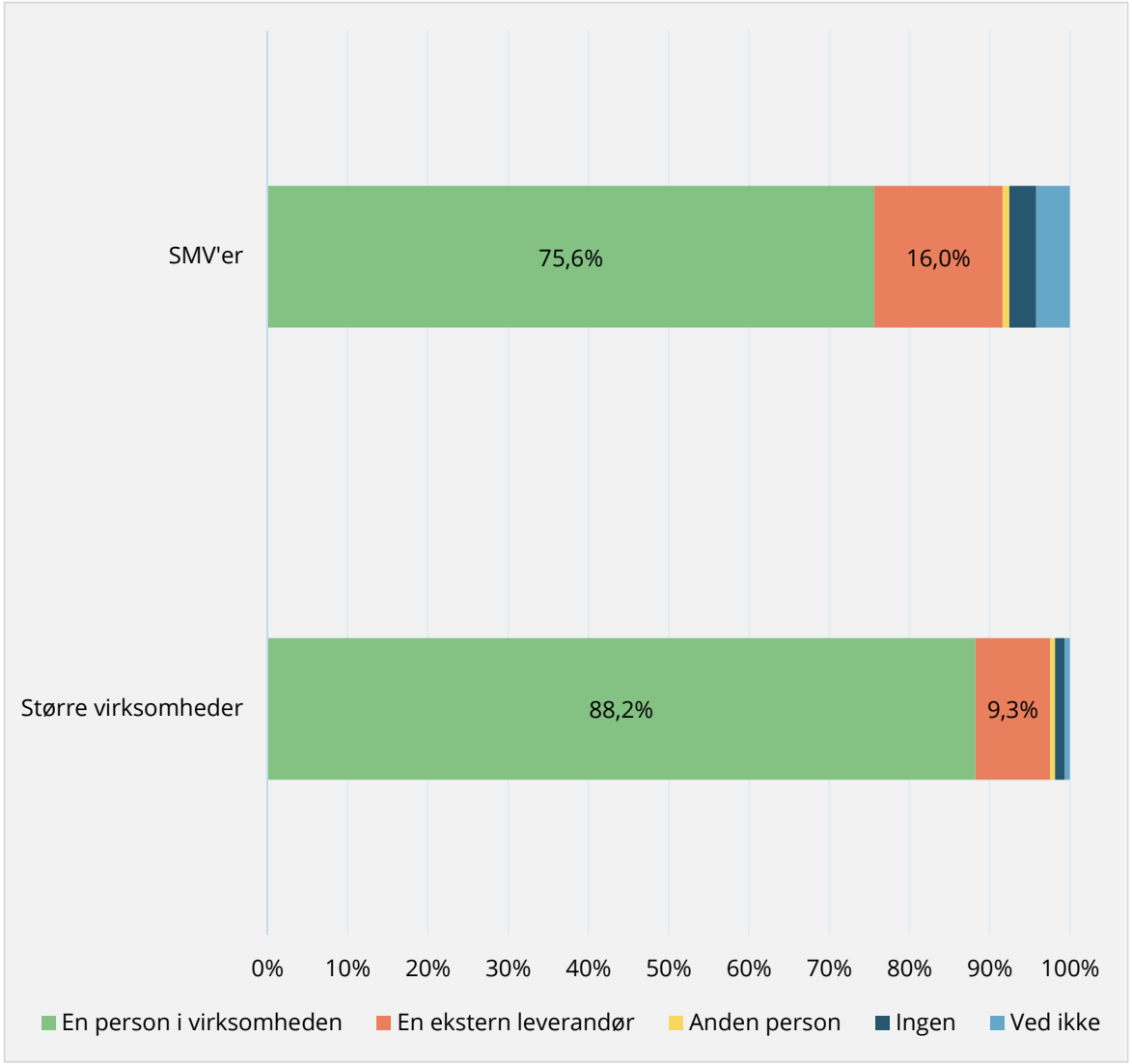
SMV'er placerer i højere grad IT-ansvaret hos en ekstern leverandør

Figuren til højre illustrerer hvor ansvaret for virksomhedernes IT-ansvar er placeret alt efter deres størrelse.

Figuren viser, at tre fjerdedele af SMV'erne angiver, at en person internt i virksomheden har ansvaret for IT- og informationssikkerheden. Blandt de større virksomheder er andelen ikke overraskende lidt højere.

En væsentlig større andel af SMV'er (16 pct.) angiver, at en ekstern person har IT-ansvaret for virksomheden, sammenlignet med større virksomheder (9,3 pct.).

Figur 4.2 Personer med ansvar for virksomhedernes IT- sikkerhed fordelt på størrelse



Note: N = 280.

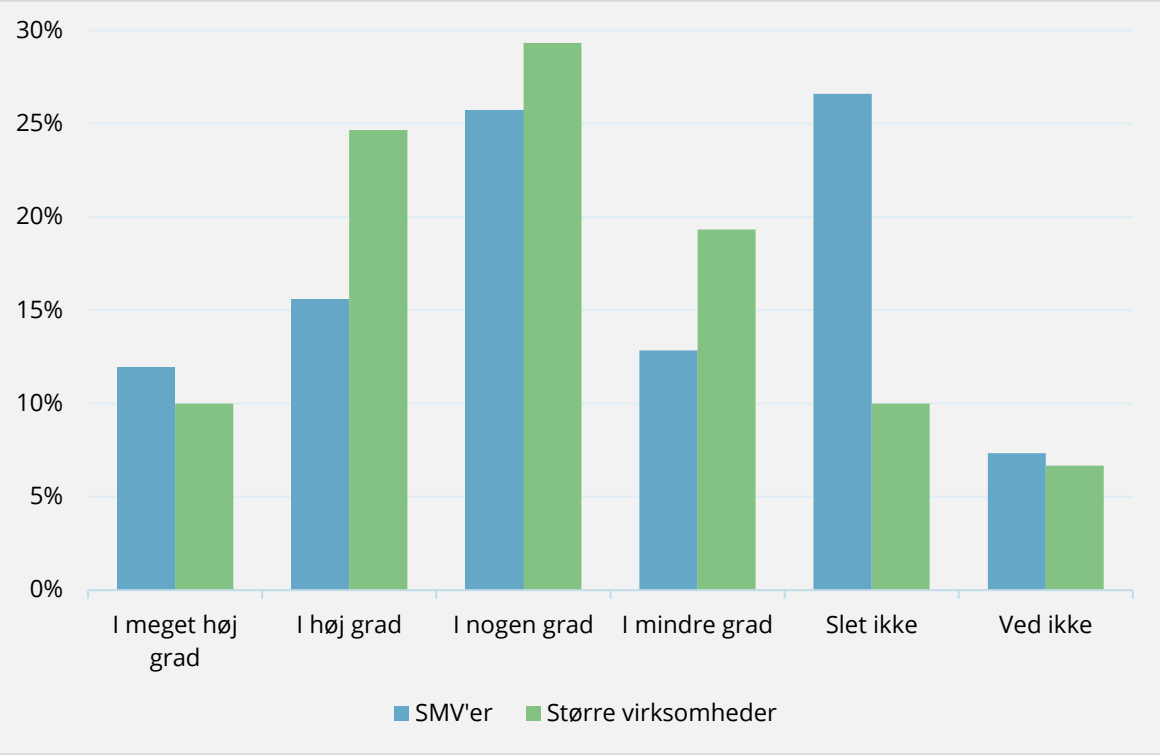
SMV'er har i markant lavere grad sat sig ind i direktivets indhold og har i lavere grad en plan

Figurerne neden for viser andelen af virksomheder inden for hver størrelseskategori, der har sat sig ind i NIS2-direktivet og dets betydning for virksomhederne samt i hvilken grad de har en plan for at leve op til direktivet.

Figur 4.3 viser, at en væsentlig større andel SMV'er (27 pct.) slet ikke har sat sig ind i direktivets indhold sammenlignet med større virksomheder (10 pct.). Cirka halvdelen af SMV'erne har i minimum nogen grad sat sig ind i direktivet, mens det for større virksomheder gælder knap to tredjedele.

Figur 4.4 viser, at næsten samme andel SMV'er og større virksomheder i minimum nogen grad har en plan for at leve op til direktivets krav. Dog har en større andel af SMV'erne (30 pct.) end de større virksomheder (23 pct.) slet ikke en plan herfor.

Figur 4.3 Virksomhederne fordelt på størrelse efter om de har sat sig ind i direktivet



Note: N = 259.

Figur 4.4 Virksomhederne fordelt på størrelse efter om de har en plan

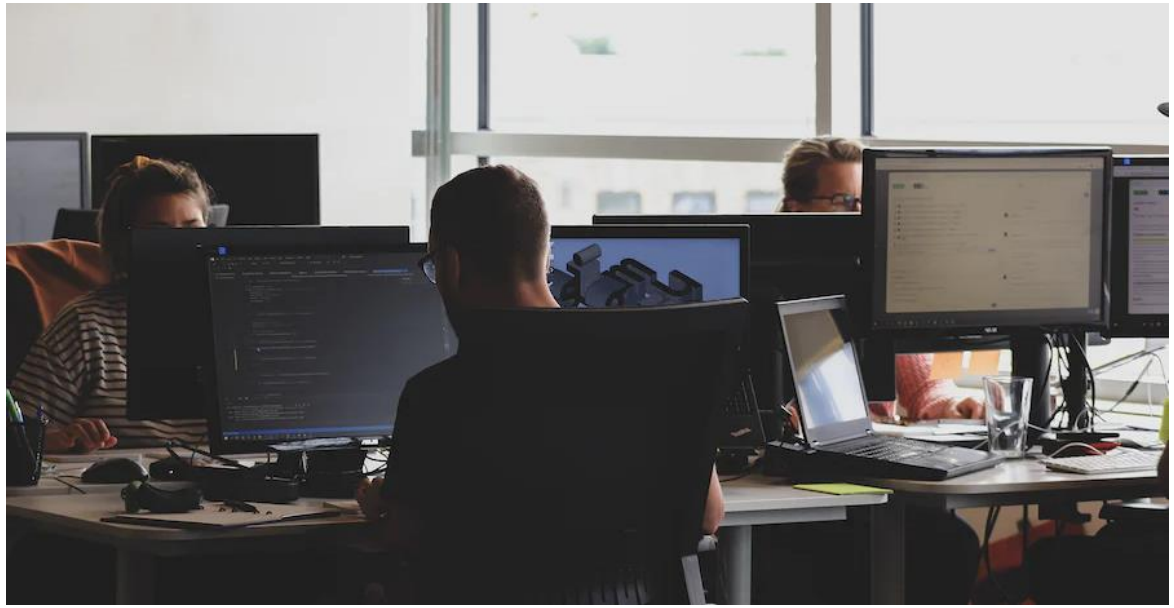
Note: N = 257.

Større virksomheder planlægger at anvende interne ressourcer, SMV'er vil anvende eksterne

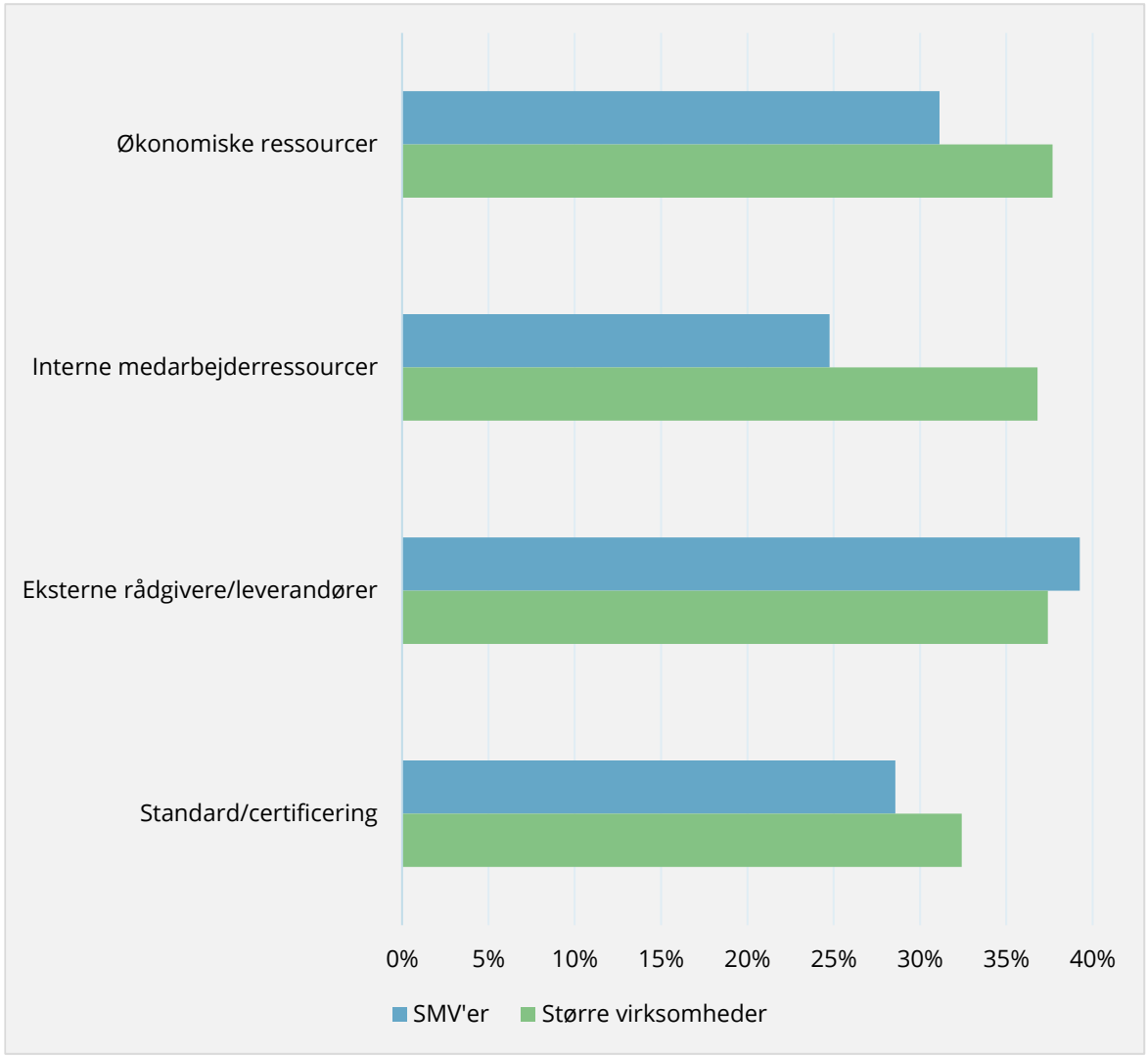
Figuren til højre viser i hvilken grad de virksomheder, der har en plan for at leve op til direktivets krav, i høj eller meget høj grad planlægger at anvende forskellige ressourcer hertil, fordelt på størrelse. De virksomheder, der i mindre grad eller slet ikke har en plan, er ikke inkluderet.

Figuren viser, at SMV'er i marginalt højere grad end de større virksomheder planlægger at benytte eksterne rådgivere eller leverandører for at leve op til direktivets krav.

Større virksomheder planlægger i væsentligt højere grad end SMV'er at anvende interne medarbejderresourcer og økonomiske ressourcer.



Figur 4.5 Indholdet af virksomhedernes plan for at leve op til direktivet fordelt på størrelse



Note: N = 249.

Større virksomheder er bedre rustet til at møde direktivets krav end SMV'erne

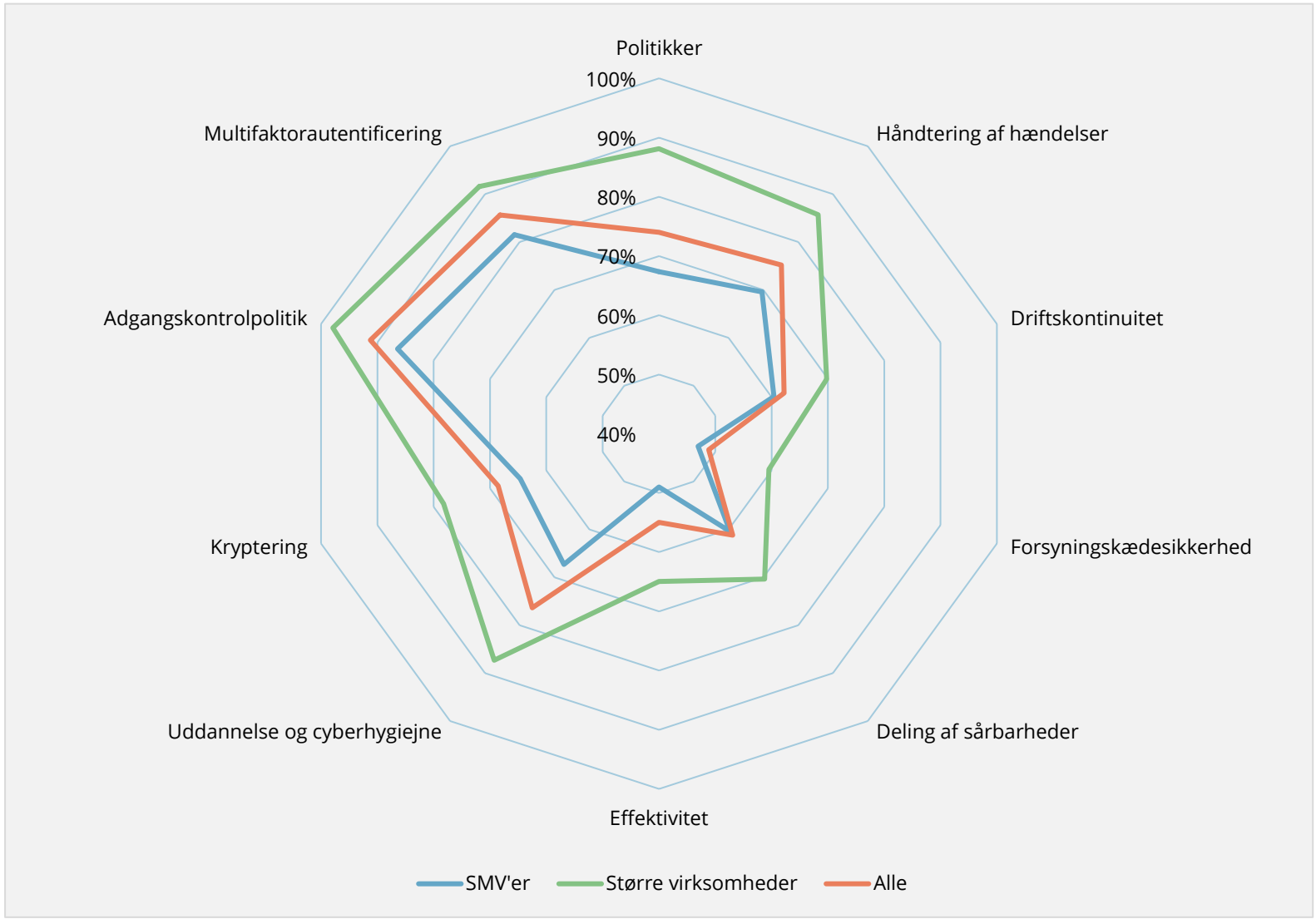
Figuren til højre illustrerer andelen af virksomheder, der lever op til hvert af direktivets 10 krav til IT- og informationssikkerhed fordelt på størrelse.

Figuren viser, at en større andel af de større virksomheder lever op til samtlige krav i direktivet sammenlignet med SMV'erne og gennemsnittet. Som tidligere nævnt lever 29,2 pct. af virksomhederne i minimum nogen grad op til samtlige af direktivets krav. For større virksomheder udgør andelen imidlertid 36,3 pct. og for SMV'er 25 pct.

Særligt i forhold til kravet om politikker, der foruden at omhandle generelle IT-sikkerhedspolitikker også inkluderer politikker og procedurer for risikoanalyse, er forskellen mellem virksomheder af forskellig størrelse stor. Ca. 14 procentpoint flere større virksomheder lever op til dette krav sammenlignet med gennemsnittet.

Andelen af SMV'er, der lever op til direktivets krav, ligger kun marginalt under gennemsnittet på flere af kravene.

Figur 4.6 Andel af virksomheder der lever op til direktivets 10 krav fordelt på størrelse



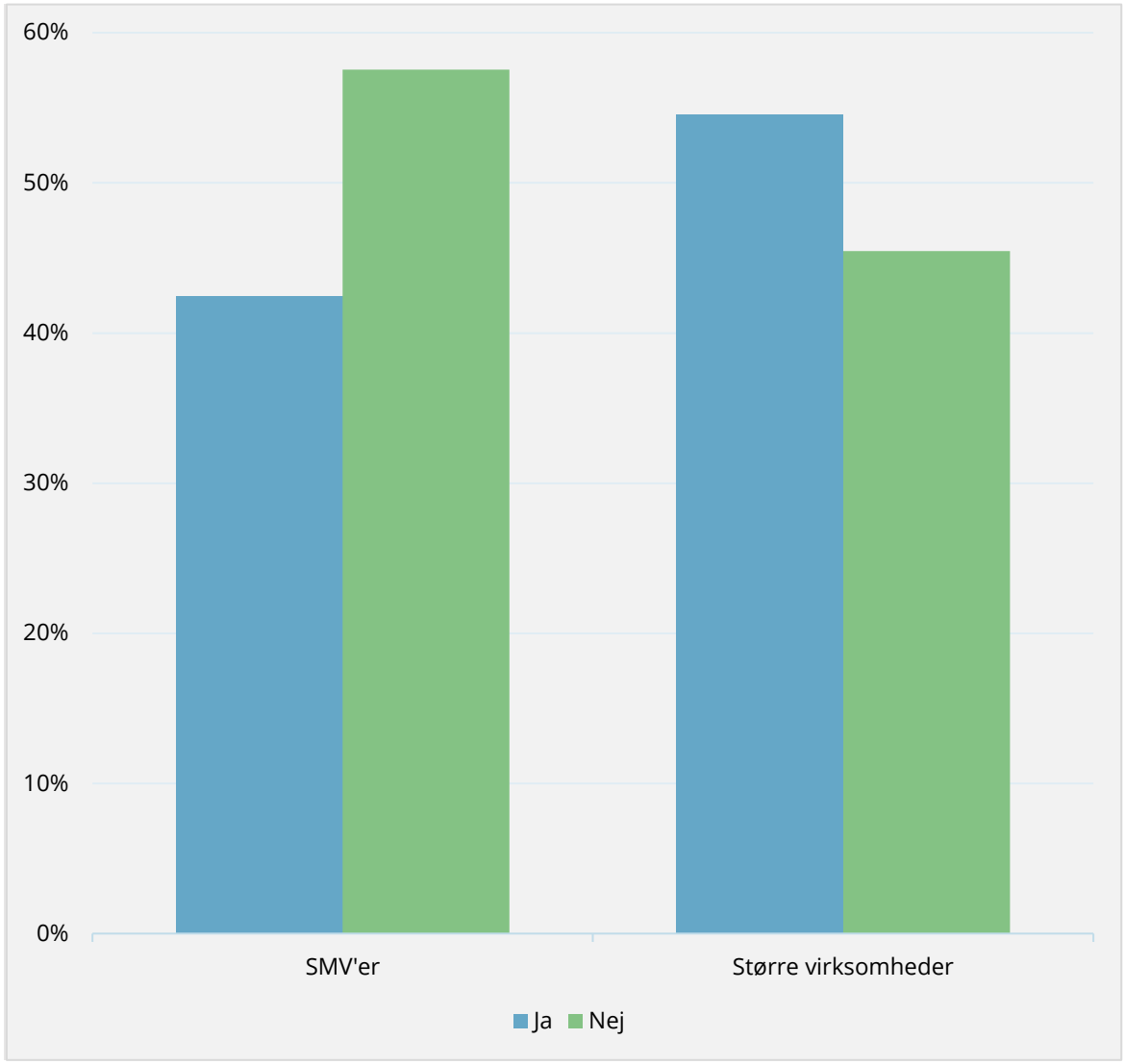
Note: N = 249. Virksomhederne skal som minimum have svaret "i nogen grad" på spørgsmålene for at blive kategoriseret som at leve op til kravene. Nogle indikatorer er udregnet som indeks over flere spørgsmål. Se bilag 1 for et overblik over hvilke spørgsmål, der afspejler hvilke indikatorer og bilag 2 for en beskrivelse af udregningsmetoden.

SMV'er kender i lavere grad til hjælpeværktøjer end større virksomheder

Figuren til højre illustrerer andelen af virksomheder fordelt på størrelse, der kender til værktøjer, der kan hjælpe dem med at øge deres IT- og informationssikkerhed.

Figuren viser, at flere større virksomheder (54,5 pct.) kender til hjælpeværktøjer sammenlignet med SMV'er (42,5 pct.). Dette kan muligvis forklare, hvorfor SMV'er i højere grad planlægger at benytte eksterne rådgivere eller leverandører til at øge deres IT- og informationssikkerhed, mens større virksomheder planlægger at anvende interne ressourcer.

Figur 4.7 Virksomheder fordelt på størrelse samt om de kender til hjælpeværktøjer



Note: N = 249.

Styrket information, best practice cases og kurser efterspørges af både store og små virksomheder

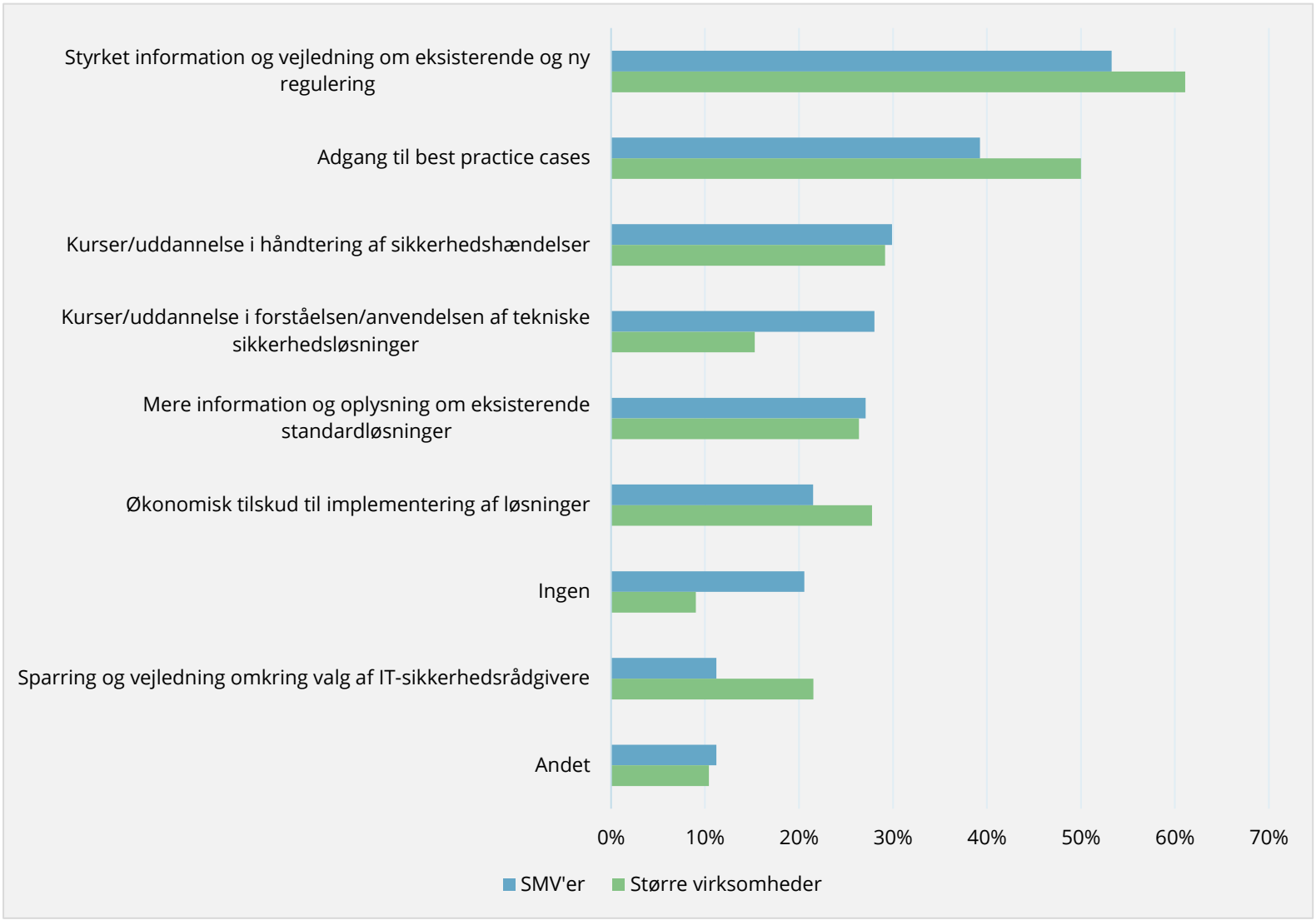
Figuren til højre viser andelen af virksomheder inden for hver sektor, der efterspørger udvalgte tiltag, der kan hjælpe dem med at øge deres IT- og informations-sikkerhed.

Figuren viser, at både store og små virksomheder i høj grad efterspørger styrket information og vejledning om eksisterende og ny regulering. Mere end halvdelen af virksomhederne har et ønske herom.

Derudover viser figuren, at større virksomheder i højere grad end SMV'er efterspørger styrket information og vejledning om eksisterende og ny regulering, adgang til best practice cases, økonomisk tilskud til implementering af løsninger samt sparring og vejledning omkring valg af IT-sikkerhedsrådgivere.

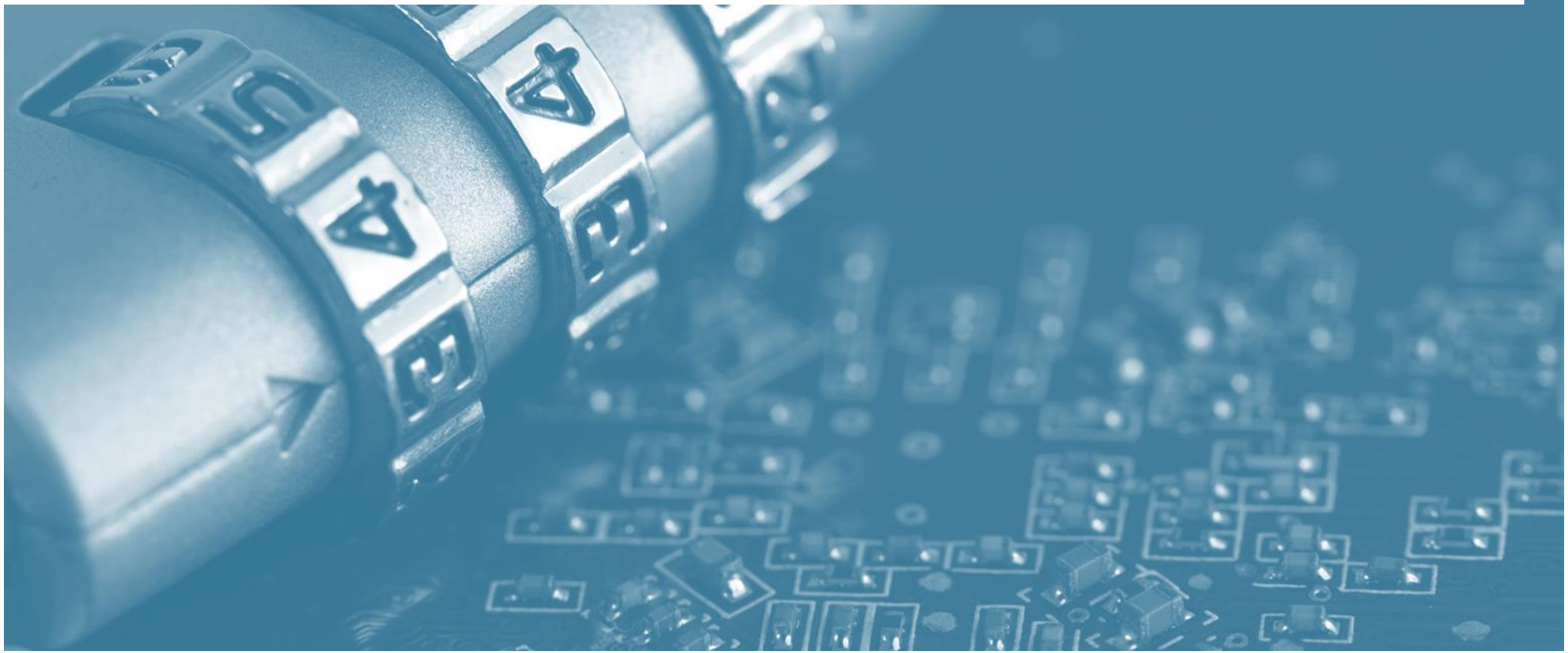
SMV'er efterspørger derimod i højere grad kurser eller uddannelse i håndteringen af sikkerhedshændelser og anvendelsen af tekniske sikkerhedsløsninger samt mere information og oplysning om eksisterende standardløsninger.

Figur 4.8 Tiltag efterspurgt af virksomhederne fordelt på størrelse



Note: N = 249. Virksomhederne havde mulighed for at vælge mere end én svarmulighed, hvorfor figuren ikke summerer til 100%.

Bilag



Bilag 1 – Oversigt over NIS2-direktivets krav og spørgeskemaets spørgsmål

Krav jf. direktivets artikel 21, stk. 2	Spørgsmål i spørgeskemaet
a) politikker for risikoanalyse og informationssystemsikkerhed	I hvilken grad har din virksomhed... - En overordnet politik for virksomhedens IT- og informationssikkerhed, der er tilgængelig for medarbejderne? I hvilken grad har din virksomhed... - Klart definerede roller og sikkerhedsansvar? I hvilken grad har din virksomhed procedurer for... - At analysere meddelelser fra overvågningssystemer? I hvilken grad har din virksomhed procedurer for... - At analysere opdagede sikkerhedshændelser?
b) håndtering af hændelser	I hvilken grad har din virksomhed... - Procedurer for håndtering af sikkerhedshændelser?
c) driftskontinuitet, såsom backup-styring og reetablering efter en katastrofe, og krisestyring	I hvilken grad har din virksomhed... - Procedurer for opretholdelse af forretningens drift under en sikkerhedshændelse? I hvilken grad gennemfører din virksomhed regelmæssigt og systematisk... - Test og revision af planer for opretholdelse af forretningens drift under en sikkerhedshændelse?
d) forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere	I hvilken grad har din virksomhed... - En politik i forhold til krav til leverandører, kunder og samarbejdspartneres sikkerhedsforpligtelser? I hvilken grad gennemfører din virksomhed regelmæssigt og systematisk... - Opfølgning på at leverandører, kunder og samarbejdspartnere lever op til deres sikkerhedsforpligtelser?
e) sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder	I hvilken grad har din virksomhed procedurer for... - At meddele leverandører, kunder og samarbejdspartnere om en eventuel sikkerhedshændelse? I hvilken grad har din virksomhed procedurer for... - At indberette sikkerhedshændelser?
f) politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici	I hvilken grad gennemfører din virksomhed regelmæssigt og systematisk... - Test og revision af IT-sikkerhedsforanstaltningers effektivitet? I hvilken grad har eller anvender din virksomhed... - Effektive processer til at overvåge og opdage potentielle sikkerhedshændelser internt? I hvilken grad har eller anvender din virksomhed... - Effektive processer til at overvåge og opdage potentielle sikkerhedshændelser blandt leverandører, kunder og samarbejdspartnere? I hvilken grad har eller anvender din virksomhed... - Regelmæssige sårbarhedstests af relevante systemer, applikationer og hjemmesider?
g) grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse	I hvilken grad har din virksomhed... - En politik i forhold til at ledere og/eller medarbejdere skal følge IT- og informationssikkerhedskurser? I hvilken grad har din virksomhed... - Fokus på at sikre gode cyberhygiejnepraksisser?
h) politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering	I hvilken grad har eller anvender din virksomhed... - Kryptografi og/eller kryptering?
i) personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver	I hvilken grad har eller anvender din virksomhed... - Adgangskontrol- og forvaltningspolitikker?
j) brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt i enheden, hvor det er relevant.	I hvilken grad har eller anvender din virksomhed... - Løsninger med multifaktorautentificering?

Bilag 2 – Metodebeskrivelse

Kortlægningen af berørte virksomheder

Kortlægningen består af virksomheder, der vurderes bliver berørt af NIS2-direktivet. Kortlægningen er opdelt på sektorer og delsektorer i henhold til NIS2-direktivets bilag 1 og 2. Der er et minimumskrav for størrelsen på virksomheder i kortlægningen. De skal have mindst 50 ansatte *og* en balance i 2021 på mindst 74 mio. kr. *og* en omsætning i 2021 *eller* bruttofortjeneste i 2021*.

De følgende sektorer er ikke en del af kortlægningen:

1. Bankvirksomheder
2. Finansielle markedsinfrastrukturer
3. DNS-tjenesteudbydere (under sektoren for digital infrastruktur)
4. Forvaltere af IKT-tjenester
5. Forskningsorganisationer
6. Offentlige forvaltningsenheder

1 og 2 er ikke taget med, idet EU's DORA-direktiv vil stille endnu højere krav end NIS2 til disse virksomheder inden for ca. samme tidshorisont. 3 er ikke taget med, idet DK Hostmaster A/S har meldt tilbage, at det ikke er muligt at kortlægge disse ud fra eksisterende registre. 4 og 5 er ikke taget med, eftersom disse først ultimo 2022 blev inkluderet som berørte sektorer af EU Kommissionen. Derudover vil dele af nr. 4 også blive omfattet af DORA-direktivet. 6 ikke taget med, eftersom det endnu er uklart i hvilket omfang, at offentlige forvaltningsenheder omfattes af direktivet.

Pba. feedback fra en række myndigheder har vi ladet domænenavnsregistreringstjenester fremgå som en sektor for sig selv, da disse behandles særskilt i direktivet.

Kortlægningen har primært taget udgangspunkt i branchekoder, der vurderes at afspejle sektorerne. Disse branchekoder er derefter blevet kvalitetssikret i sparring med relevante danske myndigheder og brancheorganisationer, der beskæftiger sig med de forskellige relevante sektorer. Derudover er der tilføjet manuelle justeringer på baggrund af input fra disse.

** Svarende til ca. 10 mio. euro. Se NIS2-direktivets artikel 2 om direktivets anvendelsesområde. For ikke at være en mikrovirksomhed/lille enhed, skal en virksomhed have en balance og en omsætning på over 10 mio. euro. Grundet manglende dækning af omsætning i CVR-registret, har vi valgt at bruge bruttofortjenesten som erstatning i nogle tilfælde.*

Udregninger i analysen

Fordi nogle af kravene i direktivet er brede, har vi i flere tilfælde stillet flere spørgsmål til samme krav for at være i stand til at vurdere, om en virksomhed lever op til det pågældende krav. Derfor har vi valgt at udregne hvorvidt en virksomhed lever op til hvert krav som et indeks af svarene på de spørgsmål, der afspejler kravet.

Svarene på spørgsmålene har fået følgende vægt:

Svarmulighed	Point
I meget høj grad	5
I høj grad	4
I nogen grad	3
I mindre grad	2
Slet ikke	1
Ved ikke/ej relevant	0

Svarene på de relevante spørgsmål er herefter summeret med ovenstående vægt og divideret med antallet af spørgsmål. Hvis denne værdi, der afspejler det gennemsnitlige svar til det pågældende krav, minimum har værdien 3 svarende til "i nogen grad", er virksomheden vurderet til at leve op til kravet.

Værdien 3 er valgt fordi det ikke er specificeret i direktivet hvornår en virksomhed kan siges at leve op til de opstillede krav. Vi har derfor valgt, at virksomhederne antages at leve op til kravene, hvis de i minimum nogen grad angiver at anvende de opstillede teknologiske foranstaltninger eller i nogen grad har politikker og procedurer på de påkrævede områder.

I opsummeringerne af hvor stor en andel af virksomhederne, der lever op til samtlige af direktivets krav – hvad enten det er på overordnet niveau, sektorniveau eller størrelsesniveau – er udregningen baseret på, at de skal opfylde hvert af de 10 opstillede krav i minimum nogen grad. Jf. ovenfor.

IRIS GROUP
CHRISTIANS BRYGGE 28, 1. SAL | DK-1559 KØBENHAVN V
IRISGROUP@IRISGROUP.DK | WWW.IRISGROUP.DK