NORD-EUROPAS STØRSTE CIO-RAPPORT

CIO ANALYTICS

11 %
har opplevd alvorlige cyberangrep de siste 12 månedene

Kun
24 %
har øvd på beredskapsplanen sin

NORGE
2025

9 av 10
tar ansvar for bærekraft

DYBDEINTERVJUER

10
Nordic Semiconductor:
– Vi skal ikke være en bremsekloss, men en partner

28
Vestland fylkeskommune:
Når trusselbildet endres – slik ruster Vestlandet seg

34
NAVTOR:
Navigasjon møter intelligens

Har du spørsmål?
Kontakt oss på e-post:
contact@cioanalytics.com

Innhold

Side #

Om rapporten
CIO Analytics er en av Nord-Europas største IT-undersøkelser. Totalt har 1273 IT-beslutningstakere sagt sine meninger om trender, kunstig intelligens, sikkerhet, kompetansebehov, IT-avdelingens rolle i digitaliseringen, og mye mer.

Respondentene er CIOs og IT-beslutningstakere i Norge, Sverige, Danmark, Finland, Estland, Latvia og Litauen (omtalt som Nord-Europa i rapporten). Svarfordelingen totalt er 59 prosent innen privat sektor og 41 prosent innen offentlig sektor.

Rapporten er utgitt av IT-selskapet Atea, en ledende leverandør av IT-infrastruktur i Norden og Baltikum.

Vil du vite mer?
Les mer om rapporten ved å skanne QR-koden:

NORD-EUROPEISKE IT-BESLUTNINGSTAKERE I 2025:

Hvordan lede i en uforutsigbar verden?

Den teknologiske utviklingen går raskere enn noen gang. Samtidig preges verden av uro og polarisering. Det er krig i Europa, økende geopolitiske spenninger, klimakrise og økonomisk usikkerhet. Hvordan tilpasser vi oss, og hvordan planlegger vi for det ukjente?

For å forstå hvordan virksomheter bør navigere i dette landskapet, har vi gjennomført den største undersøkelsen i Nord-Europa blant IT-beslutningstakere. Nesten 1300 respondenter har delt sine perspektiver om utfordringene og mulighetene som ligger foran oss. Resultatet er en rapport som gir deg verdifull innsikt i hvordan virksomheter, i både offentlig og privat sektor, tilpasser seg og planlegger for fremtiden.

IT-beslutningstakere i Nord-Europa understreker viktigheten av å ha et helhetsperspektiv. I en tid hvor nyheter raskt blir utdatert, og der det er vanskeligere enn noen gang å skille mellom sannhet og meninger. I en usikker verden er det viktig å planlegge for ulike scenarier.

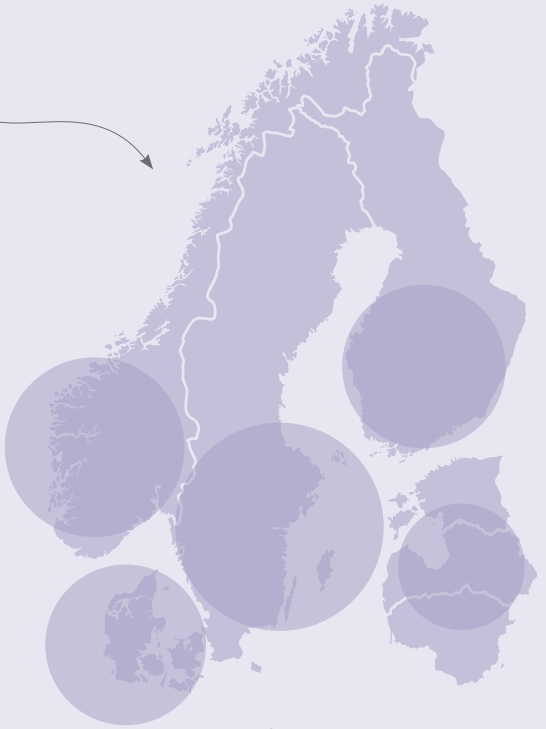
Det er tydeligere enn noen gang at eneste veien fremover er samarbeid. Nye og bedre måter å samarbeide på, både internt og mellom organisasjoner, blir avgjørende. Like viktig blir det å lære av dem som leder an, og av feilene som gjøres. Å ta del i andres erfaringer og la seg inspirere på tvers av landegrenser, vil være nøkkelen for både privat og offentlig sektor.

Vi håper denne rapporten hjelper deg med å forme din strategi, og at både analysene og intervjuene i hvert kapittel gir deg nye perspektiver og gjør deg tryggere på dine neste steg.

- Hva er IT-beslutningstakere i Nord-Europa opptatte av?
- Hvordan prioriterer de sikkerhet, kompetanse og investeringer i kunstig intelligens (AI)?
- Hvordan balanserer de innovasjon, bærekraft og geopolitiske utfordringer?

Dette er en rapport for deg som tar beslutninger, og som trenger innsikt du kan stole på.

Svarfordeling per land av totalt 1273 IT-beslutningstakere i Norge, Sverige, Danmark, Finland, Estland, Latvia og Litauen



1

I HODET TIL EN IT-BESLUTNINGSTAKER

Sikkerhet – et viktig tema i en kompleks verden

ILLUSTRASJON: ISTOCKPHOTO

IT-beslutningstakere i Nord-Europa stiller høye krav til seg selv og evnen til å håndtere en kompleks verden. En stor andel av respondentene i årets rapport mener at et helhetsperspektiv er det viktigste kjennetegnet på en god IT-beslutningstaker.

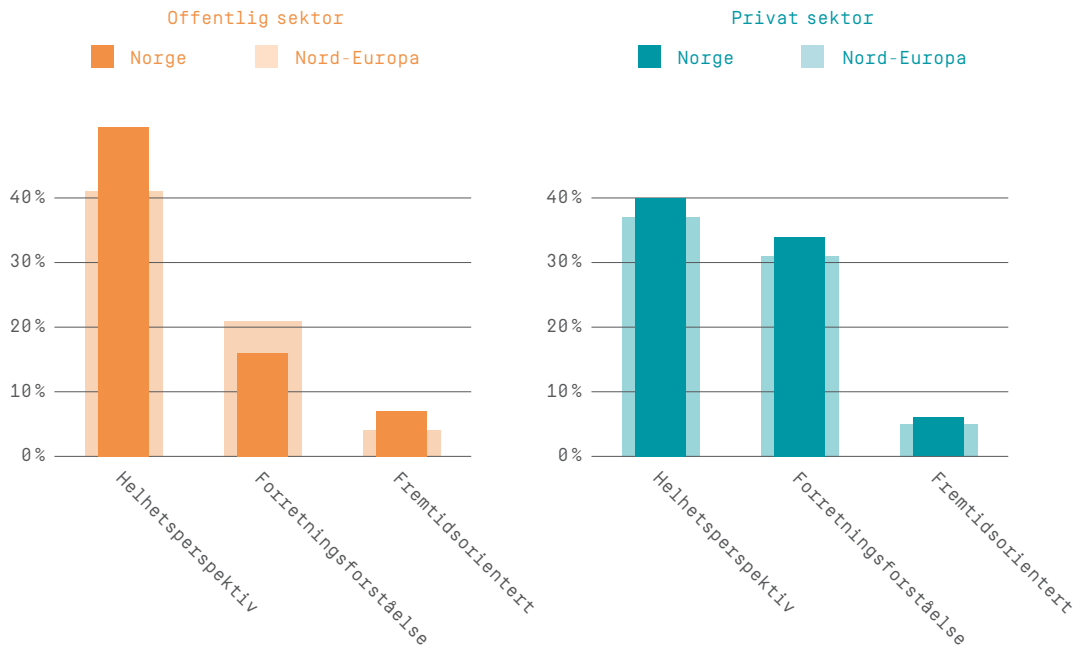
Det kan være utfordrende å administrere og forstå alle aspekter ved IT. Det krever innsikt i hvordan digitale verktøy kan brukes til opplæring, og evne til å ta informerte beslutninger basert på virksomhetens behov og ønsker. Dessuten må vi sikre at IT-investeringene er både kostnadseffektive og bærekraftige. I tillegg krever det kunnskap om relevante lover og risikoer, gode kommunikasjons- og samarbeidsevner, oversikt over teknologiske fremskritt – og ikke minst mot til å teste nye løsninger på en ansvarlig måte. Derfor er det avgjørende å omgi seg med kompetente medarbeidere.

Den usikre verdenssituasjonen krever også et høyt nivå av sikkerhetsbevissthet. De fleste IT-beslutningstakere i Norge rangerer sikkerhet som IT-avdelingens høyeste prioritet de neste tre årene. Mange sier at dette er det området de i år sannsynligvis vil investere mest i, mens de vil bruke mindre på eldre systemer. Også i resten av Nord-Europa øker andelen respondenter som sier at de ønsker å fokusere mer på sikkerhet. Det er klart at geopolitisk uro setter spor og påvirker både nåtiden og fremtiden.

I HODET TIL EN IT-BESLUTNINGSTAKER

Helhetsperspektiv på topp – slik tenker IT-lederne

Hva synes du er det viktigste kjennetegnet på en god IT-beslutningstaker?



Helhetsperspektiv havner på topp når IT-beslutningstakere i Nord-Europa blir bedt om å nevne det viktigste kjennetegnet på en god IT-leder. Det samme ser vi i Norge, i både privat og offentlig sektor. Totalt har 39 prosent valgt dette alternativet i Nord-Europa, noe som er en økning på 2 prosent fra i fjor. Dette er relativt likt i privat og offentlig sektor (henholdsvis 37 og 41 prosent). I Norge har totalt 43 prosent valgt helhetsperspektiv som kjennetegnet på en god IT-beslutningstaker.

IT-beslutningstakere bør ha et helhetsperspektiv, men det er vanskelig å forstå og administrere alle områder innen IT. For en IT-beslutningstaker er det viktig å omgi seg med kompetente medarbeidere, rådgivere og konsulenter.

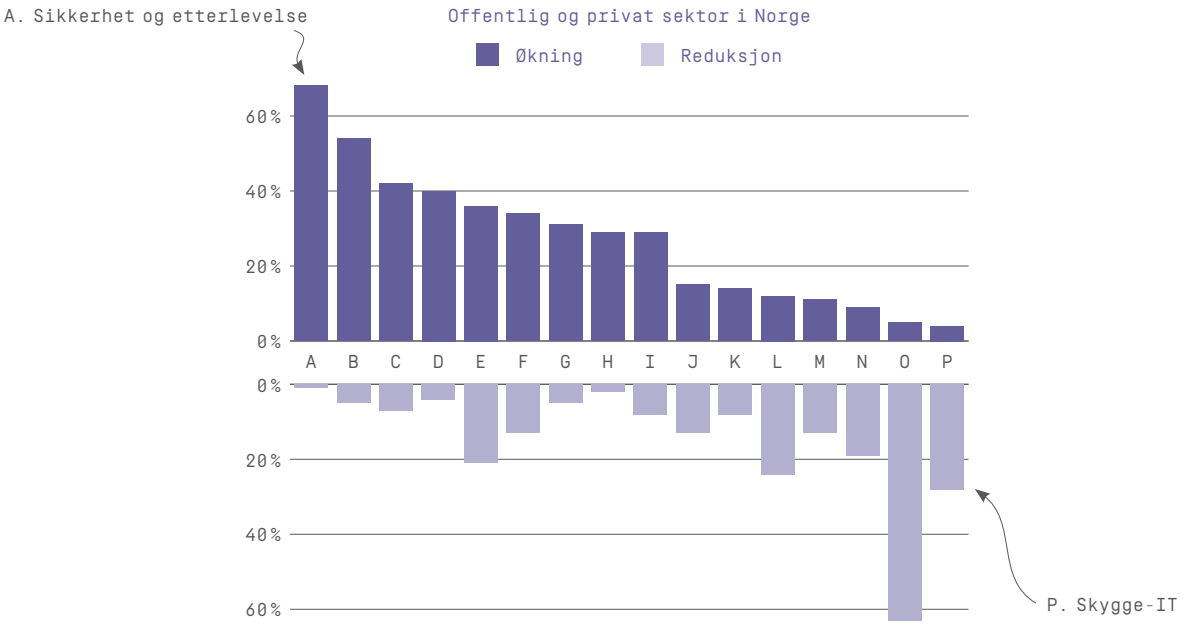
Kvalifikasjonen som blir regnet som nest viktigst totalt sett, er forretningsforståelse (27 prosent). Som en norsk IT-beslutningstaker sier: «Forretningsforståelse er avgjørende for en IT-beslutningstaker, fordi det sikrer at teknologistrategiene er i tråd med virksomhetens mål og gir målbar verdi. Det gjør det mulig for IT-ledere å prioritere tiltak som løser forretningsutfordringer, forbedrer effektiviteten og driver vekst.»

Når forretningsforståelse kombineres med teknologisk innsikt, legges grunnlaget for IT-løsninger som både er innovative og praktiske. Eksempel på dette er bruk av automatiseringsverktøy som effektiviserer driften, strategisk bruk av dataanalyse, og bruk av AI for å støtte beslutningsprosesser.

I HODET TIL EN IT-BESLUTNINGSTAKER

Norske virksomheter ruster opp IT-sikkerheten

IT-forbruket vil i år øke/reduseres på følgende områder ...



Sikkerhet er det området som IT-beslutningstakere i Nord-Europa mest sannsynlig vil bruke mer ressurser på fremover. Blant respondentene som oppgir sikkerhet som sitt hovedfokus (se side 8), sier 80 prosent at de vil bruke mer penger på dette området, på tvers av Nord-Europa. I Norge vil hele 68 prosent av private og offentlige virksomheter øke sitt IT-forbruk på sikkerhet.

De økte investeringene er sannsynligvis et resultat av en økende forståelse av sikkerhetsutfordringene.

Rapporten viser at 47 prosent av nordeuropeiske IT-beslutningstakere vil bruke mindre penger på eldre systemer, og er dermed det området der utgiftene reduseres mest. I Norge er det tilsvarende tallet enda høyere: 63 prosent. Hvorfor er uklart. Én forklaring kan være at mange IT-avdelinger oppgir at de allerede har slått sammen plattformer og ryddet opp i gamle systemer. Dessuten har gamle systemer vært et problem i over 30 år, og den økende digitaliseringshastigheten kan bety at IT-avdelinger med for mange slike systemer forsvinner fra markedet.

Et annet område norske virksomheter vil bruke mindre penger på er "skygge-IT" (27 prosent), som er systemer og løsninger utenfor IT-avdelingens kontroll. Dette signaliserer en prioritering av trygghet og kontroll. Norske virksomheter retter blikket mot mer strukturerte og sikre IT-investeringer, i takt med økte trusler og regulatoriske krav.

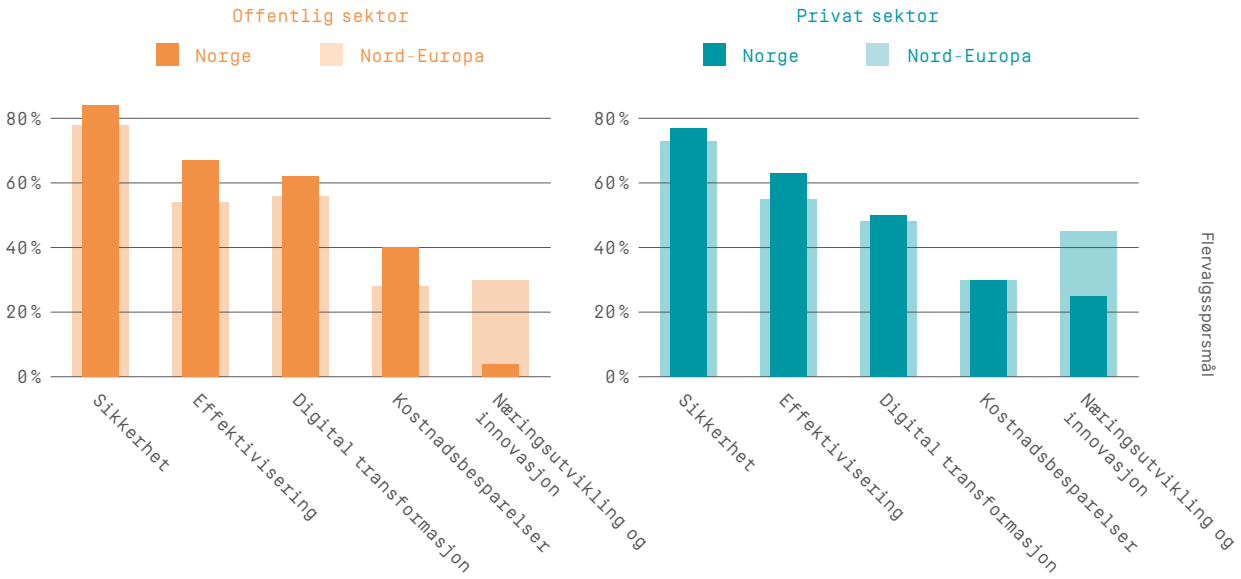
A. Sikkerhet og etterlevelse
B. Skytjenester
C. Digital transformasjon
D. Data og analyse
E. Lisenser og abonnementer [SaaS]
F. Nye applikasjoner og systemer
G. Utvikle AI-modeller
H. Eksisterende AI-tjenester
I. Prosjekter og utvikling
J. IT-støtte og personell
K. Arbeidsplass og samarbeid
L. Maskinvare
M. Telekom og nettverk
N. Datasenter og edge computing
O. Eldre systemer
P. Skygge-IT [Shadow IT]

Flervalgsspørsmål

I HODET TIL EN IT-BESLUTNINGSTAKER

Sikkerhet har fortsatt høyeste prioritet

Hva er IT-avdelingens hovedprioriteringer de neste tre årene?



I dagens verdenssituasjon er det ikke overraskende at sikkerhet vil ha topp prioritet blant IT-avdelinger i Nord-Europa de neste tre årene. Andelen som har sikkerhet på toppen av listen, har økt fra 50 prosent i fjor til 75 prosent i år. Vi gjør imidlertid oppmerksom på at informasjonssikkerhet, som var et eget svaralternativ i fjor, nå er integrert i sikkerhet. Den økte interessen for sikkerhet kommer også tydelig frem i andre deler av denne rapporten.

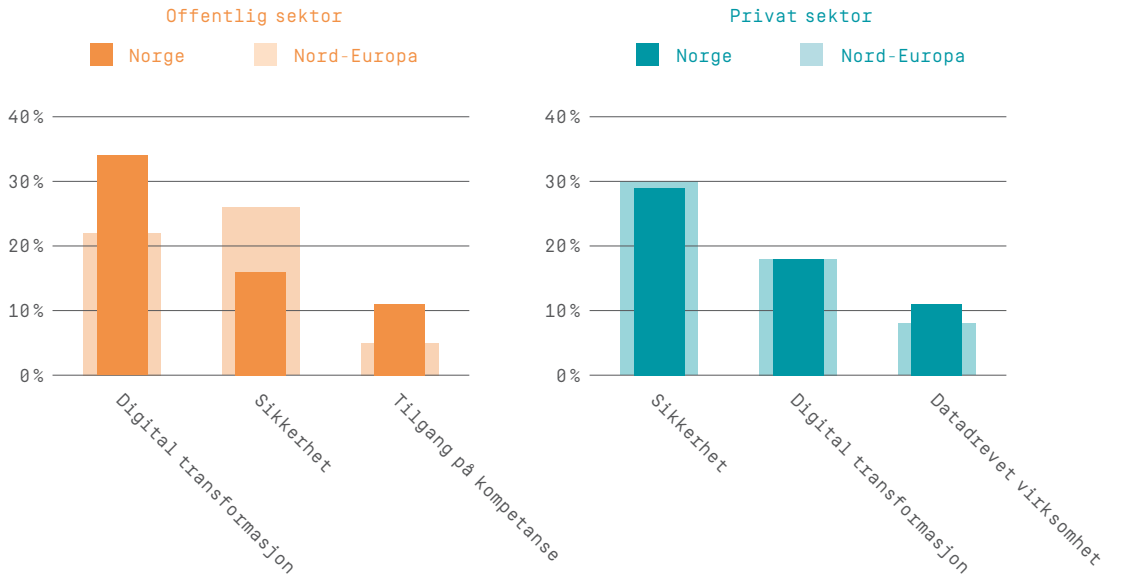
Sikkerhet må alltid vurderes som en del av nye digitale initiativer og i all digital transformasjon. Nye teknologier, for eksempel kunstig intelligens (AI), må ha en riktig balanse mellom innovasjon og sikkerhet. Ifølge det internasjonale revisjons- og rådgivningsselskapet KPMG (*Investing in cybersecurity to safeguard innovation, 2024*) fører dette ofte til omfordeling av ressurser for å sørge for at nye digitale initiativer er sikre fra starten av.

I Norge er det totalt 79 prosent som oppgir sikkerhet som IT-avdelingens hovedprioritering de neste tre årene. Effektivisering og digital transformasjon følger som viktige satsingsområder. Næringsutvikling og innovasjon, og kostnadsbesparelser kommer lengre ned på prioriteringslisten. Dette tyder på at en trygg og effektiv drift veier tyngst for IT-avdelinger fremover.

I HODET TIL EN IT-BESLUTNINGSTAKER

Sikkerhet og digital transformasjon er hovedfokuset til IT-beslutningstakere

Hva er ditt hovedfokus i rollen som IT-beslutningstaker akkurat nå?



Flervalgsspørsmål

Sikkerhet er et tema som går igjen i hele denne rapporten. Også når det er snakk om hovedfokuset til IT-beslutningstakere. Totalt for Nord-Europa har 30 prosent i privat sektor og 26 prosent i offentlig sektor sikkerhet som sitt hovedfokus. Det er også en klar sammenheng mellom dette svaret og det faktum at sikkerhet rangeres betydelig høyere som «største utfordring i fjor» og «største utfordring neste år» (se side 18–19).

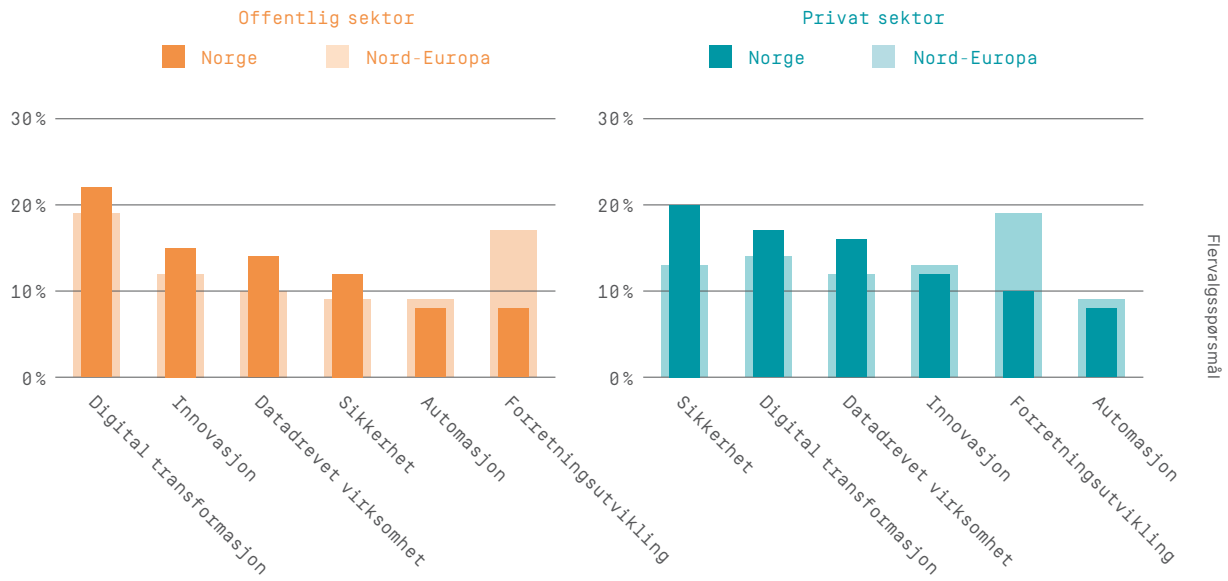
Norske IT-beslutningstakere prioriterer sikkerhet høyest i privat sektor, mens offentlig sektor setter digital transformasjon på topp. Dette er vesentlig høyere enn i Nord-Europa for offentlig sektor. Dette kan tyde på at offentlig sektor er i ferd med å ta et digitalt sprang, samtidig som sikkerhet fortsatt dominerer i privat sektor.

I offentlig sektor i Norge er sikkerhet på vei ned som hovedfokus, fra 34 til 26 prosent sammenlignet med i fjor. Samtidig øker digital transformasjon, kostnadsbesparelser og tilgang på kompetanse. En mulig konklusjon er at offentlig sektor i 2025 kan være mer påvirket av kutt og reduserte budsjetter enn av nye sikkerhetsinvesteringer.

I HODET TIL EN IT-BESLUTNINGSTAKER

Fremtidens prioriteringer for IT-beslutningstakere

Hva vil du fokusere mer på i rollen som IT-beslutningstaker?



IT-beslutningstakere i Nord-Europa ønsker å fokusere mer på sikkerhet og digital transformasjon i sin rolle. Vi ser et tydelig skille mellom privat og offentlig sektor, der privat sektor ønsker å fokusere mer på sikkerhet (20 prosent), mens offentlig sektor fremhever digital transformasjon (19 prosent). IT-beslutningstakere i Nord-Europa trekker også frem forretningsutvikling som et viktig område, i både privat og offentlig sektor.

I privat sektor har Norge tydelig høyere fokus på sikkerhet enn resten av Nord-Europa, mens Nord-Europa er mer opptatt av forretningsutvikling. Fremfor alt er det kommunale IT-ansvarlige som ønsker å satse mer på digital transformasjon. En mulig årsak er at andre virksomheter allerede har investert mye på dette området, mens kommunene har hengt etter. Norge prioriterer også innovasjon og datadrevet virksomhet høyere enn forretningsutvikling og automatisering, som vektlegges mer i Nord-Europa.

En norsk IT-beslutningstaker sier følgende om hva som er viktig å fokusere på fremover: «drive digitaliseringen fremover, samarbeide tett med virksomheten for å styrke forretningsprosesser og legge til rette for å bli datadrevet gjennom data av høy kvalitet på en felles dataplattform». Men mest av alt handler det om å få alle brikkene til å passe sammen.

I HODET TIL EN IT-BESLUTNINGSTAKER

– Vi skal ikke være en bremsekloss, men en partner

Hos Nordic Semiconductor er IT-strategien både fremtidsrettet og menneskesentrert. Å lykkes krever mer enn teknologi, det handler også om å forstå behovene til menneskene som bruker den.

Som IT-beslutningstaker i et globalt teknologiselskap, kreves det mer enn teknisk innsikt. Hos Nordic Semiconductor handler det like mye om å forstå menneskene, skape felles retning og sikre at IT-arbeidet støtter virksomhetens overordnede mål.

– Vi må forstå både teknologien og menneskene som bruker den, sier Sofi Fahlberg, IT Operations Manager i Nordic Semiconductor.

Helhetlig IT-ledelse i et globalt teknologiselskap

Nordic Semiconductor er et norsk teknologiselskap med 1500 ansatte og en omsetning på over 700 millioner dollar. Med et sterkt fotfeste innen trådløs teknologi, retter selskapet blikket mot vekst og økt digital modenhet. I sentrum for den teknologiske driften står Sofi Fahlberg, som leder den operative IT-avdelingen.

– Vi har gått fra å vokse organisk til å jobbe mer helhetlig. Nå spør vi oss hvordan IT best støtter forretningsmålene våre, forteller Fahlberg.

Et internasjonalt team med felles mål

Med en IT-avdeling som sitter i India, Finland, Filippinene og Norge, har Nordic Semiconductor valgt en modell der internasjonalt samarbeid bygger på felles kultur og mål, ikke outsourcing.

Sofi Fahlberg, IT Operations Manager, Nordic Semiconductor.

– Vi har ukentlige møter og jobber som ett team. Når alle jobber i samme organisasjon og deler mål, fungerer det overraskende bra, sier Fahlberg.

Dette samarbeidet muliggjør et tydeligere ansvar og raskere omstilling, samtidig som det styrker sikkerhetskulturen i hele virksomheten.

Fra teknisk støtte til strategisk samarbeidsparter

IT-avdelingen må balansere mellom trygg drift og rask innovasjon. Fahlberg og teamet hennes har tatt eierskap til hele livssyklusen for IT-systemer, og vurderer teknologivalg i sammenheng med risiko, verdi og bærekraft.

– Vi må kjenne hele bildet. Sikkerhet handler ikke bare om teknologi, men om forståelse og kommunikasjon. Ingeniørene våre må forstå hvorfor vi setter grenser til systemer, ikke bare oppleve dem som hinder, forteller Fahlberg.

Dette krever også en ny form for kommunikasjon mellom IT og forretning, som er forankret i tillit og felles mål.

Innovasjon med ansvar

Å balansere innovasjon og stabil drift er kanskje den største utfordringen for moderne IT-ledere. For Fahlberg handler det om å etablere rammer som gir rom for å teste nye ideer, men alltid med sikkerhet og forretningsverdi i sentrum.

– Vi skal ikke være en bremsekloss, men en partner. Derfor er det viktig å bli involvert tidlig, og at vi forstår både forretningsbehov og risiko, sier hun.

I en kompleks og global teknologihverdag har rollen som IT-beslutningstaker utviklet seg fra å være teknisk støtte, til å bli en brobygger og strategisk nøkkelrolle.

ILLUSTRASJON: ISTOCKPHOTO

2

ANSVARSOMRÅDENE TIL EN IT-BESLUTNINGSTAKER

Proaktive IT-avdelinger skaper nye forretningsmuligheter

Flere og flere IT-avdelinger ser på seg selv som proaktive overfor forretningsbehov eller hevder at de beveger seg i den retningen. Andelen reaktive IT-avdelinger går nedover. Det er gode nyheter. Proaktive IT-avdelinger skiller seg kanskje ikke ut når det gjelder resultater, men de har mindre kompetansebehov og mer teknologi i produksjonen. Reaktive IT-avdelinger fokuserer derimot mer på å vedlikeholde eksisterende systemer. I tillegg investerer proaktive IT-avdelinger mer i AI-løsninger som kan hjelpe virksomheten med å utvikle seg og skape nye forretningsmuligheter.

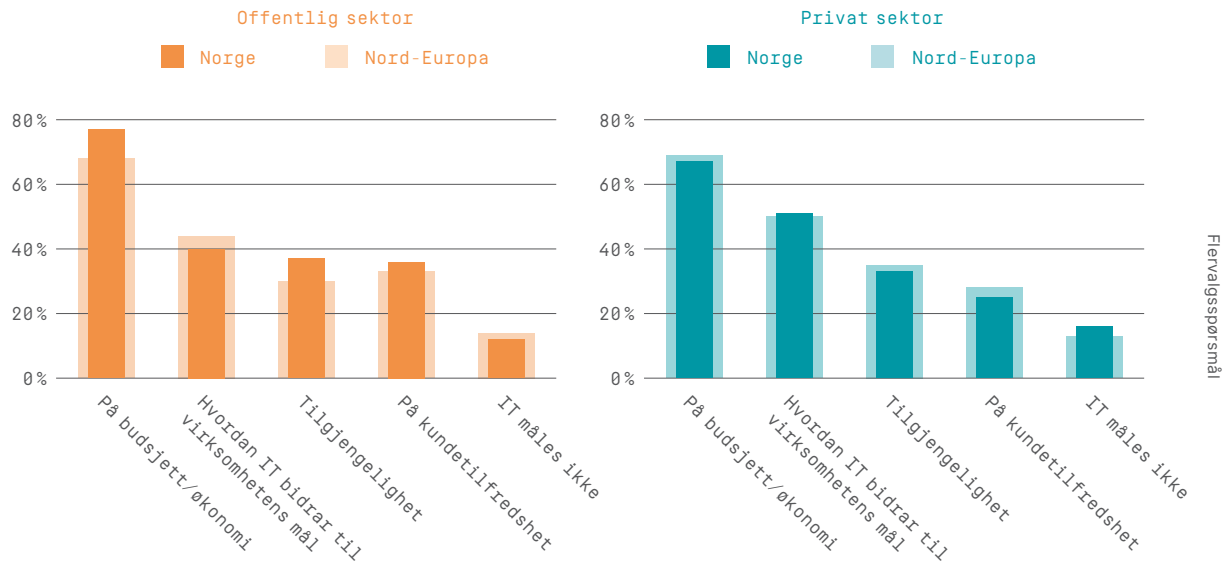
Likevel oppgir under halvparten av alle IT-avdelinger at de blir evaluert ut fra hvordan de bidrar til virksomhetens mål. Budsjett og økonomi er fortsatt den vanligste måten å måle resultatene deres på. IT-transformasjon er en viktig del av den digitale utviklingen til en virksomhet. Det er viktig å måle disse prosjektene basert på kostnad, implementeringstid og levert funksjonalitet, men aller viktigst er det å evaluere hvordan de skaper forretningsverdi. Sammenhengen mellom forretningsvirksomhet og IT styrkes hvis IT-transformasjonen knyttes til økonomiske gevinster. Dette betyr også at initiativer som kommer hele virksomheten og IT-avdelingen til gode, vil bli prioritert høyere.

Samlet sett tar IT-beslutningstakere i Nord-Europa ansvar for færre områder knyttet til virksomhetens bærekraftsmål sammenlignet med i fjor. Samtidig har etterspørselen etter bærekraftseksperter doblet seg. Nye regler og krav driver utviklingen og skaper et større behov for å samle inn og rapportere bærekraftsdata. Dette gir IT-avdelingene mulighet til ikke bare å rapportere disse dataene, men også å ta større ansvar for virksomhetens kjernekomponenter innen IT, for eksempel bærekraftige datasentre, drift og livssyklusstyring. Kanskje betyr dette at bærekraft vil bli en kjernekompetanse innen IT, og ikke bare en oppgave som er nødvendig for å etterleve regelverket.

ANSVARSOMRÅDENE TIL EN IT-BESLUTNINGSTAKER

Budsjett er fortsatt den vanligste måten å evaluere IT på

Hvordan måles og evalueres IT-avdelingen?



Uavhengig av land eller sektor, blir de fleste IT-avdelinger fortsatt evaluert primært på grunnlag av budsjett og økonomi. 48 prosent av IT-avdelinger i Nord-Europa måles ut fra hvordan de bidrar til virksomhetens mål (les mer på side 14 om hvordan resten av virksomheten ser på IT). Det er betydelig vanskeligere å måle hvordan IT bidrar til virksomhetens mål, enn å evaluere kostnadene.

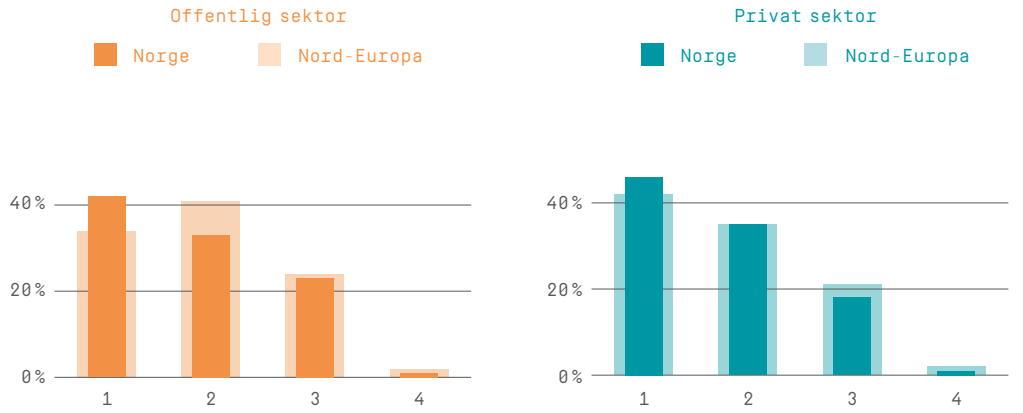
I privat sektor sier flere IT-beslutningstakere at de blir målt på bidrag til virksomhetens mål, enn i offentlig sektor: 50 sammenlignet med 44 prosent. Uavhengig av sektor blir proaktive IT-avdelinger oftere evaluert på bakgrunn av sitt bidrag til virksomhetens mål, totalt 60 prosent (se side 13). Bare 35 prosent av de som har en reaktiv tilnærming, måles på denne måten.

I Norge har det blitt færre IT-avdelinger som ikke måles i det hele tatt, samtidig som flere nå vurderes ut fra virksomhetens resultater. Andelen IT-avdelinger som evalueres basert på hvordan de bidrar til å nå virksomhetens mål, har økt fra 41 til 48 prosent.

ANSVARSOMRÅDENE TIL EN IT-BESLUTNINGSTAKER

Proaktive IT-avdelinger investerer mer i AI

Anser du IT-avdelingen din som proaktiv med tanke på hva virksomheten trenger?



1. Ja, vi møter proaktivt virksomhetens behov.
2. Nei, men vi går mot en mer proaktiv måte å jobbe på.
3. Nei, vi handler mer reaktivt når det gjelder hva virksomheten trenger.
4. Annet.

Selv om andelen IT-beslutningstakere i Nord-Europa som allerede jobber proaktivt for å møte virksomhetens behov ser ut til å være stabil, eller til og med svakt synkende, viser årets tall en positiv trend: Flere er på vei i en mer proaktiv retning. Andelen som sier de beveger seg mot en mer fremoverlent arbeidsform, har økt fra 34 til 37 prosent, samtidig som andelen som fortsatt handler reaktivt, har sunket fra 24 til 22 prosent. Det tyder på at utviklingen går riktig vei – mot et mer strategisk og langsiktig IT-lederskap.

Selv om noen ser på seg selv som proaktive, er det vanskeligere å finne en direkte sammenheng med bedre resultater. Imidlertid har disse virksomhetene et mindre kompetansebehov (se side 21), og de har også mer teknologi i produksjonen, for eksempel AI (se side 30). I tillegg blir proaktive IT-avdelinger sjelden sett på som en nødvendig kostnad av sine respektive organisasjoner, mens reaktive IT-avdelinger oftere blir oppfattet slik (se side 14).

Det er også en sammenheng mellom å handle reaktivt og å investere mindre i både nye og eksisterende AI-tjenester, data og analyse samt prosjekter og utvikling (se side 6). Dette tyder på en viss forsiktighet og en vilje til å prioritere eksisterende systemer fremfor å utvikle nye løsninger.

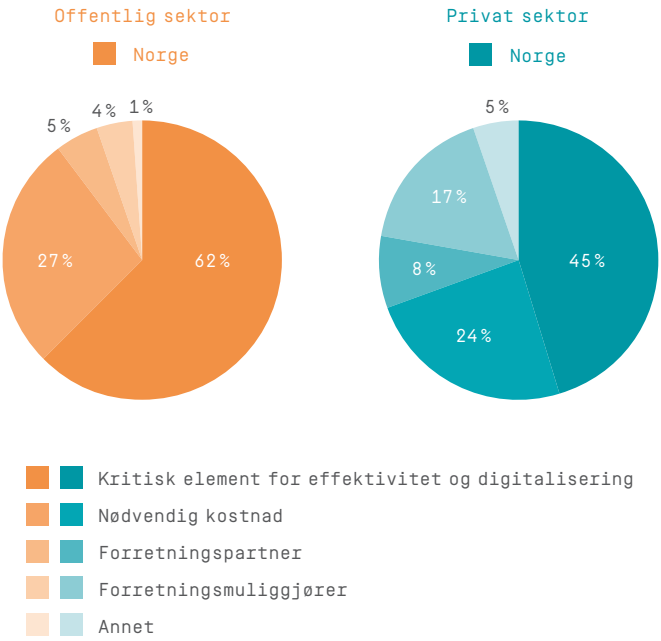
Proaktive IT-avdelinger har generelt større AI-modenhet og virker også mer villige til å investere i utvikling av både nye og eksisterende AI-modeller. Det samme gjelder holdninger til og bruk av skytjenester. 76 prosent av alle proaktive IT-avdelinger har en positiv holdning til offentlige skytjenester, sammenlignet med 65 prosent blant reaktive IT-avdelinger.

I Norge mener 45 prosent av IT-beslutningstakerne at virksomhetene deres er proaktive, noe som er over gjennomsnittet (39 prosent). Danmark og de baltiske landene rangerer seg også høyere enn gjennomsnittet, mens Sverige og Finland rangerer seg lavere. Norge rangerer også sikkerhetsspørsmål lavere på listen over utfordringer både i fjor og neste år, noe som kan være årsaken til at norske IT-beslutningstakere har kunnet jobbe mer proaktivt.

ANSVARSOMRÅDENE TIL EN IT-BESLUTNINGSTAKER

IT-avdelingens rolle i norske virksomheter

Resten av virksomheten ser på IT-avdelingen som en ...



IT-avdelingen kan oppfattes på mange måter i en virksomhet. Den kan ses på som et kritisk element for effektivisering og digitalisering, en nødvendig kostnad, en forretningspartner og en forretningsmuliggjører. Fremfor alt er det IT-avdelingens posisjon og status i virksomheten som påvirker holdningen, samt den rådende oppfatningen om forretningsutvikling og digitalisering. I det ene tilfellet er digitalisering først og fremst en måte å utvikle IT-driften på, mens det i det andre tilfellet har stor betydning for virksomhetens utvikling og forretningsmuligheter generelt.

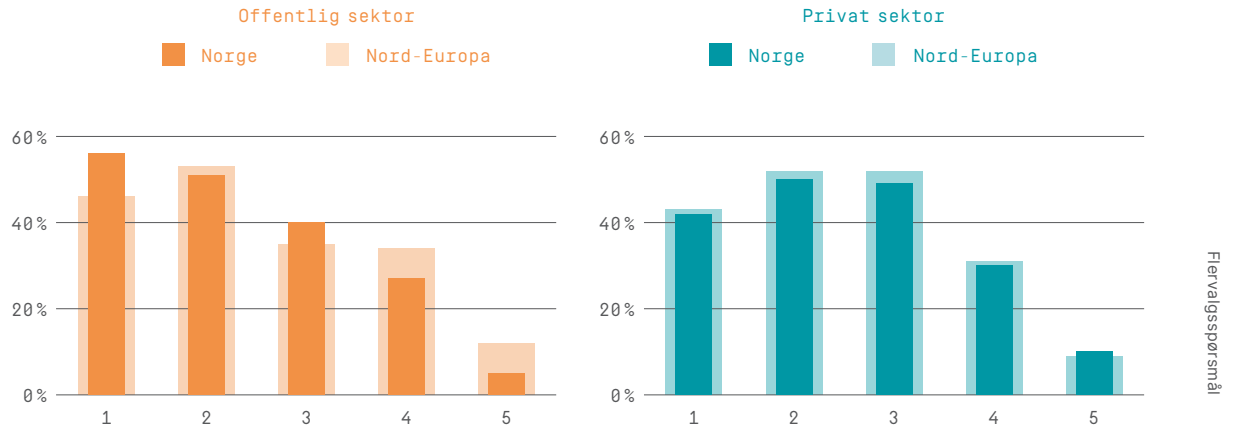
I offentlig sektor i Norge ser hele 62 prosent av virksomhetene på IT-avdelingen som et kritisk element for effektivitet og digitalisering. Kun 27 prosent oppfatter den som en nødvendig kostnad. Færre i privat sektor mener at IT-avdelingen er et kritisk element (45 prosent), men det er flere i privat sektor som ser IT som en forretningspartner eller forretningsmuliggjører sammenlignet med offentlig sektor. Disse funnene viser at privat sektor i større grad anerkjenner den strategiske verdien av IT, mens offentlig sektor i større grad ser IT som en driftskostnad.

IT-avdelingens rolle, og dermed oppfatningen av den, avhenger i mange tilfeller av virksomhetens størrelse. Muligheten til spesialisering og evnen til å bidra til virksomhetens mål er ofte mindre i små IT-avdelinger enn i store. Samtidig kan det være vanskelig for mellomstore virksomheter å finne riktig nivå på spesialisering og ansvarsfordeling. Det kan føre til ineffektivitet hvis de ofte bytter mellom ulike løsninger.

ANSVARSOMRÅDENE TIL EN IT-BESLUTNINGSTAKER

Norge går i bresjen for å samordne IT-strategien med bærekraftsmålene

Hva anser du som ditt ansvar som IT-beslutningstaker når det gjelder selskapets bærekraftsmål?



1. Digitalisere forretningsprosesser for å nå virksomhetens bærekraftsmål.
2. Sette og følge opp bærekraftsmål for IT-drift.
3. Støtte og effektivisere det interne bærekraftsarbeidet til virksomheten ved hjelp av IT- og analyseverktøy for datainnsamling og visualisering.
4. Støtte utviklingen av produkter og tjenester som hjelper kundene med å nå sine bærekraftsmål.
5. Ingen av de ovennevnte er en del av mitt ansvar.

Utvikling av nye teknologier og digital transformasjon blir stadig viktigere for bærekraftsarbeidet. Virksomheter med IT-avdelinger som anser seg selv som ansvarlige for å sette bærekraftsmål, er også mer tilbøyelige til å tilpasse IT-strategien til disse målene. Virksomheter som ikke tilpasser sine digitale strategier til bærekraftsmål, har ofte IT-beslutningstakere som ikke ser på bærekraft som sitt ansvar.

De fleste nordeuropeiske IT-beslutningstakere som ikke tar ansvar for bærekraftsmål, jobber i mindre IT-avdelinger. Større IT-avdelinger har i større grad tilpasset IT-strategiene sine til bærekraftsmål. Når IT-beslutningstakere inngår i toppledelsen, blir IT oftere oppfattet som en muliggjører av bærekraft. IT-beslutningstakere i ledelsen er mer tilbøyelige til å digitalisere for bærekraft og tilpasse IT-strategien til bærekraftsmålene.

I Norge ser 51 prosent av IT-beslutningstakerne det som sitt ansvar å sette og følge opp bærekraftsmål. Dette er litt under gjennomsnittet (53 prosent). På den annen side er det i offentlig sektor en betydelig økning i digitaliserte forretningsprosesser for å nå bærekraftsmål (fra 32 til 56 prosent) og dessuten økt bruk av IT-/analyseverktøy for å støtte bærekraftsarbeidet (fra 29 til 40 prosent). Dette viser en bevisst innsats i offentlige virksomheter for å knytte digitalisering til miljømål og la teknologi drive bærekraft.

67 prosent av norske virksomheter har en IT-strategi som er i tråd med bærekraftsmålene, noe som er høyere enn gjennomsnittet (59 prosent). Det tilsvarende tallet i Sverige er 64 prosent. Dette tyder på et nokså likt engasjement i de to landene, og sammen tar de ledelsen på dette området. En sterkere bærekraftskultur kan forklare hvorfor Norge og Sverige skårer høyere på IT-tilpasning.

ANSVARSOMRÅDENE TIL EN IT-BESLUTNINGSTAKER

Ny IT-strategi skal drive Elkems globale vekst og bærekraft

Med røtter tilbake til 1904 og et fotavtrykk på fire kontinenter, lanserer Elkem nå en ny digital strategi fram mot 2028. Målet er å balansere innovasjon og stabil drift – og sikre at teknologien støtter både vekst og bærekraft i årene som kommer.

Stolte røtter og globalt perspektiv

Grunnlagt i Norge i 1904, er Elkem i dag en av verdensledende produsenter av silisiumprodukter, med virksomhet på fem kontinenter. Selskapet har over 7200 ansatte og 31 produksjonssteder over hele verden.

– Elkem er en leverandør av silisium og silisiumprodukter, hvor vi eier hele verdikjeden, fra kvartssand til ferdige silisiumprodukter, sier Claire Førland, Infrastructure and Operations Director i Elkem.

Selskapet kombinerer stolt norsk industriarv med global kjemikompetanse.

– Vi har røtter langs norskekysten, men også store enheter i Kina og Frankrike, forteller Førland.

Elkem hjelper sine kunder med å skape og forbedre viktige innovasjoner som elektrisk mobilitet, digital kommunikasjon, helse og personlig pleie, samt smartere og mer bærekraftige byer.

Bærekraft handler også om mennesker

Bærekraft for Elkem handler ikke bare om teknologi, men også om folkene som driver utviklingen fremover. Med rundt 100 ansatte i IT-avdelingen, og 30 personer som jobber med infrastruktur og operasjoner, er mangfold et viktig fokusområde for selskapet.

– Da jeg startet var det nesten ingen kvinner i teamet og IT-avdelingen. Nå er vi flere, men vi må jobbe aktivt med hvordan vi skriver

Claire Førland, direktør for infrastruktur og drift, Elkem.

stillingsannonser for å tiltrekke flere kvinner, sier Førland.

Hun påpeker viktigheten av å senke terskelen for å tiltrekke bredere søkermasser: – Når jobbutlysninger blir for tekniske, kan det skremme bort kvinnelige kandidater, selv om de har kompetansen som kreves.

En IT-strategi for fremtiden

Elkem har nylig utgitt en ny IT- og digitalstrategi som skal vare til 2028. Men her er det ikke snakk om planer som blir liggende i en skuff:

– Strategien skal være et levende verktøy, ikke bare en presentasjon på slides. Nå handler det om å få hele teamet til å forstå og anvende prinsippene i praksis, forklarer Førland.

Førland forteller at innovasjon alltid må balanseres med stabil drift.

– Som leder for infrastruktur og operasjoner handler mitt ansvar om å bygge løsninger som ikke bare støtter dagens behov, men som også legger grunnlaget for fremtiden. Vi jobber målrettet for å skape reell digital verdiskaping, spesielt innen produksjon. Det gjør vi i tett samarbeid med forretningen, gjennom å ta i bruk ny teknologi for å modernisere infrastrukturen vår, og ved å styrke datakvalitet og datastyring.

AI i arbeidshverdagen

AI er allerede en naturlig del av Elkem sin hverdag. Selskapet har blant annet tatt i bruk Microsoft Copilot og utviklet en egen intern AI-plattform. – Vi har lansert tolv applikasjoner og har nå over 500 brukere internt, sier Førland.

Bruken av AI handler om effektivisering, men alltid med datasikkerhet i sentrum: – Målet er å gjøre arbeidsflytene smartere, samtidig som vi opprettholder fokus på datasikkerhet og personvern, forteller Førland.

En strategisk partner for fremtiden

Elkem tenker stort om fremtiden, både i teknologi, bærekraft og samfunnsansvar. – Vi ønsker ikke bare å være en støttefunksjon. Vi vil være en strategisk partner for forretningen, understreker Førland.

Med ny IT- og digitalstrategi, og en offensiv tilnærming til både bærekraft og samfunnsansvar, posisjonerer Elkem seg som en ledestjerne i en industri som må endre seg raskt for å møte globale utfordringer.

– Vi skal være en aktør som tar ansvar, utvikler oss smart, og bygger broer mellom teknologi, forretning og bærekraft, avslutter Førland.

ILLUSTRASJON: ISTOCKPHOTO

UTFORDRINGER OG KOMPETANSE I IT-AVDELINGEN

Sikkerhetsutfordringer øker etterspørselen etter kompetanse

Sikkerhet er både neste års største utfordring og det IT-beslutningstakere i Nord-Europa prioriterer høyest fremover, men det er noen forskjeller mellom landene.

Norge og Finland peker særlig på ressurser som en hovedutfordring, mens Sverige og Danmark i større grad fremhever sikkerhet som det mest krevende. Den samlede andelen som ser på sikkerhet som sin største utfordring neste år, har gått noe ned, selv om dette området fortsatt rangeres som det viktigste. Dette kan skyldes at sikkerhet ikke lenger ses på som én enkelt oppgave som skal løses én gang for alle, men som en naturlig del av det løpende arbeidet.

Sikkerhetens betydning er tydelig når det gjelder hva slags kompetanse som er etterspurt i IT-bransjen. Over halvparten av respondentene i årets rapport har behov for sikkerhetseksperter, noe som er et klart tegn på kompetansemangel på dette området. Ekspertise hentes inn gjennom leverandører i stedet for gjennom ansettelser, noe som er kostbart på lang sikt.

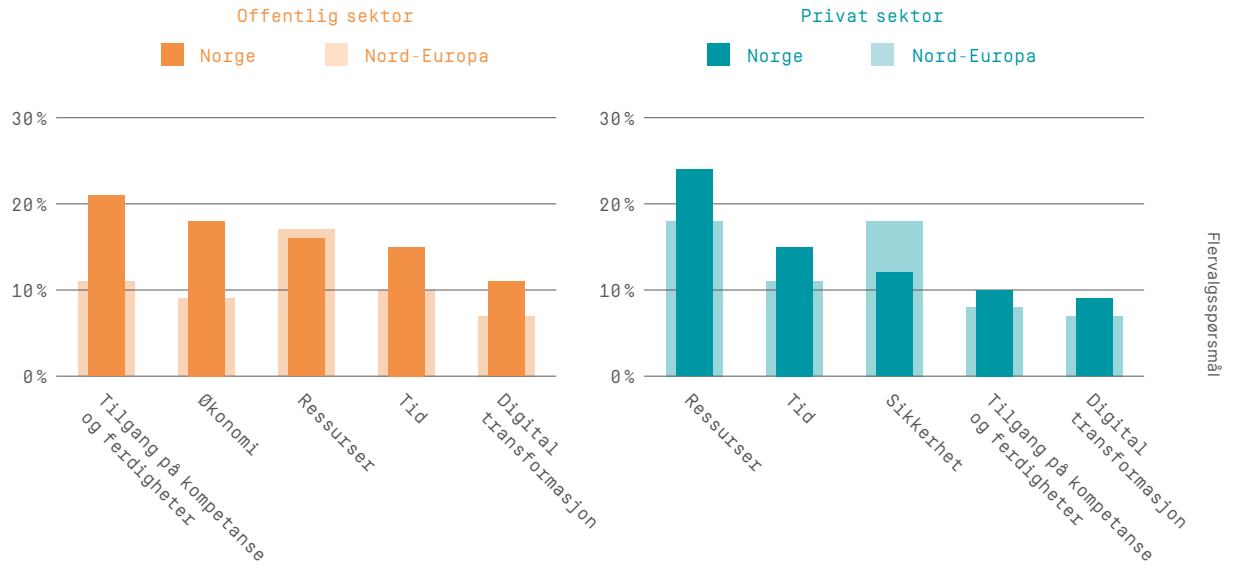
Etterspørselen etter endringsledelse øker tydelig. Dette er sannsynligvis et resultat av økt fokus på digital transformasjon, der AI og andre systemer også kan bidra til økt sikkerhet.

Kvinner er fortsatt underrepresentert i IT-bransjen, noe som ikke har endret seg fra tidligere år. I flere av landene øker imidlertid andelen kvinner som studerer tekniske fag. Dette lover godt for fremtiden.

UTFORDRINGER OG KOMPETANSE I IT-AVDELINGEN

Mangel på ressurser er en stor utfordring i Norge

Hva var IT-avdelingens største utfordring i fjor?



I fjor var mangel på ressurser den største utfordringen for nordeuropeiske IT-beslutningstakere, men andelen som peker på dette har falt fra 25 til 18 prosent. I Sverige og Danmark ble sikkerhet rangert som den største utfordringen, mens bare 12 prosent i norsk privat sektor oppgir det samme – i offentlig sektor i Norge er tallet enda lavere, med kun 11 prosent som ser på sikkerhet som den største utfordringen. Det kan skyldes at sikkerhetsarbeidet i Norge ofte håndteres utenfor IT-avdelingen, eller at NIS2-direktivet oppleves som mindre presserende her. Atea Norges modenhetsanalyser viser at teknisk sikkerhet er godt ivaretatt, men at formelle rutiner og retningslinjer ofte mangler. Samtidig skårer Norge høyt på «Ressurser» i privat sektor, som indirekte favner flere andre områder.

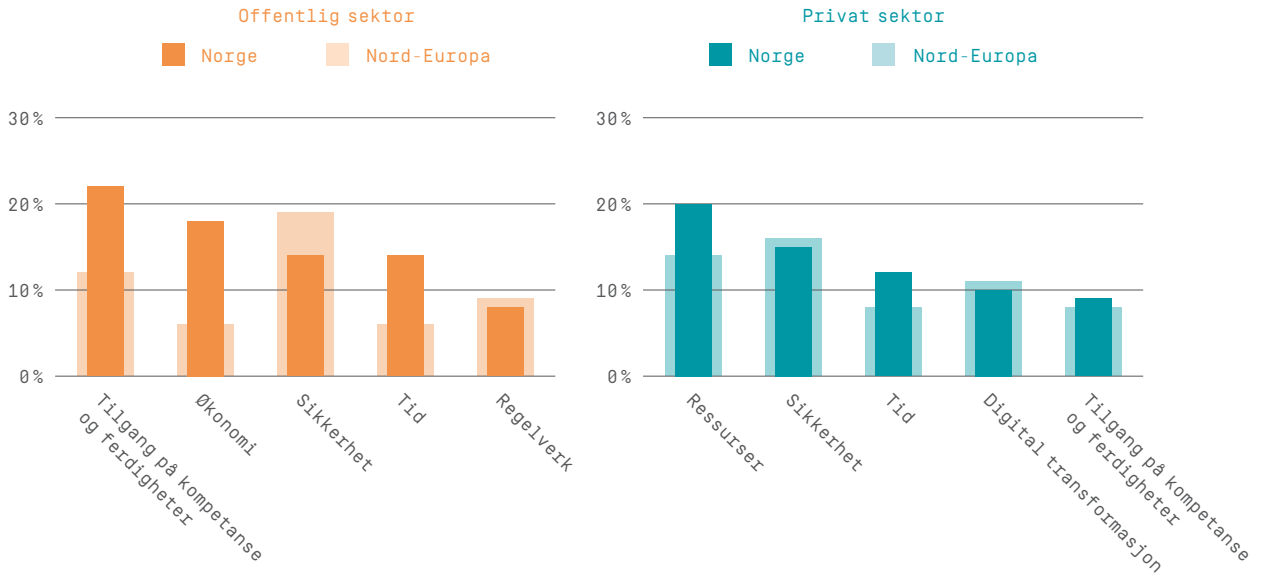
En annen faktor kan være at nordmenn prioriterer annerledes. Det stilles svært høye krav til digital transformasjon, for eksempel når myndighetene sier at Norge skal være det mest digitaliserte landet i verden innen 2030. Mangel på ressurser fører også til manglende fokus på sikkerhet, siden du trenger ressurser og mennesker for å kunne håndtere sikkerhetsbildet.

I offentlig sektor i Norge peker tilgang på kompetanse og ferdigheter seg tydelig ut som en av de største utfordringene, mens privat sektor sliter særlig med ressursmangel og tidspress. For å håndtere denne utfordringen må norske IT-avdelinger styrke teamets ferdigheter, prioritere oppgaver bedre og jobbe mer strategisk for å knytte IT-investeringer til bedriftens langsiktige visjon. Samtidig må man sikre bedre ressursstyring og samarbeid på tvers av avdelinger for å skape en mer integrert og effektiv tilnærming til digitalisering.

UTFORDRINGER OG KOMPETANSE I IT-AVDELINGEN

Tilgang på kompetanse og ressurser er neste års største utfordring

Hva tror du blir IT-avdelingens største utfordring neste år?



Sammenlignet med fjorårets største utfordring (forrige figur), viser årets forventninger at tilgang på kompetanse og ferdigheter (22 prosent) fortsatt er den klart største utfordringen i offentlig sektor i Norge. Nivået ligger stabilt høyt, noe som tyder på at dette er en vedvarende flaskehals for utvikling og gjennomføring. Økonomi, sikkerhet og tid blir også trukket frem som IT-avdelingers utfordringer neste år.

I privat sektor i Norge er bildet annerledes. Her er ressurser den største utfordringen (20 prosent), tett fulgt av sikkerhet og tid. Norge skiller seg ut ved at ressurser, og tilgang på kompetanse og ferdigheter, vurderes som større utfordringer enn våre naboland. Norske IT-avdelinger er mer bekymret for tilgang på kompetanse og ressurser enn sine nordeuropeiske kollegaer.

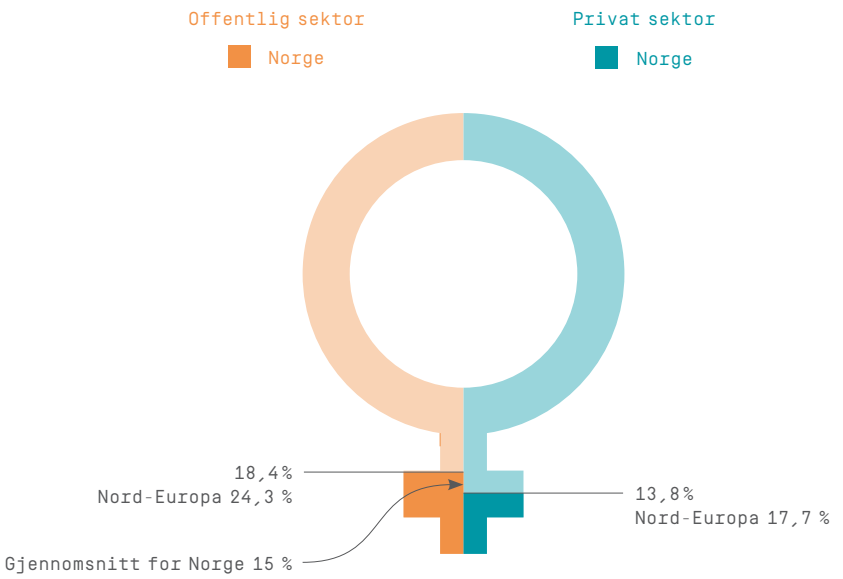
Sikkerhet trekkes frem som en av de største utfordringene for IT-avdelinger neste år – både i Norge og ellers i Nord-Europa. Det er også det området som prioriteres høyest (side 7), noe som gjenspeiles i det økende behovet for sikkerhetskompetanse (se side 21). Dette tyder på at mange virksomheter mangler nødvendig kompetanse, og understreker behovet for å sette ut tjenester og samarbeide tett med sikkerhetseksperter.

Cybertrusler er en vedvarende utfordring i Norge, og stadig mer avanserte angrep krever betydelige investeringer i cybersikkerhet. I tillegg påvirker dagens geopolitiske situasjon hvordan sikkerhetsarbeidet prioriteres i nordeuropeiske virksomheter.

UTFORDRINGER OG KOMPETANSE I IT-AVDELINGEN

Kvinner fortsatt underrepresentert i IT-bransjen – spesielt i Norge

Hvor mange kvinner jobber i IT-avdelingen?



Bare én av fem ansatte i IT-avdelinger i Nord-Europa er kvinner – en andel som ikke ser ut til å øke, til tross for stor interesse for teknologibransjen blant kvinner.

Norge skiller seg negativt ut med lavest kvinneandel i både offentlig (18 prosent) og privat sektor (14 prosent). Dette reflekterer et fortsatt kjønnsdelt arbeidsmarked, der kvinner i større grad jobber i offentlig sektor, mens menn dominerer privat sektor. Selv om 29 prosent av de ansatte i teknologibransjen i Norge er kvinner, viser denne rapporten at gjennomsnittet i IT-avdelinger er nede på 15 prosent.

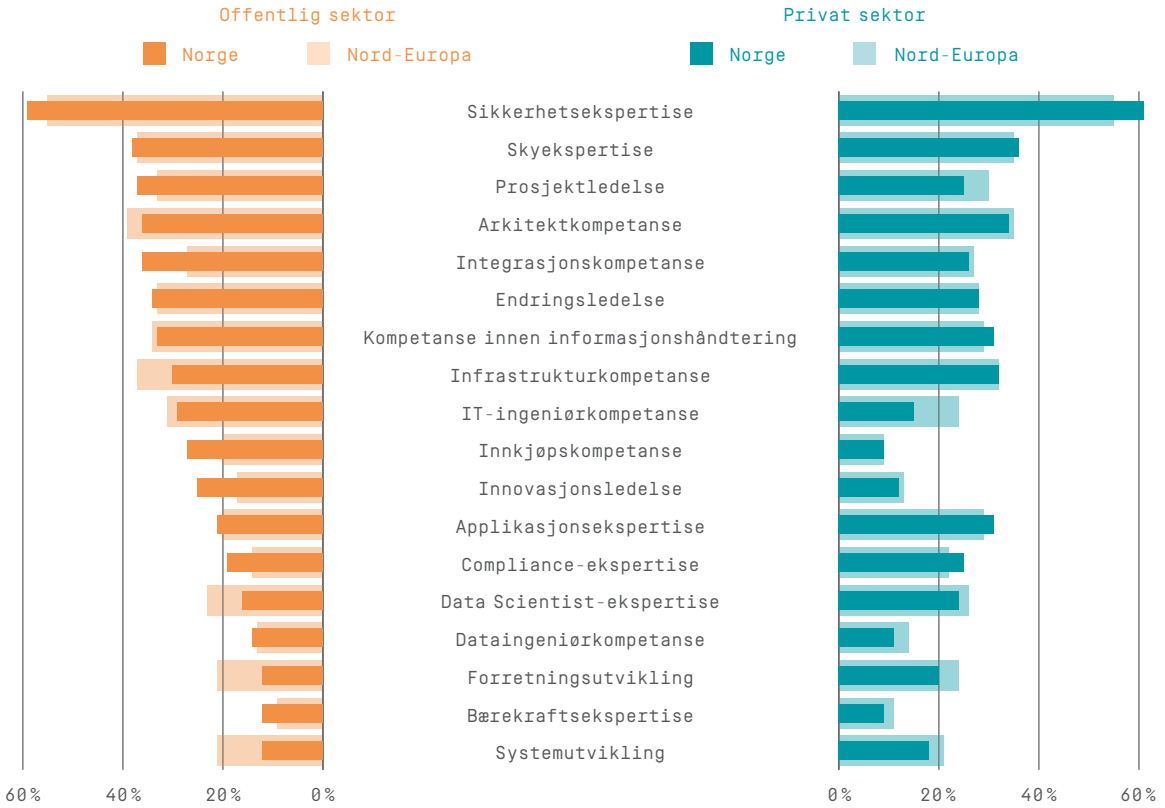
42 prosent av nordeuropeiske virksomheter har ingen kvinner i sine IT-avdelinger. Tallet stiger til 50 prosent i privat sektor. Alle landene i denne rapporten har en lav andel kvinner i IT-avdelinger, spesielt i privat sektor. Årsaken til dette er sannsynligvis at færre kvinner enn menn velger å studere STEM-fag (Science, Technology, Engineering & Mathematics), selv om de nordiske landene har flere kvinnelige STEM-studenter enn ellers i EU. Generelt er det i de nordiske og baltiske landene også færre kvinnelige rollemodeller i IT-bransjen.

IT er et bredt fagområde med mange roller å fylle. Kompetansebehovet er stort og mangfoldig (se side 21). Vi må sette søkelyset på de konkrete arbeidsoppgavene fremfor å opprettholde et utdatert og feilaktig bilde av IT. Det er viktig å få frem dette i alle land, siden det trolig kan trekke flere kvinner til bransjen. Det er allerede tegn til endring i mange nordiske land. Andelen kvinner med IT-fag som førstevalg har økt.

UTFORDRINGER OG KOMPETANSE I IT-AVDELINGEN

Stor etterspørsel etter sikkerhetseksperter

Hvilken kompetanse vil IT-avdelingen din trenge i løpet av de neste 12 månedene?



Flervalgsspørsmål

Det er en økning i etterspørselen etter kompetanse på nesten alle områder. Det er spesielt høy etterspørsel etter sikkerhetseksperter (55 prosent), IT-arkitekter (37 prosent) og skyeeksperter (36 prosent) i Nord-Europa. Det geopolitiske klimaet er fortsatt usikkert, med stadig flere cyberangrep, noe som påvirker etterspørselen etter kompetanse.

Den største forskjellen mellom i fjor og i år ser vi i etterspørselen etter endringsledelse, som har økt fra 20 til 30 prosent i Nord-Europa. Etterspørselen øker i hele Nord-Europa uavhengig av bransje eller organisasjonsstørrelse. Det ser ut til å være en sammenheng mellom behov for endringsledelse og økt fokus på digital transformasjon (se side 7–9).

Tall fra Norge viser at behovet for sikkerhetseksperter er størst – 61 prosent av virksomhetene sier dette er viktig det neste året. Norske IT-avdelinger trenger også skykompetanse (37 prosent) og arkitektkompetanse (34 prosent), noe som signaliserer en tydelig etterspørsel etter robuste og skalerbare IT-løsninger det kommende året. Offentlig sektor etterspør også prosjektledelse, mens privat sektor ser etter mer teknisk spisskompetanse. Alt i alt viser dette at norske virksomheter må både sikre seg bedre, og bygge mer moderne systemer.

For å forbli konkurransedyktige i et globalt teknologilandskap må norske virksomheter også ta tak i den økende kompetansemangelen. Dette kan innebære både internasjonal rekruttering og målrettet utvikling av etterspurte ferdigheter.

UTFORDRINGER OG KOMPETANSE I IT-AVDELINGEN

AF Gruppen: Teknologi og sikkerhet tett på prosjektene

– Vi skal være en IT-partner man kan stole på hele veien. Målet vårt er å være tett på brukerne og levere løsninger som fungerer, og gjøre hverdagen enklere og arbeidshverdagen sikrere, sier Glenn Hagelund, leder for IT Drift & Sikkerhet i AF Gruppen.

AF Gruppen er et konsern med rundt 6000 ansatte, fordelt på 140 datterselskaper, som opererer innen bygg, anlegg, energi og miljø, offshore og eiendom. Det er et komplekst landskap med mange prosjekter, der selskapene tar teknologiske valg som er fornuftige for egne behov. Det gir stor frihet, men også et behov for felles retning, struktur og sikkerhet.

– Det er viktig for oss at teknologi ikke blir en barriere, men en muliggjører. Vår oppgave er å sørge for at løsningene er teknisk solide, stabile og sikre, og at de faktisk fungerer ute i felten, sier Hagelund.

Tillit, støtte og sikkerhet i bunnen

AF Gruppen har styrket sikkerhetsmiljøet betydelig de siste årene, med god støtte fra konsernledelse og et styre som er interessert og engasjert. Det gir trygghet og retning.

– Den største utfordringen handler ofte om menneskelige feil. Regelmessige tester viser at vi har mange våkne og bevisste brukere, og det er en god sikkerhetskultur på gang. Men vi har fortsatt en vei å gå. Vår jobb er å beskytte brukerne uten å forstyrre dem unødig i det daglige, sier Hagelund.

AF Gruppen benytter både interne sikkerhetsressurser og en ekstern partner for overvåking og respons, i tillegg til automatiserte tiltak.

– Vi stopper mange angrep før brukeren i det hele tatt merker noe. Men det krever mennesker som jobber dedikert med dette,

Glenn Hagelund, leder for IT Drift & Sikkerhet, AF Gruppen

og derfor har vi en sterk partner vi samarbeider tett med for å sikre vår infrastruktur og data, forklarer han.

Sikkerhetsforståelse i hele organisasjonen

Sikkerhet handler ikke bare om teknologi, men også om kultur og forståelse på tvers av fagområder.

– Det er avgjørende med grunnleggende sikkerhetsforståelse i hele organisasjonen, ikke bare i IT. HR, økonomi og prosjektledere håndterer også verdifulle data. Vi har et ansvar for å gjøre det enklere å ta gode valg, og følge opp med støtte, opplæring og tydelige rutiner, forteller Hagelund.

AI og ny teknologi

AF Gruppen har tro på at AI og nye digitale løsninger vil skape stor verdi, særlig ute i prosjektene. Mange datterselskaper av AF Gruppen har som strategi å være ledende innen bruk av teknologi, og bruker en kombinasjon av interne ressurser og eksterne partnere for å gjøre bygging smartere, mer kostnadseffektivt og bærekraftig.

– Vi ønsker å gi selskapene frihet til å teste ut AI-løsninger og digitale verktøy selv. Vår jobb er å legge til rette for det med god datakvalitet, infrastruktur og sikkerhet. Vi skal ikke bremse initiativ, vi skal muliggjøre dem, sier Hagelund.

Han understreker samtidig at dette ikke er «plug-and-play».

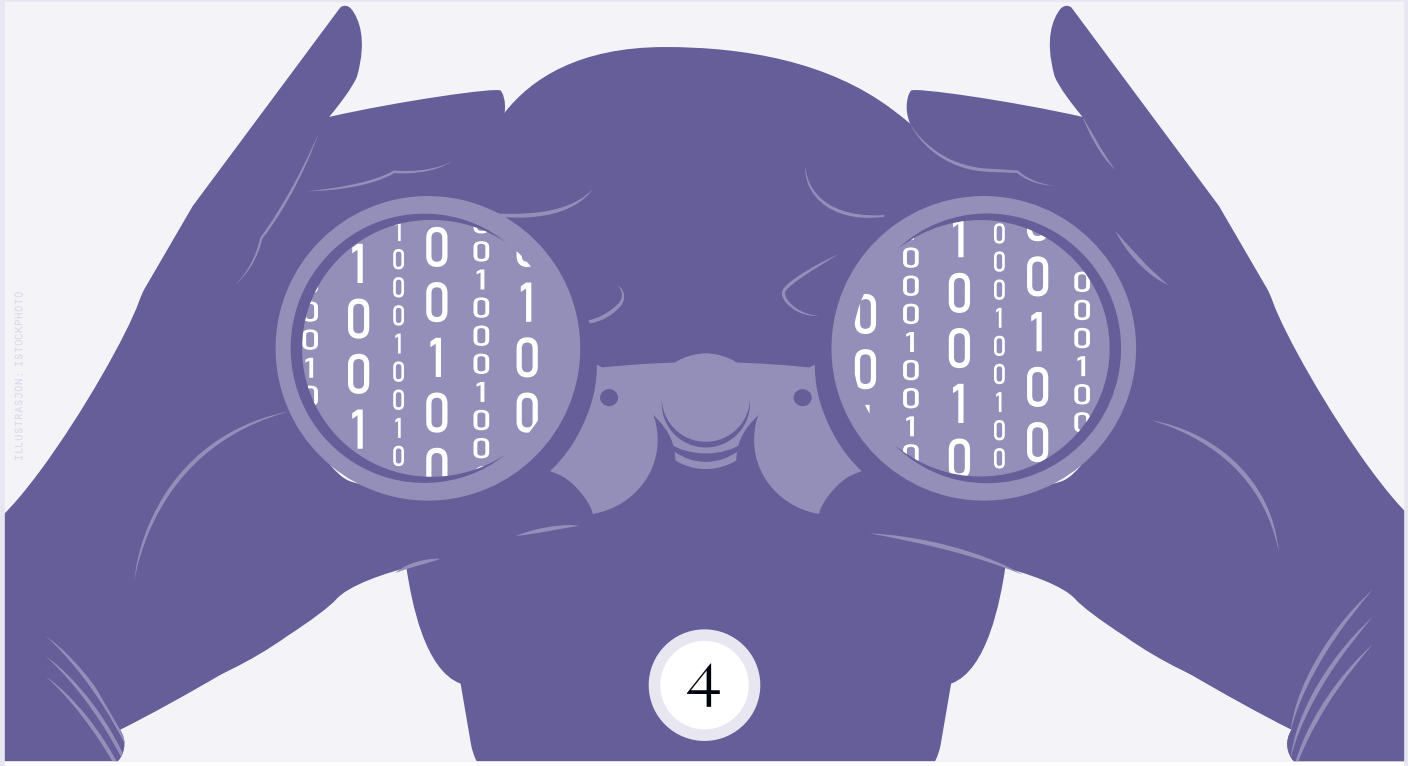
– Mange har en forventning om at AI skal løse alt med én gang, men det krever innsats, målrettet arbeid og litt planlegging. Det viktigste er å tørre å starte – teste, feile og lære underveis. Potensialet er enormt, og vi ser allerede verdien i områder som masselogistikk, planlegging og visualisering.

Blant bruksområdene nevner han droner og AI-verktøy for beregning av masser, forbedret logistikk og mer effektiv prosjektgjennomføring på byggeplass.

Verdiene skal gjenspeiles i arbeidet

Verdiene til AF Gruppen - tillit, grundighet, lønnsom vekst og frihet til å tenke nytt - gjenspeiles i måten IT-avdelingen jobber på.

– Vi skal være til å stole på, legge til rette for vekst og bidra til at våre selskaper kan være nysgjerrige, utforske ny teknologi og utvikle seg – innenfor trygge og forutsigbare rammer. Det krever balanse mellom disiplin og entreprenørånd, og det er akkurat der vi i IT skal støtte, avslutter Hagelund.



ILLUSTRASJON: ISTOCKPHOTO

4

UTVIKLE MOTSTANDSDYKTIGHET OG MOTSTÅ TRUSLER

Mer bevissthet om cyberangrep

Antallet cyberangrep øker, og det går også frem i årets rapport. Det berører alle land, og både små og store virksomheter. Men det ser ut til å være en viss motvilje mot å snakke åpent om disse angrepene.

Berørte virksomheter frykter at det vil gi et dårlig inntrykk av merkevaren deres. Det finnes imidlertid klare eksempler på det motsatte. De som forteller om erfaringene sine, gir et mer positivt inntrykk enn de som prøver å skjule det som har skjedd. En åpen diskusjon gjør dessuten at vi kan lære av hverandre.

Motstandsdyktighet handler om å være fleksibel og kunne hente seg raskt inn igjen etter en potensiell hendelse. Trusler må oppdages og håndteres i tide. Dette krever at både teknologi og prosedyrer er på plass. For en virksomhet er det svært viktig å analysere risiko, være bevisst på egen sårbarhet, ha en plan for uforutsette hendelser og ikke minst lære opp medarbeiderne sine.

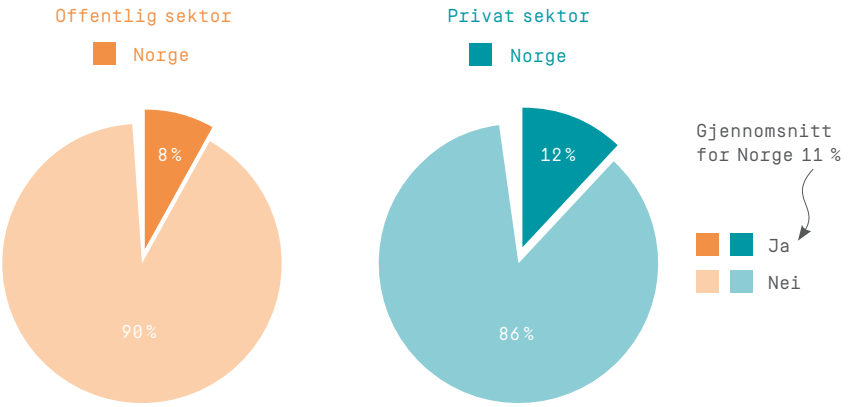
Flere virksomheter enn i fjor oppgir at de har en plan for uforutsette hendelser, som cyberangrep. Det er positivt, men for få ser ut til å ha øvd på planen sin. Det siste er like viktig. Et flertall av respondentene sier at de allerede har tilpasset eller vil tilpasse beredskapsplanene sine for å håndtere cyberangrep. Det er bekymringsfullt at enkelte ikke har gjort dette eller har planer om det, til tross for et økende antall cybertrusler over hele verden.

Nesten ingen virksomheter i Norge, uavhengig av størrelse, har hatt kunder som krever at de følger NIS2. Norske kunder vet at direktivet finnes, men har foreløpig ikke inkludert det i kontrakter med aktører i verdikjeden. Dette skyldes sannsynligvis at NIS2 ennå ikke gjelder innenfor Norges grenser.

UTVIKLE MOTSTANDSDYKTIGHET OG MOTSTÅ TRUSLER

Antall cyberangrep øker

Har dere opplevd noen alvorlige cyberangrep de siste 12 månedene?



15 prosent av nordeuropeiske IT-beslutningstakerne har opplevd alvorlige cyberangrep i løpet av det siste året. I Norge er det tilsvarende tallet 11 prosent.

De berørte kommer fra alle land og fra både små og store virksomheter, relativt jevnt fordelt mellom offentlig og privat sektor. Respondentenes tolkning av begrepet «alvorlig cyberangrep» kan variere. Ting tyder på at også mindre, mislykkede cyberangrep har blitt inkludert. Det sier noe om antall angrep, men ikke om konsekvensene av dem har blitt større. Dette kan forklare hvorfor andelen berørte er høyere enn i andre undersøkelser.

Ifølge årsrapporten til Nasjonal sikkerhetsmyndighet (NSM), Risiko 2025, regnes løsepengeangrep som den største utfordringen for norske bedrifter. Selv om andre typer angrep faktisk kan være gunstigere for de som står bak, forårsaker løsepengeangrep vanligvis større skade, siden de kan lamme hele virksomheten.

Når vi ser nærmere på tallene, viser det seg at mange norske IT-beslutningstakere som enten har en beredskapsplan for cyberangrep eller vurderer å revidere den, også har opplevd et alvorlig angrep det siste året. Blant disse er andelen som har vært utsatt for angrep 19 prosent, som er betydelig høyere enn gjennomsnittet på 11 prosent blant alle norske respondenter.

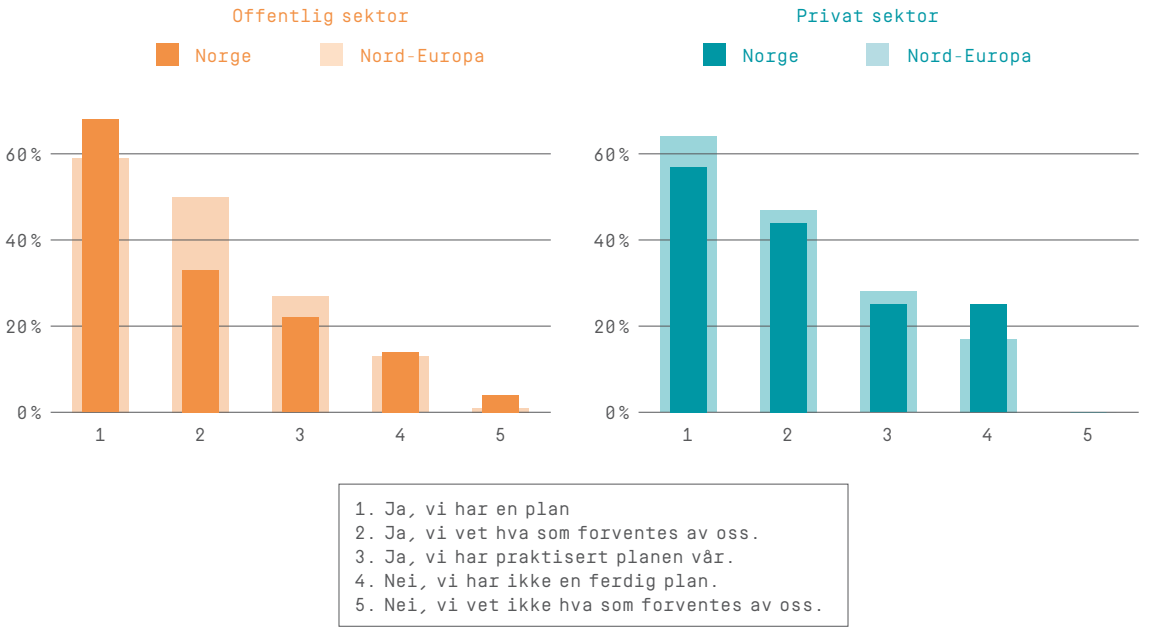
Sikkerheten blir stadig bedre, men det er en konstant dragkamp mellom det gode og det onde. Teknologiske fremskritt er én ting, men det er ofte den menneskelige faktoren som gjør at cyberangrep lykkes. Dette understreker viktigheten av å ikke bare ha en beredskapsplan, men å øve på den (se side 25).

De fleste norske respondentene understreker viktigheten av øving, systematisering og dokumentasjon. Noen fremhever behovet for å gjennomgå eksisterende planer og tilpasse dem til dagens trusler. Noen få IT-beslutningstakere peker på bruk av IT-leverandører som et middel for å oppnå bedre beredskap. Det er også tegn som tyder på at noen av respondentene er usikre på om de har gjort det som er nødvendig for å være forberedt på et angrep.

UTVIKLE MOTSTANDSDYKTIGHET OG MOTSTÅ TRUSLER

Flere beredskapsplaner, men lite øving

Har dere en plan for å håndtere uforutsette hendelser (f.eks. cyberangrep), og vet dere hva som forventes av dere?



1. Ja, vi har en plan
2. Ja, vi vet hva som forventes av oss.
3. Ja, vi har praktisert planen vår.
4. Nei, vi har ikke en ferdig plan.
5. Nei, vi vet ikke hva som forventes av oss.

Flervalgsspørsmål

Sammenlignet med fjorårets internasjonale rapport, har andelen virksomheter som har en plan for håndtering av uforutsette hendelser, økt fra 55 til 62 prosent i Nord-Europa. I Norge har imidlertid denne andelen gått ned fra 67 til 60 prosent, noe som betyr at Norge nå ligger under gjennomsnittet. Den største økningen har skjedd i Sverige, hvor andelen har steget fra 42 til 60 prosent.

Det samlede resultatet for de nordeuropeiske landene indikerer en endring i den generelle forståelsen av behovet for en beredskapsplan. Samtidig har bare 27 prosent øvd på planen sin. I Norge er tallet 24 prosent.

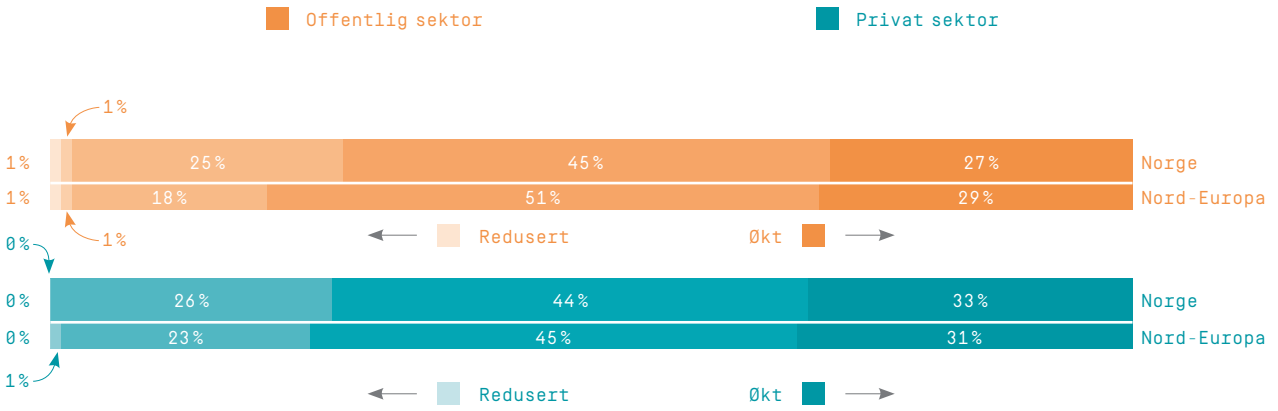
En beredskapsplan er ikke fullstendig før virksomheten har øvd på å gjennomføre den. Det er stor forskjell mellom å øve på planen innenfor IT-avdelingen, og å involvere bedriftsledelsen for å etablere en enhetlig motstandsdyktighet.

For å opprettholde, utvikle og teste virksomhetens evne til å håndtere en hendelse må vi øve, både internt i organisasjonen og i samarbeid med andre. Ved å øve er det også mulig å oppdage om planen har mangler som blir tydelige først ved gjennomføring.

UTVIKLE MOTSTANDSDYKTIGHET OG MOTSTÅ TRUSLER

Øker beredskapen mot cyberangrep

Har dere endret, eller planlegger dere å endre, beredskapen for cyberangrep?



Både offentlig og privat sektor i Norge og Nord-Europa har gjort endringer i beredskapen mot cyberangrep, eller planlegger å gjøre det. 78 prosent av IT-ledere i Nord-Europa har allerede oppdatert eller planlegger å oppdatere beredskapsplanene sine. Dette tyder på en sterk økning i beredskapen for nordeuropeiske virksomheter.

I offentlig sektor har 27 prosent i Norge og 29 prosent i Nord-Europa økt beredskapen for cyberangrep. Samtidig svarer nesten halvparten at beredskapen er uendret, og bare 1 prosent sier den er redusert. I privat sektor er bildet tydeligere: 33 prosent i Norge og 31 prosent i Nord-Europa har styrket beredskapen, og ingen har redusert den. Dette tyder på at private virksomheter er mer aktive i møte med økt cybertrussel, mens mange offentlige aktører fortsatt ikke har gjort endringer.

Til tross for dagens trusselbilde og økende antall cyberangrep, sier 22 prosent av nordeuropeiske IT-beslutningstakere at ikke har økt beredskapen, eller planlegger å gjøre det. Det siste er bemerkelsesverdig. At cyberangrep ikke oppfattes som like ødeleggende som andre organisatoriske kriser, kan kanskje forklares med virksomhetens modenhetsnivå.

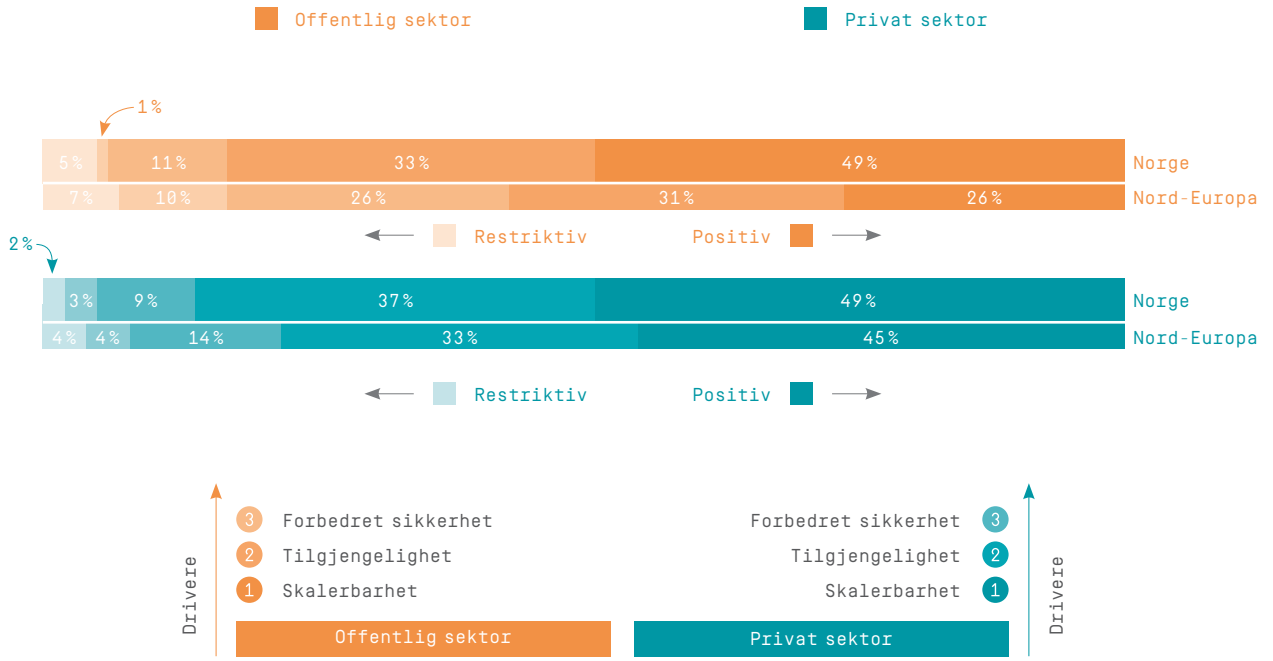
De fleste av disse virksomhetene har ennå ikke blitt angrepet selv. Virksomheter som har egen erfaring med cyberangrep, har ofte allerede en plan og er i ferd med å finjustere den. Hvis vi ser på alle landene under ett og sammenligner med fjorårets rapport, har det ikke vært nevneverdige endringer i hvordan virksomheter planlegger å tilpasse beredskapen til cyberangrep.

Mange virksomheter har planer for hvordan de skal håndtere ulike typer kriser, men IT-elementet mangler ofte. I tilfeller hvor det finnes planer, er øving nøkkelen til suksess (se side 25).

UTVIKLE MOTSTANDSDYKTIGHET OG MOTSTÅ TRUSLER

Flere virksomheter har en positiv holdning til offentlige skyløsninger

Hva er din virksomhets nåværende holdning til bruk av offentlige skyløsninger?



Holdningen til offentlige skyløsninger har utviklet seg i positiv retning, i både privat og offentlig sektor. I Norge er 85 prosent positive, noe som er betydelig høyere enn gjennomsnittet (69 prosent). Norske myndigheter har en klar strategi for skytjenester, og den oppmuntrer både offentlige og private virksomheter til å bruke offentlige skyløsninger. Norge legger stor vekt på innovasjon og produktivitet, særlig i tjenestesektoren, og er ledende innen digital transformasjon, med en 4. plass på OECDs Digital Government Index 2023. Pandemien satte også fart på omstillingen.

Uansett hvilket land vi sammenligner med, er holdningen til offentlige skyløsninger mer positiv i Norge. Forskjellen mellom høy positivitet og lav positivitet er 80 prosent, mot 53 prosent totalt. Skalerbarhet og forbedret sikkerhet er de to driverne for offentlige skyløsninger som øker mest, med totalt 20 prosent.

Juridisk usikkerhet som hindring for bruk av offentlige skyløsninger i Norge kommer på fjerdeplass for begge sektorer, og er med 23 prosent betydelig lavere enn gjennomsnittet på 53 prosent. For privat sektor synker dette tallet med 12 prosent sammenlignet med året før, til 20 prosent. For offentlig sektor er tallet 31 prosent. Til sammenligning ligger det hos gjennomsnittet på førsteplass med 70 prosent.

Norske myndigheter har fastsatt prinsipper for bruk av skytjenester i offentlig sektor, noe som bidrar til å redusere usikkerheten. I stedet ligger utfordringene hovedsakelig i å forutsi og styre kostnadene, siden regelverket stiller strenge krav om detaljerte kostnadsoversikter og åpenhet. Standardkontrakter med leverandører av skytjenester er ikke alltid tilpasset spesifikke behov og regelverk, noe som øker kompleksiteten. Videre kan investeringer i eksisterende datasentre og IT-infrastruktur også gjøre overgangen til offentlige skyløsninger vanskelig.

UTVIKLE MOTSTANDSDYKTIGHET OG MOTSTÅ TRUSLER

Når trusselbildet endres – slik ruster Vestlandet seg

I en tid med økende digitale trusler og et stadig mer krevende sikkerhetsbilde, trapper Vestland fylkeskommune opp innsatsen for å beskytte sine digitale verdier. – Vi har ikke råd til å være bakpå. Sikkerhet må være en del av hverdagen vår, og den må forankres i hele organisasjonen, sier John Arne Lillestøl, IT-direktør i Vestland fylkeskommune.

Økende trusler: Phishing og personvern

En av de største utfordringene fylkeskommunen står overfor i dag, er målrettede phishing-angrep og «man-in-the-middle»-angrep, som setter både data og brukere i fare.

– Vi ser en økende trend i e-poster som forsøker å lure ansatte til å gi fra seg sensitiv informasjon. Derfor vurderer vi løsninger som tester de ansattes årvåkenhet i slike situasjoner, sier Lillestøl.

Parallelt jobber fylkeskommunen systematisk med å sikre etterlevelse av personvernlovgivningen.

– Vi klassifiserer all programvare for å sikre at personopplysninger behandles forsvarlig. Dersom en løsning håndterer sensitiv data, skal den ha multifaktorautentisering og tydelige sikkerhetsrutiner, forklarer han.

Et sikkerhetsløft i hele organisasjonen

Vestland fylkeskommune består av 43 kommuner og har en av Norges mest omfattende IKT-organisasjoner, med nær 140 ansatte fordelt på 3 seksjoner.

Fylkeskommunen har ansvar for sentrale samfunnsoppgaver som videregående opplæring, kollektivtransport, fylkesveier, kultur og regional utvikling.

Nå setter de tydelig retning innen et område som berører alle: Digital sikkerhet. Fylkeskommunen har

John Arne Lillestøl, IT-direktør, Vestland fylkeskommune.

etablert en CISO-rolle og ansatt fire personer som jobber operativt med IKT-sikkerhet på fulltid.

– Dette er en tydelig prioritering fra vår side. Trusselbildet har endret seg, og vi må følge med i timen. Vi tar sikkerhet på alvor, understreker Lillestøl.

Sikkerhet som samfunnskritisk infrastruktur

Det handler ikke lenger bare om IT-drift og tekniske tiltak. I lys av krigen i Europa, økt geopolitisk spenning og et mer avansert trusselbilde, ser Lillestøl på sikkerhetsarbeid som samfunnskritisk.

– Sikkerhetsarbeid har fått en ny renessanse. IKT-sikkerhet er ikke lengre en teknisk støttefunksjon for organisasjonen – det er en samfunnskritisk infrastruktur, sier han.

Likevel mener han at det fortsatt mangler åpenhet i offentlig sektor

– Vi kunne nok hatt en bedre delingsstruktur rundt sikkerhetshendelser. Det er fortsatt slik at det ligger på den enkelte organisasjon å oppsøke informasjonen rundt slike hendelser. Når man tar kontakt i offentlig sektor, opplever vi god erfaringsutveksling rundt hendelser. Det er viktig at vi deler, enten direkte med hverandre eller via aktører som HelseCERT, forklarer Lillestøl.

HelseCERT er helse- og omsorgssektorens nasjonale cybersikkerhetssenter. De tilbyr sikkerhetstjenester via Nasjonalt beskyttelsesprogram og koordinerer ved sikkerhetshendelser.

Fellesskap på tvers av fylker

Vestland fylkeskommune står ikke alene i møte med de stadig økende truslene mot digital sikkerhet. Gjennom faglige samarbeidsgrupper og delingsarenaer, samarbeider fylkeskommunen tett med andre fylker i landet.

– Vi har etablert egne nettverk innen sikkerhet, drift og ledelse. Det gir stor verdi å kunne sparre med kollegaer i tilsvarende roller i andre fylker, forteller Lillestøl.

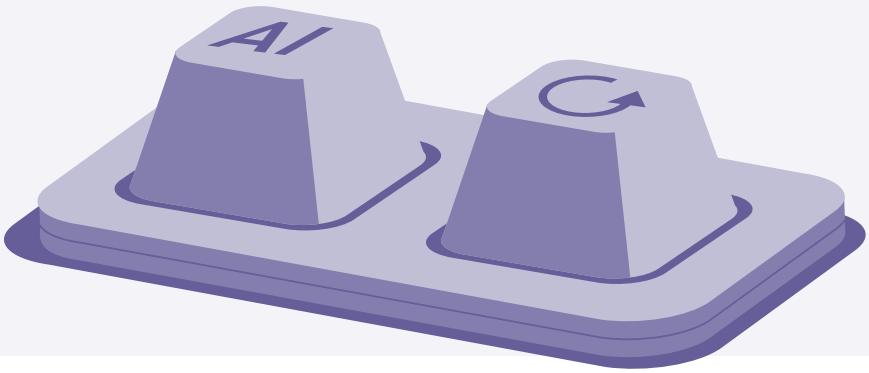
For å møte fremtidens krav, har fylkeskommunen satset målrettet på å bygge kapasitet og tydeliggjøre ansvar.

– Digitalisering og sikkerhet må utvikles parallelt. Og det gjør vi – i fellesskap, avslutter Lillestøl.

5

TEKNOLOGI OG TRANSFORMASJON FOR FREMTIDEN

Flere og flere virksomheter inntar AI-verdenen



ILLUSTRASJON: ISTOCKPHOTO

AI-utviklingen går i raskt tempo, og stadig flere IT-beslutningstakere i Nord-Europa sier at de bruker teknologien i driften og planlegger å bruke den enda mer. Dette kan tilføre organisasjonene stor verdi.

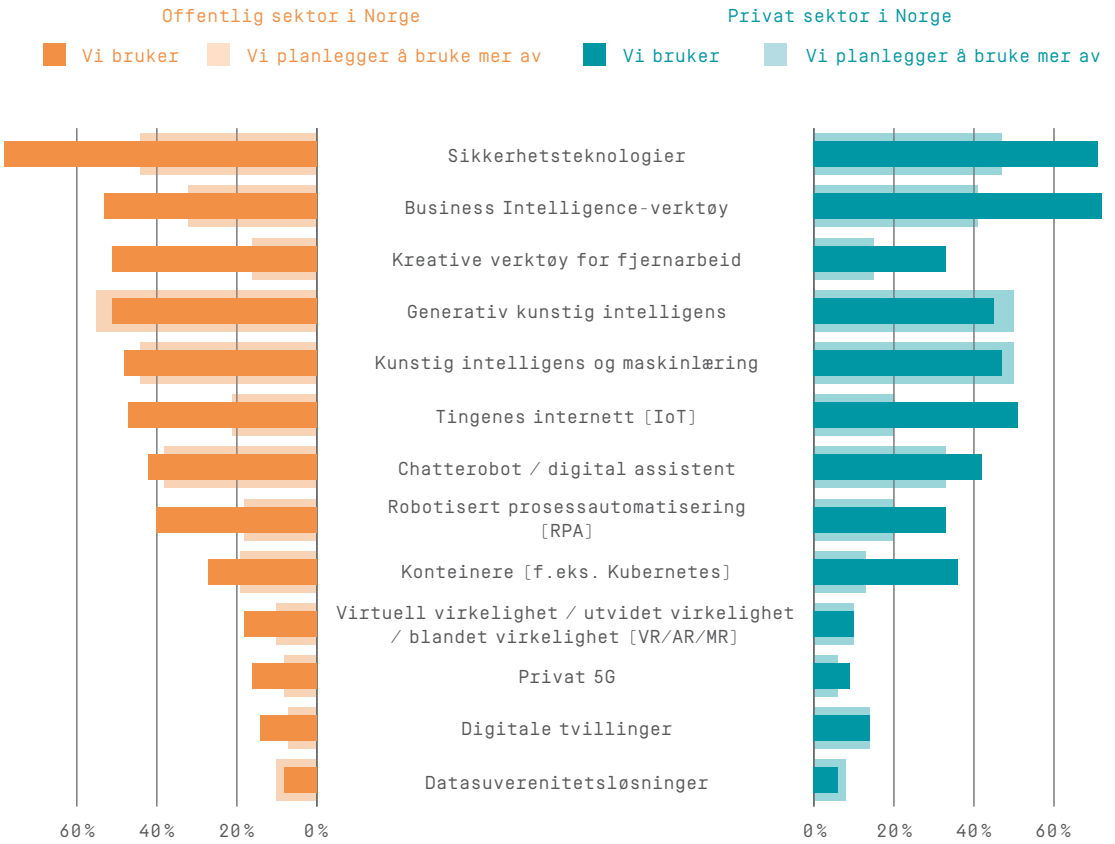
En virksomhets AI-utvikling deles vanligvis inn i fem nivåer: nybegynner, utforsker, utøver, profesjonell og skaper. Flere virksomheter ser på seg selv som utforskere og utøvere, mens færre regner seg som nybegynnere. Likevel er det få virksomheter som mener at de har skapt betydelig verdi ved hjelp av AI. Dette kan skyldes at mange hittil bare har implementert AI-verktøy som gjør arbeidet mer effektivt for den enkelte medarbeideren, men sjelden på organisasjonsnivå. Det er først i sistnevnte tilfelle at investeringene virkelig begynner å gi avkastning. Dette kan tyde på at mange virksomheter ikke har klart å integrere AI i kjerneprosessene sine.

En mulig forklaring på hvorfor virksomheter anser seg selv som mer modne, kan være en mer strukturert tilnærming til å tilrettelegge for at sluttbrukere kan benytte generative AI-løsninger i sitt daglige arbeid. Å fokusere på gevinster på individnivå, men ikke være i stand til å integrere AI i forretningsprosessene mer generelt, sier noe om virksomheters AI-modenhet. Generativ AI er ikke det eneste som finnes. Også andre typer AI-teknologi, som har vært tilgjengelige i mange år, har et stort potensial.

TEKNOLOGI OG TRANSFORMASJON FOR FREMTIDEN

Implementeringen av generativ AI er nesten doblet – og forventes å øke ytterligere

Teknologier vi bruker i produksjonen og planlegger å bruke mer av i løpet av de neste tre årene:



Flervalgsspørsmål

Det har vært mye offentlig debatt om AI-agenter og hvordan de vil revolusjonere måten vi jobber på. Denne dynamiske programvaren utfører datavitenskapelige oppgaver autonomt og samhandler med omgivelsene. Det skiller den fra tradisjonelle automatiseringsverktøy, som følger forhåndsdefinerte regler. Det antas at AI-agenter vil sette fart på bruken av AI, siden de forventes å gi god avkastning på investeringen (ROI) i form av høy automatisering. Gode resultater med generativ AI kan også bidra til å styrke andre AI-områder, for eksempel maskinlæring og prosessering av naturlig språk (Natural Language Processing, NLP).

Den økende interessen for generativ AI er tydelig. I 2024 oppga 28 prosent av IT-beslutningstakerne i Nord-Europa at de hadde implementert generativ AI i virksomheten sin. I år er det tilsvarende tallet 45 prosent. 56 prosent planlegger også å bruke det mer, og like mange har tenkt å investere mer i andre AI-teknologier og maskinlæring. Dette betyr at disse teknologiene står øverst

ILLUSTRASJON: ISTOCKPHOTO

på listen over teknologier som IT-beslutningstakere planlegger å bruke mer av, tett fulgt av sikkerhetsteknologi (53 prosent). Innføringen av AI er mer omfattende i virksomheter som anser seg selv som proaktive når det gjelder å møte virksomhetens behov (se side 13). Imidlertid er det bare en liten andel som sier at de har skapt betydelig verdi med AI (se side 33).

Sikkerhetsteknologi brukes i stor grad i både privat og offentlig sektor, henholdsvis 71 og 78 prosent i Norge. I offentlig sektor er dette det klart mest valgte svaret.

Forretningsanalyse (Business Intelligence, BI) er et vanligere verktøy i privat sektor enn i offentlig sektor: 77 prosent sammenlignet med 58 prosent i Nord-Europa. Forskjellen er tydelig også i Norge, hvor de tilsvarende tallene er 72 og 53 prosent. Det er flere forklaringer på dette. BI er et sett med tekniske prosesser som samler inn og analyserer forretningsdata for å støtte datadrevne beslutninger, og norske bedrifter er opptatt av å dra nytte av data i beslutningstaking. Disse løsningene kan tilføre organisasjonen stor verdi.

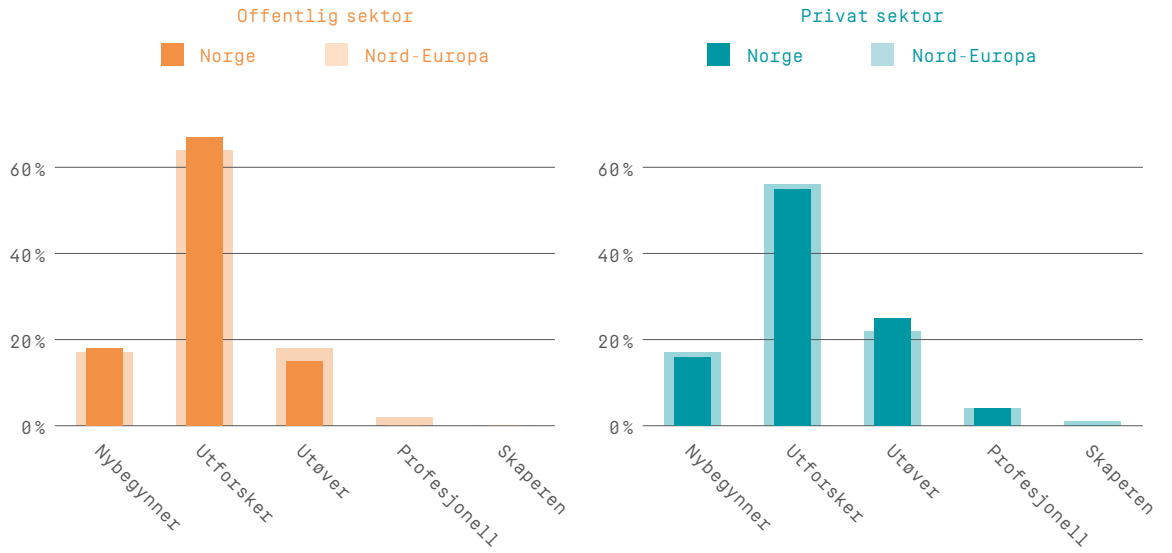
Større interesse for BI-plattformer kan knyttes til den økende interessen for generative AI-løsninger. Bruken av generativ AI har siden 2024 doblet seg i offentlig sektor i Norge: Antall virksomheter som bruker det, har økt fra 26 til 51 prosent. I privat sektor har det tilsvarende tallet økt fra 37 til 45 prosent. Alle virksomheter har generativ AI på agendaen. 2023 og 2024 var prøveårene. Bransjen signaliserer at denne bruken i 2025 og 2026 vil gi mange virksomheter avkastning på investeringen (ROI), særlig når fokuset flyttes mot AI-agenter.

Generelt sett har forretningskrav og forretningsverdi topp prioritet når det gjelder investeringer i ny teknologi. Kostnad og avkastning står også høyt på listen.

TEKNOLOGI OG TRANSFORMASJON FOR FREMTIDEN

Tydelig økning i AI-modenhet

Hvordan vurderer du virksomhetens AI-modenhet?



Flertallet (59 prosent) av nordeuropeiske IT-beslutningstakerne ser på seg selv som utforskere (ønsker å begynne med AI, første prototyper er bygd) når det gjelder AI. Samtidig er det klart at AI-modenheten har økt betydelig siden i fjor. 28 prosent anså seg selv som nybegynnere i 2024. Det tilsvarende tallet for i år er 17 prosent. Utforskere utgjorde 57 prosent i fjor, mens utøvere (AI-visjon og systematisk tilnærming påbegynt) har økt fra 12 til 20 prosent i Nord-Europa.

AI-modenheten er noe høyere i privat sektor, der 27 prosent mener at de har nådd utøver-nivå eller høyere (profesjonell eller skaper), sammenlignet med 20 prosent i offentlig sektor. I Norge er offentlig sektor fortsatt hovedsakelig i utforsker-fasen (67 prosent), mens 18 prosent er nybegynnere og 15 prosent er utøvere. Tilsvarende tall i privat sektor er 55, 16 og 25 prosent, men 4 prosent er også i profesjonell-fasen. Totalt er det 25 prosent av norske virksomheter som anser seg å være AI-modne.

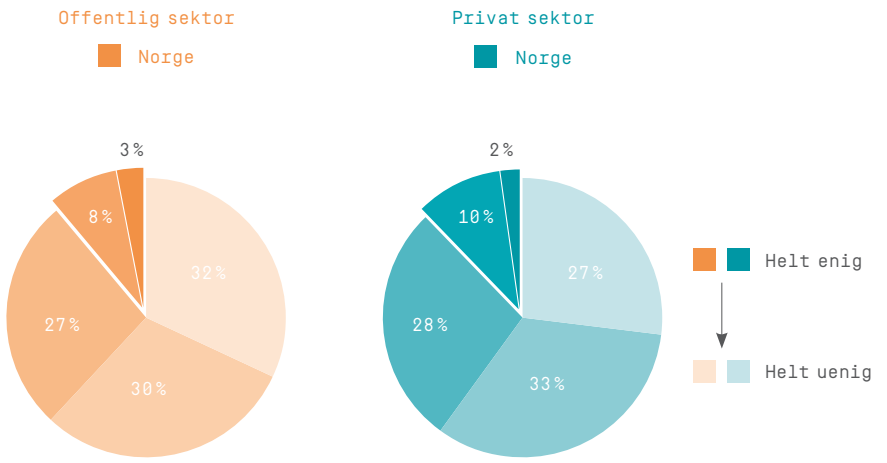
Norsk offentlig sektor ser på sikkerhetsbegrensninger som den største hindringen for AI (65 prosent), mens bare 37 prosent i privat sektor sier det samme når vi dykker ned i årsakene. Dette skyldes sannsynligvis at offentlige virksomheter håndterer mer sensitive personopplysninger, noe som medfører større juridiske begrensninger. Det er en betydelig utfordring å sikre at AI-systemer etterlever dette regelverket. I tillegg må AI-applikasjoner i offentlig sektor være åpne og kunne forklares for å opprettholde folks tillit. Dette kan begrense bruken av mer sofistikerte AI-modeller. Videre må offentlig sektor håndtere etiske spørsmål knyttet til AI, for eksempel fordommer og rettferdighet, noe som også stiller store krav til AI-systemer.

Hvis man vil utnytte AI fullt ut, er robust datahåndtering ikke bare viktig – det er grunnleggende. Likevel oppgir 55 prosent av offentlige virksomheter, og 44 prosent av private virksomheter i Norge fortsatt svak datainfrastruktur som en kritisk hindring. Privat sektor har en annen utfordring: mennesker. Nesten halvparten (47 prosent) av lederne sier at kompetanseheving hos sluttbrukere er den største hindringen for innføring av AI. Uten medarbeidere som er trygge på og dyktige til å bruke AI-verktøy, risikerer selv de mest avanserte systemene å bli underutnyttede investeringer. Konklusjonen er klar: For å lykkes med AI trenger man mer enn banebrytende teknologi – vi trenger strategisk samordning av data, verktøy og kompetanse.

TEKNOLOGI OG TRANSFORMASJON FOR FREMTIDEN

Få utnytter AI effektivt

Virksomheten min har skapt betydelig verdi med AI



Selv om 59 prosent av IT-beslutningstakerne i Nord-Europa ser på seg selv som utforskere innen AI, er det færre som anser seg som nybegynnere og flere som utøvere (se side 32). Få mener at de har skapt betydelig verdi med AI så langt. Bare 13 prosent svarte «enig» eller «helt enig» på dette spørsmålet, og enda færre i Norge: Kun 11 prosent totalt. 29 prosent av alle respondentene er helt uenige i at AI har skapt betydelig verdi.

På mange måter er dette et forventet resultat når så mange virksomheter befinner seg på de tidlige stadiene av AI-modenhet. Hjelpemidler til innholdsproduksjon, interne chatteroboter og lignende verktøy er nyttige, men gir ikke nødvendigvis store forretningsmessige fordeler. Over tid flytter fokuset seg gjerne til andre, mer verdiskapende prosesser på organisasjonsnivå. Betydelig avkastning på investeringen (ROI) kan man bare forvente når AI er integrert i virksomhetens kjerneprosesser, støtter reaktiv og prediktiv beslutningstaking, og skaper nye produkter og tjenester basert på tilgjengelige data. Den forventede utviklingen med AI-agenter vil være et stort skritt i den retningen. I Norge sier 35 prosent at de bruker AI til prosessautomatisering, noe som kan tilføre virksomhetene stor verdi.

Generelt sett ser det ut til at mange virksomheter ikke har klart å integrere AI i kjerneprosessene sine. Generativ AI er kanskje den nyeste og mest omtalte teknologien, men det finnes et stort uutnyttet potensial i andre AI-teknologier som har vært tilgjengelige i flere år. Respondenter som mener at de har oppnådd betydelige eller svært betydelige fordeler av AI, har også mye større sannsynlighet enn andre for å ha brukt AI til kundeservice og prosessautomatisering.

TEKNOLOGI OG TRANSFORMASJON FOR FREMTIDEN

Navigasjon møter intelligens

I skipsfarten er det ikke lenger bare kompass og kart som gjelder - det er algoritmer, sanntidsdata og kunstig intelligens som setter kursen for NAVTOR, teknologiselskapet med base i Egersund.

NAVTOR utvikler digitale løsninger for den globale shipping-industrien, som benyttes på over 18 000 skip verden over. Selskapet har etablert seg som en nøkkelaktør innen shipping. Målet er klart: Å gjøre navigasjon smartere, beslutningene bedre og driften mer effektiv – gjennom AI.

AI i drift – allerede i dag

– Vi bruker AI til å optimalisere ruter og forutsi vedlikeholdsbehov. Det gir bedre beslutninger, reduserer risiko og sparer verdifull tid, sier CTO Anders Holme.

AI er ikke lenger noe man eksperimenterer med, hos NAVTOR er det i operativ drift. Et godt eksempel er skipstrafikkovervåkningen, som kontinuerlig analyserer store mengder data og gir operatørene konkret beslutningsstøtte i valg av ruter. Systemet lærer over tid og foreslår blant annet den mest effektive ruten basert på en kombinasjon av maskin læring, validert maritim informasjon og menneskelig erfaring.

Resultatet? Raskere beslutninger, færre avvik og økt kontroll for rederiene.

Digitale tvillinger gir full innsikt

AI brukes også til å utvikle digitale tvillinger av skipene, virtuelle

Anders Holme, Chief Technology Officer, NAVTOR.

modeller av skip som lar operatørene simulere ulike driftsforhold. Når disse modellene kobles med AI, oppstår helt nye muligheter:

– Gjennom disse modellene kan man forutsi drivstofforbruk og CO_2-utslipp under ulike værforhold, og dermed ta smartere valg i ruteplanleggingen. Disse simuleringene gjør det mulig å optimalisere operasjoner, redusere slitasje og agere proaktivt – lenge før problemer oppstår, forteller Holme.

NAVTOR har satt seg et ambisiøst mål om å redusere CO_2-utslippene fra shipping med opp til 20 prosent, et mål som, ifølge Holme, er fullt mulig å nå med dagens teknologi.

– Vi tror teknologi og bærekraft er knyttet sammen. Våre systemer gir rederiene oversikt over CO_2-utslipp og drivstoffbruk i sanntid. Det er ikke bare miljøvennlig – det er også god business, forteller Holme.

AI som digitalt forsvar

AI er også en sentral del av NAVTORs arbeid med cybersikkerhet. Systemene som styrer skip er sårbare for digitale trusler, og her er AI en viktig del av forsvaret.

– Vi bruker AI til å overvåke uvanlig aktivitet og varsle om potensielle trusler i sanntid. Det handler om å beskytte både data og drift, sier Holme.

Med stadig mer avanserte systemer om bord, er sikkerhet en forutsetning for digitalisering - og her er AI et verktøy med stort potensial.

Fremtidens shipping er allerede i gang

Med et sterkt fokus på AI, digital transformasjon og bærekraft, er NAVTOR godt posisjonert for å lede an i fremtidens skipsfart. Teknologien som utvikles i Egersund setter en ny standard for hvordan shipping-næringen kan møte de store utfordringene innenfor både effektivitet og miljøpåvirkning.

– Vi utvikler teknologi som gir kundene våre enklere og smartere løsninger for å møte fremtidens utfordringer og bærekraftsmål. Dette er essensen av moderne shipping, avslutter Holme.

ILLUSTRASJON: ISTOCKPHOTO

Fremtiden er i våre hender

En av de viktigste oppgavene for IT-beslutningstakere er å sørge for at veikartet er tydelig utformet og godt kommunisert. Selv om IT må ta ledelsen, er det ingen som vil lykkes alene.

Alle i organisasjonen må forstå hvor dere skal og hvorfor. Ansvarsområder må være tydelig definert, og alle må være enige om prioriteringene. Strategier må omfatte både forretningsprosesser og mennesker. Det ene fungerer ikke uten det andre. Innsats må rettes mot god kommunikasjon, og det vil være nødvendig å investere i kompetanseutvikling. IT-beslutningstakere må sørge for at alle har kompetansen og ressursene som trengs for å bidra på veien videre.

Den digitale transformasjonen må følge veikartet, men også være tilpasningsdyktig overfor globale hendelser og uforutsette svingninger. IT-avdelinger må fungere både som støttefunksjon og ledestjerne, og oversette mål og visjoner til kostnadseffektive verktøy og teknologiske løsninger.

Sikkerhet vil fortsatt være avgjørende når vi navigerer gjennom innføringen av ny teknologi, robuste rammeverk og et raskt skiftende politisk klima. Dette krever at virksomheter både øker den generelle sikkerhetsforståelsen, og blir bedre til å dele kunnskap internt.

Vi må sette prosesser og mennesker i sentrum.
Til slutt må vi fortsette å lære av både fortid og nåtid. Denne rapporten er ett av flere verktøy for å lære og utvikle oss videre. Ved å dele erfaringer og bygge videre på det vi vet, kan vi sammen skape bedre løsninger for fremtiden.

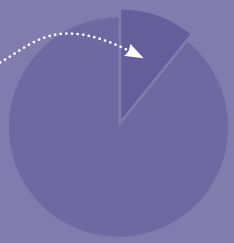
Har du spørsmål om rapporten? Ta kontakt på contact@cioanalytics.com

55 %
handler ikke proaktivt for å møte virksomhetens behov

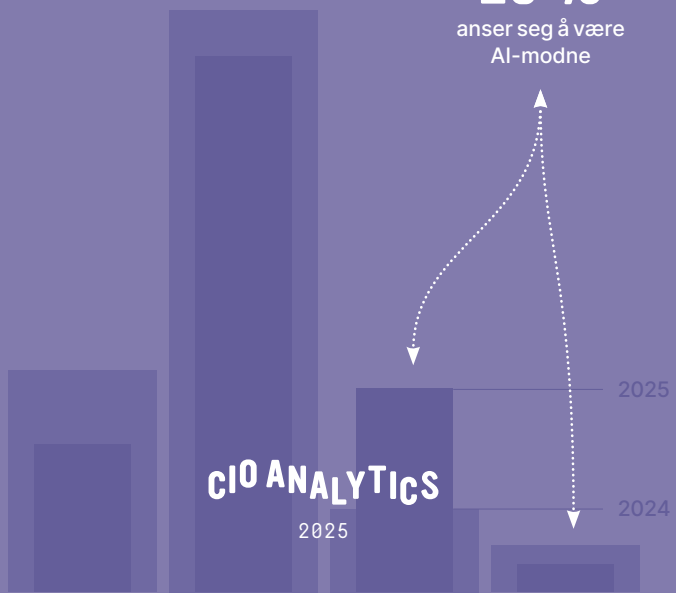
68 %
vil øke sitt forbruk på sikkerhet

Nr. 1
Den største hindringen for AI er datahåndtering

Kun
11 %
har skapt betydelig verdi med AI



25 %
anser seg å være AI-modne



CIO ANALYTICS
2025