HVORDAN SKAPER NORSKE BEDRIFTER BEVISSTHET RUNDT CYBERSIKKERHET

Ivar Mykkeltvedt

Masteroppgave- informasjonsvitenskap

Institutt for informasjons- og medievitenskap

Universitetet i Bergen

Våren 2024

Forord

Jeg vil takke alle de norske bedriftene som sa ja til å bli med i studien min. Dere ga meg et interessant innblikk og delte mye spennende kunnskap. Håper virkelig at studien kan være til nytte for dere. Veilederen min, Andreas Lothe Opdahl, vil jeg også takke for god hjelp og veiledning gjennom alle møtene våre. Videre har samboer og hele familien min støttet meg i år etter år med studier, noe jeg setter veldig pris på.

Ivar Mykkeltvedt

Sammendrag

Den økende digitaliseringen i samfunnet gjør at norske bedrifter opplever daglige cyberangrep. Bedriftsledere frykter dem mer enn noen gang på grunn av skaden de kan påføre og hyppigheten av dem. De fleste vellykkede angrepene i dag skyldes menneskelige feil. Derfor har bevissthet rundt dette temaet aldri vært viktigere. Det er alltid et behov for tiltak som skal bidra til å bedre bevisstheten i bedrifter. Antallet og hvilke tiltak som blir prioritert, varierer fra bedrift til bedrift. Grunnen til dette kan være ulike faktorer. Alt fra størrelse til bransje. Formålet med min studie var å se nærmere på tiltakene norske bedrifter bruker for å bevare og øke bevisstheten innad. Forskningsspørsmålet mitt var: *Hvordan skaper norske bedrifter bevissthet rundt cybersikkerhet?*

Studien er bygget på 16 kvalitative intervjuer med norske bedrifter av ulik størrelse og fra flere ulike bransjer. I tillegg til sammenligning av svarene fra alle bedriftene samlet, ble intervjuene tematisk analysert og sammenlignet basert på bedriftsstørrelse, offentlige/private bedrifter og bedrifter med nulltoleranse for cybersikkerhetsbrudd. Det var 12 hovedspørsmål i intervjuguiden min, 10 av dem fra en annen studie av engelske bedrifter, og de 2 siste fra en studie av jordanske bedrifter. Dette ga et ideelt grunnlag for også å sammenligne de norske bedriftene som ble intervjuet med flere utenlandske bedrifter.

Resultatene viser at intervjuobjektene som bemerket sin begrensede kunnskap, var ofte de som uttrykte størst tilfredshet med sikkerhetsarbeidet og viste minst bekymring for potensielle angrep. Nesten alle de norske selskapene tilbyr en form for kurs eller opplæring. I motsetning til mesteparten av de engelske bedriftene. Flere av kursene til de norske selskapene er derimot frivillig eller bare obligatorisk for deler av selskapet. Dermed var det en stor andel ansatte i bedriftene som ikke gjennomførte dem. En del selskaper hadde ubegrenset tilgang på nettet for ansatte. Stort sett hørtes det ut som de stolte på de ansattes vurderinger. Dette er motstridende for flere av dem, på grunn av et betydelig antall av dem svarer også at bevisstheten i bedriften er middels til under middels. En rekke små og private bedrifter virker å stole blindt på leverandør, noen av dem hørtes ikke ut til å skjønne helt hva som ble gjort for dem. Studien indikerer at norske bedrifter generelt sett har implementert flere tiltak for å skape bevissthet rundt cybersikkerhet. Likevel er det fortsatt områder som kan forbedres, med varierende behov basert på typen bedrift det er snakk om.

Innholdsfortegnelse

Tabelloversikt

Figuroversikt

Begreper

Kildekode angrep: Angripere kan teste stjålet kildekode og lage angrepsscenarier ved bruk av malware som utnytter svakheter i koden. De kan injisere malware, som bakdører, dette kan gi skjulte uautoriserte fjernadganger. De kan også plassere andre sårbarheter inn i koden uten å bli oppdaget (Geer, 2024).

Samfunnskritiske bedrifter: Samfunnskritiske bedrifter har de anleggene og systemene som er nødvendige for å opprettholde samfunnets kritiske funksjoner (Kunnskapsdepartementet, u.å.)

Hacktivisme: Hacktivisme representerer et dynamisk krysningspunkt mellom teknologi og aktivisme, der enkeltpersoner eller grupper bruker digitale verktøy for å fremme sosiale eller politiske årsaker (Gawel, 2024).

Phishing: Phishing er en form for sosial manipulering hvor en angriper forsøker å lure noen til å utføre en handling. For eksempel åpne et e-postvedlegg, klikke på en lenke eller betale en falsk regning (Datatilsynet, 2020).

Ransomeware: Ransomware er et virus som lammer digitale systemer ved å kryptere filer. Deretter krever trusselaktøren løsepenger for å låse opp krypteringen (Estil, 2024). Blir forkortet av flere intervjuobjekter og meg i denne studien til kryptering. Ordet kryptering kan også brukes til å beskrive andre typer dataangrep.

Sikkerhetspolicy: En sikkerhetspolicy skal beskrive for både ansatte, ledelse og partnere hvordan virksomheten definerer informasjonssikkerhet, og hvordan de håndterer informasjonssikkerhet (FenceNordic, u.å.). Dette handler om hvilke prinsipper sikkerheten bygges på, hvem som er ansvarlig for de forskjellige elementene, og hvordan virksomheten operativt skal jobbe med og håndheve sikkerhetsarbeidet (FenceNordic, u.å.).

Cybersikkerhet bevissthet: Bevissthet rundt cybersikkerhet innebærer å være oppmerksom på cybersikkerhet i daglige situasjoner. Å være klar over farene ved å surfe på nettet, sjekke e-post og samhandle på nettet er alle komponenter av bevissthet rundt cybersikkerhet (Koziol & Bottorff, 2022).

Malware: Malware er en variasjon av påtrengende og/ eller skadelige programvarer (Ray & Nath, 2016)

1 Introduksjon

1.1 Bakgrunn

I dag blir norske bedrifter stadig mer digitalisert, dette gjelder alle sektorer og industrier. Den gjør hverdagen mer effektiv for bedriftene, men åpner også dørene for flere nye måter å skade dem på. I 2019 satt den norske regjeringen et strategisk mål som handlet om at norske selskaper skulle digitalisere seg på en sikker og tillitsvekkende måte (Norwegian Ministeries, 2019). De skulle være i stand til å beskytte seg mot cyberhendelser (Norwegian Ministeries, 2019). NSM melder om en økning i antall forsøk på å kompromittere norske virksomheter. Cyberangrep har rett og slett blitt hverdagskost (NSM, 2022). "Et bredt spekter av trusselaktører utnytter ulike menneskelige, teknologiske og organisatoriske sårbarheter med mål om å ramme digitale verdiers konfidensialitet, integritet og tilgjengelighet" (NSM, 2023).

Et vellykket cyberangrep vil potensielt kunne ramme et selskap, både økonomisk og operasjonelt, så hardt at det i verste fall kan stå om nedleggelse. Et selskaps ansatte utgjør i dette scenarioet en stor angrepsflate. Sikkerhetsbevissthet blant de ansatte er derfor et viktig grunnlag for sikkerheten i enhver organisasjon for å unngå skadelige brudd (Dahbur et al. , 2017). Nesten alle har hørt om cybersikkerhet, men verken holdningene eller folks oppførsel reflekterer et høyt bevissthetsnivå (Bruijn & Janssen, 2017). Hele 85% av datainnbrudd er forårsaket av sosial manipulering eller menneskelig feil, et bevis på at organisasjoner ikke har råd til å forsømme betydningen av den menneskelige siden av cybersikkerhet (KnowBe4, 2022). Bevissthet rundt cybersikkerhet er derfor blitt ekstremt viktig for dagens bedrifter. Jeg har derfor gjort en kvalitativ studie av norske bedrifter og hvordan de skaper bevissthet rundt cybersikkerhet.

1.2 Studie og forskningsspørsmål

Begrepene cybersikkerhet og informasjonssikkerhet brukes ofte om hverandre (Solms &

Nierkerk, 2013). Ifølge artikkelen til Solms & Nierkerk (2013) går cybersikkerhet utover grensene til tradisjonell informasjonssikkerhet. Den omfatter ikke bare beskyttelse av informasjonsressurser, men også beskyttelse av andre aktiva, inkludert mennesker selv. I cybersikkerhet har den menneskelige faktoren en ekstra dimensjon, nemlig mennesker som potensielle mål for cyberangrep, eller til og med uvitende deltakere i et cyberangrep (Solms & Nierkerk, 2013). Dette er grunnen til at jeg har valgt å bruke begrepet "cybersikkerhet" istedenfor "informasjonssikkerhet" i studien min. Cyberangrep blir gjennomført mot alle typer bedrifter, av denne grunn har jeg intervjuet bedrifter av ulike størrelser og fra ulike bransjer. Dette for å få et større spenn av svar og mer å sammenligne.

Bevissthet rundt cybersikkerhet handler om mer enn bare kunnskap og forståelse. Det handler også om investeringer og villighet til å skape en cybersikkerhetskultur. Det forstås i økende grad at cybersikkerhet må håndteres gjennom organisatoriske tiltak og ikke bare gjennom tekniske tiltak alene (Reegård et al., 2019). Undersøkelsen min omhandler nettopp selskapenes organisatoriske tiltak og unngår detaljerte tekniske aspekter. Bedriftenes tiltak kan variere basert på ulike faktorer. Det kan være størrelse, om de er private eller offentlige, eller om de har nulltoleranse for vellykkede angrep. Dette er også faktorer jeg skal sammenligne i studien min. Jeg har valgt å plassere egne diskusjonsdeler under hvert resultat. Med mål om å oppnå bedre struktur og flyt i teksten min. Jeg har brukt spørsmål fra tidligere studier av engelske og jordanske selskaper (Erdogan et al., 2023; Dahbur et al., 2017) for å legge til et sammenligningsgrunnlag med utenlandske bedrifter. Den tematiske analysen av resultatene fra intervjuene vil fremheve tiltakene og tankene til ulike typer norske selskaper. Det finnes en datakatalog med alle intervjuene. Hvordan ser de på bedriftens egen bevissthet rundt cybersikkerhet? Hva gjør de for å øke og bevare den? Hvordan blir bevisstheten omtalt i forhold til tiltakene? Dette er spørsmål som fanger essensen i oppgaven min, og går under det litt bredere forskningsspørsmålet mitt:

Hvordan skaper norske bedrifter bevissthet rundt cybersikkerhet?

ChatGPT og Gemini har blitt brukt som skrivehjelp i oppgaven angående formuleringer og oversetting.

2 Teori

2.1 Hovedlitteratur

2.1.1 Engelske studier

Den engelske studien med tittelen "Cybersecurity Awareness and Capacities of SMEs" får 141 små og middels store engelske bedrifter til å gjennomføre en survey, for å bedre forstå nivået av cybersikkerhetsbevissthet, og praksis de bruker for å beskytte mot ulike cyberrisikoer (Erdogan et al., 2023). Studien er publisert av SINTEF (Stiftelsen for industriell og teknisk forskning) som er den største uavhengige forskningsorganisasjonen i Skandinavia (SINTEF, 2012). I studien har de bare tatt med bedrifter som har 250 eller færre ansatte i undersøkelsen sin, noe som er forskjellig fra min studie hvor jeg intervjuet bedrifter av alle størrelser. Det gir fortsatt et stort sammenligningsgrunnlag for flere av bedriftene i min undersøkelse. Deres kvantitative undersøkelse inneholder 27 spørsmål. Tretten av spørsmålene var spesifikt relatert til bevissthet rundt cybersikkerhet og cybersikkerhet praksiser (Erdogan et al., 2023). Jeg har brukt 10 av spørsmålene fra disse kategoriene som jeg mener var optimale i forhold til min undersøkelse.

De 10 spørsmålene jeg bruker fra studien er:

Tilbyr din bedrift kurs eller opplæringsmateriell til ansatte for å øke bevisstheten rundt cybersikkerhet?

Dette er et svært relevant spørsmål for å vurdere hvordan bedriftene trener ansattes forståelse av cybersikkerhet. Det er imidlertid ikke nok å bare se om bedriftene tilbyr opplæring til sine ansatte. Jeg vil også vite om det blir brukt til å måle deres forståelse. Dette er et grunnleggende tiltak for å skape bevissthet rundt cybersikkerhet i en bedrift. Derfor er det også nødvendig å spørre om.

Har din bedrift stillinger dedikert til cybersikkerhet?

Nivået av ekspertise rundt cybersikkerhet i bedriftene er interessant å vite. Blir det brukt ressurser på dette, eller er det et tiltak flere unngår. En leder for området kan selvfølgelig være med på å understreke at bedriften tar cybersikkerhet på alvor. Noen som igjen vil skape et mer bevisst arbeidsmiljø og en sterkere sikkerhetskultur.

Har dere faste møter angående cybersikkerhet?
Møter om cybersikkerhet skaper engasjement og gir mulighet for koordinering av innsats. Dette spørsmålet er sentralt for å høre om bedrifter bruker møter for å skape mer bevissthet. Det gir kontinuerlige oppdateringer angående cybertrusler for de ansatte. De ansatte får en god mulighet til å tilpasse seg relevante trusler.

Hvordan vil du karakterisere din egen kunnskap om cybersikkerhet?
Fra dette spørsmålet får jeg en innsikt i hvor bevisste og informerte intervjuobjektene er rundt cybersikkerhet. Det er nødvendig å vite hvor mye kunnskap de har om temaet med tanke på svarene jeg får fra dem. Kunnskap kan påvirke hvordan de ser på egne tiltak og bedriftens generelle bevissthet.

I hvilken grad frykter du for et cyberangrep mot din bedrift?
Deres oppfatning av risikoene de står ovenfor er avgjørende å forstå. Høy grad av frykt kan bety et sterkt fokus på å beskytte mot trusler, mens lav bekymring kan indikere det motsatte. Dette er elementer jeg vil utforske mer.

Hvordan vil du karakterisere din bedrift når det kommer til cybersikkerhet bevissthet?

Dette er kanskje det mest sentrale spørsmålet. Her vil jeg se på svaret i forhold til tiltakene deres. Noen bedrifter oppfatter kanskje bevisstheten som høy, men det er ingen tiltak eller målinger for å underbygge svaret. Det kan også gi en indikasjon på hvor effektive tiltakene deres er. Sammenligninger av svarene på dette spørsmålet, kan identifisere praksiser bedriftene mener fungerer godt for å skape og øke bevisstheten.

Hvor lenge tror du at deres kritiske applikasjoner og systemer kan være nede før det får betydelige konsekvenser for selskapet?
Dette er interessant i forhold til hvilke tiltak som blir gjort i henhold til tålelig nedetid. De mest utsatte bruker fort mer ressurser, og har mer avansert beredskapsplanlegging. Er bevisstheten høyere blant ansatte i et selskap som ikke tåler nedetid? Det primære blir å se på om tiltakene samsvarer med konsekvensene av et vellykket angrep på bedriften.

Bruker din bedrift spesifikke prosesser eller verktøy for å identifisere cybersikkerhet

sårbarheter?
Det er interessant å vurdere om bedriften aktivt jobber med å identifisere og håndtere sårbarheter i sine systemer, noe som er essensielt for å forhindre cyberangrep. Bedrifter med gjennomførte etablerte prosesser og verktøy er sannsynligvis bedre rustet til å oppdage og tette sikkerhetshull. Dette gjelder både for sårbarheter i det tekniske og for sårbarheter som åpner seg via ansatte.

Har det vært noen tidligere cyberangrep på din bedrift som du kan nevne?
Jeg vil vite mer om bedriftenes erfaringer og hvordan tiltakene ser ut basert på de. Kanskje noen har opplevd angrep, og av den grunn er mer opptatt av bevisstheten innad i selskapet. Jeg vil høre hvilke angrepsflater som ble utnyttet for å skade bedriften. Det er også interessant å vite hva de eventuelt har lært og hvilke mottrekk de har implementert for å hindre at det skjer igjen.

Hva var virkningen av det eventuelle angrepet(ene)?
Dette spørsmålet gjør at jeg forstår omfanget av de eventuelle angrepene. Jeg får også en forståelse rundt hvilke angrep de har blitt utsatt for og hva som sviktet. Angrepene har trolig gjort bedriften mer bevisst på denne type angrep og derfor tettet relaterte hull.

2.1.2 Jordanske studier

Den jordanske studien har sendt ut en undersøkelse med 31 spørsmål til 504 bedriftsansatte i landet. Forskningen tar sikte på å vurdere nivåene av følgende sårbarheter: fysisk sikkerhet, programvaresikkerhet, sosial manipulering og phishing. Målet med denne forskningen er å fastslå tilgjengeligheten, nivået av sikkerhetsopplæring og sikkerhetspolicyer (Dahbur et al., 2017). De har utformet et spørreskjema angående informasjonssikkerhetsspørsmål, scenarier og tiltak (Dahbur et al., 2017). Spørreskjemaet ble distribuert til flere bedrifter i Amman. Bedrifter som dekker flere sektorer (Dahbur et al., 2017), ikke ulikt min studie. Den primære hensikten med forskningen deres var å studere nivået av sikkerhetsbevissthet blant ansatte i disse organisasjonene (Dahbur et al., 2017). Ifølge Dahbur et al. (2017) er det fire hovedpunkter for sikkerhetsbevissthet i bedrifter. Dette er mennesker, teknologi, prosesser/ prosedyrer og retningslinjer. Disse punktene vil naturligvis komme opp via svarene til intervjuobjektene mine, på grunn av innholdet i intervjuguiden min. De hadde kategorisert spørsmålene etter hva de

handlet om. Kategoriene var følgende: fysisk sikkerhet, sikkerhets trening, retningslinjer for sikkerhet, programvaresikkerhet, sosial manipulasjon, bevissthet og phishing.

Spørsmålene jeg bruker fra denne studien er satt opp som avkryssing. De ansatte må krysse av for det som gjelder for dem, basert på alternativene. Jeg brukte disse to spørsmålene i mine intervjuer:

Kan de ansatte i bedriften surfe fritt på nettet eller er det begrenset hvilke sider de har tilgang til?
Dette spørsmålet gikk under målingen av kategoriene programvaresikkerhet, retningslinjer for sikkerhet og bevissthet. Det er et viktig tiltak med tanke på de ansattes bevissthet. Ingen begrensninger gjør at bedriften er enda mer avhengig av bevisstheten til de ansatte. Retningslinjer og praksiser som dette kan øke ansattes bevissthet rundt sikker nettbruk. Jeg mener spørsmålet kan gi et bilde på sikkerhetskulturen innad i bedriftene.

Har folk generelt begrenset tilgang til bedriftens kontorbygg?
Dette spørsmålet gikk under målingen av kategoriene fysisk sikkerhet og bevissthet. Passende tilgangskontroll er nødvendig for å hindre uvedkommende adgang til sensitive områder. Et sikkerhetsbevisst selskap vil alltid ha tiltak rundt den fysiske adgangen til kontorbyggene sine. Spørsmålet gir meg sjansen til å se nærmere på nivået av den fysiske sikkerheten og hva de tenker om den.

2.2 Modenhetsmodeller

Modenhetsmodeller er en viktig del av studien min. Modenhetsmodeller kan bli brukt til å evaluere og forbedre modenhet innen en rekke forskjellige områder, men når jeg nevner dette i min undersøkelse er det modeller med fokus på cybersikkerhet. Det finnes også flere typer modenhetsmodeller for cybersikkerhet. I de fleste av dem er bevissthet et viktig element. Disse modellene beskriver et spekter av punkter som en forventer å se i en organisasjon med en effektiv tilnærming til cybersikkerhet (Anne W, 2018). Hvert punkt vil ha en beskrivelse av de handlingene og prosessene en forventer å se til stede i bedriften, på forskjellige nivåer av modenhet (Anne W, 2018). En bedrift som søker å vurdere sin totale cybersikkerhetsmodenhet,

vil sammenligne sine egne praksiser med de som er beskrevet på nivåene for hvert punkt (Anne W, 2018). Sikkerhetstrening kan være et eksempel på et punkt (Anne W, 2018). En vurdering av dette kan gjøres ved å samle dokumentasjon på deltakelse i opplæringskurs. Kanskje undersøke eller intervjue personalet, og analysere effekten av opplæringen ved å se på spesifikk atferd hos ansatte, for eksempel personer som følger etter andre gjennom sikrede dører med adgangskort og inn i områder der sensitiv informasjon behandles (Anne W, 2018). Modenhetsmodeller kan være en effektiv måte å vurdere bevisstheten innad i bedriften. Så og si alle bedrifter bør gjennomføre en modenhetsanalyse for å avdekke hull i egen sikkerhet, sier Terje Lystad IT-sjef i Norges Bondelag (Atea, 2022). En modenhetsanalyse bidrar til å forankre informasjonssikkerhetsarbeidet i virksomhetens ledelse, skaper langsiktighet og kontinuitet i informasjonssikkerhetsarbeidet, og etablerer et startpunkt som legger grunnlaget for prioriteringer (Atea, 2022).

2.3 Annen litteratur

PwCs Cybercrime Survey

Jeg har brukt PwC sin kvantitative undersøkelse flittig til sammenligning med resultatene mine. Det var 106 respondenter som deltok i deres Cybercrime Survey og den er distribuert i samarbeid med Finans Norge (PwC, 2023). Samme som i min undersøkelse, kommer respondentene deres fra et bredt spekter av bransjer. Det er en svært liten andel av dem uten en form for lederstilling (PwC, 2023). Formålet til PwC er å belyse hvordan cybertrusler påvirker norske virksomheter (PwC, 2023), men det er mye sammenlignbar data selv om formålet deres er en anelse ulikt mitt.

Modell for organisatorisk cybersikkerhetskultur

Huang & Pearlson (2019) har laget en modell som beskriver organisatorisk cybersikkerhetskultur, med fokus på faktorene som er viktig for å bygge den og hvordan den kan måles. Studien deres handler om å hjelpe ledere til å forstå og anvende anbefalinger for å skape en mer moden cybersikkerhetskultur i deres organisasjon (Huang & Pearlson, 2019). De har flere interessante punkter rundt hvordan best mulig skape sterk bevissthet blant ansatte i en bedrift. Flere av påstandene deres går igjen i intervjuene mine, men flere faktorer ser også ut til å være

ignorert av en god del selskaper i min undersøkelse.

Påvirkningen av vellykkede cyberangrep på målrettede selskaper

Kamiya et al. (2018) har laget en studie der de undersøker hvilke selskaper som er mål for cyberangrep og hvordan de påvirkes. Denne artikkelen blir brukt som sammenligningsgrunnlag mot svarene til bedriftene på flere av spørsmålene. Både når det gjelder konsekvenser og hvem som er mest sårbare. Cyberangrep får selskaper til å revurdere risikoene de er eksponert for og deres konsekvenser (Kamiya et al., 2018). Det er interessant å vurdere hvordan opplevelser av vellykkede angrep kan forandre en bedrift med tanke på tiltak og mottrekk.

Den framvoksende rollen til CISO

For å se nærmere på CISO (Chief information security officer) rollen flere av intervjuobjektene mine hadde, har jeg brukt Hooper & McKissack (2016) sin artikkel. Den gir informasjon rundt hva som kreves i denne rollen og hvordan bedrifter skal bruke dem på en optimal måte. Når det gjelder utfordringene som organisasjoner møter når de velger en CISO, har de brukt data fra USA, Canada og New Zealand (Hooper & McKissack, 2016). CISO rollen er relevant med tanke på flere av spørsmålene mine.

Cybersikkerhetstrening i norske kritiske infrastrukturselskaper

Chowdhury et al. (2022) har sammenlignet praksis for bevissthet om cybersikkerhet og opplæring i utvalgte selskaper med kritisk infrastruktur. De gjennomførte intervjuer og sendte ut spørreskjemaer til cybersikkerhetspersonell i ulike sektorer med kritisk infrastruktur i Norge (Chowdhury et al., 2022). Dette er relevant for min studie med tanke på trening av ansatte og hvordan fremme deres cybersikkerhet bevissthet på best mulig måte. Jeg vil sammenligne deres selskapers svar og litteratur med mine resultater.

Cyberangrep– trender, mønstre og sikkerhetstiltak

Bendovschi (2015) sin artikkel om cyberangrep, deres trender, mønstre og sikkerhetstiltak gir en

oversikt over cyberkriminalitet. Han utfører en analyse av angrep rapportert over hele verden de siste tre årene før 2015 for å fastslå mønstre og trender i cyberkriminalitet (Bendovschi, 2015). Basert på resultatene av analysen, presenterer artikkelen mottiltak som selskaper kan gjennomføre (Bendovschi, 2015). Dette er relevant for min studie med tanke på tidligere angrepsmetoder. Det samme gjelder mottiltak for å stoppe disse angrepsformene. Flere av angrepsformene og mottiltakene er fortsatt vesentlig i dag.

Faktorene som påvirker cybersikkerhetsinvesteringer i private sektorselskaper

Gordon et al. (2018) sin artikkel undersøker private bedrifters investeringer i cybersikkerhetsaktiviteter. Studien viser i hvilken grad bedriftene ser på investeringer i cybersikkerhet som en kilde til et konkurransefortrinn(Gordon et al., 2018). Artikkelen deres fokuserer på den private sektoren og er derfor sentral i min sammenligning av svar fra de offentlige og private selskapene i undersøkelsen min.

Er det mulig å endre de ansattes cybersikkerhetsatferd?

Ergen et al. (2021) sin artikkel går ut på å utforske og diskutere ansattes rolle i cybersikkerhet. De har gjennomført dybdeintervjuer med åtte cybersikkerhetseksperter gjennom semi-strukturerte åpne intervjuer (Ergen et al. 2021). Studien gir perspektiver angående de ansattes cybersikkerhetsatferd, hindringer og fremmere av sikker atferd i cybersfæren (Ergen et al. 2021). Studien er viktig for min undersøkelse med tanke på sammenligning av svarene på spørsmålene som angår bevisstheten til ansatte.

3 Valg av forskningsmetode

3.1 Kvalitativ metode

For å få mest mulig dybde i dataene mine valgte jeg å gjøre kvalitative intervjuer. Kvalitativ forskning gjør undersøkelsen mer bred og åpen, noe som tillater deltakerne å fremheve saker rundt temaet som er viktigst for dem (Choy, 2014). Den lar meg også utforske perspektivene til ulike mennesker rundt et tema (Choy, 2014). Planen er å se på hvordan ulike type ledere ser på sin egen bedrift angående bevissthet rundt cybersikkerhet. Utdypningen av svarene til intervjuobjektene er fokuset i studien min. Derfor valgte jeg en kvalitativ metode fremfor en kvantitativ. Metoden gir detaljerte beskrivelser av tanken bak bedriftenes ulike tiltak. Den svarer på hvordan og hvorfor, i stedet for hvor mange eller hvor mye (Tenny et al., 2017). Intervjuobjektene får muligheten til å komme med eksempler på praksiser, strategier og utfordringer. Jeg mener også at den kvalitative metoden gir et mer levende og realistisk bilde av hvordan cybersikkerhetsbevisstheten oppleves i de ulike bedriftene. Underliggende faktorer angående effekten av de ulike tiltakene kan komme frem når jeg tilpasser oppfølgingsspørsmålene mine etter svarene jeg får. Friheten til å tilpasse oppfølgingsspørsmål gir mulighet til å oppdage nye innsikter generelt.

3.1.2 Valg av bedrifter

Jeg tok kontakt med ulike norske bedrifter via mail, og spurte om de kunne tenke seg å delta i studien. Mailen inneholdt en beskrivelse av studien, og en forespørsel om å delta. Planen var å anonymisere bedriftene som deltok, dette understreket jeg i mailen. Likevel var det en frykt helt fra starten for at bedrifter ikke ville delta med tanke på konfidensialitet, noe også flere svarte med. Det kunne kompromittere deres sikkerhetsprotokoller eller utsette dem for økte sikkerhetsrisikoer. Flere av bedriftene var veldig positive til undersøkelsen, men svarte at de ikke hadde tid til å delta. Jeg tenkte på forhånd at mange ville unngå å bli med hvis jeg hadde for mange spørsmål, og intervjuet dermed tok lang tid. Derfor valgte jeg meg ut 12 hovedspørsmål

og stipulerte intervjuet til rundt en halvtime. Til slutt var det 16 bedrifter fra 8 ulike bransjer som takket ja. Målet mitt var hele tiden å få variasjon i bedriftene. Jeg fikk tak i både offentlige og private, små og store, men også fra flere ulike industrier.

3.2 Intervjuer

Hovedspørsmålene mine ble tatt fra den engelske og jordanske studien for å få en type struktur i intervjuene og et bedre sammenligningsgrunnlag. Struktur i intervjuform er brukt for å få en effektiv måte å holde intervjuet tett fokusert på temaet jeg undersøker (Alsaawi, 2014). Det gjør også intervjuene sammenlignbare (Alsaawi, 2014).

Jeg har brukt ti av spørsmålene fra den engelske studien som jeg mener passet til mitt forskningsspørsmål i mine egne intervjuer. Jeg tok tidlig kontakt med en av forfatterne av studien via mail, for å få bekreftelse på at det var greit at jeg brukte deres studie til sammenligning. Dette var viktig ettersom denne studien ble en så stor del av min egen intervjuguide. Spørsmål 9 og 10 (fra den engelske studien) som omhandlet tidligere angrep og virkningen av dem ble flere ganger samlet til ett spørsmål, ettersom alle bedriftene hadde blitt angrepet på ulike måter. Det var likevel bare et fåtall av dem som faktisk hadde hatt en virkning. Hvis de hadde opplevd angrep med virkning, ble dette som oftest fokuset mitt ut fra disse spørsmålene.

Jeg benyttet to av spørsmålene fra den jordanske studien som omhandlet bevissthet rundt programvaresikkerhet og fysisk sikkerhet. Begge studiene tar for seg utenlandske organisasjoner som gir et interessant sammenligningsgrunnlag basert på de samme spørsmålene. Surveyene deres inneholder også kvalitative svar, ikke bare avkryssing.

Jeg har kommet med egne oppfølgingsspørsmål basert på svarene fra hovedspørsmålene. Jeg var åpen for dialog, noe som tilsier at jeg hadde en semistrukturert form på intervjuene mine (Kendall, 2014). Denne formen for intervju, gir meg muligheten til å se saker fra intervjuobjektenes side (Kendall, 2014), noe jeg var veldig opptatt av. Hvis noen svarte "nei" på spørsmål, prøvde jeg alltid å spørre hvorfor dette ikke ble prioritert. På slutten av flere intervju har jeg spurt om intervjuobjektet har noe å legge til eller føler jeg burde spurt om. Det ga dem muligheten til å avdekke erfaringer og kunnskaper de enda ikke hadde tatt opp rundt temaet. Jeg gjorde individuelle intervjuer med ulike typer ledere. De ulike rollene var:

- CISO eller leder for informasjonssikkerhet (9)
- Lederrolle eller leder av IT avdelingen (5)
- En av lederne i selskapet (uten egen IT avdeling)(2)

Ni av intervjuene var via Microsoft Teams, seks i person på kontorbygget til intervjuobjektet og ett ble gjort over telefon. Lengden på intervjuene varierte fra 15- 45 minutter.

3.2.1 Tematisk analyse

Når jeg hadde transkribert alle intervjuene, begynte jeg på den tematiske analysen. Til det benyttet jeg verktøyet "NVivo". Jeg startet med å bruke NVivo til å få organisert svarene på de ulike spørsmålene. Dette var for å kunne identifisere hvilke temaer som dukket opp fra svarene på hvert av hovedspørsmålene og to av oppfølgingsspørsmålene. Deretter samlet jeg de temaene som ble hyppigst gjentatt på hvert av spørsmålene. Jeg begynte med å se på resultatene basert på alle bedriftene samlet. Etter dette startet jeg analysedelen. Her sammenlignet jeg svarene til selskapene ut fra bedriftsstørrelse, om de var offentlige eller private og på bedriftene med nulltoleranse for nedetid. Fra analysene er det bare spørsmålene med variasjoner i de mest gjentatte temaene som er fremhevet og grundig utdypet i studien. Første analyse var av forskjellene på små, mellomstore og store bedrifter. Den andre var forskjellen på private og offentlige bedrifter. Den siste analysen jeg gjorde, var forskjellen på bedriftene med nulltoleranse for nedetid og de med en viss toleranse for nedetid. Jeg har brukt en kombinasjon av latent tematisk analyse og semantisk tematisk analyse. Med en semantisk tilnærming identifiserer jeg temaer basert på overflate betydningene av dataene (Braun & Clarke, 2006). Den latent tematiske analysen identifiserer underliggende ideer, antakelser, konseptualiseringer og ideologier (Braun & Clarke, 2006). Dette vil komme mer opp i diskusjonsdelen av studien når jeg ser på bakgrunnen for tankegangen til intervjuobjektene.

3.3 Intervjuguide

Hovedspørsmål	Faste oppfølgingsspørsmål
Q1: Tilbyr din bedrift kurs eller opplæringsmateriell til ansatte for å øke bevisstheten rundt cybersikkerhet?	**Hvis ja**: Hvilke tema omfatter kurset? Må alle ansatte gå gjennom dette? Hvis ikke, hvem må ta det?
Q2: Har din bedrift stillinger dedikert til cybersikkerhet?	**Hvis ja**: Hvor lenge har stillingen((e)) eksistert? Er de for eksempel representert i ledergruppen eller andre lederfora?
Q3: Har dere faste møter angående cybersikkerhet?	**Hvis ja**: Hvor ofte har dere disse møtene? Hvem er tilstede på disse møtene? Og: Deltar av og til toppledelsen?
Q4: Hvordan vil du karakterisere din egen kunnskap om cybersikkerhet?	**Hvis ja**: Har du utdannelse innen cybersikkerhet? Hvor lenge har du eventuelt jobbet hovedsakelig med cybersikkerhet?
Q5: I hvilken grad frykter du for et cyberangrep mot din bedrift?	**Delspørsmål:** Hvilke type angrep er du bekymret for?
Q6: Hvordan vil du karakterisere din bedrift når det kommer til cybersikkerhet bevissthet?	**Delspørsmål**: Bruker dere noen form for modenhetsmodeller?

Q7: Hvor lenge tror du at deres kritiske applikasjoner og systemer kan være nede før det får betydelige konsekvenser for selskapet?	Hvilke app-er/systemer er mest kritiske? Er de særlig beskyttet? Hvilke nødløsninger har dere på plass?
Q8: Bruker din bedrift spesifikke prosesser eller verktøy for å identifisere cybersikkerhet sårbarheter?	
Q9: Har det vært noen tidligere cyberangrep på din bedrift som du kan nevne?	
Q10: Hva var virkningen av det eventuelle angrepet(ene)?	
Q11: Kan de ansatte i bedriften surfe fritt på nettet eller er det begrenset hvilke sider de har tilgang til?	
Q12: Har folk generelt begrenset tilgang til bedriftens kontorbygg?	

4 Resultater og diskusjon

4.1 introduksjon av kapittel

Dette kapittelet vil ta opp resultatene og diskutere dem. Det er fire deler: Første seksjon vil diskutere de samlede svarene til alle bedriftene, den andre seksjonen er en sammenligning av svarene basert på bedriftsstørrelse, den tredje seksjonen er en sammenligning av svarene basert på private og offentlige bedrifter, og siste seksjon er en sammenligning av svarene basert på bedrifter med nulltoleranse for vellykkede cyberangrep og de bedriftene som ikke tar like fort skade. Første seksjon er en oppsamling av svarene til alle bedriftene. De tre siste seksjonene er analyser basert på faktorer som påvirker bedriftene.

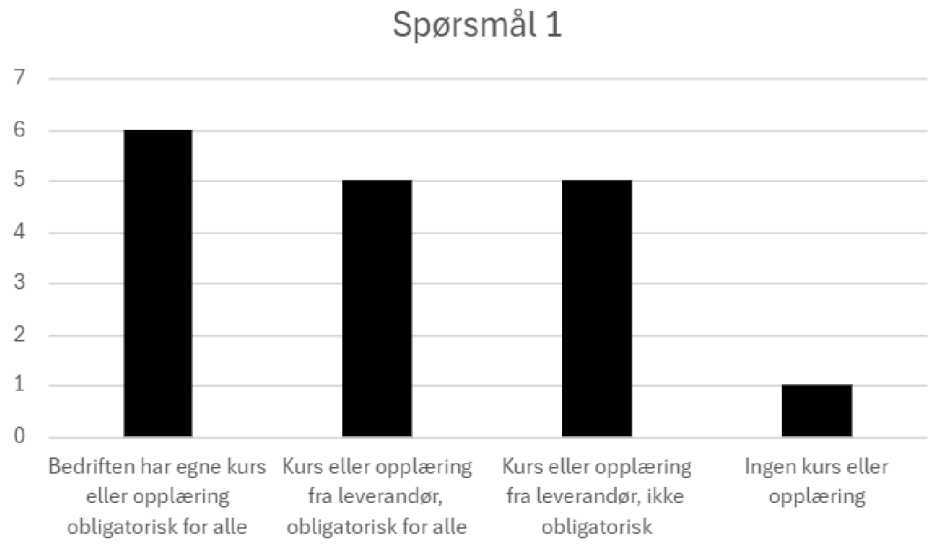
Søylediagrammene illustrerer temaene som er tatt opp flest ganger blant intervjuobjektene. Én bedrift kan selvfølgelig ha svart flere ting, som gjør at antallet i diagrammene kan overskride antallet bedrifter intervjuet som er 16. Søylediagrammenes svar varierer fra beste til dårligste praksis for cybersikkerhet basert på spørsmålet, fra venstre mot høyre. Svarene er rangert etter mine egne vurderinger via kilder. Jeg har valgt å plassere egne diskusjonsdeler under hvert resultat. Det gjør at jeg får diskutert hvert spørsmål og resultat separat fra hverandre. Jeg har laget en samlet diskusjonsdel for spørsmål 9 og 10. Dette er fordi svarene er basert på hverandre. På spørsmål 5 har jeg tatt med et oppfølgingsspørsmål i resultatene. Det samme gjelder spørsmål 6. Grunnen til dette er at det kom masse interessante svar på dem og at de passet fint til sammenligning med hovedspørsmålene. Spørsmålene uten forskjeller i analysene ligger i rekkefølgen av spørsmål og diskusjoner, men de er ikke illustrert eller diskutert rundt. Det er bare skrevet noen linjer om at svarene er like og hva som er likt. Alle punktene jeg har nevnt her gjelder for hele resultat og diskusjonsdelen av studien min.

4.2 Samlet oversikt alle bedrifter

Første delen av resultater og diskusjon, er svarene til alle bedriftene. Jeg har funnet gjentatte tema fra hvert spørsmål. Illustrasjonene i denne seksjonen viser hvilke tema som er tatt opp flest ganger blant alle bedriftene.

4.2.1 Q1: Kurs eller opplæringsmateriell

På spørsmål 1 sier de fleste at de har egne kurs eller opplæring alle ansatte må gjennom, toppledelse inkludert. Flere gir også uttrykk for at de investerer i eksterne kurs, hvor alle ansatte må delta eller gjennomføre. Like mange gjør det samme, men her er det enten frivillig for de ansatte om de vil gjennomføre, eller så er det kun en del av de ansatte i bedriften kursene eller opplæringen er obligatorisk for. Det er bare én bedrift som sier de ikke tilbyr noen form for kurs eller opplæring til de ansatte.



Figur 1. Spørsmål 1: Tilbyr din bedrift kurs eller opplæringsmateriell til ansatte for å øke bevisstheten rundt cybersikkerheten?

Diskusjon: Kurs eller opplæringsmateriell, alle bedrifter

Det er bare én bedrift som sier de ikke tilbyr noen form for kurs eller opplæring til de ansatte, noe som viser at dette er et viktig aspekt for flere av dem. De fleste bedriftene sier de tilbyr opplæring som skal stoppe ubevisste feil, mens seks bedrifter enten ikke tilbyr noe opplæring eller har frivillige kurs. Jeg snakket videre med flere om de frivillige kursene som ble tilbudt. Som oftest kom det fram at mesteparten av de ansatte unngikk å ta de aktuelle kursene.Unnskyldningen var som oftest at de ikke hadde tid til å prioritere dette eller at de hadde glemt det. I PwCs cybercrime survey svarer 67% av norske bedriftsledere at de betrakter

ansattes ubevisste handlinger som en trussel mot virksomheten sin (PwC, 2023).

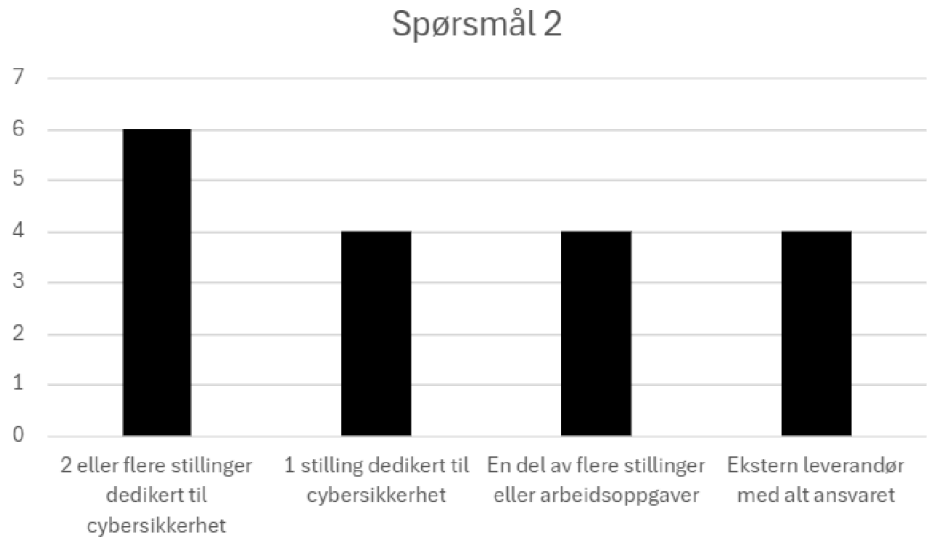
I min undersøkelse gjorde et stort antall bedrifter det slik at kursene var obligatoriske for ansatte i deler av bedriften. Dette var som oftest de som jobbet med IT i bedriften eller på kontor med egen jobb- PC. I Chowdhury et al. (2022) sin undersøkelse rundt cybersikkerhetstrening i norske selskaper, sier generelt sett alle intervjuobjektene at grunnleggende opplæring og bevissthet om cybersikkerhet bør gis til alle ansatte, men visse roller krever mer inngående opplæring. Intervjuene deres er gjort med norske selskaper innen kritisk infrastruktur, men det de sier er fortsatt noe alle norske bedrifter kan utnytte. I mine intervjuer er det flere bedrifter som utelater deler av bedriften i opplæringen. Noen av grunnene som kommer opp, er at deler av de ansatte i bedriften ikke bruker PC eller annen teknologi på jobb. De har ikke noe jobbrelatert teknologi tilgjengelig som kan utnyttes, de har ikke en jobb-mail eller tilgang på sensitiv informasjon. Men Twitter, Facebook og andre sosiale nettverkssider har blitt en del av vår daglige rutine i privat og forretningsmessig kommunikasjon (Krombholz et al., 2015), noe som tilsier at så lenge den ansatte bruker internett privat har angripere alltid en måte å utnytte dem på for å skade de privat eller selskapet de jobber for.

Flertallet sier at de enten kjøper kurs fra leverandør eller har egne kurs/opplæring de har laget selv som alle ansatte må ta, de fleste sier også at dette er E-læringskurs. Dette er ofte det mest populære innenfor trening og opplæring av ansatte på grunn av det lave ressursforbruket, den høye tilgjengeligheten og enkelheten i bruken (Chowdhury et al., 2022). E-læringskurs er også utmerket for å ha oversikt over om ansatte tar de obligatoriske kursene eller ikke. De kan tilby analyser og rapporter til ledere, pluss at de kan gi ansatte automatiserte påminnelser om at de har kurs eller opplæring de må gjennomføre.

4.2.2 Q2: Stillinger dedikert til cybersikkerhet

På spørsmål 2 sier flertallet at de har to eller flere dedikerte stillinger til cybersikkerhet. Mange har også 1 dedikert stilling, eller så er det en del av stillingen til et visst antall ansatte. En god del

lar leverandørene stå for alt ansvaret rundt cybersikkerheten og har ingen ansatte med noe form for arbeidsoppgaver på dette området.



Figur 2. Spørsmål 2: Har din bedrift stillinger dedikert til cybersikkerhet?

Diskusjon: Dedikerte stillinger til cybersikkerhet, alle bedrifter

Store deler av bedriftene jeg intervjuet hadde investert i CISO- roller(Chief Information Security Officer). CISO er en strategisk lederrolle med ansvar for å sikre at informasjonsressurser og IT-systemer er beskyttet og trygge (Hooper & McKissack, 2016). De fleste bedriftene svarte at de hadde opprettet disse stillingene for ett til to år siden. Noen brukte ikke CISO stemplet og gikk heller under tittelen «Leder for informasjonssikkerhet». Å investere i en sjef for informasjonssikkerheten, bidrar til større beskyttelse mot risiko, sikring av kontinuitet i virksomheten, raskere respons på hendelser og katastrofegjenoppretting (Hooper & McKissack, 2016). Dette er viktige aspekter når det gjelder cybersikkerhet. I intervjuene mine sier også flere CISOer at de har et for lite antall møter med ledelsen. Disse møtene er viktig for å oppdatere ledelsen rundt hva leder for informasjonssikkerhet eller CISO bidrar med, og hvordan det står til i bedriften. Så hvis ledelsen først investerer i en lederstilling for informasjonssikkerhet, bør de kanskje utnytte kompetansen i større grad. PwC skriver i sin undersøkelse at CISOer kan ha manglende tilgang til ledergrupper, noe som kan være grunnen til at 1 av 3 sa at toppledelsens manglende forståelse utgjør en trussel for virksomhetens cybersikkerhet (PwC, 2023).

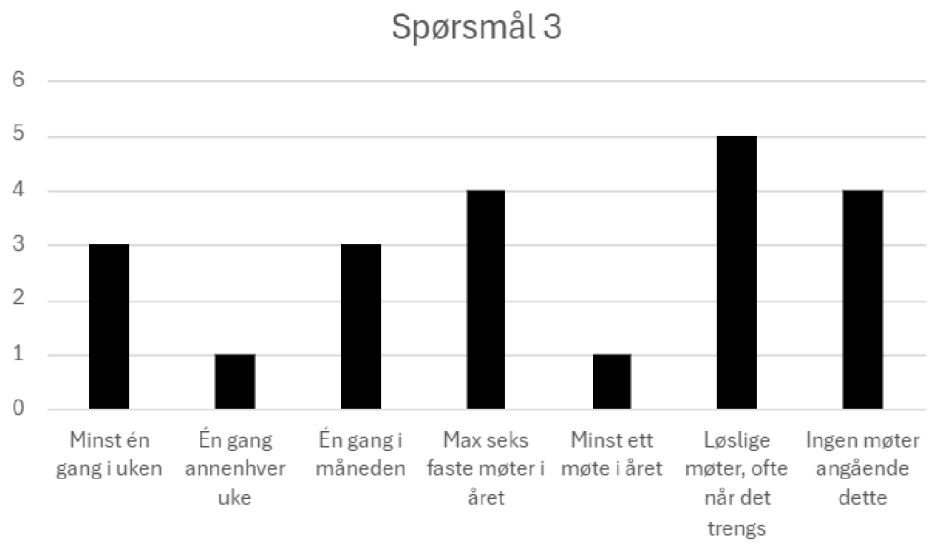
I figur 2 kan en se at flere bedrifter sier de har det som en del av stillinger eller arbeidsoppgaver. Dette kan spare ressurser og samtidig gi relativt utfyllende rapporter til ledelsen. Ulempen er at IT-sikkerheten blir utvannet blant de mange andre aspektene som IT er ansvarlig for, ikke bare med hensyn til oppmerksomhet eller rapportering, men fordi de i stor grad er usynlig i organisasjonens daglige drift, også med hensyn til budsjett tildeling (Hooper & McKissack, 2016).

Et større antall av bedriftene med deling av arbeidsoppgaver, sa at de hadde en tendens til å ta IT-sikkerheten opp når det først skjedde noe. Dette gjenspeiler det Hooper & McKissack sier i sin artikkel: Rapporteringen til ledelsen/styret ble utvannet, med mindre det hadde vært et betydelig brudd, hadde sikkerheten en tendens til å forsvinne i bakgrunnen når det gjaldt dens synlighet (Hooper & McKissack, 2016).

Mange av selskapene sier også de bruker eksterne leverandører til IT og informasjonssikkerhet. Altså har ingen fra selve bedriften noe ansvar rundt dette. I PwC sin undersøkelse var 60% av alle målrettede angrep mot virksomheter, rettet mot tredjeparter (PwC, 2023). Leverandøren bedrifter knytter seg til, har et stort ansvar når det gjelder sikkerheten. Organisasjoner velger å outsource informasjonssikkerhetsoperasjoner av ulike årsaker, som kostnadsbesparelser, tilgang til ansatte med høyspesialiserte ferdigheter og ekspertise, dedikerte fasiliteter og ansvars beskyttelse (Gupta and Zhdanov 2012). De bedriftene som fraskrev seg ansvaret rundt cybersikkerhetsrisikoen kan ha gjort lurt i dette om de ikke har kunnskapen som trengs. På en annen side vil risikoprofilen deres endre seg til å bli en kombinasjon av deres egne risikoer og et delsett av deres leverandørs risikoer (Benaroch, 2020).

4.2.3 Q3: Faste møter

På spørsmål 3 var det møter etter behov som ble mest gjentatt, ofte løselig basert på hendelser og ikke noe fast. Det var også et stort antall som svarte at de ikke hadde noen form for møter angående temaet. Det tredje svaret som ofte kom opp, var at flere hadde rundt to møter per kvartal, altså cirka seks møter i året. Et stort antall hadde også relativt hyppige møter, noen én gang i måneden, andre én gang i uken.



Figur 3. Spørsmål 3: Har dere faste møter angående cybersikkerhet?

Diskusjon: Faste møter, alle bedrifter

Som sagt er møter mellom toppledelse og ledere for informasjonssikkerheten viktig, en annen viktig dimensjon er hvordan ledelse kommuniserer cybersikkerhet med vanlige ansatte. I mine intervjuer sier over halvparten at de enten ikke har møter rundt dette, eller så har de møter ved hendelser. Dette tilsier at møter som kommunikasjonsmiddel av cybersikkerhet generelt, ikke er brukt av en stor mengde bedrifter jeg snakket med, med mindre det er ytterst nødvendig.

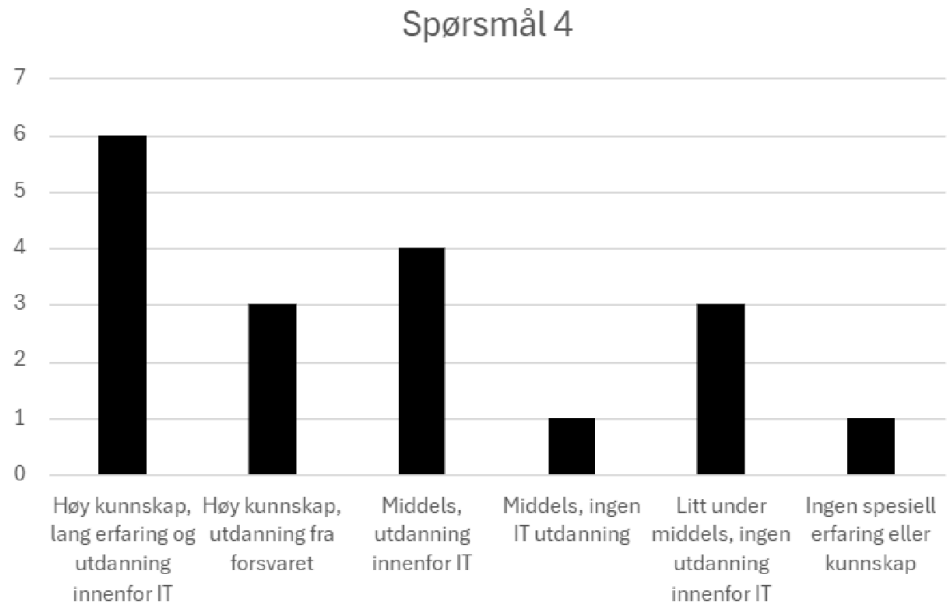
Trusselen fra interne aktører basert på menneskelig atferd, er en av de mest utfordrende aspektene ved sikkerhet å kontrollere. Det å bygge en kultur av cybersikkerhet i en organisasjon veileder ansattes atferd og øker motstanden mot cyberangrep (Huang & Pearlson, 2019). Ledere må opprette flere formelle og uformelle kanaler for å rapportere cyberhendelser og dele dynamisk cyberinformasjon (Huang & Pearlson, 2019). Her er faste eller løslige møter en essensiell metode for å gjøre nettopp dette. Dette trenger ikke være ledelsen eller en CISO sitt ansvar, selskapet må finne en leder som har ansvaret for å dyrke en kultur for cybersikkerhet og har direkte makt og myndighet til å påvirke dyrkningsprosessen (Huang & Pearlson, 2019). Uten en leder med spesifikt ansvar for å bygge kulturen, vil aktivitetene utføres tilfeldig og noen ganger hoppes helt over (Huang & Pearlson, 2019).

Flere selskaper har regelmessige møter, som oftest er dette mellom ulik ledelse noe som

selvfølgelig er optimalt på flere måter. De vanlige ansatte kan også bli inkludert i en viss mengde slike møter for å skape en kultur rundt et så kritisk tema. Antall møter og organisering av ansatte må åpenbart tilpasses bedriften det gjelder.

4.2.4 Q4: Egen kunnskap

Her svarer de fleste at de har god kunnskap, lang erfaring og utdannelse innenfor IT. Noen har også utdannelse fra forsvaret. Flere sier kunnskapen er middels, selv om de har en utdanning innenfor IT. En god del av de jeg har snakket med, påstår også at de har lite kunnskap rundt dette og ingen utdannelse innenfor IT. 5 av de 16 intervjuobjektene hadde ingen form for IT-utdanning.



Figur 4. Spørsmål 4: Hvordan vil du karakterisere din egen kunnskap om cybersikkerhet?

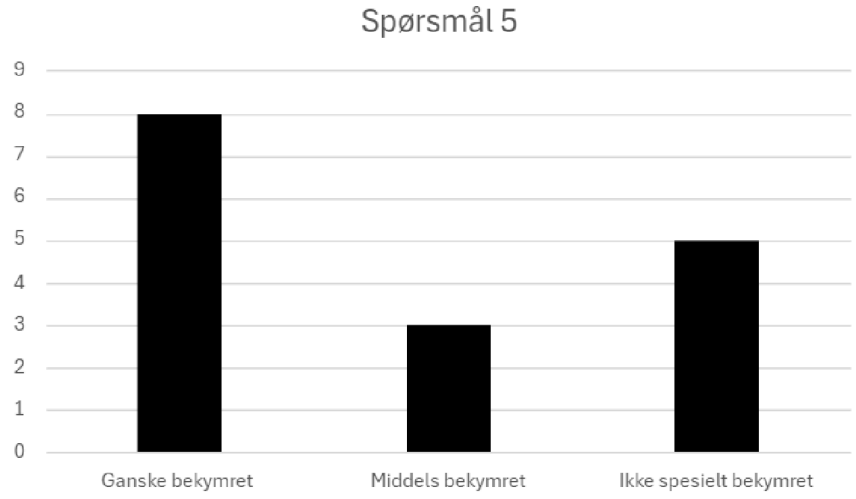
Diskusjon: Egen kunnskap, alle bedrifter

På dette spørsmålet sa mesteparten at de hadde opparbeidet seg god kunnskap og erfaring, noe som var forventet fordi ni av intervjuobjektene hadde stilling som CISO eller leder for

informasjonssikkerheten. For å håndtere sikkerhetshendelser kreves god kompetanse og forståelse av truslene (PwC, 2023). Av de som har svart at de har liten kunnskap og erfaring, eller ingen kunnskap og erfaring, er det ulike former for ledere uten IT utdanning. Dette var ledere som så sine begrensninger med tanke på bakgrunnen sin og manglende trening. I PwC sin undersøkelse svarer faktisk kun 1 av 4 ledere at de selv har manglende forståelse (PwC, 2023). Lederne som manglet egen kunnskap i mine intervjuer, hadde hyret andre selskaper til å gjøre denne delen av jobben for bedriften, noen stolte også på andre ansatte rundt dette. En del av dem sa de møtte med leverandør relativt ofte, andre nevnte ikke hvor ofte de orienterte hverandre. Flere virket til å ha et svært lite antall møter med leverandører, disse få møtene virket til å handle mer om orientering av tilstanden til bedriften enn læring og formidling av kunnskap. En del selskaper hadde ansatte med ulike spesialiseringer, for eksempel hadde intervjuobjektet ansvaret for retningslinjer, rutiner og prosedyrer, mens andre ansatte hadde kunnskap om teknisk implementering og gjennomføring. En større andel av intervjuobjektene mine hadde ikke rene tekniske kunnskaper, men mer et overordnet ansvar for organiseringen av sikkerheten i bedriften.

4.2.5 Q5: Frykt for cyberangrep

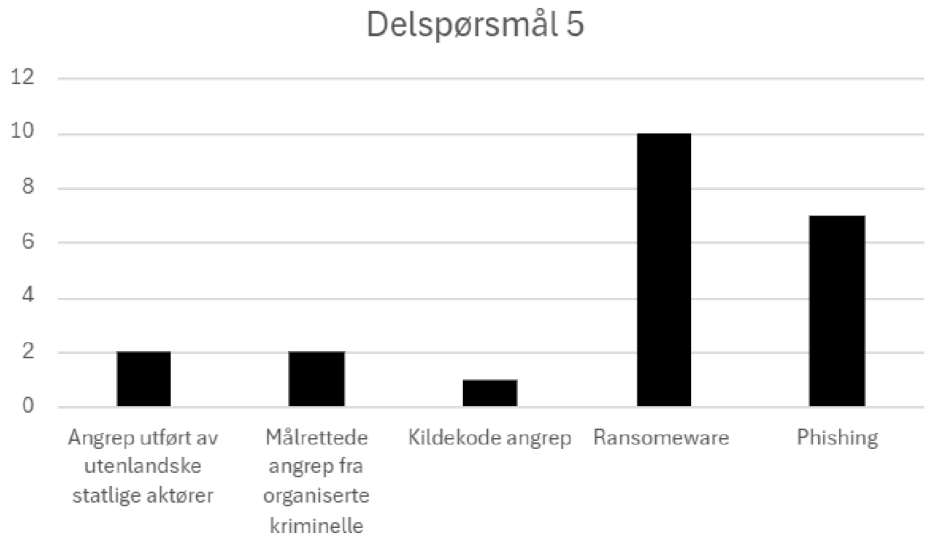
Her snakker halvparten om at de er ganske bekymret av flere grunner, men det er også en stor andel som sier de ikke er spesielt bekymret og har ulike grunner til dette.



Figur 5. Spørsmål 5: I hvilken grad frykter du for et cyberangrep mot din bedrift?

Delspørsmål Q5: Type angrep

Ransomeware er det som går klart mest igjen når det snakkes om type angrep de er mest bekymret for. Phishing blir tatt opp av en stor del. Målrettede angrep fra organiserte kriminelle og statlige aktører blir også nevnt av et fåtall.



Figur 6. Delspørsmål 5: Hvilken type angrep er du mest bekymret for?

Diskusjon: Frykt for cyberangrep/ Type angrep, alle bedrifter

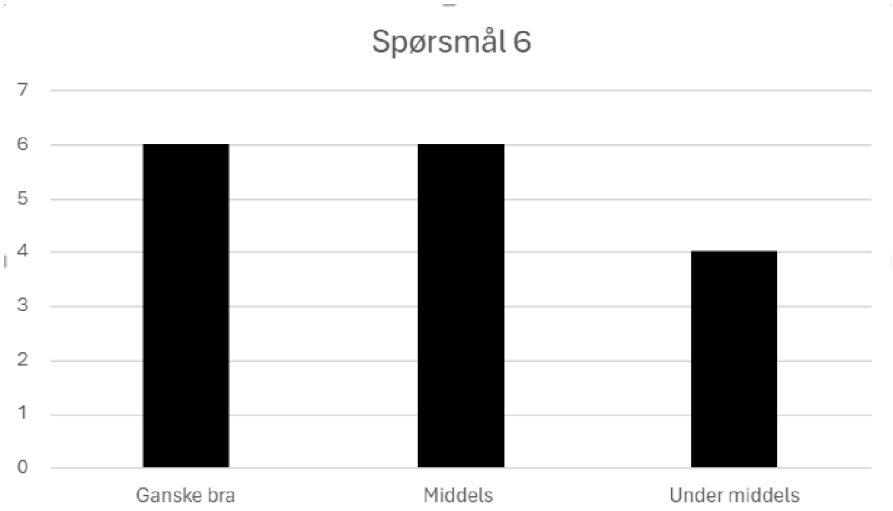
Det er flere definisjoner av begrepene cyberangrep, cyberkriminalitet, osv, som kan finnes blant den internasjonale litteraturen, men det alle definisjonene har til felles, er at de sier målet er å kompromittere konfidensialitet, integritet og tilgjengelighet av data (Bendovschi, 2015). Den halvparten som uttrykker bekymring for vellykkede cyberangrep sier det bare er et spørsmål om tid, noe som er forståelig. Fra 2019 til 2021 var det en tredobling i antall alvorlige cyberoperasjoner mot norske myndigheter og virksomheter. Dette var et antall som holdt seg på et tilsvarende nivå i 2022 (PwC, 2023). Likevel fremhever undersøkelsen til PwC en nedgang i bekymring for at et cyberangrep skal resultere i økonomisk tap eller at virksomheten skal miste kunder (PwC, 2023). En stor del sier også i mine intervjuer at de ikke er spesielt bekymret for angrep med større konsekvenser. Grunnene er ulike for dette. Noen påpeker sine mange metoder

innenfor sikkerhetsarbeid, andre snakker om forsvarsverkene sine, altså de ulike systemene de bruker. Det som går igjen flest ganger, er at de ikke er mest i faresonen. Dette er alle forståelige grunner, men bedriften skal ha ganske mange gode argumenter for å kunne si at de ikke er mest i faresonen. Cyberangrep er mer sannsynlig å forekomme hos mer synlige selskaper, selskaper med flere immaterielle eiendeler og selskaper med mindre fokus fra styret på risikostyring (Kamiya et al., 2018). Det er kategorier flere av de som sa de ikke var i faresonen, kan plasseres under. En annen sak er om cyberangrepene faktisk lykkes eller ikke.

Når det gjelder typer cyberangrep, var distribuerte tjenestenektangrep, phishing og kartleggingsaktivitet de vanligste angrepene i 2022 ifølge norske virksomheter (PwC, 2023). Ransomeware angrep, som blir svart mest i mine intervjuer, er ikke en del av de tre nevnte, men alle tre typene kan være inngangsporter for et ransomware angrep. Fra 2019 til 2023 har det faktisk vært en vesentlig nedgang i digital utpressing (ransomware) hos norske virksomheter (PwC, 2023). Flere bedrifter i intervjuene hevdet også at de hadde gjort flere tiltak mot nettopp slike angrep. Selskapenes økte bevissthet rundt slike typer angrep, kan være en av grunnene til reduksjonen av dem. PwC sier også at dette kan skyldes tilfeldigheter, og at vi må regne med at denne typen hendelser fortsatt utgjør en vesentlig trussel for norske virksomheter (PwC, 2023). Det som blir svart mye, og er på listen over mest vanlige angrep, er phishing. Phishing-angrep er svært vanlige, og det er viktig at folk får nødvendig opplæring for å stoppe slike angrep (Ansari, 2022). Det er et større antall bedrifter som sier phishing er det de er mest bekymret for, uten å ha obligatoriske kurs eller opplæring for de ansatte rundt temaet. Andre ting som blir snakket om, er målrettede angrep av organiserte kriminelle og statlige aktører. Det har vært en økning fra 35 % i 2022 til 45 % i 2023 når det gjelder målrettede angrep mot norske virksomheter (PwC, 2023). Det viser at norske bedrifter begynner å bli mer attraktive mål for angripere. Bedriftene i min studie som snakket om nettopp dette, er bekymret for de som vet hvor de kan ramme dem hardest, og har klare mål om å gjøre nettopp det. Dette er som oftest statlige aktører eller organiserte kriminelle som de påpeker. Med statlige aktører mener jeg regjeringer eller regjeringsstøttede enheter i land som bruker sine ressurser til å utføre cyberangrep mot andre.

4.2.6 Q6: Organisasjonens cybersikkerhetsbevissthet

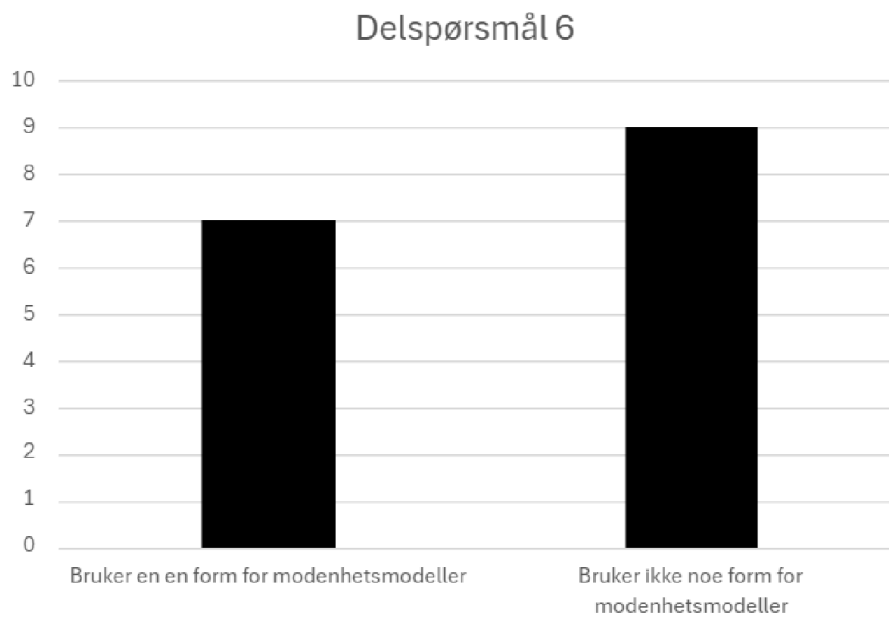
De fleste sier at den er middels eller ganske bra. Men en stor andel sier også at den ikke er god nok av ulike grunner.



Figur 7. Spørsmål 6: Hvordan vil du karakterisere organisasjonen når det kommer til cybersikkerhetsbevissthet?

Delspørsmål Q6: Modenhetsmodeller

Den største andelen av bedriftene jeg har intervjuet bruker ingen form for modenhetsmodeller, men det er nesten like mange bedrifter som bruker en variant av det for å måle modenheten rundt sikkerheten innad.



Figur 8. Delspørsmål 6: Bruker dere noen form for modenhetsmodeller?

Diskusjon: **Organisasjonens cybersikkerhetsbevissthet/ Modenhetsmodeller, alle bedrifter**

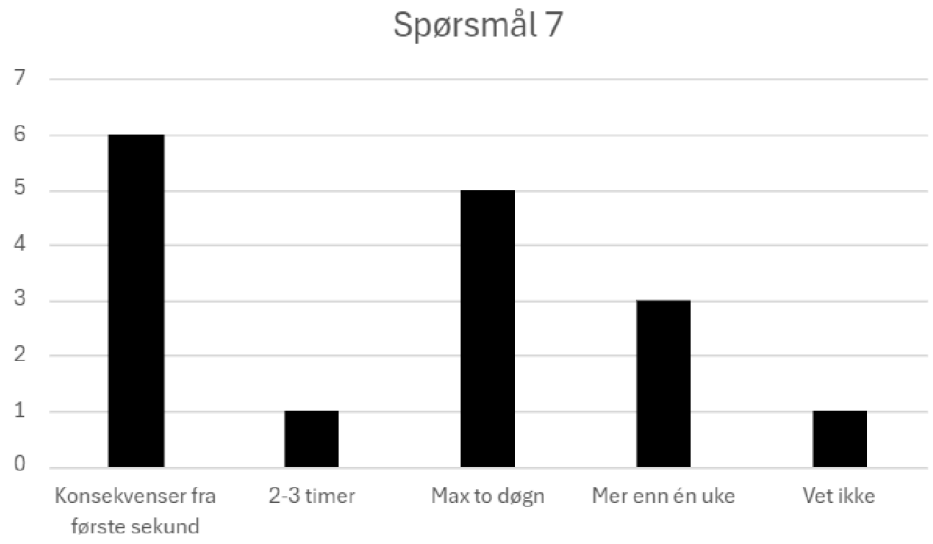
Flertallet av bedriftene som sier bevisstheten er middels eller under middels, påper at den er på vei oppover. De omtaler også fremtidige tiltak, her blir bevissthetstrening ofte nevnt. I PwC sin undersøkelse sier 47% av respondentene at "awareness" trening skal prioriteres i året som kommer (PwC, 2023). Flere bedrifter i min undersøkelse sier dette er blitt nedprioritert. Når enkeltpersoner forstår og vet hvordan de skal handle, er det mer sannsynlig at de vil handle på en måte som er i tråd med å øke cybersikkerheten (Huang & Pearlson, 2019). Noe flere i intervjuene mine virket til å forstå, og nå ta mer på alvor. PwC konkluderer også med at "forebyggende arbeid som minimerer menneskelig sårbarhet vurderes som et av de mest effektive aktivitetene virksomhetene kan prioritere"(PwC, 2023). Ansatte som er bevisst, vil være mistenksom ovenfor uvanlige e-poster, tekstmeldinger, vedlegg og annen kommunikasjon (Huang & Pearlson, 2019). En større mengde bedrifter sier at det er deler av bedriften som sliter med nettopp dette. Ofte er det ansatte som har begrenset erfaring med teknologi, eller som ikke bruker det mye i jobbsammenheng, som blir referert til.

Det er til sammen seks bedrifter som karakteriserer cybersikkerhetbevisstheten innad som middels eller ganske bra, uten å bruke noen form for modenhetsmodeller til å måle dette med. Av

de seks bedriftene, er det en del som er strengt regulert på andre måter. Flere ulike sektorer har store krav til cybersikkerheten innad i bedriftene. Dette var en av grunnene til at flere bedrifter sa bevisstheten var ganske bra, siden de møtte kravene som ble stilt. Det kan sees på som en erstatning av modenhetsmodeller, at noen utenfra vurderer bedriften etter strenge krav. På en annen side kan målinger være nødvendig for å finne den faktiske tilstanden innenfor cybersikkerhetsbevissthet og/eller cybersikkerhetsforsvarsstrategi. Den kan identifisere de nødvendige handlingene som må til for å oppnå den passende tilstanden innenfor cybersikkerhet (Möller, 2023). Dette nevner også intervjuobjektene som bruker modenhetsmodeller, det er ingen som påstår de er pålagt å bruke det, men det er en optimal måte å avdekke ting de må gjøre noe med.

4.2.7 Q7: Nedetid kritiske applikasjoner og systemer

Her forteller de fleste at de får betydelige konsekvenser fra første sekund. Nesten like mange sier de kan overleve rundt to døgn uten at det får nevneverdige konsekvenser. Noen sier også de kan klare seg en hel ukes tid uten kritiske applikasjoner og systemer. Alle jeg snakket med hadde en form for nødløsninger på plass om noe skulle skje.



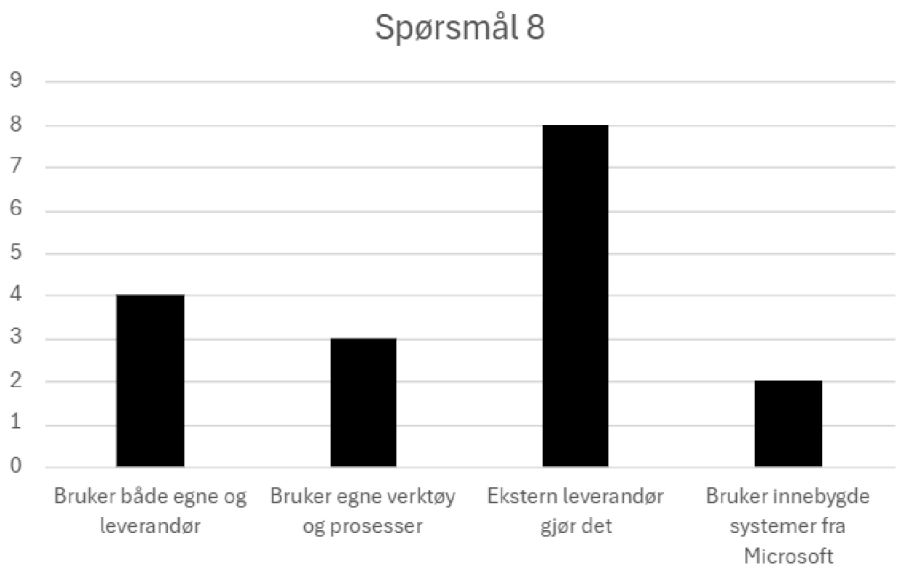
Figur 9. Spørsmål 7: Hvor lenge tror du at de kritiske applikasjonene og systemene kan være nede før det får betydelige konsekvenser?

Diskusjon: **Nedetid kritiske applikasjoner og systemer, alle bedrifter**

Her snakker flere bedrifter om at omdømme kan bli skadet hvis de har for lang nedetid. Bedriftene som har nulltoleranse for nedetid, sier at dette skjer fra første sekund. I PwC sin undersøkelse, sier også 60 % av bedriftene at de er mest bekymret for virksomhetens merkevare eller omdømme skal skades (PwC, 2023). Skade på organisasjonens omdømme som følge av en cyberhendelse, kan innebære et svekket offentlig bilde, hvor organisasjonen kan bli oppfattet som usikker eller ute av stand til å beskytte kundedata (Agrafiotis et al.,2018). De mest kritiske systemene som blir nevnt flere ganger, er de som driver økonomien og systemene kundene bruker. En større mengde bedrifter i min undersøkelse sier at de vil tape mye penger hvis nedetiden overskrider det de har svart. Dette er basert på at de ikke vil kunne fakturere kunder, og at flere kunder fort kan bytte dem ut siden de ikke leverer systemene de skal. En rekke av bedriftene med nulltoleranse, er samfunnskritiske. Største konsekvensen av sviktende systemer for disse bedriftene, er effekten det har på samfunnet. Disse sektorene har egne krav til beskyttelse av slike systemer, noe flere av dem også oppgir. Det positive fra svarene her, var at nesten alle bedriftene hadde en klar plan for nødløsninger hvis de kritiske systemene feilet. Planen gikk som oftest ut på å gå tilbake til mer manuelle løsninger og organisering ved hjelp av penn og papir. Alt vil selvfølgelig bli mer tungvint, men bedriftene ville fortsatt være oppegående. Et par bedrifter snakket om at de kunne erstatte utilgjengelige programmer med noen lignende. Det var også noen som svarte at leverandørene hadde klar planer og nødløsninger for dem.

4.2.8 Q8: Identifisering av cybersikkerhetssårbarheter

Det som helt klart går igjen mest, er leverandører med ansvaret rundt dette. Halvparten har andre som gjør dette for dem. Det er også en god del som bruker både leverandører og egne verktøy eller prosesser. Andre gjør alt selv med både egne verktøy og prosesser på dette området.



Figur 10. Spørsmål 8: Bruker din bedrift spesifikke prosesser eller verktøy for å identifisere cybersikkerhetssårbarheter?

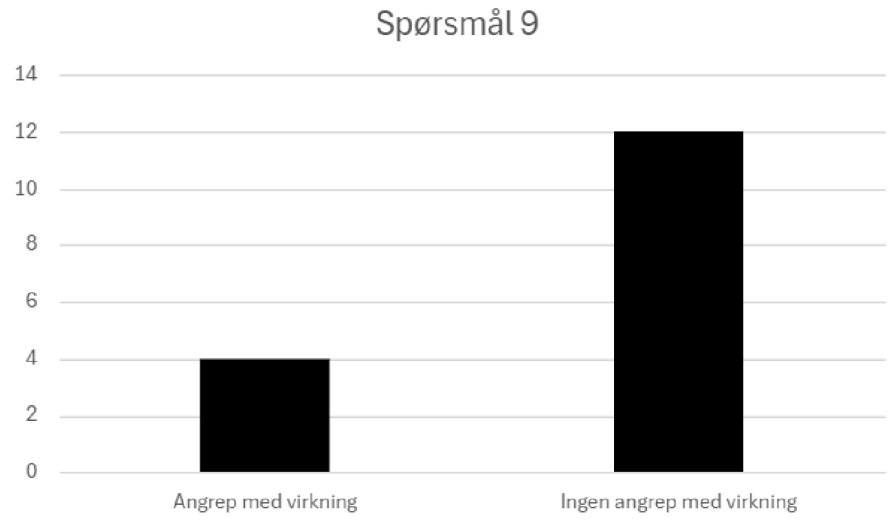
Diskusjon: **Prosesser eller verktøy identifisere cybersikkerhetssårbarheter, alle bedrifter**

Her svarer store deler at de har eksterne leverandører til dette på grunn av manglende IT-avdeling eller kunnskap innad. Dette er solide begrunnelser, men på en annen side er det mulig å utnytte dårligere sikrede underleverandører for å få tilgang til hovedleverandørens sårbarheter (PwC, 2023). Det er mulig å se dette som enda en vei inn i bedrifters systemer, men alle bedriftene med eksterne leverandører i undersøkelsen min har anerkjente selskaper, som ingen virker til å ha noen grunn til å betvile. PwC sier at 29% har opplevd hendelser forårsaket av leverandørfeil de seneste 12 månedene, som et resultat av cyberkriminalitet eller andre cybersikkerhetshendelser (PwC, 2023). Det vil alltid være en sjanse for at det skjer, men andre type hendelser har en mye høyere prosentandel i undersøkelsen deres (PwC, 2023), noe som tilsier at det ikke er leverandørfeil bedrifter skal frykte mest. Når det gjelder metoder for å identifisere cybersikkerhetssårbarheter, er SOC (Security Operations Center) det som blir klart mest tatt i bruk av bedriftene i min undersøkelse. En SOC har ansvaret for kontinuerlig og beskyttende overvåking av forretningstjenester, IT-systemer og infrastrukturer for å identifisere sårbarheter, oppdage cyberangrep, sikkerhetsbrudd, brudd på rettningslinjer og for å reagere raskt på cyberhendelser (Onwubiko & Ouazzane, 2022). Noen bedrifter i studien min har egne former

for dette, andre har hyret inn leverandører til å gjøre dette for dem.

4.2.9 Q9: Tidligere cyberangrep

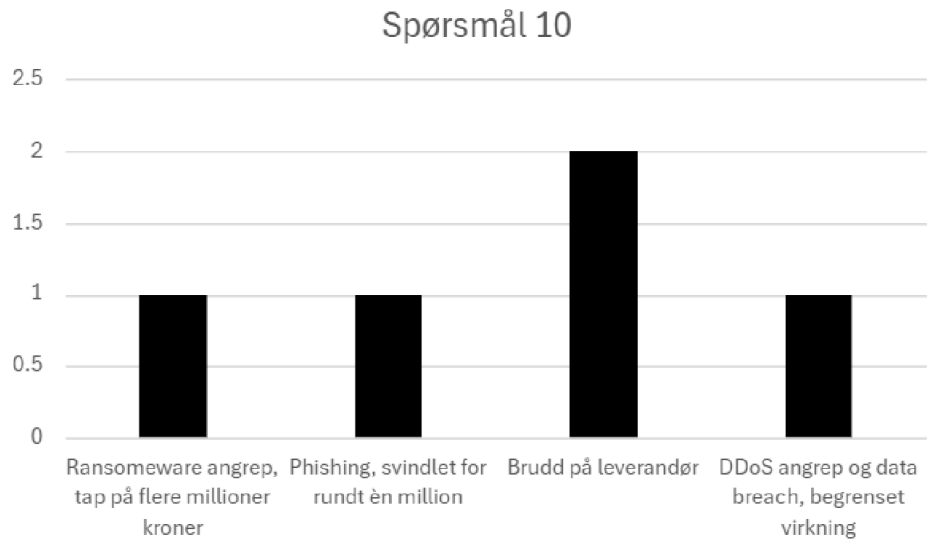
En stor mengde av intervjuobjektene sa her at det aldri hadde vært noen angrep med virkning. Så og si alle nevnte at det skjedde angrep hele tiden, men det var et fåtall som hadde hatt noen negative konsekvenser for bedriften.



Figur 11. Spørsmål 9: Har det vært noen tidligere cyberangrep på din bedrift som du kan nevne?

Q10: Virkninger cyberangrep

Det som faktisk kom opp var ransomeware angrep med tap på flere millioner, brudd på leverandører, phishing angrep med tap på rundt 1 million og til slutt en data breach med påfølgende DDoS angrep med begrenset virkning. Når jeg nevner brudd på leverandør refererer jeg til situasjoner hvor en tredjepartsleverandør, som en bedrift samarbeider med eller kjøper tjenester fra, opplever et sikkerhetsbrudd i sine systemer.



Figur 12. Spørsmål 10: Hvilke virkninger hadde cyberangrepet på bedriften?

Diskusjon: **Tidligere cyberangrep/ Virkninger cyberangrep, alle bedrifter**

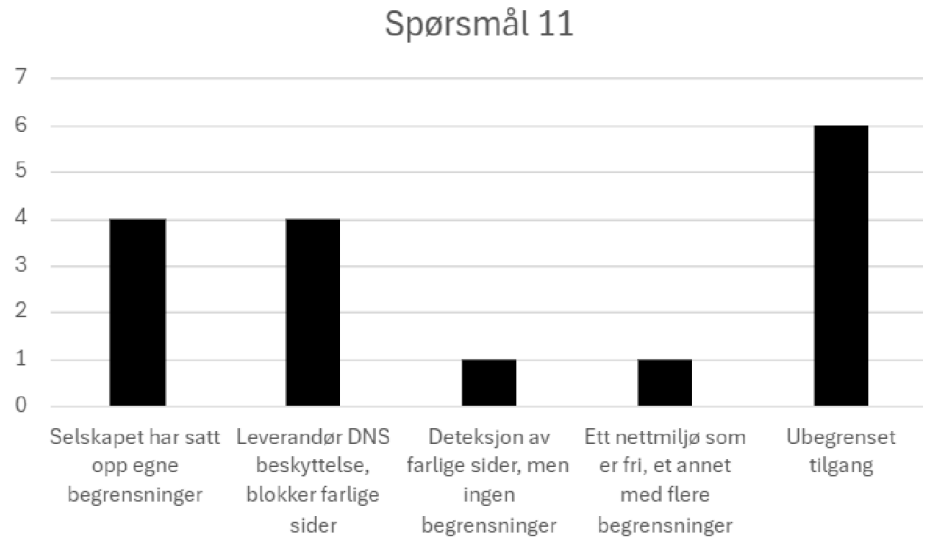
Nesten alle svarene var basert på om det hadde skjedd noen hendelser i perioden intervjuobjektet hadde jobbet der. Lengden på denne perioden varierte veldig. Noen fortalte også om angrep på bedriften fra før de begynte å jobbe der. Så og si alle bedriftene fremhevet at de ble angrepet hele tiden, som oftest var dette gjennom phishing. Det var et lite antall bedrifter som snakket om angrep som hadde hatt noen virkning på dem. Virkningen av cyberangrep omhandler som oftest tap av informasjon, forstyrrelse av forretningsdrift, inntektstap og skade på utstyr (Bendovschi, 2015). DNBs Cyber Defense Center (CDC) la fram sin årsrapport for 2022, der hadde antall cyberangrep økt, men antallet alvorlige hendelser hadde minsket (Loeb, 2023). Dette er resultater som ligner en del på mine, med tanke på hva som blir ytret av bedriftene jeg snakket med. Loeb skriver at i 2022 ble rundt 70 millioner innkommende e-post stoppet fra å nå DNBs ansatte da de var spam eller phishing (Loeb, 2023). Dette var også hovedformen for angrep bedriftene jeg intervjuet opplevde.

I undersøkelsen angående engelske selskaper, svarer 77% at de ikke har opplevd noen tidligere cyberangrep mot bedriftene sine (Erdogan et al., 2023). Av de som visste om angrep som hadde skjedd, var det 12 som sa angrepene endret integriteten til informasjon, 11 angrep gjorde informasjonssystemene utilgjengelige, mens 6 av angrepene førte til brudd på konfidensiell

informasjon (Erdogan et al., 2023). Flere av angrepene som de norske bedriftene i min studie har erfart, kan også relateres til disse kategoriene. Ransomware-angrepet som førte til at et Norsk selskap tapte flere millioner, skyldtes utilgjengeliggjøring av essensielle systemer. DDoS angrepet gjorde det samme med et annet selskap, bare at dette mest sannsynlig ikke var de viktigste systemene deres som ble berørt, og det endte med mindre konsekvenser. Data breachen de også gjennomgikk, endret integriteten til informasjon. Angripere fra utlandet gjenbrukte passord og e-postadresser fra datainnbrudd. Et annet selskap fikk brudd på leverandør der noen hadde tatt over en server og brukt den til mining. Det ble ikke nevnt hva som ble minet, men det vanligste er cryptojacking som er når noen bruker andre personers eller organisasjoners databehandlingskraft for å utvinne kryptovaluta (Jayasinghe & Poravi, 2020). Bruddet på serveren kan utgjøre en risiko for konfidensialiteten til informasjonen som er lagret på serveren, angriper kan få tilgang til sensitiv data som ligger på serveren. Det gjør også systemer utilgjengelig, siden alle ressurser på serveren blir brukt til mining i stedet for å levere de tjenestene den skal.

4.2.10 Q11: Surfe fritt på nettet

Nesten halvparten sier det er ubegrenset og folk kan besøke de sidene de vil, men det er også en hel del som har satt opp egne begrensninger, eller har leverandør som kommer med DNS beskyttelse. Med DNS beskyttelse vil alle sidene leverandøren mener er utrygge, bli blokkert.



Figur 13. Spørsmål 11: Kan de ansatte i bedriften surfe fritt på nettet eller er det begrenset hvilke sider de har tilgang til?

Diskusjon: **Surfe fritt på nettet**

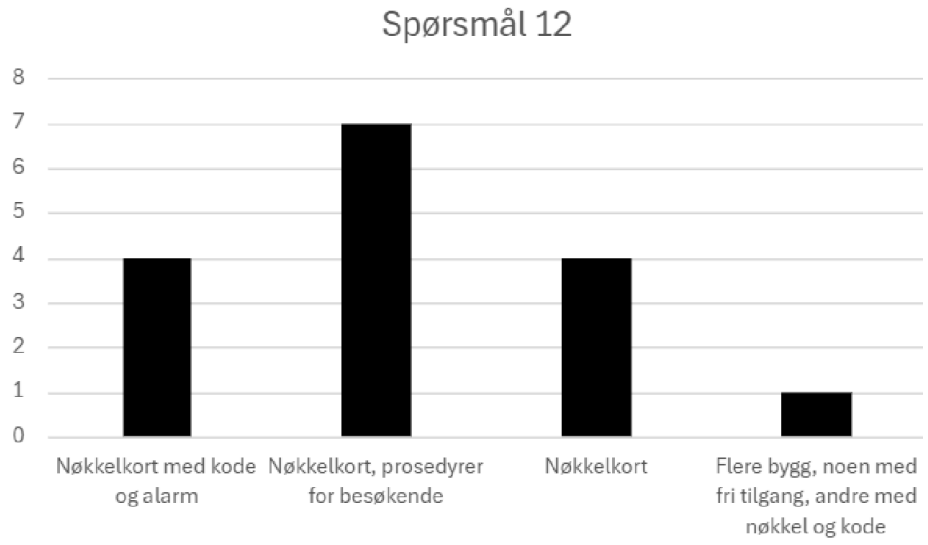
Noen av de seks bedriftene som gir ansatte ubegrenset tilgang, sier dette skal gå på sunn fornuft. Det skal være en kultur som forhindrer ansatte å skade sikkerheten. Andre bedrifter sier det er viktig å ha ubegrenset tilgang fordi jobben krever fri ferdsel på nettet. I den jordanske studien klassifiserer de programvaresikkerheten for minimal (Dahbur et al., 2017), det samme spørsmålet jeg har brukt er med å påvirke denne klassifiseringen. I den studien scoret bedrifter med ubegrenset tilgang, lavest på dette spørsmålet når det gjaldt temaene programvaresikkerhet, bevissthet og retningslinjer (Dahbur et al., 2017). Det kom fram at programvaresikkerhet ikke var det de jordanske bedriftene prioriterte høyest. I min studie har 10 av 16 bedrifter en form for sikkerhet rundt ansattes ferdsel på nettet, noe som kan tilsi at flere norske bedrifter er opptatt av dette aspektet, men programvaresikkerhet er uten tvil et omfattende tema som handler om mye mer enn bare restriksjoner angående nettbruk.

Den jordanske undersøkelsen viste også en korrelasjon mellom retningslinjer og programvaresikkerhet. Når ansatte er bedre informert om organisasjonens sikkerhetspolicy, er de følgelig mindre sårbare for sikkerhetstrusler knyttet til programvaresikkerhet, siden retningslinjene sannsynligvis vil inkludere klare regler for håndtering og sikring av programvare (Dahbur et al., 2017). Som sagt var det seks bedrifter i min undersøkelse som sa de hadde

ubegrenset tilgang, noen stolte for eksempel på kulturen og sunn fornuft. Fra tidligere spørsmål lærte jeg at fire av disse seks selskapene hadde ingen obligatoriske kurs eller opplæring ansatte måtte gjennom, heller ingen faste møter angående cybersikkerhet. Dette gjør det naturligvis vanskeligere å skape en kultur rundt bevissthet og få frem/minne de ansatte på retningslinjene som skal være med på å sikre programvaresikkerheten innad i selskapet.

4.2.11 Q12: Begrenset tilgang

De fleste bruker her nøkkelkort og kode, samtidig som besøkende har egne prosedyrer. Flere bruker bare nøkkelkort eller nøkkelkort med kode pluss alarm. Nesten alle har svart at ansatte eller andre må ha en form for nøkkel for å komme seg inn, det er kun de med et større antall bygg som sier at noen av dem har fri tilgang.



Figur 14. Spørsmål 12: Har folk generelt begrenset tilgang til bedriftens kontorbygg?

Diskusjon: **Begrenset tilgang**

I mine intervjuer sier så og si alle bedriftene at de har ulike former for fysisk sikkerhet. Det er ett selskap som har flere bygg og sier at de har policyer rundt åpenhet for publikum i deler av dem. Noen av bedriftene har mer avanserte typer sikkerhet og nevner en rekke tiltak, andre har bare lås og nøkkel. De fleste selskapene har flere sluser innover i kontorbygget sitt, ansatte har tilgang

basert på stillingen deres. Enkelte hadde også sikkerhetsvakter i lobbyen eller tilgjengelig hvis det skulle skje noe. De norske bedriftene i min undersøkelse viste at dette var en dimensjon de skulle ha kontroll på. I den jordanske undersøkelsen ble bedriftene klassifisert som bra på fysisk sikkerhet (Dahbur et al., 2017). Dette var basert på ikke bare det spørsmålet jeg brukte, men flere som omhandlet dette temaet. De tar opp hvordan fysiske sikkerhetstiltak må implementeres og opprettholdes for å sikre at arbeidsområder er trygge, og for å hindre uautoriserte personer i å få tilgang til begrensede områder (Dahbur et al., 2017).

Teknologien som finnes i de begrensede områdene, har potensial til å bli utnyttet og forårsake skade på selskapet. Den jordanske studien påpeker det å implementere mer avanserte kontroller for fysisk sikkerhet og programvaresikkerhet, er en positiv refleksjon og styrking av generell sikkerhetsbevissthet, spesielt med tanke på sosial manipulasjon og sikkerhetspolicyer (Dahbur et al., 2017). Med sosial manipulasjon menes teknikker som brukes for å få uautorisert tilgang til informasjon gjennom menneskelig interaksjon (Bendovschi, 2015). Både den fysiske sikkerheten og programvaresikkerheten rundt nettbruk, virker å være prioritert for flere av de norske bedriftene jeg intervjuet.

4.3 Sammenligning basert på bedriftsstørrelse

I denne seksjonen diskuterer jeg analysen av resultatene basert på bedriftsstørrelser. Bedriftsstørrelse har ofte stor påvirkning på cybersikkerheten. Det kan påvirke investeringer og kommunikasjon med ansatte rundt temaet. Jeg valgte derfor å gjøre en analyse med utgangspunkt i dette. Dinkova et al. (2023) har målt graden av cybersikkerhetsmodenhet i bedrifter. Det kom fram at modenhetsnivået har en tendens til å øke med bedriftens størrelse (Dinkova et al., 2023). Størrelse kan ha en tendens til å påvirke bevisstheten og tiltakene i et selskap. Dette var en faktor jeg gjerne ville undersøke nærmere.

Kategoriene av størrelse i min analyse er:

- Under 100 ansatte, der var det 5 ulike bedrifter.

- Mer enn 100 ansatte, men mindre enn 1000, der var det 5 ulike bedrifter.
- Mer enn 1000 ansatte, der var det 6 ulike bedrifter.

For å gjøre det mer forståelig, kaller jeg de bedriftene med under 100 ansatte for små bedrifter, de med mer enn 100 ansatte, men mindre enn 1000 for mellomstore bedrifter, og til slutt de med mer enn 1000 ansatte for store bedrifter.

4.3.1 Q1: Kurs eller opplæringsmateriell

Store bedrifter

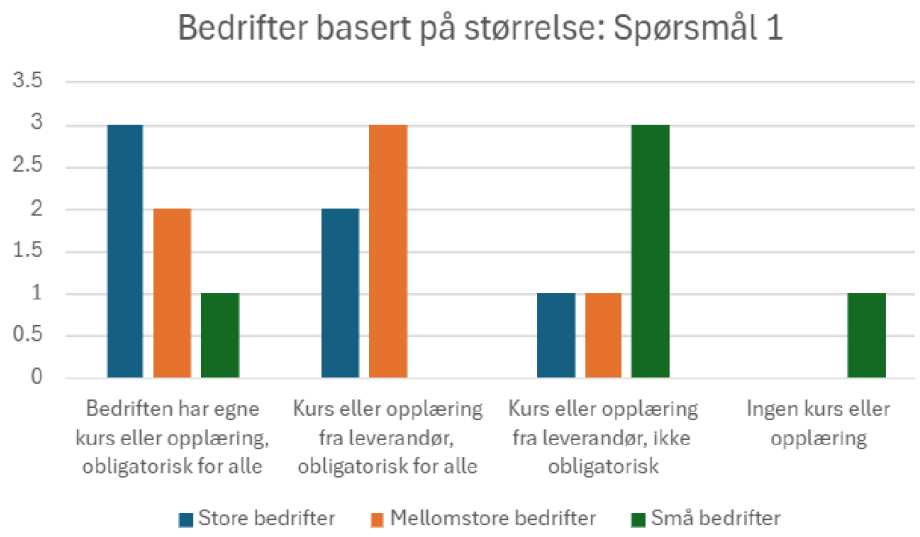
De største bedriftene sier at de har egne kurs eller opplæring. En del har også kjøpt eksterne kurs fra leverandører. Alle ansatte må her gjennom uansett stilling. Det er bare ett stort firma som kjøper eksterne kurs og sier at ikke alle må delta eller gjennomføre.

Mellomstore bedrifter

De mellomstore bedriftene kjøper som oftest kurs, men det er også noen med egne kurs eller opplæring. Her må alle ansatte også gjennom dette uansett stilling. Fra de mellomstore er det også ett av firmaene som igjen sier de kjøper kurs, men at det er frivillig om ansatte vil gjennomføre.

Små bedrifter

De små bedriftene har flest som sier de kjøper eksterne kurs uten at alle de ansatte trenger å delta. Her er det for første gang også et firma som sier de ikke tilbyr noen kurs eller opplæring. Én liten bedrift har egen opplæring alle ansatte må i gjennom.



Figur 15. Svar basert på bedriftsstørrelse, spørsmål 1: Tilbyr din bedrift kurs eller opplæringsmateriell til ansatte for å øke bevisstheten rundt cybersikkerheten?

Diskusjon: Kurs eller opplæringsmateriell, bedriftsstørrelse

På dette spørsmålet er det en klar forskjell fra de store og mellomstore bedriftene til de små, hvor det bare er ett firma som har obligatoriske kurs for alle. Av de mellomstore og store bedriftene, forklarer nesten alle at de har obligatoriske kurs eller opplæring. Et større antall påpeker også at de følger opp resultater og har flere kurs i løpet av året. Huang og Pearlson skriver at de har snakket med flere cybersikkerhetsteam, som har indikert at kun én opplæringsklasse ved oppstart ikke er tilstrekkelig for å opprettholde langsiktige atferdsmønstre (Huang & Pearlson, 2019). Regelmessig og variert opplæring er derfor nødvendig (Huang & Pearlson, 2019). Dette nevner også et av selskapene. De stiller spørsmål rundt hvor ofte og hvilket nivå opplæringen skal ligge på. Av de mellomstore og store bedriftene var det et fåtall som bare snakket om kurs for nye ansatte. De fleste snakket om flere ulike former for kurs ansatte måtte gjennom så lenge de jobbet i selskapet. En av formene for kursing og læring som ble gjentatt relativt ofte, var simulerte phishing- forsøk. De hadde kort varighet og var derfor lettere å få ansatte til å regelmessig gjennomføre.

De små bedriftene har en del ulike svar her. De fleste prioriterer innad i bedriften hvem som bør ha opplæring, og gir de ansatte muligheten til å ta kurs. Ett av selskapene bruker leder til å

videreformidle kunnskapen han eller hun får gjennom foredrag og kurs. Leder tar da med seg info rundt hva som er viktig for bedriften, og snakker med de ansatte om dette. Den mindre bedriften som sier de ikke har kurs eller opplæring, uttrykker at de har andre driftsmessige prioriteringer. Det blir samtidig påpekt at de ansatte ikke har nok forståelse til å gjennomføre kurs rundt dette temaet basert på bransjen de er i.

I den engelske undersøkelsen fokuserer de på bedrifter med mindre enn 250 ansatte, noe som tilsvarer deler av de mellomstore bedriftene og alle de små bedriftene i min undersøkelse. Derfor er de også lettest å relatere til i min studie. Undersøkelsen av de engelske bedriftene viser at bare 19% av dem tilbyr opplæring innen cybersikkerhet for sine ansatte (Erdogan et al., 2023), noe som er ganske annerledes fra de norske bedriftene i min studie der alle utenom ett selskap tilbyr en form for kurs eller opplæring. Hvis man vurderer obligatoriske kurs, er svarene fra den engelske studien ikke så forskjellig fra de små bedriftene i min undersøkelse. Det er likevel en forskjell ved at de engelske selskapene melder om moderat til høy bevissthet (Erdogan et al., 2023). De små norske bedriftene melder derimot om middels til lav bevissthet blant de ansatte. Så svarene deres på spørsmål 6 i mine intervjuer samsvarer mer med svarene rundt kurs og opplæring.

4.3.2 Q2: Stillinger dedikert til cybersikkerhet

Store bedrifter

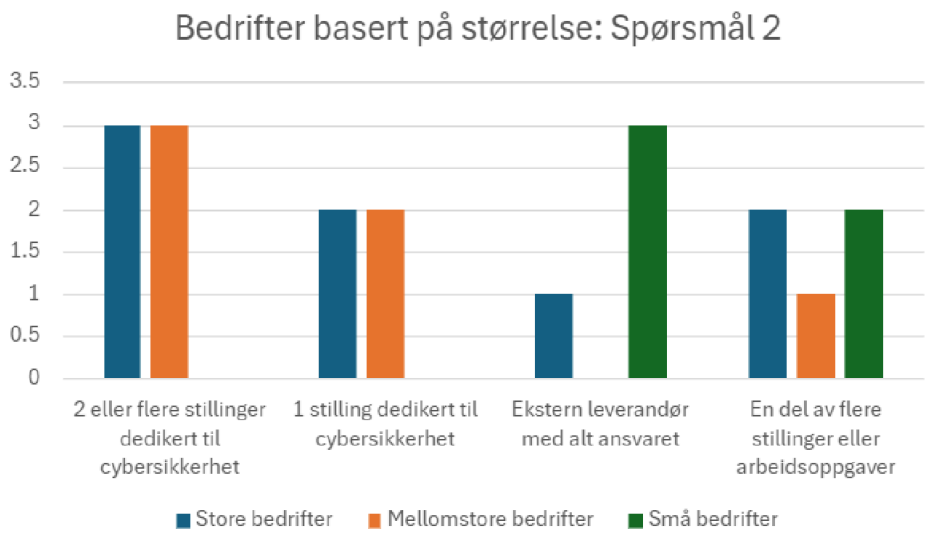
Et større antall av de store bedriftene hadde enten én eller flere stillinger dedikert til cybersikkerhet. Noen hadde også det som en del av stillinger eller arbeidsoppgaver. Ett av selskapene hadde en ekstern leverandør som tok seg av dette for dem.

Mellomstore bedrifter

De mellomstore bedriftene hadde også et stort antall med én eller flere dedikerte stillinger. Det var også et firma som hadde det som en del av flere stillinger eller arbeidsoppgaver.

Små bedrifter

De små bedriftene hadde enten en ekstern leverandør med alt ansvaret rundt dette, eller så var det en del av stillinger eller arbeidsoppgaver.



Figur 16. Svar basert på bedriftsstørrelse, spørsmål 2: Har din bedrift stillinger dedikert til cybersikkerhet?

Diskusjon: Stillinger dedikert til cybersikkerhet, bedriftsstørrelse

På dette spørsmålet var det også et stort sprik fra de mellomstore og store bedriftene til de små selskapene. De små bedriftene sitt hovedargument på dette spørsmålet er at de er for liten til å ha dedikerte stillinger rundt cybersikkerhet, noe som er et velbegrunnet argument med tanke på at de fleste små bedrifter generelt har færre ressurser å investere i informasjonsteknologi og sikkerhet (Wolf et al., 2021). Den økonomiske situasjonen for 2023 og 2024 medfører også lavere investeringsvilje i cybersikkerhetstiltak generelt for norske bedrifter (PwC, 2023). Fra 2022 til 2023 viser også cybercrime survey en 10 prosent nedgang rundt ledelsens fokus på å oppnå den rette balansen mellom de cybertruslene virksomheten står ovenfor og investeringer i cybersikkerhet (PwC, 2023). Spørsmålet er om de små bedriftene jeg intervjuet har valgt riktig med tanke på balanse når de erstatter den dedikerte rollen med å fordele ansvaret til en rekke ansatte, eller gi alt ansvar til en leverandør. Blant de mellomstore og store bedriftene legger flesteparten stor vekt på å ha én eller flere dedikerte stillinger til cybersikkerhet. Ledere må selv

ta ansvar for å velge det som passer bedriften deres med tanke på trusler og økonomi.

Av de engelske bedriftene hadde 1 av 3 selskaper dedikerte stillinger til cybersikkerhet (Erdogan et al., 2023), noe som er et relativt høyt antall med tanke på at det bare er selskaper med mindre enn 250 ansatte. I en annen Europeisk og Amerikansk undersøkelse, fant Dimopoulos et al. (2004) at mindre enn 30 % av småbedrifter og mindre enn 5 % av mikrobedrifter hadde en sikkerhetsadministrator eller noen med formell IT-sikkerhetskompetanse. Mine og utenlandske studier virker å vise til at de fleste små bedrifter ikke prioriterer dedikerte sikkerhetsroller. Så kan selvfølgelig små bedrifter defineres ulikt med tanke på antall ansatte, men mine definisjoner av det er relativt lik kildene som brukes.

4.3.3 Q3: Faste møter

Store bedrifter

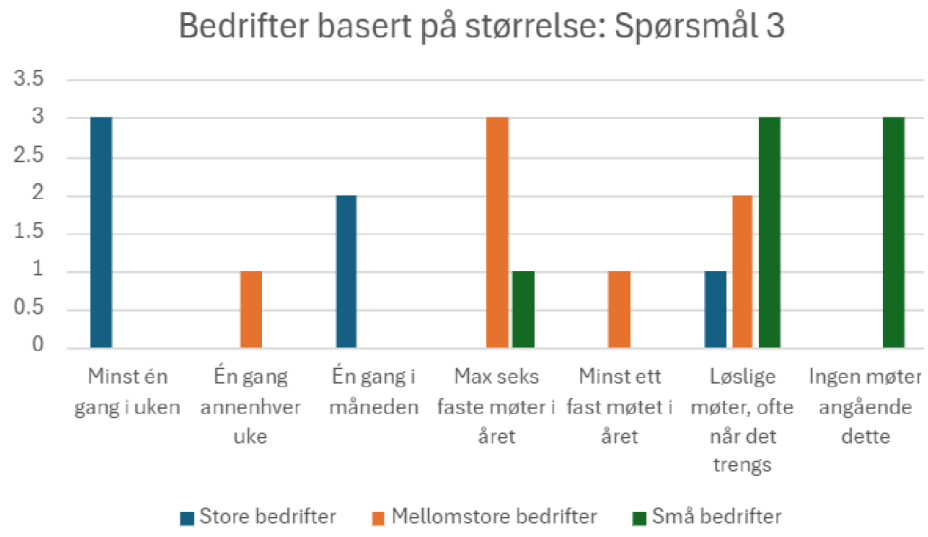
De store bedriftene har stort sett faste møter 1 gang i uken eller måneden. Det var også ett selskap med løselige møter basert på når de trengte det.

Mellomstore bedrifter

De mellomstore bedriftene hadde rundt seks faste møter i året, noen hadde ofte to per kvartal. Her var det også flere med løselige møter når det trengtes. Ett av firmaene hadde møter annenhver uke.

Små bedrifter

De små bedriftene hadde flest som sa de enten ikke hadde noen møter rundt dette eller løselige møter hvis det trengtes. Ett selskap hadde faste møter innad rundt seks ganger i året.



Figur 17. Svar basert på bedriftsstørrelse, spørsmål 3: Har dere faste møter angående cybersikkerhet?

Diskusjon: Faste møter, bedriftsstørrelse

Av de små selskapene sier et klart flertall at de ikke har faste møter angående cybersikkerhet, men tar det opp på møter ved hendelser. Majoriteten av de store bedriftene har faste møter relativt regelmessig. Som oftest er det faste møter mellom ulike former for ledere. For de vanlige ansatte kan det komme opp på ulike møter, men dette virker ganske tilfeldig. Det kan være vanskelig å inkludere alle ansatte i hyppige møter rundt temaet, spesielt hvis selskapet har et høyt antall ansatte. Det å ha cybersikkerhet på dagsordenen i daglig drift vil jo uunngåelig gjøre ansatte mer bevisste på cybersikkerhet (Erdogan et al., 2023). Noen av de mellomstore og store bedriftene i undersøkelsen min nevner at de prøver å flette cybersikkerhet inn der de kan. Dette kan for eksempel være i presentasjoner, kurs eller generelle møter.

Av de engelske selskapene, sier 50% at de diskuterer cybersikkerhet av og til, 36% sier at de aldri diskuterer det innad (Erdogan et al., 2023). Svarene fra de engelske bedriftene minner litt om svarene fra de mindre norske bedriftene. De norske bedriftene som sa de av og til diskuterte cybersikkerhet. Dette gjorde de enten med leverandør eller med det begrensede antallet ansatte de hadde. Noen små selskaper sa at de ikke prioriterte møter rundt dette, og at det nesten aldri ble diskutert.

4.3.4 Q4: Egen kunnskap

Store bedrifter

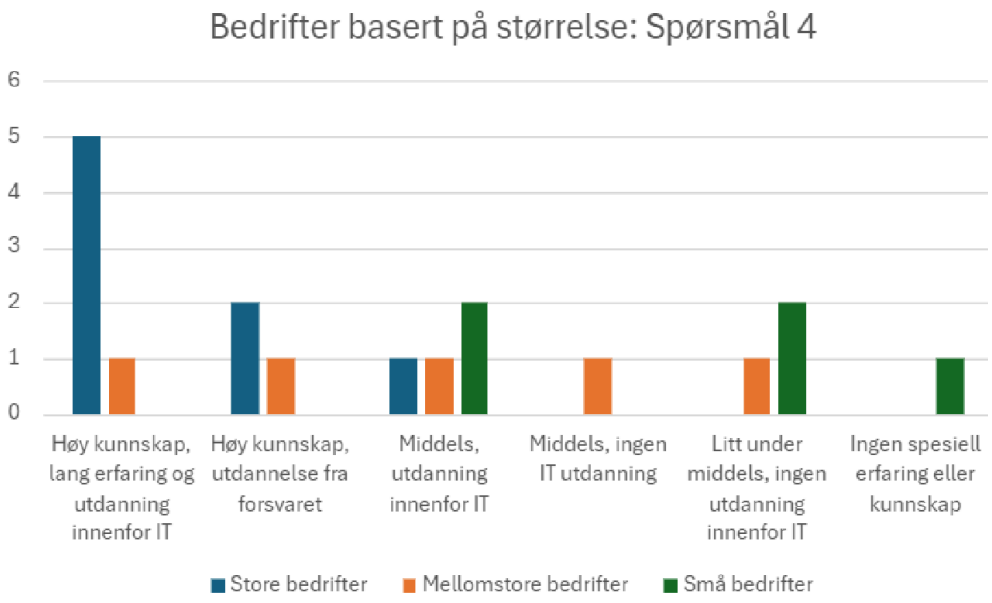
De største bedriftene har nesten bare folk som kategoriserer kunnskapen sin som høy med lang erfaring og utdannelse innenfor IT. Det er også to stykker som har utdannelse fra forsvaret. Bare én fra de store bedriftene sier at de har middels kunnskap rundt cybersikkerhet, selv om de har utdanning innenfor IT.

Mellomstore bedrifter

De mellomstore bedriftene har faktisk bare splittede svar. Det var umulig å plassere folk i samme kategori. To ansatte svarer at de har høy kunnskap, men de har ulike bakgrunner, den ene er fra forsvaret, den andre har lang erfaring og vanlig utdannelse innenfor IT. To andre sier den er middels, ene har utdanning innenfor IT, den andre har ikke. Det er også én person som sier kunnskapen er lav rundt dette temaet og har ingen utdanning innenfor IT.

Små bedrifter

De små bedriftene har flere som sier at de har lav kunnskap rundt cybersikkerhet og ingen IT utdannelse. Like mange sier den middels til bra og har utdanning innen IT. Det er også én person her som sier de har absolutt null kunnskap eller erfaring rundt dette.



Figur 18. Svar basert på bedriftsstørrelse, spørsmål 4: Hvordan vil du karakterisere din egen kunnskap om cybersikkerhet?

Diskusjon: Egen kunnskap, bedriftsstørrelse

Fra de store og mellomstore selskapene var det som oftest en form for CISO eller leder for IT driften som jeg kunne intervjue. De små bedriftene hadde som oftest ikke egne IT avdelinger. En kvalifisert og ansvarlig IT-avdeling er vanlig i store bedrifter, men ikke i små bedrifter (Tam et al., 2021). Dette gjelder dem med under 50 ansatte (Tam et al., 2021), noe jeg har en del av i min studie. Det var ikke veldig overraskende at flere av intervjuobjektene fra de mindre bedriftene hadde begrenset kunnskap rundt nettopp dette.

I den engelske undersøkelsen sier flertallet av de som blir undersøkt, at de har moderat til grunnleggende kunnskap (Erdogan et al., 2023). Så og si halvparten sier den er moderat til ekspert (Erdogan et al., 2023). Blant de mellomstore og små norske bedriftene i min undersøkelse, som kan sammenlignes med de engelske basert på størrelse, er det en overveiende del som svarer at kunnskapen deres er middels til under middels. De engelske bedriftene har altså flere som påstår at de har høyere kunnskap angående dette.

4.3.5 Q5: Frykt for cyberangrep

Store bedrifter

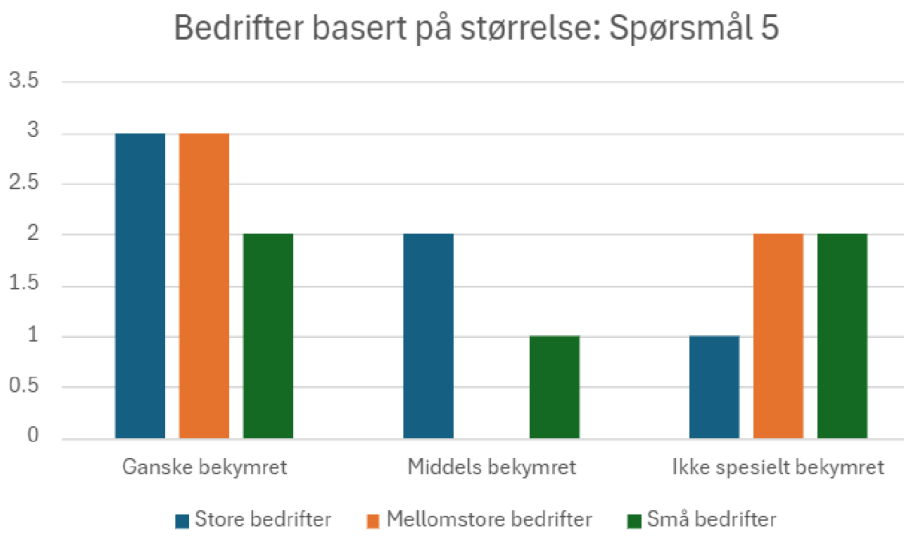
Av de store bedriftene sier de fleste at de er ganske bekymret av flere grunner. Noen andre sier de er middels bekymret. Én person sier de ikke er spesielt bekymret.

Mellomstore bedrifter

Av de mellomstore er det to stykker som sier de ikke er spesielt bekymret og tre andre som påstår de er ganske bekymret. Så relativt jevnt mellom de to kategoriene der.

Små bedrifter

Av de små er det like mange som sier de ikke er spesielt bekymret og ganske bekymret. Én person sier at de er middels bekymret.



Figur 19. Svar basert på bedriftsstørrelse, spørsmål 5: I hvilken grad frykter du for et cyberangrep mot din bedrift?

Delspørsmål 5: Type angrep

På dette spørsmålet var det ransomware og phishing som gikk igjen mest for alle bedriftene. Én mellomstor og én stor bedrift snakker også om statlige angrep. Det samme gjelder organiserte kriminelle med målrettede angrep.

Diskusjon: Frykt for cyberangrep, bedriftsstørrelse

Det er de små og mellomstore bedriftene som snakker mest om at de ikke er spesielt bekymret. Flesteparten som sier dette, mener at det er andre bedrifter som vil være lettere eller bedre mål for angripere. De snakker da om bedrifter med samme størrelser som dem selv, eller bedrifter i samme bransje. Noen nevner også kvaliteten på sine leverandører som grunnen til at de ikke er bekymret. Alt i alt er det flest av de mellomstore og små bedriftene som sier de er ganske bekymret. Dette ligner veldig på svarene til de engelske bedriftene der 60% sier de er moderat til ganske bekymret (Erdogan et al., 2023), men samtidig er det en høy andel som sier de ikke er bekymret (Erdogan et al., 2023).

En studie av Nederlandske selskaper viser at små og mellomstore bedrifter investerer mindre i cybersikkerhet enn store bedrifter, men rapporterer ikke om flere cyberhendelser eller lavere lønnsomhet (Dinkova et al., 2023). Grunnen til dette kan jo være at de små og mellomstore selskapene går under radaren til angripere, noe flere i studien min nevner. De store selskapene i studien min er mer synlig og får antakeligvis flere medieomtaler hvis de opplever negative cyberhendelser. Et av intervjuobjektene fra de store bedriftene fremhever for eksempel oppmerksomhet som en type motivasjon for angripere. Dette hadde media nå skjønt og begynt å tone ned DDoS saker blant annet. Tidligere har jeg snakket om at cyberangrep er mer sannsynlig å forekomme hos selskaper med mindre fokus fra styret på risikostyring (Kamiya et al., 2018). På spørsmålene som omhandler akkurat dette, virker det som at flere av de små selskapene er de som nedprioriterer det. Så det tyder på at uansett størrelse er det elementer som gir grunn til bekymring.

4.3.6 Q6: Organisasjonens cybersikkerhetsbevissthet

Store bedrifter

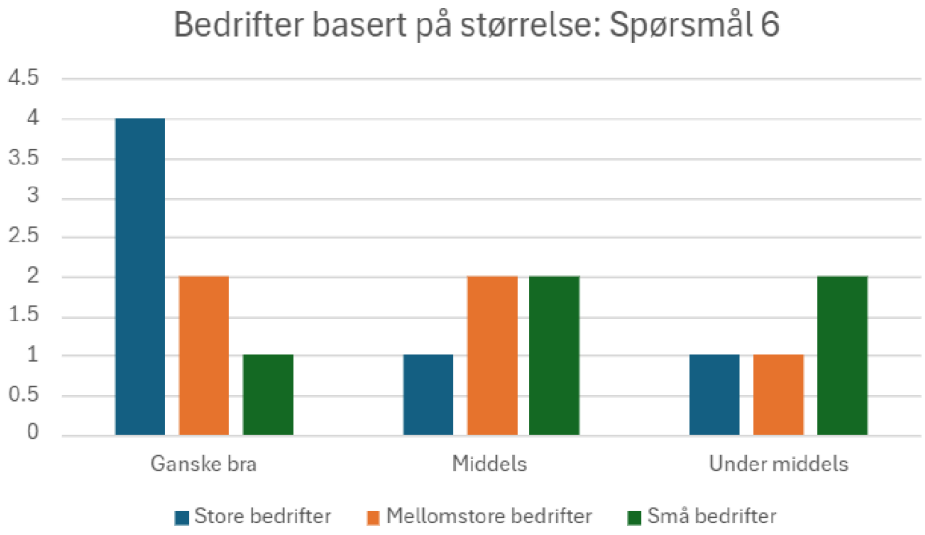
De store bedriftene svarer klart mest at den er ganske bra.

Mellomstore bedrifter

De mellomstore bedriftene svarer splittet mellom middels og ganske bra, utenom én som sier den er ganske lav.

Små bedrifter

De små bedriftene bytter om dette og svarer splittet mellom middels og ganske lav. Utenom én som sier den er ganske bra.



Figur 20. Svar basert på bedriftsstørrelse, spørsmål 6: Hvordan vil du karakterisere organisasjonen når det kommer til cybersikkerhetsbevissthet?

Delspørsmål Q6: Modenhetsmodeller

Store bedrifter

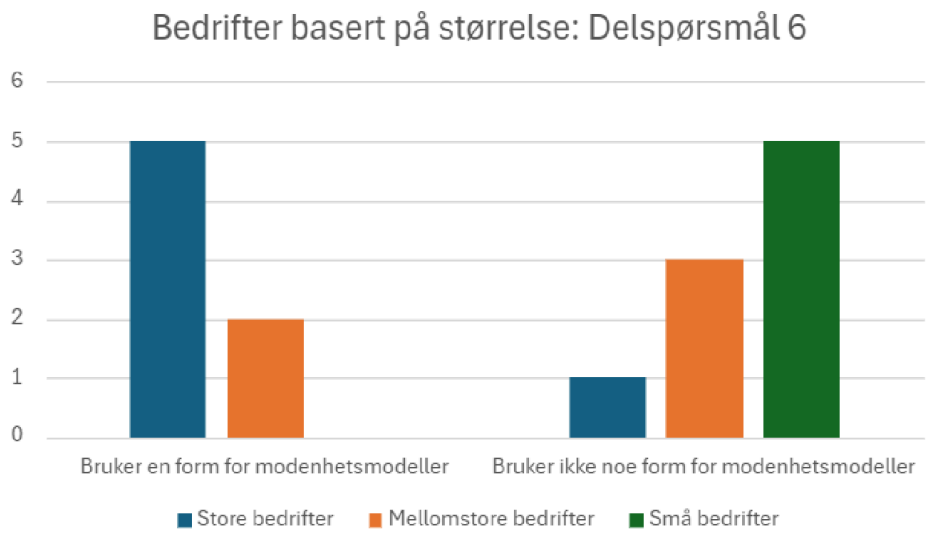
Av de største bedriftene bruker alle utenom én bedrift en form for modenhetsmodell.

Mellomstore bedrifter

Av de mellomstore bedriftene er det flest som ikke bruker noe form for modenhetsmodeller. Det er nesten like mange som bruker det.

Små bedrifter

Av de små bedriftene er det ingen som bruker modenhetsmodeller.



Figur 21. Svar basert på bedriftsstørrelse, delspørsmål 6: Bruker dere noen form for modenhetsmodeller?

Diskusjon: Organisasjonens cybersikkerhetsbevissthet/ Modenhetsmodeller, bedriftsstørrelse

Av de små bedriftene er det ingen som bruker en form for modenhetsmodeller. Samtidig sier et klart flertall at bevisstheten innad er middels til under middels. De store og mellomstore sier den er middels til ganske bra. Av de store bruker nesten alle en form for modenhetsmodeller, noe som gjør svarene relativt sikre. Dette gjelder ikke for flesteparten av de mellomstore bedriftene.

I studien av de engelske bedriftene, sier 54% at den er moderat og 26% at bevisstheten er høy (Erdogan et al., 2023). Dette er ganske annerledes fra de små bedriftene i min studie, som er mer på andre siden av skalaen. På spørsmål 1 i min studie er det et fåtall små bedrifter som har obligatoriske kurs eller opplæring for ansatte, som understreker deres utsagn om lav bevissthet blant de ansatte. Opplæring fremmer selvfølgelig bevisstheten om informasjonssikkerhet og informerer brukere om viktigheten av informasjonssikkerhet (Huang & Pearlson, 2019). De engelske selskapene har også bare 19% som tilbyr trening eller opplæring (Erdogan et al., 2023), men i motsetning til de små norske bedriftene kategoriserer de bevisstheten som moderat til høy. De små selskapene i min undersøkelse ser ut til å ha en forståelse for at tiltak er nødvendig for å

kunne påstå at bevisstheten er høy.

Flere av de store selskapene, og noen mellomstore, snakker om kartlegging via NSM (Nasjonal sikkerhetsmyndighet) sine grunnprinsipper på spørsmål 6. NSM har utarbeidet konkrete anbefalinger til sikkerhetsarbeid. De skal være relevante for alle virksomheter (Didgir, u.å.). Dette er en oppskrift som ikke bare de større bedriftene kan bruke, men også de mindre selskapene. Ved hjelp av prinsippene til NSM er det mulig å måle modenheten sin, men NSM har utelatt bevissthetskomponenten fra prinsippene sine, noe også ett av intervjuobjektene mine tar opp. Så ved bruk av denne som en modenhetsmodell, vil den ikke inkludere de ansattes bevissthet. Intervjuobjektet som nevner dette, sier at de bruker phishing trening blant annet for å måle bevisstheten. NSM sine grunnprinsipper pluss egne tester har etter hvert vist seg å gi gode resultater. Selskapene kan altså ikke bare bruke NSM sine grunnprinsipper for å måle hele modenhets aspektet. Slik noen av de store og mellomstore bedriftene ga inntrykk av i intervjuene mine.

4.3.7 Q7: Nedetid kritiske applikasjoner og systemer

Store bedrifter

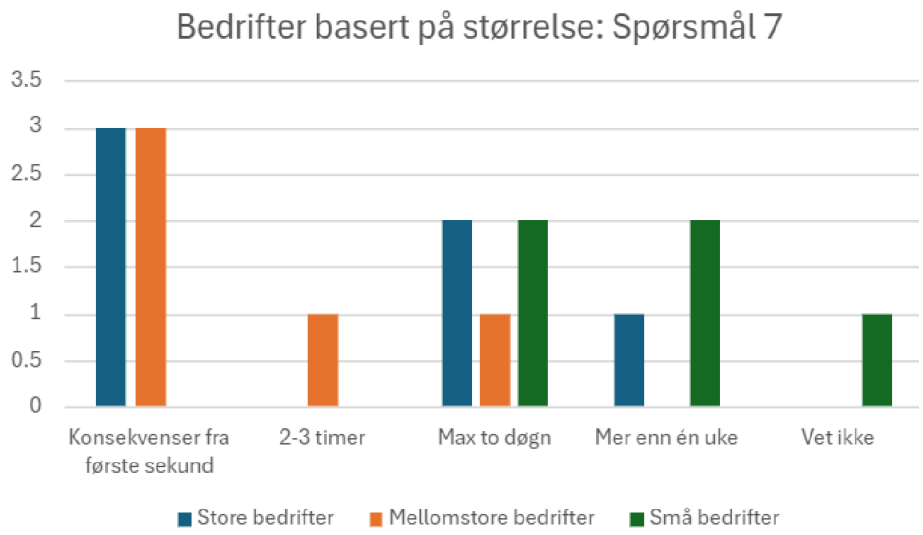
De største bedriftene har flest som sier de får betydelige konsekvenser fra første sekund. Det er nesten like mange som sier at rundt to døgn ville gått greit. Ett selskap sier at de kunne klart seg i mer enn én uke.

Mellomstore bedrifter

De mellomstore bedriftene sier også flest ganger at de får større konsekvenser fra første sekund. Her er det også én bedrift som tåler rundt to døgn, i tillegg til én annen som sier de hadde klart seg et par timer.

Små bedrifter

De små bedriftene har veldig splittede svar, men det som går mest igjen er mer enn én uke eller max to dager. Her er det også noen som ikke vet og ikke greier å svare på spørsmålet.



Figur 22. Svar basert på bedriftsstørrelse, spørsmål 7: Hvor lenge tror du at de kritiske applikasjonene og systemene kan være nede før det får betydelige konsekvenser?

Diskusjon: Nedetid kritiske applikasjoner og systemer, bedriftsstørrelse

Det er interessant å høre at de små selskapene generelt tåler å være lenger uten kritiske systemer eller applikasjoner. De store og mellomstore bedriftene snakker mest om omdømme og at det blir kritisk veldig fort, men dette blir ikke nevnt mye av de små. De tar opp fakturering og regnskap som det mest kritiske, penger må komme inn for at bedriften skal gå rundt.

De engelske selskapene er på samme størrelse som de små og deler av de mellomstore selskapene i min undersøkelse. De engelske virksomhetene er ganske spredt i sine svar, men nesten halvparten sier de kunne klart seg én dag eller mindre (Erdogan et al., 2023). Det er bare 29% som svarer mer enn én dag og 22% sier de ikke vet (Erdogan et al., 2023). Så det er et stort antall med kritiske systemer som ikke kan være lenge nede. De små norske bedriftene i min undersøkelse ser ut til å klare seg lenger uten slike systemer. Det er vanskelig å se hvorfor, men de små norske selskapene virker til å ha en form for beredskapsplan hvis noe skulle skje. Noen har forberedt seg ganske nøye og har en plan for alt de skal gjøre. Dette har de gjort alene eller via leverandør. Andre har programmer eller systemer klare til å erstatte de utilgjengelige. Dette kan være en av grunnene til at de små norske bedriftene er mer selvsikker angående tidsperspektivet.

Kritiske systemer virker å være ekstra beskyttet hos flere av de store og mellomstore bedriftene. En god del har nulltoleranse for nedetid som gjør at dette er naturlig. Noen av de største selskapene er underlagt særskilte krav og det er ofte begrenset tilgang til de kritiske systemene. Mange selskaper står overfor den utfordrende oppgaven med å vedlikeholde flere identiteter og legitimasjoner på tvers av organisasjonens teknologiske infrastruktur (Mohammed, 2011). De store og mellomstore bedriftene har mange ansatte og må hele tiden ha kontroll på hvem som har tilgang til hva. Dette gjelder både fysisk og via teknologi. Hvis samtlige ansatte har tilgang til alle systemer i et stort selskap, kan det gjøre kritiske systemer mer utsatt. Huang & Pearlson (2019) har et eksempel som underbygger dette, i 2017 opplevde ulike finansfirma tilfeller av målrettede phishing-e-poster rettet mot spesifikke enkeltpersoner med tilgang til bedriftens systemer. Flere ansatte med nøkkelen gir også flere mål for angriperne. Selv med de mest avanserte verktøyene, kan sårbarheten skapt av menneskelig feil eller hensikt, noen ganger gjøre teknologiske forsvarsverk rett og slett utilstrekkelige (Huang & Pearlson, 2019). Begrenset tilgang til kritiske systemer vil alltid være en ekstra beskyttelse, og ble prioritert av en rekke store og mellomstore bedrifter i mine undersøkelser.

4.3.8 Q8: Identifisering av cybersikkerhetssårbarheter

Store bedrifter

Av de store bedriftene er det flest som bare bruker leverandør til å gjøre dette. Så kommer de som bruker både egne og leverandører samtidig. Det er også et selskap som snakker om at de bruker innebygde systemer fra Microsoft og sine egne verktøy.

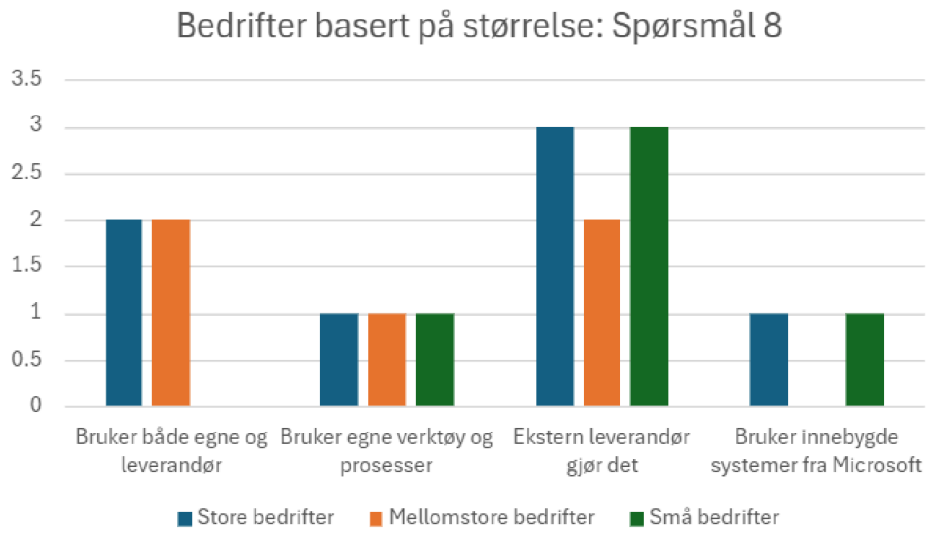
Mellomstore bedrifter

Blant de mellomstore bedriftene er det like mange som benytter både interne ressurser og eksterne leverandører som kun bruker eksterne leverandører. Et av selskapene bruker også sine egne verktøy og prosesser.

Små bedrifter

Av de små bedriftene er det flest som har eksterne leverandører som fikser dette for seg. Her er

det også ett av selskapene som snakker om innebygde systemer fra Microsoft.



Figur 23. Svar basert på bedriftsstørrelse, spørsmål 8: Bruker din bedrift spesifikke prosesser eller verktøy for å identifisere cybersikkerhetssårbarheter?

Diskusjon: Prosesser eller verktøy identifisere cybersikkerhetssårbarheter, bedriftsstørrelse

Nesten alle de store bedriftene har en SOC via leverandør. Dette viser seg å være det viktigste verktøyet de har for å oppdage sårbarheter. Det er også noen mellomstore selskaper som bruker dette, men de fleste snakker om ulike verktøy fra leverandør. Av de små bedriftene bruker de fleste leverandør, men det virker ikke som alle helt forstår hva de gjør for dem. Leverandørene skriver på fagspråk til dem, som gjør det vanskelig for ledere eller ansatte uten IT- bakgrunn å skjønne. Leverandørene kan eventuelt sette seg ned med kundene og deretter forklare verktøy og retningslinjer på en forståelig måte. Dette kan vise seg å være den mest effektive tilnærmingen. Det er bare én av de små bedriftene som sier de har hatt flere møter med leverandør og skal møte dem igjen for oppfølging. Noen av de små bedriftene gir inntrykk av at så lenge leverandøren er et større anerkjent selskap, trenger de ikke ha kontroll på det som blir gjort for dem.

I undersøkelsen av jordanske bedrifter fra 2012 til 2017, hadde kategorien sikkerhetsprogrammer gått ned fra 54% til 42% (Dahbur et al., 2017). Det var altså et minkende fokus på programmer som kan oppdage sårbarheter. Alle de store og mellomstore bedriftene i min undersøkelse viser

til metoder og systemer som skal hjelpe de med dette, det virket til å ligge høyt på listen av prioriteringer.

Av de engelske selskapene svarer 62% at de ikke bruker noen programmer til dette, og 23% vet ikke om de gjør det (Erdogan et al., 2023). Selv om flere av de små bedriftene i mine intervjuer ikke forstår alt som skjer, er de sikre på at de har programmer som skal hjelpe dem. Noen har selvfølgelig tatt flere forhåndsregler enn andre. Med mer avanserte systemer via leverandør eller noe de har bygget selv.

4.3.9 Q9: Tidligere cyberangrep

Store bedrifter

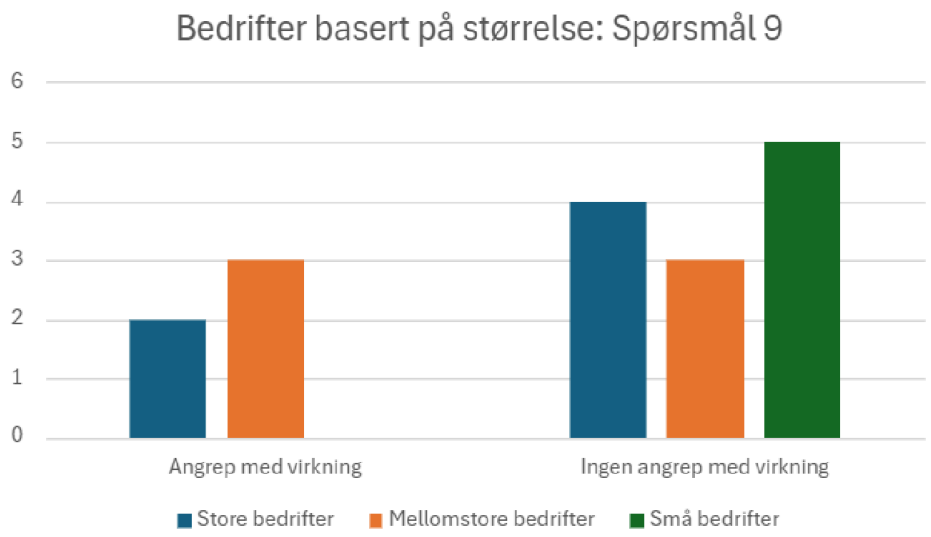
Mesteparten av de store bedriftene hadde ikke opplevd noen angrep med virkning på dem.

Mellomstore bedrifter

Av de mellomstore bedriftene var det flest som ikke hadde opplevd angrep med virkning, men nesten like mange snakket om brudd på leverandører. Det var også ett av selskapene som hadde opplevd DDoS angrep og data breach, men med begrenset virkning.

Små Bedrifter

Av de små selskapene hadde ikke noen opplevd angrep med noe spesiell virkning.



Figur 24. Svar basert på bedriftsstørrelse, spørsmål 9: Har det vært noen tidligere cyberangrep på din bedrift som du kan nevne?

Q10: Virkninger cyberangrep

Store bedrifter

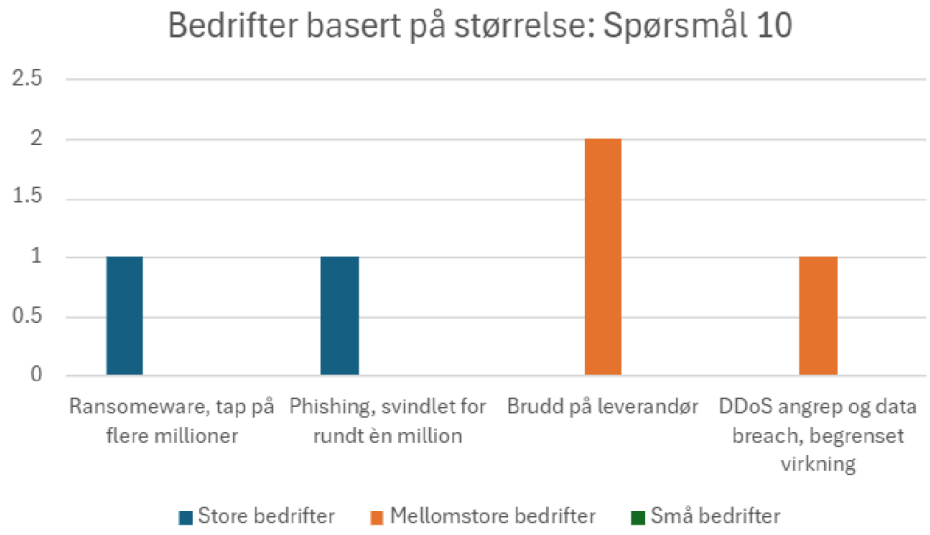
Det var en bedrift som hadde opplevd et ransomware angrep hvor de tapte flere millioner, og et annet selskap som hadde opplevd et phishingangrep med tap på rundt én million.

Mellomstore bedrifter

To selskap har opplevd brudd på leverandører. Det var også ett selskap som hadde opplevd DDoS-angrep og data breach, men med begrenset virkning.

Små bedrifter

Ingen vellykkede angrep på dem.



Figur 25. Svar basert på bedriftsstørrelse, spørsmål 10: Hvilke virkninger hadde cyberangrepet på bedriften?

Diskusjon: **Tidligere cyberangrep/ Virkninger cyberangrep, bedriftsstørrelse**

Det er altså ingen små selskaper i min undersøkelse som har opplevd angrep med virkning. To av de store selskapene som har blitt rammet av angrep, har også opplevd de største tapene som følge av det. De mellomstore bedriftene har opplevd flest angrep med virkning. Den store bedriften som tapte mange millioner på grunn av ransomware angrep, påpeker at det gjorde bedriften mye mer fokusert på cybersikkerheten og personvern. Det har skapt et vedvarende fokus på at det ikke skal skje igjen. Det mellomstore selskapet som opplevde DDoS angrep og data breach, sier noe ganske likt. De fikk tettet hull i systemer og oppdaget at DDoS beskyttelsen ikke var optimal på noen tjenester. Så det har ikke bare vært negative konsekvenser fra angrepene. De har brukt dem til å gjøre nødvendige endringer og forbedringer.

De små bedriftene har ikke opplevd noen vellykkede angrep. Dette kan forsterke argumentene til de små bedriftene som sa de ikke var veldig bekymret, av de engelske selskapene med noenlunde samme størrelse var det bare 15% som svarte at de hadde opplevd angrep (Erdogan et al., 2023). Det er studier som antyder at vellykkede angrep er noe flere må forvente, i 2017 sa kommisjonen for mindre bedrifter i New South Wales Australia at 60% av små og mellomstore bedrifter ville bli påvirket av en cybersikkerhetshendelse (Millaire et al., 2017). Betydelig mer enn halvparten av alle cyberangrep er rettet mot små og mellomstore bedrifter, dette antallet øker jevnt, de kan

tilby mange av de samme gevinstene og bruker mye mindre ressurser på cybersikkerheten (Millaire et al., 2017). Derfor vil det alltid være mulig å se de små og mellomstore bedriftene sin sak fra ulike sider.

4.3.10 Q11: Surfe fritt på nettet

Store bedrifter

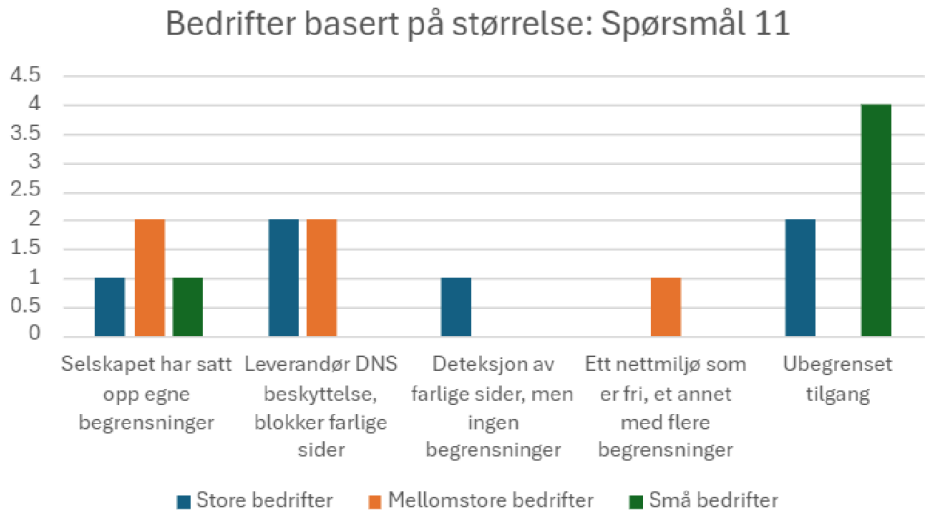
De største bedriftene hadde flere som enten hadde ubegrenset tilgang eller DNS beskyttelse fra leverandør som blokkerte sider. Ett selskap hadde deteksjon av farlige sider, men ingen begrensninger. Et annet hadde begrensninger laget av selskapet selv.

Mellomstore bedrifter

Av de mellomstore var det flest som enten hadde DNS beskyttelse fra leverandør eller begrensninger laget av selskapet selv. Ett selskap hadde ulike nettmiljø, et som var fri og et som var begrenset.

Små bedrifter

De små bedriftene hadde nesten bare ubegrenset tilgang, utenom én bedrift som hadde egne begrensninger.



Figur 26. Svar basert på bedriftsstørrelse, spørsmål 11: Kan de ansatte i bedriften surfe fritt på nettet eller er det begrenset hvilke sider de har tilgang til?

Diskusjon: **Surfe fritt på nettet, bedriftsstørrelse**

De store bedriftene som sier de har ubegrenset tilgang på nettsider, uttrykker at dette er av ulike grunner. Den ene bedriften stoler mer på kulturen innad og at alle ansatte følger deres retningslinjer. Denne bedriften svarer også på spørsmål 6 at bevisstheten i bedriften er ganske bra. Den andre bedriften bemerker at jobben krever et åpent nettmiljø, men melder om lav bevissthet via modenhetsmodellene de bruker. Ansattes bevissthet er viktig for å opprettholde retningslinjer angående et fritt nettmiljø. De små selskapene med ubegrenset nettbruk gir ikke noe spesiell utdypning rundt hvorfor. Det kan tyde på at de små bedriftene ikke prioriterer dette, og at de akkurat nå stoler på de ansattes egne vurderinger. Her er det imidlertid også flere av dem som svarer at bevisstheten er middels til lav på spørsmål 6. Alle de mellomstore bedriftene har en form for begrensninger og virker å ta det veldig på alvor. Enkelte av dem svarer at de krever at jobb- PC ikke blir brukt i privat sammenheng.

Det er interessant å høre noen av de mellomstore og store bedriftene snakke om de ansattes mobiler på dette spørsmålet. Her er det meget forskjellige svar. Noen har samme begrensninger på mobilen som PC-en, andre har ignorert mobilen på dette punktet. Andre har ekstra beskyttelse rundt mobilen. Et intervjuobjekt fra en mellomstor bedrift sier at det er vanskeligere å regulere en mobiltelefon og sentralisere styringen av bruken. Det blir nevnt at det blir en slags blanding av privat bruk og jobbruk via mobiltelefonen. Et annet intervjuobjekt fra en stor bedrift svarer at skille mellom privatperson og ansatt er mye mer visket ut enn det var tidligere. For mange tenker jo at når de går fra jobb, så går de fra jobb, men de gjør jo egentlig ikke det, de har med seg jobb på mobilen og jobb- PCen hjem for eksempel. Et selskap nevner at de setter opp alternative løsninger når ansatte skal på jobbreiser til visse land. De får ikke ha med egen mobil eller PC.

Ansatte kan bruke sine personlige telefoner til å få tilgang til ulike arbeidsrelaterte funksjoner. For eksempel bedriftens mobilapplikasjoner, kontaktinformasjon for selskap og ansatte, eller laste ned forretningsdokumenter (Ameen et al., 2021). Noen av de store og mellomstore bedriftene i min studie, hadde implementert restriksjoner mot deler av dette. Disse funksjonene gjør sikkerheten til telefoner til et enda mer pressende problem (Ameen et al., 2021). McAfee sin rapport fra 2018 melder at sikkerheten til telefoner kan bli kompromittert av ulike trusler som tap

av enheten, angrep via operativsystemet (Android eller Apple iOS), usikre nettverk, svake autentiseringsprosesser, dårlig datasikkerhet, utilstrekkelig personvern, virus, skadelig programvare og SMS-baserte angrep (McAfee, 2018). Så mobilen er et viktig aspekt når det gjelder sikkerhet. Den blir stadig mer ansett som en datamaskin, som et av intervjuobjektene mine påpeker. Nesten alle de små selskapene i intervjuene mine oppgir ingen informasjon angående sikkerhet rundt mobil, men det virker lite sannsynlig at de har noen begrensninger her, basert på at nesten ingen har begrensninger på de ansattes PCer. Det er bare ett lite selskap med like begrensninger på mobil og PC. Et mellomstort selskap svarer faktisk at de har større begrensninger på mobilen enn PC. Dette er basert på at de ikke trenger visse mobil funksjoner til arbeidet, og derfor er det sperret av. Tiltak ut fra nytte kan være en smart vei å gå når det gjelder sperring av potensielle trusselvinduer.

4.3.11 Q12: Begrenset tilgang

Store bedrifter

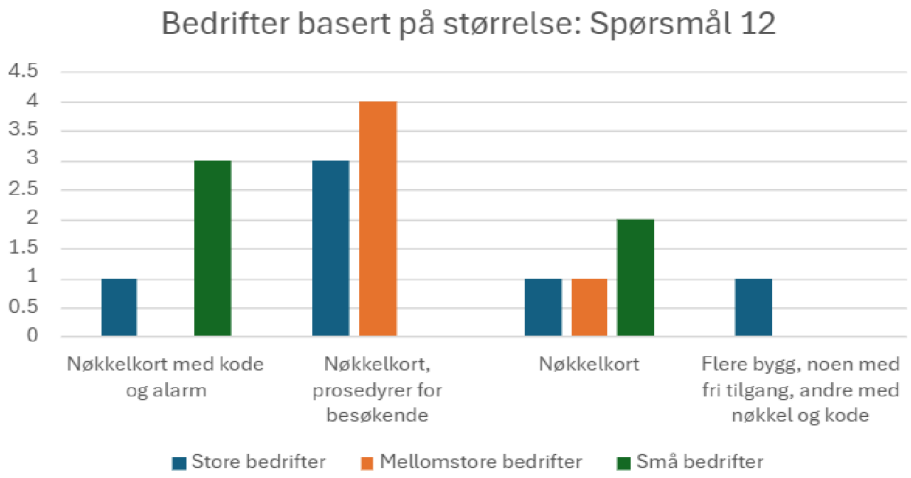
Av de store bedriftene sa de fleste at de hadde nøkkelkort. Besøkende hadde egne prosedyrer. Noen brukte nøkkelkort og alarm, andre hadde flere bygg der det var fri tilgang til noen av dem.

Mellomstore bedrifter

De mellomstore bedriftene hadde flest som sa de brukte nøkkelkort samtidig som besøkende hadde egne prosedyrer. Ett selskap brukte bare nøkkelkort.

Små bedrifter

De små nevnte mest nøkler og kode pluss alarm. To bedrifter sa de bare brukte nøkkelkort.



Figur 27. Svar basert på bedriftsstørrelse, spørsmål 12: Har folk generelt begrenset tilgang til bedriftens kontorbygg?

Diskusjon: **Begrenset tilgang, bedriftsstørrelse**

Alle selskapene hadde en form for fysisk sikkerhet. En del av de mellomstore og store bedriftene hadde prosedyrer for besøkende. De har også større lokaler og flere har tilgangskontroll på ulike etasjer eller viktige rom. De små selskapene har åpenbart mindre kontorer. Ingen av dem snakker om prosedyrer for besøkende, men besøkende virker heller ikke som noe de pleier å ha. Et lite selskap sa de hadde som rutine å låse skjermene på datamaskinene når de forlot kontorene, noe ingen andre selskaper i undersøkelsen min snakket noe om.

Mesteparten av de små, store og mellomstore selskapene har en type deteksjonsmidler ifølge intervjuene mine. NSM sine grunnprinsipper for fysisk sikkerhet påpeker at en viktig understøtte av barrierer, er deteksjonsmidler i form av ulike sensorer som IR, termisk, kamera eller bevegelse (NSM, 2020). Mange av de store og mellomstore selskapene sier de følger disse prinsippene. At de har dette er dermed ikke veldig overraskende, men det er også tre av fem små bedrifter som har en versjon av dette. Et lite selskap har også opprettet flere barrierer innover i lokalet sitt. Dette virker normalt for de mellomstore og store selskapene med større bygg, men ikke for de andre små bedriftene. Fysiske barrierer bør opprettes der det er behov for å fysisk hindre eller forsinke en trusselaktør (NSM, 2020). De små bedriftene må hele tiden ta vurderinger rundt trusselbilde og om det er mulig å gjøre kontorene enda sikrere basert på dette.

4.4 Sammenligning av offentlige og private bedrifter

Private og offentlige selskaper er en annen faktor jeg ville undersøke. Offentlige selskaper har en tendens til å ha mer stabile budsjett tilegnet cybersikkerhet. De private er kanskje mer varierende rundt budsjetteringen basert på bransje og størrelse. Offentlige bedrifter er vanligvis underlagt strengere krav til cybersikkerheten, basert på at de kanskje håndterer mer sensitive data. Cybersikkerhetskulturen til de private kan variere mer ut fra ledelsens engasjement. Dette er bare noen få av grunnene til at jeg vil se nærmere på offentlige og private selskaper.

Denne analysen er basert på de offentlige og private bedriftene jeg intervjuet. Det var til sammen 5 offentlige og 11 private bedrifter jeg snakket med.

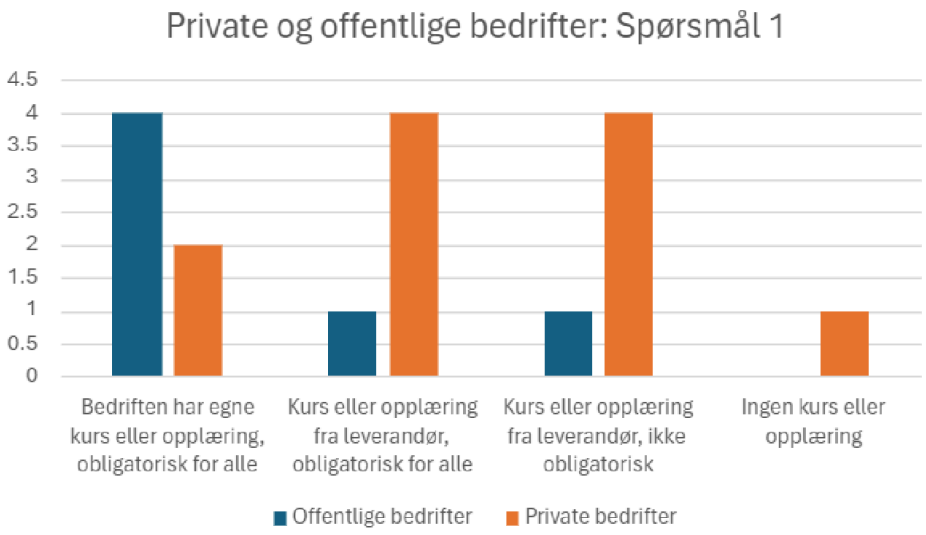
4.4.1 Q1: Kurs eller opplæringsmateriell

Offentlige bedrifter

Av de offentlige var det klart flest som sa de hadde egne kurs som alle de ansatte måtte i gjennom. Toppledelse inkludert. Det var også to bedrifter som kjøpte kurs. For det ene selskapet var det obligatorisk. Det andre hadde egne kurs som var obligatorisk, men det som var kjøpt av leverandør var frivillig.

Private bedrifter

Av de private var det flest som kjøpte kurs eller opplæring av leverandør. Det var like mange som gjorde dette frivillig som obligatorisk. Det var noen som hadde egne obligatoriske kurs og én bedrift som ikke tilbød noe som helst form for opplæring eller kurs.



Figur 28. Svar basert på offentlige og private bedrifter, spørsmål 1: Tilbyr din bedrift kurs eller opplæringsmateriell til ansatte for å øke bevisstheten rundt cybersikkerhet?

Diskusjon: Kurs eller opplæringsmateriell, private og offentlige

De offentlige bedriftene snakket klart mest om egne kurs og opplæring som alle måtte gjennom. De private bedriftene prioriterte kurs eller opplæring via leverandør. Det var også flere som sa det var frivillig å ta kurset/opplæringen. En rekke av de private selskapene sier de har kurs basert på den ansattes rolle. Vanlige ansatte får ofte bare generelle kurs. Ofte er det bare en del av bedriften som har obligatoriske kurs. Noen svarer at de ikke tvinger alle ansatte til å ta kursene, men at de er opptatt av det. Av de offentlige bedriftene er det nesten ingen som sier de spesifiserer kursene. Her er nesten alle kursene eller opplæringen obligatorisk, men kursene er mer generelle. Så å si alle de offentlige selskapene gjentar kursene sine. Noen gjentar de annethvert år, andre sender de ansatte gjennom dem relativt ofte med kort varighet på kursene. Av de private bedriftene er det bare et fåtall som svarer at kursene blir gjentatt. En undersøkelse som ble gjort rundt kurs for ansatte, fant ut at etter å ha deltatt hadde ansatte generelt en tendens til å glemme 50% av informasjonen i løpet av en time, 70% av informasjonen var glemt innen 24 timer og 90% innen én uke (Kohn, 2014). Derfor kan det være avgjørende at opplæring i bevissthet integreres i de ansattes daglige oppgaver, for å støtte oppbevaring og anvendelse av den oppnådde kunnskapen (Ghafir et al., 2018).

Q2: Stillinger dedikert til cybersikkerhet

På spørsmål 2 svarer begge ganske likt, det er fem selskap som har én dedikert stilling eller mer fra både de offentlige og private. De private har også mange ansatte som har det som en del av stillingen sin, eller en ekstern leverandør som har ansvaret for det.

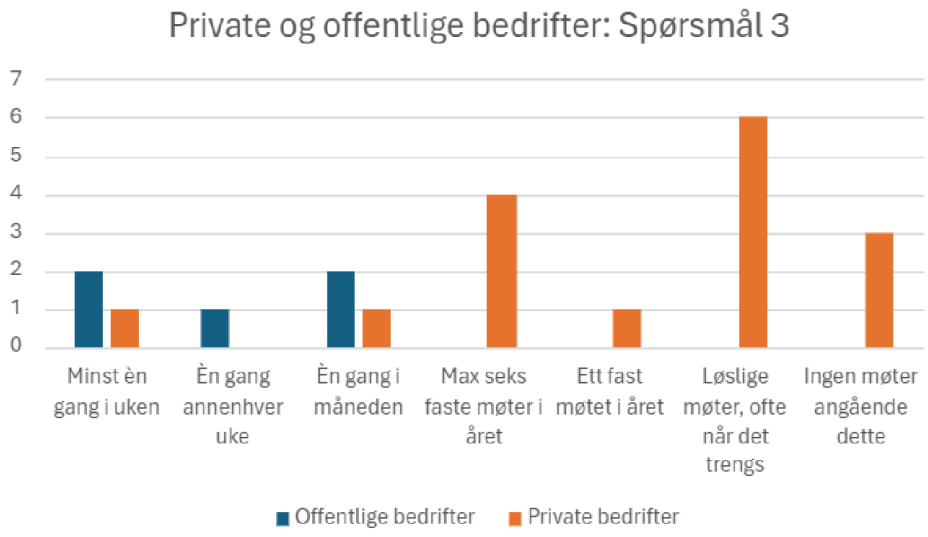
4.4.2 Q3: Faste møter

Offentlige bedrifter

De offentlige bedriftene sa flest ganger at de hadde faste møter én gang i uken eller én gang i måneden. Det var også én bedrift som hadde et møte annenhver uke.

Private bedrifter

Det som ble sagt mest av de private bedriftene var at de hadde løselige møter etter behov. Det var også mange som hadde rundt seks faste møter i året. Et større antall her sa også at de ikke hadde noen møter rundt dette.



Figur 29. Svar basert på offentlige og private bedrifter, spørsmål 3: Har dere faste møter angående cybersikkerhet?

Diskusjon: Faste møter, private og offentlige

De offentlige bedriftene virket til å ha oftere møter enn de private angående dette temaet. Mesteparten av de private bedriftene har enten kvartalvise møter (cirka 4 i året) eller møter hvis det skjer noe. De virker også til å ha flere møter angående temaet der vanlige ansatte er involvert. Det er hyppige møter innad i bedriften, men cybersikkerhet er nesten aldri hovedtema på disse møtene.

Av de offentlige har flere faste møter på ulike nivåer i organisasjonen, ofte er det med forskjellige former for ledelse. Der blir tilstanden til bedriften tatt opp. Det blir snakket om hva de kan forbedre og hvordan vanlige ansatte svarer på eventuelle kurs eller opplæring. Økonomi er også et viktig tema. Hvor skal pengene brukes? Hvilke sikkerhetstiltak skal prioriteres? Generelt ser det ut som de offentlige bedriftene er mer proaktive i møtearbeidet sitt, mens en større del av de private involverer vanlige ansatte i møter rundt dette.

Samtidig som organisasjoner håndterer dagens utfordringer, står de også overfor oppgaven med å forberede seg på fremtidige (Watkins, 2014). Møter med alle ansatte kan hjelpe på samme måte som kurs og hindre fremtidige angrep via dem. Møter med ledelsen er ekstremt viktig for planlegging og rapportering. Det er viktig å ha et helhetlig bilde av bedriften med tanke på bevissthet, siden sårbarheter og risikoer oftere enn forventet skyldes sikkerhetsbrudd skapt (selv utilsiktet) av selskapets egne ansatte (Bendovschi, 2015). Derfor kan inkludering av hele bedriften i slike møter være essensielt.

4.4.3 Q4: Egen kunnskap

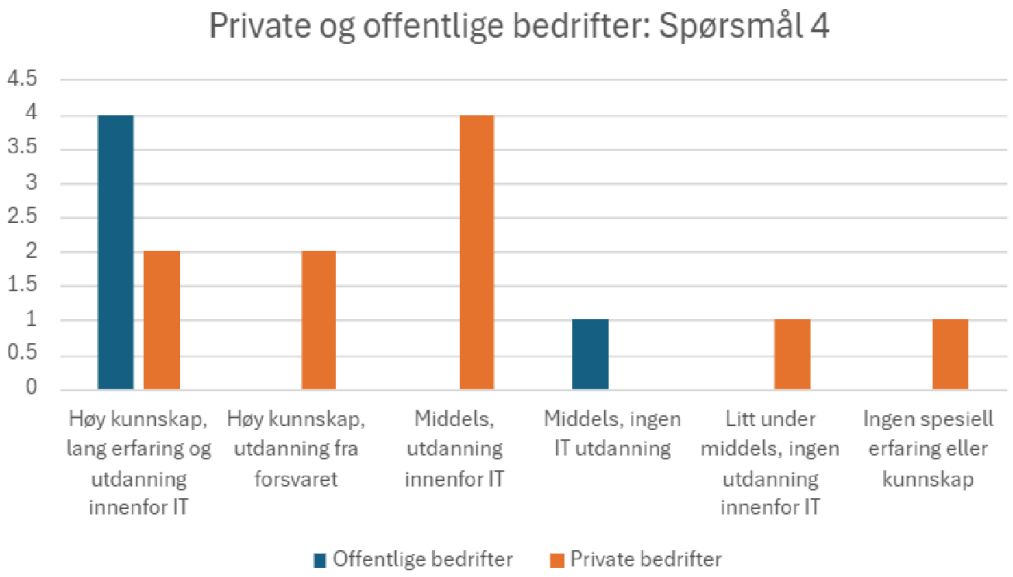
Offentlige bedrifter

Her hadde et klart flertall av intervjuobjektene fra de offentlige bedriftene høy kunnskap, lang erfaring og utdanning innenfor IT.

Private bedrifter

Av de private sa flest at den var middels selv om de hadde en utdanning innenfor IT. Det var også et større antall som sa den var under middels og hadde ingen utdanning innenfor IT. En del

hadde også høy kunnskap og lang erfaring enten fra forsvaret eller utdanning innenfor IT.



Figur 30. Svar basert på offentlige og private bedrifter, spørsmål 4: Hvordan vil du karakterisere din egen kunnskap om cybersikkerhet?

Diskusjon: **Egen kunnskap, private og offentlige**

Av de offentlige selskapene jeg snakket med, hadde alle en CISO eller leder for informasjonssikkerhet. De private bedriftene er ganske mange flere og det er stor forskjell på kunnskapen til hver enkelt. En god del har også dedikerte stillinger til cybersikkerhet, men et større antall av de private ser ut til å unngå å investere i en CISO eller leder for sikkerheten. Noen selskaper er små og har begrenset med midler, men noen virker til å ha store nok ressurser til dette. Det forsterker kanskje Gordon et al. (2018) sin påstand om at bedrifter i privat sektor kan ha en sterk tendens til å underinvestere i cybersikkerhetsaktiviteter (Gordon et al., 2018). En viktig årsak til dette er at cybersikkerhetsinvesteringer primært betraktes som kostnadsbesparende investeringer, fordi de største fordelene fra slike investeringer vanligvis kommer fra å unngå eller redusere kostnadene forbundet med cybersikkerhetsbrudd (Gordon et al., 2018). I private bedrifter er kostnadsbesparende investeringer generelt vanskeligere å

rettferdiggjøre enn inntektsgenererende investeringer (Gordon et al., 2018). Det er de største private selskapene og et fåtall av de mellomstore som anskaffer seg en leder for sikkerheten. De offentlige bedriftene var relativt store, noe som kan være grunnen til at alle intervjuobjektene mine derfra hadde såpass med kunnskap og erfaring, i tillegg til sine sentrale roller innenfor sikkerhet.

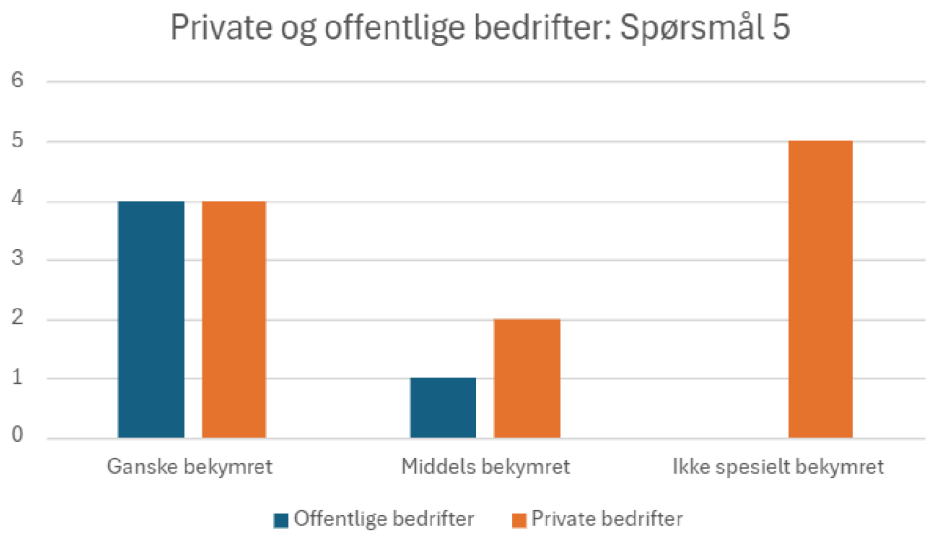
4.4.4 Q5: Frykt for cyberangrep

Offentlige bedrifter

De offentlige bedriftene har et klart størst antall som sier de er ganske bekymret for et cyberangrep med virkning mot bedriften. Det er bare én person som sier de er middels bekymret.

Private bedrifter

Av de private bedriftene er det flest som sier de ikke er spesielt bekymret, men samtidig er det et høyt antall som sier de er ganske bekymret.



Figur 31. Svar basert på offentlige og private bedrifter, spørsmål 5: I hvilken grad frykter du for et cyberangrep mot din bedrift?

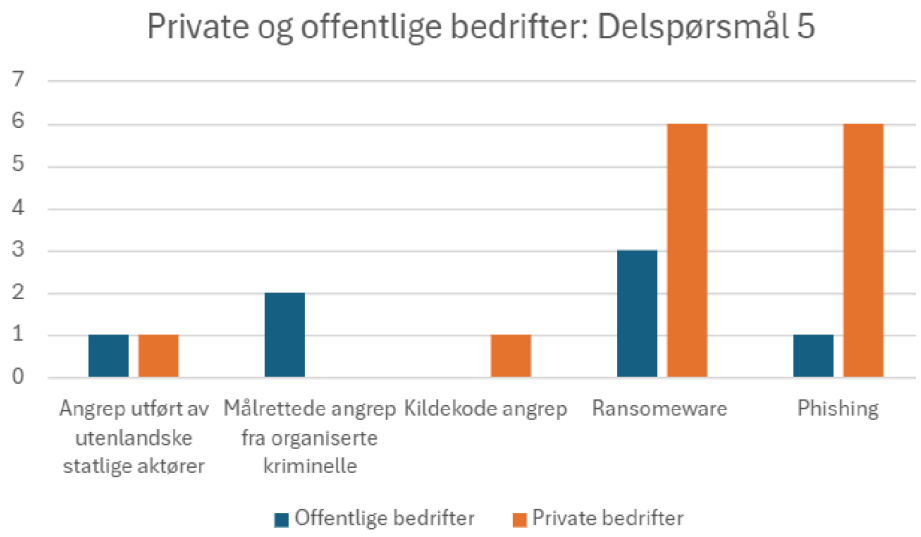
Delspørsmål Q5: Type angrep

Offentlige bedrifter

Av de offentlige sier flest at de er bekymret for ransomeware, men flere er også bekymret for målrettede angrep fra organiserte kriminelle.

Private bedrifter

Av de private er det phishing og ransomeware som blir sagt klart mest, nesten av alle sammen.



Figur 32. Svar basert på offentlige og private bedrifter, delspørsmål 5: Hvilken type angrep er du mest bekymret for?

Diskusjon: **Frykt for cyberangrep/ type angrep, Private og offentlige**

Nesten alle de offentlige selskapene sier de er ganske bekymret, flere sier de blir angrepet ekstremt ofte. En bedrift påstår det bare er et spørsmål om tid før det skjer angrep som vil påvirke dem. En andel av de private bedriftene som svarte at de var ganske bekymret, nevner også at de opplever en enorm mengde angrep. Både de private og offentlige uttrykker at phishing angrep er det de opplever klart mest, men de private virker mer bekymret for phishing enn de offentlige, som synes å tenke mer på andre typer angrepsformer. En studie av offentlige organisasjoner i Latin Amerika utrykker at de vanligste angrepsformene der, er sosial manipulasjon og nettverksangrep (Toapanta, 2020). Phishing er en type sosial manipulasjon og

ransomware kan distribueres gjennom nettverksangrep. Det fremstår som at de opplever mye av de samme angrepene som bedriftene i min undersøkelse. De private bedriftene later til å være mest bekymret for de dominerende angrepstypene.

Det er bare private selskap som oppgir at de ikke er spesielt bekymret. De fleste omtaler egne systemer og leverandører som grunn til dette. En studie fra 2015 viser at den offentlige sektoren som oftest er målet for cyber-etterretningsvirksomhet, cyber-krigføring og hacktivisme, men i det store bilde retter cyber-kriminalitet seg mot alle forretningssektorer (Bendovschi, 2015). Det er lite som tilsier at den private sektoren skal være mindre bekymret for alvorlige sikkerhetsbrudd, basert på mønster fra tidligere angrep. Ifølge Gordon et al. (2018) øker pengebruken på cybersikkerhet blant private selskaper. Basert på intervjuene mine, virker det også slik blant de fleste private selskapene i min undersøkelse, dette fører mest sannsynlig til mer selvsikkerhet. Pengene blir brukt på anerkjente leverandører og egne systemer laget av ansatte med kunnskap på området.

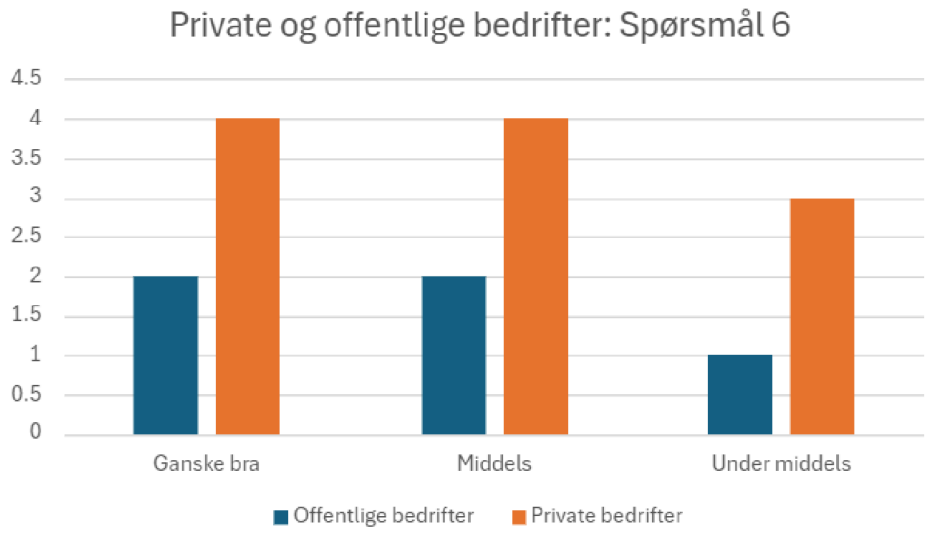
4.4.5 Q6: Organisasjonens cybersikkerhetsbevissthet

Offentlige bedrifter

De offentlige bedriftene sier for det meste at den er middels til ganske bra.

Private bedrifter

De private bedriftene svarer så og si likt med tanke på størrelsen til de to kategoriene.



Figur 33. Svar basert på offentlige og private bedrifter, spørsmål 6: Hvordan vil du karakterisere organisasjonen når det kommer til cybersikkerhetsbevissthet?

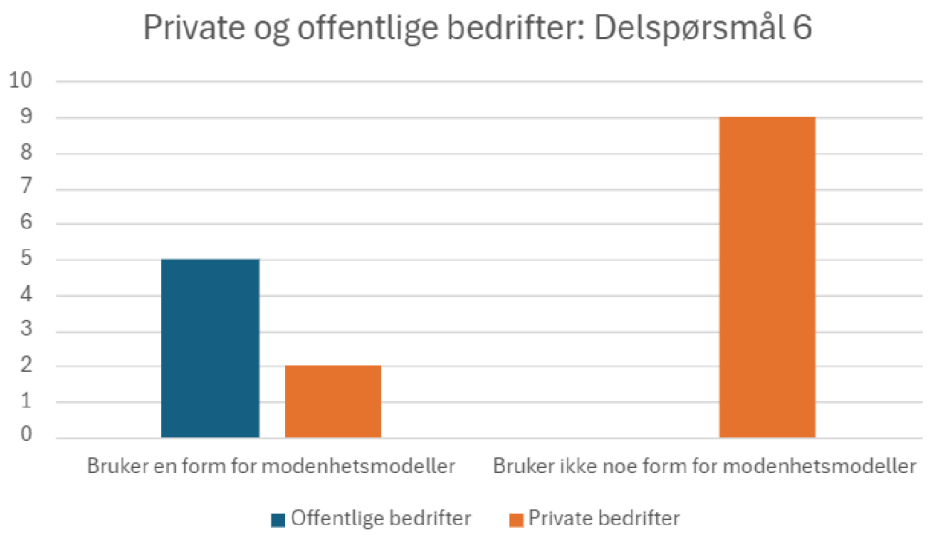
Delspørsmål Q6: Modenhetsmodeller

Offentlige bedrifter

Alle de offentlige bedriftene bruker en form for modenhetsmodeller til å måle dette.

Private bedrifter

Av de private bedriftene bruker nesten ingen modenhetsmodeller.



Figur 34. Svar basert på offentlige og private bedrifter, delspørsmål 6: Bruker dere noen form for modenhetsmodeller?

Diskusjon: Organisasjonens cybersikkerhetsbevissthet/ Modenhetsmodeller, private og offentlige

Alle de offentlige bedriftene bruker en form for modenhetsmodeller som gjør svarene deres angående bevisstheten mer troverdig, det samme gjelder to private selskap. Noen av de private selskapene har også strenge myndighetskrav eller undersøkelser ansatte må gjennomføre. Dette underbygger deres svar rundt bevisstheten, men det er fortsatt en god del av bedriftene som ikke har konkrete argumenter for hvorfor bevisstheten er middels til ganske bra. Dette kan være et eksempel på Dunning-Kruger-effekten. Studien påstår at personer med lite kompetanse innenfor et spesifikt område, vurderer seg selv urealistisk positivt (Dunning, 2011). Uten nok kunnskaper rundt cybersikkerhet og selskapets egen bevissthet rundt dette, er det vanskelig å vurdere sin egen bedrift og den ender kanskje opp mer positiv enn den burde.

Nå gjelder ikke dette alle de private som svarer middels til ganske bra rundt bevisstheten, uten noen form for målinger. Det er også intervjuobjekter med nok kunnskap til å gi en forholdsvis realistisk vurdering. I PwC sin undersøkelse svarer bare 26% at de har mindre grad av tillit til cybersikkerheten i privat sektor (PwC, 2023). Så private bedrifter har relativt høy tillit blant individer i Norge. Bevissthet blant ansatte er et viktig aspekt for å opprettholde cybersikkerheten og dermed unngå mistillit blant folk flest. Derfor er former for målinger og tester viktig. Av de

offentlige bedriftene snakkes det mest om spørreundersøkelser og phishing- tester.

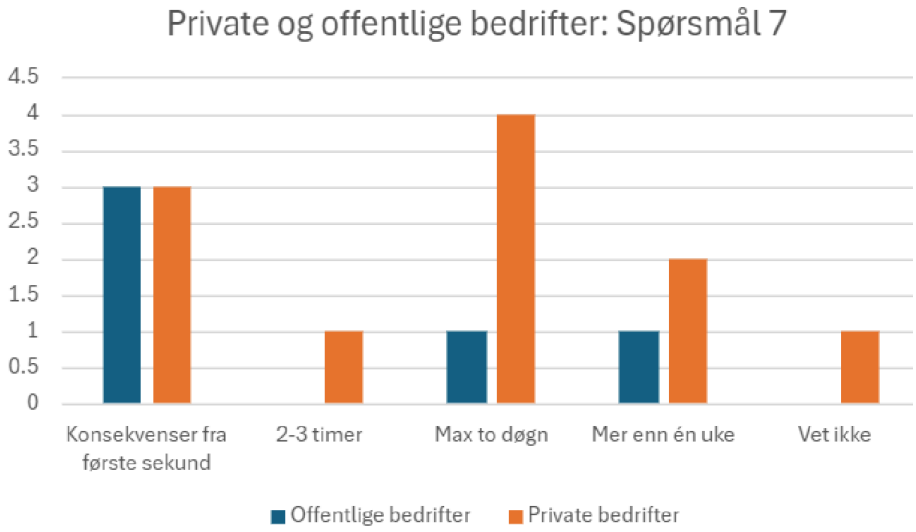
4.4.6 Q7: Nedetid kritiske applikasjoner og systemer

Offentlige bedrifter

De fleste offentlige bedriftene sier at det får betydelige konsekvenser fra første sekund. Ett av selskapene påstår at de klarer seg mer enn én uke og et annet sier rundt to dager.

Private Bedrifter

Av de private bedriftene er det flest som antyder at de klarer seg rundt to døgn, men også en god del som mener det får konsekvenser fra første sekund.



Figur 35. Svar basert på offentlige og private bedrifter, spørsmål 7: Hvor lenge tror du at de kritiske applikasjonene og systemene kan være nede før det får betydelige konsekvenser?

Diskusjon: Nedetid kritiske applikasjoner og systemer, private og offentlige

Alle de offentlige bedriftene i undersøkelsen min driver samfunnskritiske instanser, som gjør det naturlig at flere har nulltoleranse for nedetid på flere av systemene sine. Av de private selskapene er det et ganske stort sprik mellom svarene. De som sier de har nulltoleranse for nedetid virker

mest opptatt av rykte og tap av penger. En rekke private og noen offentlige bedrifter er også ganske selvsikker rundt nødløsningene sine, derfor sier de at det er mulig å klare seg en stund uten systemene sine. De offentlige er mer bekymret for nedetid angående driften. De private tenker generelt mer på økonomi og omdømme. Flere av de offentlige bedriftene fremhever at de har særskilte krav fra myndighetsorganer for å unngå angrep som fører til nedetid på viktige systemer. De private bedriftene snakker nesten ikke om dette, selv de som kan være kritisk for samfunnet. Det private næringsliv har en betydelig innvirkning på økonomisk og nasjonal sikkerhet (Watkins, 2014). Myndighetene kunne hatt flere av de samme særskilte kravene til utvalgte private bedrifter. Et fåtall får det via dem eller egen bransje, men det ser ut til at flere har ingenting å forholde seg til. Det trenger ikke bare være krav om tiltak. Kanaler for deling av viktig informasjon angående ulike cybersituasjoner med statlige myndigheter, er også et sentralt tiltak. I 2013 lanserte for eksempel Storbritannia et Cyber Security Information Sharing Partnership. En plattform der regjeringen og privat sektor raskt og konfidensielt kan dele trusselinformasjon (Fadia et al., 2020).

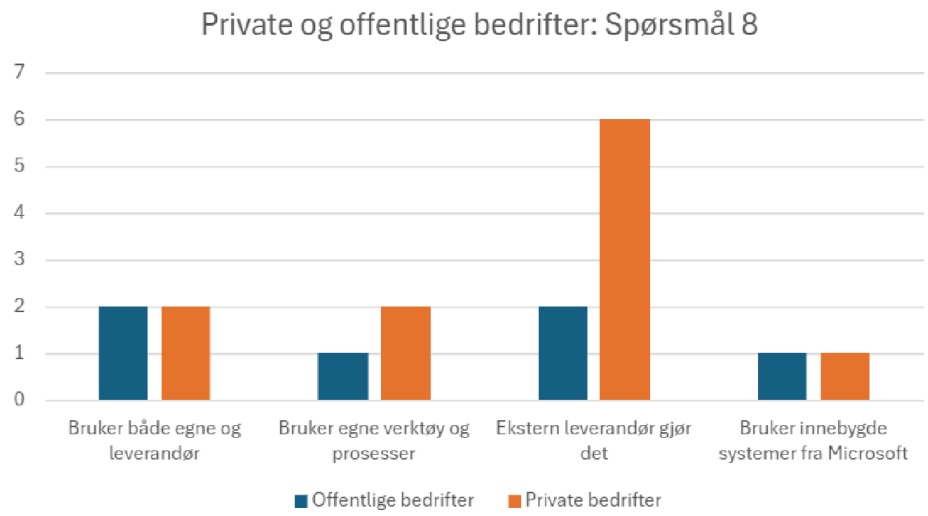
4.4.7 Q8: Identifisering av cybersikkerhetssårbarheter

Offentlige bedrifter

Av de offentlige selskapene er det like mange som bruker både ekstern leverandør og egne verktøy eller prosesser, som det er med kun ekstern leverandør med ansvaret rundt dette. Det er også et selskap som sier de kun bruker sine egne verktøy.

Private bedrifter

De private svarer som oftest at de har eksterne leverandører til å fikse dette for dem. Det er også en del som bruker sine egne verktøy eller både leverandør og egne prosesser.



Figur 36. Svar basert på offentlige og private bedrifter, spørsmål 8: Bruker din bedrift spesifikke prosesser eller verktøy for å identifisere cybersikkerhetssårbarheter?

Diskusjon: Prosesser eller verktøy identifisere cybersikkerhetssårbarheter, private og offentlige

De fleste offentlige bedriftene har en SOC (Security Operations Center) tjeneste til å oppdage sårbarheter. Dette gjelder også noen av de private selskapene. Blant de private aktørene er det flest som plasserer all sin tillit hos sin leverandør. De offentlige bedriftene har ofte mer kommunikasjon med leverandørene sine og myndigheter. Flere offentlige bedrifter nevner krav fra myndigheter som omhandler identifisering av sårbarheter rundt samfunnskritiske systemer.

Det er et fåtall bedrifter fra både de offentlige og private som er medlem av samarbeidsgrupper innad i bransjen sin. Gruppene det blir snakket om gir en trusselvurdering og bransjespesifikke data angående cybersikkerhet. Bedriftene får sårbarhetsvarsler og løsninger for å fikse de nevnte sårbarhetene. Det høres ut til å være veldig bransjeorientert og lite kommunikasjon på tvers av bransjer eller mellom offentlige og private bedrifter generelt. Leu et al. (2023) skriver at et samarbeid mellom offentlige og private enheter samt deling av trusselinformasjon, er avgjørende for å identifisere nye trusler og utvikle proaktive mottiltak. Bedriftene bør etablere mekanismer for å samle inn trusselinformasjon fra ulike kilder, inkludert offentlige myndigheter, bransjegrupper og sikkerhetsleverandører (Leu et al., 2023). De private bedriftene som bare forholder seg til leverandør, kan opprette flere kommunikasjonskanaler for å bedre prosessen

rundt identifisering av cybersikkerhetssårbarheter. Det virker som de offentlige selskapene har en større mengde plattformer for deling av informasjon og trusler, enn det de fleste private bedriftene i min undersøkelse innehar.

Q9: Tidligere cyberangrep/ Q10: Virkninger cyberangrep

På spørsmål 9 og 10 var det klart flest fra begge parter som sa at de aldri hadde opplevd angrep med virkning. Begge hadde også opplevd alvorlige angrep.

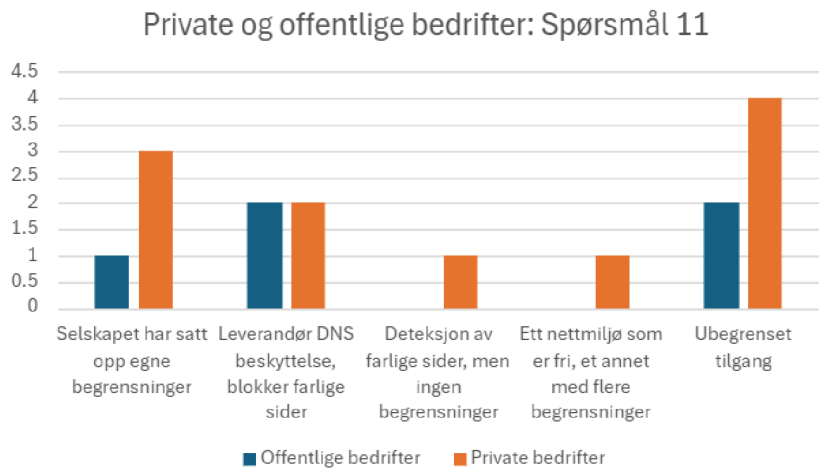
4.4.8 Q11: Surfe fritt på nettet

Offentlige bedrifter

Blant de offentlige er det like mange som sier de har DNS beskyttelse fra leverandør, som sier de har ubegrenset tilgang. Det er også et selskap som nevner at de har satt opp egne begrensninger.

Private bedrifter

De private sier flest ganger at de har ubegrenset tilgang, men en god del selskaper har også satt opp sine egne begrensninger.



Figur 37. Svar basert på offentlige og private bedrifter, spørsmål 11: Kan de ansatte i bedriften surfe fritt på nettet eller er det begrenset hvilke sider de har tilgang til?

Diskusjon: **Surfe fritt på nettet, private og offentlige**

Det er bare små private selskaper som har ubegrenset tilgang på nettet. Ingen nevner noen spesiell grunn for dette. Alle de syv andre private selskapene har former for begrensninger. Noen mer avanserte enn andre, men alle virker opptatt av det. De offentlige bedriftene uten begrensninger sier at dette er nødvendig med tanke på det de holder på med. Resten av dem har systemer for å sette de begrensningene som trengs i forhold til bransjen sin. De små private bedriftene som ikke har noen begrensninger må selvfølgelig finne en balanse angående investeringer rundt dette. Mindre private selskaper kan få en spesiell konkurransefordel grunnet cybersikkerhet aktiviteter, fordi de fleste små bedrifter ikke har store summer å bruke på nettopp dette (Gordon et al., 2018). I USA kan for eksempel cybersikkerhet tiltak ha betydelig verdi i forbindelse med å drive forretning med offentlige etater. Selskap som har adressert risikostyring angående cybersikkerhet på en måte som er konsistent med et visst rammeverk, får en lettere vei til offentlige kontrakter (Gordon et al., 2018). Mindre norske private bedrifter har også muligheter til å skaffe seg fordeler på markedet ved å investere mer. Kanskje ikke helt de samme som de amerikanske selskapene, men begrensninger som sikrer bedriften enda mer kan gi partnere og kunder enda større grunn til å stole på dem. Dermed oppnår de en fordel i motsetning til andre mindre private som velger å ignorere investeringer rundt dette. Det trenger ikke bare

være et beskyttende tiltak, men også et potensielt lønnsomt et for de mindre private selskapene.

Q12: Begrenset tilgang

Spørsmål 12 har nokså like svar fra både de offentlige og private bedriftene.

4.5 Sammenligning av vaktsomme og ubekymrede bedrifter

I dette avsnittet diskuterer jeg resultatene av analysen for bedriftene med nulltoleranse for cyberangrep med en form for virkning, og bedrifter som sa de ikke opplevde øyeblikkelig større konsekvenser av et vellykket cyberangrep.

Bedriftene med nulltoleranse har kanskje mer avanserte og flere tiltak. Kommunikasjonen deres innad er potensielt mer regelmessig. Store ressurser blir fort brukt på tiltak rundt cybersikkerheten og bevisstheten til ansatte. Disse aspektene gjorde at det var en interessant faktor å sammenligne.

I denne analysen var det 6 bedrifter som svarte at de hadde nulltoleranse for dataangrep med en form for virkning på dem. Det var 10 bedrifter som sa de ikke opplevde øyeblikkelig større konsekvenser av et vellykket dataangrep på dem. For å forkorte de to kategoriene vil jeg kalle de som hadde nulltoleranse for dataangrep med en form for virkning på dem, for de vaktsomme. Jeg vil kalle de som ikke opplevde øyeblikkelig større konsekvenser av et vellykket dataangrep på dem, for de ubekymrede.

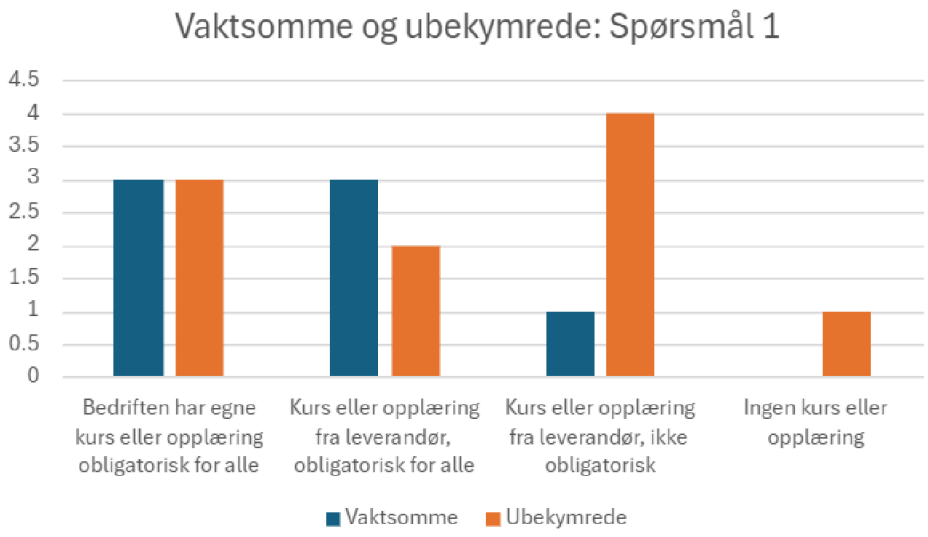
4.5.1 Q1: Kurs eller opplæringsmateriell

Vaktsomme bedrifter

Av de vaktsomme sa alle at de enten brukte egne kurs eller opplæring alle ansatte måtte gjennomføre, eller så kjøpte de kurs fra en leverandør som alle ansatte måtte gjennom. Et selskap hadde både frivillige kurs og obligatoriske.

Ubekymrede bedrifter

Fra de ubekymrede sa flest at de kjøpte kurs eller opplæring fra leverandør, men det var her frivillig om de ansatte ville ta de eller ikke. Det var også en del som hadde egne kurs som alle ansatte måtte ta.



Figur 38. Svar basert på vaktsomme og ubekymrede bedrifter, spørsmål 1: Tilbyr din bedrift kurs eller opplæringsmateriell til ansatte for å øke bevisstheten rundt cybersikkerhet?

Diskusjon: **Kurs eller opplæringsmateriell, vaktsomme og ubekymrede**

Av de ubekymrede var det flest som hadde frivillige kurs, det var også ett selskap som ikke hadde noen form for kurs eller opplæring. Halvparten av dem har enten egne kurs eller kurs fra leverandør som er obligatoriske. Alle de vaktsomme bedriftene har obligatorisk opplæring eller kurs, men ett av selskapene har flere moduler og én av dem er ikke obligatorisk. Dette selskapet meldte at mange unngikk å ta denne modulen siden den ikke var obligatorisk. En av bedriftene med obligatoriske kurs, stiller spørsmål rundt hvor effektive kursene er. Dette fordi mange fort bare "trykker" seg gjennom kursene. De har ingen testing av kunnskapene de ansatte sitter igjen med etter kursene/opplæringen. En form for testing kan for eksempel være gjennom spørsmål de må ha riktig på for å komme seg videre i opplæringen.

Noen av de vaktsomme selskapene har ansvar for kritisk infrastruktur og er underlagt detaljerte krav til sikkerhet i lover og forskrifter. Innholdet i kursene deres er derfor rettet mot dette. De snakker mer om løpende opplæring for å hele tiden opprettholde forståelsen. Dette kan fungere som en erstatning for testing av kunnskap, men de kjører også simulerte phishing forsøk på ansatte og får statistikk igjen fra testene. Så for dem er det en kombinasjon. Trussellandskapet innen cybersikkerhet utvikler seg kontinuerlig (Chowdhury et al., 2022). For å holde tritt med det nyeste landskapet, bør innholdet i cybersikkerhet treningen oppdateres jevnlig (Chowdhury et al., 2022). Derfor kan løpende kurs og testing være et viktig punkt for å henge med utviklingen. Det er et lite antall ubekymrede bedrifter med hyppige gjentagelser av kurs. Dette ser ut til å være mer vanlig for de vaktsomme. Som en løsning på den kontinuerlige utviklingen, uttrykker intervjuobjektene i Chowdhury et al. (2022) sin undersøkelse, at selskaper kan investere mer i oppdatering og evaluering av innhold, og kontinuerlig vurdere nåværende tiltak for å forsikre seg om at prosedyrene er oppdaterte i forhold til trusselbildet. Kontinuerlig oppdatert trening basert på trusselbilde kan gjøre ansatte bevisst på hvilke kunnskaper de må ha for å unngå digitale risikoer i det aktuelle tidsrommet.

Q2: Stillinger dedikert til cybersikkerhet

På spørsmål 2 har de vaktsomme én eller flere dedikerte stillinger til cybersikkerhet. De ubekymrede har også en god del bedrifter med én eller flere dedikerte stillinger. Det er lite forskjeller generelt.

Q3: Faste møter

På spørsmål 3 har både de vaktsomme og ubekymrede bedriftene veldig like spredte svar.

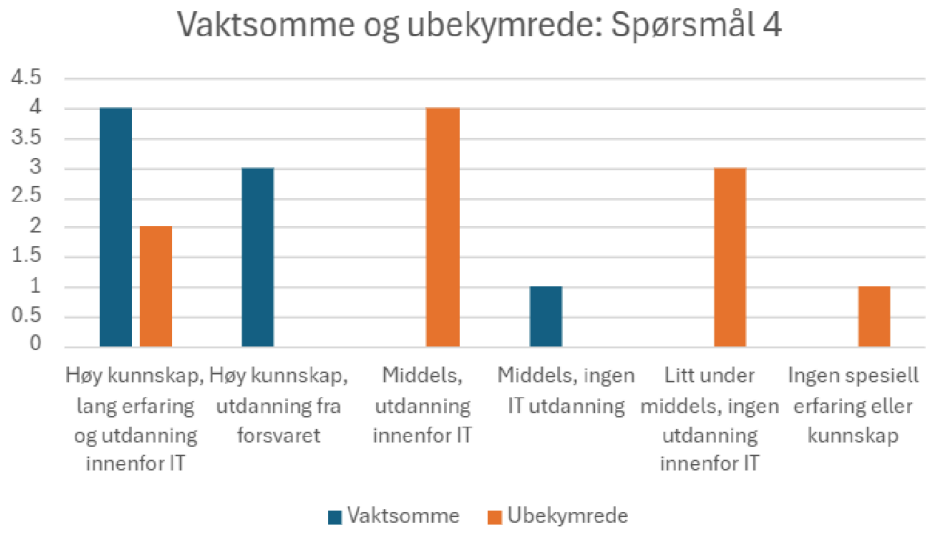
4.5.2 Q4: Egen kunnskap

Vaktsomme bedrifter

Av de vaktsomme bedriftene sier nesten alle at de har høy kunnskap og lang erfaring. Ett intervjuobjekt sier den er middels og har ingen IT utdanning.

Ubekymrede bedrifter

De ubekymrede bedriftene påstår at kunnskapen er middels eller litt under middels som oftest. De som sier middels har IT utdanning, de som sier litt under middels har ingen IT utdanning.



Figur 39. Svar basert på vaktsomme og ubekymrede bedrifter, spørsmål 4: Hvordan vil du karakterisere din egen kunnskap om cybersikkerhet?

Diskusjon: Egen kunnskap, vaktsomme og ubekymrede

Av de vaktsomme bedriftene, er det to av intervjuobjektene mine som har lang erfaring og utdanning, pluss utdanning fra forsvaret. Nesten alle har minst 10 års erfaring med sikkerhetsfaget og en form for lederstilling innenfor dette området. De ubekymrede har flere med mindre erfaring, noen med veldig lite. Det er seks stykker som har utdanning innenfor IT og ingen med utdannelse fra forsvaret. Det er mer generelle lederstillinger og mindre lederstillinger angående sikkerhet. Å utvikle, revidere og administrere informasjonssikkerhet avhenger av profesjonell ekspertise for å oppnå ønsket informasjonssikkerhetsstyring (Haqaf & Koyuncu, 2018). En leder for informasjonssikkerheten kan være løsningen her, men de fleste av bedriftene uten umiddelbare virkninger ser ut til å tenke at leverandøren deres løser dette. En informasjonssikkerhetsleder skal sikre at sikkerhetsprosesser, systemer, retningslinjer, standarder og veiledninger etableres, kommuniseres og forbedres på tvers av hele organisasjonen for å

beskytte informasjonsressurser (Haqaf & Koyuncu, 2018). Et spørsmål er om leverandørene kan kommunisere retningslinjer og standarder på en like god måte som en intern sjef med dette ansvaret.

Et av intervjuobjektene i undersøkelsen min tar opp hvor utsatte ansatte kan være. Det blir sagt at mange er økonomisk presset i disse tider, derfor er ansatte kanskje enda mer sårbare hvis noen kommer og sier "kan du ikke gi meg den informasjonen, så får du så og så mye penger". En rapport viser at 35 % av ansatte ville selge organisasjonens data for riktig pris (Clearswift, u.å.). Informasjonssikkerhetsledere er derfor under press når de håndhever retningslinjer for å beskytte organisatoriske eiendeler mot brudd begått av ansatte (Liu et al., 2020). En leder på dette området kan hele tiden veilede og hjelpe med å opprettholde retningslinjer, en leverandør kan gjøre det samme, men er kanskje ikke like aktiv i selskapet.

Q5: Frykt for cyberangrep/ Delspørsmål 5: Type angrep

På spørsmål 5 er svarene nesten helt like, begge parter er ganske bekymret for å bli rammet av et vellykket dataangrep. Det er forsåvidt overraskende at de vaktsomme og ubekymrede svarer likt på dette spørsmålet, med tanke på kategoriseringen. Det er også veldig likt når det gjelder delspørsmål 5. Begge parter har ransomware og phishing som de to typene angrep de er mest bekymret for.

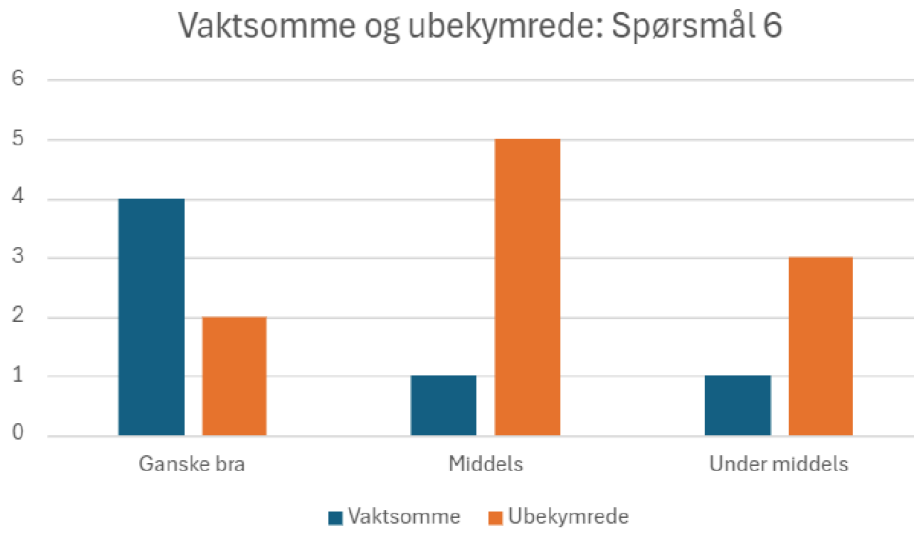
4.5.3 Q6: Organisasjonens cybersikkerhetsbevissthet

Vaktsomme bedrifter

Av de vaktsomme bedriftene sier klart flest at cybersikkerhetbevisstheten er ganske bra.

Ubekymrede bedrifter

De ubekymrede bedriftene svarer som oftest at bevisstheten er middels eller under middels.



Figur 40. Svar basert på vaktsomme og ubekymrede bedrifter, spørsmål 6: Hvordan vil du karakterisere organisasjonen når det kommer til cybersikkerhetsbevissthet?

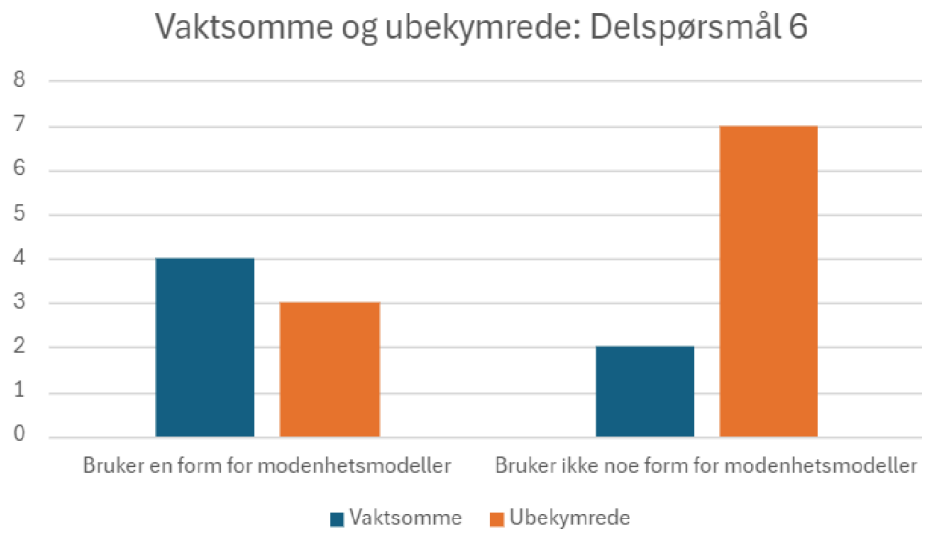
Delspørsmål Q6: Modenhetsmodeller

Vaktsomme bedrifter

De fleste vaktsomme bedriftene bruker modenhetsmodeller.

Ubekymrede bedrifter

Av de ubekymrede bedriftene bruker nesten ikke noen av dem modenhetsmodeller.



Figur 41. Svar basert på vaktsomme og ubekymrede bedrifter, delspørsmål 6: Bruker dere noen form for modenhetsmodeller?

Diskusjon: Organisasjonens cybersikkerhetsbevissthet/ Modenhetsmodeller, vaktsomme og ubekymrede

Av de vaktsomme bedriftene er det fire som bruker en form for modenhetsmodell, men bare to av de som bruker det, svarer at bevisstheten er ganske bra. De to selskapene som ikke bruker modenhetsmodeller påstår begge at bevisstheten er ganske bra. Dette er fordi de har strenge myndighetskrav eller blitt revidert eksternt gjennom ulike konsulentbyråer. De ubekymrede bedriftene svarer som oftest at bevisstheten er middels, de fleste kommenterer at dette er fordi deler av bedriftene er over snittet bevisst, ofte er dette IT ansatte, men det er også deler som ikke har mye erfaring med teknologi og er derfor mindre bevisst. Bare to av de fem selskapene som svarte dette, bruker en modenhetsmodell. Ingen av bedriftene som sier den er under middels, bruker en form for modenhetsmodeller av de ubekymrede. De vaktsomme selskapene virker mest oppmerksom på å måle bevisstheten sin, samtidig er det de som er klart mest fornøyd med bevisstheten innad i bedriftene sine.

Ansatte er den primære sårbarheten i et selskap, uavhengig av størrelse eller omfang (Kemper, 2019). Så bevisstheten er viktig uansett type bransje, drift og systemer. Et intervjuobjekt fra de vaktsomme selskapene fremhever hvor vanskelig det er å formidle risikoen til de ansatte. Det blir

sagt: "Vi har ikke klart å oversette det til noe som det går an å snakke om". De har svært mange systemer og flere kritiske med mange sikkerhetstiltak, men utenforstående (ansatte som ikke tilhører sikkerhetsgruppen) skjønner ikke helt hvordan dette fungerer og arbeidet sikkerhetsgruppen gjør. Derfor er det vanskelig å snakke med dem angående dette. Hvis vanlige ansatte forstår grunnleggende sikkerhetstiltak og hvordan de fungerer, kan det være med på å øke bevisstheten. Dette kan være spesielt viktig med tanke på tiltak rettet mot kritiske systemer. I en kvalitativ studie ble cybersikkerheteksperter spurt om gapet mellom holdninger til cybersikkerhet og sikker atferd blant ansatte. En deltaker sa "Det store gapet skyldes det faktum at ansatte ser risikoene langt borte fra seg selv, de mener at det er selskapet som må gjøre tiltak, ikke de ansatte" (Ergen et al., 2021, s. 219). Det er mulighet for at ansatte tenker at alt ansvaret ligger på selskapet, og de som arbeider med sikkerheten. Derfor trenger de ikke tilegne seg den grunnleggende kunnskapen som virkelig trengs for å skjønne hvordan de ideelt sett skal beskytte bedriften. Selskapet og deres sikkerhetsansatte kan samtidig ha som mål å gjøre kommunikasjonen mest mulig forståelig.

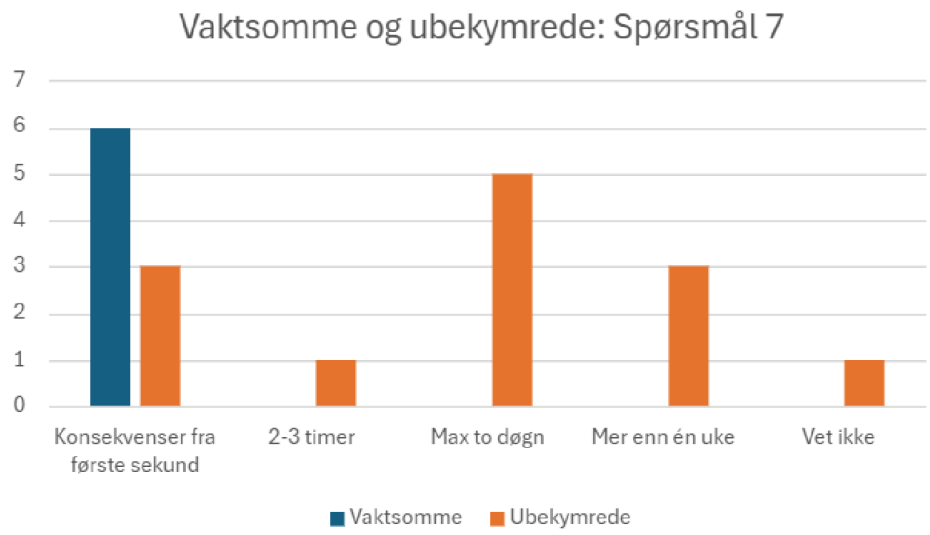
4.5.4 Q7: Nedetid kritiske applikasjoner og systemer

Vaktsomme bedrifter

Her sier selvfølgelig de vaktsomme at det får øyeblikkelige konsekvenser

Ubekymrede bedrifter

De uten derimot, sier som oftest at de kunne klart seg rundt to døgn uten kritiske applikasjoner og systemer. Alle har en form for nødløsninger på plass.



Figur 42. Svar basert på vaktsomme og ubekymrede bedrifter, spørsmål 7: Hvor lenge tror du at de kritiske applikasjonene og systemene kan være nede før det får betydelige konsekvenser?

Diskusjon: **Nedetid kritiske applikasjoner og systemer, vaktsomme og ubekymrede**

Blant de vaktsomme bedriftene er det flere som svarer at cyberangrep får umiddelbare konsekvenser for deres rykte og økonomi, like mange av dem har samfunnskritiske systemer som ikke tåler nedetid. De ubekymrede bedriftene har ganske varierte svar. Noen sier de holder rimelig lenge, en hel ukes tid. De som påstår dette svarer, at det er fordi de har nødløsninger som fint kan erstatte de eksisterende. Det kan være alt fra lignende programmer til mer manuelle løsninger. Selskapene som kan greie seg rundt to dager har systemer som er viktig for å holde driften gående, men de greier seg fortsatt en god stund uten dem.

En mengde bedrifter fra begge kategoriene kobler nedetid med dårlig omdømme blant nåværende kunder eller fremtidige. En studie av 45 firmaer fra 2002- 2018 sier at selskaper opplever en 26–29% økning i verdi av selskapets omdømme eller gode rykte ved gjennomsnittlige datainnbrudd (Makridis, 2021). Grunner til dette kan være at selskapet reagerer på datainnbruddet på en måte som viser ansvarlighet og effektiv krisehåndtering, eller øker investeringene angående cybersikkerhetstiltak og teknologisk infrastruktur for å stoppe fremtidige hendelser. Dette punktet nevnte flere av de som hadde opplevd vellykkede angrep i min undersøkelse. Samtidig er nyheter om cyberangrep mot bedrifter alltid negative (Leroy, 2022). For eksempel falt aksjene til teknologiselskapet Apple med mer enn 4% på én dag etter

rykter om en hack i skytjenesten deres i september 2014 (Leroy, 2022). Selskaper som blir rammet av store og fremtredende innbrudd opplever en nedgang på 5–9% i verdi av selskapets omdømme (Makridis, 2021). Så å si alle de vaktsomme selskapene har vitale systemer som gjør at et hvert vellykket angrep på dem vil fremstå stort fordi det vil påvirke såpass mange. Derfor er det forståelig at dette er et viktig aspekt for en mengde av dem med tanke på nedetid.

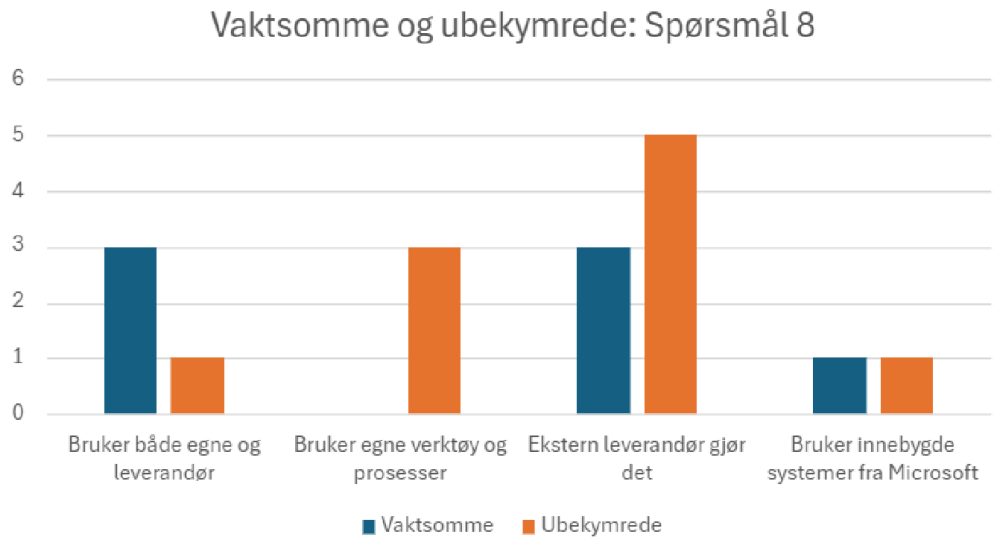
4.5.5 Q8: Identifisering av cybersikkerhetssårbarheter

Vaktsomme bedrifter

De fleste vaktsomme bedriftene sier de enten bruker både egne verktøy og leverandør til å gjøre dette, eller så har ekstern leverandør fullstendig kontroll over dette.

Ubekymrede bedrifter

Av de ubekymrede er det flest som sier de bruker ekstern leverandør til å gjøre dette. En god del bruker også bare sine egne verktøy. Det er veldig få som bruker både eksterne leverandører og egne verktøy eller prosesser.



Figur 43. Svar basert på vaktsomme og ubekymrede bedrifter, spørsmål 8: Bruker din bedrift spesifikke prosesser eller verktøy for å identifisere cybersikkerhetssårbarheter?

Diskusjon: **Prosesser eller verktøy identifisere cybersikkerhetssårbarheter, vaktsomme og ubekymrede**

Flere av de vaktsomme bedriftene har mange tiltak på dette punktet. Bedriftene som bruker leverandør gir inntrykk av at de har god kontroll på hva de gjør for dem og hvordan de gjør det. Alt som blir oppdaget og gjort for dem virker godt kommunisert. Av de ubekymrede er det flest som svarer at leverandør har kontroll på dette. Et større antall høres usikker ut på hva leverandøren egentlig gjør for dem. De få bedriftene i denne kategorien som bruker egne verktøy snakker mest om programmer for scanning og penetrasjonstester. Scanne- verktøy er programvarer brukt til å identifisere potensielle sårbarheter i et datasystem eller nettverk (Tundis et al., 2018). Penetrasjonstester er testing av sikkerheten til et IT-system ved å forsøke å bryte noen eller alle sikkerhetsaspektene til systemet, via de samme verktøyene og teknikkene som en angriper kunne ha gjort (NCSC, 2017). Nesten alle selskapene med nulltoleranse driver med pentester (Penetrasjonstester), og har programvarer til å identifisere sårbarheter.

En del er også med i grupper for kommunikasjon mellom bedrifter i bransjen sin, eller får informasjon via myndigheter rundt potensielle angrepsvektorer. Myndigheter trenger å øke bevisstheten i samfunn angående programmene som adresserer trusler i deres digitale rom, samt de ulike teknologiske verktøyene som hjelper dem med å dra nytte av dagens teknologi og unngå trusler (Alhayani et al., 2021). NSM (Nasjonal sikkerhetsmyndighet) sine grunnprinsipper skal hjelpe med dette, men et større antall ubekymrede bedrifter gir inntrykk av at de enten ikke har hørt om dem eller ikke bruker dem aktivt, noe som tilsier at anbefalingene kanskje ikke er kommunisert ut godt nok til generelle bedrifter, eller at bedriftene selv unngår å bruke dem. De vaktsomme selskapene ser generelt ut til å ha flere verktøy og prosesser enn de ubekymrede bedriftene, noe som kan sees på som naturlig.

4.5.6 Q9: Tidligere cyberangrep

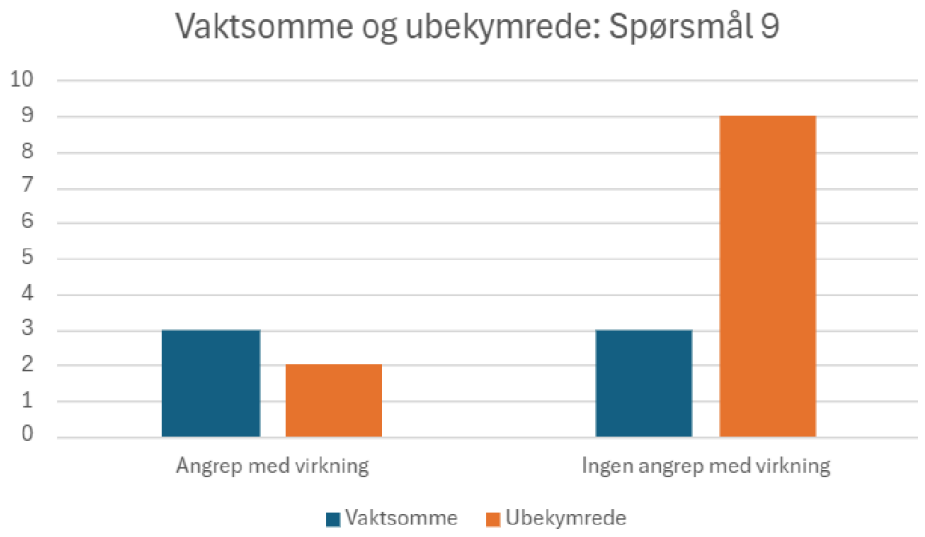
Vaktsomme bedrifter

De vaktsomme har klart mest vellykkede angrep mot seg av de to kategoriene. Det er like mange

vellykkede angrep som det er selskaper som ikke har opplevd noen angrep med virkning. Noe av det de har opplevd er data breach, ransomware og phishing.

Ubekymrede bedrifter

De ubekymrede selskapene har nesten ikke opplevd noen vellykkede angrep på bedriften sin, det er bare to selskap som melder at det har vært brudd på leverandøren deres.



Figur 44. Svar basert på vaktsomme og ubekymrede bedrifter, spørsmål 9: Har det vært noen tidligere cyberangrep på din bedrift som du kan nevne?

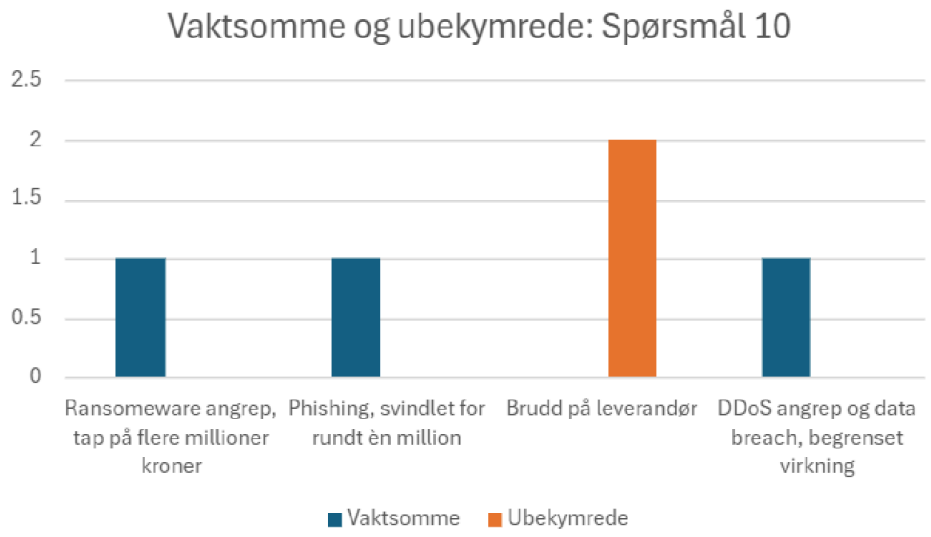
Q10: Virkninger cyberangrep

Vaktsomme bedrifter

Flere av de vaktsomme har opplevd mange forskjellige typer angrep med negative følger.

Ubekymrede bedrifter

Av de ubekymrede selskapene, er det er to selskaper som melder at det har vært brudd på leverandøren deres.



Figur 45. Svar basert på vaktsomme og ubekymrede bedrifter, spørsmål 10: Hvilke virkninger hadde cyberangrepet på bedriften?

Diskusjon: Tidligere cyberangrep/ Virkninger cyberangrep, vaktsomme og ubekymrede

Av de vaktsomme bedriftene er det like mange som har opplevd angrep med konsekvenser som uten konsekvenser. To selskaper har tapt mye penger på kryptering og phishing, noe som også var de to metodene bedriftene var mest bekymret for. Noen selskap svarer at angrepene med virkning har hatt en positiv effekt med tanke på tetting av hull i forsvaret deres, og mer fokus blant ledelsen. De har blant annet økt investeringene rundt det tekniske for å unngå at det skal skje igjen. De ubekymrede bedriftene har opplevd svært få angrep med noe form for effekt. Her er det to bedrifter som nevner angrep på leverandøren, men bare ett selskap hørtes ut til å ha fått større konsekvenser fra det.

Resultatene fra intervjuene mine, motstrider at angripere retter seg mot selskaper med forsvar som er lettere å bryte gjennom (Kamiya et al., 2018). De vaktsomme bedriftene høres ut til å ha flere tiltak og mer robuste forsvarsverk, men det er fortsatt de som opplever flest angrep med større konsekvenser. Undersøkelsen min støtter at selskaper er mer sannsynlig å oppleve cyberangrep når de er store, større økonomisk fleksibilitet, har høyere verdi og flere immaterielle eiendeler (Kamiya et al., 2018). De vaktsomme kan se ut til å gjennomgå en større mengde

avanserte målrettede angrep. De fleste ubekymrede selskapene har ikke fått føle på et angrep med effekt. Dette kan kanskje være et element som gir dem en falsk trygghet eller selvtillit, og at de derfor ender opp med mindre sikkerhetstiltak.

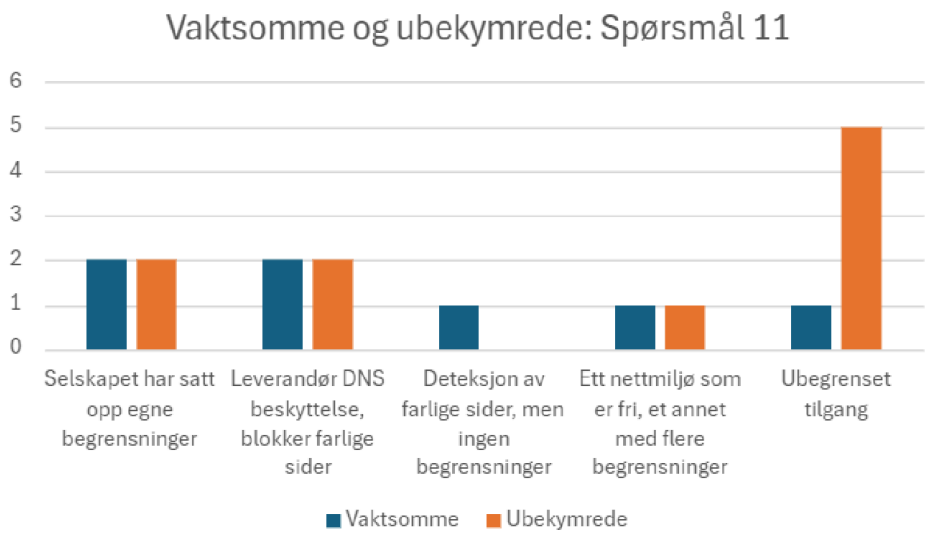
4.5.7 Q11: Surfe fritt på nettet

Vaktsomme bedrifter

Av de vaktsomme bedriftene er det bare ett selskap som sier de har ubegrenset tilgang. Flere har leverandør med DNS beskyttelse eller egne begrensninger. Ett selskap har deteksjon av farlige sider.

Ubekymrede bedrifter

De ubekymrede selskapene har flest selskaper som sier de har ubegrenset tilgang. Her er det også flere med DNS beskyttelse fra leverandør og egne begrensninger.



Figur 46. Svar basert på vaktsomme og ubekymrede bedrifter, spørsmål 11: Kan de ansatte i bedriften surfe fritt på nettet eller er det begrenset hvilke sider de har tilgang til?

Diskusjon: Surfe fritt på nettet, vaktsomme og ubekymrede

Det ene vaktsomme selskapet som svarer at de har ubegrenset tilgang, påpeker at dette er fordi jobben de ansatte gjør krever dette. Det er interessant å se at et selskap i samme kategori og bransje velger å benytte seg av DNS beskyttelse. Så det er tydelig at ikke alle i denne bransjen tenker likt. De fleste bedriftene uten umiddelbare konsekvenser og ubegrenset tilgang virker bare ikke å bry seg med dette tiltaket. I studien til Ergen et al. (2021) sier en cybersikkerhetekspert at ansatte kan overvurdere kunnskapen sin angående cybersikkerhet, og dermed laste ned skadelige programvarer eller applikasjoner med tanker om at det er trygt. Hvis det ikke er trygt, stoler de på at selskapet har antivirus programmer til å stoppe prosessen før det skjer noe alvorlig (Ergen et al., 2021). Studien av engelske selskaper sier også at flere deltagere har en oppfatning av sin egen cybersikkerhetsbevissthet som er langt mer optimistisk enn den burde være (Erdogan et al., 2023). Et selskap med god nok beskyttelse rundt nettbruk, vil oppdage og kanskje stoppe dette før store skader skjer, eller før noe skjer i det hele tatt. Nettbruken til ansatte vil alltid være en mulig inngangsport for ulike typer angrep, derfor kan det være viktig å begrense mulighetene ansatte har til å åpne disse portene. Sikkerhetsatferdene må gjøres enkle for ansatte (Ergen et al., 2021). Det skal være vanskelig for ansatte å ufrivillig skade selskapet via nettbruk. Mange av de ubekymrede bedriftene har ubegrenset tilgang, og gjør det kanskje litt lettere for egne ansatte å gjøre slike feil.

Q12: Begrenset tilgang

På spørsmål 12 er det veldig likt. De vaktsomme har litt flere selskaper med rutiner for besøkende.

5 Konklusjon og videre arbeid

Dette kapittelet vil oppsummere studien og hvilke svar jeg har fått på forskningsspørsmålet mitt. Jeg vil også skrive en del om videre arbeid og litt om svakheter ved undersøkelsen. Forskningsspørsmålet mitt var:

Hvordan skaper norske bedrifter bevissthet rundt cybersikkerhet?

De norske bedriftene i undersøkelsen min virker generelt sett opptatt av bevisstheten rundt cybersikkerhet, men det finnes selvfølgelig unntak og ulikheter. Det er flere forskjeller i tiltak basert på ulike faktorer som påvirker bedriften. En del bedrifter sliter med å få alle ansatte til å gjennomføre cybersikkerhetskurs. Noen har også frivillige kurs som de fleste ansatte unngår å ta. Dette gjaldt spesielt små private bedrifter. Kursing og opplæring er essensielt for å øke bevisstheten i bedrifter. Det nevner nesten alle intervjuobjektene mine og litteraturen generelt. Det er et punkt som er mulig å forbedre hos flere ved hjelp av oppfølgingsverktøy og obligatorisk testing eller kursing. De fleste store og mellomstore selskapene har stillinger innad som omhandler cybersikkerhet. Mange bruker leverandører i tillegg. Naturlig nok hadde ikke de små selskapene dedikerte stillinger, men flere virket å stole blindt på leverandør- uten at de skjønte helt hva som ble gjort for dem. Det er viktig at selskapene er bevisst på angrepsflatene og forstår hva leverandøren gjør for dem. Leverandør gir ingen immunitet mot alle typer angrep, så det er avgjørende at bedriftene skjønner selv hva de kan gjøre for å forhindre dette.

De store offentlige bedriftene prioriterte hyppige møter angående cybersikkerheten. Flere av de andre bedriftstypene responderte bare med møter hvis situasjonen oppstod eller unngikk dette fullstendig. Rutinemessige møter angående cybersikkerhet vil utvilsomt skape en større cybersikkerhetskultur. Dette gjelder uansett om det bare er blant lederne i selskapet eller med resten av de ansatte. Store deler av bedriftene er mest bekymret for phishing og ransomware angrep. En del av dem som er mest bekymret for phishing angrep har enten frivillige kurs eller ingen i det hele tatt. De virket ikke til å ha noen effektive strategier for å stoppe slike angrep. Flere sa det var på vei til å skaffe seg dette, men hørtes ut til å stole på leverandør i mellomtiden. Dette gjaldt som oftest små og mellomstore private selskaper som svarte de ikke var spesielt bekymret for angrep.

De fleste mener at bevisstheten er ganske bra innad i bedriften sin. Spesielt store bedrifter med nulltoleranse for nedetid svarte dette. Disse selskapene hadde som oftest også en form for modenhetsmodell til å måle det med. Det var interessant å se at de små bedriftene var minst bekymret for angrep, men samtidig oppga mest at de hadde lav til middels bevissthet innad i selskapet.

Bare mellomstore og store bedrifter hadde opplevd vellykkede angrep mot dem. Dette kan underbygge hvorfor de små bedriftene ikke var spesielt bekymret. Selskapene som ikke hadde blitt utsatt for vellykkede angrep, var generelt mindre bekymret og mer sikker på at det ikke ville skje med dem. Mangelen på en slik erfaring kan gi en falsk trygghet rundt sikkerhetsrutinene. En del av dem hadde mindre tiltak rundt cybersikkerhetbevisstheten, enn selskapene som hadde vært gjennom slike scenarioer.

Det var overraskende at flere av selskapene som kanskje er mest fornøyd med sitt sikkerhetsarbeid, ikke bruker noen form for modenhetsmodeller. Noen av dem erstattet det med eksterne selskaper som evaluerte dem. Men samtidig var det mange som mente sikkerhetsarbeidet var godt nok, uten å ha noen målinger rundt effekten av det. Flere av intervjuobjektene som bemerket sin begrensede kunnskap, var samtidig de som uttrykte størst tilfredshet med sikkerhetsarbeidet og viste minst bekymring for potensielle angrep. Dette var som oftest utelukkende på grunn av leverandørene deres eller andre ansatte i selskapet. I den engelske studien virket bedriftene også å ha en tendens til å stole på at cybersikkerhet håndteres i andre deler av selskapet eller av andre personer (for eksempel tredjepartstjenester) (Erdogan et al., 2023). Dette lignet på en god del av de små og mellomstore bedriftene i min undersøkelse. Forskjellen var at de engelske meldte om relativt høy bevissthet innad i selskapet (Erdogan et al., 2023). De norske bedriftene av samme størrelse i min studie svarte som oftest at den var middels til under middels. De norske bedriftene hadde kanskje et mer realistisk syn på akkurat dette punktet basert på tiltak og egen kunnskap.

Den største forskjellen er at nesten alle de norske selskapene tilbyr en form for kurs eller opplæring. Av de engelske er det bare 19% som tilbyr dette (Erdogan et al., 2023). Problemene rundt kursene til de norske selskapene, er at flere er frivillig eller bare obligatorisk for deler av selskapet. Derfor er det en stor andel ansatte i bedriftene som ikke gjennomfører dem. Når det gjelder nettsikkerhet og fysiske begrensninger fremstår både de jordanske og norske bedriftene i

mine intervju ganske likt. Den fysiske sikkerheten i de jordanske bedriftene er god (Dahbur et al., 2017). Samme kan jeg si om så og si alle de norske i min studie. Programvaresikkerheten til de jordanske selskapene blir kategorisert som minimal (Dahbur et al., 2017). Kategoriseringene deres er basert på flere spørsmål enn bare de to spørsmålene (spørsmål 11 og 12 i min studie) jeg brukte. Flere selskaper hadde ubegrenset tilgang på nettet. Stort sett hørtes det ut som de stolte på de ansattes vurderinger. Dette er motstridende for flere av dem, på grunn av et større antall av dem svarer også at bevisstheten i bedriften er middels til under middels. Det hjelper heller ikke at flere av de samme selskapene bare hadde frivillige kurs eller opplæring for deler av bedriften.

5.1 Svakheter

En av svakhetene med kvalitativ analyse, er at det ikke er noe objektivt verifiserbart resultat (Choy, 2014). Det betyr at det ikke finnes klare målbare bevis som gjør at jeg kan hundre prosent bekrefte eller avkrefte resultatene jeg får fra analysen min. Med tanke på analysen skulle jeg selvfølgelig gjerne hatt flere intervjuobjekter fra andre norske bedrifter. Det ville underbygget svarene jeg fikk i analysen enda mer. Det burde også vært flere enn fem offentlige bedrifter med på studien. Antallet er litt for lite i forhold til antall private selskaper. Det samme gjelder bedrifter med nulltoleranse for vellykkede angrep på dem. Jeg skulle gjerne hatt mer enn seks slike bedrifter. På grunn av dette kan jeg ikke være sikker på at resultatet representerer de offentlige selskapene og bedriftene med nulltoleranse. Deler av analysen baseres på mine erfaringer og tolkninger som aldri vil være 100% sikker.

Noen intervjuobjekter var mer villig til å dele informasjon enn andre. Derfor varierte også lengden på de ulike intervjuene en god del. Deler av spørsmålene var dermed ikke alltid sammenlignbare mellom informantene fordi noen hadde utdypet mer enn andre. I analysene mine diskuterer jeg resultatene med større forskjeller og utelater dem med større likheter. På grunn av dette fokuset på forskjeller, har jeg kanskje unnlatt å diskutere noen av spørsmålene med interessante like svar. Et eksempel kan være svarene fra de vaktsomme og ubekymrede bedriftene på spørsmål 5 angående frykt for cyberangrep. Her er det veldig like svar. Det er overraskende at de vaktsomme og ubekymrede svarer likt på dette spørsmålet, med tanke på at de vaktsomme kan oppleve såpass store problemer av et vellykket angrep. Like svar på spørsmål

som dette med interessante faktorer, skulle jeg ha diskutert mer.

5.2 Fremtidig arbeid

Gjennom studien har det kommet fram viktige punkter som kan være med i framtidig arbeid. Det er for eksempel ekstremt få selskaper som refererer til kunstig intelligens (KI) generelt i intervjuene mine. Dette er et meget aktuelt tema som jeg valgte å ikke stille noen spørsmål rundt i denne studien. Dette var fordi jeg tenkte det var et rent teknisk element og det tekniske var ikke fokuset i undersøkelsen min. KI kan brukes til å forbedre cybersikkerhet, men også til mer avanserte former for angrep. Den har kapasitet til å etterligne en mengde av skreddersydde scenarioer som sikkerhetsteamet og organisasjonen kan trene på for å forberede seg på faktiske trusler (PwC, 2023). Den kan bruke store mengder data om cyberangrep til å simulere og forbedre for eksempel phishing tester, eller lage spørreundersøkelser til ansatte basert på tidligere angrep som har gått via ansatte. Av denne grunn kan KI brukes til å forsterke bevisstheten i alle typer bedrifter. Derfor kunne det vært et viktig element å undersøke i fremtidige studier.

Et annet punkt er de ansatte. Intervjuobjektene mine har vært utelukkende ulike former for ledere. Jeg ville gjerne sammenlignet svarene til vanlige ansatte, med det en av lederne deres har sagt. Da kunne jeg sett på perspektivet til de ansatte og vurdert erfaringene de hadde rundt bevisstheten i selskapet. Dette kunne potensielt vært ansatte som ikke hadde noe å gjøre med IT-driften. Det hadde vært interessant å høre hvordan denne gruppen hadde opplevd tilstanden og tiltakene. Vanlige ansatte vil alltid være en potensiell risiko med tanke på kunnskap og bevissthet. Et av intervjuobjektene mine omtaler et eksempel på dette. En situasjon som skjedde i en annen bedrift: “Tre ansatte jobbet i to og en halv time for å klare å åpne et vedlegg som alle burde forstått ikke skulle åpnes. Når den første personen ikke klarte det, hentet hun en annen, men de fikk det heller ikke til. Deretter involverte de en tredje person, og til slutt krypterte de alt i bedriften”. Ansattes mening og syn på bevisstheten og tiltakene som blir gjort i bedriften vil derfor alltid være av betydning.

Basert på resultatene mine hadde det vært interessant å se forskjellene i sikkerhetsarbeidet

mellom bedrifter som hadde vært rammet av vellykkede cyberangrep, og de som ikke hadde opplevd det. Prioriterer de forskjellige tiltak, har de tatt flere forhåndsregler og kommuniserer de cyber policy oftere med ansatte? Spørsmålene kunne blitt brukt i en ny kvalitativ undersøkelse av dette. Et annet eksempel som kunne vært sett på, var forskjellen på bedrifter som bruker modenhetsmodeller eller vurderinger av sikkerhetstiltak, og de som ikke velger å bruke det. Jeg ville hørt om de uten målinger var mer positive til sikkerheten og bevisstheten. Det kan virke slik i min undersøkelse, men en mer inngående studie av dette temaet kunne gitt tydeligere svar. Som jeg har sagt tidligere i studien min, er cybersikkerhet noe som utvikler seg konstant. Av den grunn er det ekstremt viktig med videre forskning på ulike temaer innenfor dette området.

Referanseliste

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1). https://doi.org/10.1093/cybsec/tyy006

Alhayani, B., Taher, S., Zahi, D. & Mohammed, H. (2021). *Best ways computation intelligent of face cyber attacks*. Hentet fra: https://www.researchgate.net/publication/349946354_Best_ways_computation_intelligent_of_face_cyber_attacks

Alsaawi, A. (2014). A critical review of qualitative interviews. *European Journal of Business and Social Sciences, 2014, Vol. 3, No. 4.* https://doi.org/10.2139/ssrn.2819536

Ameen, N., Tarhini, A., Shah, M. H., Madichie, N., Paul, J., & Choudrie, J. (2021). Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. *Computers in Human Behavior*, *114*, 106531. https://doi.org/10.1016/j.chb.2020.106531

Ansari, F. M., Sharma, K. P., Dash, B., (2022). Prevention of Phishing Attacks Using AI-Based Cybersecurity Awareness Training. *International Journal of Smart Sensor and Adhoc Network.* Vol.3, Article 6. Hentet fra: https://www.researchgate.net/profile/Bibhu-Dash-5/publication/362112009_Prevention_of_Phishing_Attacks_Using_AI-Based_Cybersecurity_Awareness_Training/links/62d6e554593dae2f6a28d4e0/Prevention-of-Phishing-Attacks-Using-AI-Based-Cybersecurity-Awareness-Training.pdf

Atea. *Modenhetsanalyse for informasjonssikkerhet*. (2022). Atea AS. Hentet fra: https://www.atea.no/it-sikkerhet/modenhetsanalyse/

Atea. *Norges Bondelag tar IT-sikkerhet på alvor*. (2022). Atea AS. Hentet fra: https://www.atea.no/kundereferanser/norges-bondelag/

Benaroch, M. (2020). Cybersecurity Risk in IT Outsourcing—Challenges and Emerging Realities. In: Hirschheim, R., Heinzl, A., Dibbern, J. (eds) Information Systems Outsourcing. *Progress in IS*. Springer, Cham. Hentet fra: https://doi.org/10.1007/978-3-030-45819-5_13

Bendovschi, A. (2015). Cyber-attacks – trends, patterns and security countermeasures. *Procedia Economics and Finance*, *28*, 24–31. https://doi.org/10.1016/s2212-5671(15)01077-1

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*. Hentet fra: https://doi.org/10.1191/1478088706qp063oa

Chowdhury, N., Nystad, E., Reegård, K., & Gkioulos, V. (2022). Cybersecurity training in Norwegian critical infrastructure companies. *International Journal of Safety and Security Engineering*, 12(3), 299–310. https://doi.org/10.18280/ijsse.120304

Choy, L. T. (2014). The Strengths and Weaknesses of Research Methodology: Comparison and Complimentary between Qualitative and Quantitative Approaches. *Journal of Humanities and Social Science 19(4):99-104.* https://www.researchgate.net/publication/269752866_The_Strengths_and_Weaknesses_of_Research_Methodology_Comparison_and_Complimentary_between_Qualitative_and_Quantitative_Approaches

Clearswift. (u.å). *What's your employees' price?*. Hentet fra: https://www.clearswift.com/sites/default/files/documents/Infographics/Clearswift_What_is_your_employees_price_infographic.pdf

Dahbur, K., Bashabsheh, Z., Bashabsheh, D., (2017). Assesment of Security Awareness : A Qualitative and Quantitative Study. *Scholarly Journal*, Vol.13, 37-58, 101-102. https://www.proquest.com/openview/ba98a8bc4cf71224c96295ee6eeea0fe/1?pq-origsite=gscholar&cbl=28202

Datatilsynet. *Phishing - hvordan beskytte virksomheten*. (2020). Datatilsynet. Hentet fra: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/phishing---hvordan-beskytte-virksomheten/hva-er-phishing/

De Bruijn, H., & Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1–7. https://doi.org/10.1016/j.giq.2017.02.007

Departementene. (2019). *Nasjonal strategi for digital sikkerhet*. Regjeringen. Hentet fra: https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/nasjonal-strategi-for-digital-sikkerhet.pdf

Didgir. *NSMs grunnprinsipper*. (u.å.). Digitaliseringsdirektoratet. Hentet fra: https://www.digdir.no/informasjonssikkerhet/nsms-grunnprinsipper/2219

Dinkova, M., El-Dardiry, R., & Overvest, B. (2023). Should firms invest more in cybersecurity? *Small Business Economics*. Hentet fra: https://doi.org/10.1007/s11187-023-00803-0

Dimopoulos, V., Furnell, S., Jennex, E. M., Kritharas, I. (2004). *Approaches to IT Security in Small and Medium Enterprises.* Hentet fra: https://www.researchgate.net/publication/221148270_Approaches_to_IT_Security_in_Small_and_Medium_Enterprises

Dunning, D. (2011). The Dunning–Kruger Effect. *Advances in Experimental Social Psychology*, *44*(44), 247–296. https://doi.org/10.1016/b978-0-12-385522-0.00005-6

Erdogan, G., Halvorsrud, R., Boletsis, C., Tverdal, S., & Pickering, J. (2023). Cybersecurity awareness and capacities of SMEs. *Proceedings of the 9th International Conference on Information Systems Security and Privacy*, 296- 304. https://sintef.brage.unit.no/sintef-xmlui/handle/11250/3056514

Ergen, A., Ünal, N.A., Saygili, S.M. (2021). Is It Possible to Change the Cyber Security Behaviours of Employees? Barriers and Promoters. *Academic Journal of Interdisciplinary Studies*. Hentet fra: https://www.richtmann.org/journal/index.php/ajis/article/view/12588

Estil, S. (2023). *Hva er løsepengevirus og hvordan beskytte seg mot angrep?*. Visma Software. Hentet fra: https://www.vismasoftware.no/artikler/hva-er-losepengevirus-og-ransomware-og-hvordan-beskytte-seg-mot-angrep

Fadia, A., Nayfheh, M., Noble, J., (2020) *Follow the leaders: How governments can combat intensifying cybersecurity risks*. Hentet fra: https://www.mckinsey.com/industries/public-sector/our-insights/follow-the-leaders-how-governments-can-combat-intensifying-cybersecurity-risks

FenceNordic. (u.å). *Sikkerhetspolicy*. FENCE. Hentet fra: https://fencenordic.com/tjenester/informasjonssikkerhetspolicy

Gawel, H. (2024). *Hacktivism*. Internet Policy Review. Hentet fra: https://policyreview.info/glossary/hacktivism

Geer, D.(2024). *The risks of source code breaches*. Acm.org. Hentet fra: https://cacm.acm.org/news/the-risks-of-source-code-breaches/

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., Jabbar, S., & Baker, T. (2018). Security threats to critical infrastructure: the human factor. *The Journal of Supercomputing*, *74*(10), s. 4986–5002. https://doi.org/10.1007/s11227-018-2337-2

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2018). Empirical Evidence on the Determinants of Cybersecurity Investments in Private Sector Firms. *Journal of Information Security*, *09*(02), 133–153. https://doi.org/10.4236/jis.2018.92010

Gupta, A & Zhdanov, D. (2012). Growth and sustainability of managed security services networks: An economic perspective. *MIS Quarterly: Management Information Systems*, 36(4), 1109- 1130. https://doi.org/10.2307/41703500

Haqaf, H., & Koyuncu, M. (2018). Understanding key skills for information security managers. *International Journal of Information Management*, *43*, 165–172. https://doi.org/10.1016/j.ijinfomgt.2018.07.013

Hooper, V., & McKissack, J. (2016). The emerging role of the CISO. *Business Horizons*, 59(6), 585–591. https://doi.org/10.1016/j.bushor.2016.07.004

Huang, K., & Pearlson, K. (2019). *For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture*. Hentet fra: https://scholarspace.manoa.hawaii.edu/items/c2f05c8b-a609-4c08-8dea-2d1c4e453b88

Jayasinghe, K & Poravi, G. (2020). *A Survey of Attack Instances of Cryptojacking Targeting Cloud Infrastructure*. Hentet fra: https://www.researchgate.net/publication/340278271_A_Survey_of_Attack_Instances_of_Cryptojacking_Targeting_Cloud_Infrastructure

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. (2018). *What is the impact of successful cyberattacks on target firms?* National Bureau of Economic Research. Hentet fra: https://www.nber.org/system/files/working_papers/w24409/w24409.pdf

Kemper, G. (2019). Improving employees' cyber security awareness. *Computer Fraud & Security*, *2019*(8), 11–14. https://doi.org/10.1016/s1361-3723(19)30085-5

Kendall, L. (2014). The Conduct of Qualitative Interviews: Research Questions, Methodological Issues, and Researching Online. In *Handbook of Research on New Literacies* (pp. 133-149). Taylor and Francis. https://doi.org/10.4324/9781410618894-7

KnowBe4. (2022). *Introducing the Security Culture Maturity Model*. Hentet fra: https://www.bu.edu/tech/files/2022/08/Resource_Security-Culture-Maturity-Model-WP_EN-US.pdf

Kohn, A., (2014). *Brain Science: The Forgetting Curve-the Dirty Secret of Corporate Training*. Hentet fra: https://www.learningguild.com/articles/1379/brain-science-the-forgetting-curvethe-dirty-secret-of-corporate-training/?rd=1

Koziol, J. (2022). Cybersecurity Awareness: What it is and how to start. *Forbes Advisor*. Hentet fra: https://www.forbes.com/advisor/business/what-is-cybersecurity-awareness/

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, *22*, 113–122. https://doi.org/10.1016/j.jisa.2014.09.005

Kunnskapsdepartementet. (u.å.). *Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor*. Regjeringen. Hentet fra: https://www.regjeringen.no/no/dokumenter/styringsdokument-for-arbeidet-med-samfunns-sikkerhet-og-beredskap-i-kunnskapssektoren/id2512037/?ch=9

Leroy, I. (2022). The relationship between cyber-attacks and dynamics of company stock: the role of reputation management. *International Journal of Electronic Security and Digital Forensics*, 14(4), 309. https://doi.org/10.1504/ijesdf.2022.123891

Leu, D. M., Udroiu, C., Raicu, G. M., Gârban, H. N., & Șcheau, M. C. (2023). Analysis of some case studies on cyber attacks and proposed methods for preventing them. *Romanian Journal of Informatics and Automation*. 33(2), 119–134. https://www.researchgate.net/publication/371947489_Analysis_of_some_case_studies_on_cyber attacks_and_proposed_methods_for_preventing_them

Liu, C., Wang, N., & Liang, H. (2020). Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment. *International Journal of Information Management*, 54, 102152. https://doi.org/10.1016/j.ijinfomgt.2020.102152

Loeb, L. (2023). Færre alvorlige cyberangrep enn tidligere. *DNB Nyheter.* Hentet fra https://www.dnb.no/dnbnyheter/no/samfunn/faerre-alvorlige-cyberangrep-enn-tidligere

Tam, T., Rao, A., & Hall, J. (2021). The good, the bad and the missing: A Narrative review of cyber-security implications for Australian small businesses. *Computers & Security*, *109*, 102385. https://doi.org/10.1016/j.cose.2021.102385

Tenny, S., Brannan, M.J., Brannan, D.G., (2017). *Qualitative Study*. Hentet fra: https://europepmc.org/article/NBK/nbk470395

This is SINTEF. (2012). SINTEF. Hentet fra: https://www.sintef.no/globalassets/upload/konsern/media/fakta-tekster/sintef_faktaark_2012_e.pdf

Toapanta, S. M. T., Cobeña, J. D. L., & Gallegos, L. E. M. (2020). Analysis of cyberattacks in public organizations in Latin America. *Advances in Science Technology and Engineering Systems Journal*, *5*(2), 116–125. https://doi.org/10.25046/aj050215

Tundis, A., Mazurczyk, W., & Mühlhäuser, M. (2018). A review of network vulnerabilities scanning tools: Types, capabilities and functioning. *Proceedings of the 13th International Conference on Availability, Reliability and Security.* Hentet fra: https://dl.acm.org/doi/10.1145/3230833.3233287

Makridis, C. A. (2021). Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018. *Journal of Cybersecurity*, 7(1). https://doi.org/10.1093/cybsec/tyab021

McAfee. (2018). *Key mobile threat takeaways from the 2018 mobile threat report*. McAfee Blog. Hentet fra: https://www.mcafee.com/blogs/mobile-security/key-mobile-threat-takeaways-2018-mobile-threats-report/

Millaire, P., Sathe, A., & Thielen, P. (2017). *What All Cyber Criminals Know: Small & Midsize Businesses With Little or No Cybersecurity Are Ideal Targets*. Chubb. Hentet fra: https://www.chubb.com/content/dam/chubb-sites/chubb-com/us-en/business-insurance/simple-measures-to-create-cyber-risk-management-program/documents/pdf/17010201-cyber-for-small_midsize-businesses-10.17.pdf

Mohammed, A. I., (2011). Identity and Access Management System: a Web-Based Approach for an Enterprise. *International Journal of Advanced and Innovative Research*. Vol.1, Iss. 4. Hentet fra: https://www.researchgate.net/profile/Ishaq-Azhar-Mohammed/publication/353887611_Identity_and_Access_Management_System_a_Web-_Based_Approach_for_an_Enterprise/links/6116a022169a1a0103fc6432/Identity-and-Access-Management-System-a-Web-Based-Approach-for-an-Enterprise.pdf

Möller, D.P.F. (2023). *Cybersecurity Maturity Models and SWOT Analysis*. Guide to Cybersecurity in Digital Transformation. Advances in Information Security, vol 103 . Springer, Cham. Hentet fra: https://doi.org/10.1007/978-3-031-26845-8_7

NCSC(National Cyber Security Centre). (2017). *Penetration testing*. Hentet fra: https://www.ncsc.gov.uk/guidance/penetration-testing

NSM. *Cyberangrep har blitt hverdagskost*. (2022). Nasjonal sikkerhetsmyndighet. Hentet fra: https://nsm.no/aktuelt/digitalt-risikobilde-2022-cyberangrep-har-blitt-hverdagskost

NSM. (2023). *Cybersikkerhet*. Nasjonal sikkerhetsmyndighet. Hentet fra:

https://nsm.no/regelverk-og-hjelp/rapporter/cybersikkerhet/

Onwubiko, C., & Ouazzane, K. (2022). Challenges towards building an effective Cyber

Security Operations Centre. *arXiv*. Hentet fra: http://arxiv.org/abs/2202.03691

PwC. (2023). *Cybercrime Survey 2023*. Hentet fra:

https://publikasjoner.pwc.no/cybercrime-survey-2023/

Ray, A & Nath, A. (2016). Introduction to Malware and Malware Analysis: A brief overview. *International Journal of Advance Research in Computer Science and Management Studies*. Volume 4, Issue 10. Hentet fra: https://www.scribd.com/document/477968182/V4I10-0008

Reegård, K., Blackett, C., Katta, V., (u.å.). *The Concept of Cybersecurity Culture.* Hentet fra: https://www.researchgate.net/profile/Kine-Reegard/publication/336149766_The_Concept_of_Cybersecurity_Culture/links/5d9321a9458515202b7789f1/The-Concept-of-Cybersecurity-Culture.pdf

Von Solms, R., & van Niekerk, J. (2013). From information security to cyber security.

Computers & Security, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Watkins, B. (2014). *The Impact of Cyber Attacks on the Private Sector.* Mindpoint Group. Hentet fra: https://www.amo.cz/wp-content/uploads/2015/11/amocz-BP-2014-3.pdf

Wolf, F., Aviv, A. J., & Kuber, R. (2021). *Security Obstacles and Motivations for Small Businesses from a CISO's Perspective*. Hentet fra: https://www.usenix.org/conference/usenixsecurity21/presentation/wolf

W, Anne. (2018). *Maturity models in cyber security: what's happening to the IAMM?*. NCSC (National cyber security center). Hentet fra:

https://www.ncsc.gov.uk/blog-post/maturity-models-cyber-security-whats-happening-iamm