MASTEROPPGAVE

Emnekode: LED5018

Navn: Andreas Lucas Wold

Digital sikkerhetskultur i store norske virksomheter

Dato: 28.11.2023

Totalt antall sider: 89

NORD universitet

www.nord.no

Abstract:

In recent times, there has been an increase in cyber-attacks against Norwegian and international businesses. The actors behind it can be deliberate in their choices and attack vectors or they can be completely random based on which systems they gain access to. The common denominator is that for the actors behind the attacks, there is often a financial gain. Digital security culture is a highly topical topic, and in recent times it is the managers of the businesses who get reviewed in the literature and who are designated as responsible for security, the level of security, and the digital security culture. I have therefore arrived at the following problem:

"To what extent have managers in large Norwegian businesses introduced a digital security culture in the business, and how are measures and investments in security technology and expertise prioritized to reduce the risk of being exposed to cyber-attacks?"

The concept of digital security culture is quite new, and most of the literature has been published in recent years. I have chosen to look at traditional theories around organizational culture, security culture, risk and supplemented with newer theory around digital security culture. Where, among other things, managers' responsibilities, management systems and costs linked to cyber-attacks. The project was carried out as a descriptive design with quantitative method and cross-sectional survey. The data collection was done by means of a pre-coded anonymous survey which was sent out by e-mail and where 38 C-level managers replied. The data were then processed in SPSS and Excel for analyses.

The results of the survey show that the businesses have, to some extent, largely introduced a digital security culture in the businesses in line with Dan Blum's maturity model. Analyzes support this in that the anchoring of security work in management is linked to digital security culture and management measures within digital security culture. The businesses characterize the risk of being exposed to cyber-attacks as being to some extent, and investments and measures in security technology and increasing the competence of personnel help to reduce the risk of cyber-attacks to a large extent. The businesses prioritize increased competence of key personnel in information and cyber security as the highest priority measures to reduce the risk of being exposed to cyber-attacks. Analyzes further show that there is no connection between prioritized measures within security technology, increased competence, the effect of measurements or the outsourcing of security work against the risk of being exposed to cyber-attacks. This contradicts current explored theory.

Sammendrag:

I nyere tid har det vært en økning av cyberangrep mot norske og internasjonale virksomheter. Aktørene bak kan være bevisste i sine valg og angrepsvektorer eller de kan være helt tilfeldig ut fra hvilke systemer de får tilgang til. Fellesnevneren er at for aktørene bak angrepene så er det ofte en økonomisk vinning. Digital sikkerhetskultur er et høyaktuelt tema, og i nyere tid er det lederne i virksomhetene som får gjennomgå i litteraturen og som blir utpekt som ansvarlig for sikkerheten, og nivået av sikkerheten, og den digitale sikkerhetskulturen. Jeg har derfor kommer frem til følgende problemstilling:

«I hvilken grad har ledere i store norske virksomheter innført digital sikkerhetskultur i virksomheten, og hvordan prioriteres tiltak og investeringer i sikkerhetsteknologi og kompetanse for å minske risikoen for å bli utsatt for cyberangrep?»

Begrepet digital sikkerhetskultur er ganske nytt, og mesteparten av litteraturen er publisert de siste årene. Jeg har valgt å se på tradisjonelle teorier rundt organisasjonskultur, sikkerhetskultur, risiko og supplert med nyere teori rundt digital sikkerhetskultur. Hvor det blant annet er sett på leders ansvar, styringssystemer og kostander knyttet opp til cyberangrep. Prosjektet ble gjennomført som et deskriptivt design med kvantitativ metode og tverrsnittsundersøkelse. Datainnsamlingen ble gjort ved en prekodet anonym spørreundersøkelse som ble sendt ut per e-post og hvor 38 ledere på c-nivå. Dataene ble deretter behandlet i SPSS og Excel for analyser.

Resultatene fra undersøkelsen viser at virksomhetene har i noen grad til stor grad innført digital sikkerhetskultur i virksomhetene opp mot Dan Blums modenhetsmodell. Analyser støtter dette opp ved at forankring av sikkerhetsarbeid i ledelsen har sammenheng med digital sikkerhetskultur og ledelsestiltak innen digital sikkerhetskultur. Virksomhetene karakterisere risikoen for å bli utsatt for cyberangrep til å være i noen grad, og investeringer og tiltak i sikkerhetsteknologi og økning av kompetanse hos personell bidrar til å minske risikoen for cyberangrep i stor grad. Virksomhetene prioriterer økt kompetanse hos nøkkelpersonell innen informasjon- og cybersikkerhet som høyeste prioriterte tiltak for å minske risikoen for å bli utsatt for cyberangrep. Analyser viser videre at det er ingen sammenheng mellom prioriterte tiltak innen sikkerhetsteknologi, økt kompetanse, effekt av målinger eller outsourcing av sikkerhetsarbeid opp mot risikoen for å bli utsatt for cyberangrep. Dette motstrider gjeldende utforsket teori.

Forord:

Denne masteroppgaven vil avslutte mitt masterstudium i MBA ved Nord Universitet. Oppgaven omhandler Digital sikkerhetskultur i store norske virksomheter og er et tema jeg har interessert meg for tilbake til 2018. Feltet har hatt store utfordringer fra et organisatorisk ledelsesperspektiv, men også kulturelt.

Prosessen har vært veldig interessant og lærerik, og har gitt meg et større innblikk i både digital sikkerhetskultur, men også metodefaget og utallige dypdykk i havet av relevant og ikke relevant faglitteratur. Jeg håper oppgaven kan gi noe nytt til feltet digital sikkerhet, og at den også kan komme andre til gode som måtte finne interessen av fagfeltet.

Jeg ønsker å rette en takk til min veileder, Johan Olaisen, for meget gode samtaler, veiledning og konstruktive tilbakemeldinger gjennom prosessen. Jeg ønsker også å rette en takk til de ve Nord Universitet som har bistått til oppgaven via mail. Også vil jeg gi en takk til alle de anonyme store virksomhetene som svarte på min spørreundersøkelse, uten de hadde det ikke blitt en oppgave! Og takk til min arbeidsgiver som ha gitt meg mulighet å fullføre studiet.

Det har vært utfordrende å kombinere fulltidsjobb med mer sammen med studiet. Jeg vil gi en spesiell takk til min samboer og venner som har vært tålmodige og forståelsesfull.

Innholdsfortegnelse

Oversikt over figurer

Oversikt over tabeller:

Oversikt over vedlegg:

1. Vedlegg 1 – Digitalsikkerhetskultur i store norske virksomheter spørreundersøkelse
2. Vedlegg 2 – Kodebok spørreundersøkelse

Begrepsordliste

- **Digital sikkerhet, informasjonssikkerhet, IKT-sikkerhet eller cybersikkerhet.**
  Begreper som ofte blir benyttet om hverandre. Til felles for alle er beskyttelsen av informasjon eller verdier, og hvor det blir en definisjon om det er digital- eller fysisk sikring (Digdir, uå). Digital sikkerhet handler om å styre risikoen i oppgaver og tjenester som er avhengige av digital- teknologi eller tjenester og innføre tiltak for å minke risikoen (Digdir, uå).
  I denne oppgaven vil begrepet digital sikkerhet/cybersikkerhet bli benyttet, og vil være en samledefinisjon for også de øvrige begrepene
- **Cyberangrep**
  Definisjon på trusler virksomhetene står ovenfor og som de prøver å beskytte seg mot digitalt.
- **Styringssystem**
  Styringssystem for informasjonssikkerhet er de kontinuerlige prosessene og aktivitetene som skal sikre oversikt og internkontroll samt et systematisk og helhetlig arbeid med informasjonssikkerheten.
- **Rammeverk**
  Et sett med prosesser, kontrollere og definering av krav.
- **Tiltak**
  Prosess, aktivitet eller løsning som har en hensikt å gjøre en endring eller oppnå noe. I dette tilfellet opp mot digital sikkerhetskultur.
- **C-nivå**
  Høytstående rangerte ledertitler i virksomheter eller organisasjon.

1.0 Innledning

I senere tid har det vært en økning av cyberoperasjoner og dataangrep både mot norske- og internasjonale virksomheter. Nasjonal sikkerhetsmyndighet (NSM) viser i sin årlige sikkerhetsrapport «Risiko 2023» at det har vært en tredobling av alvorlige cyberoperasjoner mot norske myndigheter og virksomheter siden 2019 – 2021, og at nivået av antallet alvorlige og svært alvorlige hendelser i 2022 har vært lik som forrige år (NSM, 2023, s. 18). Der imot har antallet vellykkede kompromitteringer vært lavere i 2022 (ibid). Cyberoperasjoner og dataangrep kan ramme enhver virksomhet og ofte flere samtidig eller på tvers (NSM, 2022, s. 26). NSM påpeker at de ser et økt fokus hos virksomheter innen sikkerhetsarbeid, innførte tiltak og innrapporteringer av hendelser, men at det fortsatt er et gap mellom ønsket sikkerhetsnivå og status i mange virksomheter (NSM, 2023, s. 18).

«*For det første øker gapet mellom trusselen og sikkerhetsnivået i norske virksomheter og samfunnsfunksjoner. Det skyldes blant annet at bevisstheten og kompetansen om trussel- og risikobildet og hva som utgjør god nok sikkerhet, er for svak. Sikkerhetstiltakene er ikke dimensjonert for det reelle trusselbildet eller innføres ikke raskt nok når nye sårbarheter oppstår. Forståelsen for trussel- og risikobildet må økes og tiltak må iverksettes nå. Dette er et ledelsesansvar*.» (NSM, 2022, s.8; Wold, 2022).

Hydro ble rammet av et løsepengevirus i 2019 som bidro til at 22 000 datamaskiner måtte frakobles, og det tok flere måneder før systemene var tilbake i normalt drift (Wernersen, 2020; Wold, 2022). Da Stortinget august 2020 og mars 2021 ble utsatt for cyberangrep var det for sistnevnte en nulldagssårbarhet som ble utnyttet, og hvor systemene ikke var blitt oppdaterte til nyere versjoner i tide (Strand et al. 2020; Gausen et al., 2021; NSM, s. 27; Wold, 2022, s. 1). Utnyttelsen av programvaresårbarheter har vært en stor del årsaken til de fleste cyberangrep de siste årene, og tiden fra en sårbarhet blir kjent til den utnyttes har blitt kortere. Dette viser til viktigheten med en bevisst og tilstedeværende sikkerhetskultur i norske virksomheter, både hos ansatte og ledere (NSM, 2023, s. 19).

Cyberoperasjoner- og angrep kan ha store økonomiske konsekvenser på virksomheter, men det kan også få konsekvenser for enkelt individer eller kunder av virksomheten hvis data havner på avveie (NSM, 2022, s. 26; Wold, 2022 s. 1). Flere virksomheter eller personer tror ikke de kan være mål for cyberangrep fordi de «ikke har noen verdier».

Kostnader av å bli utsatt for et cyberangrep for små og mellomstore virksomheter (SMB) kan variere, men kan i verste fall få enorme økonomiske konsekvenser (Rinaldi, 2023). I følge Kaspersky er gjennomsnittlig kostnad for et cyberangrep mot små og mellomstore virksomheter alt fra 98 000 dollar – 118 000 dollar (Kaspersky, 2020; Wold, 2022). IBMs årlige sikkerhetsrapport om kostnader for å bli utsatt for cyberangrep har et gjennomsnitt på verdensbasis på 4.35 millioner dollar, og er en økning på 26% fra 2021 (IBM, 2022). Cyberangrepet mot Hydro var beregnet til å koste virksomheten 350 millioner norske kroner (Wilberg, 2023).

Oppgaven skal med bakgrunn i overnevnte se på i hvilken grad digital sikkerhetskultur er innført i store norske virksomheter, hvordan ledelsen er involvert, og hvilke investeringer og tiltak som er gjort for å sikre bedriftene digitalt. Temaet har hatt høyt fokus i samfunnet de siste årene, men det er lite forskning i Norge på området, og spesielt mot større virksomheter, noe som gjør det interessant å undersøke nærmere.

1.1 Aktualisering

I Risiko 2022 poengteres det at det grunnleggende sikkerhetsnivået i norske virksomheter er for lavt (NSM, 2022, s.36; Wold, 2022). Digital årvåken og sikkerhetskultur blant ansatte er en viktig faktor, men det er ikke tilstrekkelig for å beskytte virksomheter mot cyberoperasjoner og cyberangrep (NSM, 2021, s. 14; Wold, 2022). En kommer ikke utenom digitale og tekniske sikkerhetsløsninger som kan forhindre eller redusere omfanget. Et redusert digitalt sikkerhetsnivå på enkelte områder kan også føre til flere sårbarheter på andre områder. Dette betyr at sikkerhetsfokuset hos virksomheter må omfatte både organisatoriske, teknisk og menneskelig nivå (NSM, 2021, s. 14; Wold, 2022).

I henhold til en studie fra universitet i Melbourne hvor forholdet mellom organisasjonskultur og digital sikkerhetskultur ble studert, så viste et av funnene at sikkerhetskultur må forenes som en del av organisasjonskulturen ved å øke kompetansen til de ansatte (Lim et al, 2009, s. 94). Dette vil bidra til at virksomheten beskytter sine verdier og informasjon bedre. De påpeker også at den ekte sikkerhetskulturen defineres av de ansattes forståelse og verdier rundt sikkerhet, og at dette vil definere deres handlinger og atferd innen digital sikkerhetskultur (ibid; Wold, 2022).

Bergsjø og Windvik poengterer at det er lederne i virksomheten som er ansvarlig for sikkerheten, og nivået av sikkerheten. For å få til et godt sikkerhetsnivå så må dette være forankret i ledelsen og i styret for virksomheten, og det bør være et styringssystem som

ivaretar og beskriver hvordan virksomhetene skal håndtere sikkerhetsarbeid, tiltak, investeringer og aktiviteter (Bergsjø & Windvik, s. 27, NSM 2021).

Innen cybersikkerhet og informasjonssikkerhet så er det ofte menneskelige feil, mangel på kunnskap og tekniske svakheter i systemer som er årsaken til at cyberangrep er vellykkede. I henhold til Næringslivets Sikkerhetsråds Mørketallsundersøkelse, 2020, var hovedårsakene til sikkerhetsbrudd på grunn av tilfeldigheter og uflaks, og menneskelige feil som nummer 2 (NorSIS, 2020).

I de siste årene har det vært et økt søkelys på sikkerhetskultur og cybersikkerhet, dette har ført til en økning på forskning relatert til disse temaene, men det er fortsatt begrenset litteratur å finne i Norge. I resten av verden har dette hatt et større fokus, men litteraturen er fortsatt noe begrenset.

Ved Nord universitet ble det levert to masteroppgaver i 2021 som forsket på sikkerhetskultur og cybersikkerhet.

Pettersen, 2021 forsket på hvordan persepsjon og håndtering av cyberrisko var i små og mellomstore virksomheter. Funnene fra studien viser at cyberrisko ble oppfattet som en stor trussel blant små- til mellomstore virksomheter, og hvor de fleste var avhengig av IT-systemer i daglige virket. Kun 32% hadde gjennomført opplæring på ansatte innen digital sikkerhet, og 40% hadde prosedyrer og styringssystem (Pettersen, 2021, s. 73). Resultatene viste også til at bedriftsledere så på cyberrisko på lik linje med operasjonell risiko. For mellomstore virksomheter var utvalget lite for å bekrefte om mellomstore virksomheter hadde en høyere persepsjon av risiko. Innført tiltak og tillit til håndtering av cyberangrep var signifikante, men kunne ikke si noe om tiltak eller tillit til håndtering var til stede før hendelsene (ibid, s. 74).

I den andre masteroppgaven levert av Gunnes, 2021, omhandlet digital sikkerhetskultur i samfunnskritiske funksjoner og da spisset mot finans-kraft og justissektoren. Hovedfunnene i oppgaven viser at arbeidet med innføring av digital sikkerhetskultur vil i all hovedsak være lik for alle virksomheter, og at det ikke krever noe mer å innføre enn annet sikkerhetsarbeid (Gunnes, 2021, s. 124). Det bemerkes også at den menneskelige faktoren ofte er det svakeste ledd, og at opplæring av ansatte for å øke bevisstheten og atferden rundt digital sikkerhetskultur og tiltak settes høyt (ibid, s. 124). Manglende strategier og fokus på sikkerhet fra ledelsen kan føre til uklare ansvarsforhold.

Lederne må sørge for forankring av digital sikkerhet helt til toppen av virksomheten, og det må utarbeides et styringssystem som blir kommunisert både horisontalt og vertikalt i virksomheten (Gunnes 2021, s. 123). For å oppnå dette er ledelsen avhengig av riktig informasjon om risiko- og trusselbildet. Gunnes påpeker også at en videre forskning på funnen opp mot ansatte og ledere vil kunne gi et bedre svar på hvordan nivået av digital sikkerhetskultur er i norske virksomheter.

Med bakgrunn i avsnittene ovenfor vil det være interessant videre i oppgaven og studere hvordan nivået av digital sikkerhetskultur er i norske virksomheter, hvilken involvering har lederne, har de et styringssystem for digital sikkerhet, og måler de effekten på kulturen og innførte tiltak. Med bakgrunn i Pettersen og Gunnes sin forskning så vil det også være interessant å se på hvor mye virksomhetene investerer i kompetanseheving og sikkerhetsteknologi, og om dette måles, og for de virksomhetene som har vært utsatt for cyberangrep, kom tiltakene og kulturen før eller etter hendelsene.

1.2 Problemstilling og forskningsspørsmål

Med en egeninteresse innenfor cybersikkerhet, organisasjonsutvikling og digital sikkerhetskultur og med utgangspunkt i funn fra rapporter, teorier og forskning så er det tydelig at digital sikkerhetskultur trenger større fokus i virksomheter. Det må forankres i ledelsen, og de er ansvarlige for at de ansatte får opplæring og blir mer bevisste rundt digital sikkerhet. Det ble derfor et naturlig ønske å forske videre på hvordan lederne i virksomheter har innført digital sikkerhetskultur. Jeg kom derfor frem til følgende problemstilling:

«I hvilken grad har ledere i store norske virksomheter innført digital sikkerhetskultur i virksomheten, og hvordan prioriteres tiltak og investeringer i sikkerhetsteknologi og kompetanse for å minske risikoen for å bli utsatt for cyberangrep?»

For å videre kunne besvare problemstillingen kom jeg frem til følgende forskningsspørsmål:

1. I hvilken grad har ledere i virksomhetene innført digital sikkerhetskultur?
    a. Har de forankret sikkerhetsarbeid i ledelsen, og har dette sammenheng med innført styringssystem for sikkerhet og digital sikkerhetskultur som en del av strategien?
2. Har prioriteringer av tiltak sammenheng med risiko for å bli utsatt for cyberangrep?
3. Har investeringer i teknologi og kompetanse sammenheng med risiko for å bli utsatt for cyberangrep?

1.3 Operasjonalisering og avgrensning

1.3.3 Sikkerhetskultur og digital sikkerhetskultur

Sikkerhetskultur er den del av organisasjonskulturen i en virksomhet, og handler om hvordan organisasjons atferds- og oppfatningsmønstre innad er med å bestemme hvordan virksomheten håndterer og oppfatter sikkerheten (Blum, 2020, s. 97). Det er en sammenslåing av virksomheters oppfattelse og oppførsel innenfor IT, sikkerhetssystemer, sikkerhetspolicyer og operasjonelle sikkerhetspraksiser eller prosjekter. Sikkerhetskulturen er under konstant utvikling både fra teknologi og menneskers erfaringer med sosiale- og digitale interaksjoner. Sikkerhetskulturen kan også ha en effekt på virksomhetens risikooppfattelser, gjeldende bestemmelser og regler, eller påvirke kostnader og investeringer positivt eller negativt (ibid). Virksomhetens ledere kan selve velge om de vil ignorere det eller om de vil utnytte det til det positive. Den generelle sikkerhetskulturen i en virksomhet kan en anse å omhandle både fysisk og digital sikkerhet, men da i forskjellige domener, men empirien vil være gjeldene for begge. For denne oppgaven er det den digitale sikkerhetskulturen i virksomhetene som skal utforskes.

Digital sikkerhet, informasjonssikkerhet, IKT-sikkerhet eller cybersikkerhet er begreper som ofte blir benyttet om hverandre. Til felles for alle er beskyttelsen av informasjon eller verdier, og hvor det blir en definisjon om det er digital- eller fysisk sikring (Digdir, uå). Digital sikkerhet handler om å styre risikoen i oppgaver og tjenester som er avhengige av digital-teknologi eller tjenester og innføre tiltak for å minke risikoen (Digdir, uå).

I denne oppgaven vil begrepet digital sikkerhet/cybersikkerhet bli benyttet, og vil være en samledefinisjon for også de øvrige begrepene. I tillegg vil cyberangrep bli benyttet som definisjon på trusler virksomhetene står ovenfor og som de prøver å beskytte seg mot.

1.3.4 Ledelse innen digital sikkerhetskultur

Ivaretakelse av digital sikkerhet og kultur er et virksomhetsansvar (Regjeringen, 2019). Dette betyr at lederne i virksomheten er ansvarlig for at risikovurderinger, policyer, styringssystem og andre nødvendige tiltak er iverksatt for den totale sikkerheten i virksomheten. For å få til et godt sikkerhetsnivå så må den digitale sikkerhetskulturen være forankret i ledelsen og i styret til virksomheten, og det bør være et styringssystem som ivaretar og beskriver hvordan virksomhetene skal håndtere sikkerhetsarbeid, tiltak, investeringer og aktiviteter (Bergsjø & Windvik, s. 27; NSM 2021; Wold, 2022).

Det vil med bakgrunn i overnevnte være interessant å se på hvordan ledere og virksomheten styrer en eventuell digital sikkerhetskultur, og er det innført et styringssystem for digital sikkerhet. Det vil også være naturlig å se på hvordan virksomhetene prioriterer tiltak for å redusere risikoen for å bli utsatt for cyberangrep. For virksomheter som har vært utsatt for cyberangrep vil det også være interessant å se på kostnader og om sikkerhetskultur og tiltak var innført i forkant eller ikke. Oppgaven vil ikke se på hvilke typer angrep virksomheten er utsatt for.

1.3.5 Virksomhetens investeringer i sikkerhetsteknologi og kompetanseutvikling

Sikkerhetskulturen får stadig større fotfeste i virksomheter, og dette fordi erkjennelsen av at sikkerheten til en virksomhet er avhenger like mye av de ansattes holdninger og kompetanse, som tekniske løsninger, og IT-avdelingen (Nätt, 2021, s. 365). Menneskelige feil, dårlig oppførsel og uheldigheter er ofte hovedårsakene til at virksomheter blir utsatt for cyberangrep (Blum, 2020, s. 91). Virksomheter må ha fokus på kompetanseutvikling i form av sikkerhetsopplæring og bevisstgjøring av ansatte, og ikke bare fokusere på digitale sikkerhetstjenester- og teknologi. Virksomheter har ofte en tendens til å investere hyppig på sikkerhetsteknologi istedenfor å la ansatte bruke tid på kursing innen digital sikkerhet fordi sistnevnte anses som for kostbart og problematisk (Nätt, 2021, s. 366). Sikkerhetsteknologi i oppgaven er teknologi som øker sikkerhetsnivået til virksomheten, og som er med på å senke risikoen for å bli utsatt cyberangrep.

For oppgavens del vil det derfor være interessant å se nærmere på hva virksomheters investeringer er innen sikkerhetsteknologi og kompetanseutvikling, og i hvilken grad ledelsen er involvert. Dette bør også ses på i sammenheng med omsetningen til virksomheten. Det kan også vil også være aktuelt å utforske hvilke metoder som benyttes for å øke ansattes kompetanse, og om effektene av investeringer måles for å se om de faktisk utfører det de var tiltenkt.

1.3.6 Små og mellomstore virksomheter og forskningsdesign

Små og mellomstore virksomheter er definert både nasjonalt og internasjonalt, men definisjonene på antall ansatte eller omsetning kan være forskjellig for om de er store, mellomstore eller små (Erichsen et al, 2018). For denne oppgaven er det valgt å ta

utgangspunkt i den norske modellen da forskningen retter seg mot norske virksomheter. Med bakgrunn i forskningen gjort av Pettersen, 2021 om virksomheters persepsjon av cyberrisko var utvalget av virksomheter i kategorien mellomstor og stor lite representert. Med bakgrunn i dette skal oppgaven omfatte store norske virksomheter, som er virksomheter med ansatte over 250 (Erichsen et al, 2018).

Valget av forskningsdesign falt på deskriptivt design og kvantitativ metode med en tverrsnittsundersøkelse. Dette vil bli ytterligere belyst i metodekapittelet.

1.4 Oppgavens oppbygning

Oppgavens oppbygning videre vil ta for seg følgende temaer:

Kapitel 2 – Teori – vil gå gjennom de sentrale teoriene for oppgaven som organisasjonskultur, sikkerhetskultur, digital sikkerhetskultur og virksomheters oppfattelse av risiko.

Kapitel 3 – Metode – omhandler hvilken forskningsmetodikk og modell som blir brukt for å gjennomføre undersøkelsen.

Kapitel 4 – Analyse – presenterer data og funn gjort i undersøkelsen opp mot valgt metode og modell.

Kapitel 5 – Resultater – presentere resultatene og hvor de diskuteres opp mot relevant teori og presenterer konklusjon.

2.0 Teoretiske momenter

2.1 Organisasjonskultur

Organisasjonskultur har blitt forsket på siden 1920-tallet, og har hatt forskjellige opphav og teorier om hvordan det skal defineres. Det som imidlertid bidro til begrepets popularitet innen forskning var at det ble hevdet at suksessen til virksomheter kom fra hvordan kulturen i virksomhetene var. Det var ikke før på 1980-tallet at en begynte å få en fundamental forståelse for hva organisasjonskultur er gjennom Edgar H. Scheins bok «Organizational culture and leadership» fra 1984. (Bang, 2020, s. 24). En populær definisjon på organisasjonskultur som er gjengitt i flere bøker og publikasjoner er fra Deal & Kennedy (1982): «*Kultur er måten vi gjør tingene på her hos oss» (Bang, 2020).*

Bang selv velger å definere organisasjonskultur på følgende vis, og er et forklarende begrep enn Deal & Kennedy (Bang, 2020, s. 23):

«*Organisasjonskultur er de sett av felles verdier, normer og virkelighetsoppfatninger som utvikler seg i en organisasjon når medlemmene samhandler med hverandre og omgivelsene, og som kommer til uttrykk i medlemmenes handlinger og holdninger på jobben*»

Innad i en virksomhet og organisasjon vil det kunne oppstå andre kulturer enn organisasjonskulturen, også kalt subkulturer (Bang 2020, s. 27). Martin (1992), definerte dette som differensieringsprinsippet og retter oppmerksomheten mot alle subkulturene som eksisterer i en organisasjon, og forholdet mellom dem. Motsetningen til dette kalles integrasjonsperspektivet hvor hele organisasjonen eller virksomheten ses på som en kultur, og defineringen av hva kulturen består av bestemmes av organisasjons lederne (Bang, 2020, s.27; Jacobsen et al., 2016. s.143). Subkulturer består av medlemmer innad i organisasjonen som samhandler jevnlig, identifisere seg selv eller blir opplevd av andre som en egen gruppe innad i organisasjonen. De deler ofte felles utfordringer, normer, verdier og virkelighetsoppfatninger som de handler ut fra. Det vil alltid oppstå undergrupper eller subkulturer innad i en organisasjon eller virksomhet (Bang, 2020, s. 29). Schein (referert i Bang, 2020, s. 29; Schein, 2017) hevder at kulturer kan utvikles i en hvilken som helst gruppe forutsatt at følgende betingelser er tilsted: a) Gruppen må ha vært lenge nok samme til å ha opplevd betydningsfulle problemer, b) de må ha hatt muligheter til å løse problemer og observert effekten av løsningene, og c) gruppen må ha tatt inn nye medlemmer og overført kompetansen for hvordan en løser problemene til dem. Dette betyr at kultur kan utvikles i

hvilken som helst gruppe, uavhengig av størrelse og bakgrunn. Det være avdelinger eller andre yrkesgrupper i organisasjonen (Bang, 2020, s. 29). I tillegg vil ulike fagmiljøer, profesjoner, personlige karakteristika, og kulturelle bakgrunner fra tidligere utdanninger og arbeid være relevant for hvordan og hvilke kulturer som dannes (Jacobsen & Thorsvik, 2016). En utfordring med subkulturer er at det kan oppstå konflikter mellom dem. Faren er størst når subkulturer får utvikle seg i en retning hvor selektiv persepsjon og rasjonalisering i kombinasjon med mangelfull informasjonstilgang. Dette gjør at ansatte innen en subkultur mener deres arbeid eller jobb er viktigere enn andre oppgaver i organisasjonen, og skaper en form for gruppetenking. Klarer en å unngå dette så kan subkulturer være støttende og fremmende ovenfor hverandre eller eksistere helt uavhengige og derav ikke påvirke hverandre (Jacobsen & Thorsvik, 2016; Bang, 2020).

Lederne i en organisasjon eller virksomhet betraktes ofte som de viktigste kulturskaperne fordi det er de som sitter med mest makt til å kunne prege organisasjonen i forhold til deres virkelighetsdefinisjoner (Schein, 1983, 2017; Bang, 2020). Grunnlegger eller virksomhetsledere i bedrifter og organisasjoner har en stor påvirkning av hvordan kulturen bygges og utvikles fordi de sitter på forretningsidéen, retning, strategi, og hvordan det skal realiseres. De sitter også med styringen på hvordan investeringer og pengene skal brukes (Bang, 2020). Schein (2010; referert i Bang 2020) viser til seks kanaler som lederne kan påvirke organisasjonskulturen:

1. Hva ledere systematisk retter oppmerksomhet mot, måler og kontrollerer i organisasjonen. Med dette så menes det at lederne aktivt kommunisere hva de tror på, verdier og antakelser de har gjennom de områdene innen virksomheten eller organisasjonen som de er opptatt av. De kommunisere også ut de områder de ikke mener er viktig, og det er et budskap i seg selv.
2. Lederes reaksjoner på kritiske hendelser og kriser i en organisasjon eller virksomhet. Under slike hendelser som truer organisasjonen eller virksomheten må lederne ta stilling til hvordan dette skal løses. Gjennom det vil det kunne skapes nye verdier, normer og virkelighetsoppfatninger som vil sette seg i kulturen.
3. Hvordan ledere fordeler ressurser. Lederne eller styrene bestemmer ofte hvordan organisasjonen eller virksomhetene skal investere og hvordan budsjettene internt er oppsatt. Dette forteller noe om hva lederne prioriterer som viktig innad. Hvis lederne i en virksomhet velger å tredoble

opplæringsbudsjettet inne digital sikkerhetskultur, og sørger for at det også settes av tid til dette, så sender det et signal i virksomheten om at digital sikkerhet er viktig, og skal prioriteres og at det verdsettes at det brukes tid på.

4. Bevisst rollemodellering, veiledning og trening. Ledernes atferd i forhold til hva de prioriterer, hvordan de kommuniserer, omtaler kollegaer eller generelt måten de gjøre ting på, vil kommunisere ut til resten av virksomheten hva som er akseptabelt å ikke i form av verdier. Dette kan de også benytte bevisst som et verktøy.
5. Kriterier for fordeling av belønning og status. Ansatte eller medlemmer i en organisasjon eller virksomhet vil lære hva som verdsettes og ikke av lederne gjennom deres formelle eller uformelle belønningssystemer. Ledere får dermed kommunisert ut prioriteringer, verdier og antakelser opp mot den atferden de ønsker og verdsetter.
6. Kriterier for rekruttering, seleksjon, forfremmelse, omplassering og oppsigelse. Lederne styrer ofte ansettelsesprosesser eller har delegert ansvar videre til andre ledere. De kan dermed styre og velge ut riktige personer som passer inn i kulturen med visse verdier og antakelser. I tillegg kommer ledelsens kriterier synlig frem i hvem som blir forfremmet, omplasseres eller i verste fall sies opp.

Organisasjonskultur og subkulturer er viktig for virksomheter, og lederne har og kan derfor ha stor påvirkning for hvordan kulturer utvikler seg eller ikke. Prioriterer de kulturen antar de også at den er funksjonell, og med å bidra til å nå virksomheten eller organisasjonen mål og suksess (Bang, 2020, s. 123) Dette vil være særdeles viktig opp mot digital sikkerhetskultur.

2.2 Sikkerhetskultur

Sikkerhet i en virksomhet eller organisasjon vil være sterkt knyttet opp mot organisasjonskulturen, og sikkerhetskultur blir ofte forstått og forklart som en subkultur (Wiley et al, 2019). Fokuset på sikkerhetskultur er relativt nytt, men begrepet ble først nevnt i forbindelse med Tsjernobyl-ulykken i 1986 for å beskrive hendelsene (Reason, 1997; Gunnes, 2020). Definisjon av sikkerhetskultur handler om verdier, rutiner, kunnskap, holdninger, bevissthet og motivasjon om hvordan sikkerhet oppfattes blant de ansatte i en virksomhet.

Sikkerhetskultur er et samspill i en virksomhet om hva som er farlig og hvordan en håndterer risiko og tiltak for å forhindre eller redusere farene. Hvordan sikkerhetskulturen er i en virksomhet vil også kunne være avgjørende for om det velges enkle løsninger, enn den mer utforende løsningen for å få god nok sikkerhet (Aven et al, 2004, s. 34; Gunnes 2020). Grunnen til at dette har fått et større fokus i senere tid, er erkjennelsen av at for å opprettholde et tilstrekkelig sikkerhetsnivå så avhenger de like mye av ansatte holdninger og kompetanse, enn tekniske og fysiske løsninger (Natt, 2021, s.364). Nätt poengterer videre at fokuset på sikkerhetsopplæring og bevisstgjøring blant ansatte har hatt lite fokus, og at fysiske eller digitale sikkerhetsløsninger er enklere å implementere, møter mindre motstand, og ansvaret kan legges på driftsavdelingene.

Bergsjø og Windvik poengterer at det er lederne i virksomheten som er ansvarlig for sikkerheten, og nivået av sikkerheten. For å få til et godt sikkerhetsnivå og samspill så må dette være forankret i ledelsen og styret for virksomheten, og det bør være et styringssystem som ivaretar og beskriver hvordan virksomhetene skal håndtere sikkerhetsarbeid, tiltak, investeringer og aktiviteter (Bergsjø & Windvik, s. 27; NSM 2021; Jacobsen & Thorsvik, 2013).

I en studie gjennomført i Australia så de på forholdet mellom organisasjonskultur, sikkerhetskultur og bevissthet rundt digital sikkerhet hos ansatte. Studien fant et signifikant forhold mellom organisasjonskultur, sikkerhetskultur og bevissthet rundt digital sikkerhet. Videre fant de at en tydelig definert sikkerhetskultur er det som fremmer ansattes bevissthet innen digital sikkerhet, og at dette igjen vil kunne gi ringvirkninger opp mot organisasjonskulturen (Wiley et al, 2019).

2.3 Digital sikkerhetskultur

Digitaliseringen av virksomheter har før til en nye utfordringer innen digital sikkerhet. I henhold til undersøkelser gjort av Gartner (2020; referert i Blum, 2020) mener 87% av toppledere at digitalisering av virksomhetene er en prioritet. Av disse hadde bare 40% gjennomført digitaliseringen i større skala. Digital transformasjon i virksomheter krever mer fokus på digital sikkerhet, og det betyr ikke nødvendigvis mer informasjonsteknologi (IT), men der imot flere sårbare IT-systemer. Ofte utvikles nye teknologier og systemer uten tilstrekkelig sikkerhet innebygd som gjør virksomheter mer sårbar og øker angrepsflaten for kriminelle (Blum, 2020, s. 3). Menneskelige feil eller tilfeldige hendelser er ofte årsaken eller en medvirkende årsak til nesten et hvert cyberangrep eller digitale angrep mot en virksomhet (Blum, 2020; Nätt, 2021; NSM 2021; Parenty & Domet, 2020; NOU 2015:13; Gunnes, 2020).

Digital sikkerhetskultur omfatter begrepene informasjonssikkerhet, cybersikkerhet, IKT-sikkerhet og digital sikkerhet, og hvordan virksomheter håndterer og styrer dem. Det kan videre defineres som beskyttelsen av informasjon, personer, verdier og teknologi. Som med organisasjons- og sikkerhetskultur defineres digital sikkerhetskultur som et sett med holdninger, forutsetninger, tro, verdier og kunnskap som ansatte eller interessenter har og bruker for å samhandle med en virksomhets digitale systemer og prosedyrer til enhver tid (Da veiga & Eloff, 2010).

Norsk senter for informasjonssikring, NORSIS, har utviklet en modell med kjerneområder som skal definere digital sikkerhetskultur. I modellen består digital sikkerhetskultur av sammenhengen mellom sikkerhetsatferd, kunnskap, læring og interesse, styring og kontroll, holdninger til digitalisering og digital sikkerhet og riskooppfattelse (refert i Digdir u.å).

Figur 1: Digital sikkerhetskultur, NorSIS (referert via Digdir, u.å),

Parenty og Domet (2020) viser til at selv om billioner dollar har blitt brukt på digital sikkerhet har det nødvendigvis ikke utgjort en forskjell. Dette på grunn av et ensidig fokus rett mot teknologi og ikke det som er viktig for en virksomhet, nemlig risiko rettet mot virksomhetens operasjoner og dens strategiske retning. Virksomheter må se mot hva som er deres viktigste aktiviteter og verdier, og hvordan cyberangrep- og trusler kan påvirke disse. Først når en virksomhet har gjort det kan en virksomhet vite hvordan de skal prioritere tiltak for å beskytte dem. Videre fremhever de at styret og toppledelsen i en virksomhet må sette seg inn i hva digital sikkerhet er, og hvis de ikke vet det, så må det tydelig vektlegges i den hensikt at de skal kunne styre den digitale sikkerheten og tilhørende risiko (Parenty & Domet, 2020, s. 9).

Digital sikkerhetskultur er under konstant utvikling, og bør derfor være en del av virksomhetens strategi (Blum, 2020, s. 94). Hvis ikke digital sikkerhet er sett på som strategisk og ikke blir prioritert i virksomheten så vil heller ikke det forbedre kulturene, eller bedre sikkerheten (Blum, 2020, s. 94). Hvis virksomheter skal kunne øke den digitale sikkerhet så må de ha den rette katalysatoren- og det er styret og toppledelsen i virksomheten. Digital sikkerhet, kultur og tiltak starter i toppen av virksomheten hvor retning og omfang bestemmes. Der fra vil det gå nedover i virksomheten til resten av organisasjon. Fokuset på digital sikkerhet og risiko skifter fra digitale teknologier eller spesialister innen IT til virksomhetens ledere (Parnety & Domet, 2020).

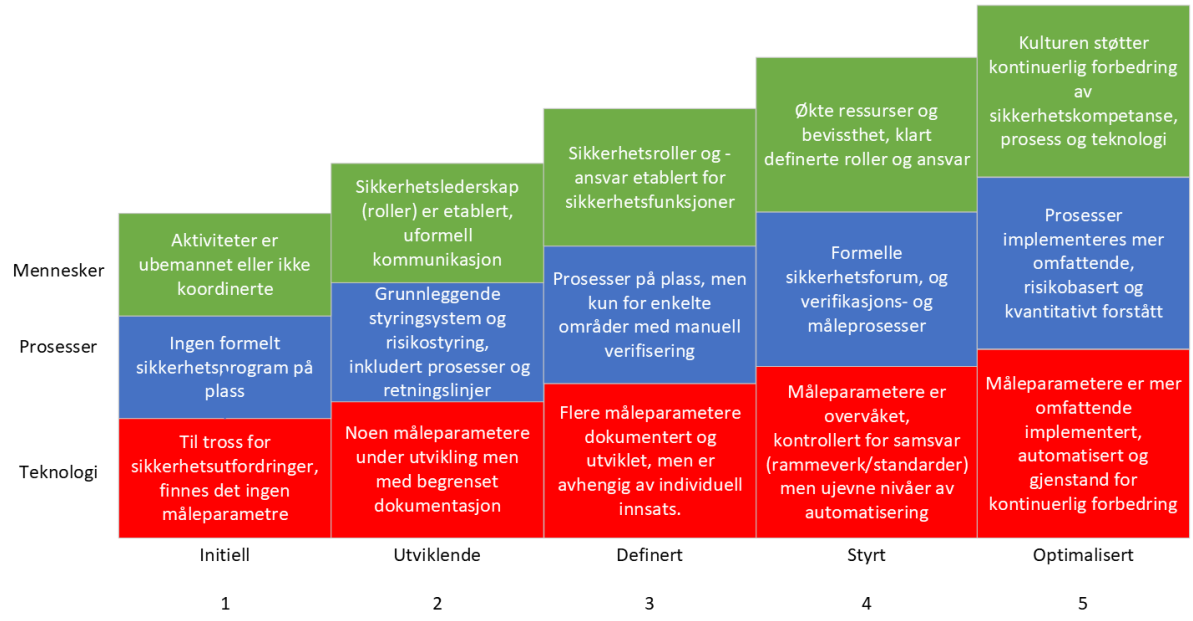
Fitzgerald (2007- refert i Lim et al, 2009) mener at en hver organisasjon eller virksomhet har forskjellige prioiteringer og nivåer av digital sikkerhetskultur, og at eksisterende organisasjon- og sikkerhetskultur kan være bestemmende for nivået av digital sikkerhetskultur. Men, hvor verdier og atferd til ansatte i forhold til sikkerhetskulturen vil være styrende for hvordan ansatt oppfatter sikkehetshendelser. Andre funn som ble gjort i studien viser til blant annet:

- Digital sikkerhetskultur ikke var implementert inn i organisasjonskulturen.
- Investeringer i sikkerhets-løsninger og kultur var minimale.
- Mangelen på ansvar og oppfølging fra ledelsen, og hvis digital sikkerhet var tilstede var det kun et fåtall som var ansvarlig for sikkerheten.
- Digital sikkerhet ble ansett som unødvendig og ble møtt med motstand.
- Mangelfull oppfattelse av risiko- digital sikkerhet gikk ut over produktivitet og effektivitet, og ikke ansett som en god investering.

Blum (2020, s. 27) fremlegger seks fokusområder for virksomheter innen digital sikkerhet, men de må tilpasses etter størrelsen og ønsket omfang i virksomheten.

- Skap en god digital sikkerhetkultur og styringsystem for digital sikkerhet.
- Håndtering av risiko opp mot virksomhetens arbeidsområder, aktivteter og verdier.
- Etabler et grunnnivå for kontroll i virksomheten
- Forenkle og rasjonalisere teknologi og sikkerhet
- Styring og kontroll av tilganger uten å skape problemer for virksomheten
- Innføre tiltak for cyber- angrep, deteksjon, repons og gjennoppretting.

Blum (2020, s. 27) har utviklet en modenhetsmodell for å kartlegge hvilket nivå virksomheter har i forhold til digital sikkerhetskultur. Den tar for seg tre faktorer som er den menneskelige, prosesser/styringssystem for sikkerhet, og teknologi. Modellen består av fem nivåer som en virksomhet kan plasseres i. Modellen er oversatt til norsk, og der av kan noen oversettelser være misvisende.



Figur 2: Den rasjonelle modenhetsmodellen for digital sikkerhetskultur (Blum. 2020a).

Nivå nummer 1 – virksomheter mangler formelle sikkerhetspolicyer og et funksjonelt styringssystem for sikkerhet. Gjennomsnittsverdien ligger mellom 1 og 2. De fleste virksomheter ligger over dette nivået, men det finnes fortsatt noen som er her (Blum, 2020a). I dagens digitale verden anses det som uakseptabelt å havne på dette nivået, gitt at de eier eller styrer digitale systemer, eller må svare til aksjonærer, investorer, regulatorer eller skattebetalere. Virksomheter som havner på dette nivået bør anskaffe dedikert sikkerhetspersonell eller funksjoner, og få på plass et team for sikkerhetsstyring og øke antallet i virksomheten som jobber med sikkerhet og styring av sikkerhet.

Nivå nummer 2 – virksomheter har et fungerende styringssystem for sikkerhet, hvor enkelte prosesser, teknologier og infrastruktur fungerer som tiltenkt, og de har flere tiltak under utvikling. De mangler sikkerhet i dybden og teknologi ligger på et og samme nivå. Det er også lite nivåer av ansvarliggjøring i virksomheten. De har heller ikke innført systemer for deteksjon, respons og gjenoppretting av data. For disse virksomhetene handler det om å fikse

eventuelle svakheter, og fortsette å bygge på den digitale sikkerhetskulturen stein for stein (Blum, 2020a).

Nivå nummer 3 – Virksomhetene har etablert et omfattende sett med virksomhetsomspennende sikkerhetsprosesser, styringssystem, policyer og dokumenterte tekniske måleparametre. De er der imot avhengige av enkeltes individuelle innsats. Prosesser innenfor endringsledelse, revisjon og leverandørsikkerhet må forbedres. Mer arbeid er også nødvendig innen rollespesifikke sikkerhetskunnskaper- og bevissthet, fremme sikkerhetsovervåkning, analyser og tilgangskontroll. For disse virksomhetene bør de fokusere på revisjoner, endringsledelse, og mer avansert sikkerhetsovervåking inkludert målinger for å øke nivået innen verifisering og ansvarliggjøring, og økt sikkerhet. I tillegg bør de ta i bruk nøkkelindikatorer (KPI) for å besvare om sikkerheten er god nok. De fleste virksomheter ligger på dette nivået, og er ansett som «the sweet spot» (Blum, 2020a).

Nivå nummer 4 – Virksomhetene har definert og bygget et omfattende sett med kontrollere og styringssystem innen digital sikkerhet for mennesker, prosesser og teknologi. Imidlertid er de fortsatt avhengige av manuelle prosesser og de står ovenfor utfordringer med å opprettholde styringssystemet for sikkerhet i møte med kontinuerlige endringer i trussel-, regulerings-, teknologi- og virksomhetslandskapet de er i. Virksomheter på dette nivået bør fokusere på mer automasjon for å gjøre ting mer kostnadseffektivt og skalerbart (Blum, 2020a).

Nivå nummer 5 – Virksomheter på det øverste nivået i modellen har organisatoriske sikkerhetsprogrammer som har nesten alt. De er «state of the art» innen sikkerhet, og har hevet nivået for organisasjonsomspennende sikkerhetsprosesser, teknologisk infrastruktur, ansvarliggjøring, målinger og berginger, og automasjon. Men, ikke alle virksomheter på dette nivået er nødvendigvis opptatt av kontinuerlig forbedringer at de vil fortsette å øke eller opprettholde investeringer og ressursbruk på digital sikkerhet. Virksomheter på dette nivået vil møte utfordringer med å bli værende. Et slikt nivå krever høye investeringer og krever kontinuerlig risiko- virksomhet-, teknologi- og finansanalyser i møte med endringer. Virksomhetene på dette nivået fokuserer på bærekraft og tilpasningsevne ved fortsatt arbeid med arkitektoniske tilnærminger til abstrakte og fremtidssikre prosess- og teknologigrensesnitt. De har også en organisasjonskultur som aksepterer endringer i sikkerhet og risikorelatert arbeid (Blum, 2020a).

Gjennom flere kartlegginger av virksomheter på internasjonalt nivå har Blum (2020) sammenlignet alle bransjer og domener og målt et gjennomsnitt til 2.75, noe han bemerker er

altfor lavt. Finansiell sektor har vært i frontlinjene i forhold til trusselnivå og reguleringer fra myndighetssektorer, og gjennomsnitt har vært rundt 3.5. Han bemerker også at virksomheter som myndigheter, helse, høyteknologi, produksjon og universiteter bør ligge opp mot 3.5. Noen av dem, inkludert finans mener han burde ligge høyere.

2.3.1 Måling av digital sikkerhetskultur

Målinger av digital sikkerhetskultur og dets omfang kan være utfordrende, og vanskelig å determinere hva en faktisk skal måle. Likevel vil det være en fordel for virksomheter å ha måleparameter på digital sikkerhetskultur, sikkerhetsteknologi og kompetanseutvikling (Blum, 2020; Nätt, 2021). Hvordan skal en vite om kurs i kompetanseutvikling på ansatte inne digital sikkerhet har fungert, hvis en ikke kan måle det? Er det noen grupper med ansatte som skiller seg ut? Og, hvordan skal en vite om investeringer i sikkerhetsteknologi har bidratt til å sikre og minske risikoen det var tiltenkt til uten å målinger utført på de ansatte.

Slike målinger og kartlegginger kan gjøres ved hjelp av for eksempel spørreundersøkelser, intervjuer, nøkkeltallsindikatorer eller testing av ansatte direkte med kjente cyberangrep som for eksempel e-postangrep som phishing (Blum, 2020, s. 117; Nätt, 2021, s. 366).

Bergen kommune testet sine ansatte i et phishingangrep hvor 16,5% oppga brukernavn og passord (Nätt, 2020). Også ansatte innen digital sikkerhet kan gå på slike hendelser, som da Intel Security testet sine tidligere ansatte og kun 3% av 19000 ansatte klarte å detektere alle phishing e-postene. Det skal også sies at ingen kompetanseutviklingsprogram eller opplæringsprogram kan fjerne denne risikoen. Det skal kun én person som klikker på feil lenke i en e-post eller vedlegg for et slik angrep skal være vellykket (Parnety & Domet, 2020).

For å skape en positiv holdning i en virksomhet til sikkerhetsarbeid og digital sikkerhetskultur skal en der imot være forsiktig med å håne, omtale eller identifisere personer som eventuelt har gått på cyberangrep. At ansatte tørr å varsle, og at varslingskulturen for sikkerhetshendelser opprettholdes er viktig (Nätt, 2021).

Blum (2020) viser til tre måleparametre for å måle digital sikkerhetskultur.

1. Effekten av kommunikasjonen rundt digital sikkerhet ut til ansatte i virksomheten.
2. Effekten av digital sikkerhetsopplæring
3. Finne nøkkelindikatorer for å måle den digitale sikkerhetskulturen over tid.

2.3.2 Styringssystemer innen digital sikkerhetskultur

Styringssystemer eller sikkerhetsstandarder handler om hvordan sikkerhetsarbeid skal organiseres og gjennomføres i en virksomhet. Sikkerhetsarbeid på et overordnet nivå med prosesser og sikkerhetsledelse er stort sett likt for alle virksomheter, selv om virksomhetene er ulike både i størrelse og oppsett (Nätt, 2021, s. 362). Sistnevnte ble også presentert som funn i masteroppgaven til Gunnes (2020) opp mot digital sikkerhetskultur. Det er laget, og prøvd å lage mange styringssystemer både av virksomheter selv, men også av større internasjonale sikkerhetsorganisasjoner. Sistnevnte med bakgrunn i at virksomheter selv skal slippe å finne opp hjulet på nytt, og der av å spare tid og ressurser (Nätt, 2021).

Fordeler ved å følge internasjonale anerkjente standarder er at flere kan vite hva én snakker om eller henvender til. Det kan også være et kvalitetsstempel utad mot bedriftskunder, leverandører, myndigheter eller partnere, da spesielt om det leder til en godkjent sertifisering. Standardene vil kunne hjelpe med å sortere og prioritere sikkerhetsarbeidet i hele virksomheten, men dette kan også være omfattende fordi de er generelle og ikke tilpasset den enkelte virksomhets organisering. Standardene kan også bli et hovedmål i seg selv, i stedet for et verktøy på vei mot bedre sikkerhet, kvalitet og kontroll (Nätt, 2021).

Svakhetene ved internasjonale standarder er blant annet at de er laget for et bredt spekter av virksomheter. Derav er suksesskriteriet for hvor relevant de er helt avhengig av hvordan de blir implementert. Digitale sikkerhetsprioriteringer til et atomkraftverk er og vil være helt annerledes enn fra ett hotell. Ergo, ingen standard, uansett hvor god den er utformet, kan gi spesifikk veiledning til alle virksomhetene i eksistens (Parnety & Domet, 2020, s. 27). Selv standarder utgitt innen samme bransje har ikke garanti for at den gir nok hjelp eller veiledning mot virksomheten som tar den i bruk. American Chemistry Council publiserte en sikkerhetsstandard, men den nevnte ingen ting om spesielle sikkerhetsutfordringer eller tiltak innen industrielle kontrollsystem som den var tiltenkt for. I tillegg kan også standarder være «utgått på dato» ved at de har eksistert i mange år uten revisjoner. Et eksempel er ISO/IEC 27001 som ble utgitt i 2005, og det tok åtte år før den var revidert, og seneste nå nylig i 2022 (Parnety & Domet, 2020).

Mange virksomheter benytter internasjonale standarder og utvikler de til sine egne. Det er også de som lager sine egne fra start. Felles for de begge er de bør være rett mot egen virksomhet, og må kunne håndtere vekst (Parnety & Domet, 2020).

I henhold til mørketallsundersøkelsen 2022 hadde 51% styringssystem eller rammeverk. En nedgang på 12% fra 2020, mot 53% i 2018, og 50% i 2016. Store virksomheter har rammeverk i større grad enn mindre virksomheter, henholdsvis 81% for store virksomheter definert som 100 ansatte eller flere. Trenden for om virksomheter har innført styringssystem eller rammeverk har stagnert og har en negativ utvikling. Undersøkelsen fant også at de med innført styringssystem opplevde flere hendelser mot virksomheten enn andre, og at sikkerhetshendelser oppdages ved internkontroller eller sikkerhetsmonitorering/måling (NSR, 2022). For de uten styringssystem kan det antyde at de ikke får med seg eller registrer sikkerhetshendelser, eller om de har vært eller blir angrepet.

2.3.3 Investeringer og kostander innen digital sikkerhet

Virksomheter og organisasjoner vil alltid være utsatt for cyberangrep eller digitale angrep uavhengig om de er intensjonelle eller ikke. En skulle kanskje tenke seg at virksomheter hadde god kontroll over digital sikkerhet og ressurser og kunnskap nok til å motstå det. I virkeligheten viser det seg at virksomheter har flere ulike sikkerhetsutfordringer, det være mangel på kunnskap og ressurser, eller mangelen på styringssystemer for sikkerhet og prosesser (Nätt, 2021, s. 346).

Virksomheter vil alltid styres av økonomi, og der av kan følgende regnestykke benyttes for å avgjøre om et preventivt tiltak eller mottiltak skal innføres eller ikke (Nätt, 2021):

«estimert tap * sannsynlighet > kostnaden til mottiltak» (Natt, 2021, s. 346).

Hvis en investering koster 300 000 kroner, og estimert tap er på 1 million kroner, og sannsynligheten er 10%, så vil tapet være 100 000 kroner. Ergo er det ikke lønnsomt, eller god bedriftsledelse å gjennomføre (Nätt, 2021, s. 346).

Kostanden av cyberangrep mot en virksomhet er vanskelig å gi spesifikke tall på, da de varierer mye alt etter omfanget av angrepet, og hva det er som blir utsatt. I tillegg hvis trusselaktørene vet hvem de angriper så gjør de ofte også bakgrunnssjekker på regnskap for å vite hva de kan kreve i eksempelvis et løsepengevirus (Guim, 2021).

Guim (2021) viser til en gjennomsnittskostnad for små og mellomstore virksomheter som blir utsatt for cyberangrep:

- Små virksomheter (1-49) har en gjennomsnittskostnad på $24 000 hver i 2020.
- Mellomstore virksomheter (40 – 249) har en gjennomsnittskostnad på $50 000 dollar hver i 2020.
- Store virksomheter (250 – 999) har en gjennomsnittskostnad på $133 000 dollar hver i 2020.
- Enterprise virksomheter (1000+) har en gjennomsnittskostnad på $504 000 dollar hver i 2020.

For å sette ting ytterligere i perspektiv og hvor vanskelig det er å estimere kostnader for cyberangrep så kostet angrepet på Hydro i 2019 dem 350 millioner norske kroner (Wilberg, 2023). IBM (2022) estimerer et gjennomsnitt på $4.35 millioner, og i mørketallsundersøkelsen 2022 (NSR, 2022) gjennomført på 2500 norske virksomheter er snittet på 43.159 kroner. Det er derfor store forskjeller i gjennomsnittet ut ifra hvilken empiri og tallgrunnlag de er basert på.

Guim (2021) viser videre til kostnader for tiltak innen digital sikkerhet for virksomheter, og at også dette vil variere basert på størrelsen på virksomheten og omsetning. Det estimeres at virksomheter bruker mellom 6% - 14% av IT-budsjettet, og gjennomsnittet ligger på rundt 10%. De har kalkulert følgende kostnader knyttet til investeringer og tiltak på digital sikkerhet:

- Små virksomheter $500 000 dollar eller mindre per år
- Mellomstore virksomheter $500 000 - $2 millioner dollar per år
- Store virksomheter $2 millioner - $5 millioner per år.

2.4 Virksomheters oppfattelse av risiko

Risiko handler om å håndtere trusler, sårbarheter, usikkerhet og tap av tjenester eller verdier i en virksomhet (Blum, 2020). For å håndtere dette må virksomheter ha innført risikostyring som en del av styringssystemet for sikkerhet (Nätt, 2021. s 353). Virksomheter vil aldri kunne håndtere alle sikkerhetshendelser, men en kan gjøre det så sikkert en kan ut fra tilgjengelige ressurser, kunnskap og styring. For å strukturere arbeidet med risiko må dette settes i et system hvor risikovurderinger- og analyser er sentrale (Nätt, 2021). Før en starter med risikovurdering- og analyser må det identifiseres hvilke risikoer som eksisterer i virksomheten og hva det er en skal beskytte eller forhindre (Parnety & Domet, 2020, s. 57). Hva er virksomhetenes mest kritiske aktiviteter i det daglige og hvilke trusler kan identifiseres mot dem. Nätt (2021) viser til følgende steg for å starte en risikoanalyse som også omtales som risiko- og sårbarhetsanalyse:

1. Planlegging og organisering.
   Hvem er ansvarlig, hvilket område gjelder analysen for, tidsplan.
2. Lage kategorier av sannsynlighet.
   Inndelingen i kategorivariabler, ofte 1-3 eller 1-5.
3. Lage kategorier av konsekvenser.
   Inndeling av kategorivariabler, ofte 1-3 eller 1-5.
4. Definere akseptabel risiko.
   Hvilket nivå er akseptert risiko- sammenheng med sannsynlighet x konsekvens = risiko.
5. Identifisere hendelser.
   Hvilke hendelser eller trusler skal være med i analysen.
6. Estimere sannsynlig og konsekvens for hver hendelse.
   Rangering av hendelsen i forhold til sannsynlig og konsekvens basert på erfaringer både internt og eksternt.
7. Beregne risiko for hver hendelse.
   Sette risikoverdier inn i tabell.
8. Lage prioriteringsliste
   Plassering av risikoene i en liste hvor hva som må håndteres først.

9. Utarbeide risikoreduserende tiltak
   Hvilke tiltak kan iverksettes, bør vente, eller kan gjennomføres for å mitigere risikoen for virksomheten.
10. Utarbeid tiltaksplan.
    Tiltaksplan viser hvilke tiltak som gir beste risikoreduserende effekt i forhold til kostnad, tidsplan, effekt for sikkerhet.
11. Gjennomføre og teste.
    Iverksetting av tiltak i henhold til tiltaksplan og kontrollere om de har effekt.
12. Evaluere, endre og dokumentere
    Risikotiltak må vurderes kontinuerlig, og om mulig måles for å kontrollere om de faktisk har redusert risikoen mot virksomheten.

Risiko- og sårbarhetsanalyser vil være til stor hjelp for virksomheter hvis de gjennomføres korrekt, og arbeidet må også forankres opp i ledelsen og eventuelt styrene for virksomheten (Blum, 2020; Nätt, s .358). Dokumentasjon og kontrollering av slike prosesser er også en viktig gevinst av arbeidet, i tillegg til at det tydelig kommuniseres ut til relevante interessenter opp mot virksomheten hva som faktisk er risikoen (Blum, 2020, s. 149; Nätt, 2021).

«Now we recognize cyber risk is really business risk, and my job as CEO is to manage business risk» Richard Lancaster, CEO of CLP, Asia. » (Parnety & Domet, 2020, s. 57).

Utfordringene ved håndtering av risiko-, styring og analyser er at metodene ofte ikke sier noe om hvordan en skal dekke mest mulig av sikkerhetshendelser opp mot virksomheten. Det er derfor viktig med en klar styring, ledelse og ikke minst erfaring med slike prosesser. Det handler om å sette sammen riktig personer med riktig kompetanse og forståelse av hva som skal risikovurderes for at resultatene skal bli gode (Nätt. 2021). Nätt (2021) viser også til at mange virksomheter og ledere har et større fokus på å vise at slike prosesser er gjennomført, enn at de faktisk er dekkende for virksomheters risikoer, eller at tiltak er innført for å mitigere risikoen.

I mørketallsundersøkelsen fra NSR (2022) er det et funn som viser at det største innside-problemet i en organisasjon eller virksomhet er en ledelse som ikke erkjenner cybertrusselen.

2.5 Forskningsspørsmål

Etter en gjennomgang av teori, enkelte funn og problemstillingen ovenfor har jeg kommet frem til følgende forskningsspørsmål med tilhørende hypoteser:

4. I hvilken grad har ledere i virksomhetene innført digital sikkerhetskultur?
    a. Har de forankret sikkerhetsarbeid i ledelsen, og har dette sammenheng med innført styringssystem for sikkerhet og digital sikkerhetskultur som en del av strategien?
5. Har prioriteringer av tiltak sammenheng med risiko for å bli utsatt for cyberangrep?
6. Har investeringer i teknologi og kompetanse sammenheng med risiko for å bli utsatt for cyberangrep?

Basert på forskningsspørsmålene har jeg kommet frem til følgende hypoteser:

- H1a: Forankring av sikkerhetsarbeid i ledelsen har sammenheng med innført digital sikkerhetskultur
- H1b: Forankring av sikkerhetsarbeid sammenheng med ledelsestiltak innen digital sikkerhetskultur
- H2a Prioriterte tiltak i sikkerhetsteknologi innen cybersikkerhet har sammenheng med risiko for å bli utsatt for cyberangrep
- H2b: Prioriterte tiltak i kompetanseøkning har sammenheng med risiko for å bli utsatt for cyberangrep
- H2c: Prioriterte tiltak i outsourcing av sikkerhetsarbeid har sammenheng med risiko for å bli utsatt for cyberangrep?
- H3a: Investeringer i kompetanse og sikkerhetsteknologi har sammenheng med risiko for å bli utsatt for cyberangrep?

3.0 Metodiske momenter

3.1 Forskningsdesign og metode

Hensikten med oppgaven er å finne ut i hvilken grad har ledere i store norske virksomheter innført sikkerhetskultur i virksomheten, og hvordan prioriteres tiltak og investeringer i sikkerhetsteknologi og kompetanse for å minske risikoen for å bli utsatt for cyberangrep.

Problemstillingen ble førende for valget av metode. Siden tiden til disposisjon for gjennomførelse er begrenset, og det er ikke noe økonomiske midler tilgjengelig for å kunne utført en longitudinell undersøkelse ble det naturlig å velge et deskriptivt kvantitativt design med tversnittundersøkelse for å besvare problemstillingen (Johannessen, Christoffersen & Tufte, 2011, s. 78).

Undersøkelsen vil derfor bare kunne gi svar i den gitte tiden spørreundersøkelsen er tatt. Det betyr at jeg mest sannsynlig ikke kan dra konklusjoner over tid eller i forkant, men heller kunne gi antydninger og trender i det gitte tidspunkt. Ved få respondenter vil det også være vanskelig å gjøre en generalisering på eventuelle funn ovenfor eksempelvis alle store norske virksomheter visa versa. Det ble videre valgt en deduktiv tilnærming, hvor hypotesene blir formet etter at empirien er på plass (Johannesen et al, 2011, s. 467).

3.2 Utforming av spørreundersøkelse, utvalg og datainnsamlingsteknikk

Datainnsamlingen ble utført ved en digital spørreundersøkelse via nettskjema. Spørsmålene ble utformet med bakgrunn i problemstillingen og en forstudie for relevant teori og tidligere undersøkelser innenfor samme tema. For innhenting av enheter og populasjon ble proff.no benyttet for å hente ut de virksomheter i Norge som ville være relevant. Fordi tiden til disposisjon ikke tillot sannsynlighetsutvalg eller tilfeldig utvalg ble det naturlig å velge bekvemmelighetsutvalg for denne undersøkelsen (Johannesen et al, 2011).

3.2.1. Utvalg

Utvalget i spørreundersøkelsen var satt til store norske virksomheter hvor antallet ansatte er over 250 (Erichsen et al, 2018). Deretter ble det også gjort en vurdering på selskapsform hvor aksjeselskap, allmennaksjeselskap, enkeltmannsforetak, og ansvarlig selskap ble valgt. Det ble også satt en begrensing på at virksomhetene måtte være registrert som aktive selskap, og de måtte ha oppgitt e-postadresse. For å få tilgang til proff.no var jeg nødt til å gi universitet for å få tilgang til å kunne hente ut og eksportere en liste med populasjon.

Følgende kriterier ble satt for utvalget:

- Virksomheter registret i hele landet.
- Antall ansatte: 250 – 5000
- Selskapsform: AS, ASA, ENK, ANS.
- Aktive bedrifter
- Kontaktinformasjon: E-postadresse.

Dette ga et bruttoutvalg på 847 virksomheter, hvor av 501 virksomheter var registret med e-post adresse.

3.2.3. Utforming av spørreundersøkelsen

Selve utformingen av spørreundersøkelsen ble utført ved å finne andre relevante spørreundersøkelser fra blant annet Pettersen 2021, Gunnes 2022, IBM 2022, NSR 2022, med flere for å se om en kunne finne spørsmål som passet opp mot min problemstilling. For de spørsmålene som var relevante så måtte de skrives om for å passe inn i denne spørreundersøkelsen. Dette gjør at de ikke kan benyttes som direkte sammenlikninger mot hverandre (Johannessen et al, 2011). Det ble også utført en kort forstudie på relevant teori som ville passe inn mot problemstillingen for utforming av spørsmål

For å sørge for at spørreundersøkelsen målte faktisk det den skulle måle var det viktig være nøyaktig i oppbyggingen av spørsmålene slik at intervallverdiene ble hensiktsmessig. Det ble derfor valgt en strukturert predefinert likert fem punkt skala med et ekstra punkt for vet ikke (ordinal variabel) for de fleste spørsmål (Johannesen et al, 2011, s. 273). To spørsmål ble formulert som dikotome/nominell variabel og hadde til hensikt å kun utelukke feile svar, eller kartlegge om styringssystem var innført eller ikke. Et spørsmål ble valgt som åpent fordi svaret på spørsmålet omhandler kostnad, og det ville derfor kunne variere stort fra respondent til respondent. I tillegg ble det også spurt noen atferds- og holdningsspørsmål for å kartlegge

virksomheters atferd rundt sikkerhetskultur og holdninger rundt ledelsenes ansvar innen digital sikkerhetskultur.

Undersøkelsen ble videre bygget opp via et tankekartprogram hvor flyten i spørreskjemaet ble tydelig, og hvor eventuelle ytterligere avklaringer og definisjoner på spørsmålene kunne tydeliggjøres for respondentene. Siden problemstillingen og hensikten med undersøkelsen var å måle virksomhetene på et gitt tidspunkt og informasjon om firma ikke var relevant ble det valgt en helt anonym spørreundersøkelse hvor ingen personopplysninger kunne spore tilbake til person eller virksomhetene.

Det ble også brukt tid på å definere hvem det var ønskelig skulle besvare spørreundersøkelsen, og siden virksomhetenes leder er i fokus så ble det naturlig å skrive om dette i innledningen til spørreundersøkelsen, og å velge ut rolle inne c-nivå-struktur for besvarelsen. Undersøkelsen ble så utformet og kodet i nettskjema, før den ble testet på kollegaer og venner

3.3 Datainnsamlingsteknikk

For å kunne hente inn dataene fra undersøkelse var det nødvendig å finne en metode som gjorde dette effektivt, kontra og sende ut én og én e-post eller som en bulk. I tillegg kom utfordringene med å prøve å unngå spam-filtre eller andre e-postfiltret som ville blokkere e-postene.

Virksomhetene ble hentet ut i en liste fra proff.no og sortert på selskapsnavn og e-post-adresse, deretter ble listen sortert fra a-å. For å unngå at e-postene ikke ble mottatt så ble det brukt Powerapp for å automatisere utsendelsene av e-postene. Informasjon, bakgrunn og lenke til nettskjema ble beskrevet gjennom utforming av en generell e-post i Flyt fra Microsoft. For å forhindre at de ble fanget opp av spamfilter ble e-postene sendt ut én og én av powerapp. Etter en uke ble det purret, og en ny purring uken etter. Spørreundersøkelsen var ute i 3.5 uke. Siden spørreundersøkelsen skulle være anonym var det ikke behov for å sende inn meldeskjema for godkjenning i forhold til behandling og bearbeiding av personopplysninger.

Av de 501 virksomhetene som det ble sendt ut e-post til kom noen i retur grunnet ikke-fungerende e-post-adresse. Det ble brukt noe tid på å finne nye e-postadresser og for å sende ut nye e-poster, men siden dette var ganske tidkrevende ble det satset på de som allerede var korrekt. Totalt sett kom det inn 38 svar som ble med videre i undersøkelsen som resulterer i en svarprosent på 7,6%. av bruttoutvalget. Dette er en liten svarprosent for en kvantitativ studie hvor en helst ønsker så mange respondenter som mulig. Men det er ikke uventet i slike spørreundersøkelser som dette hvor virksomheter mottar mange undersøkelser fra studenter i samme periode, og at en generelt over tid har sett en fallende prosent på slike undersøkelser fra 80 – 90% til 30 – 40% (Johannesen et al, 2011, s. 263).

3.4 Operasjonalisering av spørsmål

Denne delen tar for seg spørsmålene som ble brukt i spørreundersøkelsen, hva som var hensikten bak dem i forhold til hva de skulle måle og hvordan de ble operasjonalisert. Spørreundersøkelsen med svaralternativer er vist i vedlegg 1.

Dataene fra spørreundersøkelsen ble behandlet i Excel og i IBMs SPSS.

Spørsmål 1:

Er dette temaet relevant for din virksomhet?

Kontrollvariabel. Spørsmålet for å luke ut respondenter som ville kunne svare urimelig på spørreundersøkelsen, og derav relabilitet til svarene fra de respondentene, og for totalen.

Spørsmål 2:

Hvilken stilling har du?

Spørsmålet har til hensikt å tydeliggjøre for respondentene at det er toppledelsen som er ønskelig som respondenter. Kontrollvariabel.

Spørsmål 3:

Hvor mange ansatte er det i virksomheten?

Kontrollvariabel for å kunne benyttes i analyser, og for å kunne kontrollere normalfordelingen på utvalget.

Spørsmål 4:
I hvilken grad er virksomheten avhengig av IT-systemer for å opprettholde den daglige driften?

Kontrollvariabel for å luke ut virksomheter som ikke mener de er avhengige av IT-systemer for daglig drift som vil være en selvfølge innen digital sikkerhetskultur.

Spørsmål 5:
I hvilken grad har virksomheten innført digital sikkerhetskultur som en del av organisasjonskulturen?

Hensikten med denne variabelen var å kunne måle hvilket nivå respondentene og virksomhetene mener de ligger i forhold til innføring av digital sikkerhetskultur opp mot Blums modenhetsmodell som ser på faktorer tre faktorer for modenhetsnivå: mennesker, prosesser og teknologi.

Spørsmål 6:
I hvilken grad er sikkerhetsarbeid innen digital sikkerhet/cybersikkerhet forankret i ledelsen?

Spørsmålet skal måle i hvilken grad arbeid med digital sikkerhet og cybersikkerhet er forankret i ledelsen, og vil antyde at digital sikkerhetskultur er prioritert.

Spørsmål 7:

Har virksomheten innført et styringssystem/rammeverk for digital sikkerhet/cybersikkerhet?

Hensikten er måle om virksomheter har innført styringssystem for digital sikkerhet og cybersikkerhet. Denne er koblet opp teoriene om at virksomheter må ha et fungerende styringssystemer for å ha kontroll på sikkerheten.

Spørsmål 8:
I hvilken grad vil du karakterisere risikoen for at virksomheten kan bli utsatt for cyberangrep?

Målparameter for å kontrollere i hvordan respondentene og virksomhetene anser risiko for at de kan bli utsatt for cyberangrep. Den vil si noe om de anerkjenner risiko eller ikke.

Spørsmål 9:
I hvilken grad er du enig i følgende påstand: Sikkerhetskultur i virksomheten er et ledelsesansvar?

Spørsmålet skal måle om respondentene er enig i påstanden at sikkerhetskultur er et ledelsesansvar. Vil kunne determinere om virksomhetene har tatt sikkerhetskultur på alvor. Basert på teori fra Schein 210, Bang 2020, Blum 2020, Bergsjø og Windvik 2018 om at lederne er ansvarlig for sikkerhetskulturen.

Spørsmål 10:
I hvilken grad er du enig i følgende påstand: Virksomheten trenger mer kompetanse innen digital sikkerhet/cybersikkerhet

Spørsmålet skal måle om respondentene er enige i påstanden om at virksomheter trenger mer kompetanse innen digital sikkerhet og cybersikkerhet. Spørsmålet her hentet og omskrevet fra Pettersen, 2021.

Spørsmål 11:
Hvordan prioriterer virksomheten tiltak innen digital sikkerhet/cybersikkerhet for å redusere risikoen for cyberangrep?

Hensikten med spørsmålet er å finne ut hvilke tiltak virksomheter og respondentene benytter for å minske risikoen for å bli utsatt for cyberangrep. Tiltakene må være tilpasset og generalisert for alle respondentene og vil si noe om hvordan og hvilke av tiltakene de prioriterer ut fra rangering. Tiltakene her hentet teorier og undersøkelser fra Blum, 2020 og Risiko 2022 med flere.

Spørsmål 12:

Hva var omsetningen til virksomheten i 2022 i kroner?

En kontrollvariabel som har til hensikt å kartlegge omsetningen til virksomhetene for å senere kunne estimere andelen i minimal og maksimalverdi som respondentene benytter årlig på tiltak og er bunnet opp mot teori fra Guim 2021, IBM-rapport 2022, og NSR-rapport 2022.

Spørsmål 13:
Hvor stor andel av virksomhetens omsetning vil du anslå brukes årlig på digital sikkerhet-/cybersikkerhetstiltak, angitt i prosent? (0 – 35%)?

Har til hensikt å måle cirka årlig andel av omsetningen til virksomhetene som brukes årlig på digital sikkerhet/cybersikkerhetstiltak og det vil være interessant og se gjennomsnitt som brukes på digital sikkerhet. Bakgrunnen for spørsmålet er knyttet opp mot Guim 2021 hvor det estimeres 6% - 14% årlig på digitale sikkerhetstiltak.

Spørsmål 14:
Hvor stor andel av virksomhetens omsetning vil du anslå virksomheten bruker årlig på kompetanseøkning av ansatte innen digital sikkerhet-/cybersikkerhetstiltak? (1 – 12%)

Hensikten med spørsmålet er å måle og estimere et hvor mye virksomheter benytter på kompetanseutvikling på ansatte i virksomhetene, og vil si noe om de fokuserer på ansatte kompetanse og utvikling kontra digital teknologi (Blum, 2020).

Spørsmål 15:
Har virksomheten vært utsatt for cyberangrep? (Ja/Nei/VI))
Kontrollvariabel som har til hensikt måle hvor mange av utvalget som har vært utsatt for cyberangrep, og er et ledende spørsmål til 15a.

Spørsmål 15a:
Hva vil du anslå dette kostet virksomheten økonomisk? Skriv inn anslått beløp i norske kroner.

Oppfølgingsspørsmål til oppgave 15 hvis respondentene har vært utsatt for cyberangrep og har til hensikt å måle kostnadene cyberangrepet kostet virksomhetene, og er hentet fra IBM 2022, NSR 2022 og Guim 2021.

Spørsmål 15b:
I hvilken grad var sikkerhetskultur og investeringer i sikkerhetsteknologi implementert før hendelsene?

Spørsmålet har til hensikt å si noe om tiltak og sikkerhetskultur var innført før hendelsen inntraff, og er basert på Pettersen 2021 funn.

Spørsmål 16:

I hvilken grad er digital sikkerhetskultur en del av virksomhetens strategi?

Har til hensikt å måle om digital sikkerhetskultur er en del av strategien til virksomhetene og er bunnet opp i Blum 2020 teori om at digitale sikkerhetskulturen må være forankret i ledelsen og styret. Spørsmålet vil også si noe om hvor mange i utvalget som har dette forankret.

Spørsmål 17:

I hvilken grad styres investeringer i sikkerhetsteknologi fra ledelsen?

Spørsmålet har til hensikt å måle om investeringer i sikkerhetsteknologi er forankret i ledelsen og vil kunne si noe om styringssystemer for sikkerhet til virksomhetene i utvalget.

Spørsmål 18:

I hvilken grad styres investeringer i kompetanseutvikling fra ledelsen?

Spørsmålet har samme hensikt som spørsmål 17, men da mot kompetanseutvikling i hele virksomheten.

Spørsmål 19:

I hvilken grad har virksomheten delegert ansvaret til egne roller/avdelinger for ivaretakelse av digital- sikkerhetsteknologi og sikkerhetskultur?

Spørsmålet har til hensikt å måle om ledelsen har delegert ansvar og roller innen digital sikkerhetsledelse ned i strukturen og er koblet opp mot styringssystem for digital sikkerhet, og er basert på Blum 2021 og Fitzgerald 2007 et al.

Spørsmål 20:

I hvilken grad måler virksomheten effekten av digital sikkerhetskulturen i virksomheten?

Hensikten med spørsmålet er å finne ut om virksomheter i utvalget har innført måleparameteret for å finne ut om innførte tiltak og investering har en effekt over tid, og for å eventuelt kunne gjøre justeringer. Knyttet opp mot teori fra Blum 2021, Nätt 2021, og Partney et al 2020.

Spørsmål 21:
I hvilken grad måler virksomheten effekten av digitale sikkerhetsteknologi?

En oppfølging av spørsmål 22, hvor spørsmålet har til hensikt å finne ut om virksomheter i utvalget har innført måleparametere for å finne ut om innførte tiltak og investering har i digital sikkerhetsteknologi har hatt en effekt over tid, og for å eventuelt kunne gjøre justeringer. Knyttet opp mot teori fra Blum 2021, Nätt 2021, og Partney et al 2020.

Spørsmål 22:
Hvilke av følgende metoder benyttes for å øke ansatte kompetanse innen digital sikkerhet/cybersikkerhet?

Spørsmålet har til hensikt å måle hvilke metoder virksomheter i utvalget benytter for å øke kompetanse innen digital sikkerhet og cybersikkerhet.

Eksterne kurs, Interne kurs, Informasjonsmailer, Informasjon over intranett, Møter, Muntlig kommunikasjon, Annet, Vet ikke

Spørsmål 23:
Hvordan måler ledelsen sikkerhetsnivået i virksomheten innen digital sikkerhet/cybersikkerhet i virksomheten?

Statusrapporter, Informasjonsmailer, Møter, Muntlig kommunikasjon, Simuleringer på ansatte, Årlige eller halvårlige sikkerhetsrapporter, Annet, Vet ikke

Spørsmål 24:

I hvilken grad anser virksomheten at investeringer i sikkerhetsteknologi bidrar til å minske risikoen for cyberangrep?

Har til hensikt å måle hvordan virksomhetene selv vurderer at investeringer i sikkerhetsteknologi fører til minket risiko for å bli utsatt for cyberangrep.

Spørsmål 25:

I hvilken grad anser virksomheten at investeringer i økt kompetanse hos personell innen digital sikkerhet bidrar til å minske risikoen for cyberangrep?

Samme som spørsmål 24, men da rettet mot økt kompetanse hos personell innen digital sikkerhet.

3.6 Databehandling:

Spørreundersøkelsen ble gjennomført via nettskjema.no og det var nettskjema som tok imot alle responsene. I forkant av utsendelsen hadde jeg prekodet spørreskjemaet slik at alle punktene hadde en definert verdi fra 1 – 5 eller tilsvarende. Da undersøkelsen ble avsluttet ble dataene eksportert rett inn i SPSS og Excel for videre analyser, og fordi nettskjema gir mulighet til å eksportere rett til SPSS ble dette gjort samt et .csv-format for Excel. Kodingen gjennomført på forhånd gjorde at jeg i SPSS kunne få beskrivelsene for verdiene inn i SPSS.

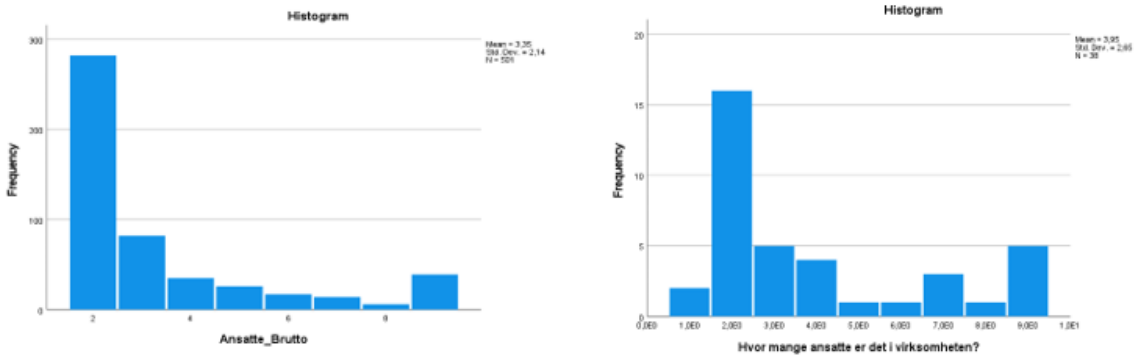
SPSS ble i hovedsak brukt til å gjennomføre frafallsanalyser, reliabilitetstester, normalfordeling og korrelasjon- og regresjonsanalyser. Resten ble utført ved bruk av pivot-tabeller i Excel.

3.7 Validitet

Validitet handler om at måleparameterene måler det de skal måle, og ikke. En skiller på indre, ytre- og begrepsvaliditet. For indre validitet sjekkes dette senere ved hjelp av frafallsanalyse. For den ytre validiteten har noen av spørsmålene vært hentet fra andre spørreundersøkelser, men de har vært endret på og kan derfor ikke benyttes som ytre validitet. Begrepsvaliditeten var prøvd å opprettholdes ved hjelp av flytskjemaet for konstruksjon av spørreskjemaet, gode beskrivelser for spørsmål hvor det kunne være tvetydelig hva de mente, og også å få testet ut undersøkelsen før den ble sendt ut til det faktiske utvalget.

3.8 Frafallsanalyse

Det ble utført frafallsanalyse for å vurdere fordeling av utvalget, både brutto og netto. Respondentene ble fordelt på en likert skala fra 1 – 9. Figur 3 viser normalfordelingen på bruttoutvalget, og figur 4 viser nettoutvalget. Gjennomsnitt for brutto var på 3,35, og netto på 3.95. Gjennom en Shapiro-Wilks-test har begge $p < 0,05$, nærmere bestemt $p < 0,001$ på begge, som betyr at dataene er ikke normalfordelt. Testen tar høyde for at H0 er normalfordelt, og at $p > 0,05$ (Bergsaker, A.S, 2022). Histogrammene viser også dette, med et noe overrepresentert utvalg av virksomheter med færre ansatte, 250-500. Dette støttes også av en ekstrem positiv skjevhet med verdier 1,650 for brutto, og en positiv 0,970 for nettoutvalget.



Figur 3:Normalfordeling bruttoutvalg

Tabell 1: Statistikk og test av normalfordeling bruttoutvalg

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Ansatte_Brutto	501	99,8%	1	0,2%	502	100,0%

Descriptives

			Statistic	Std. Error
Ansatte_Brutto	Mean		3,35	,096
	95% Confidence Interval for Mean	Lower Bound	3,16	
		Upper Bound	3,54	
	5% Trimmed Mean		3,11	
	Median		2,00	
	Variance		4,580	
	Std. Deviation		2,140	
	Minimum		2	
	Maximum		9	
	Range		7	
	Interquartile Range		2	
	Skewness		1,650	,109
	Kurtosis		1,513	,218

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Ansatte_Brutto	,299	501	<,001	,670	501	<,001

a. Lilliefors Significance Correction

Tabell 2: Statistikk og normalfordelingstest nettoutvalg

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Hvor mange ansatte er det i virksomheten?	38	7,6%	464	92,4%	502	100,0%

Descriptives

			Statistic	Std. Error
Hvor mange ansatte er det i virksomheten?	Mean		3,95	,430
	95% Confidence Interval for Mean	Lower Bound	3,08	
		Upper Bound	4,82	
	5% Trimmed Mean		3,83	
	Median		3,00	
	Variance		7,024	
	Std. Deviation		2,650	
	Minimum		1	
	Maximum		9	
	Range		8	
	Interquartile Range		4	
	Skewness		,970	,383
	Kurtosis		-,558	,750

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Hvor mange ansatte er det i virksomheten?	,245	38	<,001	,791	38	<,001

a. Lilliefors Significance Correction

3.7 Måleinstrumenter

Variablene i spørreundersøkelsen er hovedelementene for måleinstrumentene i denne undersøkelsen. Det er likevel satt sammen noen sammensatte mål i den hensikt å styrke validitet og relabilitet for sammensatte egenskaper som er ønskelig å måle med flere variabler- heretter kalt indikatorer (Johannessen et al, 2011).

3.7.1 Ledelsetiltak innen digital sikkerhetskultur

Dette målet er sammensatt av indikatorene:

- Spørsmål 7 – har virksomheten innført et styringssystem/Rammeverk for digital sikkerhet/cybersikkert
- Spørsmål 16 – I hvilken grad er digital sikkerhetskultur en del av virksomhetens strategi
- Spørsmål 17 – I hvilken grad styre investeringer i sikkerhetsteknologi fra ledelsen
- Spørsmål 18 – I hvilken grad styres investeringer i kompetanseutvikling fra ledelsen.

  En ulempe er at spørsmål 7 er en nominell/dikotom variabel, mens de andre er ordinale, noe som kan gi utslag i analysene.

3.7.2 Prioriterte tiltak i kompetanseøkning

Dette målet er sammensatt av indikatorer fra spørsmål 11 – Hvordan prioriterer virksomheten tiltak innen digital sikkerhet/cybersikkerhet:

- Økt kompetanse hos de ansatte
- Økt kompetanse i ledelsen eller ledere
- Økt kompetanse hos nøkkelpersonell innen informasjon- og cybersikkerhet
- Økt antall ansatte med spesialkompetanse i digital sikkerhet/cybersikkerhet

3.7.3 Prioriterte tiltak i outsourcing av sikkerhetsarbeid

Dette målet er også sammensatt av indikatorer fra spørsmål 11 - Hvordan prioriterer virksomheten tiltak innen digital sikkerhet/cybersikkerhet:

- Outsourcing av sikkerhetsarbeid til konsulenter
- Outsourcing av sikkerhetsarbeid til virksomheter med spesialkompetanse på informasjon- og cybersikkerhet

3.7.4 Effekten av måling av digital sikkerhetskultur og sikkerhetsteknologi

Dette målet er sammensatt av spørsmål 20 – I hvilken grad måler virksomheten effekten av digital sikkerhetskultur i virksomheten og spørsmål 21 – i hvilken grad måler virksomheten effekten av digital sikkerhetsteknologi. Måling av effekt er et tiltak, og det er derfor ønskelig å ta de med i senere analyser.

3.7.5 Investeringer i kompetanse og sikkerhetsteknologi

Dette målet er sammen av:

- Spørsmål 24 – I hvilken grad anser virksomheten at investeringer i sikkerhetsteknologi bidrar til å minske risikoen for cyberangrep
- Spørsmål 25 - I hvilken grad anser virksomheten at investeringer i økt kompetanse hos personell innen digital sikkerhet bidrar til å minske risikoen for cyberangrep?

3.8 Reliabilitet og validitet for sammensatte mål

Formålet med å gjennomføre relabilitet- og validitetstest for de sammensatte målene er for å

kontrollere intern pålitelighet og diskriminant validitet, i den hensikt å kunne slå sammen variablene, også kalt indikatorer til et sammensatt mål, og får kunne benytte de i senere analyser (Johannessen et al, 2011, s. 274). Cronbachs alfa skal ha en verdi over 0,7 for at det skal være god intern validitet og relabilitet (UCLA, u.å).

3.8.1 Ledelsetiltak innen digital sikkerhetskultur

Det ble gjennomført en relabilitetstest med Cronbachs alfa for indikatorene som inngår i Ledelsetiltak innen digital sikkerhetskultur.

Case Processing Summary

		N	%
Cases	Valid	38	100,0
	Excluded[a]	0	,0
	Total	38	100,0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
,678	,678	4

Figur 4: Relabilitetstest Ledelsestiltak innen digital sikkerhetskultur

Cronbachs alfa havnet på 0,678, og ved å fjerne indikatoren styringssystemer som også nevnte i beskrivelsen av det sammensatte målet så ville verdien steget til 0,738. Jeg har likevel valgt å ta med denne videre på 0,678 da styringssystem for sikkerhet er en viktig faktor opp mot forskningsspørsmålene.

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
Har virksomheten innført et styringssystem/rammeverk for digital sikkerhet/cybersikkerhet?	13,03	5,378	,252	,091	,738

Figur 5: Økning av Cronbachs verdi for Ledesestiltak inn digital sikkerhetskultur

Det ble også gjennomført normalitetsfordeling for å se om indikatorene var normalfordelt eller ikke. For alle indikatorene ble H0 for normalitetstest bekreftet som antyder en skjevhet i alle indikatorene- noen mindre enn andre. Q-Q plottene viser tydelig dette sammen med histogrammet

Tabell 3:Normalitetsfordeling for indikatorer for Ledelsestiltak innen digital sikkerhetskultur

Indikatorer:	Shapiro	Skewness
I hvilken grad har virksomhetene innført digital sikkerhetskultur som en del av organisasjonskulturen	P < 0,001	,179
I hvilken grad er sikkerhetsarbeid innen digital sikkerhet/cybersikkerhet forankret i ledelsen	P < 0,001	-,398
Har virksomheten innført et styringssystem/rammeverk for digital sikkerhet/cybersikkerhet	P < 0,001	-1,238
I hvilken grad er digital sikkerhetskultur en del av virksomhetens strategi	P < 0,003	-,147

3.8.2 Prioriterte tiltak i kompetanseøkning og outsourcing av sikkerhetsarbeid

Det ble gjennomført en relabilitetstest ved hjelp av Cronbachs alfa på spørsmål 11 «Hvordan prioriterer virksomheten tiltak innen digital sikkerhet/cybersikker for å redusere risikoen for cyberangrep» og siden indikatorene i variabelen gjelder for to sammensatte mål er de kjørt i samme test.

Case Processing Summary

		N	%
Cases	Valid	38	7,6
	Excluded[a]	464	92,4
	Total	502	100,0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
,699	7

Figur 6: Relabilitetstest Prioriterte tiltak i kompetanseøkning og outsourcing av sikkerhetsarbeid

Ved første analyse med alle indikatorene på variabelen ble verdien 0,699, tilnærmet 0,7, som antyder høy validitet og relabilitet.

Ã˜kt antall ansatte med spesialkompetanse i digital sikkerhet/cybersikkerhet	29,39	27,759	,132	,753

Figur 7:Økning av Cronbachs verdi for Prioriterte tiltak i kompetanseøkning og outsourcing av sikkerhetsarbeid

Hvis jeg fjernet indikatoren «økt antall ansatte med spesialkompetanse i digital sikkerhet/cybersikkerhet» steg verdien betraktelig, det gjorde også verdien på variablene seg imellom fra 0,412 til 0,600. Indikatoren ble derfor fjernet fra måleinstrumentet, og Cronbachs alfa ble på 0,753.

Det ble også gjennomført normalitetsfordeling for indikatorene på dette sammensatte målet. Også her blir H0 bekreftet og viser skjevhet i fordelingene- noe som også bekreftes av Q-Q plottene og histogrammet.

Tabell 4:Normalitetsfordeling for indikatorer for Prioriterte tiltak i kompetanseøkning og outsourcing av sikkerhetsarbeid

Indikatorer:	Shapiro	Skewness
Økt kompetanse hos de ansatte	P < 0,006	-,594
Økt kompetanse i ledelsen eller ledere	P < 0,001	-,057
Økt kompetanse hos nøkkelpersonell innen informasjons- og cybersikkerhet	P < 0,002	-0,820

3.8.3 Effekten av måling av digital sikkerhetskultur og sikkerhetsteknologi

Det ble gjennomført relabilitetstest med Cronbachs alfa for indikatorene i om virksomhetene måler effekten av digital sikkerhetskultur og digital sikkerhetsteknologi. Resultatet for Cronbachs alfa ble på 0,567- og er lavt i forhold til ønsket verdi over 0,7. Men på grunn av analyser velger jeg likevel og ta den med videre. Her mangler det også frafall på to respondenter.

Case Processing Summary

		N	%
Cases	Valid	36	94,7
	Excluded[a]	2	5,3
	Total	38	100,0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
,567	,568	2

3.8.4 Investeringer i kompetanse og sikkerhetsteknologi

Det ble gjennomført en relabilitetstest med Cronbachs alfa for indikatorene som inngår i investeringer i kompetanse og sikkerhetsteknologi. Fordi antallet indikatorer kun er to var det ikke forventet at denne skulle bli høy. Cronbachs alfa havnet på 0,595 som i seg selv er for lavt i forhold til 0,7, men velger likevel å ta den med grunnet de videre analysene.

Case Processing Summary

		N	%
Cases	Valid	38	100,0
	Excluded[a]	0	,0
	Total	38	100,0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
,595	,596	2

Figur 8:Relabilitetstest for investeringer i kompetanse og sikkerhetsteknologi

Normalfordelingen på disse indikatorene er de eneste som stiger over p > 0,05 og er nærmere normalfordelt enn hos de andre sammensatte målene. Dette bekreftes ytterligere av Q-Q plottene og histogrammet.

Tabell 5: Normalfordeling for indikatorer for investeringer i kompetanse og sikkerhetsteknologi

Indikatorer:	Shapiro	Skewness
Outsourcing av sikkerhetsarbeid til konsulenter	P < 0,067	-,016
Outsourcing av sikkerhetsarbeid til virksomheter med spesialkompetanse på informasjon- og cybersikkerhet	P < 0,086	-,270

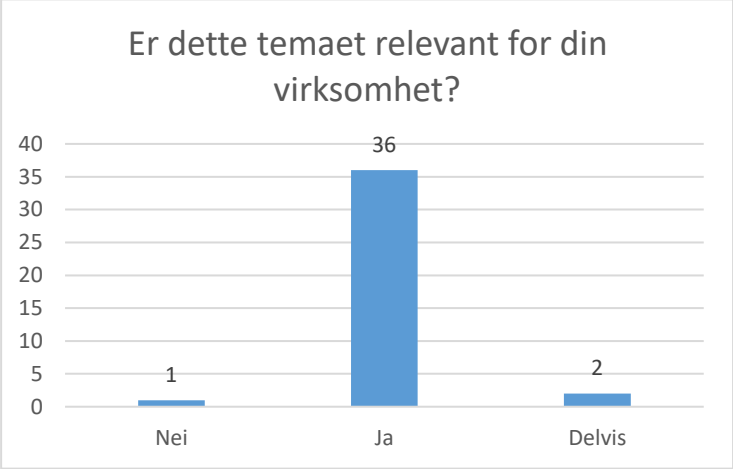
4. Analyse

4.1 Beskrivende statistikk

Spørsmål 1:

Er dette temaet relevant for din virksomhet?

Én respondent svarte nei, 36 respondenter svart ja, og 2 svarte delvis om temaet «Digital sikkerhetskultur i norske virksomheter» er relevant.

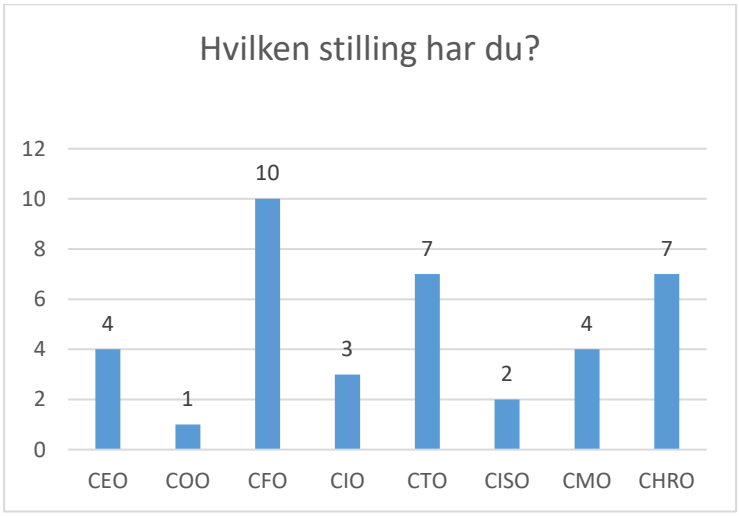


Figur 9: Histogram for spørsmål 1

Spørsmål 2:

Hvilken stilling har du?

Histogrammet viser en god fordeling av respondentene i forhold til stilling og roller på c-nivå i ledelsen, hvor henholdsvis Chief Financial Officer, Chief Technology Officer og Chief Human Resources er de største.

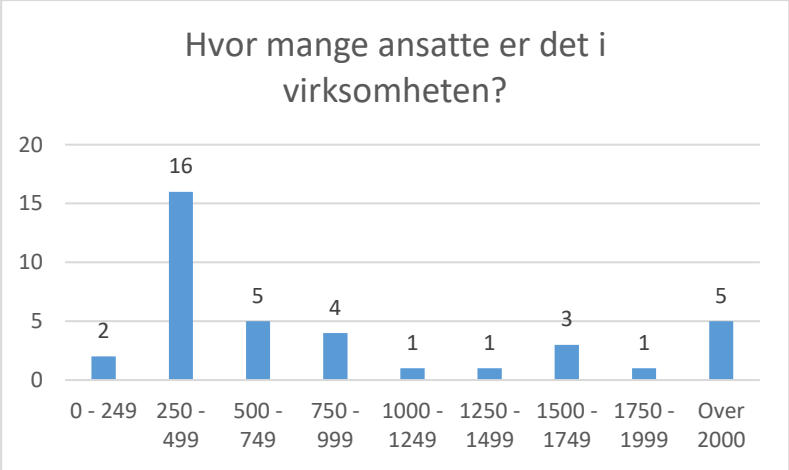


Figur 10: Histogram for spørsmål 2

Spørsmål 3:

Hvor mange ansatte er det i virksomheten?

Histogrammer viser fordelingen av respondentene og virksomhetenes antall ansatte. Fordelingen er fordelt på alle variablene, men hvor 250 – 499 utgjør hele 16 stykk og utgjør 42,1% av utvalget.



Figur 11: Histogram for spørsmål 3

Spørsmål 4:

I hvilken grad er virksomheten avhengig av IT-systemer for å opprettholde den daglige driften?

Alle respondentene viser til at de er avhengige av IT-systemer i stor grad til i svært stor grad.

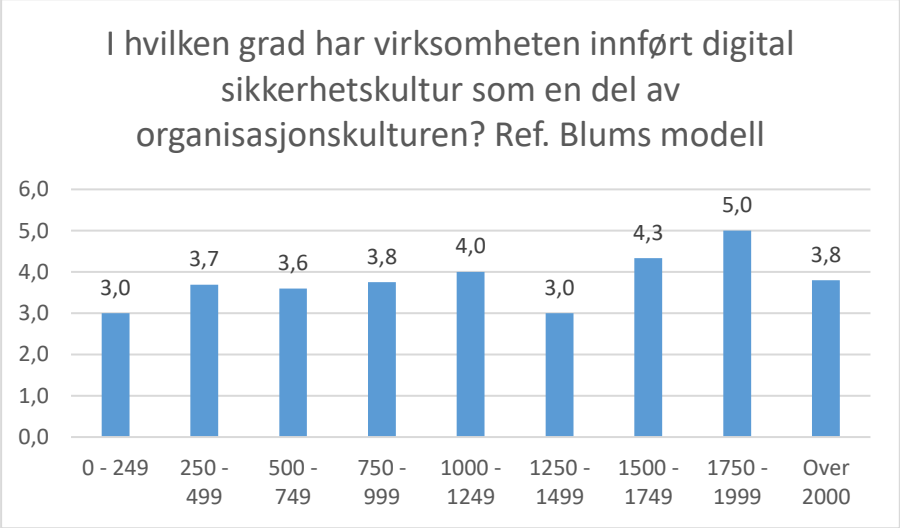
Tabell 6: Spørsmål 4 - avhengighet av IT-systemer

Svar	% av svar
Vet ikke	0 %
I liten grad	0 %
I noen grad	0 %
I stor grad	13,16 %
I svært stor grad	86,84 %
	100,00 %

Spørsmål 5:

I hvilken grad har virksomheten innført digital sikkerhetskultur som en del av organisasjonskulturen??

Histogrammet og tabellen viser respondentens svar i forhold til om de har innført digital sikkerhetskultur i virksomheten. Gjennomsnitte for alle ligger på 3,7.



Figur 12: Histogram spørsmål 5 - innført digital sikkerhetskultur

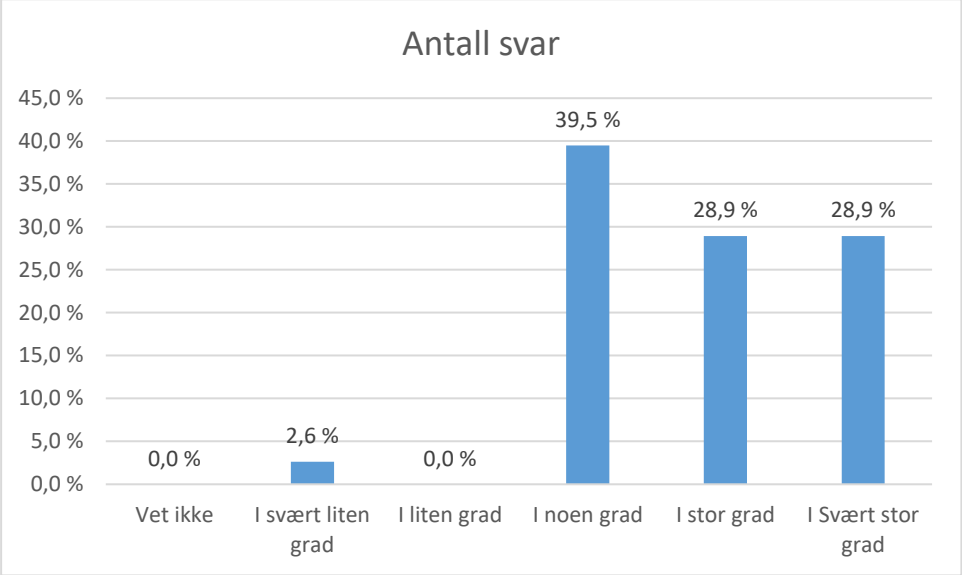
Tabell 7: Spørsmål 5 - innført digital sikkerhetskultur

Antall ansatte:	Innført sikkerhetkultur iht. Blums modell	Antall respondenter
0 - 249	3,0	3
250 - 499	3,7	16
500 - 749	3,6	5
750 - 999	3,8	4
1000 - 1249	4,0	1
1250 - 1499	3,0	1
1500 - 1749	4,3	3
1750 - 1999	5,0	1
Over 2000	3,8	5
Totalsum	3,74	39

Spørsmål 6:

I hvilken grad er sikkerhetsarbeid innen digital sikkerhet/cybersikkerhet forankret i ledelsen?

Spørsmålet viser i hvilken grad sikkerhetsarbeid er forankret i ledelsen hos virksomhetene, hvor 39,5% ligger på i noen grad og 28,9% på i stor grad og i svært stor grad. Gjennomsnittet ligger på 4,81 og tilnærmet i stor grad.

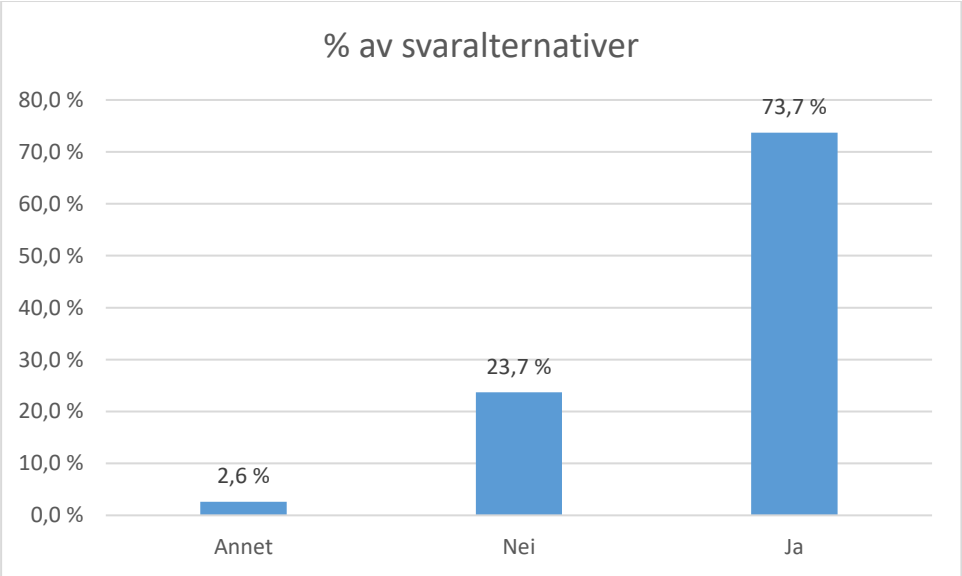


Figur 13: Histogram spørsmål 6 - forankring av sikkerhetsarbeid i ledelsen

Spørsmål 7:

Har virksomheten innført et styringssystem/rammeverk for digital sikkerhet/cybersikkerhet?

Histogrammet viser at 73,68% av 38 respondenter/virksomheter har innført et styringssystem for digital sikkerhet/cybersikkerhet, og hvor 23,7% ikke har innfør det. 2,6% svarer annet.



Figur 14: Histogram spørsmål 7 - styringssystem/rammeverk

Spørsmål 8:

I hvilken grad vil du karakterisere risikoen for at virksomheten kan bli utsatt for cyberangrep?

Vurdering av virksomhetens risiko for å bli utsatt for cyberangrep, gjennomsnittet for alle respondentene ligger på 4,38, så rett i overkant av i stor grad.

Tabell 8:Spørsmål 8 - risiko for å bli utsatt for cyberangrep

Antall ansatt	Risko for at virksomhet kan bli utsatt for cyberangrep
0 - 249	3,00
250 - 499	4,19
500 - 749	4,40
750 - 999	5,25
1000 - 1249	4,00
1250 - 1499	4,00
1500 - 1749	5,00
1750 - 1999	6,00
Over 2000	4,60
Totalsum	**4,38**
Total Antall	38,00

Spørsmål 9:

I hvilken grad er du enig i følgende påstand: Sikkerhetskultur i virksomheten er et ledelsesansvar.

Tabellen nedenfor viser at hele 89,5% er svært enige i at sikkerhetskultur i virksomheten er et ledelsesansvar, og 10,5% er delvis enig.

Tabell 9: Spørsmål 9 - Påstand: Sikkerhetskultur er et ledelsesansvar

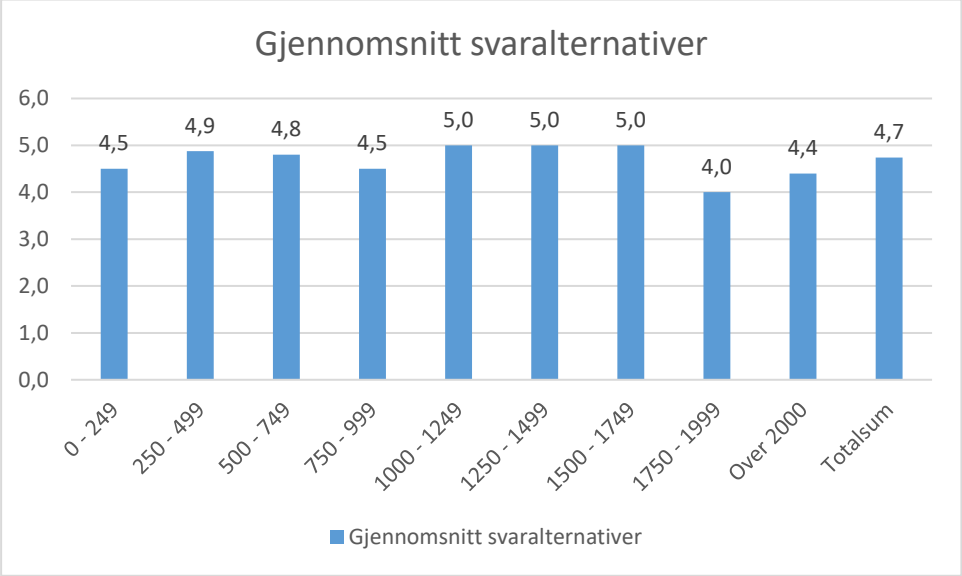
Svar	% av svaralternativer
Vet ikke	0,0 %
Ikke Enig	0,0 %
Delvis enig	10,5 %
Svært enig	89,5 %
Totalsum	**100,0 %**
Antall	38

Spørsmål 10:

I hvilken grad er du enig i følgende påstand: Virksomheten trenger mer kompetanse innen digital sikkerhet/cybersikkerhet?

Histogrammet viser en oversikt over gjennomsnittet fordelt over virksomhetens størrelse basert på antallet ansatte. Variansen ligger fra 4 – i noen grad til i stor grad, og hvor gjennomsnittet er 4,7 tilnærmet i stor grad.

Tabell 10: Spørsmål 10 - Virksomhetene trenger mer kompetanse innen digital sikkerhet/cybersikkerhet

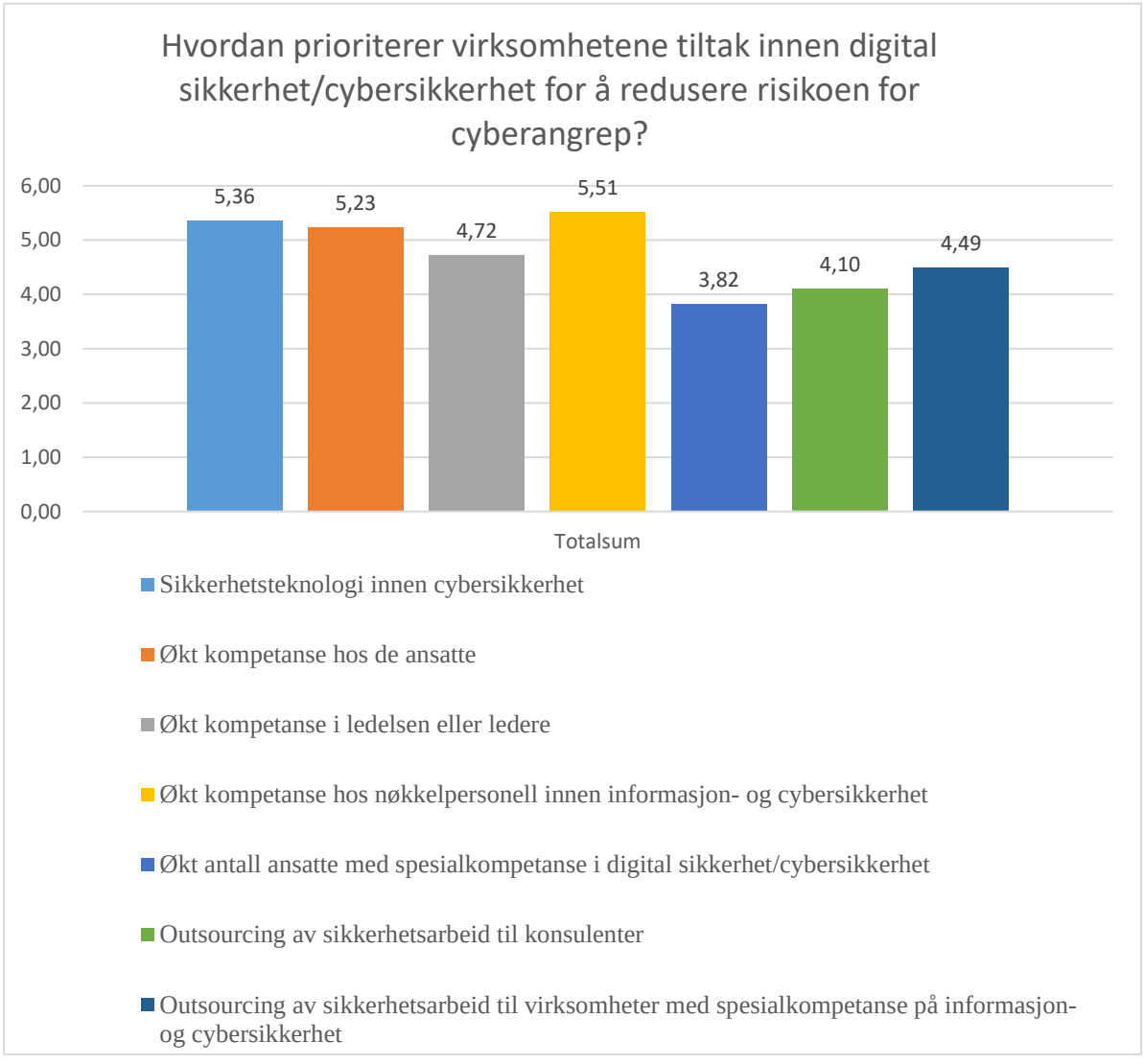


Spørsmål 11:

Hvordan prioriterer virksomheten tiltak innen digital sikkerhet/cybersikkerhet for å redusere risikoen for cyberangrep?

Virksomhetene fikk valgene å rangere punktene nedenfor på en skala fra 1 – 7 over hva de mente var deres prioriteringer på tiltak for å redusere risikoen for cyberangrep.

Økt kompetanse hos nøkkelpersonell, sikkerhetsteknologi innen cybersikkerhet og økt kompetanse hos ansatte og var de tre øverste etterfulgt av økt kompetanse i ledelsen eller lederne.

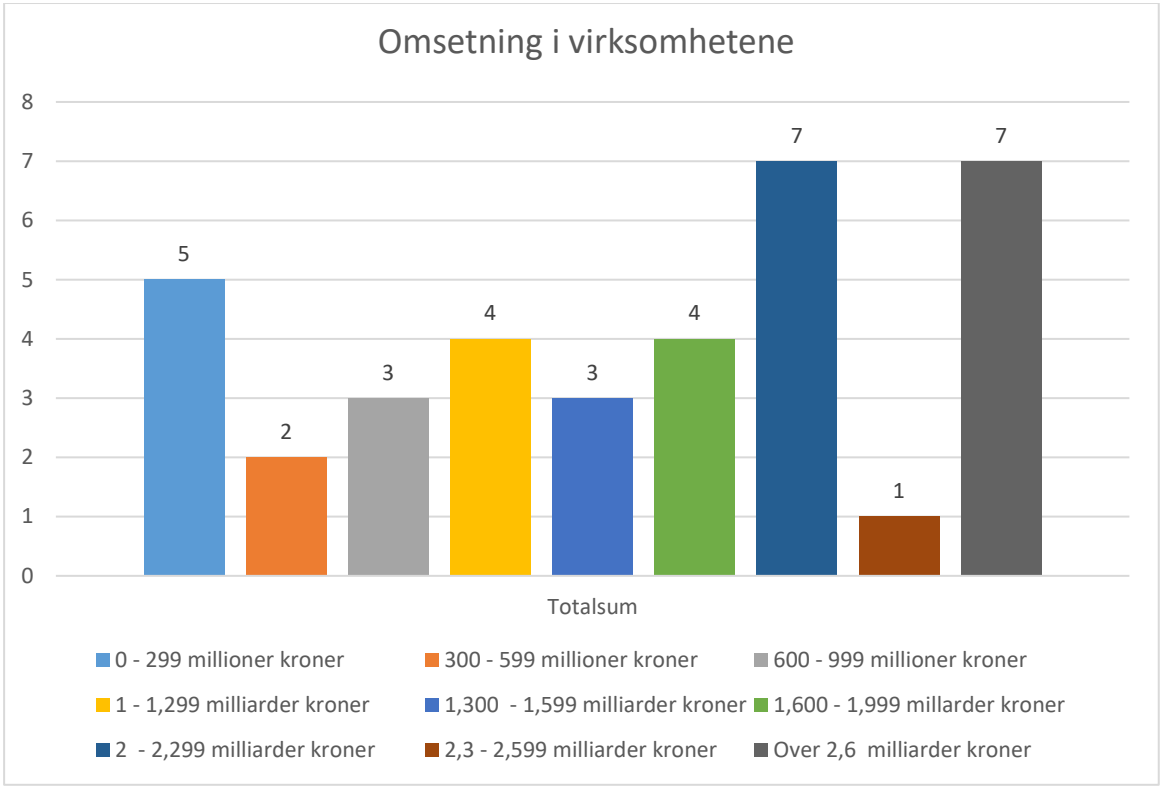


Figur 15: Spørsmål 11 - Prioritering av tiltak innen digital sikkerhet/cybersikkerhet

Spørsmål 12:

Hva var omsetningen til virksomheten i 2022 i kroner?

Histogrammet viser omsetningen til virksomhetene fordelt på antallet ansatte, og prosentsats for antallet. En normalfordeling i tabellen.



Figur 16: Spørsmål 12 - Omsetning til virksomheter i 2022 i kroner

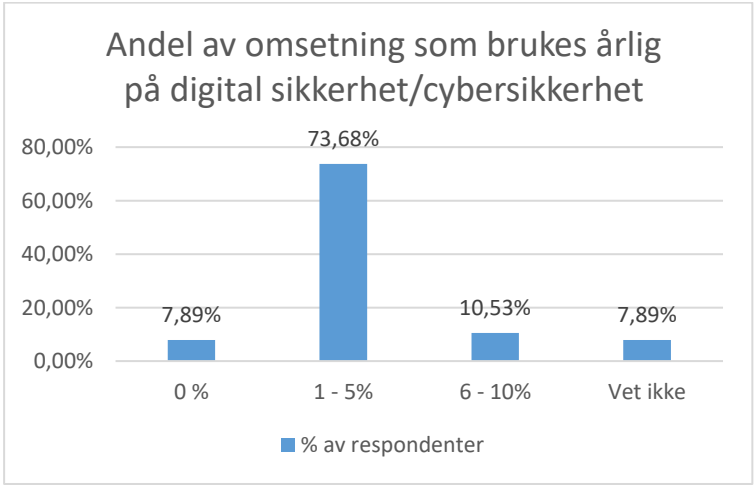
Spørsmål 13:

Hvor stor andel av virksomhetens omsetning vil du anslå brukes årlig på digital sikkerhet-/cybersikkerhetstiltak, angitt i prosent?

En oversikt anslått prosentsats virksomhetene bruker årlig på sikkerhet- cybersikkerhetstiltak angitt i prosent. Den likerte skalaen burde være ned justert og hatt flere alternativer fra 0 – 10 prosent. 73,68% bruker 1 – 5% årlig av virksomhetens omsetning, 10,53% bruker 6 – 10%, og 7,89% vet ikke eller bruker 0%.

Tabell 11: Spørsmål 13 - Andel av omsetning brukt årlig på digitale sikkerhetstiltak

Svar	Antall	% av svar
0 %	3	7,89 %
1 - 5%	28	73,68 %
6 - 10%	4	10,53 %
Vet ikke	3	7,89 %
Totalsum	**38**	**100,00 %**



Figur 17: Histogram spørsmål 13 – Andel av omsetning brukt årlig på digitale sikkerhetstiltak

Spørsmål 14:

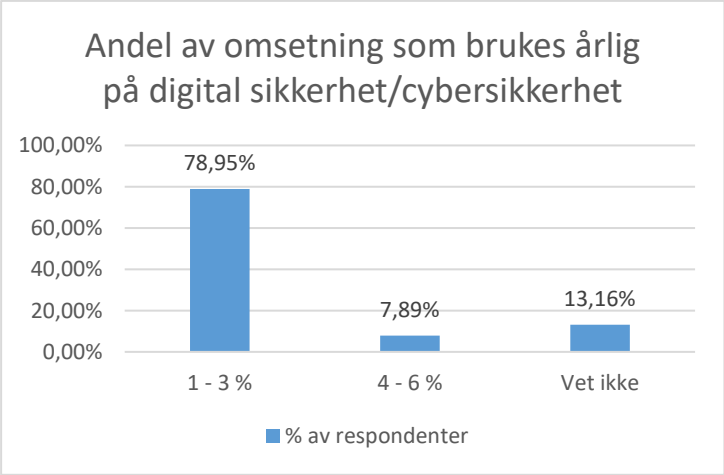
Hvor stor andel av virksomhetens omsetning vil du anslå virksomheten bruker årlig på kompetanseøkning av ansatte innen digital sikkerhet-/cybersikkerhetstiltak

Anslag i prosent på virksomheters årlige investering i kompetanseøkning av ansatte i digital sikkerhet- cybersikkerhet. Denne skalaen burde også hatt flere mindre prosentsatser.

Tabellen og histogrammet viser at 78,95% bruker 1 – 3% mot kompetanseøkning av ansatte og 7,89% bruker 4 – 6%, og 13,16% vet ikke.

Tabell 12: Spørsmål 14 - Andel av omsetning brukt årlig på kompetanseøkning av ansatte

Svar	Antall	% av respondenter
1 - 3 %	**30**	**78,95 %**
4 - 6 %	3	7,89 %
Vet ikke	5	13,16 %
Totalsum	**38**	**100,00 %**



Figur 18: Spørsmål 13 - Andel av omsetning brukt årlig på kompetanseøkning av ansatte

Spørsmål 15:

Har virksomheten vært utsatt for cyberangrep?

Tabellen nedenfor viser antallet respondenter/virksomheter som har vært utsatt for cyberangrep. Hele 15 virksomheter, og 39,47% av utvalget totalt.

Tabell 13: Spørsmål 15 - Har virksomheten vært utsatt for cyberangrep?

Svar	Antall	% av respondenter
Vet ikke	4	10,53 %
Nei	19	50,00 %
Ja	15	39,47 %
Totalsum	**38**	**100,00 %**

Spørsmål 15a:

Hva vil du anslå dette kostet virksomheten økonomisk? Skriv inn anslått beløp i norske kroner.

Tabellen nedenfor viser anslått kostand for virksomhetene som har vært utsatt for cyberangrep. Et gjennomsnitt på 1,22 millioner, median på 300 000,- og en min verdi på 20 000,- og en maksverdi på 5 000 000.

Det var ikke alle respondenter som svarte ja som svarte på denne, og noen skrev setninger uten tall som det ble bedt om, så de ble forkastet. Av de som var igjen ble det regnet ut gjennomsnitt, median og min/max.

Tabell 14: Spørsmål 15a - Anslå kostnad til virksomheten etter og vært utsatt for cyberangrep

Beregning	Beløp
Gjennomsnitt	**kr 1 221 250,00**
Median	kr 300 000,00
Min	kr 20 000,00
Max	kr 5 000 000,00

Spørsmål 15b:

I hvilken grad var sikkerhetskultur og investeringer i sikkerhetsteknologi implementert før hendelsene?

Virksomhetene i forhold til om de hadde innført sikkerhetskultur og investeringer var implementer før hendelsene. Gjennomsnitt på 4,4 – i noen grad.

Tabell 15: Spørsmål 15b - I hvilken grad var sikkerhetskultur og investeringer i sikkerhetsteknologi implementert før hendelsene?

Svar	Antall	% av respondenter
I svært liten grad	1	6,67 %
I liten grad	0	0 %
I noen grad	8	53,33 %
I stor grad	4	26,67 %
I svært stor grad	2	13,33 %
Totalsum	**15**	**100,00 %**

Spørsmål 16:

I hvilken grad er digital sikkerhetskultur en del av virksomhetens strategi?

Tabellen nedenfor viser at av virksomhetene som hadde innført digital sikkerhetskultur som en del av strategien, var det et gjennomsnitt på 4,15 som er litt over middels grad.

Tabell 16: Spørsmål 16 - I hvilken grad er digital sikkerhetskultur en del av virksomhetens strategi?

Svar	Antall	% av respondenter
I svært liten grad	2	2,53 %
I liten grad	6	11,39 %
I middels grad	17	43,04 %
I stor grad	10	31,65 %
I svært stor grad	3	11,39 %
Totalsum	**38**	**100,00 %**

Spørsmål 17:

I hvilken grad styres investeringer i sikkerhetsteknologi fra ledelsen?

Virksomhetenes grad av styring på investeringer innen sikkerhetsteknologi fra ledelsen. Gjennomsnitt på 4,52 – i noen grad til i stor grad.

Tabell 17: Spørsmål 17 - I hvilken grad styres investering av sikkerhetsteknologi fra ledelsen?

Svar	Antall	% av respondenter
I liten grad	6	15,79 %
I noen grad	13	34,21 %
I stor grad	12	31,58 %
I svært stor grad	7	18,42 %
Totalsum	**38**	**100,00 %**

Spørsmål 18:

I hvilken grad styres investeringer i kompetanseutvikling fra ledelsen?

Tabellen nedenfor viser i hvilken grad investeringene i kompetanseutvikling var styrt av ledelsen. Et gjennomsnitt på 4,34 – i noen grad.

Tabell 18: Spørsmål 18 - I hvilken grad styres investeringer i kompetanseutvikling fra ledelsen?

Svar	Antall	% av svar
I svært liten grad	1	3 %
I liten grad	6	16 %
I noen grad	12	32 %
I stor grad	17	45 %
I svært stor grad	2	5 %
Totalsum	**38**	**4,342105263**

Spørsmål 19:

I hvilken grad har virksomheten delegert ansvaret til egne roller/avdelinger for ivaretakelse av digital- sikkerhetsteknologi og sikkerhetskultur?

Tabellen nedenfor viser om virksomhetene hadde delegert ansvar til egne roller eller avdelinger for ivaretakelse av digital- sikkerhetsteknologi og sikkerhetskultur. Gjennomsnitt på 4,68, i stor grad mot i svært stor grad.

Tabell 19: Spørsmål 19 – I hvilken grad har virksomheten delegert ansvar til egne roller/avdelinger

Svar	Antall	% av svar
I svært liten	2	5,26 %
I liten grad	1	2,63 %
I noen grad	14	36,84 %
I stor grad	11	28,95 %
I svært stor g	10	26,32 %
Totalsum	**38**	**100,00 %**

Spørsmål 20:

I hvilken grad måler virksomheten effekten av digital sikkerhetskulturen i virksomheten?

I hvilken grad virksomheten hadde innført målinger på effekten av digital sikkerhetskultur. Et gjennomsnitt på 3,81 – i noen grad.

Tabell 20: Spørsmål 20 - I hvilken grad måler virksomheten effekten av digital sikkerhetskultur

Svar	Antall	% av svar
Vet ikke	1	2,63 %
I svært liten grad	4	10,53 %
I liten grad	6	15,79 %
I noen grad	19	50,00 %
I stor grad	6	15,79 %
I svært stor grad	2	5,26 %
Totalsum	**38**	**100,00 %**

Spørsmål 21:

I hvilken grad måler virksomheten effekten av digital sikkerhetsteknologi?

Tabellen nedenfor viser i hvilken grad virksomhetene måler effekten av sin digitale sikkerhetsteknologi. Gjennomsnitt på 3,57 som er midt mellom i liten grad og i noen grad. Og hvor ca 1/3 mener de måler effekten av deres digitale sikkerhetsteknologi noen grad.

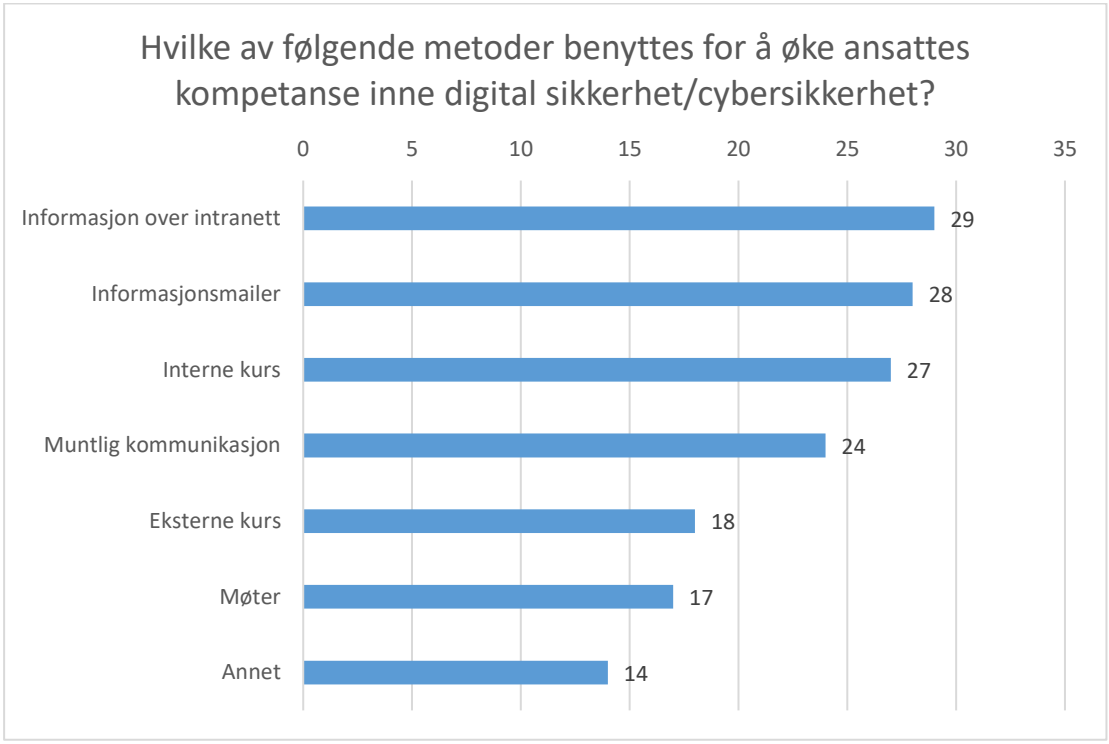
Tabell 21: Spørsmål 21 - I hvilken grad måler virksomheten effekten av digital sikkerhetsteknologi?

Svar	Antall	% av Svar
Vet ikke	1	2,63 %
I svært liten grad	7	18,42 %
I liten grad	9	23,68 %
I noen grad	12	31,58 %
I stor grad	8	21,05 %
I svært stor grad	1	2,63 %
Totalsum	**38**	**100,00 %**

Spørsmål 22:

Hvilke av følgende metoder benyttes for å øke ansatte kompetanse innen digital sikkerhet/cybersikkerhet?

Histogrammer nedenfor viser hvilke metoder som ble benyttet i virksomhetene for å øke ansattes kompetanse innen digital sikkerhet/cybersikkerhet. Funnen viser at informasjon over intranett, e-post, interne kurs og muntlig kommunikasjon er de mest brukte metodene.

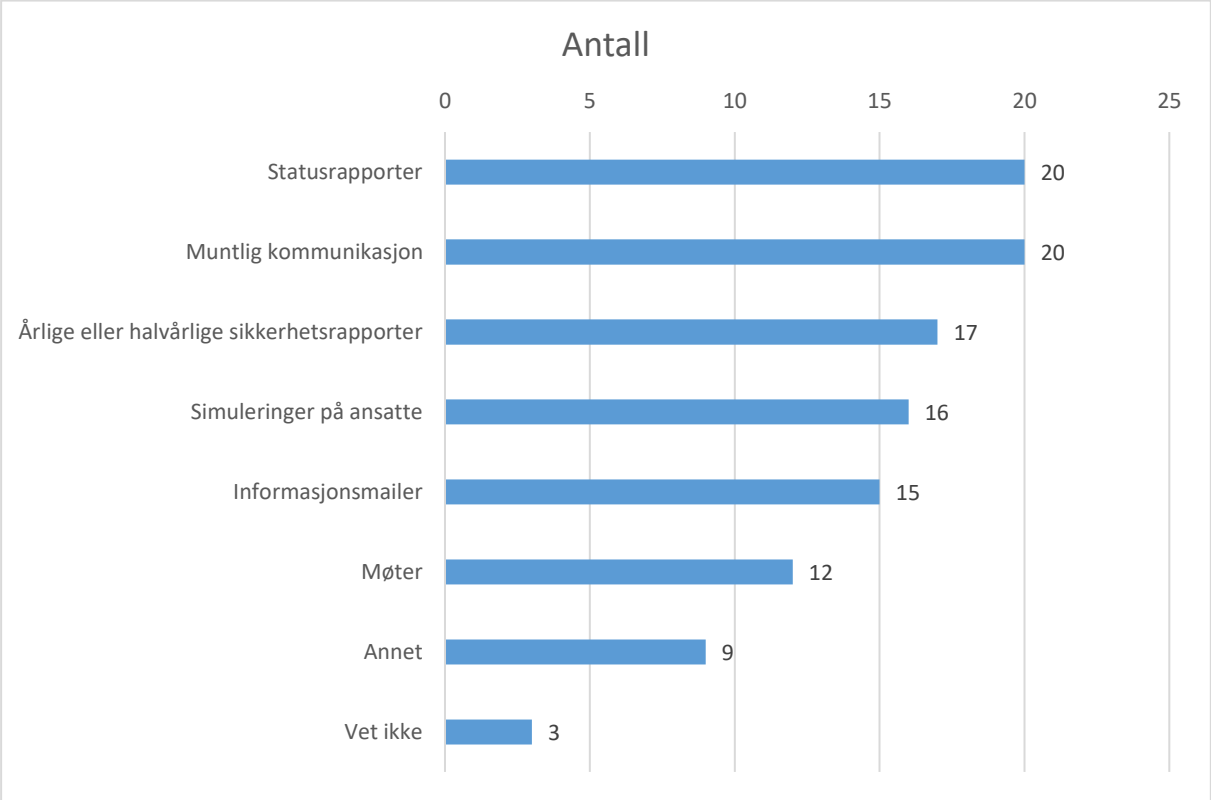


Figur 19: Spørsmål 22 - Benyttede metoder for økning av ansattes kompetanse innen digital sikkerhetskultur

Spørsmål 23:

Hvordan måler ledelsen sikkerhetsnivået i virksomheten innen digital sikkerhet/cybersikkerhet i virksomheten?

Hvordan ledelsen måler sikkerhetsnivået i virksomheten ut fra noen velkjente metoder. Statusrapporter, muntlig kommunikasjon, årlig- eller halvårlige rapporter, simuleringer på ansatte og informasjonermaler var de 5 øverste rangerte metodene for å måle sikkerhetsnivået innen digital sikkerhet/cybersikkerhet.



Figur 20: Spørsmål 23 - Metoder for måling av sikkerhetsnivå innen digital sikkerhet/cybersikkerhet

Spørsmål 24:

I hvilken grad anser virksomheten at investeringer i sikkerhetsteknologi bidrar til å minske risikoen for cyberangrep?

Tabellen nedenfor viser hvordan virksomhetene så på investeringer i sikkerhetsteknologi var med på å minske risikoen for cyberangrep. *4,89, som er tilnærmet i stor grad.*

Tabell 22: Spørsmål 24 - Anseelse av om investeringer i sikkerhetsteknologi minsker risiko for cyberangrep

Svar	Antall	% av svar
I liten grad	1	2,63 %
I middels grad	10	26,32 %
I stor grad	19	50,00 %
I svært stor grad	8	21,05 %
Totalsum	**38**	**100,00 %**

Spørsmål 25:

I hvilken grad anser virksomheten at investeringer i økt kompetanse hos personell innen digital sikkerhet bidrar til å minske risikoen for cyberangrep?

Tabellen nedenfor viser hvordan virksomhetene ser på investeringer i økt kompetanse på personell som et tiltak for å minske risikoen for cyberangrep. Gjennomsnitt på 4,94, som er tilnærmet i stor grad.

Tabell 23: Spørsmål 25 - Anseelse av om investeringer i økt kompetanse hos personell innen digital sikkerhet minsker risikoen for cyberangrep

Svar	Antall	% av svar
I liten grad	1	2,63 %
I middels grad	8	21,05 %
I stor grad	21	55,26 %
I svært stor grad	8	21,05 %
Totalsum	**38**	**100,00 %**

4.2 Bivariate analyser

Bivariate analyser handler om og finne samsvar eller samvariasjon, også kalt korrelasjon mellom variabler. Metoden som her er benyttet er Pearson R, som angir hvor sterk lineær sammenheng det er mellom to variabler (Johannessen et al, 2011, s. 320). Pearsons R er en standard koeffisient som skal variere mellom -1 og 1, hvor 0 tilsvarer ingen lineær sammenheng. Cohen og Holliday (1982) definerer følgende regler for å definere styrken på sammenhengene (Johannesen et al, 2011)

- 0,00 – 0,19 Veldig svak
- 0,20 – 0,39 Svak
- 0,40 – 0,69 Moderat
- 0,70 – 0,89 Høy
- 0,90 – 1,00 Meget høy

Jeg velger der imot å benytte meg av en enklere skala (Bergsaker, A.S, 2022)

- $R \geq 0,1$ Liten effekt
- $R \geq 0,3$ Middels
- $R \geq 0,5$ Stor

Det er i hovedsak hypotesene opp mot forskningsspørsmålene som jeg skal gjøre bivariate analyser på. Det ble også gjennomført ikke-parametriske- og spearmans'rho korrelasjon for å kunne sammenlikne hvis noen av hypotesene ikke var signifikante, uten at det utgjorde en forskjell.

4.2.1 Hypotese 1a og 1b

De første hypotesene som skal testes er:

- H1a: Forankring av sikkerhetsarbeid i ledelsen har sammenheng med innført digital sikkerhetskultur
- H1b: Forankring av sikkerhetsarbeid sammenheng med ledelsestiltak innen digital sikkerhetskultur

Det ble kjørt Pearson korrelasjon på H1a hvor resultatene ble:

$r(36) = .47, p = .003$ – Middels korrelasjon

For H2a ble resultatene:

$r(36) = .65, p < .001$ – Stor korrelasjon

Begge hypotesene er signifikante innenfor et intervall for $P \leq 0.05$. Og gir derfor støtte til at både digital sikkerhetskultur og sammensatte ledelsestiltak har sammenheng med forankring av sikkerhetsarbeid i ledelsen.

4.2.2 Hypotese 2a, 2b og 2c

Følgende hypoteser skal testes for korrelasjon:

- H2a Prioriterte tiltak i sikkerhetsteknologi innen cybersikkerhet har sammenheng med risiko for å bli utsatt for cyberangrep
- H2b: Prioriterte tiltak i kompetanseøkning har sammenheng med risiko for å bli utsatt for cyberangrep
- H2c: Tiltak i måling av digital sikkerhetskultur og teknologi i kompetanseøkning har sammenheng med risiko for å bli utsatt for cyberangrep
- H2d: Prioriterte tiltak i outsourcing av sikkerhetsarbeid har sammenheng med risiko for å bli utsatt for cyberangrep

Det ble gjennomført Pearson korrelasjon for H2a med følgende resultater:

$r(36) = .44$, $p = .005$ – Middels korrelasjon

Det ble gjennomført Pearson korrelasjon for H2b med følgende resultater:

$r(36) = .44$, $p = .006$ – Middels korrelasjon

Det ble gjennomført Pearson korrelasjon for H2c med følgende resultater:

$r(34) = .38$, $p = .024$ – Liten korrelasjon

Det ble gjennomført Pearson korrelasjon for H2d med følgende resultater:

$r(34) = -.001$ $p = .996$ – ingen korrelasjon

Hypoteser H2a, H2b og H2c er alle signifikante innenfor et intervall for $P \leq 0.05$.

Hypotese H2d er ikke signifikant på variabelen.

På bakgrunn av resultatene så betyr det at prioriterte tiltak innen sikkerhetsteknologi, kompetanseøkning og måling av digital sikkerhetskultur har sammenheng med risiko for å bli utsatt for cyberangrep.

4.2.3 Hypotese 3a

Følgende hypoteser skal testes for korrelasjon

- H3a: Investeringer i kompetanse og sikkerhetsteknologi har sammenheng med risiko for å bli utsatt for cyberangrep

Det ble gjennomført Pearson korrelasjon for H3a med følgende resultater.

r(36) = .29, p =.08 – ingen korrelasjon

Investering i kompetanse og sikkerhetsteknologi har ifølge testen ingen sammenheng med risiko.

4.2.4 Oppsummering hypoteser Pearson r korrelasjonsanalyse

Tabell 24: Oppsummering hypoteser Pearson r korrelasjon

Hypoteser korrelasjonsanalyse:	**Verdier og styrke på korrelasjon**
H1a: Forankring av sikkerhetsarbeid i ledelsen har sammenheng med innført digital sikkerhetskultur	r(36) = .44, p =.005 Middels korrelasjon
H1b: Forankring av sikkerhetsarbeid sammenheng med ledelsestiltak innen digital sikkerhetskultur	r(36) = .65, p < .001 – Stor korrelasjon
H2a Prioriterte tiltak i sikkerhetsteknologi innen cybersikkerhet har sammenheng med risiko for å bli utsatt for cyberangrep	r(36) = .44 p =.005 Middels korrelasjon
H2b: Prioriterte tiltak i kompetanseøkning har sammenheng med risiko for å bli utsatt for cyberangrep	r(36) = .44, p =.006 Middels korrelasjon
H2c: Tiltak i måling av digital sikkerhetskultur og teknologi i kompetanseøkning har sammenheng med risiko for å bli utsatt for cyberangrep	r(34) = .38, p =.024 Liten korrelasjon
H2d: Prioriterte tiltak i outsourcing av sikkerhetsarbeid har sammenheng med risiko for å bli utsatt for cyberangrep	r(34) = -.001 p =.996 ingen korrelasjon
H3a: Investeringer i kompetanse og sikkerhetsteknologi har sammenheng med risiko for å bli utsatt for cyberangrep	r(36) = .29, p =.08 ingen korrelasjon

4.3 Multivariat regresjonsanalyse

Videre utføres det multivariat regresjonsanalyse på hypotesene for å faktisk kunne si om det er sammenheng mellom variablene i hypotesen. Multivariate regresjonsanalyse forutsetter at alle relevante og ingen irrelevante uavhengige variabler være tatt med. Sammenhengen mellom de uavhengige variablene og den avhengige må være lineær, og sammenhengene må være additave. I tillegg må restleddet, eller residualene være normalfordelt rundt regresjonslinjen og være jamt fordelt (homoskedastisitet). Hvis kriteriene ikke er møtt kan det føre til feil i hypotesetestingen (Johannessen et al, 2011).

4.3.1 Hypotese 1a og 1b

Avhengig variabel:

- I hvilken grad er sikkerhetsarbeid innen digital sikkerhet/cybersikkerhet forankret i ledelsen

Uavhengig variabel:

- I hvilken grad har virksomheten innført digital sikkerhetskultur som en del av organisasjonskulturen?
- Sammenslått variabelt ledelsestiltak innen digital sikkerhetskultur

Tabellen nedenfor viser regresjonsanalysen for H1a og H2b. F-verdien viser at modellen er signifikant på $p < 0,001$, og forklart varians $R^2 = 0,44$ eller beskriver den avhengige variabelens variabilitet på modellen. Beta-verdien (B) forklarer de uavhengige variablenes effekt på den avhengige variabelen- her 0,293 for digital sikkerhetskultur som en del av organisasjonskulturen og 0,193 for ledelsestiltak innen digital sikkerhetskultur.

Digital sikkerhetskulturvariabelen er ikke signifikant opp mot den avhengige variabelen med en p =,079. Ledelsestiltak innen digital sikkerhetskultur har der imot en signifikans på $p < 0,001$. VIF verdiene ligger på 1,201 så det er ikke fare for multikolinearitet.

Med bakgrunn i B-verdien for H1a, og en margin på 0,021 for at den skulle vært signifikant, og en korrelasjonsverdi på r=,47 og korrelasjonssignifikans på p =,001 velger jeg beholde den i fare for å forkaste feil hypotese.

H1b er signifikant og støtter opp om at ledelsestiltak innen digital sikkerhetskultur har sammenheng med i hvilken grad sikkerhetsarbeid innen digital sikkerhet/cybersikkerhet er forankret i ledelsen.

Tabell 25: Regresjonsanalyse av Hypotese 1a og 1b

F	Antall	R	R^2	Justert R^2	Std Feil	
15,566 (p < 0,001)	37	0,686	0,441	0,471	0,714	
Variabel	**B**	**Std. avvik**	**Std. B**	**t**	**Sign**	**VIF**
Digital sikkerhetskultur som en del av organisasjonskulturen	**0,293**	0,162	0,244		**0,079**	1,201
Ledelsestiltak innen digital sikkerhetskultur	**0,193**	0,047	0,549		**<,001**	1,201
Konstant	0,545	0,775		0,703		

4.3.2 Hypotese 2a, 2b, 2c og 2d

Avhengig variabel:

- I hvilken grad vil du karakterisere risikoen for at virksomheten kan bli utsatt for cyberangrep

Uavhengig variabel:

- Prioriterte tiltak i sikkerhetsteknologi inne cybersikkerhet
- Prioriterte tiltak i kompetanseøkning
- Tiltak i måling av digital sikkerhetskultur
- Prioriterte tiltak i outsourcing

F-verdien viser at modellen er signifikant på p = 0,019, og med R^2 = 0,22 forklarer det den avhengige variabelens variabilitet på modellen. For de flest B-verdiene har vi noe påvirkning, men ingen av de uavhengige variablene er signifikante med verdier fra 0,105 – 0,884. Dette kan dog skyldes at dataene ikke er lineære eller normalfordelte, og at dette da for utslag på modellen. Dette bekreftes av normale P-P-plot som viser residualer som ligger utenfor normalfordelings-linjen (Bergaker, A.S, 2022). VIF-verdiene ligger fra 1,160 til 1,402 som betyr at det ikke er fare for multikolinearitet.

Hypoteser 2a, 2b, 2c og 2d må i dette tilfellet forkastes. P-P-plot og regresjon ligger i vedlegg.

Tabell 26: Regresjonsanalyse av Hypotese 2a, 2b, 2c og 2d

F	Antall	R	R^2	Justert R^2	Std Feil
3,450 (p = 0,019)	36	0,555	0,219	0,308	0,685

Variabel	B	Std. avvik	Std. B	t	Sign	VIF
Prioritert tiltak innen sikkerhetsteknologi	0,204	0,131	0,276	1,559	0,129	1,402
Prioriterte tiltak innen kompetanseøkning	0,061	0,049	0,224	1,248	0,221	1,441
Prioriterte tiltak innen måling av digital sikkerhetskultur	0,118	0,071	0,269	1,669	0,105	1,160
Prioriterte tiltak innen outsourcing av sikkerhetsarbeid	-0,007	0,045	-0,025	-0,147	0,884	1,293
Konstant	1,622	0,817		0,056	0,056	

4.3.3 Hypotese 3a

Avhengig variabel:

- I hvilken grad vil du karakterisere risikoen for at virksomheten kan bli utsatt for cyberangrep

Uavhengig variabel:

- Investeringer i kompetanse og sikkerhetsteknologi

F-verdien viser her at modellen ikke er signifikant med en p = 0,080 og med en R^2 =,057. B-verdien er også nokså lav på 0,181. Den uavhengige variabelen har en p = ,08 som tilsvarer at den ikke er signifikant. Den har der imot en korrelasjonssignifikans på p = ,04 som er middels, og en r=,287. Også her viser normal P-P plot residualer som ligger utenfor normalfordelingslinjen. VIF-verdi på 1 betyr at det ikke er fare multikolinearitet:

Tabell 27: Regresjonsanalyse av Hypotese 3a

F	Antall	R	R^2	Justert R^2	Std Feil
3,243 (p = 0,080)	36	0,287	0,83	0,057	0,772

Variabel	B	Std. avvik	Std. B	t	Sign	VIF
Investering i sikkerhetsteknologi og kompetanse	0,181	0,100	0,287	1,801	0,080	1,000
Konstant	2,667	0,997		2,675	0,110	

Jeg velger med bakgrunn i dataene og forkaste hypotese H3a. P-P-plot og regresjon er ligger i vedlegg.

4.4.4 Oppsummering hypotesetesting multivariat regresjon

Tabell 28: Oppsummering hypoteser multivariat analyse

Hypoteser multivariat regresjonsanalyse:	**Beholdes eller forkastes:**
H1a: Forankring av sikkerhetsarbeid i ledelsen har sammenheng med innført digital sikkerhetskultur	**Beholdes**
H1b: Forankring av sikkerhetsarbeid sammenheng med ledelsestiltak innen digital sikkerhetskultur	**Beholdes**
H2a Prioriterte tiltak i sikkerhetsteknologi innen cybersikkerhet har sammenheng med risiko for å bli utsatt for cyberangrep	**Forkastes**
H2b: Prioriterte tiltak i kompetanseøkning har sammenheng med risiko for å bli utsatt for cyberangrep	**Forkastes**
H2c: Tiltak i måling av digital sikkerhetskultur og teknologi i kompetanseøkning har sammenheng med risiko for å bli utsatt for cyberangrep	**Forkastes**
H2d: Prioriterte tiltak i outsourcing av sikkerhetsarbeid har sammenheng med risiko for å bli utsatt for cyberangrep	**Forkastes**
H3a: Investeringer i kompetanse og sikkerhetsteknologi har sammenheng med risiko for å bli utsatt for cyberangrep	**Forkastes**

5. Resultater

Resultatene fra analysen vil her bli presentert opp mot problemstilling, forskningsspørsmål og relevant teori. Hensikten med undersøkelsen var å finne ut i hvilken grad har ledere i store norske virksomheter innført digital sikkerhetskultur i virksomheten, og hvordan prioriteres tiltak og investeringer i sikkerhetsteknologi og kompetanse for å minske risikoen for å bli utsatt for cyberangrep?

5.1 Diskusjon

5.1.1 Digital sikkerhetskultur i store norske virksomheter

Alle respondentene er avhengig av IT-systemer i stor- til svært stor grad, noe som er en forutsetning for digital sikkerhetskultur. Hvordan sikkerhetskulturen er i en virksomhet vil også kunne være avgjørende for om det velges enkle løsninger, enn den mer utforende løsningen for å få god nok sikkerhet (Aven et al, 2004, s. 34; Gunnes 2020). Lederne i en organisasjon eller virksomhet betraktes ofte som de viktigste kulturskaperne fordi det er de som sitter med mest makt til å kunne prege organisasjonen i forhold til deres virkelighetsdefinisjoner (Schein, 1983, 2017; Bang, 2020).

Virksomhetene i denne undersøkelsen har i noen grad – stor grad innført digital sikkerhetskultur som en del av organisasjonskulturen med et gjennomsnitt på 3,7 opp mot Blum (2020) sin modenhetsmodell. Dette tilsvarer nivå 3 -definert eller nivå 4-styrt i modellen.

Blum har kartlagt og sammenlignet flere bransjer og domener og målet et gjennomsnitt på 2,75, noe han bemerker er for lavt sett opp mot generell digital sikkerhetskultur. Han påpeker videre at finansiell sektor, myndigheter, helsesektor, høyteknologiske virksomheter, produksjonsvirksomheter og universiteter bør tilstrebe et nivå på rundt 3.5 som også kalles «the sweet spot». For virksomhetene i denne undersøkelsen er de allerede over dette nivået, noe som er meget positivt for norske virksomheter hvis det stemmer. Ifølge undersøkelser gjort av Gartner (2020) mente 87% av toppledere at digitalisering av virksomhetene hadde prioritet, men det i realiteten bare vare 40% som hadde gjennomført digitalisering. Fordi dette er kvantitativ analyse gjennomført på en bestemt tid vil det være vanskelig å si om resultatene er eksakte, og det kan derfor ikke generaliseres i en større populasjon.

Hvis virksomhetene ligger på nivå 3 i Blum (2020) modell betyr det at virksomheten har etablert et omfattende sett med virksomhetsomspennende sikkerhetsprosesser, styringssystem, policyer og dokumenterte tekniske måleparametere. De er dog avhengige av enkeltindividers innsats, og prosesser innenfor endringsledelse, revisjon og leverandørsikkerhet må forbedres. Mer arbeid er også nødvendig innen rollespesifikke sikkerhetskunnskaper- og bevissthet, fremme sikkerhetsovervåkning, analyser og tilgangskontroll. For disse virksomhetene bør de fokusere på revisjoner, endringsledelse, og mer avansert sikkerhetsovervåking inkludert målinger for å øke nivået innen verifisering og ansvarliggjøring, og økt sikkerhet (Blum, 2020).

For de som ligger på nivå 4 eller høyere vil det si at virksomhetene har definert og bygget et omfattende sett med kontrollere og styringssystem innen digital sikkerhet for mennesker, prosesser og teknologi. Imidlertid er de fortsatt avhengige av manuelle prosesser og de står ovenfor utfordringer med å opprettholde styringssystemet for sikkerhet i møte med kontinuerlige endringer i trussel-, regulerings-, teknologi- og virksomhetslandskapet de er i. Virksomheter på dette nivået bør fokusere på mer automasjon for å gjøre ting mer kostnadseffektivt og skalerbart (Blum, 2020a).

For virksomhetene er 89,5% av respondentene enige i at sikkerhetskultur i virksomheten er et ledelsesansvar, men i om sikkerhetsarbeid er forankret i ledelsen så er det 39,5% som svarer i noen grad, og 57,8% likt fordelt på stor- og i svært stor grad. Dette betyr at litt over halvparten av respondentene i undersøkelsen har forankret sikkerhetsarbeidet i ledelsen. Dette kan igjen tolkes opp mot Blums nivå 3, og at det fortsatt er arbeid som gjenstår med forankring av sikkerhetsarbeid i ledelsene.

Videre viser analysene at 73,7% av respondentene har innført styringssystem eller rammeverk for virksomhetene, og hvor 23,7% ikke har det. Virksomhetene hadde også i middels grad innført digital sikkerhetskultur som en del av strategien, og investeringer innen sikkerhetsteknologi og kompetanse var i styrt fra ledelsen i noen grad – stor grad. Bergsjø et al, (2018) og NSM (2021) viser til at lederne i virksomheten er ansvarlig for at styringssystem og andre nødvendige tiltak er iverksatt for den totale sikkerheten i virksomheten. For å få til et godt sikkerhetsnivå så må den digitale sikkerhetskulturen være forankret i ledelsen og i styret til virksomheten, og det bør være et styringssystem som ivaretar og beskriver hvordan virksomhetene skal håndtere sikkerhetsarbeid, tiltak, investeringer og aktiviteter.

Analyser opp mot forskningsspørsmålene viser at digital sikkerhetskultur og sammensatte ledelsestiltak, herunder: innført styringssystem, digital sikkerhetskultur er en del av virksomhetens strategi, og i hvilken grad investeringer i sikkerhetsteknologi og kompetanse styres av ledelsen har sammenheng med forankring av sikkerhetsarbeid i ledelsen. Dette bekreftes også av gjeldende med teorier.

Digital sikkerhetskultur er under konstant utvikling, og bør derfor være en del av virksomhetens strategi (Blum, 2020, s. 94). Hvis ikke digital sikkerhet er sett på som strategisk og ikke blir prioritert i virksomheten så vil heller ikke det forbedre kulturene, eller bedre sikkerheten (Blum, 2020, s. 94). Hvis virksomheter skal kunne øke den digitale sikkerhet så må de ha den rette katalysatoren- og det er styret og toppledelsen i virksomheten. Digital sikkerhet, kultur og tiltak starter i toppen av virksomheten hvor retning og omfang bestemmes. Der fra vil det gå nedover i virksomheten til resten av organisasjon. Fokuset på digital sikkerhet og risiko skifter fra digitale teknologier eller spesialister innen IT til virksomhetens ledere (Parnety & Domet, 2020).

5.1.2 Prioriteringer av tiltak og investeringer i sikkerhetsteknologi og kompetanse for å minske risikoen for å bli utsatt for cyberangrep

Virksomhetene i undersøkelsen karakteriserer risikoen for å bli utsatt for å bli utsatt for cyberangrep til å være i noen grad. Virksomhetene anser også at investeringer i sikkerhetsteknologi og økning av kompetanse hos personell bidrar til å minske risikoen for cyberangrep i stor grad. Risiko handler om å håndtere trusler, sårbarheter, usikkerhet og tap av tjenester eller verdier i en virksomhet (Blum, 2020).For å håndtere dette må virksomheter ha innført risikostyring som en del av styringssystemet for sikkerhet (Nätt, 2021. s 353).

Hele 39,5% av virksomhetene har vært utsatt for cyberangrep, og av disse kostet det virksomhetene fra 20 000 norsker kroner til 5 millioner norske kroner, med et gjennomsnitt på 1,22 millioner kroner og en median på 300 000 kroner. Disse verdiene må tolkes meget forsiktig da utvalget og antallet respondenter er veldig få. Kostanden av cyberangrep mot en virksomhet er vanskelig å gi spesifikke tall på, da de varierer mye alt etter omfanget av angrepet, og hva det er som blir utsatt (Guim, 2021). For virksomhetene som var utsatt for cyberangrep hadde 53,3% i noen grad implementert sikkerhetskultur og investeringer i sikkerhetsteknologi før hendelsene, mens 26,7% hadde innført i stor grad.

Nätt (2021) poengterer vider at virksomhetene må ha fokus på kompetanseutvikling i form av sikkerhetsopplæring og bevisstgjøring av ansatte, og ikke bare fokusere på digitale sikkerhetstjenester- og teknologi. For virksomhetene i undersøkelsen trenger de i stor grad mer kompetanse innen digital sikkerhet/cybersikkerhet, og de har alle innført ulike metoder for å øke ansattes kompetanse innen digital sikkerhet og cybersikkerhet. Informasjon over virksomheters intranett, e-poster, interne kurs og muntlig kommunikasjon er de mest fremtredende. 78,95% av virksomhetene benytter 1-3% av omsetningen på kompetanseøkning av ansatte innen digital sikkerhet/cybersikkerhet, og 7,89% bruker 4 – 6%. Dette vil også være varierende ut fra størrelsen på virksomheten.

Virksomhetene prioriterer økt kompetanse hos nøkkelpersonell innen informasjon- og cybersikkerhet høyest av prioriterte tiltak innen digital sikkerhet/cybersikkerhet for å redusere risikoen for cyberangrep. Deretter kommer sikkerhetsteknologi inne cybersikkerhet, økt kompetanse hos ansatte og ledere. Øking i antall ansatte med spesialkompetanse innen digital sikkerhet/cybersikkerhet og outsourcing av sikkerhetsarbeid havner nederst. Men det er ikke mye varians som skiller variablene. Av virksomhetene er det 73,7% som bruker 1 – 5% av årlig omsetning på digitalt sikkerhet- og cybersikkerhetstiltak, og 10,5% som bruker 6 – 10%. Dette stemmer også med Guim (2021) estimat om at virksomheter bruker mellom 6% - 14% av IT-budsjettet, og gjennomsnittet ligger på rundt 10%. Denne skalaen i samråd med den forrige kunne nok vært justert ned til mindre varianser for å få mer nøyaktige målinger.

Målinger av digital sikkerhetskultur og dets omfang kan være utfordrende, og vanskelig å determinere hva en faktisk skal måle. Likevel vil det være en fordel for virksomheter å ha måleparameter på digital sikkerhetskultur, sikkerhetsteknologi og kompetanseutvikling (Blum, 2020; Nätt, 2021). Virksomhetene måler effekten av digital sikkerhetskultur og digital sikkerhetsteknologi i virksomheten i noen – stor grad.

Videre analyser av forskningsspørsmål med regresjonsanalyse viser ingen sammenheng mellom prioriterte tiltak innen sikkerhetsteknologi, økt kompetanse hos ansatte, effekt av målinger eller outsourcing av sikkerhetsarbeid opp mot risikoen for å bli utsatt for cyberangrep. Gjeldende teori tilsier at det burde være en form for sammenheng, men resultatene kan skyldes at dataene ikke er lineære opp mot regresjonslinjen og at de spriker for mye mot en retning, eller at enkelte residualer ligger for langt unna linjen slik at det blir dårlig homoskedastisitet. Korrelasjonsanalysene viser samsvar på enkelte, men det er ikke nok for å kunne trekke sammenhenger med sikkerhet.

5.2 Konklusjon

Det har gjennom denne undersøkelsen vært sett på i hvilken grad ledere i store norske virksomheter har innført digital sikkerhetskultur i virksomheten, og hvordan prioriteres tiltak og investeringer i sikkerhetsteknologi og kompetanse for å minske risikoen for å bli utsatt for cyberangrep.

Resultatene viser at virksomhetene er avhengig av IT-systemer. Virksomhetene har i noen grad til stor grad innført digital sikkerhetskultur opp mot Dan Blums rasjonelle modenhetsmodell, henholdsvis nivå 3 og 4. Av virksomhetene er 89,5% enige i at sikkerhetskultur er et ledelsesansvar, og hvor 57,8% likt fordelt på i stor og i svært stor grad har forankret sikkerhetsarbeid i ledelsen. Videre hadde 73,7% av virksomhetene innført styringssystem eller rammeverk, og i middels grad innført digital sikkerhetskultur som en del av strategien. Analyser viser også at digital sikkerhetskultur og ledelsestiltak innen digital sikkerhetskultur har sammenheng med forankring av sikkerhetsarbeid i ledelsen.

Virksomhetene karakterisere risikoen for å bli utsatt for cyberangrep til å være i noen grad, og investeringer i sikkerhetsteknologi og økning av kompetanse hos personell bidrar til å minske risikoen for cyberangrep i stor grad. Hele 39,5% av virksomhetene hadde vært utsatt for cyberangrep, og hvorav 53,3% i noen grad hadde implementert sikkerhetskultur og investeringer i sikkerhetsteknologi før hendelsene, og 26,7% hadde innført i stor grad. Virksomhetene trenger i stor grad kompetanse innen digital sikkerhet, og 78,9% bruker 1-3% av omsetningen på investering i kompetanseøkning av ansatte. Videre prioriterer de økt kompetanse hos nøkkelpersonell innen informasjon- og cybersikkerhet som høyeste prioriterte tiltak for å minske risikoen for å bli utsatt for cyberangrep. Det er heller ingen sammenheng mellom prioriterte tiltak innen sikkerhetsteknologi, økt kompetanse, effekt av målinger eller outsourcing av sikkerhetsarbeid opp mot risikoen for å bli utsatt for cyberangrep. Dette er noe motstridig mot gjeldende teori.

5.3 Videre forskning

Ut fra resultater og bearbeidelsen av materialet ville det vært interessant for en fremtidig studie å gå mer i dybden på Dan Blums rasjonelle modenhetsmodell og å faktisk måle sikkerhetsnivået i virksomheter og om de stemmer med eget antatt nivå på modellen.

6. Referanser

Bang, H. (2020). Organisasjonskultur. (5.utg.). Oslo: Universitetsforlaget.

Bergsaker, A.H. (2022). Statistisk analyse i SPSS. Universitetet i Oslo. https://www.uio.no/for-ansatte/kompetanse/tema/data/it-forskning/spss/spss2022_oppf.pdf

Bergsjø, Håkon & Ronny Windvik. (2018). Cybersikkerhet for ledere – hvordan beskytte din virksomhet (1. utg). Universitetsforlaget.

Blum, Dan. (2020). Rational Cybersecurity for Business: The Security Leaders' guide to Business alignment.Silver spring: Apress Media LCC

Blum, Dan (2020a, 16. Februar). How to Assess Security Maturity and Make Improvements.

https://security-architect.com/how-to-assess-security-maturity-and-roadmap-improvements/

Da Veiga, A., Eloff, J.H.P. (2010) A framework and assessment instrument for information security culture. Computers & Security. Volume 29, Issue 2, September 2009. https://doi.org/10.1016/j.cose.2009.09.002

Departementene, 30.1.2019. Nasjonal strategi for digital sikkerhet. https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/nasjonal-strategi-for-digital-sikkerhet.pdf

Digitaliseringsdirektoratet, Digdir. (u.å). Informasjonssikkerhet – Veileder i kompetanse- og kulturutvikling inne digital sikkerhet. Hentet 10. Mai 2023 fra: https://www.digdir.no/informasjonssikkerhet/veileder-i-kompetanse-og-kulturutvikling-innen-digital-sikkerhet/2141

Fitzgerald, T. (2007). Building Management Commitment through Security Councils, or Security Council Critical Success Factors. In H. F. Tipton (Ed.), Information Security Management Handbook (pp. 105-121). Hoboken: Auerbach Publications.

Guim, T. (2021, 7. juli). Cost of Cyber Attacs vs. Cost of Cyber Security in 2021. https://pchtechnologies.com/cost-of-cyber-attacks-vs-cost-of-cyber-security-in-2021/

Gunnes, Tone. (2021). Digital sikkerhetskultur i samfunnskritiske funksjoner – en studie av hva som kjennetegner digital sikkerhetskultur innen finans-, kraft- og justissektoren. [Masteroppgave, Nord Universitet]. Nord Open Research. Archive: https://nord.instructure.com/courses/19190/pages/doktorgradsavhandlinger-og-masteroppgaver?module_item_id=236706

IBM (2022, juli). Cost of Data Breach Report 2022. https://www.ibm.com/resources/cost-data-breach-report-2022

Jacobsen, Dag Ingvar. & Thorsvik, Jan. (2016). Hvordan organisasjoner fungerer. (4. utgave og opplag). Oslo: Fagbokforlaget

Johannessen, Asbjørn., Christoffersen, Line., & Tufte, Per Arne. (2011). Forskningsmetode for økonomiske-administrative fag (3. utgave). Abstrakt forlag.

Kaspersky Labs (2020) IT security Economics 2020: Part 2 – How businesses can minimize the cost of a data breach. Hentet fra: https://www.kaspersky.com/blog/it-security-economics-2020-part-2

Lim, J. S., Chang, S., Maynard, S., & Ahmad, A. (2009). Exploring the Relationship between Organizational Culture and Information Security Culture. DOI: https://doi.org/10.4225/75/57b4065130def

Martin, J. (1992). Cultures in organizations. Three perspectives. New York: Oxford University Press.

Norsk sikkerhetsmyndighet, NSM. (2020, 29. Mai). Veileder i sikkerhetsstyring https://nsm.no/getfile.php/132933-1591350417/Filer/Dokumenter/Veiledere/veileder-i-sikkerhetsstyring.pdf Sandvika: NSM

Norsk sikkerhetsmyndighet, NSM. (2021, 28. oktober). IKT-Risikobilde https://nsm.no/getfile.php/137495-1635323653/Filer/Dokumenter/Rapporter/NSM_IKT-risikobilde_2021_ny_B_enkeltside.pdf

Norsk sikkerhetsmyndighet, NSM. (2022, 11. Februar). Risiko2022. Hentet fra https://nsm.no/getfile.php/1312547-1676548301/NSM/Filer/Dokumenter/Rapporter/Risiko%202023%20-%20Nasjonal%20sikkerhetsmyndighet.pdf

Norsk sikkerhetsmyndighet, NSM. (2023, 13. Februar). Risiko2023 https://nsm.no/regelverk-og-hjelp/rapporter/risiko-2023 NSM

NOU 2015: 13. *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digitalisert verden*. Justis- og beredskapsdepartementet. Hentet fra https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf

Næringslivets sikkerhetshetsråd, NSR, (2020, 7. September). Mørketallsundersøkelsen 2020: Tilfeldigheter viktigste årsak at sikkerhetsbrudd oppstår.

Næringslivets sikkerhetsråd, NSR, (2022, 20. september). Mørketallsundersøkelsen 2022

https://www.nsr-org.no/aktuelt/morketallsundersokelsen-2022-er-na-tilgjengelig

Nätt, T.H., Heide, C.F. (2021). Datasikkerhet: Ikke bli svindlerens neste offer. Oslo: Gyldendal.
Hentet fra: https://web-p-ebscohost-com.ezproxy.nord.no/ehost/ebookviewer/ebook/bmxlYmtfXzMzMjY3ODBfX0FO0?sid=19eb66b0-6d03-48a5-97e0-ccaf7dee9945@redis&vid=0&format=EB&rid=1

Parenty, Thomas J., Domet, Jackj J. (2020) A leader's guide to Cybersecurity, Why boards need to lead- and how to do it. Boston, MA: Harvard Business Review Press

Pettersen, Thomas. (2021). Persepsjon og håndtering av cyberrisiko i små og mellomstore virksomheter. [Masteroppgave, Nord Universitet]. Nord Open Research. Archive. https://nordopen.nord.no/nord-xmlui/bitstream/handle/11250/2788431/Petersen.pdf?sequence=1&isAllowed=y

Reason, J. (1997). Managing the Risks of Organizational Accidents. Aldershot: Ashgate
Hentet fra: https://ebookcentral-proquest-com.ezproxy.nord.no/lib/nord/reader.action?docID=4387688

Rinaldi, A. (6. Mars 2023) The Cost of Cybersecurity and How to Budget it. Business.com. Hentet fra: https://www.business.com/articles/smb-budget-for-cybersecurity/

Schein, E.H., Schein, P. (2017). Organizational culture and leadership, kapittel 4 og 12. New Jersey: John Wiley & Sons, Inc.

Strand, Tormod. Gundersen, M. Mjaaland, O. (2020, 10. Desember) Stortinget ikke alene: Massivt hackerangrep mot Norge. Hentet fra: https://www.nrk.no/norge/stortinget-ikke-alene_-massivt-hackerangrep-mot-norge-1.15277734

Telenor. (u.å). Hva er cyberangrep. Hentet 5. April 2023 fra https://www.telenor.no/sikkerhet/cyberangrep/

Wernersen, C. (2020, 9. September) Ti store dataangrep: Måtte rive ut ledninger til 22.000 datamaskiner. Hentet fra: https://www.nrk.no/urix/ti-store-datangrep_-norge-var-blant-landene-som-ble-rammet-av-lospengeviruset-petya-1.15144202

Wilberg, Erik. (2023). Strategiboken: Alt du behøver å vite for ledere og styremedlemmer. Oslo: Hegnar Media AS

Wiley, A., McCormac, A. & Calic, D. (2019). More than the individual: Examining the relationship between culture and Information Security Awareness. Elsevier, Computers & Security volume 88, January 2020. https://doi.org/10.1016/j.cose.2019.101640

Wold, A.L (2022). Hvordan er sikkerhetskulturen i norske virksomheter, og hvordan prioriteres tiltak og investeringer for å hindre cyberangrep? [Upublisert semeteroppgave i Anvendt Metode]. Nord Universitet.

UCLA (u.å) Statistical Consulting Group. Hentet 22. Mai 2023 fra https://stats.oarc.ucla.edu/spss/faq/what-does-cronbachs-alpha-mean/

Nettskjema

Vedlegg 1 - Spørreundersøkelse

Digital sikkerhetskultur i norske virksomheter

Spørreundersøkelse om digital sikkerhetskultur i store norske virksomheter.

Spørreundersøkelsen er en del av en masteroppgave i MBA-studiet ved Nord Universitet.

Bakgrunn:
I de siste årene har det vært en økning av cyberoperasjoner og dataangrep både mot internasjonale- og norske virksomheter.
Nasjonal sikkerhetsmyndighet påpekte i sin sikkerhetrapport "**Risiko 2022**" at gapet mellom trusselen og sikkerhetsnivået i norske virksomheter og samfunnsfunksjoner øker. Det skyldes blant annet at bevisstheten og kompetansen om trussel- og risikobildet og hva som utgjør god nok sikkerhet, er for svak.
Sikkerhetstiltakene er ikke dimensjonert for det reelle trusselbildet eller innføres ikke raskt nok når nye sårbarheter oppstår. Forståelsen for trussel- og risikobildet må økes og tiltak må iverksettes nå.
Hensikt:
Hensikten med undersøkelsen er å undersøke i hvilken grad ledere i store norske virksomheter har innført sikkerhetskultur i virksomheten, og hvordan prioriteres tiltak og investeringer i sikkerhetsteknologi og kompetanse for å minske risikoen for å bli utsatt for cyberoperasjoner.
Personvern:
Spørreundersøkelsen er helt anonym og vil ikke samle inn eller lagre personopplysninger som kan spores tilbake til deg som respondent eller ditt firma.
Spørreundersøkelsen vil være innom temaer som sikkerhetsledelse og -kultur, økonomi og måleparmetere for sikkerhetsnivå.

1. Er dette temaet relevant for din virksomhet?

Ta stilling til bakgrunnen i introduksjonen.

- Ja
- Delvis
- Nei
- Vet ikke

2. Hvilken stilling har du?

- Chief Executive Officer | CEO
- Chief Operating Officer | COO
- Chief Financial Officer | CFO
- Cheif Information Officer | CIO
- Chief Technical Officer | CTO
- Chief Information Security Officer | CISO
- Chief Marketing Officer | CMO
- Chief Human Resource Officer | CHRO
- Annet

3. Hvor mange ansatte er det i virksomheten?

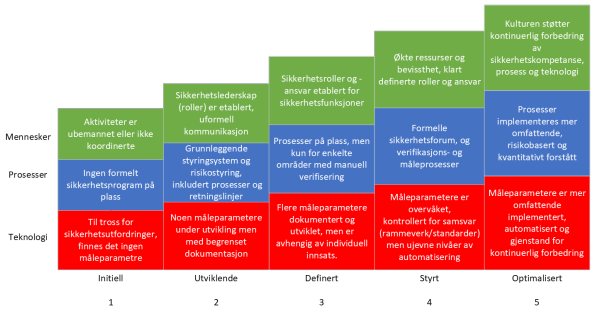
- 0 - 249
- 250 - 499
- 500 - 749

Nettskjema

750 - 999
1000 - 1249
1250 - 1499
1500 - 1749
1750 - 1999
Over 2000
Vet ikke

4. I hvilken grad er virksomheten avhengig av IT-systemer for å opprettholde den daglige driften?

I svært stor grad
I stor grad
I noen grad
I svært liten grad
I liten grad
Vet ikke



5. I hvilken grad har virksomheten innført digital sikkerhetskultur som en del av organisasjonskulturen??

I bildet ovenfor en en tabell som viser hvilken modenhetsgrad en virksomhet har i forhold til cybersikkerhet og sikkerhetskultur.
1 - **Det laveste nivået** hvor svært få tiltak innen cybersikkerhet og digital sikkerhetskultur er tilstede.

Eksempel: Lite sikkerhetsteknologi for å beskytte digital infrastruktur, ingen formelle prosesser og styringssystemer for sikkerhet og kultur er tilstede.
5 - **Det høyeste nivået** hvor tiltak innen cybersikkerhet og digital sikkerhetskultur er optimalisert og forbedringer skjer kontinuerlig.

Eksempel: Virksomheten har innført styringssystemer og rammeverk for cybersikkerhet og digital sikkerhetkultur. Virksomheten har egne ansatt eller avdelinger som håndtere cybersikkerhet og digital sikkerhetskultur.
Prosesser er automatiserte. Alle ansatte uavhengig av nivå i virksomheten har/får stadig påfyll av kompetanse innen cybersikkerhet. Ledelsen mottar statusrapporter eller tilsvarende om innførte tiltak innen sikkerhetskultur eller digital sikkerhetsteknologi.

Svar på spørsmålet med utgangspunkt i bildet ovenfor, og ranger din virksomhet på en skala fra **LAV 1 - 5 HØY**

Vet ikke

1
2
3
4
5

6. I hvilken grad er sikkerhetsarbeid innen digital sikkerhet/cybersikkerhet forankret i ledelsen?

I svært stor grad
I stor grad
I noen grad
I svært liten grad
I liten grad
Vet ikke

7. Har virksomheten innført et styringssystem/rammeverk for digital sikkerhet/cybersikkerhet?

Eksempler på styringsystem og rammerverk innen digital sikkerhet/cybersikkerhet:

NSMs Grunnprinsipper for IKT-sikkerhet 2.0
NIST rammeverk
CIS Controls
ISO/IEC 27001 og 27002
Ja
Nei
Vet ikke
Annet

8. I hvilken grad vil du karakterisere riskoen for at virksomheten kan bli utsatt for cyberangrep?

I svært stor grad
I stor grad
I noen grad
I liten grad
I svært liten grad
Vet ikke

9. I hvilken grad er du enig i følgende påstand: Sikkerhetskultur i virksomheten er et ledelsesansvar

Enig
Delvis enig
Ikke enig
Vet ikke

10. I hvilken grad er du enig i følgende påstand: Virksomheten trenger mer

kompetanse innen digital sikkerhet/cybersikkerhet

- I svært stor grad
- I stor grad
- I middels grad
- I liten grad
- I svært liten grad
- Vet ikke

11. Hvordan prioriterer virksomheten tiltak innen digital sikkerhet/cybersikkerhet for å redusere risikoen for cyberangrep?

Ranger tiltakene i radene nedenfor fra **LAV 1** - **7 HØY**.
Hvor av **1** er **laveste prioritet** og **7** er **høyeste prioritet.**
Tiltak kan ha samme rangeringsverdi.

Sikkerhetsteknologi innen cybersikkerhet

- 1 - lavest prioritet
- 2
- 3
- 4
- 5
- 6
- 7 - høyest prioritet

Økt kompetanse hos de ansatte

- 1 - lavest prioritet
- 2
- 3
- 4
- 5
- 6
- 7 - høyest prioritet

Økt kompetanse i ledelsen eller ledere

- 1 - lavest prioritet
- 2
- 3
- 4
- 5
- 6
- 7 - høyest prioritet

Økt kompetanse hos nøkkelpersonell innen informasjon- og cybersikkerhet

- 1 - lavest prioritet
- 2

3
4
5
6
7 - høyest prioritet

Økt antall ansatte med spesialkompetanse i digital sikkerhet/cybersikkerhet

1 - lavest prioritet
2
3
4
5
6
7 - høyest prioritet

Outsourcing av sikkerhetsarbeid til konsulenter

1 - lavest prioritet
2
3
4
5
6
7 - høyest prioritet

Outsourcing av sikkerhetsarbeid til virksomheter med spesialkompetanse på informasjon- og cybersikkerhet

1 - lavest prioritet
2
3
4
5
6
7 - høyest prioritet

12. Hva var omsetningen til virksomheten i 2022 i kroner?

0 - 299 millioner kroner
300 - 599 millioner kroner
600 - 999 millioner kroner
1 milliard - 1,299 milliarder kroner
1,300 milliarder - 1,599 milliarder kroner
1,600 milliarder - 1,999 millarder kroner
2 milliarder - 2,299 milliarder kroner
2,300 millarder kroner - 2,599 milliarder kroner

Over 2,6 milliarder kroner

Vet ikke

13. Hvor stor andel av virksomhetens omsetning vil du anslå brukes årlig på digital sikkerhet-/cybersikkerhettiltak, angitt i prosent?

0%

1 - 5%

6 - 10%

11 - 15%

16 - 20%

21 - 25%

26 - 30%

31 - 35 %

Over 35%

Vet ikke

14. Hvor stor andel av virksomhetens omsetning vil du anslå virksomheten bruker årlig på kompetanseøkning av ansatte innen digital sikkerhet-/cybersikkerhettiltak

1 - 3%

4 - 6%

7 - 9%

10 - 12%

Over 12%

Vet ikke

15. Har virksomheten vært utsatt for cyberangrep?

Ja

Nei

Vet ikke

15a. Hva vil du anslå dette kostet virksomheten økonomisk? Skriv inn anslått beløp i norske kroner.

Dette elementet vises kun dersom alternativet «Ja » er valgt i spørsmålet «15. Har virksomheten vært utsatt for cyberangrep?»

Eksempel: 10 000 kroner, 100 000 kroner, 10 millioner, 100 millioner.

15b. I hvilken grad var sikkerhetskultur og investeringer i sikkerhetsteknologi implementert før hendelsene?

Dette elementet vises kun dersom alternativet «Ja » er valgt i spørsmålet «15. Har virksomheten vært utsatt for cyberangrep?»

I svært stor grad

I stor grad

I noen grad

I liten grad

I svært liten grad

Vet ikke

16. I hvilken grad er digital sikkerhetskultur en del av virksomhetens strategi?

- I svært stor grad
- I stor grad
- I middels grad
- I liten grad
- I svært liten grad
- Vet ikke

17. I hvilken grad styres investeringer i sikkerhetsteknologi fra ledelsen?

- I svært stor grad
- I stor grad
- I noen grad
- I liten grad
- I svært liten grad
- Vet ikke

18. I hvilken grad styres investeringer i kompetanseutvikling fra ledelsen?

- I svært stor grad
- I stor grad
- I noen grad
- I liten grad
- I svært liten grad
- Vet ikke

19. I hvilken grad har virksomheten delegert ansvaret til egne roller/avdelinger for ivaretakelse av digital- sikkerhetsteknologi og sikkerhetskultur?

- I svært stor grad
- I stor grad
- I noen grad
- I liten grad
- I svært liten grad
- Vet ikke

20. I hvilken grad måler virksomheten effekten av digital sikkerhetskultur i virksomheten?

Med overnevnte menes det om virksomheten har innført målinger av investeringer i den digitale sikkerhetskulturen som omfatter:

- Effekten av sikkerhetsrelatert kommunikasjon i virksomheten
- Effekten av sikkerhetrelatert informasjon innad i virksomheten
- Effekten av sikkerhetsprogram for opplæring av ansatte
- I svært stor grad
- I stor grad
- I noen grad

- I liten grad
- I svært liten grad
- Vet ikke

21. I hvilken grad måler virksomheten effekten av digital sikkerhetsteknologi?

Med overnevnte menes det om virksomheten har innført målinger for om investeringer i digital sikkerhetsteknologi øker sikkerheten mot cyberangrep.

- I svært stor grad
- I stor grad
- I middels grad
- I liten grad
- I svært liten grad
- Vet ikke

22. Hvilke av følgende metoder benyttes for å øke ansatte kompetanse innen digital sikkerhet/cybersikkerhet?

Her kan du **velge flere valg.** Velg de valgene om stemmer overens i din virksomhet.

- Eksterne kurs
- Interne kurs
- Informasjonsmailer
- Informasjon over intranett
- Møter
- Muntlig kommunikasjon
- Annet
- Vet ikke

23. Hvordan måler ledelsen sikkerhetsnivået i virksomheten innen digital sikkerhet/cybersikkerhet i virksomheten?

Her kan du **velge flere valg.** Velg de valgene om stemmer overens i din virksomhet.

- Statusrapporter
- Informasjonsmailer
- Møter
- Muntlig kommunikasjon
- Simuleringer på ansatte
- Årlige eller halvårlige sikkerhetsrapporter
- Annet
- Vet ikke

24. I hvilken grad anser virksomheten at investeringer i sikkerhetsteknologi bidrar til å minske risikoen for cyberangrep?

- I svært stor grad
- I stor grad
- I middels grad
- I liten grad

I svært liten grad
Vet ikke

25. I hvilken grad anser virksomheten at investeringer i økt kompetanse hos personell innen digital sikkerhet bidrar til å minske risikoen for cyberangrep?

I svært stor grad
I stor grad
I middels grad
I liten grad
I svært liten grad
Vet ikke

Vedlegg 2 - Kodebok spørreundersøkelse

1. Er dette temaet relevant for din virksomhet?

var1_tema_virksomhet

3	Ja
4	Delvis
2	Nei
1	Vet ikke

2. Hvilken stilling har du?

var2_stilling

1	Chief Executive Officer | CEO
2	Chief Operating Officer | COO
3	Chief Financial Officer | CFO
4	Cheif Information Officer | CIO
5	Chief Technical Officer | CTO
6	Chief Information Security Officer | CISO
7	Chief Marketing Officer | CMO
8	Chief Human Resource Officer | CHRO
9	Annet

3. Hvor mange ansatte er det i virksomheten?

var3_ansatte

1	0 - 249
2	250 - 499
3	500 - 749
4	750 - 999
5	1000 - 1249
6	1250 - 1499
7	1500 - 1749
8	1750 - 1999
9	Over 2000
10	Vet ikke

4. I hvilken grad er virksomheten avhengig av IT-systemer for å opprettholde den daglige driften?

var4_ITsystemer_daglig

6 I svært stor grad

5 I stor grad

4 I noen grad

3 I svært liten grad

2 I liten grad

1 Vet ikke

5. I hvilken grad har virksomheten innført digital sikkerhetskultur som en del av organisasjonskulturen?

var5_sikkerhetskultur_i_virksomheten

6 Vet ikke

1 1- I svært liten grad

2 2- I liten grad

3 3 - I noen grad

4 4- I Stor grad

5 5- I svært stor grad

6. I hvilken grad er sikkerhetsarbeid innen digital sikkerhet/cybersikkerhet forankret i ledelsen?

var6_sikkerhet_forankret_i_ledelsen

6 I svært stor grad

5 I stor grad

4 I noen grad

3 I svært liten grad

2 I liten grad

1 Vet ikke

7. Har virksomheten innført et styringssystem/rammeverk for digital sikkerhet/cybersikkerhet?

var7_styringsystem_i_virksomheten

4 Ja

2 Nei

3 Vet ikke

1 Annet

8. I hvilken grad vil du karakterisere riskoen for at virksomheten kan bli utsatt for cyberangrep?

var8_risiko

6 I svært stor grad

5 I stor grad

4 I noen grad

3 I liten grad

2 I svært liten grad

1 Vet ikke

9. I hvilken grad er du enig i følgende påstand: Sikkerhetskultur i virksomheten er et ledelsesansvar

var9_sikkultur_ledelsesansvar

5 Enig

4 Delvis enig

3 Ikke enig

1 Vet ikke

10. I hvilken grad er du enig i følgende påstand: Virksomheten trenger mer kompetanse innen digital sikkerhet/cybersikkerhet

var10_virk_Okkompetanse_digital

6 I svært stor grad

5 I stor grad

4 I middels grad

3 I liten grad

2 I svært liten grad

1 Vet ikke

11. Hvordan prioriterer virksomheten tiltak innen digital sikkerhet/cybersikkerhet for å redusere risikoen for cyberangrep?

var11_Siktek Sikkerhetsteknologi innen cybersikkerhet

1 1 - lavest prioritet

2 2

3 3

4 4

5 5

6 6

7 7 - høyest prioritet

var12_oKompansatte Økt kompetanse hos de ansatte

var13_oKompledelse Økt kompetanse i ledelsen eller ledere

var14_oKompnokkel Økt kompetanse hos nøkkelpersonell innen informasjon- og cybersikkerhet

var15_oAntallAnsNok Økt antall ansatte med spesialkompetanse i digital sikkerhet/cybersikkerhet

var16_OutSikkarbeid Outsourcing av sikkerhetsarbeid til konsulenter

var17_OutSikkerarbeid_virksom Outsourcing av sikkerhetsarbeid til virksomheter med spesialkompetanse på informasjon- og cybersikkerhet

12. Hva var omsetningen til virksomheten i 2022 i kroner?

var18_Omset2022

1 0 - 299 millioner kroner

2 300 - 599 millioner kroner

3 600 - 999 millioner kroner

4 1 milliard - 1,299 milliarder kroner

5 1,300 milliarder - 1,599 milliarder kroner

6 1,600 milliarder - 1,999 millarder kroner

7 2 milliarder - 2,299 milliarder kroner

8 2,300 millarder kroner - 2,599 milliarder kroner

9 Over 2,6 milliarder kroner

10 Vet ikke

13. Hvor stor andel av virksomhetens omsetning vil du anslå brukes årlig på digital sikkerhet-/cybersikkerhettiltak, angitt i prosent?

var19_AndelOmsDigSik

1 0%

2 1 - 5%

3 6 - 10%

4 11 - 15%

5 16 - 20%

6 21 - 25%

7 26 - 30%

8 31 - 35 %

9 Over 35%

10 Vet ikke

14. Hvor stor andel av virksomhetens omsetning vil du anslå virksomheten bruker årlig på kompetanseøkning av ansatte innen digital sikkerhet-/cybersikkerhettiltak

var20_AndelOmsKompet

1 1 - 3%

2 4 - 6%

3 7 - 9%

4 10 - 12%

5 Over 12%

6 Vet ikke

15. Har virksomheten vært utsatt for cyberangrep?

var21_utCyberangrep

3 Ja

2 Nei

1 Vet ikke

15a. Hva vil du anslå dette kostet virksomheten økonomisk? Skriv inn anslått beløp i norske kroner.

var22_kostCyberangrep

Fritekst

15b. I hvilken grad var sikkerhetskultur og investeringer i sikkerhetsteknologi implementert før hendelsene?

var23_sikInvestcyberangrep

6 I svært stor grad

5 I stor grad

4 I noen grad

3 I liten grad

2 I svært liten grad

1 Vet ikke

16. I hvilken grad er digital sikkerhetskultur en del av virksomhetens strategi?

var24_DigSikstrategi

6 I svært stor grad

5 I stor grad

4 I middels grad

3 I liten grad

2 I svært liten grad

1 Vet ikke

17. I hvilken grad styres investeringer i sikkerhetsteknologi fra ledelsen?

var25_styrInvestSikLed

6 I svært stor grad

5 I stor grad

4 I noen grad

3 I liten grad

2 I svært liten grad

1 Vet ikke

18. I hvilken grad styres investeringer i kompetanseutvikling fra ledelsen?

var26_styrInvestKompLed

6 I svært stor grad

5 I stor grad

4 I noen grad

3 I liten grad

2 I svært liten grad

1 Vet ikke

19. I hvilken grad har virksomheten delegert ansvaret til egne roller/avdelinger for ivaretakelse av digital- sikkerhetsteknologi og sikkerhetskultur?

var33_virkDelAnsRollerAvd

6 I svært stor grad

5 I stor grad

4 I noen grad

3 I liten grad

2 I svært liten grad

1 Vet ikke

20. I hvilken grad måler virksomheten effekten av digital sikkerhetskultur i virksomheten?

var27_malEffSikkultur

6 I svært stor grad

5 I stor grad

4 I noen grad

3 I liten grad

2 I svært liten grad

1 Vet ikke

21. I hvilken grad måler virksomheten effekten av digital sikkerhetsteknologi?

var28_malEffDigsiktek

6 I svært stor grad

5 I stor grad

4 I middels grad

3 I liten grad

2 I svært liten grad

1 Vet ikke

22. Hvilke av følgende metoder benyttes for å øke ansatte kompetanse innen digital sikkerhet/cybersikkerhet?

var29_metOkKompsAns

1 Eksterne kurs

2 Interne kurs

3 Informasjonsmailer

8 Informasjon over intranett

4 Møter

5 Muntlig kommunikasjon

6 Annet

7 Vet ikke

23. Hvordan måler ledelsen sikkerhetsnivået i virksomheten innen digital sikkerhet/cybersikkerhet i virksomheten?

var30_malSiknivaCybsec

1 Statusrapporter

2 Informasjonsmailer

3 Møter

4 Muntlig kommunikasjon

5 Simuleringer på ansatte

6 Årlige eller halvårlige sikkerhetsrapporter

7 Annet

8 Vet ikke

24. I hvilken grad anser virksomheten at investeringer i sikkerhetsteknologi bidrar til å minske risikoen for cyberangrep?

var31_virkInvestSiktekRisk

6 I svært stor grad

5 I stor grad

4 I middels grad

3 I liten grad

2 I svært liten grad

1 Vet ikke

25. I hvilken grad anser virksomheten at investeringer i økt kompetanse hos personell innen digital sikkerhet bidrar til å minske risikoen for cyberangrep?

var32_virkInvestOkompDig

6 I svært stor grad

5 I stor grad

4 I middels grad

3 I liten grad

2 I svært liten grad

1 Vet ikke