MASTEROPPGAVE

Emnekode: BE304E

Navn: Camilla F. Christoffersen, Jakob S. Grønmo og Karianne P. Sunde

Kampen mot skjulte fiender

Dato: 23.05.2023

Totalt antall sider: 115

NORD universitet

www.nord.no

Forord

Forskningsprosjektet har blitt gjennomført som en avslutning av våre masterstudier i "Master of Science in Business" ved Nord universitet. Masteroppgaven er en del av prosjektet "Transformative capabilities of the accounting profession: Study of Norwegian small and medium accounting practices.[1]Masteroppgaven gir et dypere innblikk i små og mellomstore bedrifters (SMB) håndtering av cybertrusler.

Vi ønsker å rette en stor takk til alle som har bidratt i forskningsprosjektet. Særlig til våre informanter og case-bedrifter, som har tatt seg tid til å delta i forskningsprosjektet. Takk for deres raushet til å dele deres praksiser forbundet med cybersikkerhet. Dere bidrar med verdifull kunnskap til forskningsfeltet.

En ekstra takk til vår veileder Anatoli Bourmistrov og biveileder Silje Aakre for kontinuerlig oppfølging og konstruktive tilbakemeldinger. Det har bidratt til å styrke det teoretiske og heve forskningsprosjektets akademiske nivå.

Prosjektet har vært utfordrende, men fremfor alt både spennende og lærerikt. Vi har tilegnet oss masse nyttig kunnskap innenfor et aktuelt og krevende fagfelt. Dette er kompetanse vi ikke ville vært foruten, og som vi tar med oss videre.

Bodø, 23. mai 2023

Camilla F. Christoffersen — Camilla Fleines Christoffersen

Jakob S Grønmo — Jakob Severinsen Grønmo

Karianne P. Sunde — Karianne Pettersen Sunde

[1] TRANSACT-prosjektet finansieres av Norges forskningsråd (NFR), prosjektnummer 301717 www.nord.no/transact.

Sammendrag
Masteroppgavens formål er å få kunnskap om små og mellomstore bedrifter sin håndtering av cybertrusler. Tidligere litteratur og egen forskning vil videre benyttes for å besvare følgende problemstilling: *"Hvordan bruker små og mellomstore bedrifter sine styringssystemer for å håndtere cybertrusler?"*

Vi har gjennom forskningen belyst tre hovedaspekter innenfor cybersikkerhet; styringssystemer, håndtering og tiltak. På bakgrunn av deres sårbarhet knyttet til kunnskapsmangel og utilstrekkelige ressurser når det gjelder håndtering av cybertrusler (Skotnes, 2017) studerer vi fire små og mellomstore bedrifter (SMB). I tillegg utgjør SMBer 99 % av bedriftene i Norge (NHO, i.d). For å skape et bredt perspektiv representerer case-bedriftene ulike bransjer og geografiske områder. Dette bidrar til å styrke forskningens relevans for flere deler av næringslivet.

Forskningen viser at små og mellomstore bedrifter stort sett håndterer cybertrusler gjennom tjenesteutsettelse. Det er kombinasjonen av fagfeltets kompleksitet og utfordringer knyttet til å anskaffe riktig kompetanse som gjør at bedriftene velger denne løsningen. En kombinasjon av tjenesteutsetting og intern IT kompetanse skaper en proaktiv tilnærming, som ikke svekker kunnskapen internt i bedriften. Praktisering av IT-kompetanse internt bidrar til en sikkerhetskultur med større fokus på cybersikkerhet, og tilrettelegger for økt interaksjon. Opplæring av ansatte er en utslagsgivende faktor i håndtering av cybertrusler. Ledelsen trenger å styrke internkontrollen gjennom kartlegging av ansattes risikoappetitt, individuelle vurderinger og oppfatning av risiko. En kombinasjon av e-læring og personlig kontakt styrker opplæringen og former ansattes atferdsmønster.

Under forskningsprosjektet har vi gjennomført dybdeintervju med fire case-bedrifter, fire ekspertintervju og ett prøveintervju. For å avdekke ansattes perspektiv har vi sendt ut spørreundersøkelser til case-bedriftene og tilleggsutvalget Alumni (113 respondenter).

Gjennom forskningen har vi avdekket følgende hovedfunn: (1) Majoriteten av bedriftene tjenesteutsetter cybersikkerheten. (2) Det er ingen tydelig kobling mellom styringssystem og cybersikkerhet. (3) Det er ubalanse mellom styringssystemets «kontrollspaker» internt i bedriftene.

Abstract
The purpose of the master's thesis is to gain knowledge about small and medium-sized companies' handling of cyber threats. Previous literature and own research will also be used to answer the following question: "*How do small and medium-sized companies use their management systems to deal with cyber threats?"*

Through the research, we have highlighted three main aspects of cyber security; management systems, handling, and measures. Based on their vulnerability linked to a lack of knowledge and insufficient resources when it comes to handling cyber threats (Skotnes, 2017), we study four small and medium-sized enterprises (SMEs). In addition, SMEs make up 99% of companies in Norway (NHO, i.d). To create a broad perspective, the case- companies represent different industries and geographical areas. This helps to strengthen the research's relevance for several parts of the business world.

The research shows that small and medium-sized companies mostly deal with cyber threats through outsourcing. It is the combination of the complexity of the field and the challenges associated with acquiring the right skills that make companies choose this solution. A combination of outsourcing and internal IT competence creates a proactive approach, which does not weaken the knowledge internally in the company. Practicing IT competence internally contributes to a security culture with a greater focus on cyber security and facilitates increased interaction. Employee training is a decisive factor in dealing with cyber threats. Management needs to strengthen internal control by mapping employees' risk appetite, individual assessments, and perception of risk. A combination of e-learning and personal contact strengthens the training and shapes employees' behavior patterns.

During the research project, we conducted four in-depth interviews with each case company, four expert interviews, and one test interview. To uncover the employees' perspective, we have sent out surveys to the case companies and the additional Alumni committee (113 respondents).

Through the research, we have uncovered the following main findings: (1) The majority of companies outsource cyber security. (2) There is no clear link between management systems and cyber security. (3) There is an imbalance between the management system's "control levers" within the companies.

Figurliste

Tabell

Grafer

Innholdsfortegnelse

1.0 Innledning

Innledningen presenterer først hvordan digitaliseringen har endret samfunnet, men også skapt nye utfordringer knyttet til cybertrusler. Dette danner grunnlaget for vår problemstilling og motivasjon for oppgaven. I oppgavens bakgrunn presenteres tre sentrale tema for forskningen; cybersikkerhet og cybertrusler, hvordan cybertrusler utgjør en utfordring som små og mellomstore bedrifter og tjenesteutsetting. Deretter går vi gjennom relevant litteratur for oppgavens problemstilling. Basert på eksisterende forskning og kunnskap presenteres oppgavens forskningsspørsmål og avslutningsvis oppgavens struktur.

1.1 Aktualisering

Digitalisering og teknologisk utvikling har skapt store samfunnsendringer. En voksende effektivitet knyttet til prosesser og infrastruktur har vokst frem. Det har gitt oss nye tjenester og revolusjonert måten vi kommuniserer med hverandre (Regjeringen, 2015 s.15). Men hva med den mørke siden av digitalisering?

Teknologien har blitt en betydelig pådriver av digitale kriminalitetsutfordringer og trusler (Politiet, 2023, s.3). En av de mest komplekse, tekniske og politiske utfordringene vi møter i den moderne verden er cybersikkerhet (Stevens, 2018 s.1). Trusselen setter store økonomiske investeringer i spill. Globale utgifter knyttet til cybersikkerhet tilsvarer 150 billioner dollar per år (Chertoff, 2023). Parallelt forventes det en økning på 15 prosent per år knyttet til cyberangrep (Morgan, 2020). Et vellykket cyberangrep vil direkte påvirke virksomhetens oppdrag, produksjonsevne, økonomi, og omdømme (Perez, 2020).

På myndighetsnivå oppleves håndtering og regulering av cyberkriminalitet komplisert grunnet fenomenets geografiske omfang. Dagens tilnærming til cyberkriminalitet resulterer i en ineffektiv håndtering av trusselen (Politiet, 2023 s.7). Dette skyldes begrenset lovgivning på tvers av landegrenser, som gjør at cyberkriminelle opplever en lav oppdagelsesrisiko (Politiet, 2023 s.7). Arenaen for cyberkriminalitet gir de kriminelle anonymitet, skaper forbindelser og fjerner geografisk avstand. Som et resultat av dette har fenomenet gjort cybersikkerhet til en topp prioritet på den sikkerhetspolitiske agendaen (Dysvik, 2021 s. V).

Norge er et digitalisert samfunn (Politiet, 2023 s.6). Nordmenns bruk av informasjons- og kommunikasjonsteknologi (IKT) og digitale tjenester ligger i verdenstoppen (Regjeringen, 2021 s.16). Til tross for dette er den nasjonale sikkerhetstenkingen umoden. Den tillater kriminelle å utnytte Norges digitale sårbarhetsflate (Politiet, 2023 s. 13). Fra 2019 til 2021 observeres en tredobling av alvorlige cyberoperasjoner rettet mot norske myndigheter og virksomheter (NSM, 2023 s.18). Først og fremst er det små og mellomstore bedrifter som blir angrepet i dag (Myrvold, 2022). I norsk sammenheng faller 99 prosent av virksomhetene innenfor kategorien SMB (NHO, i.d).

Små og mellomstore bedrifter (SMB) antar at det er lav risiko for at de rammes av cyberangrep, mens i realiteten er de målrettede ofre (Skotnes, 2017). Fremover forventes det en økning i vellykkede cyberangrep mot SMBer, ettersom flere av dem ikke har kompetansen og ressursene til å beskytte seg selv (Politiet, 2023, s. 47). Mangelen på ekspertise internt resulterer i at bedriftene søker tjenesteutsetting eksternt. Likevel ser det ut som at intern kompetanse er særlig viktig som et tiltak for å håndtere cybersikkerhet (Wilson et.al, 2022 s. 398). De kriminelle er klar over SMBers sårbarheter, og utnytter dette (Myrvold, 2022).

Gordon et al. (2008) insisterer på at rett utforming og bruk av styringssystemer kan ha en effektiv påvirkning for å motvirke cyberangrep. Samtidig skaper ressursmangel problemer for SMBers muligheter til å etablere gode styringssystemer, som også tar for seg cybersikkerhet (Politiet, 2023 s.47).

1.1.1 Problemstilling

Ut fra aktualiseringen er det utarbeidet følgende problemstilling:

"*Hvordan bruker små og mellomstore bedrifter sine styringssystemer for å håndtere cybertrusler?"*

Problemstillingen inkluderer styringssystemer, hvor vi tar utgangspunkt i kontrollspakene i rammeverket Four Levers of Control (Simons, 1995). Tilnærmingen bidrar til kartlegging av hvorvidt små og mellomstore bedrifter benytter kontrollspakene i håndtering av cybertrusler.

1.1.2 Valg av tema og motivasjon

Formålet med oppgaven er å forske på hvordan små og mellomstore bedrifter bruker sine styringssystemer for å håndtere cybertrusler. Vi studerer fire bedrifter som har blitt utsatt for cybertrusler i ulik grad. Ved å avdekke nødvendige suksessfaktorer i håndteringen, vil forskningen kunne bidra til mer robuste og kunnskapsrike SMBer i fremtiden.

I Norge representerer SMBer en stor del av næringslivet. Hele 99 prosent av bedriftene i Norge er kategorisert innenfor dette (NHO, i.d). SMBene anser ikke seg selv som sårbare for cyberangrep, mens i realiteten er de målrettede ofre. Sårbarheten skyldes mangel på økonomiske ressurser, men også lite kunnskap om cybersikkerhet. De kriminelle er også klar over mangelen på ressurser hos SMB, og vil derfor utnytte dette for å lykkes i angrepene (Myrvold, 2022).

Motivasjonen for å velge styringssystemer og cybersikkerhet baseres på en rekke ulike faktorer. For det første ønsker vi å forske på et tema som er både interessant og aktuelt. Vi ønsker å kunne bidra med forskningskunnskap som vil forbedre samfunnet på sikt. Cybersikkerhet og cyberkriminalitet er temaer i rivende utvikling, og det oppdages stadig nye kunnskapshull. Dessuten opplever vi mangel på forskning på SMB når det gjelder dette fenomenet. Det er stor risiko for å bli utsatt, som kan medføre fatale konsekvenser som påvirker både jobb og privatliv. Vi opplever at temaet er tabu å snakke åpent om, og noe folk flest ikke har mye kunnskap om. Målet er å øke kunnskapen, bryte tabuer og avdekke bedriftens strategier og håndtering av cybertrusler. Motivasjon kommer dermed fra temaets viktighet, og et ønske om å kunne tilføre nyttig kunnskap.

1.2 Bakgrunn

Bakgrunnen presenterer sentrale tema for oppgaven. Kapittelet innledes med en innføring i cybersikkerhet og cybertrusler. Videre rettes fokuset mot små og mellomstore bedrifter og deres utfordringer knyttet til håndtering av cybertrusler. Avslutningsvis går vi nærmere innpå tjenesteutsettelse som en strategi.

1.2.1 Cybertrusler

Internett har ekspandert og gitt både privatpersoner, bedrifter og kriminelle nye muligheter. Som brukere opplever vi at den virtuelle og fysiske verden går i ett, og dette har skapt økt bekymring for de potensielle konsekvensene (Langø & Sandvik, 2013). Den teknologiske utviklingen går hyppigere, den effektiviserer hverdagen, men parallelt øker den digitale sårbarhetsflaten (NSM, 2023 s.9). En konsekvens av den raske utviklingen innenfor teknologien er behovet for å beskytte seg mot cybertrusler. Nasjonal sikkerhetsmyndighet (NSM, 2023, s. 18) rapporterer at det har vært en tredobling i alvorlige cyberoperasjoner i tidsrommet 2019 til 2021. Lite kunnskap om cybersikkerhet blant de ansatte og ledelsen har blitt utnyttet for cyberoperasjoner mot norske virksomheter. Politiet (2023) peker mot flere utbredte metoder og varianter av sosial manipulasjon, phishing og påloggingsforsøk (Politiet, 2023). I fremtiden påpekes det et stort potensial innenfor den kunstige intelligensen for bedrifter. Men det kan ikke utelukkes at dette vil bli utnyttet av ondsinnede aktører (Bjørkeng, 2023).

1.2.2 Små og mellomstore bedrifters utfordringer knyttet til håndtering av cybertrusler

Forskning viser at SMB ikke installerer robuste sikkerhetstiltak som skal gå mot trusler. Resultatet av dette er at de kriminelle får en tiltrekning mot SMB, og danner hovedgrunnlaget for småbedriftssvikt (Ruaju & Verhaart, i.d). De større selskapene har dermed flere ressurser og mer avanserte systemer for å oppdage og forhindre angrep. Hackere bruker derfor de små og mellomstore bedriftene for å få tilgang til de større bedriftene (Skotnes, 2017). Dette understreker viktigheten av å adressere små og mellomstore bedrifter, siden de kan undervurdere rollen sin i denne konteksten. En trenger mer kunnskap om de er forberedt, forstår og praktiserer faget.

For små og mellomstore bedrifter skapes utfordringer grunnet mangel på kunnskap, ressurser og ekspertise (Wilson et al., 2022, s.398). Kombinert med optimistiske risikovurderinger, resulterer det i at ledelsen gjerne flytter ansvaret til informasjonsteknologisk avdelingen (IT–avdeling), eller benytter tjenesteutsettelse som løsning (Lorentzen, 2021, s.51). Skotnes (2017) mener at små og mellomstore bedrifter selv anser det som lav sannsynlighet for at de rammes av cyberangrep. SMBene viser til tendenser, hvor de føler seg immune eller sikre mot ondsinnede angrep (Batista, 2021). Mens på den andre siden viser realiteten det motsatte.

Små bedrifter opererer med mindre sofistikerte sikkerhetssystemer, og brukes som en brikke for å hacke større bedrifter (Batista, 2021). Mange av SMBene er ikke forberedt på å håndtere et angrep (Batista, 2021). Dette underbygges av Johanson (2019) som opplyser at 60 % av små selskaper som har vært utsatt for et cyberangrep eller datainnbrudd går konkurs innen seks måneder.

Det menneskelige aspektet opp mot individets holdninger er viktig innenfor cybersikkerhet. En gjentagende utfordring for SMB er fornektelse av muligheten for cyberangrep (Wilson et. al, 2022, s.398). Det foreligger bagatellisering av bedriftens dataressurser som at det er lite verdt, og konkludering med at virkningen av et angrep er minimal. Dette kan skyldes en indre kognitiv konflikt mellom atferd og kunnskap (Wilson et.al, 2022 s. 398). Dette resulterer i at en distraherer seg fra problemet, siden tanken på cybertrusler skaper en negativ effekt. Dessuten er det utfordrende å bringe atferd og holdninger i samsvar, spesielt i lys av cybersikkerhet (Wilson et.al, 2022 s. 398). På en annen side viser forskning på SMB og deres persepsjon av cyberrisiko høy bevissthet rundt trusselen. Knyttet opp mot et ønske om mer kunnskap og erfaring fra tidligere. Men det er ikke samvariasjon mellom deres persepsjon og tiltak som blir innført (Petersen, 2021). I denne sammenheng er mangelen på kunnskap og forståelse en tydelig barriere.

Undersøkelser tyder på at SMB ikke tar cybertrusler på alvor. En undersøkelse viser at 52% av deltakerne mente at cyberkriminalitet var av liten risiko (Wilson et.al, 2022 s. 397). Dette støttes av en undersøkelse hvor de forsket på 370 små bedrifters tilnærming opp mot risikostyring og cybertrusler. Funnene viste at kun 6,5% hadde skriftlige sikkerhetsprosedyrer (Berry & Berry, 2018). Videre fant undersøkelsen at 74% bruker sikkerhetsbeskyttelse i form av antivirus. Men dette var mindre enn halvparten som holdt tritt med utviklingen (Berry & Berry, 2018). I norsk sammenheng, så støttes dette av Nasjonalsikkerhetsmyndighet sin rapport for "Risiko 2023". Det er fortsatt mange norske bedrifter som ikke oppdaterer sine system, til tross for at det er kjente sårbarheter (NSM, 2023 s.19). Kostnader knyttet til opprettholdelse av cybersikkerheten er en utfordring. De mangler også som regel ekspertise internt, og vil da søke eksternt til tjenesteutsetting. Likevel ser det ut som at intern kompetanse er viktig i vellykkede tiltak (Wilson et.al, 2022 s. 398).

1.2.3 Tjenesteutsettelse

SMB møter samme cybertrusler som større organisasjoner, men har ikke tilsvarende ressurser til å håndtere risikoen (Horn, 2017). Dette resulterer i tjenesteutsetting som innebærer at en annen virksomhet tar over arbeidsoppgaver som bedriften tidligere selv har stått for (VISMA, i.d). Flere bedrifter vil benytte seg av slike tjenester for å redusere kostnader og få fokus på andre ting i bedriften (Polizzo, 2023). Dette gir SMBene muligheten til å fokusere på bedriftens fagfelt og kjerneverdier, og heller tjenesteutsette aktiviteter som ikke inngår i det (Polizzo, 2023). Det er ofte enklere for bedriftene å bruke et firma som er spesialisert på fagfeltet enn å ansette. Hvis man benytter en ekstern leverandør slipper man kostnad knyttet til personalkostnader (Eliassen og Korneliussen, 2018).

Selv om det er mye positivt med tjenesteutsetting så foreligger det naturlig nok negative konsekvenser. Noen ulemper er at virksomhetene kan miste kontroll over bedriften og at en undervurderer den faktiske kostnaden med det. Det er utfordrende om en vil gå fra tjenesteutsetting til tjenesteinnsetting (å ansette en fast i bedriften for å gjøre jobben som før ble gjort utenfor bedriften) (Deloitte, 2016). Grunnet formalisering og underleggelse av strengere prosedyrer enn ved å ha en egen ansatt i selskapet (Deloitte, 2016). Det trekkes også frem bevis som tyder på at eksterne leverandører ikke klarer å gi den tilpassede omsorg som et dedikert internt team kan gi (Benz & Chatterjee, 2020).

1.2.4 Manglende kunnskap og avgrensning av forskningsfelt

Det er tydelige behov for videre forskning på feltet på bakgrunn av cyberkriminalitens hyppige utvikling (Dysvik, 2021 s.100). På bakgrunn av at det er mange forslag til videre forskning, trekker vi kun frem noen. Det er mange hull i litteraturen når det gjelder identifisering, risiko, behandling og den generelle håndteringen av cyberrisiko (Eling et.al, 2021). Tidligere studier nevner undersøkelsesbasert forskning for å skape en mer generell forståelse som et gap i litteraturen. Det påpekes et behov for å studere den overordnede forståelsen av fenomenet og dens alvorlighetsgrad (Eling et.al, 2021). Vi ønsker å forske på deler av dette, gjennom en spørreundersøkelse for å skape en dypere forståelse av de ansattes oppfatning av risiko og cybersikkerhet.

Videre oppfordres det til forskning på risikostyring og metoder innen risikoanalyse. Det etterlyses forskning på prosess og rammeverk, hvor man tar for seg toppledelsens beslutningstaking og selskapsstyring (Eling et.al, 2021). For å svare på forskningsspørsmålet vårt vil vi imidlertid vurdere styringssystemer, ledelse og beslutningstaking. For å skape et mer nyansert syn inkludere de ansatte.

Det er utført mye forskning på risikostyring, framsyn og cybersikkerhet hver for seg. Men det er behov for å beskrive og analysere beste praksis (Bourmistrov & Aakre, 2020, s.61). Dette oppfyller vår oppgave, da vi ønsker å se hvordan SMBene bruker styringssystemene for å håndtere cybertrusler. Vi vil derfor dekke en kombinasjon av hull i litteraturen. Ved at vi inkluderer prosesser rundt bedriftens strategier, ledelse beslutninger.

1.3 Forskningsspørsmål

På bakgrunn av problemstillingen utformes tre ulike forskningsspørsmål. Disse ser nærmere på sentrale elementer innenfor besvarelse av problemstillingen. Deriblant små og mellomstore bedrifters utfordringer, strategier og styringssystemer opp mot cybertrusler.

- FS1: Hvordan er cybertrusler utfordrende for små og mellomstore bedrifter?
- FS2: Hvilke tiltak eller strategi bruker små og mellomstore bedrifter til å håndtere cybertrusler?
- FS3: Hvordan brukes styringssystemer til å håndtere cybertrusler?

1.4 Oppgavens struktur

Innledningsvis i kapittel 1 redegjøres det for en aktualisering av oppgaven og videre presentasjon av oppgavens problemstilling. Deretter refleksjoner knyttet til valg av tema begrunnet med motivasjon. Videre presenteres bakgrunnen med fokus på cybertruslers utfordringer for SMB og tjenesteutsetting som strategi. Avslutter kapittel 1 med gjennomgang avgrensning av forskningsfeltet, forskningsspørsmål og oppgavens struktur. Kapittel 2 tar for seg oppgavens teori, og oppgavens teoretiske rammeverk. Kapittel 3 presenterer metoden og våre valg gjennom forskningsprosessen. I form av datainnsamlingsprosess, rekruttering, intervjuguide, utvalg og analyse av data. Kapittel 4 tar for seg funn, hvor vi strukturerer empirien ut fra vårt teoretiske rammeverk.

Videre presenteres bedriftens erfaring og håndtering av cybertrusler. Vi trekker frem og diskuterer tjenesteutsettelse som strategi og i lys av cybersikkerhet. Videre belyses utfordringer med cybersikkerhet og tiltak for fremtiden. Kapittelet avsluttes med statistikk fra spørreundersøkelsen med tilleggsutvalget Alumni. Kapittel 5 innebærer diskusjon av funnene og teorien opp mot forskningsspørsmålene. Kapittel 6 er konklusjonen på problemstillingen.

2.0 Teori og teoretisk rammeverk

I dette kapittelet skal oppgavens teoretiske grunnlag belyses. Teorier som presenteres omhandler ulike forhold som kan ha betydning når det gjelder håndtering av cybersikkerhet. Sentralt i oppgaven er fokuset på bedriftenes styringssystemer og det menneskelige aspektet. Dermed vil teorier som omhandler atferd, forståelse av risiko, internkontroll, beslutningstaking og overvurdering av egne evner vektlegges. Videre en redegjørelse av det kontrollspakene innenfor rammeverket for oppgaven. Rammeverket bidrar med utforming av oppgaven, og peker mot nyttige elementer i håndtering av cybertrusler.

2.1 Økonomistyring

Økonomistyring er styring av organisasjonens ressurser og tilrettelegge for målene som er satt (Winther, Øyen & Ottesen, 2006). Økonomistyringen reflekterer viktigheten rundt strategiske spørsmål, men også operasjonelle problemer. Det omhandler organisasjonens holdninger og implementering av planer opp mot mål (Emmanuel & Otley, s.6), men det er også selve prosessen hvor ledere sikrer ressurser og bruker disse effektivt for å oppnå sine mål (Anthony, 1965). For SMBene vektlegges ikke cybersikkerhet i økonomistyringen. En mulig forklaring er fraværet av sterke insentiver for SMB til å innføre cybersikkerhetstrategier. Kombinert med mangel på kapital for å innføre cybersikkerhetsstrategier, som resulterer i at SMBene har en svak tilnærming til cybertrusler (Perez, 2020 s.3). Noe som er risikofylt på bakgrunn av at økonomistyring skal bistå med utvikling av og opprettholdelse av et levedyktig atferdsmønster (Otley, 1999).

Små og mellomstore bedrifters underskudd på ressurser, arbeidsstyrke og avanserte sikkerhetsverktøy vanskeliggjør bekjempelsen av cybertrusler (Perez, 2020 s. iii). Samtidig vier SMBene ikke noe betydelig budsjett til sikkerhet. Som et resultat er det utfordrende å implementere omfattende cybersikkerhetsstrategier som oppfyller budsjettet (Perez, 2020 s. 9). Det kreves tidlig investering i ressurser, som mulig kan redusere økonomiske tap ved uunngåelige angrep (Corallo, Lazoi, & Lezzi, 2020).

2.1.1 Styringssystemer

Det finnes en rekke ulike definisjoner på styringssystemer, som både overlapper og viker fra hverandre (Malmi & Brown, 2008 s. 288). Definisjonen av styringssystemer har derfor utviklet seg gjennom årene fra et fokus på økonomisk kvantifiserbar informasjon til også et fungerende verktøy for å hjelpe ledelsen å fatte beslutninger (Chenhall, 2003 s. 129).

Formålet med styringssystemer er å gi ledere kontroll på hvorvidt organisatoriske mål oppfylles. Samtidig som det skal balansere effektivitet opp mot de ansattes muligheter og kreativitet (Chenhall, 2003 s. 129). Videre peker Merchant & Otley (2006) mot at formålet er innhenting av nyttig informasjon som skal hjelpe i beslutninger, planlegging og evalueringer (Widener, 2007, s. 1).

Økonomistyringssystemets funksjon i praksis påvirkes av flere faktorer innenfor design, mobilisering, men også organisatorisk atferd (Ingebrigtsen & Lavbakk, 2007 s. 13) Innenfor det økonomiske styringsperspektivet foreligger det et fokus opp mot den atferdsmessige dimensjonen. Busch (2005) begrunner dette basert på målsettingene som må oppnås gjennom de ansatte. Merchant & Van der Stede (2007) trekker frem at styringskontroll er nødvendig for å beskytte seg mot at ansatte gjør noe bedriften ikke ønsker. Det er mennesker innad i bedriftene som får ting til å skje, og hvis lederne hadde hatt tillit til de ansatte, så ville det ikke vært et behov for styringssystemer. Dette støttes av Abernethy & Chua (1996) sin forståelse av styringssystemer peker på at mekanismene er designet for å øke sjansen for at aktørene i bedriften vil oppføre seg i samsvar med målene (Malmi & Brown, 2008 s. 289).

Det atferdsmessige aspektet er sentralt i håndtering av cybertrusler, hvor det oppleves utfordringer knyttet styring av atferden til mennesker. En mulig forklaring er at sikkerhetstiltakene ikke tar riktig hensyn til den menneskelige atferden (Ricci, Breitinger & Baggili, 2019). Det er et behov for cybersikkerhetsstrategier som er hensynsfull mot det menneskelige aspektet. Videre dyrkelse av sikkerhetsfokusert kultur og oppmuntring til god atferd (Perez, 2020 s.27). Gordon et al. (2008) insisterer på at rett utforming og bruk av styringssystemer kan ha en effektiv effekt på å motvirke cyberangrep. Men ressursmangel skaper problemer for SMBers muligheter til å etablere gode styringssystemer som også tar for seg cybersikkerhet (Politiet, 2023 s.47).

SMBenes manglende kapasitet vanskeliggjør å utøve balanse mellom kontroll og muligheter, og fatte komplekse beslutninger. Det foreligger også vanskeligheter med å identifisere hva den optimale balansen faktisk er (Chenhall, 2003). For å lykkes trekkes en rekke egenskaper frem, hvor blant annet profesjonalitet, maktforhold og autonomi vektlegges. Et resultat av en bedrifts manglende evne til å praktisere overnevnte skaper ustabilitet, langsomme beslutninger og dårlig ytelse (Chenhall, 2003).

2.2 Teorier tilknyttet forskningen

Innenfor håndtering av cybertrusler utpekes menneskets rolle som spesielt viktig. Den menneskelige atferden utgjør en unik risiko for en organisasjon, som ikke kan løses ved å investere i kompleks teknologi (Perez, 2020 s.29). Derfor skal vi ta for oss teorier som viser elementene ved individet som er avgjørende i håndtering av cybertrusler. De viktige elementer er til knyttet individets risikovilje, beslutninger og overvurdering av egne evner. Fra bedrifts perspektivet tar vi for oss internkontrollen og valg knyttet til tjenesteutsetting.

2.2.1 Risikovilje og internkontroll

Risiko er overalt. Det er alltid en risiko for hendelser, men det handler om hvordan en unngår dem (Arnoldi, 2009, s 1). Risikovilje avhenger av hva organisasjonen bør akseptere for å nå sine mål, inkludert tiltak for å redusere risiko (Aakre, 2020). Men omhandler også individets holdninger og omfavnelse av risikoaksept. Forskning viser at mennesker har ulik oppfatning av risiko, og dette påvirker den strategiske beslutningen. Ved at risikoappetitten viker fra organisasjonens påståtte vilje til å ta risiko påvirker det utfallet av handlinger rundt cybersikkerhet. Risikoappetitten varierer altså mellom individer og nivåer, og vil påvirke de individuelle vurderingene og oppfatningen av risiko (Power, 2004). Dersom ledelsen ikke lykkes med å implementere de samme holdningene når det gjelder forståelse og aksept av risiko, innebærer det en stor risiko i seg selv.

Dysvik (2021) påpeker at folk har kjent en større sårbarhet enn noen gang før, hvor ansatte omtales som «det svakeste punktet». Det brukes derfor store ressurser for å sikre at de blir bevisstgjort om sikkerhetskultur og atferd. Dysvik (2021) viser at det er krevende å lære opp ansatte, men ansatte viser at de forstår aspektet. Forskningen viser imidlertid at flere ansatte gjør ting de ikke burde. For eksempel samme passord og usikkerhet rundt svindelforsøk, men de holder fortsatt kontakt med IT-teamet i frykt for konsekvenser (Dysvik, 2021). Noe som illustrerer en stor fare i forskjellen på risikovilje og den enkelte ansattes forståelse.

I lys av individets risikooppfatning vil internkontroll spille en viktig rolle i håndteringen av cyberrisiko. Internkontroll er virksomhetens egen kontroll, og fungerer som en kvalitetssikring som skal oppdage utfordringer i tide (NHO, i.d.). Studier om internkontroll viser at små og mellomstore bedrifter er spesielt utsatt for svindel.

Årsakene bak dette er uformell internkontroll og nærhet til ledelsen som gjør at ansatte kjenner en «beskyttelse» (Kulset & Meidelsen, 2020 s. 4). Dette illustrerer viktigheten av å se på medarbeideren og internkontrollrollen.

Aakre (2020b, s.3) trekker frem et meget interessant funn med tanke på toppledelsens overvåking. Intervjuer avdekket at toppledelsen sjelden overvåket prosessen med å tilpasse eksternt regelverk inn i interne risikovurderinger og rutiner. Den ansvarlige for risikostyringen er med andre ord ikke direkte involvert i prosessen, i hvert fall sjeldent i en tidlig fase. Dette synliggjør problemet og viktigheten av et veletablert system og prosess mot internkontroll.

2.2.2 Beslutningsteori

Beslutningsteorien omhandler hvordan rasjonelle individer skal oppføre seg under usikkerhet og risiko (Alijoyo, 2021). I bedrifter må beslutninger tas hele tiden. Både på ledernivå, men også på operativt nivå. Derfor er det viktig å understreke den enkeltes rolle innenfor cybersikkerhet. Menneskelig atferd en unik risiko for en organisasjon som ikke kan løses ved å investere i kompleks teknologi (Perez, 2020 s. 29). For å kunne håndtere cybersikkerhet er det derfor viktig at alle individer er koordinert innenfor beslutningstaking. Bevisstgjøring med utgangspunkt i individet til virksomhetens perspektiv fremheves som en løsning (Bendovschi, 2015 s. 30). Formålet er å skape en sammenheng mellom de ansattes beslutninger og toppledernes interesser.

Den "riktige" avgjørelsen vil være viktig foran, under og etter et cyberangrep. Ved "feil" avgjørelse kan dette være en stor risiko for selskapet, og ikke minst for selskapets fremtid. Cyberangrep kan knyttet direkte opp mot den menneskelige atferden (Evans et al, 2016). Derfor er det viktig at alle ansatte har felles kunnskap for både å oppdage angrep, men også for å forhindre dem. "Feil" avgjørelser er et resultat av at avgjørelsen tar og at mer informasjon burde blitt samlet, før personen valgte å ta en beslutning på vegne av virksomheten (Goodman, 1993). Enkeltpersoner kan anta at de tar den riktige avgjørelsen, og at de har kunnskap om alle mulige alternativer (Turpin & Marasi, 2004.s. 144). I realiteten er det komplisert på grunn av at ledere og enkeltpersoner mangler tilgang til all informasjon. Dette vanskeliggjør å fatte et rasjonelt valg (Turpin & Marasi, 2004.s. 144).

Bedrifter kan investere i opplæringsmoduler og brukervennlige verktøy, men kan ikke redegjøre for ansattes oppførsel i virksomheten (Yazdanmehr & Wang, 2016). Ledelsen kan derfor legge et grunnlag for hvordan de ønsker at en ansatt skal informere om risikofylte handlinger, men en kan ikke vite hvordan den enkelte vil opptre. I motsetning til de digitale systemene, så vil tydelig lederskap, positiv stimuli og motivasjon være til nytte for de ansatte. (Yazdanmehr & Wang, 2016).

2.2.3 Dunning-Kruger-effekten

Dunning-Kruger-effekten omhandler overvurdering av egen kunnskap. Enkelt personer med lavere ferdigheter mener de sitter på mer kunnskap enn de faktisk gjør. Dette kan forklares av at menneskers ignoranse ofte er usynlig for dem (Dunning, 2011). Dunning-Kruger- effekten forklarer at menneskene lider av en dobbel byrde ved at de kommer til en feilaktig konklusjon og ender med å ta uheldige valg (Dunning & Kruger, 1999). Hatton (2020) viser til at det er de ansatte med lavest kunnskap som har størst mulighet til å trykke på en "phising" e-post. I enkelte SMB-er ser det ut til at jo bedre risikostyringssystemet oppfattes, desto mindre forberedt er ansatte på å håndtere risikoene relatert til styringssystemet (Vakulchuk et al, 2023) Dette viser at Dunning-Kruger-effekten også gjør seg gjeldende innenfor cybersikkerhet. Ved å gi de ansatte mer trening og kunnskap sikrer en seg mer seg mot Dunning-Kruger-effekten (Hatton, 2020). Men det er ikke bare ansatte som kan preges av denne effekten. Fra et tjenesteutsettings perspektiv, så viser Hatton (2020) til at tilbydere av IT tjenester også overvurderer egen evne i forhold til cybersikkerheten. Noe som illustrerer en sårbarhet som bedrifter som benytter seg av tjenesteutsettelse står i.

2.2.4 Transaksjonskostnadsteori - "Make or buy"

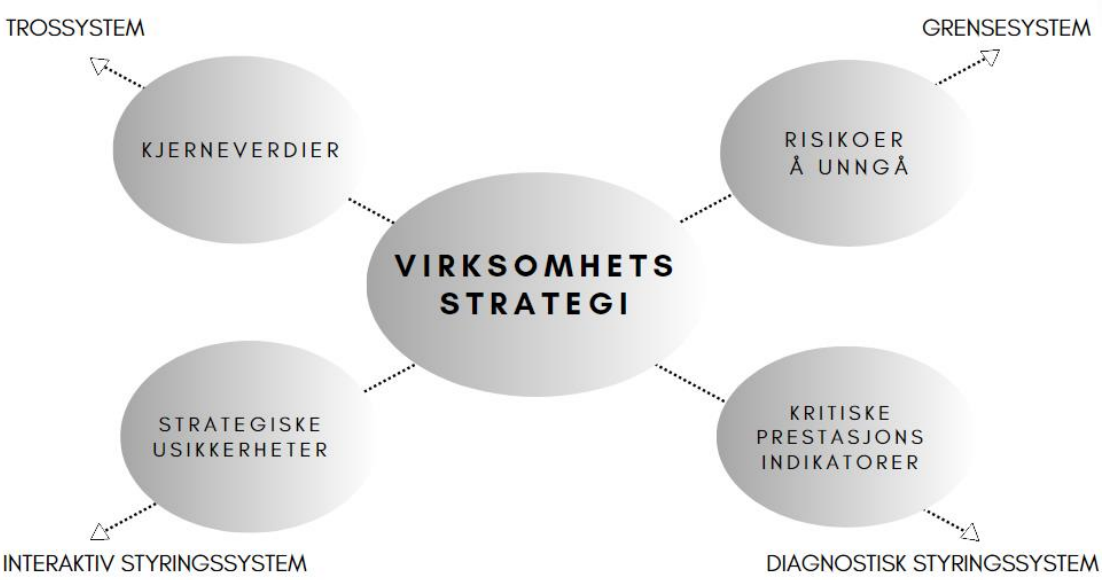
Fra et organisatorisk perspektiv handler transaksjonskostnadsteori om minimering av produksjons og transaksjonskostnader. Transaksjonskostnadsteori blir ofte sett på som opphavet til tjenesteutsetting (Hätönen & Eriksson, 2009). Teorien bidrar med å forklare valgene knyttet til tjenesteutsetting og tjenesteinnsetting. Før bedriftene velger om å tjenesteutsette må de se hvilken strategi som passer best for de og vurdere både produksjon og transaksjonskostnaden. For at tjenesteutsetting skal lønne seg er det nødvendig at transaksjonskostnadene er lavere enn produksjonskostnadene (Zakharova, 2020, s.13 og 17). Før bedriftene velger å gjøre den økonomiske transaksjonen, så handler det om å se helheten av transaksjonen.Det omhandler den faktiske kostnaden bedriftene har ved å tjenesteutsette deler av produksjonen.

Deretter for å vurdere om det er verdt det, og om en skal "make or buy" (Kolltveit et al., 2009, s.16). Når alle kostandene er tatt i betraktning tas det en beslutning (Monash University, i.d).

2.3 Teoretisk rammeverk - Levers of Control (LoC)

Rammeverket Levers of Control (Simons, 1995) anses som et av de mest anerkjente og brukte styringssystemene innenfor økonomistyring litteraturen (Martyn et al,. 2016). Bakgrunnen for rammeverket stammer fra organisasjonens tunnelsyn i strategiutforming. Simons (1995) mente at det hadde blitt underkommunisert hvordan strategi skulle kontrolleres og implementeres. Noe av det mest elementære med Simons rammeverk er at strategien ikke bare er en bestemmelse fra ledelsen, men et felles mål som blir utarbeidet av alle nivåer i bedriften. Levers of Control-rammeverket hevder at strategisk usikkerhet og risiko påvirker valgene vi tar og bruken av kontrollsystemene. Dette får igjen innvirkninger på den organisatoriske læringen og effektiv bruk av lederens oppmerksomhet (Simons, 2000). Simons (1995) omhandler individer i organisasjonene i flere perspektiver og er derfor verdifull å inkludere i denne forskningen. Rammeverket kan bidra til å kartlegge i hvilken grad bedrifter benytter seg av rammeverkets kontrollspaker for å håndtere cybertrusler. Denne tilnærmingen gir en indikasjon på om det foreligger en sammenheng mellom styringssystemet og cybersikkerhet.

Rammeverket består av fire kontrollspaker som sammen skal bidra til å utforme en god virksomhetsstrategi. Kontrollspakene er *grensesystemer, trossystemer, diagnostiske kontrollmekanismer og interaktive kontrollmekanismer.*



Figur 1: Simons kontrollspaker (Simons, 1995) *Kilde: Egenprodusert figur*

Ofte vil det være utfordrende å benytte alle kontrollspakene, og i noen tilfeller vil kontrollspakene ha motstridende krefter som gjør dem vanskelige å balansere. Derfor er det lederens ansvar å finne en balanse mellom de motstridende kreftene som vil skape en best mulig virksomhetsstrategi (Mundy, 2009).

2.3.1 Balanse

Et styringssystem har som hensikt å finne en balanse mellom styring og kontroll i en organisasjon. Styring bidrar med å sikre at organisasjonen kan produsere produkter av høy kvalitet, eller effektive resultater når ledelsen ikke har mulighet til å overvåke situasjonen personlig (Deshler, 2017). Kontroll betyr at arbeidsledelsen kommer som et resultat av avgjørelser tatt av en enkeltperson eller en ledergruppe (Deshler, 2017).

Balanse er en av de viktigste faktorene for at de fire kontrollspakene i rammeverket skal lykkes. Widener (2007) studerte kontrollspakenes relasjon på tvers av styringssystemene, som viser til at de avhenger og utfyller hverandre. Samspillet mellom de fire kontrollspakene skal skape en god balanse i organisasjonen. Simons legger opp til at de ansatte både skal kunne utfolde seg kreativt, men også bruke kontrollspakene til å begrense og kontrollere de ansattes adferd (Mundy, 2009).

Forskjellige forfattere har imidlertid understreket at små og mellomstore bedrifters underutviklede ledelsesprosesser, evner og mangel på ressurser hindrer dem i å oppnå en slik balanse (Pesalj et al,. 2018). I mindre organisasjoner blir arbeidsoppgavene mer sammensluttet enn i store bedrifter (Pesalj et al,. 2018). Dette kan skape rolleforvirring, som igjen kan forklare den manglende evnen til å oppnå god balanse i styringssystemet.

2.3.2 Trossystemer

Trossystemet er en måte for virksomheten å kommunisere visjonen og planene for virksomheten. For organisasjonen bidrar det til å sikre at oppførselen til de ansatte gjenspeiler bedriftens verdier (Tessier & Otley, 2012). Simons (1995) presiserer at alle organisasjoner er skapt for et formål. Disse formålene blir ofte kommunisert ut til kunder og ansatte gjennom et trossystem. Virksomheten benytter også kjerneverdier for å skape engasjement i organisasjonene. Typisk er trossystemer konsise, verdifulle og inspirerende (Simons, 1995). I dag kreves det klare trossystemer av kunder. Dette ser vi spesielt innen teknologibransjen, hvor kunder har et sterkt behov for å kjenne seg igjen i verdiene til merkene (Drive, 2019).

Kraften til et tilfredsstillende trossystem innebærer at hele organisasjonen jobber mot et felles mål. Kjerneverdiene skal gi veiledning, selv om verdiene kan være mer diffuse enn konkrete (Simons, 2000). Et velfungerende trossystem skal ikke bare være et overhengende budskap, men heller et verktøy for ansatte for hvordan de skal opptre i uklare situasjoner. Det er en sammenheng mellom trossystem og grensesystemer. Trossystemene åpner opp for at de ansatte kan utfolde seg kreativt, mens grensesystemene har som hensikt å begrense de ansatte slik at de ikke sklir ut fra det feltet organisasjonen jobber med. Det må med andre ord være en balanse mellom disse kontrollspakene for at rammeverk skal fungere optimalt (Martyn et al, 2016).

Simons (1995) argumenter også for at det ikke er nok at bedrifter har nedskrevne mål og visjoner. Disse visjonene må også vises direkte fra ledernes handlinger. Dette skaper troverdighet både overfor kunder, men også for de ansatte. Når det gjelder ledelseskontroll mot cyberkriminalitet, så er trossystemet gunstig for å kommunisere visjonen til virksomheten. For eksempel, «vi har som mål å være best på å bevare informasjonen om kundene våre». Trossystemet er ofte med vilje gjort så bredt som mulig, slik at det påvirker større deler av organisasjonen (Simons, 1995).

Nødvendigheten ved å ha et trossystem som fokuserer på cybersikkerhet blir bare viktigere. Trossystemet har som hensikt å være et hjelpemiddel for de ansatte, slik at de kan vet hvordan de skal takle eventuelle problemer (Simons, 1994, s. 36). Opp mot dette vil et tydelig trossystem knyttet opp mot cybersikkerhet kunne bidra til at ansatte vet hvordan de skal håndtere cybertrusler. Videre at arbeidet mot et felles mål resulterer i at cybersikkerheten blir ivaretatt.

2.3.3 Grensesystemer

For å kontrollere ansatte i virksomheten foreligger det behov for grenser. Disse vil hjelpe med å fortelle de ansatte hva de ikke skal gjøre og begrense forretningsrisiko (Simons, 1995). Disse grensene varierer mye mellom ulike bransjer. Trossystemet spesifiserer positive idealer, mens grenser fungerer som en barriere basert på definerte forretningsrisikoer (Simons, 1994, s. 39). Når det er sagt, så er det viktig å ikke forveksle grensene med regler. Det må heller betraktes som en ramme for hvilke områder bedriften ikke skal bedrive (Simons, 1994, s. 40).

Grensesystemer har som hensikt å utnytte ansattes kreativitet, samtidig som det setter en stopper for aktivitet som kan skade bedriftens virksomhetsområde (Simons, 1995). Grensesystemer er satt på bakgrunn av lederens manglende evne til å overvære alt som skjer i bedriften (Simons, 1994, s. 40). Selv om noen kan oppfatte rammer som en begrensing, kan andre finne det trygt å vite hvor grensene går. Dermed klarer de å utfolde seg mer kreativt innenfor de gitte rammene de har (Simons, 1994, s. 40).

I lys av cyberangrep er grensesystemer relevant for å ivareta cybersikkerheten. Et tydelig grensesystem vil bidra til å minimere negative konsekvenser som cyberangrep medfører. Menneskelig atferd utgjør en unik risiko for en organisasjon, som ikke kan løses ved å investere i kompleks teknologi (Perez, 2020 s. 29). Dette peker mot viktigheten av et grensesystem som begrenser menneskers mulighet til å gjøre feil.

2.3.4 Diagnostiske kontrollmekanismer

Diagnostiske kontrollsystemer er en mer «streng» kontrollspak som bygger på tilbakemeldingskontroll og måling av ytelsen (Simons, 1995). Diagnosesystemet har samme funksjon i en organisasjon. Den er der for å oppdage feil eller gi tilbakemelding hvis noe ikke fungerer optimalt. Videre behandles tilbakemeldingene som skaper evaluering av ansatte og metodene som benyttes (Tessier & Otley, 2012). Diagnosesystemet har en struktur slik at kontrollen ofte blir tatt fra lederhold. Det foreligger derfor et behov for systemer eller tilbakemeldingsplattformer som lar dem overvåke de ansatte (Tessier & Otley, 2012).

Diagnostiske mål blir ofte bundet opp mot prestasjon. Enten om det er økonomiske resultater som gjenspeiles i budsjetter, eller om det er personlige mål som kan observeres gjennom tester (Mundy, 2010). Diagnostiske kontrollsystemer er særlig relevante i lys av cybersikkerhet. Et godt strukturert diagnosesystem vil kunne avdekke mangler, og er fordelaktig å etablere før et eventuelt cyberangrep. Samtidig har systemet som hensikt å gjøre det lettere for lederne å spore utviklingen av målene. Dette gjelder for enkeltpersoner og for hele organisasjonen. Denne formen for kontrollsystem er mer egnet i store selskaper på grunn av større avstand fra topplederne til de ansatte som fører til ukonsekvent kontakt. I noen tilfeller er det vanskelig å ikke bruke denne kontrollspaken. Det finnes eksempler på mindre virksomheter som fokuserer for mye på diagnosesystemet, og mister kontrollen over de ansatte (Mundy, 2010).

Den diagnostiske kontrollspaken fokuserer på å måle fastsatte og konkret mål. (Simons, 1994, 1995) I et cyberperspektiv blir den derfor særdeles aktuell i form av måling av ansatte og tilbakemeldinger rundt trusselbildet og systemer. Bedrifter kan derfor bruke denne kontrollspaken som et hjelpemiddel, for å utarbeide et grunnlag for utbedringer av cybersikkerheten.

2.3.5 Interaktive kontrollmekanismer

Interaktive kontrollmekanismer er knyttet til personlig kontakt og informasjonsutveksling (Kruis, et al., 2016). Dette er interessant å se på i forhold til å håndtere cybertrusler, da dette spiller en viktig rolle. God informasjonsutveksling kan bringe selskapet nærmere ved å oppmuntre til en informasjonsstrøm fra de ansatte til topplederne.

Dette er på mange måter en mer ressurskrevende tilnærming, men gevinsten ved et slikt system er langt større enn den diagnostiske. Systemet skal motivere de ansatte til å ta nye beslutninger og utfordre seg selv i nye retninger (Simons, 1995).

Simons (2010, s. 158) poengtere at "*alle følger med på det lederen følger med på*". Dette bygger videre på at lederen må delta aktivt i arbeidshverdagen for å kunne forstå hvilke regler og systemer bedriften trenger for å fungere optimalt. Lederens mulighet til å delta i daglig drift er ikke alltid like stor. Det kan derfor være viktig å opprette plattformer og arenaer der lederne kan kommunisere med de ansatte. Ved å ha god intern kommunikasjon vil organisasjonen være bedre rustet til å avstå fra eventuelle situasjoner som kan virke krevende. Dette vil også hjelpe organisasjonen å være proaktiv for eventuelle hendelser eksempelvis et cyberangrep (Langfield-Smith, 1997). Ved svak interaktiv styring risikerer den organisatoriske læringen å svekkes. Simon (1994) trekker også frem at kommunikasjon skjer best ved ansikt til ansikt. Videre at man bør opprette arena for å skape dialog for å fremme en effektiv læringsprosess. Et viktig element er også å involvere ansatte på tvers av hierarkiske nivåer (Simons, 1994). En tettere og mer informert bedrift vil også være bedre egnet til å selv kunne forstå omfanget av cybertrusler og selv håndtere dem.

2.3.6 Kritikk av rammeverket

Selv om Simons rammeverk er et av de mest brukte innen økonomistyring litteratur utsettes det for kritikk. Det er blant annet kritisert for å være for vagt beskrevet når det kommer til balansen og det er vanskelig å finne en beskrivelse på hvordan denne balansen skal se ut i praksis (Ferreira & Otley, 2009). Rammeverket er også kritisert for å ha for dårlige beskrivelser av de forskjellige kontrollspakene. (Tessier & Otley, 2012). Det er ikke gjort noen forsøk på å gjøre definisjonen mer forståelig, selv om det er gjort forsøk på å utbedre selve rammeverket som en helhet (Malmi & Brown, 2008). Rammeverket har også mottatt kritikk for å rette for lite fokus mot de sosio-ideologiske kontrollene, og heller kun fokusere på toppledelsen (Collier, 2005).

3.0. Metode

I dette kapittelet skal vi forklare metoden og fremgangsmåten vi har benyttet. Vi skal gå nærmere innpå den kvalitative og kvantitative metoden, og videre beskrive og begrunne våre valg i denne prosessen. Vi skal gå mer i detalj i utformingen av intervjuguiden og intervjuprosessen. Deretter skal vi gå mer i dybden rundt oppbyggingen av spørreundersøkelsen. Avslutningsvis skal vi presentere vårt utvalg og hvorfor vi ønsket at de skulle bidra til forskningen.

3.1 Litteraturstudie

Litteraturgjennomgang refererer til en gjennomgang av eksisterende litteratur innenfor et fagområde. Hensikten med dette er å lage en samlet oppsummering og evaluere forskningen, men også demonstrere hvordan det passer opp mot egen forskning innenfor et større fagfelt (USC Libraries, 2022). Metoden vi har brukt er «scope review», som har hjulpet oss å forstå bredden av litteraturen. Tilnærmingen har gitt oss innblikk i hvilken forskning og kunnskap som finnes på området. Videre hvordan forskningen er gjennomført og hvilken kunnskap som mangler på området (USC Libraries, 2022).

Vi ser at det er kommet en del ny forskning på cybersikkerhet de siste årene, noe som kan skyldes fenomenets fremvekst og usikkerhet. Vi har gjennomgått artikler og rapporter som handler om cybersikkerhet og cyberkriminalitet. Spesielt har vi benyttet oss av nasjonale rapporter knyttet til risiko og sikkerhet, deriblant Nasjonal sikkerhetsmyndighet (NSM, 2022:2023) og Kripos (2023).

Når det kommer til praktiske aspekter ved litteraturgjennomgang, brukte vi Google Scholar og Oria som database. Nøkkelordene våre var i hovedsak "Cybertrusler / Cyberthreaths", "Cybersikkerhet / Cybersecurity", "Internkontroll / Internal control", "Styringssystemer /Management control systems" og "Risiko / Risk". For å lære mer om bruken av styringssystem har vi undersøkt litteratur knyttet til Levers of Control.

Videre søkte vi spesielt etter litteratur som var rettet mot SMB, da dette er vår avgrensning. Gjennom våre veiledere har vi fått tildelt magasiner, artikler og råd om aktuelle forskningsprosjekter. For å supplere til dette har vi også brukt medier for å aktualisere omfanget knyttet til cybertrusler.

3.2 Datainnsamlingsprosess - Kvalitativ og kvantitativ

I forskningen vår har vi valgt å benytte oss av både kvantitativ og kvalitativ datainnsamling. De er begge gode på egenhånd, men ofte så utfyller og styrker de hverandre også (Skilbrei, 2019, s.17). Gjennom denne tilnærmingen får vi en bredere forståelse av cybersikkerhetens praksis. Vi mener denne kombinasjonen har gitt oss det mest nøyaktige bildet av bedriftene, ledelsen og de ansatte. Ved bruk av kvantitativ undersøkelse får en kartlagt hva bedriftens strategi, tiltak og utfordringer innebærer. Ved den kvalitative undersøkelsen fikk vi avdekket ansattes oppfatning og kunnskap relatert til bedriftens cybersikkerhet. For å underbygge vår forskning sendte vi ut tilsvarende spørreundersøkelse til et utvalg av tidligere studenter (Alumni). Denne dataen bidrar til å verifisere det lederne, ekspertene, og ansatte sier om temaet. Gjennom bruk av både kvalitativ og kvantitativ undersøkelse tilegnet vi oss et bredt grunnlag for å besvare problemstillingen.

Under forskningen har vi fullført totalt 9 intervjuer. Utvalget vårt består av bedrifter som opererer i forskjellige bransjer og geografiske områder, som gjør at vi treffer flere typer små og mellomstore bedrifter. Denne tilnærmingen styrker forskningen vår innenfor SMB, siden vi avdekker strategier og utfordringer knyttet til flere bransjer.

For å skape forståelse innenfor cyberdomene, så har våre eksperter representert ulike deler av fagfeltet. Vi har fått tilegnet oss et akademisk perspektiv, leverandørens perspektiv og IT ansatt sitt perspektiv. Dette har gitt oss ulike innfallsvinkler på tematikken, som forsterker forskningen vår.

3.2.1 Kvalitativ metode

Den kvalitative metoden fokuserer på å gi dybde, nyanser og variasjon i fenomenet som undersøkes (Iversen, 2011, s. 179). Metoden tilrettelegger for å tilegne seg mer fyldige og detaljerte beskrivelser (Johannessen, Christoffersen og Tufte, 2020 s.105). Vi innhentet dermed den kvalitative dataen gjennom semistrukturerte dybde intervju. Denne tilnærmingen ga oss detaljene, som kunne falle bort i den kvantitative delen av forskningen vår. Dermed fikk vi svar på spørsmål som trengte mer reflekterte og utbredte svar. I vårt tilfelle ønsket vi å lære mer om hvilken strategi og praksis bedriftene benytter. Den kvalitative metoden egner seg godt for å få handlinger og intensjoner og erfaringer rundt et tema (Johannessen, Christoffersen og Tufte, 2020, s.105). Tilnærmingen var derfor helt avgjørende for å forstå hva bedriftene håndtering av cybersikkerhet.

Vi brukte en semistrukturert intervjuguide (vedlegg 4 og 5) for å ha friheten til å forme intervjuet underveis. Dette er en blanding av strukturert og ustrukturert intervju, hvor man har strukturert ulike tema og problemer som en ønsker å få svar på. Ved å ha et semistrukturert intervju krever det mer fra informantene, ettersom informantene de må svare på mer utdypende spørsmål (Ghauri, Grønhaug og Strange, 2020, s.115). Fra intervjuguiden er det åpne spørsmål, slik at informantene svarer med egne ord, og ikke formes av forskerens ord slik det ofte blir gjennom spørreundersøkelse (Johannessen, Christoffersen og Tufte, 2020, s.105). Alle informantene fikk ekstra spørsmål utenfor den intervjuguiden som var forberedt, ettersom det dukket opp informasjon som føltes naturlig å følge opp i samtalen. Dette resulterte i en mer helhetlig samtale og med flyt. Dette er noe som er til sterkt nytte med kvalitativ metode, fordi en får en dypere samtale med informanten (Johannessen, Christoffersen og Tufte, 2020, s.105)

3.2.2 Kvantitativ metode

Kvantitativ metode uttrykkes i form av rene tall eller andre mengdetermer (Grønmo, 2012, s.123). I oppgaven innhentet vi den kvantitative dataen gjennom spørreundersøkelser. Disse gikk ut til case-bedriftens ansatte og utvalget av tidligere studenter (Alumni).

I kvantitativ undersøkelse er det spørreundersøkelse som er mest vanlig, og den metoden er det vi også valgte å bruke. Ved bruk av denne metoden var det viktig å vite på forhånd hva en skal spørre om, og hva forskeren ønsker av de som deltar i spørreundersøkelsen. Ettersom en ikke kan endre på undersøkelsen når den først er sendt ut, så er det en fordel at andre tester den først. Slik at man unngår misforståelser i spørsmålene, og får høre andres oppfatning av spørreundersøkelsen (Johannessen, Christoffersen og Tufte, s. 285 og 295). Når man lager en spørreundersøkelse kan det for flere være viktig at det ikke blir mange eller for vanskelige spørsmål. Da risikerer man at deltakerne ikke ønsker å besvare den, og derfor bør en holde seg under 30 spørsmål for å ikke ha en for omfattende undersøkelse (Johannessen, Christoffersen og Tufte, 2020 s. 295).

Ofte ved bruk av spørreundersøkelser starter en bakgrunnsinformasjon i form av alder og kjønn, før en går videre til spørsmål som det forskes på. For å svare på spørsmålene blir det ofte brukt skalaer for å kunne best mulig treffe det deltakerne mener om temaet. Partall alternativer blir flittig brukt for å unngå at en kan svare "nøytral" slik som en gjør om det er fem alternativer. Det er som oftest fire eller fem skalaer bortover hvor en skal svare på til helt uviktig → svært viktig eller fra aldri → alltid.

Bruk av spørreundersøkelse må være selvinstruerende og entydig formulert (Johannessen, Christoffersen og Tufte, 2020, s. 293).

3.3 Rekruttering – finne informantene

Rekrutteringsprosessen er den delen vi brukte mest tid på gjennom hele oppgaven. For å finne de rette informantene til prosjektet krevde det en del innsats fra oss og veilederne. Vi ønsket i hovedsak å komme i kontakt med bedrifter som enten har blitt angrepet eller forsøkt angrepet. Vi startet med å sende e-post til både NSM (Nasjonal sikkerhetsmyndighet), Kripos og IT-avdelingen ved universitetet i håp om at de kunne hjelpe oss med å finne aktuelle kandidater. Dette førte ingen steder, derfor brukte vi vårt personlige nettverk for å få tak i informanter. Internett har også vært et nyttig verktøy vi har brukt i søken etter egnede bedrifter og eksperter. Etter noe tid kom vi i kontakt med fire bedrifter som ønsket å delta. Dette er bedrifter fra forskjellige steder i Norge og fra ulike bransjer. Dette gjør at vi får et bredere innsyn på små og mellomstore bedrifters håndtering av cybertrusler.

Ekspertene til oppgaven kom vi i kontakt med gjennom nettverket vårt og ved å bruke internett som verktøy. Ved å søke etter informanter som har varierende kompetanse rundt cybersikkerhet. Etter hvert klarte vi å få til fire intervjuer med eksperter som har god erfaring med tematikken til forskningen. Noen representerer erfaring fra næringslivet, mens andre har en akademisk tilnærming. I tillegg til ekspertintervjuene hadde vi et prøveintervju med en informant som har mye kunnskap om cybersikkerhet. Med hensikt å få mer bakgrunnsinformasjon og for å gjøre en gjennomgang før vi gikk ut på bedriftene og ekspertene. Dette var noe som hjalp oss å både formulere spørsmålene bedre, men også få mer innblikk fra noen som har annen kunnskap enn oss. I løpet av tre uker ble alle intervjuene gjennomført, og transkribert for å analysere dataen som ble funnet i intervjuene.

3.4 Kvalitativ forskning – Intervju

For å få mest mulig dybde og nøyaktig beskrivelse av håndtering av cybersikkerhet, gjennomførte vi flere semistrukturerte dybdeintervju. Hensikt å få en fritt flytende samtale om tema, som kunne tilpasses informantens kunnskap underveis. I intervjuene så er det en som spør spørsmålene, og informanten følger opp med svar av dette.

Fra intervjuguiden er det åpne spørsmål, slik at en får informanten til å svare i egne ord, og ikke kun bruke ord som forskeren har foreslått, slik som det ofte blir når en har en spørreundersøkelse (Johannessen, Christoffersen og Tufte, 2020, s.105).

Bedriftene vi har tatt for oss er mellomstore bedrifter med variasjon på 60-130 ansatte. Bedriftene som er over 100 ansatte har kun en liten administrativ avdeling, men en stor operativ avdeling. Vi vurderer det dermed slik at de ansatte i den administrative avdeling er hovedfokuset i vår datainnsamling. På grunnlag av at det er den administrative avdelingen som eksponeres for cyberangrep gjennom digitale verktøy som er knyttet til bedriften.

I oppgaven vil informantene og case-bedriftene referere til fiktive navn. Disse kjennemerkene er gitt under.

Informant	**Kjennemerke**
Leder / IT	Studentservice AS
Leder / IT	Regnskap AS
Leder / IT	IT-utviklere AS
Leder / IT	Fiskeribedrift AS
Ekspert	Akademisk ekspert
Ekspert	IT-leverandør
Ekspert	IT-ansatt
Ekspert	PhD stipendiat

Tabell 1: Kjennemerke

3.4.1 Intervjuguide for lederne / IT- stilling

Vi bygde opp intervjuguiden (vedlegg 5) slik at spørsmålene er delt inn i kategorier som dekker alle kontrollspakene i Simons rammeverk (Simons, 1995). Vi stilte ingen direkte spørsmål som refererte til det teoretiske rammeverket, fordi vi ikke kunne anta at det kjent for alle informantene. Spørsmålene var indirekte rettet mot hver enkelt kontrollspak med cybersikkerhet som kontekst. Hensikten å kunne avdekke i hvilken grad bedriftene benyttet seg av hver enkelt kontrollspak ubevisst. Intervjuguiden ble delt inn etter bakgrunn, selskap, angrep, cybersikkerhet, opplæring, læring og refleksjon. Vi ønsket å se hvordan selskapet opererte innenfor feltet. Videre ønsket vi å lære mer om deres erfaring i forhold til å bli hacket eller forsøkt hacket og lærdommer knyttet til dette.

Utvalg 1: Ledende/ IT stilling i bedrift

Intervjuet var et semistrukturert dybdeintervju, som ble gjennomføres med enten en med ledende/ IT stilling i bedrift. Intervjuene hjalp oss med å avdekke utformingen av styringskontrollsystemet deres opp mot cybersikkerhet. Informantene utdypet angående selskapets struktur og deres ledelseskontrollsystem. Men også hvilke tiltak og strategier bedriftene benytter for å håndtere cybertruslene. Hensikten med intervjuet med virksomhetene er å synliggjøre prosessene og praksisene som benyttes.

Vi gjennomførte et intervju per case-bedrift. Vi ettersendte også noen ekstra spørsmål på e-post, der vi følte det manglet noe etter å ha transkribert intervjuene.

3.4.2 Gjennomføring av intervju med case-bedriftene

Intervjuene med en av lederne/IT av bedriftene ble gjort fysisk, og de tre andre ble gjort via den digitale plattformen Teams. Før vi startet intervjuene hadde vi lest oss opp på bedriftens bakgrunn, og sett over intervjuguiden som var forberedt på forhånd. Ved intervjuets begynnelse hadde vi en kort introduksjon av oss som studenter. Videre stilte vi noen enkle spørsmål om navn, nåværende posisjon og bedrift for å bli bedre kjent med informantene. Vi opplevde at dette hjalp til med å skape en bedre flyt under intervjuet, før vi startet med de faglige spørsmålene. Under intervjuet tok en av studentene styringen, for å gjøre det enklere og skape mer struktur i prosessen. De to andre studentene supplerte med tilleggsspørsmål hvis en ønsket å vite mer fra lederne.

Vi hadde utarbeidet spørsmål innenfor en rekke ulike temaer som vi anså som essensielle, for å kunne besvare forskningsspørsmålene. Etter spørsmålene om bakgrunn og bedriften gikk vi over til den mer faglige delen, og deres oppfatning av cybersikkerhet. Etter en samtale rundt deres oppfatning av cybersikkerhet førte det naturlig over til bedriftens arbeid rundt tematikken. I denne delen av intervjuet ønsket vi å få vite rutinene til ledelsen og de ansatte rundt tematikken. Hvordan de håndterer eller ikke håndterer cybertrusler. Vi stilte spørsmål angående tidligere erfaringer rundt angrep, og hva som er planen ved et potensielt angrep. Videre stilte vi spørsmål om opplæring innad bedriften, men også eventuelt lærdom og refleksjon. Siden intervjuene var semistrukturert så tilpasset vi naturlig underveis. Etter hvert som vi intervjuet flere, tilegnet vi oss mer kunnskap og kunne spørre om enkeltes meninger knyttet til andres svar. Spesielt etter intervjuene med ekspertene ble det lettere å spørre spørsmål utenfor intervjuguiden. Deriblant bruk av etisk hacking for å måle ansattes prestasjoner opp mot cybersikkerhet.

Avslutningsvis spurte vi om de hadde noe de ønsket å tilføye til intervjuet, eller om de hadde noe annet de ønsket å informere oss om. I noen av intervjuene hadde lederne mye de ønsket å si om saken, mens andre ikke hadde mer informasjon å dele. Flere av informantene uttrykte at de var glade for at vi forsket på cybersikkerhet. At det var et aktuelt tema som trengs mer kunnskap om.

Etter endt intervju sendte vi ut spørreundersøkelse til lederne/ IT, slik at de kunne sende det ut til de bedriftens ansatte.

3.4.3 Intervjuguide for eksperter

Utarbeidelse av intervjuguiden for eksperter (vedlegg 4) er delt inn i tre kategorier: bakgrunn, cybersikkerhet og cyberangrep, og små og mellomstore bedrifter. Temaer vi snakket om inkluderte opplæring, forebygging, hackerens intensjoner og svindelmetoder. Her forventet vi å innhente ulike erfarings- og meningsutvekslinger, som styrket vårt bidrag til forskningen.

Kombinasjonen av utvalget ga oss en indikasjon på hvilke trusler som er aktuelle, men også hvordan virksomhetene jobbet for å forhindre cyberangrep. Trusselbildet utvikler seg hele tiden, og derfor ønsket vi oppdatert kunnskap fra noen som er eksponert problematikken.

Utvalg 2: Eksperter

For å oppnå dypere kunnskap og forståelse av teamet, så gjennomføre vi semistrukturert dybdeintervju med eksperter med forskjellig erfaring. Da fikk vi flere ulike erfaringer og perspektiver på cybersikkerhet som ga oppgaven et bredt fundament.

Vi har gjennomført totalt fire intervjuer, hvor ekspertene har ulike erfaringer innen cybersikkerhet.

3.4.4 Gjennomføring av ekspertintervju

Alle ekspertintervjuene ble gjennomført via den digitale plattformen Teams. På grunnlag av at flere av våre eksperter holdt til i andre deler av landet, og det ble derfor naturlig å gjøre det digitalt. I likhet med bedriftenes intervju startet vi med å introdusere oss og prosjektet vi utfører. Intervju strukturen ble lik som ved bedriftene, slik at en av oss holdt intervjuet og resten kunne supplere med spørsmål hvis ønskelig. Videre gikk vi over til informantene slik at de kunne fortelle om seg selv, sin bakgrunn og nåværende posisjon. Ved å få enda mer kunnskap om deres bakgrunn, så tilegnet vi oss forståelse for deres innfallsvinkel på tema.

Etter en innledende samtale om oss og deres bakgrunn gikk vi over til spørsmålene vi hadde forberedt. Her gikk vi innom temaer som cybersikkerhet og cyberangrep. Vi hadde noen spørsmål forberedt på forhånd, men ettersom ekspertene kom med ulike perspektiver på teamet, så tilpasset vi oss underveis Etter hvert skiftet vi fokus på SMB, hvor vi ønsket å få deres syn på SMB og hvilken kunnskap de satt på i forhold til hvordan SMBer bør håndtere trusselen. Ettersom vi hadde hatt noen intervjuer med bedrifter, så fikk vi også spurt om deres mening om våre funn.

Ved slutten av intervjuet ble det samtaler om de forskjellige temaene innenfor cyber. Vi spurte om de hadde noe å legge til, og de fleste ekspertene hadde mye de ønsket å si om teamet og tips til forskningen. Samtalene med ekspertene var av stor nytte, og ga oss tilgang til kunnskap vi ikke kunne fått foruten deres hjelp.

3.5 Kvantitativ forskning - Spørreundersøkelse

Vi sendte ut spørreundersøkelser til de ansatte i bedriftene for å få et bredere perspektiv på cybersikkerheten i bedriftene. Spørreundersøkelsen (vedlegg 6 og 7) bidrar til å skape et mer realistisk og transparent bilde av virksomhetens virkelighet.

Gjennom innhenting av informasjon fra hver enkelt ansatt er det lettere å finne ut hva som bør endres i møte med cyberangrep. Datainnsamlingen fra undersøkelsen hjelper forståelsen av hvordan SMB bør håndtere cyberangrep på individnivå. Spørreundersøkelsene var helt like til alle bedriftene, men de fikk egen link slik at vi kunne analysere dataen separat. Videre se om det var samsvar mellom leder / IT og de ansatte om prosedyrene til arbeidsplassen.

3.5.1 Gjennomføring av spørreundersøkelsen

Undersøkelsesstrukturen deltes inn i følgende kategorier: om deg, bedrift, cybersikkerhet, opplæring i bedriften og kultur i bedriften. Vi tok utgangspunkt i at vi ønsker korte holdepunkter rundt å bli kjent med deltakeren, deriblant kjønn og alder, men samtidig opprettholde anonymiteten. Spørreundersøkelsen har blitt sendt ut til ansatte i case-bedriftene og Alumni, derfor har vi delt dem inn i to ulike utvalg.

Utvalg 3: Ansatte fra case-bedriftene

Utvalget til undersøkelsen (vedlegg 6) var de ansatte i de fire case-bedriftene. Tanken var å avdekke faktorer som bidro til å svekke bedriften. De ansatte som fikk spørreundersøkelsen, er i hovedsak de som jobber administrativ avdeling og dermed benytter digitale verktøy knyttet til bedriften. Dette er de som får henvendelser innenfor cybertrusler. Det er derfor ganske store forskjeller i antall ansatte, og ansatte som faktisk fikk spørreundersøkelsen.

Utvalg 4: Alumni

Det siste utvalget besto av Alumni, som gjennomførte samme spørreundersøkelse (vedlegg 7) som de ansatte fra bedriftene. Dette er et nettverk for tidligere studenter fra Handelshøgskolen ved Nord universitet som har meldt seg inn som en del av Alumni etter endt bachelor, master eller doktorgrad.

Spørreundersøkelsen ble laget på plattformen nettskjema.no som er anbefalt av SIKT, og det var grunnen til at vi valgte å begynne oss av denne. Da vi skulle lage skjemaet brukte vi lang tid på å få spørsmålene til å passe best mulig til teori og ønsket forskning. Vi brukte også andre masteroppgaver til inspirasjon for å formulere spørsmål og hva spørreundersøkelsen bør inneholde. Deretter ble det fram og tilbake mellom oss og veileder for å få mest mulig ut av spørreundersøkelsen. Vi valgte å utforme en spørreundersøkelse der vi hadde både prekodede og åpne svar (Johannessen, Christoffersen og Tufte, 2020, s. 286).

Dette gjorde vi for å tilpasse slik at hvis noen hadde noe de ville tilføye, så kunne de det. Vi ønsket også informantens egne ord om cybersikkerhet som ble en fritekst boks. Tilnærmingen tilrettela for at informantene ikke følte seg låst, og fikk dele sin ærlige oppfatning.

Etter spørreundersøkelsen ble ferdig, sendte vi den ut til case-bedriftene og tilleggsutvalget vårt Alumni. Dette er en gruppe som er ferdigstudert fra Handelshøgskolen, og fikk tilsendt undersøkelsen på e-post. Dette har gitt oss statistikk på spørsmål som har latt oss avkrefte eller bekrefte antagelser som vi har dannet oss. Vi har også forsøkt å binde innholdet i spørreundersøkelsen, opp mot hovedtrekkene som intervjuguiden. Dette gjorde det mulig å avdekke hva som fungerer og hva som må forbedres i bedriftene. På Alumni-undersøkelsen fikk vi 113 svar, som vi skal analysere i funnene.

3.6 Analyse

Transkribering og videre analyse av intervjuene var tidskrevende. På bakgrunn av at intervjuene inneholdt en del ny kunnskap, som skapte lærerike samtaler. Etter fullført transkribering ble alle intervjuene analysert og kodet. Vi kodet det etter kontrollspakene i Simons rammeverket, for at funnene enklere kunne struktureres etter kontrollspakene. Videre la vi inn kommentarer hvis noe var nyttig å bemerke seg i henhold til funn og diskusjon. Vi har også benyttet fargekoder, for å kategorisere funn. Etter endt analyse ettersendte vi spørsmål vi følte var ubesvart til enkelte case-bedrifter, for å kunne svare bedre på problemstilling og forskningsspørsmål.

For å analysere datamaterialet fra spørreundersøkelsene benyttet vi nettskjema.no sitt verktøy. De tilbyr rapport av datamaterialet, som blir grafisk fremstilt. Ut fra rapporten kunne vi tolke dataen og videre sammenligne case-bedriftene. Ved spørreundersøkelsen til Alumni benyttet vi også av nettskjema.no. Spørreundersøkelsen var tilnærmet lik som til case-bedriftene, for å kunne sammenligne de to ulike utvalgene. Spørreundersøkelsen til Alumni ga mer datamateriale, som gjorde det vanskeligere å analysere siden informantene hadde mer spredte oppfatninger knyttet til cybersikkerhet. Utvalgene kombinert gjorde at vi treffer et bredt spekter av informanter.

3.7 Kvalitet i forskning og etiske avveininger

I dette kapittelet går vi nærmere inn på den etiske delen av forskningen. Vi skal videre presentere validiteten og relabiliteten knyttet til forskningen. Avslutningsvis fokusere på forskningsdesignet og datainnsamlingsprosessen.

3.7.1 Personvern og datahåndtering

I forskningen forholder vi oss til SIKT sine retningslinjer når det kommer til personvern. Før deltagelse i forskningen fikk alle informantene et informasjonsskriv med et samtykkeskjema. Her ble informantene informert om rettighetene sine og at de kunne trekke seg fra forskningsprosjektet, uten noe videre konsekvens. Ettersom vi skriver om et tema som er sårbart om det kommer i feil hender, så var det viktig å anonymisere. I hele oppgaven har case-bedriftene fått tildelt fiktive navn. For at de ikke skal være gjenkjennbare. Dette var en vurdering som ble tatt av oss og veilederne.

For å få gjennomføre forskningen behøvde vi godkjenning fra SIKT. Dette gjorde vi via TRANSACT-portalen i SIKT. Vi sendte inn intervjuguide, spørreundersøkelse og informasjonsskriv (vedlegg 1 - 7), og fikk raskt en godkjenning av prosjektet. Under forskningen har vi forholdt oss til TRANSACTs datahåndteringsplan.

3.7.2 Reliabilitet

Reliabilitet angår pålitelighet, og angir hvorvidt undersøkelsen viser den virkelige situasjonen. Videre i hvilken grad resultatet kan etterprøves. Relabiliteten måles i høy eller lav grad (Sander, 2022). Innenfor forskningen vår gjorde vi både kvalitativ og kvantitativ forskning. I vår forskning benyttet vi oss av Alumni som et utvalg, som representer tidligere studenter. Selv om vi fikk god respons fra spørreundersøkelsen, så foreligger det en mulighet for at andre respondenter kunne oppnådd andre svar enn oss.

3.7.3 Validitet

Validitet peker mot gyldighet og relevans. Den måler om forskningen faktisk måler det den skal måle (Sander, 2019). I all hovedsak vil resultatene i en undersøkelse vurderes som valid hvis de er fri for feil (Villasís-Keever et al, 2018). Når det kom til å ta dette i betraktning i vår oppgave, så har vi lagt til rette for at informantene skal finne et svaralternativ som appellerer til dem. Spørreundersøkelsen inneholdt en rekke ulike alternativer, og noen bokser med fri tekst slik at validiteten styrkes.

I oppgaven ble alle informantene gjort anonyme med hensikt å generere sannferdige svar fra våre informanter. Spesielt med tanke på at vårt tema kan oppleves som tabu, og at informanten ikke ønsker sitt navn offentliggjort (Thagaard, 2013, s.29). Gjennom denne tilnærmingen åpner vi opp for å innhente mest mulig virkelighetsnære svar.

3.7.4 Refleksjon rundt forskningsdesign og datainnsamling

I datainnsamlingen er det gjennomført semistrukturert intervju for case-bedriftene. Hvor vi har blitt kjent med hvordan designet er opp mot verdier, kontroll, visjon, informasjonsutveksling og grenser. Samtidig har vi fått innsikt i deres miljøs natur, teknologi, størrelse, struktur, strategi og nasjonale kultur, da det kan bidra til å forstå organisasjonen bedre (Chenhall, 2003 s.1). Hensikten med å snakke med flere ulike bedrifter vil være å kunne avdekke hva noen gjør rett og andre gjør feil. Da kan vi fremheve forskjeller som gjør at noen lykkes og andre ikke. Vi har en antagelse om at det er vanskelig å identifisere en metode som passer for alle virksomheter når det gjelder håndtering av cybersikkerhet. Men vi tror det er mulig å avdekke faktorer som bør vektlegges.

4.0 Funn

Dette kapittelet presenterer funnene fra forskningen. Funnene skal beskrive og analysere deres styringssystem opp mot Simons (1995) kontrollspaker med cybersikkerhet som kontekst. Funnene vil videre presentere bedriftens erfaring og håndtering av cybertrusler. Videre en diskusjon knyttet til ulike aspekter ved tjenesteutsettelse. Videre belyses utfordringer med cybersikkerhet og tiltak for fremtiden. Avslutningsvis presenteres statistikk fra spørreundersøkelsen med tilleggsutvalget Alumni.

4.1 Styringssystem

Funnene vi skal presentere i første del av kapittelet er delt inn i kontrollspakene til Simons (1995). Våre funn fra intervjuene vil dermed kategoriseres innenfor trossystemet, grensesystemet, diagnostiske kontrollmekanismer og interaktive kontrollmekanismer.

4.1.1 Trossystemer

Fra teorien ser vi viktigheten og kraften av et tilfredsstillende trossystem, hvor en gjennom verdier kan styrke jobben mot et felles mål (Simons, 2000) og ivaretakelse av cybersikkerheten. Med hensikt å bli bedre kjent med bedriftene, så stilte vi spørsmål angående deres visjon og verdier. Forskningen viser at majoriteten har visjoner og verdier, men med noe ulik tilnærming.

Et fellestrekk for bedriftene er at verdiene reflekterer hvordan en ønsker å bli oppfattet hos kunde og utad. Verdier som ærlighet, tillit og profesjonalitet er blant verdier som nevnes hos bedriftene. Men Regnskap AS trekker frem et større perspektiv, som viser til at bedriften bidrar til samfunnet.

> Regnskap AS*: "Dette handler om bærekraftig verdiskapning. Dette fører til et levende lokalsamfunn som er knyttet opp til lys i husene, sponsing av breddeidrett"*

IT - utviklere AS sine verdier fokuserer mer på bedriftens ytelse. Verdiene retter seg mot hvordan bedriften faktisk jobber. At de skal utfordre markedet ved bruk av ny teknologi, og at de skal holde seg oppdaterte. En kan trekke noen likheter til Studentservice AS i forhold til ønsket om hvordan det organisatoriske skal være, men med et større fokus på hvordan en oppfattes eksternt.

> Studentservice AS*: "Å hilse på hverandre når vi møtes og arbeidsmiljø. Men mye går på hvem vi er som organisasjon"*

Verdiene bidrar til å forme den organisatoriske atferden. Verdiene har dermed til hensikt å påvirke væremåten til de ansatte, slik at de er samkjørt med bedriftens ønske. Dette illustrerer sammenhengen mellom trossystemet og grensesystemet, hvor en sørger for at de ansatte ikke sklir ut fra organisasjonens rammer. Dette fører oss videre inn på viktigheten av balanse mellom kontrollspakene (Martyn, 2016). Vi observerer ulike tilnærminger når det kommer til verdiene. Men uavhengig av tilnærmingen bedriftene har, så gir det et bedre grunnlag for suksess (Simons, 1995).

Verdier må kommuniseres, slik at de blir implementert og forankret hos de ansatte. Vi observerer strategier som å ta verdiene opp i fellesskap, men også i onboarding prosessen. Studentservice AS valgte å gjennomføre en revidering av verdiene med ansattmedvirkning.

> Studentservice AS*: "Så da var det større diskusjoner om hvilke verdier vi setter pris på, hvorfor disse og hva betyr det å ha disse verdiene"*

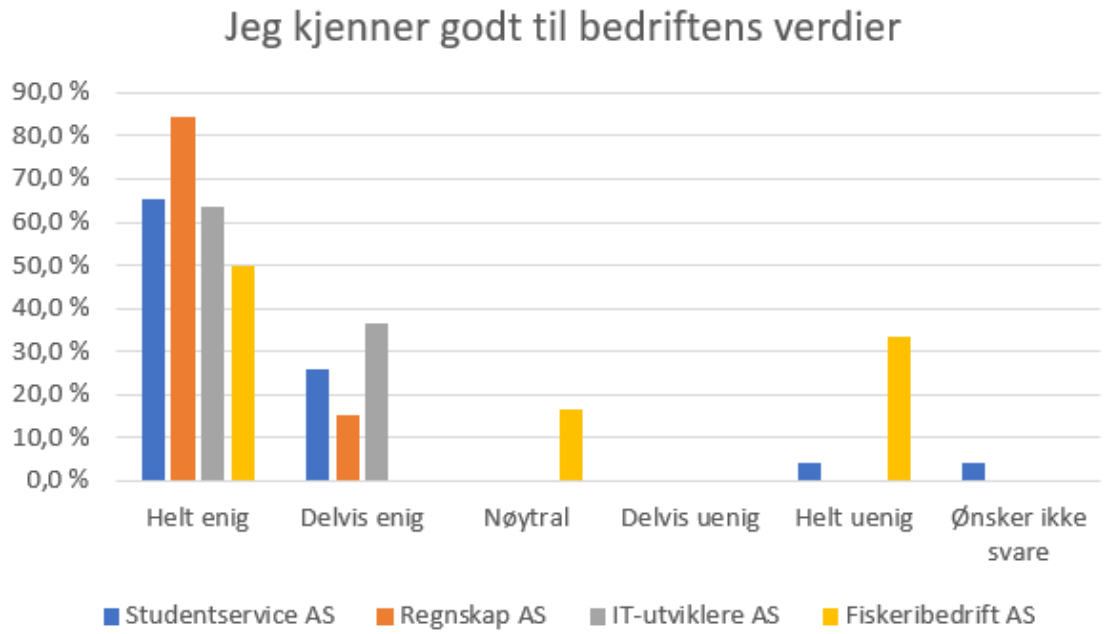
Dette kan ha positiv effekt i den forstand at ansatte får mer eierskap til verdiene, siden de blir inkludert og får en stemme i avgjørelsen. For Studentservice AS er verdiene også et viktig tema for de nyansatte, som skal bidra til å få dem inn i organisasjonens tankesett. Vi observerer en lik tilnærming hos IT - utviklere AS.

> IT - utviklere AS: "*Jeg har nettopp vært gjennom en rekrutteringsperiode for å ansette nye folk, og presentert det en del ganger"*

Dette viser til at verdiene konsekvent blir presentert, og muligens er det et viktig element i implementering av verdier hos ansatte. På en annen side legger ikke IT - utviklere AS skjul på at alle nødvendigvis ikke kan alle verdiene.

> IT - utviklere AS*: "Vi tar det opp på hvert allmøte." "Sånn at ansatte skal være kjent med dem, men jeg tror ikke alle kan de på rams sånn sett"*

For å kunne teste hvorvidt de ansatte kjenner seg igjen i påstander fra ledelse / IT. Så har vi gjennomført en spørreundersøkelse til de ansatte. Denne grafiske fremstillingen illustrerer ansattes kjennskap til bedriftens verdier. Vi ser at en høy andel av de ansatte er "helt enig" og "delvis enig" i at de kjenner til verdiene. Det har forekommet enkelt svar på "ønsker ikke å besvare" og "helt uenig". Men i den grafiske fremstillingen utgjør dette en så liten prosentandel at det ikke utgjør en graf. Vi vurderer det også som mindre relevant, da det realistiske bildet illustreres godt gjennom helt enig og delvis enig grafene.



Graf 1: Bedriftens verdier. Den grafiske fremstillingen viser svarene i prosent.

Verdiene knytter seg også opp mot selve visjonen til bedriftene. Dette belager seg mye på hva bedriftens ønsker å være og bli oppfattet som. Simons (1995) argumenter for at det ikke er nok at bedrifter har nedskrevne mål og visjoner. Disse visjonene må også vises direkte fra ledernes handlinger. Det er dette som skaper troverdighet både overfor kunder, men også for de ansatte. Regnskap AS viser til en viktighet rundt knyttet til oppfattelsen hos ansatte og kunder.

> Regnskap AS*: "Det er veldig viktig at vi "springer" til nærmeste telefon når kunden trenger oss. For å få de ansatte og kundene til å forstå at vi står til rådighet hvis det skulle trenges. Det er mest det vi søker etter"*

Fokuset på mennesker kan vi også gjenkjenne i IT - utviklere AS sin visjon. Samtidig har de ulikt fokusområde, hvor IT - utviklere AS retter fokuset mer mot bedrifter og næringslivet.

> IT - utviklere AS*: "Visjonen er at vi skal gjøre hverdagen bedre for personene som jobber i små og mellomstore bedrifter"*

Trossystemet er ofte med vilje gjort så bredt som mulig, slik at det påvirker større deler av organisasjonen (Simons, 1995). Ofte vil det være en lang vei å gå for å oppnå visjonen. Men på veien mot visjonen, så trekker Studentservice AS frem en viktig poengtering. Det handler om *hvordan* en skal klare å nå denne visjonen, og at en skal komme dit på rett måte i lys av verdiene.

> Studentservice AS*: "Så vi har en visjon for både hvor vi skal være, men også en visjon for hvordan type tjenester vi skal levere og hvor gode vi skal være, og hvordan vi skal komme dit"*

De overnevnte bedriftene har dermed et fokus på visjon som konsept, men det samme fokuset finner vi ikke hos Fiskeribedrift AS.

> Fiskeribedrift AS: "*Men sånn overordnet bedrifts visjon har vi egentlig ikke. Aldri tenkt på det"*

Oppsummert ser vi at majoriteten har veletablerte trossystem, men ingen har tydelig kobling til cybersikkerhet. Praktisering av denne kontrollspaken mot cybersikkerhet ville vært et element som kunne være veiledende for de ansatte, og dermed resultert i ivaretakelse av cybersikkerheten.

4.1.2 Grensesystemer

For å ivareta kontroll i virksomheten er det et behov for grenser. Disse vil hjelpe med å fortelle de ansatte hva de ikke skal gjøre og begrense forretningsrisikoen (Simons, 1995). Menneskelig atferd utgjør en unik risiko for en organisasjon, som ikke kan løses ved å investere i kompleks teknologi (Perez, 2020 s.29). Et tydelig grensesystem innenfor cybersikkerheten kan derfor redusere negative konsekvenser som cyberangrep medfører. Det er derfor svært relevant å stille spørsmål til case-bedriftene knyttet til grenser i arbeidshverdagen.

I hensikt å begrense benytter Studentservice AS mandater innenfor blant annet faktura, innkjøp og avtalesignering. De praktiserer også avdelingsmessige godkjenninger, hvor leder må godkjenne. Dette fungerer som en form for begrensning og kontroll for lederne. De bekrefter videre at de har egne prosedyrer for dem som har bestillingsmyndighet.

> Studentservice AS: "*Da har vi prosedyrer på alle som har bestillingsmyndighet*"

Denne type tilnærming med fokus på betaling og godkjenninger observerer vi også i Fiskeribedrift AS.

> Fiskeribedrift AS: "*Hvis vi ser på betaling for eksempel, så er det ingen som kan betale uten at det blir godkjent. Det er fire øyne prinsippet på alt*"

IT - utviklere AS har også noen klare grenser for de ansatte når det kommer til betaling.

> IT - utviklere AS*:* "Det *er rollestyrt, alt etter hvilken rolle en har. Det er ikke alle som har lov til å gjøre betalinger. Det er bare økonomisjef og sånt. Det er ikke fritt frem, om noen skal kjøpe noe må det gjennom leder. Som går som et godkjennings ledd"*

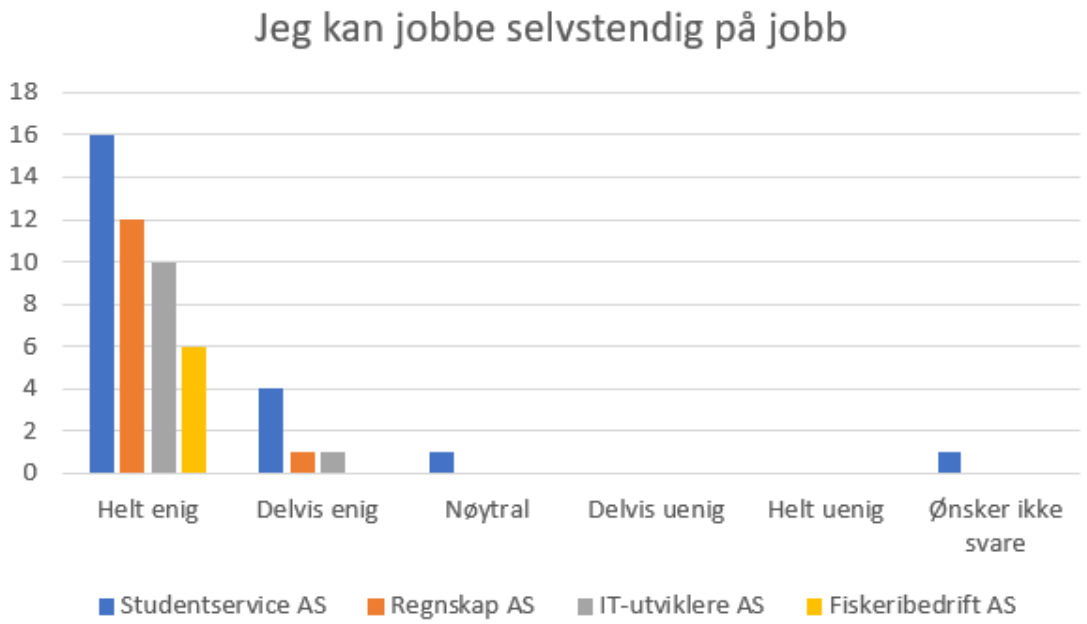
Når vi spør Regnskap AS angående begrensninger i form av myndighet, så trekker informanten fram at de opererer i forhold til Finanstilsynet og bokføringsloven. De opplever dermed ikke samme behov for kontroll i form av myndighet.

> Regnskap AS*: "Vår bransje jobber litt spesielt i forhold til andre. Vi har ikke så mye innkjøp i vår bedrift. Det er kundene våre som kjøper ting. Der har vi en policy om at vi ikke godkjenner betalinger for kundene våre, det må de gjøre selv. Måten vi opererer på er mye styrt av Finanstilsynet og bokføringsloven. For oss selv har vi derfor ikke hatt noe behov for det"*

De er dermed mer kontrollert av et høyere organ, som videre setter grenser for bedriften som helhet og ikke kun for de ansatte. Vi observerer dermed at majoriteten av begrensninger omhandler et økonomisk perspektiv. På en annen side viste Fiskeribedrift AS til andre begrensninger som må til for å fremme hensyn til medarbeiderne. De presenterer klare retningslinjer for hvordan ansatte kan oppføre seg på sosiale medier i arbeidstiden.

> Fiskeribedrift AS*: "Nei altså, med tanke på når dem her om bord og er på jobb. Hva som blir sendt derfra og ha respekt for sine kollega og ikke legge ut bilder. Det er en del policy. Men å være etiske for arbeidsplassen og dine kollegaer gjennom sosiale medier er viktig for oss"*

Dette begrenser dermed atferden til de ansatte, men virker å være nødvendig i lys av trivsel og bedriftens policy. Dette er ikke et funn vi har gjort hos de andre, men det kan skyldes at bedriftene tilhører ulike bransjer. Utenom ovennevnte tematikk, så praktiserte de ikke grenser for de ansatte.



Graf 2: Selvstendighet på jobb. Den grafiske fremstillingen baserer seg på antall personer, som har svart på hvert enkelt alternativ.

Som illustrert i diagrammet ovenfor ser en at majoriteten av de ansatte føler at de kan jobbe selvstendig i jobben sin. Dette gjenspeiler det inntrykket vi satte igjen etter intervjuene med lederne til de ansatte. De fleste hadde den oppfatningen av at de ansatte hadde stor arbeidsfrihet og handlingsrom til å utfolde seg. Vi kan dermed bekrefte en samvariasjon mellom intervjuet og spørreundersøkelsen. På den ene siden skaper dette autonomi, som er en viktig egenskap for å lykkes.

Oppsummert ser vi at flere av case-bedriftene ikke viser til tydelig grensesystemer i forhold til cybersikkerhet. Dette skaper en forventning og tillit til at de ansatte skal håndtere trusler riktig. Et tydelig grensesystem innenfor cybersikkerhet skaper rammer, som kan gjøre både ansatte og bedriften tryggere.

4.1.3 Diagnostiske kontrollmekanismer

Det diagnostiske systemet representerer måling av ytelse og fungerer som en tilbakemelding på kontroll (Simons, 1995). I et cyberperspektiv ble det derfor nyttig å spørre case-bedriftene angående deres tilbakemelding og måling av ytelse hos ansatte. Gjennom intervjuene har vi blitt gjort kjent med at ved tjenesteutsettelse mottar bedriftene rapporter.

De får konkrete sikkerhetstiltak og konstante anbefalinger, som kan knyttes opp mot å oppdage feil og tilbakemelding. Vi kan dermed påstå at tjenesteutsettelse tar en stor rolle i den diagnostiske kontrollmekanismen. Bedriftene bruker derfor denne kontrollspaken som et hjelpemiddel, for å utarbeide et grunnlag til forbedring av cybersikkerheten.

Studentservice AS bruker sin leverandør som en sparringspartner, hvor de også får tilbakemeldinger som kan identifisere om systemet må forbedres. Dette gir bedriften en klar indikasjon på hvordan ytelse sikkerhetssystemene deres har.

> Studentservice AS*: "Så har vi leverandør som er vår driftspartner, som gjør sikkerhetsanbefalinger, skanner systemene våre kvartalsvis for angrepsflater, spesielt servere og sånne ting"*

Regnskap AS har i likhet med store deler av de andre bedriftene benyttet seg av tjenesteutsetting av IT-tjenestene sine. Men for å forsikre seg om at tilbudet er nødvendig, så har de benyttet seg av en ekstern part til å se over tilbudet.

> Regnskap AS: *"Vi har jo en leverandør på IT-løsningene våre som vi har regelmessig kontroll med. Men i dette tilfellet så følte vi at det de fortalte oss burde vi få sjekket ut. Så det blir litt som i revisorbransjen. Så vi fikk en IT-revisor til å gå gjennom å se at det vi drev med var fornuftig*"

Regnskap AS fortsetter med at de ser videre på en løsning der de får tilbakemelding fra systemet.

> Regnskap AS*:* "*Også driver vi også å vurdere SOC-løsning. Altså at man monitorer enheten, med et varselsystem. Som da varsler de som har peiling på cybersikkerhet. Per nå har vi kontroll på alle enheter, så vi har kontroll på det hvis noe skjer. Men vi ønsker å få på plass en slik «SOC» Security Operation Center. Da tar man det et nivå opp"*

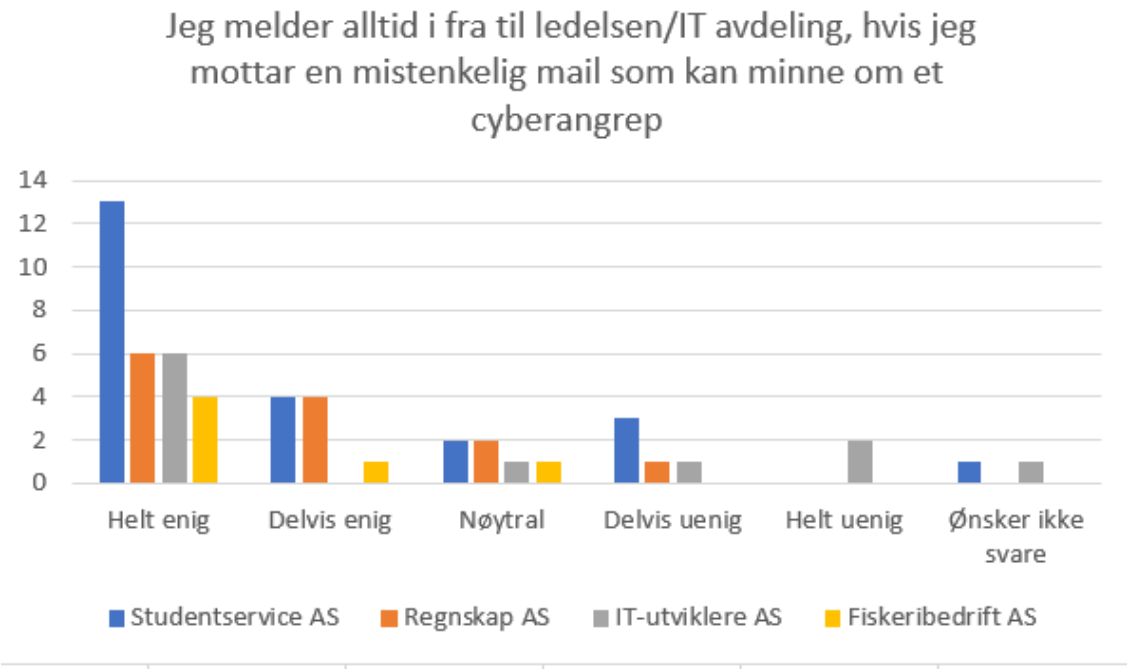
Studentservice AS har en tilsvarende løsning, hvor de får tilbakemelding fra systemet. Det vil derfor varsles hvis det kommer e-poster fra avsendere, som har tilnærmet lik e-postadresse som det vanligvis kommuniseres med. Dette gjør at de ansatte ikke blir like sårbar for "dårlige" svindelforsøk.

> Studentservice AS*: "Så har vi en innstilling i 365, som ser tilnærmet like e-post adresser, og dermed varsler. Man får dermed en stor advarsel. De som mottar e-posten, vil se det. Hvis resten matcher og det ser ut som et impersonation forsøk"*

Kostnadene ved å ansette noen internt til den tilsvarende jobben som tjenesteutsettelse gjør er ganske betydelig. Dette er noe IT - ansatt trekker frem:

> IT - ansatt*: "Dyrt i den forstand at folk har ekstremt høye lønninger, at du kanskje ikke har råd i en liten bedrift til å ansette en som forventer en årslønn på 1.2 millioner for å gjøre en grunnleggende jobb innafor sikkerhet"*

Fra de ansattes perspektiv ble de under spørreundersøkelsen spurt om de meldte ifra, hvis en mistenkelig e-post kunne minne om et cyberangrep. Vi kan observere at det var spredte svar fra alle bedriftene.



Graf 3: Tilbakemeldingskultur. Den grafiske fremstillingen baserer seg på antall personer, som har svart på hvert enkelt alternativ.

Spørreundersøkelsen viser at ansatte melder ifra til ledelse/IT. Men svarene kan tyde på forskjeller mellom hva de ansatte mener er relevant å melde ifra om. Dette kan knyttes opp til hver enkeltes oppfatning av cybertrusler, og hva som faktisk utgjør en risiko.

Etisk hacking ble også trukket fram som en effektiv metode av flere av ekspertene. Men ingen av bedriftene valgte å benytte seg av denne metoden.

> IT - utviklere AS*: "Vi har ikke gjort noe social engineering. Det hadde sikkert vært interessant, men"*

Regnskap AS begrunner valget med å ikke benytte seg av etisk hacking, som et resultat av at det kan føre til en del andre uønskede effekter.

> Regnskap AS*: "Vi har ikke gjort dette enda. Jeg tror vi kommer ganske langt med de tiltakene vi har gjort nå. Jeg har selv vært utsatt for test-e-poster og det er klart det kan være lærerikt, men det kan også føre til en del andre effekter man ikke ønsker. Så*

jeg tror mer på å ha arkene, kursene og planen klar. Slik at alle kommer opp på et høyt nok nivå"

Ekspertene vi har snakket med har også hatt noen innvendinger om bruken av etisk hacking som verktøy.

Informant: "Det er delvis utbredt, sånn personlig er jeg litt skeptisk til det, fordi man skal være ryddig i hvordan det gjennomføres for å på en måte ha etikken på sin side. Hvis det går på at man på en måte «lurer» ansatte, så kan jo det være ubehagelig for de som jobber der"

Oppsummert ser vi at majoriteten av case-bedriftene tjenesteutsetter cybersikkerheten til en leverandør. I lys av dette kan det skape en avhengighet til leverandøren som gjør at man risikerer å miste kontroll og kunnskap internt.

4.1.4 Interaktive kontrollmekanismer

Denne kontrollspaken er knyttet til personlig kontakt og informasjonsutveksling. Ved god informasjonsutveksling kan selskapet komme nærmere gjennom oppmuntring til en informasjonsstrøm fra de ansatte til topplederne (Kruis, et al., 2016). Disse fordelene er også av betydning i håndtering av cybertrusler. Derfor spurte vi bedriftene spørsmål angående kommunikasjon og informasjonsflyt mellom de ansatte og ledere. En tettere og mer informert bedrift vil også være bedre egnet til å selv kunne forstå omfanget av cybertrusler og selv håndtere dem.

Bedriftene i forskningen jobber med ulike fagfelt og er dermed organisert ulikt. Dette påvirker også hvordan de kommunisere med hverandre. Halvparten av bedriftene har operative avdelinger. Hos disse kan vi se at kommunikasjonen preges av mer personlig kontakt, og at generell informasjon deles i form av fysiske møter.

Fiskeribedrift AS: "*Cybersikkerhet en del av sikkerhetsstyringssystemet. Så det blir gått igjennom i revisjon og da er de ansvarlige på båtene som deltar i det møtet, og så blir det tatt møte med hele mannskapet om bord. Vi går igjennom når vi har oppdatert etiske retningslinjer og varslinger"*

En annen faktor som gjør det interaktive systemet svært relevant for cyberangrep er systemets oppbygning. Det kan endres etter hvert som markedet og verden utvikler seg. Når det gjelder formidling av informasjon internt i administrative avdelinger brukes ulike kommunikasjonsverktøy. I lys av cybersikkerhet, ser en at enkelte bruker også verktøyet for å informere de ansatte rundt cybersikkerheten.

> IT - utviklere AS*: "Det kan være at folk blir nedringt av spanske nummer eller får samme type e-post. Da bruker vi å gå ut å informere alle på "SLACK" om at man må være litt obs. At det har vært mye telefoner eller e-poster. Vi prøver å dele slik kunnskap så fort som mulig"*

Regnskap AS bruker et annet kommunikasjonsverktøy, men bruker det også iblant til å informere eller oppdatere de ansatte angående cybersikkerheten.

> Regnskap AS*: «Vi har «Workplace» som verktøy som blir mye brukt til å kommunisere ut intern informasjon. Og noen ganger så gjelder dette IT-sikkerhet"*

Regnskap AS belyser likevel at det finnes delte meninger til bruken av kommunikasjonsverktøyet. Videre at det kan være utfordrende å nå ut til de en ønsker.

> Regnskap AS*: "Men det er klart at det er ikke alle som til enhver tid sjekker «Workplace», og det er delte meninger om hvor ofte man burde sjekke det. Og de som man helst aller helst ønsker å nå ut til, er ofte de som leser det sjeldnest. Målet er ikke å gjøre de beste bedre, men heller å få de dårligste bedre"*

Ved tettere oppfølging av lederen, så får man en større innvirkning på de ansattes arbeidsvaner (Simons, 2010, s. 158). Noen av bedriftene er geografisk spredt, og flere av bedriftene reflekterer rundt dette. Regnskap AS kan fortelle at de lokale kontorene eksponeres for mer informasjonsstrøm mellom ansatte og ledere.

> Regnskap AS*: "På de lokale kontorene så er terskelen lavere for å snakke med ledelsen. Det meste går via daglig leder og team leder"*

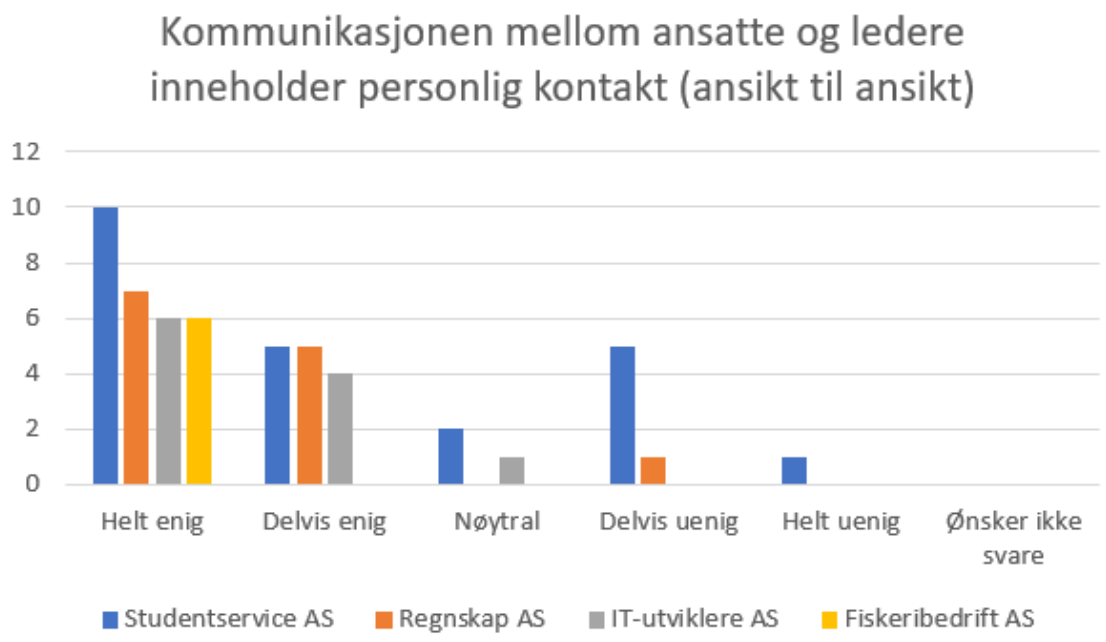
Dette støttes av Studentservice AS, som stort sett har personlig kontakt, men uttrykker videre at det naturligvis er en utfordring, når en har kontorer spredt rundt i landet.

> Studentservice AS*: "Det er litt vanskelig det geografiske med 7 byer. Det er lettere på en liten avdeling å ha personlig kontakt, men nå blir det jeg som er et mellomledd"*

Kommunikasjon via hverandre kan dermed oppleves ineffektivt. Dette fører til at Studentservice AS har automatisert repeterende formaliteter.

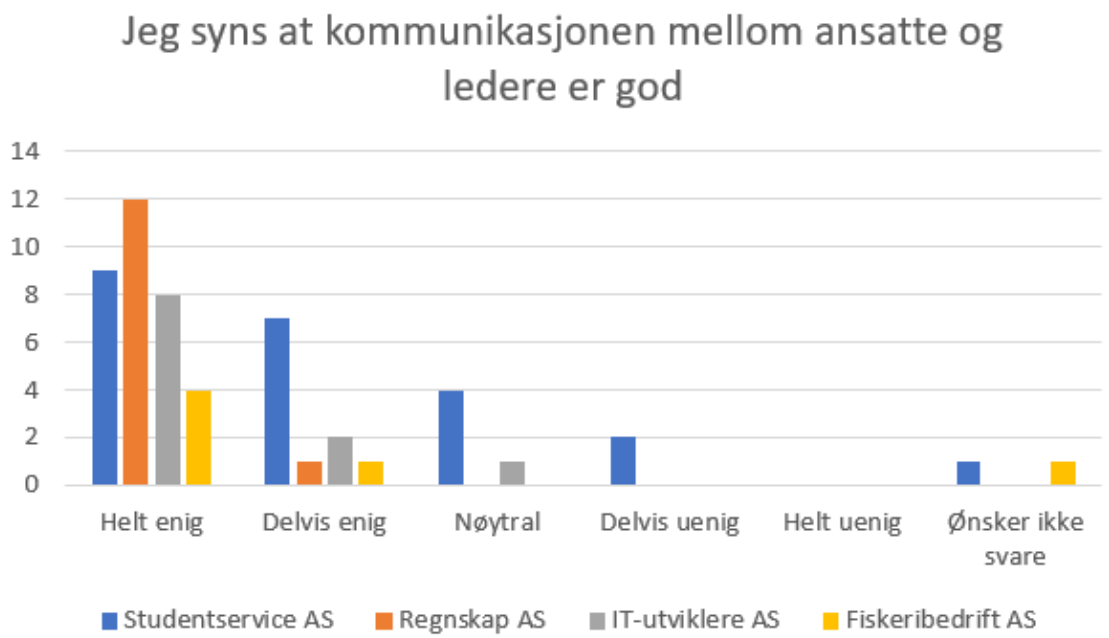
> Studentservice AS*: "Istedenfor å spørre, så får man mer formelle bestillinger og forbedrer kommunikasjonsflyten"*

For å skape et mer nyansert bilde, så spurte vi de ansatte spørsmål som var relatert til den interaktive kontrollspaken. Grafene som presenteres er knyttet til hvorvidt det foreligger personlig kommunikasjon, og om de mener kommunikasjonen er god.



Graf 4: Personlig kontakt. Den grafiske fremstillingen baserer seg på antall personer, som har svart på hvert enkelt alternativ.

Grafene viser ansattes mening opp til påstanden om at ansatte og ledere har personlig kontakt. Vi kan observere en overvekt på "helt enig" i alle bedriftene. Det er helt samkjørt i Fiskeribedrift AS, mens det foreligger delte meninger hos Studentservice AS. Muligens kan dette skyldes at en hører til ulike avdelinger, og har forskjellige stillinger.



Graf 5: Kommunikasjon mellom ansatte og leder. Den grafiske fremstillingen baserer seg på antall personer, som har svart på hvert enkelt alternativ.

Når det kommer til de ansattes oppfatning om at kommunikasjonen er god mellom ansatte og ledere, så ser man noen tydelige forskjeller tvers case-bedriftene. I lys av cybertrusler er denne kontrollspaken viktig for å samkjøre ansatte og bedrift. En etablert plattform og informasjonsstrøm knyttet til cybersikkerhet er avgjørende for en vellykket håndtering.

4.2 Erfaring og håndtering av cybertrusler

For å få bedre forståelsen av bedriftenes situasjon rundt cybertrusler, så skal vi kort presentere bedriftenes erfaringer. Felles for bedriftene er at de alle har opplevd svindelforsøk i form av phishing. Da er det som regel innenfor direktørsvindel, hvor svindlere utgir seg for å være CEO eller lignende. På det jevne utsettes majoriteten for spam e-poster, men med ulik hyppighetsgrad. Noen bedrifter har fått falske fakturaer, men også mer alvorlige tilfeller i form av løsepengevirus på en gammel server og hacking av pc. Men ingen har opplevd å bli svindlet. Når det kommer til forsøkene, så er det variasjon i hvor sofistikerte de opplever at cyberangrepene er.

4.2.1 Tjenesteutsetting som strategi

For å få innsikt i bedriftenes håndtering av cybertrusler opp mot cybersikkerhet, så stilte vi spørsmål angående deres strategi knyttet til et eventuelt angrep. Majoriteten av bedriftenes strategier kjennetegnes av tjenesteutsettelse. Men alle bedriftene har fortsatt sine særtrekk, som er med på å forme deres håndtering av cybertrusler. Vi opplever at noen strategier domineres av tjenesteutsettelse, mens andre har en mer proaktiv tilnærming internt. Grunnet bedriftenes ulike størrelser, opplever vi ulikheter i antall IT-arbeidere i bedriftene. Vi kan observere at de mer "ressurssterke" innenfor IT internt har mer overskudd til å gjøre cybersikkerhetsrelatert arbeid innad i bedriften. Mens de som har tjenesteutsettelse avhenger at den eksterne leverandøren gjør arbeidet.

I motsetning til de andre bedriftene, så benytter ikke IT-utviklere AS seg av tjenesteutsetting. Dette medfører at det stilles høyere krav til ressurser som skal kunne suppleres til vedlikehold av cybersikkerheten. Internt tvinges de dermed til å være mer årvåken i lys av denne problematikken.

> IT - utviklere AS*: "Vi er proaktive. Vi holder hele tiden på å forbedre rutinene. Å sperre ned det vi kan sperre ned tilganger. Sørge for å ha nok beskyttelse foran våre systemer. Slik vi kan håndtere det på en fornuftig måte"*

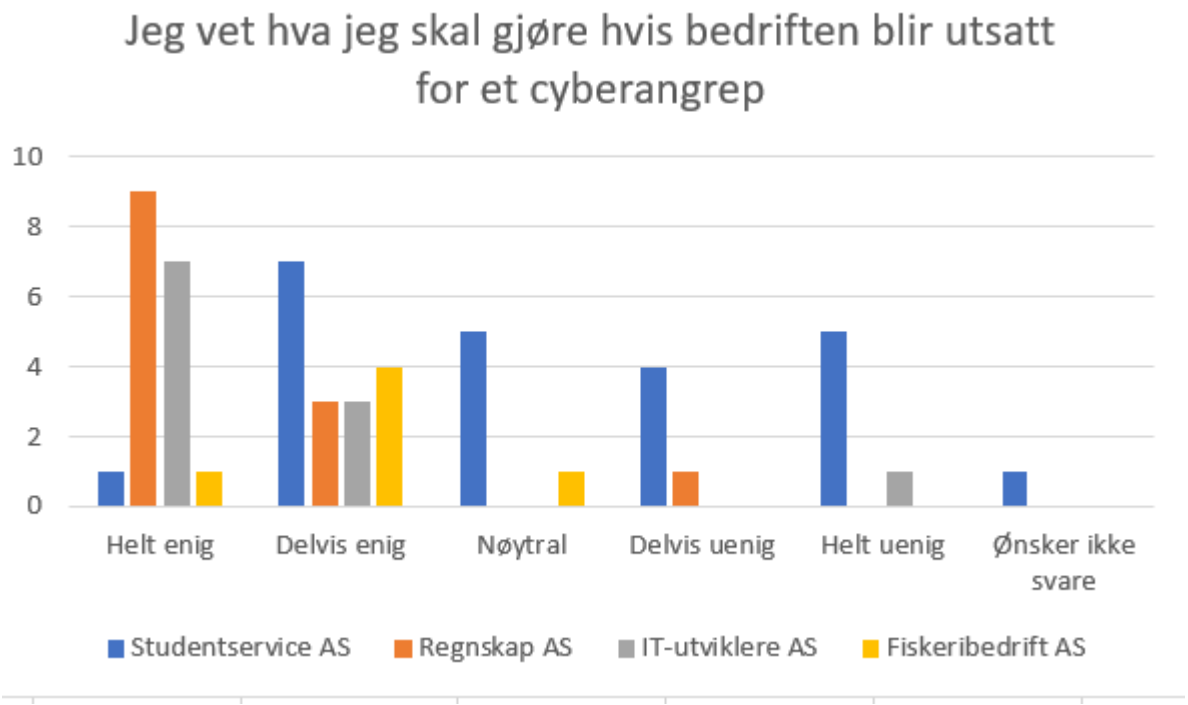
Regnskap AS har en kombinasjon av internt og eksternt arbeid av cybersikkerheten. De har en egen IT avdeling internt, tjenesteutsetting og tredjeparts IT revisor. I forhold til hva de skal gjøre hvis de blir utsatt for et cyberangrep, så har de ansatte et eget ark med fremgangsmåte på pulten sin.

> Regnskap AS: *"Det arket her er rekkefølgen på hva man skal gjøre. Starte med å varsle, og stegene forklart. Dette er min plan som er litt mer avansert enn de ansattes plan. De vanlige ansatte skal ikke begynne å håndtere situasjonen og gjenopprette. De skal bare varsle ... Så står det diverse nummer de kan ringe … Vår leverandør, Politiets nasjonale cyberkrimsenter, Nasjonal cybersikkerhet, Økokrim"*

Fiskeribedrift AS har en beredskapsplan, men vektlegger tjenesteutsetting. Man kan her trekke likheter opp til Studentservice AS, hvor strategien deres er å følge den eksterne leverandøren sin plan og retningslinjer. Videre mener de at de mangler egne prosedyrer, men at temaet er på agendaen i nær fremtid.

> Studentservice AS*: "Men vi har stort sett på alle systemer en ekstern aktør som jobber med dette på et helt annet nivå og har retningslinjer på hvordan man skal gå frem. Vi har ikke definert egne"*

Ansattes kunnskap knyttet til håndtering av cyberangrep gir en indikasjon på hvorvidt strategien fungerer. Ut fra den grafiske fremstillingen ser vi at ansatte i Studentservice AS mangler kunnskap om hva de skal gjøre hvis de blir utsatt for cyberangrep. Dette kan skyldes at de tjenesteutsetter og har lite IT kunnskap internt. Men også at tematikken er dårlig kommunisert i dag og skal komme på agendaen i fremtiden. På den andre siden viser Regnskap AS en høy andel som er helt enig, og gir en indikasjon på at en kombinasjon av tjenesteutsettelse, intern IT kompetanse og tredjeparts revisor er vellykket.



Graf 6: Rutiner med cyberangrep. Den grafiske fremstillingen baserer seg på antall personer, som har svart på hvert enkelt alternativ.

4.3 Tjenesteutsettelse av cybersikkerhet

Vi skal gå mer i dybden på tjenesteutsettelse problematikken, siden det er et sentralt funn for majoriteten av bedriftene. Dette var noe vi også har fått bekreftet av de ekspertene vi har snakket med.

> PhD stipendiat*: "Så jeg vil si at det er veldig normalt å tjenesteutsette cybersikkerhet"*

Dette støttes av Wilson (2022), hvor SMB sin mangel på ekspertise internt resulterer i at en søker tjenesteutsetting eksternt. Likevel ser det ut som at intern kompetanse er særlig viktig i vellykkede tiltak (Wilson et.al, 2022 s. 398). Videre skal vi presentere sentrale elementer knyttet til tjenesteutsettingen.

Høye kostnader og tillit til leverandør

Fiskeribedrift AS gikk for to år siden over til å tjenesteutsette alt av cybersikkerhet. Dette kom som et resultat av at de merket det økende fokuset på cybersikkerhet, og at de følte de trengte mer kompetanse for å sikre seg.

> Fiskeribedrift AS*: "Bedrift X fikk se på det, og kom med et tilbud der de skiftet ut alt og la alt opp i skyen. Det var sånn det kom. Vi måtte ha nye servere fordi det var et puslespill av servere fra tidligere"*

Studentservice AS benytter seg også av en ekstern leverandør for å vedlikeholde og kontrollere systemene deres.

> Studentservice AS*:* "*Bedrift X er vår IT-driftspartner, så de drifter våre servere og nettverk. Vi har ikke mulighet til å gjøre det med 1 person, så de har da konstante sikkerhetsanbefalinger. Men så må jeg inn å si ja til alt da"*

Dette bekrefter problematikken til SMB i form av at manglende ressurser er en faktor. Samtidig er vi blitt gjort kjent med at kostnaden ved å tjenesteutsette cybersikkerhet er betydelig for SMB, men sikringen oppleves som en nødvendighet.

> Fiskeribedrift AS*: "En ting er at det er dyrt. Samtidig så skjer det så mye at du greier ikke, hvis du er en relativt stor bedrift og skal ha ansvar for IT sikkerhet, samtidig følge med på hva som skjer. Det er klart det er dyrt, det er blitt en dyr fast kostnad, vi må bare ha det så det er enkelt …. Vi bruker ganske mange hundre tusener. Så har vi såpass tillitt til dem"*

Ut fra intervjuene virker det som flere av bedriftene utviser svært høy tillit til sine leverandører. De forteller at de stoler på leverandøren og noen prøver å stille kritiske spørsmål. Til tross for dette ender case-bedriftene i praksis opp med en relasjons basert på tillit, selv om de har et ønske om kontroll.

> PhD stipendiat: *"Og dilemmaet om de ønsket tillit eller kontroll over en leverandør. Der valgte alle kontroll, men det er jo tillit man ser i praksis. Og grunnen til det er at man ikke har ressurser eller kompetanse til å stille de riktige spørsmålene til leverandøren. Så dem har på en måte bare den opparbeidete tillitten til systemet, og ikke til selve bedriften. Alle andre gjøre det så da kan man liksom anse det som trygt"*

Hos flere av bedrifter virker det som en effekt av tjenesteutsetting er ansvarsfraskrivelse knyttet til cybersikkerhet. Videre at det ikke reflekteres noe rundt verken det eller leverandørens kommersielle intensjon. Regnskap AS derimot har en mer kritisk tilnærming til tjenesteutsettelse og viser til refleksjon rundt tillit. De benytter en tredjepart IT revisor for å se over tilbudet, og får da bekreftet utenom en kommersiell kontekst om tilbudet er relevant for bedriften.

> Regnskap AS: *"Vi har jo en leverandør på IT-løsningene våre som vi har regelmessig kontroll med. Men i dette tilfellet så følte vi at det de fortalte oss burde vi få sjekket ut. Så det blir litt som i revisorbransjen. Så vi fikk en IT-revisor til å gå gjennom å se at det vi drev med var fornuftig"*

Regnskap AS sammenligner tjenesteutsettelse med en form for forsikring, og viser at en ikke nødvendigvis tar problemet innover seg grunnet manglende kunnskap. Dette tar oss tilbake til den indre kognitive konflikten knyttet til cybertrusler, som resulterer i at en distraherer seg fra problemet. Dette grunnet at det skaper en negativ effekt (Wilson, 2022 s. 398). Samtidig synes det at bedriftene som har mindre ressurser innenfor IT ikke har noe annet valg enn tjenesteutsette. Regnskap AS viser derimot til refleksjon rundt problematikken, og trekker frem at mangelen på kompetanse vanskeliggjør å ta selvstendige avgjørelser.

> Regnskap AS*: "Det er også noe systemkritikk her som jeg syns dere burde ta fatt i. Det blir litt det samme som å selge forsikring … Også kommer en sikkerhetsekspert som sier at du må investere en million i dette nye systemet som sikrer deg mot det ene og andre. Når du kjøper disse tjenestene så er du virkelig på herrens mark, for da aner du virkelig ikke hva du har. For når noen anbefaler en løsning så kan det være vanskelig å si imot det. Hvis du kjøper en bil for eksempel så er det litt enklere. Da vet du hva du har behov for … Men innen IT-sikkerhet så har du ikke peiling. Der tror jeg det er mange som ikke tar tak i det eller gidder å ta det innover seg. Det blir litt som i luksusfellen hvor de lar være å åpne alle regningene"*

Kommersiell industri - Har tjenesteutsettelse gått for langt?

Vi har blitt eksponert for cybersikkerhet og tjenesteutsettelse som en kommersiell industri. I likhet med andre bransjer er også IT-bransjen ute etter å tjene mest mulig penger.
Vi observerer at bedriftene mener at denne type investering er helt nødvendig. Potensielle konsekvenser ved å ikke være sikret er katastrofale. De er dermed svært villige til å bruke mye penger på cybersikkerheten, men det er ikke til å legge skjul på at leverandørene skal tjene penger. For å belyse ulike perspektiver på dette, så presenterte vi våre tidligere funn fra intervjuene til en ekspert med kunnskap innenfor tjenesteutsetting.

PhD stipendiat mener at tjenesteutsettelse har gått for langt, og at det har blitt en hvilepute for mange bedrifter.

> PhD stipendiat: *"Men jeg ser en tendens med dem jeg har snakket med til nå at flere ser på muligheten til å få litt mer in house kompetanse og ikke være naiv og tenke at alle vil oss godt. Og da kan man prøv og dra litt konklusjoner om tjnesteutsetting har utbredt seg for mye og at det er blitt litt for vanlig"*

Dette er noe vi har sett en tendens til hos nesten alle bedriftene vi har snakket med. De tjenesteutsetter tjenester, fordi de ikke har kunnskap eller ressurser til å håndtere det selv. Men det tyder på at det har blitt en farlig hvilepute for mange. Dette har gjort bedriftene veldig avhengig av leverandørene. PhD stipendiat trekker også inn at dette er en bevisst strategi av leverandøren, for å gjøre bedriftene veldig avhengig av systemene deres. Vi ønsket å grave litt dypere rundt dette, og stilte derfor ekspertene spørsmål rundt bruk av en tredjepart for å vurdere validiteten ved tilbudene.

> PhD stipendiat*: "Men tredjeparts er jo selvfølgelig en måte å forsikre seg på at man ikke er blitt lurt eller har tatt dumme valg. Da får man en situasjon som kalles en «vendor lock in effekt». At du har blitt helt låst til leverandøren din. For det er jo det gjerne som leverandør har som mål på sikt, altså at du investerer i en tjeneste"*

Leverandørens perspektiv

Leverandører tilbyr ulike forsikringspakker, som kan tilpasses til bedrifters behov. Vi spurte en leverandør av tjenesteutsettelse av IT-sikkerhet om hvorvidt de pusher på løsninger til kundene sine.

> IT - leverandør*: "Nei. Vi belyser trusselbildet, også legger vi frem løsninger for å begrense det. Hvordan det blir lagt fram tror jeg er opp til dagsformen på selger. Men jeg hører ofte folk som kommer til oss og sier vi skulle hørt på dere. Dette ble dyrt. Jeg syns ikke vi er nok flinke til å fortelle hvor mange som blir hacket, og hvor kjipt det er. Men vi ønsker ikke å overselge noe til kundene. Vårt spørsmål til alle er å finne ut hva verdiene deres er verdt også kan vi bygge en sikkerhetsløsning som er avhengig av hva du ønsker å sikre"*

En av våre eksperter viser til samme antakelse, hvor informanten er sikker på at aktørene i Norge ikke ønsker å overselge.

> IT - ansatt*: "Ofte er det snakk om betydelige summer, og ofte er det pakke-tjenester, men også times fakturerte tjenester. Jeg er ganske sikker på om en drar til en av de store aktørene i Norge, så er ikke de interessert i å selge noe som er "overkill". Det handler om å tilpasse løsningene til formålet"*

På en annen side viser leverandøren til at du fortsatt har ansvar, og det kan være en faktor som forsvinner i tjenesteutsettelse.

> IT - leverandør*: "Men selv om du kjøper en tjeneste så er det fortsatt bedriften sitt ansvar, men du vet at det blir tatt vare på av noen andre som kan IT-sikkerhet"*

4.4 Utfordringer knyttet til cybersikkerhet håndtering

Gjennom forskningen vår har vi blitt gjort kjent med en rekke utfordringer knyttet til SMB sin håndtering av cybertrusler. For å kunne bidra til forskningsfeltet, så vurderer vi det som avgjørende å trekke frem sentrale utfordringer. Derfor vil vi videre utheve utfordringer, knyttet til kompetanse, ressurser og opplæring.

Kompetanse og ressurser

For å kunne håndtere cybertrusler er det behov for kompetanse og ressurser. I sammenheng med SMB opplever vi at dette er en utfordring, siden de ikke har overskudd til å fokusere på beredskapen knyttet til cybertrusler.

> Akademisk ekspert: *"De står i skvis da på den ene siden, de vet at de må ha god beredskap, på en annen side så mangler de folk og kompetanse til å nettopp ha det"*

Vi har blitt gjort kjent med at flere av bedriftene benytter tjenesteutsettelse som en mulighet. Muligens kan dette forklares med at det er utfordringer knyttet til å skaffe den riktige kompetansen internt.

> Akademisk ekspert: *"Virksomheter har trøbbel med å skaffe ansatte som har den type kompetanse "*

Fiskebedriften nevner også den samme problematikken. Informanten trekker frem at for SMB er det for komplekst å håndtere alene, men det er utfordrende å få tak i folk internt.

> Fiskebedrift AS: "*Vi ikke har særlig intern kompetanse på cyber og IT sikkerhet … Det begynner å bli ganske komplekst dette her. Du skal ha ganske flinke folk, og det er det vanskelig å få tak i …. En ting er at du kan litt, men for å ha nok kompetanse så, så er det vanskelig å få folk og du må ha en litt større organisasjon"*

Kombinasjonen av fagfeltets kompleksitet og anskaffelse av riktig kompetanse internt gjør det utfordrende. Det er krevende å skaffe seg likeverdig kompetanse. Samtidig som den fraværende kunnskapen fører til at en tjenesteutsettelser for å sikre seg. Det oppleves som vanskelig å ta selvstendige valg innenfor tjenesteutsetting grunnet mangelfull kjennskap til fagfeltet. Vi ser tendenser til at ansvaret flyttes til IT avdeling eller tjenesteutsetting. Noe som kan resultere i at de resterende ansattes opplæring innenfor cybersikkerhet faller fra.

> Studentservice AS: *"Ved større hendelser, så føler vi instrukser til leverandøren, i mindre hendelser, hvis noen skal begynne å betale ut, da vi interne rutiner, men det er ikke noe vi har informert alle ansatte om"*

Det indikerer at tjenesteutsettingen kan svekke kompetansen internt. Ved å "kjøpe seg trygghet" kjenner en muligens mindre på behovet til å informere alle ansatte.
I denne sammenheng er mangelen på kunnskap og forståelse en tydelig barriere. Både menneskelige og digitale ressurser er viktig. I likhet med kompetanse, så trekkes cybersikkerhet også som utfordrende å få tak i.

> IT leverandør: *"Det er veldig få ressurser som kan IT-sikkerhet, det er en mangelvare"*

Flere av de SMBene har ikke mulighet til å sette av ressurser til cybersikkerheten. Det kan dermed oppleves som umulig å bygge egne avanserte systemer. Men også arbeid knyttet til vedlikehold og oppdatering av trusselbilde. Likevel trekkes problematikken knyttet til SMB sitt fokus på dette. De mindre bedriftene har mer fokus på det de produserer, og ikke på cybertrusler.

> IT- utviklere AS: *"Jeg tror ikke folk er åpen om det, for det går jo på omdømme til bedriften, og rutinene de har på plass. Så er det det å sette av nok ressurser til kunne oppdatere det å gjøre forhåndsarbeidet for å sikre. Jeg tror ikke alle har fokus på det. Jo mindre bedriften er jo mindre fokus blir det på å kun fokusere på det en produserer. En tar seg ikke råd til å operere sikkert"*

Opplæring

Innenfor opplæring trekkes det menneskelige perspektivet frem. Det er observert at valgene til individene påvirker utfallet av angrep. Siden vellykkede angrep ofte starter med feil beslutninger fra et individ (Economist, 2019 s.52). Viktigheten rundt det menneskelige aspektet innenfor suksessfulle cyberangrep, har blitt tydeliggjort under forskningen. Videre at en blir hacket gjennom mennesker.

> Akademisk ekspert: *"Så det er rett og slett den menneskelige, dårlig dømmekraft. Det er ikke bare dårlig dømmekraft, selv de beste blir lurt, men det går gjennom vår hjerne at vi blir lurt som mennesker, og vi åpner da døren inn i våre systemer, som da blir infisert av angrepet. Det er nr. 1, gjennom mennesker"*

Dette presiserer viktigheten av god opplæring hos de ansatte. Videre forteller en av ekspertene om utfordring i form av språkbruk under opplæring. Innenfor IKT bransjen brukes vanskelige ord og uttrykk, som gjør at ansatte ikke forstår hva som blir sagt under opplæringen.

> IT- ansatt: *"Jeg tror den største feilen vi som jobber med informasjonssikkerhet gjør er at vi snakker et språk som brukerne ikke forstår. Vi er så dypt inn i vår egen verden, vi har en terminologi vi bruker oss imellom som gir mening. Men i det du går til noen som jobber med lønn, HR eller andre og du begynner å prate om fagspråket (sosical engineering, ransomware) så går det bare rett over hodet uansett. Noe vi har jobbet veldig mye med er å snakke et språk andre faktisk forstår, klar tale"*

Videre påpekes det at opplæringen ikke trenger å være komplisert, og at videoblogg konsept kan fungere som et verktøy. Samtidig tydeliggjør informanten at viktigheten av språk som forstås under opplæring.

> IT - ansatt*: "Opplæring i sikkerhet trenger ikke å være så vanskelig, stort eller omfattende. Vi har en slik tilnærming til at vi driver med opplæring av vi lager en videoblogg post på sånt 3 minutter konsept ...* Jeg mener det skal være en kontinuerlig læring, og igjen på et språk en forstår*"*

Bedriftene vi har snakket med har forskjellige metoder de gjør opplæring til de ansatte på. Vi observerer opplæring som foregår internt, men også bedrifter som bruker eksternt hjelp. IT - utviklere AS bruker intern opplæring, og gjør dette i form av blant annet allmøte og nasjonal sikkerhetsmåned.

> IT - utviklere AS*: "Det kan skje på allmøte at han som er sikkerhetsansvarlig kanskje går gjennom eller repeterer hva en skal gjøre. Typisk har du klikket på en link på en mail så slå av pc-en, dratt ut nettverkskontakten og si ifra til en voksen. Men det gjøres ofte når det er den nasjonale sikkerhetsmåneden i oktober, for at det er lettere å huske å repetere informasjonen"*

IT-utviklere AS har en egen sikkerhetsansvarlig, som informerer og gir opplæring på hvordan de ansatte i bedriften skal håndtere truslene. Mens for Fiskeribedrift AS har de ikke IT kompetanse internt, så de velger en annen metode. De mottar opplæring fra deres leverandør. Regnskap AS har også kursing og har utarbeidet egen handlingsplan for ansatte, hvor de har et ark med instrukser under et eventuelt cyberangrep.

Studentservice AS har per i dag lite fokus på opplæring innenfor IT, hvor de legger frem at det står på agendaen at det er dårlig kommunisert i dag. De ønsker en større plattform før iverksetting av forbedringer starter. De avventer dermed en større strategi til bedriften har blitt mer systematisert.

4.5 Tiltak for små og mellomstore bedrifter til håndtering av cybersikkerhet

For å kunne avdekke nødvendige suksessfaktorer innenfor cybersikkerhet, kan en naturligvis trekke frem de ovennevnte faktorene. At en øker fokuset mot trusselbilde, opplæring, kompetanse og ressurser. Gjennom intervjuene med akademiske eksperter og eksperter innenfor næringslivet, spurte vi om konkrete tiltak for små og mellomstore bedrifter. Perspektivet er i form av hva en kan gjøre for å være proaktiv. Vi avdekker i hovedsak funn som vi kan kategorisere innenfor den menneskelige og tekniske dimensjonen.

Innenfor det menneskelige perspektivet opplyses gode rutiner og bevisst hos ansatte som et tiltak. For å implementere dette hos ansatte, så nevnes “Nasjonal sikkerhetsmåned" og rutiner som passer i praksis og for menneskene.

> Informant: *“Sånn som jeg ser at funker for mange er med å gjennomføre “Nasjonal sikkerhetsmåned". Ha noen små drypp av opplæring. Også så langt det lar seg gjøre, rigge systemer og rutiner som funker for menneske og i praksis”*

I praksis kan en gi jevne drypp i hva som beveger seg, og hvordan en kan behandle ting som avviker fra normalen. Ofte under cyberangrep er det noe som er annerledes, så en opplæring innenfor hva en bør se etter kan være verdifull. Dette kan en bygge videre på og hjelpe å skjerpe oppmerksomheten. Men en kan også benytte seg av verktøy for opplæringen i form av e-leksjoner og nett moduler.

> Informant: *"E-leksjoner-kurs tenker jeg er et godt sted å starte. Det er jo mye læringsteori om at man lærer best hvis man gjør det selv. Det finnes en del lavthengende frukt, nett moduler som man kan klikke rundt på. Okei, klarer vi å se at dette er phishing eller ikke? Sånne typer ting"*

Tilnærmingene starter dermed ved opplæring og bevissthet hos de ansatte. For å bevege seg videre, nevner flere av ekspertene utarbeidelse av en plan for hendelseshåndtering.

> Akademisk ekspert*: "Men så må det også ha en innøvd plan for å håndtere hendelser, det klart dette tar jo tid. Det koster penger å drive å øve på sånt. Å ha god beredskap"*

Når det kommer til hvordan en kan gjennomføre dette, så belyser informanten ulike metoder.

> Informant: *"Sette opp plan for hendelseshåndtering, definere roller bedre, gjennomføre øvelse, invitere tekniske systemer eller koble seg på ekstern kompetanse. Det kan være ulike løsninger der"*

Innenfor det teknologiske perspektivet, nevnes investering i sikkerhetstiltak og god brukerautentisering (2 faktor sertifisering). Videre at en må få en god beredskap som en start, og at en oppnår dette gjennom øving og innøvde planer.

> Akademisk ekspert*: "For det første, å øve på å hente sikkerhetskopi, altså backup, den må være helt knirkefri. Så de får den med en gang"*

Når vi spør om hva SMB gjør feil, så trekkes nok en gang mangel på kompetanse og tid som en årsak. Konsekvensen av dette er at en ikke får oppdatert systemene sine, som utgjør en risiko. IT - leverandør mener at sikkerheten bør kjøpes som en tjeneste, og at de samme anbefalingene kommer fra offentlige instanser. Videre at de som har kunnskap om sikkerhet vil mene det samme.

> IT - leverandør*: "Den største feilen de gjør er å ikke oppdatere systemene sine fordi de ikke har kompetanse eller tid til det. Løsningen er å kjøpe sikkerhet som en tjeneste. Og det sier Nasjonal sikkerhet, Politiet osv. Alle som kan sikkerhet, sier dette. Bare finn en leverandør du stoler på, og som er tilpasset den sektoren du er i"*

Andre viktige elementer som nevnes er å skille admin-kontoer og vanlige brukerkontoer. Slik at det skapes et skille mellom IT og vanlig konto. En av ekspertene støttes dette og trekker frem at en må ha god styring på brukerkontoer. Men det legges også et fokus på oppdatering og konfigureringer.

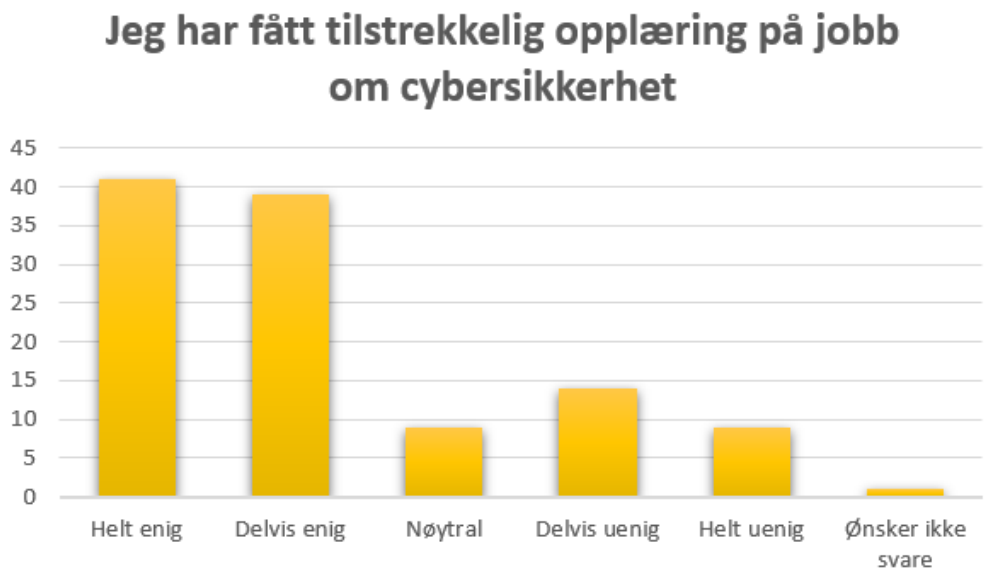
> Akademisk ekspert*: "De må rask oppdatering av programvare, og god konfigurering av brannmurer og den type ting. Ha god styring på brukerkontoer. God brukerautentisering, gjerne 2. faktor, altså sterk brukerautentisering"*

Oppsummert så kan aktuelle tiltak være:

- Øke ansattes bevissthet - ved leksjoner og nettmoduler
- Skape gode rutiner som passer i praksis og for menneskene (F.eks i forhold til varsling)
- Nasjonal sikkerhetsmåned
- Utarbeide en plan for hendelseshåndtering - og informere alle om denne
- Jevn opplæring - øvelser og innøvde planer
- Videoblogg konsept
- Investere i sikkerhetstiltak
- God brukerautentisering (2 faktor)
- Oppdatere systemer selv eller kjøpe som tjeneste (Tjenesteutsetting)
- Følge NSM sine grunnprinsipper
- God brukerstyring, konfigurering av brannmur og oppdatering av programvare

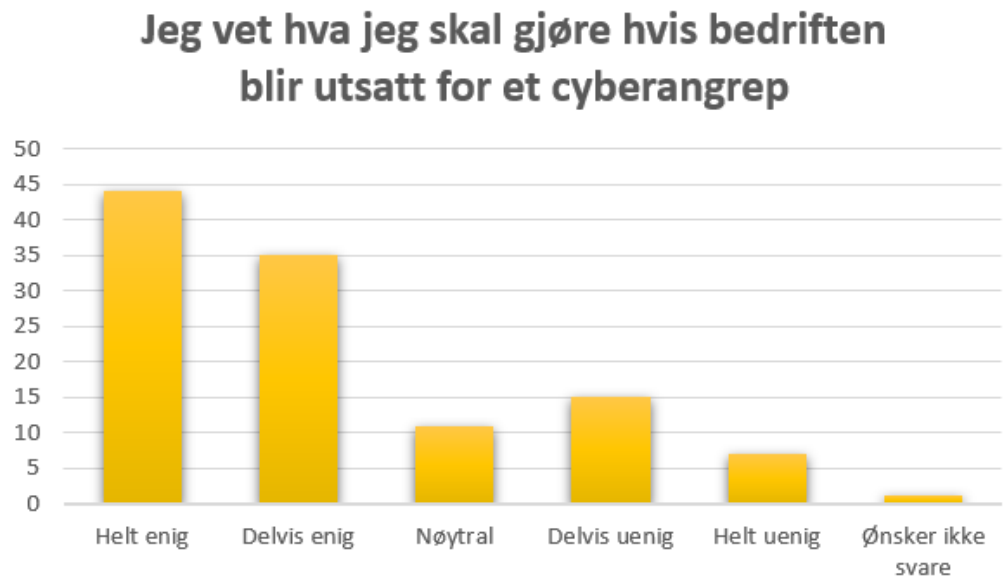
4.6 Spørreundersøkelse av tidligere studenter

For å styrke og supplere til forskningen, så har vi sendt ut samme spørreundersøkelse til Alumni. Dette er et nettverk for tidligere studenter fra Handelshøgskolen ved Nord universitet som har meldt seg inn som en del av denne gruppen. Vi har tatt utgangspunkt i spørsmål angående opplæring, kunnskap under cyberangrep, relasjon til ledere og ønsket om mer kunnskap.



Graf 7: Opplæring (Alumni). Den grafiske framstillingen viser antall svar per alternativ. Totalt antall svar: 113

I denne grafiske fremstillingen vises antall personer som har besvart på de ulike alternativene. Vi observerer dermed en tung overvekt på 70% som er "delvis enig" og "helt enig" i påstanden. De resterende 30% er fordelt på de andre svaralternativene. Svarene uttrykker at majoriteten av utvalget føler de har mottatt tilstrekkelig opplæring på jobb om cybersikkerhet.



Graf 8: Rutiner ved cyberangrep (Alumni). Den grafiske framstillingen viser antall svar per alternativ. Totalt antall svar: 113

I denne grafiske fremstillingen viser en oversikt over hvem som vet hva de skal gjøre, hvis bedriften blir utsatt for et cyberangrep. Vi kan se at grafen viser tydelig likhet med grafen over, og dette kan muligens være i samvariasjon med opplæringen. Det er en høy andel som er "delvis enig" og "helt enig" i at de vet hva de skal gjøre hvis bedriften blir utsatt for cyberangrep.

Graf 9: Kontakt med leder (Alumni). Den grafiske framstillingen viser antall svar per alternativ. Totalt antall svar: 113

Flertallet av utvalget føler de kan spørre lederne sine om hjelp, hvis det skulle være noe de er usikre på om er trygt. Dette kan gi en indikasjon på en god informasjonsutveksling mellom lederne og ansatte.

Graf 10: Fokus på cybersikkerhet (Alumni). Den grafiske framstillingen viser antall svar per alternativ. Totalt antall svar: 112

Når det kommer til et ønske om at bedriftene skal sette mer fokus på cybersikkerheten, ser en at 54,5% vil det. Samtidig er det en relativt stor andel på hele 32,1% som ikke ønsker det. De resterende 13,4% ønsker ikke å besvare og det kan skyldes flere årsaker. Muligens kan det være at de er fornøyde med opplæringen i dag.

Oppsummert ser vi at opplæring er til stede, og at det samsvarer med hvorvidt de vet hva de skal gjøre under et cyberangrep. Det tyder på god informasjonsflyt mellom ledere og ansatte. Men ønsket om at bedriften skal sette mer fokus på cybersikkerhet er varierende.

Oppsummering av funn

Oppsummert har vi gjort oss opp følgende hovedfunn gjennom datainnsamlingen. Vi ser at tjenesteutsetting er en strategi som de fleste av case-bedriftene benytter seg av. De begrunner dette med mangel på kunnskap og ressurser til å håndtere det selv. Vi observerer at enkelte av case-bedriftene gjør seg svært avhengig av leverandøren, og dermed faller fokuset på cybersikkerhet bort internt. Dette resulterer i mangelfull opplæring av ansatte hos enkelte av case-bedriftene. Videre kan komplisert språk hemme ansattes opplæringen. Cybersikkerhet vektlegges i liten grad i case-bedriftenes styringssystemer. Både styringssystem og opplæring blir nedprioritert som en konsekvens av at flere av case- bedriftene ikke selv håndterer problemene. Dette legger til rette for at hver enkelt ansattes risikoapetitt, individuelle risikovurdering og oppfatning av risiko får utfolde seg fritt. Dette som en konsekvens av svak opplæring kombinert med et uklart styringssystem rettet mot cybersikkerhet.

5.0 Diskusjon

I dette kapittelet skal vi presentere funnene i kapittel 4 og teori fra kapittel 2. Hensikten er å tolke funnene opp mot teorien, og videre prøve å forstå sammenhengene. Formålet med kapittelet er å kunne besvare problemstillingen: "*Hvordan brukers små og mellomstore bedrifter sine styringssystemer for å håndtere cybertrusler?"* Vi har strukturert diskusjonskapittelet med å svare på de tre forskingsspørsmålene vi har utarbeidet.

- FS1: Hvordan er cybertrusler utfordrende for små og mellomstore bedrifter?
- FS2: Hvilke tiltak eller strategi bruker små og mellomstore bedrifter til å håndtere cybertrusler?
- FS3: Hvordan brukes styringssystemer til å håndtere cybertrusler?

I den første delen skal vi se forskningsspørsmål 1. "*Hvordan er cybertrusler utfordrende for små og mellomstore bedrifter?"* Vi skal trekke inn elementene som vanskeliggjør håndtering av cybertrusler for SMB. Deriblant opplæring som kompliseres av språk, individets risikoappetitt og overvurdering av egne evner.

5.1 Cybertrusler produserer en negativ "dominoeffekt"

Tidligere forskning viser at utfordringer for SMB skapes på grunn av mangel på kunnskap, ressurser og ekspertise (Wilson et al., 2022, s.398). Dette samsvarer med vår forskning, hvor sentrale funn er utfordringer knyttet til å skaffe dyktige folk med riktig kompetanse internt. Muligens er dette en forklarende faktor til hvorfor SMB ser seg nødt til å benytte tjenesteutsettelse. Samtidig gjør tjenesteutsetting at cybersikkerhet blir mindre synlig for de ansatte i bedriftene. Vi observerer dette som en slags negativ "dominoeffekt", hvor tjenesteutsettelse hemmer fokuset på cybersikkerhet i bedriften. Dette svekker kompetansen og opplæring av ansatte bortprioriteres. Dette kan peke mot utfordringene knyttet til ressurser. Opplæring er veldig ressurskrevende, og er noe bedrifter viser en tendens til å ikke prioritere (Economist, 2021 s. 20). Våre funn viser varierende fokus på opplæring knyttet til cybersikkerhet. Mindre bedrifter har mer fokus på det de produserer, som gjør at cybersikkerhet og opplæring bortprioriteres. Det resulterer i at opplæring for resterende ansatte kan bli svak eller fraværende. Enkelte av case-bedriftene klarer å kombinere egen produksjon i tillegg til et fokus på cybersikkerhet. Dette i form av opplæring og informasjonsdeling rundt trusselbildet.

Språk som hemmer læring

Våre funn viser at en årsak til manglende opplæring kan være språkbruk. Innenfor IKT-bransjen brukes en egen terminologi, som for utenforstående kan virke uforståelig. Denne terminologien omfatter ord og uttrykk som ofte stammer fra det engelske språket kombinert med tekniske forkortelser. Dette gjør at opplæring blir utfordrende for ansatte uten IKT-bakgrunn. Dermed kan fullført opplæring skape en falsk trygghet for ledere i bedriftene. Realiteten kan være at ansatte har gjennomført kurs, uten et utbytte som gir bedre grunnlag for å forstå cybersikkerheten. En av ekspertene trekker frem at opplæringen ikke trenger å være vanskelig, stor eller omfattende. Man kan styrke læringen gjennom et språk folk flest forstår, i form av tydelig tale og ukomplisert opplæring. En løsning kan være gjennom e-læring med fokus på den språklige tilnærmingen.

Individets risikovurdering er en trussel

Det menneskelige aspektet innenfor suksessfulle cyberangrep har blitt tydeliggjort i intervjuene. Vellykkede angrep starter ofte med en feil vurdering fra et individ (Economist, 2019 s.52). Som en forklaring viser Wilson (2022) til optimistiske risikovurderinger, som kan forklares av Dunning-Kruger-effekten hvor menneskers ignoranse blir usynlig for dem. Wilson (2022) viser til at ledelsen har tendenser til å flytte ansvaret. Det blir ofte flyttet til IT-avdelingen basert på deres kompetanse (Lorentzen, 2021, s.51). Noe vi ser i funnene, hvor ansvaret flyttes til IT avdeling eller en ekstern leverandør. Dette kan resultere i at de resterende ansattes opplæring innenfor cybersikkerhet blir nedprioritert.

I håndtering av cybertrusler spiller risikoappetitten, individuelle vurderinger og oppfatningen av risiko inn (Aakre, 2020). Dersom ledelsen ikke lykkes med å implementere de samme holdningene innenfor forståelse og aksept av risiko utgjør det en trussel for bedriften. Forskningen vår viser at majoriteten føler at de kan jobbe selvstendig. Det er derfor enda viktigere at kompetansen og risikoviljen hos de ansatte samsvarer med organisasjonen. Ledelsen kan derfor legge et grunnlag for hvordan de ønsker at en ansatt skal informere om risikofylte handlinger, men en kan ikke vite hvordan den enkelte vil opptre (Goodman, 1993). Aakre (2020b, s.3) trekker frem at toppledelsen sjeldent overvåker prosessen med å tilpasse eksternt regelverk inn i interne risikovurderinger og rutiner. Dette synliggjør en mangel på kontrollering av risikovurderinger og rutiner. Dette kombinert med risiko for falsk trygghet gjennom ansattes opplæring er kritisk. Ledelsen trenger å styrke internkontrollen gjennom kartlegging av ansattes risikoappetitt, oppfatning av risiko og individuelle vurderinger.

Vi mener dette er nødvendige suksessfaktorer i håndtering av cybertrusler.

Undervurdering av risiko og konsekvenser

Spørreundersøkelsen til de ansatte viser variasjon knyttet til om en gir beskjed til ledelse eller IT om en mistenkelig e-post som kan minne om et cyberangrep. En høy andel mener de vet hva de skal gjøre hvis bedriften blir utsatt for cyberangrep. En kan likevel stille seg kritisk til hvorvidt de ansatte har kjennskap til hva som faktisk kan være et cyberangrep. Hvis opplæringen kan karakteriseres som svak, vil det være utfordrende å kunne identifisere et cyberangrep. En kan ikke utelukke at det foreligger overvurdering av egne evner som i Dunning-Kruger effekten. Men som belyst i teorien så er det ikke bare ansatte som overvurdere egne evner. Hattton (2020) påstår også at tjenesteutsetting overvurdere egne evner som en konsekvens av at de må vinne tillit hos kundene. Dysvik (2021) viser at det er krevende å lære opp ansatte, men ansatte viser at de forstår cybersikkerhet. På den andre gjør flere ansatte ting de ikke burde (Dysvik, 2021). For eksempel bruk av samme passord og usikkerhet rundt svindelforsøk. Likevel holder de ansatte fortsatt kontakt med IT-teamet i frykt for konsekvenser (Dysvik, 2021). Dette illustrerer en forskjell på risikovilje og den enkelte ansattes forståelse. Dette peker mot at å skape en sikkerhetskultur og implementere retningslinjer for atferd er avgjørende for å bedre cybersikkerheten.

Resultater fra Alumni-spørreundersøkelsen, viser at majoriteten mener at de har fått tilstrekkelig opplæring på jobb om cybersikkerhet. Svarene viser en sammenheng mellom opplæring og kunnskap knyttet til håndtering av cyberangrep. En kan belyse perspektivet om en noen gang får tilstrekkelig opplæring. Eksperter understreker at det er gjennom mennesker en blir hacket. Dette skyldes blant annet dårlig dømmekraft, som et resultat av for lite kunnskap før avgjørelsen tas (Goodman, 1993). Undersøkelsen viser likevel at hele 32,1% ikke ønsker mer fokus på cybersikkerhet. Muligens kan dette være forbundet med overdreven optimisme knyttet til egen kunnskap og risikovurderinger.

5.2 Tjenesteutsetting– tillit til underleverandøren kan øke kostnader og ansvarsfraskrivelse

I denne delen skal vi besvare forskningsspørsmål 2: *"Hvilke tiltak eller strategi bruker små og mellomstore bedrifter til å håndtere cybertrusler?"*. Vi skal videre diskutere tjenesteutsetting som strategi. Avslutningsvis se på hvilke tiltak case-bedriftene har implementert i dag, og hvilke som anbefales av eksperter fremover.

Våre funn viser til at alle har rustet opp cybersikkerheten i løpet av de siste årene, men at case-bedriftenes tilnærminger er forskjellige. Noen sikrer seg selv internt, mens andre får hjelp eksternt. Vi har også observert en kombinasjon av begge deler.

Tjenesteutsettelse som strategi

For majoriteten av bedriftene i forskningen oppleves cybertrusler for komplekst å håndtere alene. Det oppfattes som umulig å bygge egne avanserte systemer og skaffe egen likeverdig kompetanse som eksterne leverandører. Dette er i tråd med tidligere forskningen som peker på at mangel på intern ekspertise resulterer i at bedrifter søker kompetanse eksternt (Wilson et.al, 2022 s. 398).

Funnene våre viser at SMBene har utfordringer knyttet til kunnskap og ressurser. For disse bedriftene er det derfor en trygghet at andre tar seg av cybersikkerheten. På en annen side gjør dette at man risikerer å miste kontrollen, og at man undervurderer den faktiske kostnaden ved tjenesteutsettelse (Deloitte, 2016). I tillegg viser funnene våre systemkritikk knyttet til tjenesteutsetting. I likhet med andre bransjer er også IT-bransjen ute etter å tjene mest mulig penger. Det kan dermed ikke utelukkes at SMBene risikerer å overkjøpe tjenester de ikke forstår og trenger. Deres manglende kompetanse innenfor fagfeltet utgjør dermed en risiko for å kjøpe mer enn bedriftens behov. En av ekspert informantene våre jobber med å levere tjenesteutsettelse, og mener at de ikke overselger tjenester. Informanten mener de utarbeider sikkerhetsløsninger som samsvarer med bedriftenes behov.

En av case-bedriftene har en mer kritisk tilnærming til tjenesteutsettelse. Derfor benytter de en tredjeparts IT- revisor for å se over tjenesteutsettings-tilbudet for å få bekreftet utenom en kommersiell kontekst om det er relevant for bedriften. Andre case bedrifter viser derimot minimal refleksjon knyttet til leverandørens kommersielle intensjon. Ut fra intervjuene viser flere av bedriftene høy tillit til sine leverandører. De forteller at de stoler på leverandøren, men prøver å stille kritiske spørsmål. En av ekspertene trekker frem at mangel på ressurser og kompetanse gjør det utfordrende å stille de riktige spørsmålene til leverandøren. For bedriftene er det derfor vanskelig å ta en rasjonell beslutning, ettersom en ikke vet konsekvensene av beslutningen. Det er vanskelig å vite om en tar den riktige avgjørelsen og at en har kunnskap om alle mulige alternativer (Turpin & Marasi, 2004.s. 144). En blir fort avhengig av leverandøren sin, og på lang sikt kan dette bli en svakhet for bedriftene. Selv om bedriftene uttrykker et ønske om kontroll over leverandøren, så ender de i praksis opp med en relasjon basert på tillit.

En potensiell effekt av tjenesteutsetting er ansvarsfraskrivelse knyttet til cybersikkerhet. Gjennom tjenesteutsettelse kan ledelsen føle en mangel på kontroll, eller at de ikke er oppdatert slik en leder bør være på hendelser i bedriften (Deloitte, 2016). Samtidig viser vår forskning at mener ekstern hjelp er helt nødvendig. Konsekvensen av å ikke være sikret kan være katastrofal i form av økonomiske tap og svekket omdømme. Bedriftene er dermed svært villige til å bruke mye penger på cybersikkerhet. Men det synes å gå på bekostning av drivkraften til å tilegne seg intern IT-kompetanse. Kostnader knyttet til opprettholdelse av cybersikkerheten er også en utfordring. Dette er en kostnad som vil fortsette å stige, ettersom kravene til god sikkerhet blir høyere. Samtidig trekkes det linjer mot at tjenesteutsetting har utbredt seg i for stor grad. Når det er sagt, innebærer det kostnader ved å ansette noen til å gjøre en tilsvarende jobb internt i bedriften.

Grunnet bedriftenes ulike størrelser varierer antall IT-arbeidere i bedriftene. Vi observerer at de som har bygget opp IT-kompetanse internt, har mer overskudd til å gjøre cybersikkerhet relatert arbeid innad i bedriften. Eksempelvis gjennom forbedring av rutiner, begrensning av tilganger og sørge for nok beskyttelse av systemene. Mens de som har tjenesteutsetting avhenger at den eksterne leverandøren gjør arbeidet. Funnene viser at IT-kyndig arbeidskraft er både dyrt og mangelfullt. Dermed synes tjenesteutsettelse å være det eneste logiske alternativet for små og mellomstore bedrifter. Samtidig vil tjenesteutsetting gi rom for fokus på andre områder i bedriften, som økt faglig kompetanse og oppdatert kunnskap på andre områder (Polizzo, 2023).

I kontekst av bedriftsundersøkelsene er det variasjon i ansattes kunnskap til håndtering av cyberangrep. Dette kan peke tilbake på case-bedriftenes ulike strategitilnærming. I Studentservice AS synes tjenesteutsetting å svekke ansattes kunnskap til håndtering av cyberangrep. Regnskap AS stikker seg positivt ut, som kan vise til at en kombinasjon av ekstern og intern kompetanse er nøkkelen. Dette skaper en proaktiv tilnærming, som gir bedriften større eierskap i egen cybersikkerhet. Samtidig som kunnskapen innad bedriften ikke nedtrappes som et resultat av tjenesteutsettelse.

Tiltak

Tidligere forskning viser til at SMB ikke installerer robuste sikkerhetstiltak som skal gå mot trusler (Ruaju & Verhaart, i.d). Resultatet av dette er at kriminelle får en tiltrekning mot SMB, og danner hovedgrunnlaget for småbedriftssvikt (Ruaju & Verhaart, i.d). Gjennom vår data avdekker vi variasjon i tiltak som har blitt implementert.

Casebedriftene får konkrete sikkerhetstiltak og jevnlige anbefalinger fra leverandøren. Dette samsvarer med funn fra ekspertinformantene som anbefaler sikkerhetstiltak. I tillegg legges det også opp til fokus på god brukerautentisering. Flere av våre ekspertinformanter anbefaler økt oppmerksomheten knyttet til nasjonal sikkerhetsmåned. Dette kan fungere som et holdepunkt, men fokuset må eksistere året rundt. Det bør være en jevn opplæring, hvor en øker ansattes bevissthet. Forskningen vår viser at opplæring kan være utfordrende. Blant annet på grunn av språkbruken som hemmer opplæringen. Tiltak som kan iverksettes er å benytte seg av e-læring. I form av videoblogg konsept, e-leksjoner og nettmoduler, som kan forbedre læringen og appellere til flere.

Regnskap AS benytter en egen IT-avdeling internt, tjenesteutsetting og tredjeparts IT-revisor. De har også en plan og et ark med fremgangsmåte for de ansatte under et potensielt cyberangrep. Det fremstiller en mer selvstendig og kritisk tilnærming opp til tjenesteutsettelse, hvor en ikke har mistet fokus og opplæring internt. Samtidig samsvarer det med ekspertenes anbefalte tiltak knyttet til gode rutiner som passer i praksis og for menneskene. På generell basis oppfordrer flere av ekspertene til å følge NSM sine grunnprinsipper, oppdatering av programvare og konfigurering av brannmur.

5.3 Cybertrusler møtes med ubalanserte styringsspaker

I dette kapittelet skal vi diskutere forskningsspørsmål 3: *"Hvordan brukes styringssystemer til å håndtere tiltak mot cybertrusler?*" Vi ønsker videre å belyse hvilken rolle Simons (1995) kontrollspaker har i case-bedriftens håndtering av cybersikkerhet. Videre studere kontrollspakenes opp mot hverandre, og hvordan balansen mellom kontrollspakene skaper muligheter og utfordringer for case-bedriftene.

Konflikt mellom trossystem og grensesystem

De fleste case-bedriftene har tydelige verdier som gjenspeiles i de ansatte. Verdiene kjennetegnes av hvordan en ønsker å bli oppfattet, men også ønsket organisatorisk atferd, ytelse i bedriften og bidrag til samfunnet. Men verdiene viser ingen tydelig kobling opp mot cybersikkerhet. Dette kan anses som en konsekvens av tjenesteutsetting, som resulterer i at cybersikkerhet ikke praktiseres internt. Når det er sagt, synes verdiene å være koblet opp til casebedriftenes formål og fagområde. Simons presiserer at alle organisasjoner er skapt for et formål. Dette formålet blir ofte kommunisert ut til kunder og ansatte gjennom et trossystem (Simons, 1995). Vi observerer at case-bedriftenes verdier samsvarer med denne teorien, fordi verdiene knyttets opp bedriftenes formål og ikke cybersikkerhet. På en annen side kan man ikke utelukke at et veletablert trossystem innenfor cybersikkerhet kan fungere som et nyttig verktøy. Da verdier er en måte for organisasjonen å sikre at oppførselen til de ansatte gjenspeiler bedriftens verdier (Tessier & Otley, 2012).

Et av de mest krevende aspektene med cybersikkerhet er hvordan hvert enkelt individ har en ulik oppfatning av risiko (Aakre, 2020). Et fraværende trossystem innenfor cybersikkerhet tillater ansatte å håndtere trusler ulikt. Som en konsekvens legger det til rette for ulik risikoappetitt. Bakgrunnen for en rekke vellykkede cyberangrep kommer fra menneskelige feil (Economist, 2019 s. 52), som kan knyttes opp mot Dunning-Kruger-effekten. Hvor man ser at det er de med minst kompetanse som oftest overvurderer egne evner (Dunning, 2011). En potensiell konsekvens av et fraværende trossystem kombinert med optimistisk risikovurderinger medfører økt sårbarhet knyttet til cyberangrep.

Widener (2007) studerte kontrollspakenes relasjon på tvers av styringssystemene, som viser til at de avhenger og utfyller hverandre. Et manglende trossystem kan skape problemer i balansen mellom trossystemet og grensesystemet. Et resultat av et oppdatert trossystem vil være at grensesystemet blir enklere å forholde seg til. Grensesystemet skal hjelpe lederne til å lage klare rammer og anvisninger som de ansatte skal følge (Simons, 1995). Flere av case-bedriftene viser ikke til tydelige grenser i forhold til cybersikkerheten. Derfor legges det opp til at de ansatte skal oppfatte trusler selv og melde ifra til ledelse/IT. Dette skaper en forventning og tillit til at de ansatte skal håndtere trusler riktig. Dette innebærer en risiko, da man ikke kan utelukke at ansattes egen risikooppfatning danner ulike trossystem. Med et fraværende fokus på cybersikkerhet i trossystemet kombinert med et uklart grensesystem, så er det utfordrende for case-bedriftene å håndtere cybertrusler. Som nevnt i teorien, så kan

årsaken til dette være at små og mellomstore bedrifters underutviklede ledelsesprosesser og mangel på ressurser hindrer dem i å oppnå en balanse mellom kontrollspakene (Pesalj et al, 2018).

Ubalanse mellom interaktive kontrollmekanismer og diagnostiske kontrollmekanismer

De diagnostiske kontrollmekanismene bygger på tilbakemeldingskontroll og måling av ytelse (Simons, 1995). Våre funn viser at tjenesteutsettelse tar en stor rolle i den diagnostiske kontrollmekanismen i form av at case-bedriftene mottar kvartalsrapporter og tilbakemeldinger fra leverandøren. Når det er sagt, viser vår data at språkbruk er en barriere innenfor læringen. Med det belyst, så kan man trekke paralleller til at språket i rapportene kan bli for avansert. slik at bedriftene mister forståelsen av hva rapportene egentlig forteller. Dette medfører at den interaktive kontrollmekanismen blir svekket, fordi ledelsen ikke forstår omfanget av den diagnostiske kontrollmekanismen. Samtidig avhenger case-bedriftene av at leverandøren overvåker og måler ytelsen. Som et resultat risikerer case-bedriftene å miste kontroll over denne diagnostiske kontrollspaken. Tiltak for å håndtere ubalansen mellom kontrollmekanismene vil være at SMBer inntar en mer delaktig rolle innenfor cybersikkerhet. Som frembringer et økt fokus innenfor bedriftens egne ytelser og målinger.

Det som er utfordrende i lys av den interaktive kontrollspaken er språk under opplæring, som gjør at ansatte ikke forstår informasjonen som blir formidlet. Man står da overfor et gap mellom måten man kommuniserer ønsket læring, til språk ansatte forstår under læringen. Våre funn viser at avansert språk kan komplisere opplæringen. Dette kommer i stor grad av at språket tar utgangspunkt i det engelske språket med tekniske forkortelser. Dette gjør at kommunikasjonsutvekslingen er vanskeligere å tolke for de ansatte, og den interaktive kontrollspaken blir svak. Fra teorien viser Simons (1994) at ved en svak interaktiv kontrollspak svekkes den organisatoriske læringen. Tiltak som kan bidra til økt læring i den interaktive kontrollspaken vil være ansikt-til-ansiktkommunikasjon. Vi observerer også at ved IT-ekspertise internt dyrkes en kultur med lavere terskel for å spørre om hjelp. Samtidig tilrettelegges det for ansikt-til-ansikt kommunikasjon. Simons (1994) mener at ved personlig kontakt så fremmer man læringen. Dette kan være et viktig element innenfor opplæring av cybersikkerhet for de ansatte, fordi man åpner opp for toveiskommunikasjon. Dermed kan opplæringen forbedres i form av tilbakemelding, hvis man ikke forstår opplæringen.

Ofte vil det være utfordrende å oppfylle alle kontrollspakene, og i noen tilfeller vil kontrollspakene ha motstridende krefter som gjør dem vanskelige å balansere (Mundy, 2010). På en annen side så er det viktig med autonomi for de ansatte, samtidig er det viktig å finne en balanse (Chenhall, 2003). For å oppnå en balanse mellom disse to kontrollmekanismene, må organisasjoner integrere kontrollspakene på en komplementær måte. Dette betyr at mens de bruker diagnostiske kontrollsystemer for å overvåke ytelse og identifisere områder for forbedring, bør de også gi muligheter for ansatte til å gi tilbakemelding, dele ideer og samarbeide gjennom interaktive kontrollsystemer. Denne tilnærmingen kan bidra til å fremme en kultur for ansvarlighet, tillit og kontinuerlig forbedring. Framfor en kultur hvor det er høy grad av ansvarsfraskrivelse fordi for få parter er involvert i cybersikkerheten.

6.0 Konklusjon

Formålet med denne masteroppgaven er å få et dypere innblikk i små og mellomstore bedrifter sin håndtering av cybertrusler. Vår problemstilling er: *«Hvordan bruker små og mellomstore bedrifter sine styringssystemer for å håndtere cybertrusler?»*. Forskningen har tatt utgangspunkt i hvordan små og mellomstore bedrifter håndterer cybertrusler. Case-bedriftene representerer ulike bransjer og geografiske områder. I forskningen vår har vi valgt å benytte oss av både kvantitativ og kvalitativ datainnsamling. I form av intervju med bedrifter, eksperter og spørreundersøkelse til bedriftens ansatte. Gjennom våre forskningsspørsmål har vi dannet grunnlag for å kunne besvare problemstillingen.

Gjennom forskningen vår har det menneskelige aspektet som en faktor for vellykkede angrep blitt tydeliggjort. Derfor er opplæring det mest effektive virkemiddelet for å være proaktiv i møte med cyberangrep. Innenfor den interaktive spaken kompliserer avansert terminologi opplæringen. Dette skaper et gap mellom måten man kommuniserer ønsket læring, til språk som ansatte forstår under opplæring. Dette medfører en svak interaktiv kontrollmekanisme som svekker den organisatoriske læringen.

Flere av case-bedriftene viser ikke til tydelige grensesystemer for cybersikkerhet. Dette skaper en forventning og tillit til at de ansatte skal håndtere trusler riktig. Likevel er dette risikofylt, fordi en ikke kan vite hvordan den enkelte vil opptre. Trossystemene viser heller ingen tydelig kobling opp mot cybersikkerhet. Dette skaper grobunn for at hver enkeltes risikoappetitt, individuelle risikovurderinger og oppfatning av risiko får utfolde seg fritt. Det kan derfor ikke utelukkes at tilfeller med overvurdering av egne evner kan forekomme. En potensiell konsekvens av optimistiske risikovurderinger er økt sårbarhet knyttet til cyberangrep.

Balanse er en av de viktigste faktorene for at rammeverket skal lykkes. Kontrollspakenes relasjon på tvers av styringssystemene viser til at de avhenger og utfyller hverandre (Widener, 2007). Vi har gjennom forskningen observert en svak bruk av styringssystemer for å håndtere cybertrusler. Funnene våre viser at case-bedriftene har et utydelig grensesystem og et fraværende trossystem rettet mot cybersikkerhet. Den avanserte terminlogien kompliserer den interaktive spaken. Tjenesteutsettelse gjennom den diagnostiske kontrollspaken bidrar til en avhengighet til leverandøren, og risiko for å miste fokus på cybersikkerhet internt. Dette skaper en ubalanse i styringssystemet. Det kan forklares av et mønster hvor små og

mellomstore bedrifters underutviklede ledelsesprosesser og evner. Videre at deres mangler på ressurser hindrer dem i å oppnå balanse (Pesalj et al, 2018).

For å skape en balanse mellom styringssystemene må organisasjoner integrere kontrollspakene på en komplementær måte. SMBer må også styrke fokuset på cybersikkerhet internt ved å danne et tydelig trossystem som kan virke veiledende for de ansatte, og som får cybersikkerhet på dagsordenen. Grensesystemet kan forsterkes ved gode rutiner, strategier og retningslinjer som er egnet menneskers atferd. Deretter øke ansattes bevissthet gjennom leksjoner i form av e-læring og personlig kommunikasjon fra lederne. Ledelsen må også styrke internkontrollen gjennom å kartlegge ansattes risikoappetitt, individuelle vurderinger og oppfatning av risiko for å samkjøre ansattes beslutninger med bedriftens retningslinjer.

For å styrke den diagnostiske kontrollspaken må SMBene ta mer eierskap i cybersikkerheten gjennom oppbygning av intern IT-kompetanse. Ved fokus på ytelse og identifisering av områder for forbedring, og tilrettelegging for tilbakemelding og samarbeid gjennom interaktive kontrollsystemer. En kombinasjon av ekstern og intern kompetanse skaper en proaktiv tilnærming, som ikke svekker kunnskapen internt i bedriften. Praktisering av IT-kompetanse internt bidrar til en sikkerhetskultur med større fokus på cybersikkerhet, og tilrettelegger for økt interaksjon. Det økte fokuset kan skape en positiv dominoeffekt, hvor hver enkelt kontrollspak får en relasjon til cybersikkerhet. Ringvirkninger av dette er bedre kommunikasjon, opplæring og forutsigbar atferd fra ansatte i lys av cybersikkerhet.

Gjennom forskningen har vi avdekket følgende hovedfunn: (1) Majoriteten av bedriftene tjenesteutsetter cybersikkerheten. De begrunner dette med mangel på kunnskap og ressurser til å håndtere det selv. Vi observerer at enkelte av case-bedriftene gjør seg svært avhengig av leverandøren, og dermed faller fokuset på cybersikkerhet bort internt (2) Det er ingen tydelig kobling mellom styringssystem og cybersikkerhet. Cybersikkerhet vektlegges i liten grad i case-bedriftenes styringssystemer. Både styringssystem og opplæring blir nedprioritert som en konsekvens av at flere av case- bedriftene ikke selv håndterer problemene. (3) Det er ubalanse mellom styringssystemets «kontrollspaker» internt i bedriftene. På bakgrunn av små og mellomstore bedrifters mangel på ressurser og underutviklede ledelsesprosesser og evner.

6.1 Videre forskning

Datamaterialet består av intervju med fire små og mellomstore bedrifter og eksperter i tillegg til spørreundersøkelse i case-bedriftene og Alumni. Alumni representerer kun personer med grad fra Handelshøgskolen i Bodø. Ved å sende spørreundersøkelsen til flere enn kun dette utvalget, så kunne det gitt oppgaven mer bredde. Videre kunne en forsket på enda mindre bedrifter enn det som ble gjort. I vår forskning dreide det seg i hovedsak om mellomstore bedrifter. Vi tror at ved å fokusere på enda mindre bedrifter, så kan en avdekke flere interessante funn. På bakgrunn av at de opererer med enda færre ressurser, som gjør at cybertrusler kan oppleves som enda mer omfattende.

Ettersom cybertrusler er under kontinuerlig utvikling, så finnes det en rekke elementer som kan forskes videre på. En kan studere nærmere håndtering av nye metoder innenfor hacking, blant annet leverandørkjedeangrep. Gjennom forskningen har vi også kjent med etisk hacking som en metode for å styrke ansattes forståelse. Dette er et tema som har vært interessant å forske på i lys av hvordan dette påvirker det sosiale og etiske aspektet i bedriften. Videre kan det være spennende å studere lederes strategi for cybersikkerhet, og om ansattes oppfatning samsvarer. Vår forskning viser at tjenesteutsetting er utbredt. I lys av dette vil det være særlig relevant å forske nærmere på hvordan styringssystemer og styringsmuligheter påvirkes av tjenesteutsetting. Videre se dybden av de faktiske konsekvensene av tjenesteutsetting. Deretter forske på om det finnes andre løsninger, som gir mer eierskap i egen cybersikkerhet.

Litteraturliste

Aakre, S. (2020). *"Just tell us what to do" Regulations and cyber risk appetite in the electric power industry*. https://nordopen.nord.no/nord-xmlui/bitstream/handle/11250/2772702/Aakre.pdf?sequence=4

Aakre, S. (2022). *From intangibility to "fluid" tangibility of cyberrisk: localisation, visualisation, and prevention* [Doktor Avhandling, Nord Universitet]. https://nordopen.nord.no/nord-xmlui/bitstream/handle/11250/3033551/Aakre_excl_art.4.pdf?sequence=4

Abernethy, M.A. & Chua, W.F. (1996). A Field Study of Control System "Redesign": The Impact of Institutional Processes on Strategic Choice. *Contemporary Accounting Research*, *13*(2), 569–606. https://doi.org/10.1111/j.1911-3846.1996.tb00515.x.

Alijoyo, A. (2021, 18. October). *Risk Management and Decision-Making Theory*. Indonesia Risk Management Professional Association. https://irmapa.org/risk-management-and-decision-making-theory/.

Anthony, R. (1965). *Planning and Control Systems A Framework for Analysis. Division of Research, Graduate School of Business Administration, Harvard University, Boston. - References - Scientific Research Publishing*. Scirp.org. https://www.scirp.org/(S(i43dyn45teexjx455qlt3d2q))/reference/ReferencesPapers.aspx?ReferenceID=1673779.

Arnoldi, J. (2009). *Risk: An introduction*. Https://researchgate.net/Publication/261945373_Risk_An_Introduction_by_Jakob_Arnoldi.

Batista, A. (2021, 23. November). *How small and medium-sized businesses can prevent potential cyber threats*. Peerspot.com. https://www.peerspot.com/articles/how-small-and-medium-sized-businesses-can-prevent-potential-cyber-threats

Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance*, *28*, 24–31. https://doi.org/10.1016/s2212-5671(15)01077-1

Benz, M. & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons*, *63*(4), 531–540. https://doi.org/10.1016/j.bushor.2020.03.010.

Berry CT, Berry RL. An initial assessment of small business risk management approaches for cyber security threats. Int J Bus Contin Risk Manag. 2018;8(1):1–10. doi:10.1504/IJBCRM.2018.090580.

Bjørkeng, P. K. (2023, 29. Mars). *KI lurte menneske trill rundt. Nå krever over 1000 eksperter forbud.* Aftenposten.no. https://www.aftenposten.no/kultur/i/P4aqye/ki-lurte-menneske-trill-rundt-naa-krever-over-1000-eksperter-forbud

Bourmistrov, A. & Aakre, S. (2020). *Framsyn som risikoradar. Hvordan kan scenarioanalyse forbedre cybersikkerhet?* https://nordopen.nord.no/nord-xmlui/bitstream/handle/11250/2677552/Bourmistrov.pdf?sequence=6

Busch, T. (2005). Økonomistyring i et organisasjonsteoretisk perspektiv : Tor Busch. In E. Døving & Å. Johnsen (Eds.), Organisasjonsteori på norsk (pp. 141-158). Bergen: Fagbokforl., cop. 2005.

Chenhall, R. H. (2003). Management control systems design within its organizational context: findings from contingency-based research and directions for the future. *Accounting, Organizations and Society*, *28*(2-3), 127–168. https://doi.org/10.1016/S0361-3682(01)00027-7

Chertoff, M. (2023, 13. April). *Cyber Risk Is Growing. Here's How Companies Can Keep Up*. Harvard Business Review. https://hbr.org/2023/04/cyber-risk-is-growing-heres-how-companies-can-keep-up

Collier, P. M. (2005). Entrepreneurial control and the construction of a relevant accounting. *Management Accounting Research*, *16*(3), 321–339. https://doi.org/10.1016/j.mar.2005.06.007

Corallo, A., Lazoi, M. & Lezzi, M. (2020). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. *Computers in Industry*, *114*, 103165. https://doi.org/10.1016/j.compind.2019.103165.

Deloitte. (2016). *Guide til outsourcing En rapport til Finansforbundet*. https://www.finansforbundet.no/content/uploads/2020/10/Outsourcing-guide_Deloitte-1.pdf

Deshler, R. (2017, 20. Desember). *Control Vs. Governance in Organization Design*. AlignOrg Solutions. https://alignorg.com/control-vs-governance-organization-design/

Drive. (2019, 16. Juli). *Why Audiences Are Attracted to Brands With a Belief System*. Drive Creative Agency. https://drivecreativeagency.com/why-audiences-are-attracted-to-brands-with-a-belief-system/

Dunning, D. (2011, 1. Januar). *Chapter five - The Dunning–Kruger Effect: On Being Ignorant of One's Own Ignorance* (J. M. Olson & M. P. Zanna, Eds.). ScienceDirect; Academic Press. https://www.sciencedirect.com/science/article/abs/pii/B9780123855220000056?via%3Dihub

Dysvik, S. (2021). *Cybersikkerhet - Et spill i kontinuerlig utvikling* [Masteroppgave. Universitetet i Oslo]. https://www.duo.uio.no/bitstream/handle/10852/88011/Masteroppgave---v-ren-2021---Siren-Dysvik.pdf?sequence=3&isAllowed=y.

Eliassen, N. & Korneliussen, I. (2018). *Outsourcing – borte bra men hjemme best?* [Masteroppgave. Universitetet i Tromsø]. https://munin.uit.no/bitstream/handle/10037/13922/thesis.pdf?sequence=2&isAllowed=y

Emmanuel, C. R. & Otley, D. T. (1985). *Accountig for management control*. Van Nostrand Reinhold.

European Commission. (2003). *SME definition*. Single-Market-Economy.ec.europa.eu. https://single-market-economy.ec.europa.eu/smes/sme-definition_en.

Evans, M., Maglaras, L. A., He, Y. & Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks*, *9*(17), 4667–4679. https://doi.org/10.1002/sec.1657.

Ferreira, A. & Otley, D. (2009). The design and use of performance management systems: An extended framework for analysis. *Management Accounting Research*, *20*(4), 263–282. https://doi.org/10.1016/j.mar.2009.07.003

Ghauri, P. N., Grønhaug, K. & Strange, R. (2020). *Research methods in business studies: a practical guide* (5 utg.). Cambridge University Press.

Gjensidige. (2022, 10. November). *Økt risiko for cyberangrep: Små og mellomstore bedrifter er ekstra utsatt*. Gjensidige.no/Godtforberedt. https://www.gjensidige.no/godtforberedt/content/flere-cyberangrepsforsok-retter-seg-mot-smb

Goodman, S. K. (1993. Oktober). *Information needs for management decision-making - ProQuest*. https://www.proquest.com/docview/227753357?pqorigsite=gscholar&fromopenview=true

Gordon, L. A., Loeb, M. P., Sohail, T., Tseng, C.-Y. & Zhou, L. (2008). Cybersecurity, Capital Allocations and Management Control Systems. *European Accounting Review*, *17*(2), 215–241. https://doi.org/10.1080/09638180701819972.

Grønmo, S. (2012). Kvalitative og kvantitative metoder: Begreper og distinksjoner. *Sosiologisk Tidsskrift*, *20*(01), 85–91. https://doi.org/10.18261/issn1504-2928-2012-01-06.

Hätönen, J. & Eriksson, T. (2009). 30+ years of research and practice of outsourcing – Exploring the past and anticipating the future. *Journal of International Management*, *15*(2), 142–155. https://doi.org/10.1016/j.intman.2008.07.002.

Hatton, S. (2020, 8. Januar). *Cybersecurity Threat: The Dunning Kruger Effect*. Endsight.net. https://www.endsight.net/blog/cyber-security-threat-the-dunning-kruger-effect

Horn, A. (2017, 11. Desember). *Cybersecurity Should Be a Top Concern for Middle-Market Companies*. SmallBizDaily. https://www.smallbizdaily.com/cybersecurity-middle-market-companies/

Ingebrigtsen, J. N. P. & Lavbakk, Ø. (2007). *Strategi & Økonomistyring – hvor er sammenhengen?* [Masteroppgave, Handelshøgskolen i Bodø]. https://nordopen.nord.no/nord-xmlui/bitstream/handle/11250/140722/Ingebrigtsen_Jan.pdf?sequence=1&isAllowed=y

Iversen, A. B. (2011). Kvalitative og kvantitative metoder – et kontinuum? *Sosiologisk Tidsskrift*, *19*(02), 175–183. https://doi.org/10.18261/issn1504-2928-2011-02-04

Johannessen, A., Christoffersen, L. & Tufte, P. A. (2020). *Forskningsmetode for økonomisk-administrative fag* (4 utg.). Abstrakt Forlag.

Johanson, R. (2019, 2. Januar). *60 Percent of Small Companies Close Within 6 Months of Being Hacked*. Cybercrime Magazine. https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/#:~:text=Beyond%20the%20financial%20consequences%20of

Kolltveit, B. J., Reve, T. & Lereim, J. (2009). *Prosjekt strategi, organisering, ledelse og gjennomføring* (2 utg.). Universitetsforlaget.

Kruger, J. & Dunning , D. (1999). *Unskilled and Unaware of It: How Difficulties in Recognizing One's Own Incompetence Lead to Inflated Self-Assessments*. APA PsycNet. https://doi.org/10.1037/0022-3514.77.6.1121

Kruis, A. - M., Speklé, R. F. & Widener, S. K. (2016). The Levers of Control Framework: An exploratory analysis of balance. *Management Accounting Research*, *32*, 27–44. https://doi.org/10.1016/j.mar.2015.12.002

Kulset, E. H. M. & Meidelsen, K. H. R. (2020). Internkontroll som virkemiddel for å hindre underslag og svindel på innkjøpsområdet. *47-56*. https://nordopen.nord.no/nord-xmlui/handle/11250/2677257

Langfield-Smith, K. (1997). Management control systems and strategy: A critical review. *Accounting, Organizations and Society*, *22*(2), 207–232. https://doi.org/10.1016/s0361-3682(95)00040-2

Langø, H.-I. & Sandvik, K. B. (2013). Cyberspace og sikkerhet. *Internasjonal Politikk*, *71*(02), 221–228. https://doi.org/10.18261/issn1891-1757-2013-02-05

Lorentzen, V. Ø. (2021). *Cyberkriminalitet mot næringslivet: en studie av løsepengevirusangrep mot norske virksomheter* [Masteroppgave. Universitetet i Oslo]. https://www.duo.uio.no/bitstream/handle/10852/89417/1/LEVERINGSKLAR.pdf

Malmi, T. & Brown, D. A. (2008). Management control systems as a package—Opportunities, challenges and research directions. *Management Accounting Research*, *19*(4), 287–300. https://doi.org/10.1016/j.mar.2008.09.003

Martyn, P., Sweeney, B. & Curtis, E. (2016, 5. September). *Strategy and control: 25 years of empirical use of Simons' Levers of Control framework*. https://www.emerald.com/insight/content/doi/10.1108/JAOC-03-2015-0027/full/html

Merchant, K. A. & Van der Stede, W. A. (2011. September). *Management Control Systems: Performance Measurement, Evaluation and Incentives*. https://www.researchgate.net/publication/291530228_Management_Control_Systems_Performance_Measurement_Evaluation_and_Incentives

Monash University. (i.d.). *Transaction Cost Theory*. Monash Business School. https://www.monash.edu/business/marketing/marketing-dictionary/t/transaction-cost-theory#:~:text=%22A%20theory%20accounting%20for%20the

Morgan, S. (2020, 13. November). *Cybercrime to cost the world $10.5 trillion annually by 2025*. Cybercrime Magazine. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Mundy, J. (2010). Creating dynamic tensions through a balanced use of management control systems. *Accounting, Organizations and Society*, *35*(5), 499–523. https://doi.org/10.1016/j.aos.2009.10.005

Myrvold, K. (2022, 4. Juli). *SMB-virksomheter er offeret i 8 av 10 vellykkede ransomware-angrep*. Digi.no. https://www.digi.no/artikler/debatt-smb-virksomheter-er-offeret-i-8-av-10-vellykkede-losepengevirus-angrep/520753

NHO. (i.d.). *Fakta om små og mellomstore bedrifter (SMB)*. Www.nho.no. Retrieved May 11, 2023, from http://nho.no/tema/sma-og-mellomstore-bedrifter/artikler/sma-og-mellomstore-bedrifter-smb/

NSM/ Nasjonal sikkerhetsmyndighet. (2023). *Risiko 2023 Økt uforutsigbarhet krever høyere beredskap*. https://nsm.no/getfile.php/1312547-1676548301/NSM/Filer/Dokumenter/Rapporter/Risiko%202023%20-%20Nasjonal%20sikkerhetsmyndighet.pdf

Otley, D. (1999). Performance management: a framework for management control systems research. *Management Accounting Research*, *10*(4), 363–382. https://doi.org/10.1006/mare.1999.0115

Perez, C. (2020. August). *A Cybersecurity Strategy for the Small Business - ProQuest*. Proquest.com. https://www.proquest.com/docview/2451164245?fromopenview=true&pq-origsite=gscholar&parentSessionId=e3CFjLRJb4QQiujsn6c9M8Csy1R6Oy75uRRb7%2FJZR6s%3D.

Pešalj, B., Pavlov, A. & Micheli, P. (2018). *The use of management control and performance measurement systems in SMEs: A levers of control perspective*. https://www.emerald.com/insight/content/doi/10.1108/IJOPM-09-2016-0565/full/html?casa_token=ycB40r9iOk4AAAAA:7avNdrf3_nh1yPdI9nNikYvJ3bssiivbo_F2Q6VM7MhEeyrvwsAPovBjdyURT7MobrIEcIwusV2_gOe3-9A7jX9SvWH02Py1wrHeX5piOZetj-xSvhI.

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

Politiet. (2023). *Cyberkriminalitet 2023*. https://www.politiet.no/globalassets/04-aktuelt-tall-og-fakta/datakriminalitet/cyberkriminalitet-2023.pdf

Polizzo, G. (2023, 19. Mars). *Why SMEs Should Consider Outsourcing Too*. Supply & Demand Chain Executive. https://www.sdcexec.com/professional-development/retention/article/22766468/cloudstaff-why-smes-should-consider-outsourcing-too

Power, Michael. 2004. "The Risk Management of Everything: Rethinking the Politics of Uncertainty." Demos, 71.

PricewaterhouseCoopers. (2021, 27. Juli). *SMEs in the World of Cyber - An Insight*. PwC. https://www.pwc.com/mt/en/publications/technology/smes-in-the-world-of-cyber.html

PricewaterhouseCoopers. (2022). *Cybercrime-rapporten 2022 | PwC Norge*. PwC. https://www.pwc.no/no/pwc-aktuelt/pwcs-cybercrime-survey.html

Raju, R. & Verhaart, M. (i.d.). *Impact of Cybercrime on SMEs*. https://www.citrenz.ac.nz/conferences/2016/pdf/2016CITRENZ_2_Poster_Raju_Cybercrime_30-2.pdf

Regjeringen. (2015). *NOU Digital sårbarhet - sikkert samfunn*. https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf

Regjeringen. (2021). *Digital hele livet*. https://www.regjeringen.no/contentassets/8f8751780e9749bfa8946526b51f10f4/digital-hele-livet.pdf.

Ricci, J., Breitinger, F. & Baggili, I. (2019). Survey results on adults and cybersecurity education. *Education and Information Technologies*, *24*(1), 231–249. https://doi.org/10.1007/s10639-018-9765-8.

Sander, K. (2022). *Reliabilitet*. EStudie.no. https://estudie.no/reliabilitet/

Sander, K. (2019). *Validitet*. EStudie.no. https://estudie.no/validitet/

Simons, R. (1994). How New Top Managers Use Control Systems as Levers of Strategic Renewal. *Strategic Management Journal*, *15*(3), 169–189. https://www.jstor.org/stable/2486965

Simons, R. (1995. Mars). *Control in an Age of Empowerment*. Harvard Business Review. https://hbr.org/1995/03/control-in-an-age-of-empowerment

Simons, R. (2000). *Performance measurement and control systems for implementing strategy*. Pearson.

Skotnes, R. Ø. (2017, 20. September). – *Cybersikkerhet er ikke en byrde, men en samfunnsverdi*. Aftenbladet.no. https://www.aftenbladet.no/meninger/debatt/i/2QOO4/cybersikkerhet-en-samfunnsverdi-vi-alle-maa-beskytte

Stevens, T. (2018, 1. Juli). *Global Cybersecurity: New Directions in Theory and Methods*. Papers.ssrn.com. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3199051

Tessier, S. & Otley, D. (2012). A conceptual development of Simons' Levers of Control framework. *Management Accounting Research*, *23*(3), 171–185. https://doi.org/10.1016/j.mar.2012.04.003.

Thagaard, T. (2018). *Systematisk og innlevelse: En innføring i kvalitativ metode* (4th ed.). Fagbokforlaget.

The Economist. (2019). How will this end? What's at stake in Hong Kong. *The Economist [Magasin]*.

The economist. (2021). Broadbandits -The surging cyberthreats from spies and crooks. *The Economist. [Magasin]*.

Turpin, S. M. & Marais, M. A. (2004). Decision-making: Theory and practice. *ORiON*, *20*(2), 143–160. https://www.ajol.info/index.php/orion/article/view/34246

USC Libraries. (i.d.). *Research Guides: Organizing Your Social Sciences Research Paper: 5. The Literature Review*. Libguides.usc.edu. https://libguides.usc.edu/writingguide/literaturereview#:~:text=Literature%20reviews%20are%20designed%20to.

Vakulchuk, R., Henk, O. & Bourmistrov, A. (2023). Oppfattet risiko og beredskap. *Praktisk Økonomi & Finans*, *39*(1), 17–33. https://doi.org/10.18261/pof.39.1.3.

Villasís-Keever, M. Á., Márquez-González, H., Zurita-Cruz, J. N., Miranda-Novales, M. G. & Escamilla-Núñez, A. (2018). Research protocol VII. Validity and reliability of the measurements. *Revista Alergia México*. https://pubmed.ncbi.nlm.nih.gov/30602211/

VISMA. (i.d.). *Hva er outsourcing?* Visma.no. https://www.visma.no/eaccounting/regnskapsordbok/o/outsourcing/#:~:text=Outsourcing%20betyr%20at%20en%20virksomhet

Widener, S. K. (2007). An empirical analysis of the levers of control framework. *Accounting, Organizations and Society*, *32*(7-8), 757–788. https://doi.org/10.1016/j.aos.2007.01.001

Wilson, M., McDonald, S., Button, D. & McGarry, K. (2022). It Won't Happen to Me: Surveying SME Attitudes to Cyber-security. *Journal of Computer Information Systems*, 1–13. https://doi.org/10.1080/08874417.2022.2067791

Winther, T., Øyen, A. H. & Ottesen , L. (2006). *Grunnleggende bedriftsøkonomi*. Oslo Gyldendal Akademisk.

Yazdanmehr, A. & Wang, J. (2016). Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems*, *92*, 36–46. https://doi.org/10.1016/j.dss.2016.09.009.

Zakharova, S. (2020). *Suksessfaktorer ved outsourcing av regnskapstjenester: en kvantitativ tverrsnittstudie* [Masteroppgave, Oslo Met]. https://oda.oslomet.no/oda-xmlui/bitstream/handle/10642/9462/Zakhorova_%C3%98AMAS_2020.pdf?sequence=2.

Vedlegg

Vedlegg 1: Informasjonsskriv til eksperter

Vil du delta i forskningsprosjektet

«Cybersikkerhet»?

Dette er et spørsmål til deg om å delta i et forskningsprosjekt. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

I dette forskningsprosjektet ønsker vi undersøke hvordan bedrifter håndterer cyberangrep ulikt. Videre avdekke nødvendige suksessfaktorer for å lykkes i sin strategi opp mot cybersikkerhet.

Hvem er ansvarlig for forskningsprosjektet?

Forskningsprosjektet er en del av TRANSACT, og Handelshøgskolen (HHN) ved Nord Universitet er ansvarlig. Veileder for masteroppgaven er Anatoli Bourmistrov, og oppgaven skrives av Jakob Severinsen Grønmo, Karianne Pettersen Sunde og Camilla Fleines Christoffersen.

Hvorfor får du spørsmål om å delta?

Du har fått tilbudet om å delta på intervju, fordi du har mye kunnskap om cybersikkerhet og vil hjelpe oss å forstå temaet bedre. Vi vurderer derfor at du sitter på kunnskap som kan hjelpe oss å besvare problemstillingen.

Hva innebærer det for deg å delta?

Metoden som kommer til å brukes i prosjektet er intervju og spørreundersøkelse. Relevant for deg vil dette kun omfatte et intervju.

Intervju

Det kommer til å gjennomføres et semi-strukturert intervju, som skal føre til en samtale om temaet begrenset til informantens kunnskap. Intervjuet er estimert å vare i ca. 45 minutter. Avvik kan forekomme.

Opplysningene som samles inn, kommer til å bli registrert ved et lydopptak som kommer til å bli lagret frem til oppgaven er levert. Oppbevaring av materiale skal følges i henhold til prosjektet TRANSACT.

Det er frivillig å delta

Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg. Dette kommer ikke til å påvirke deg i noen sammenheng ved din arbeidsgiver eller i fremtiden.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

- Det er kun studentene og veileder som kommer til å ha tilgang til dataen som blir hentet.
- All informasjon som kommer fram kommer til å bli anonymt behandlet, og for å skille mellom bedriftene blir det laget nummer for å anonymisere bedriftene.
- Dataen kommer til å bli lagret hvor det er kun veileder og studentene kommer til å ha tilgang.

Hva skjer med personopplysningene dine når forskningsprosjektet avsluttes?

Ettersom prosjektet er en del av TRANSACT til Nord Universitet er det ønskelig at dataen blir brukt videre i fremtiden, men at alle data skal lagres i anonymisert form.

Hva gir oss rett til å behandle personopplysninger om deg?

Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Handelshøgskolen (HHN) ved Nord Universitet har Sikt – Kunnskapssektorens tjenesteleverandør vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Dine rettigheter

Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke opplysninger vi behandler om deg, og å få utlevert en kopi av opplysningene
- å få rettet opplysninger om deg som er feil eller misvisende
- å få slettet personopplysninger om deg
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Hvis du har spørsmål til studien, eller ønsker å vite mer om eller benytte deg av dine rettigheter, ta kontakt med:

Jakob Grønmo, +47 476 21 228.

Karianne P. Sunde, +47 486 06 192

Camilla Christoffersen, +47 483 04 325

Handelshøgskolen i Bodø, Nord universitet, Anatoli Bourmistrov, +47 909 56 042

Vårt personsvernombud: Toril Irene Kringen, personvernombud@nord.no, +47 740 22 750

Hvis du har spørsmål knyttet til vurderingen som er gjort av personverntjenestene fra Sikt, kan du ta kontakt via:

- Epost: personverntjenester@sikt.no eller telefon: 73 98 40 40.

Med vennlig hilsen

	Jakob Grønmo Karianne P. Sunde Camilla Christoffersen
Anatoli Bourmistrov	
(Forsker/veileder)	Studenter

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet cyber sikkerhet, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- å delta i intervju

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

----

(Signert av prosjektdeltaker, dato)

Vedlegg 2: Informasjonsskriv til ledere/ IT – ansvarlig i case-bedriftene

Vil du delta i forskningsprosjektet «Cybersikkerhet»?

Dette er et spørsmål til deg om å delta i et forskningsprosjekt. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål
I dette forskningsprosjektet ønsker vi undersøke hvordan bedrifter håndterer cyberangrep ulikt. Videre avdekke nødvendige suksessfaktorer for å lykkes i sin strategi opp mot cybersikkerhet.

Hvem er ansvarlig for forskningsprosjektet?
Forskningsprosjektet er en del av TRANSACT, og Handelshøgskolen (HHN) ved Nord universitet er ansvarlig. Veileder for masteroppgaven er Anatoli Bourmistrov, og oppgaven skrives av Jakob Severinsen Grønmo, Karianne Pettersen Sunde og Camilla Fleines Christoffersen.

Hvorfor får du spørsmål om å delta?
Du har fått tilbudet om å delta på intervju, fordi du har en ledende posisjon i en av utvalgte bedriftene. Vi vurderer derfor at du sitter på kunnskap som kan hjelpe oss å besvare problemstillingen.

Hva innebærer det for deg å delta?
Metoden som kommer til å brukes i prosjektet er intervju og spørreundersøkelse. Relevant for deg vil dette kun omfatte et intervju.

Intervju
Det kommer til å gjennomføres et semi-strukturert intervju, som skal føre til en samtale om temaet begrenset til informantens kunnskap. Intervjuet er estimert å vare i ca. 45 minutter. Avvik kan forekomme.

Opplysningene som samles inn, kommer til å bli registrert ved et lydopptak som kommer til å bli lagret frem til oppgaven er levert. Oppbevaring av materiale skal følges i henhold til prosjektet TRANSACT.

Det er frivillig å delta
Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg. Dette kommer ikke til å påvirke deg i noen sammenheng ved din arbeidsgiver eller i fremtiden.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger
Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

- Det er kun studentene og veileder som kommer til å ha tilgang til dataen som blir hentet.
- All informasjon som kommer fram kommer til å bli anonymt behandlet, og for å skille mellom bedriftene blir det laget nummer for å anonymisere bedriftene.
- Dataen kommer til å bli lagret hvor det er kun veileder og studentene kommer til å ha tilgang.

Hva skjer med personopplysningene dine når forskningsprosjektet avsluttes?
Ettersom prosjektet er en del av TRANSACT til Nord universitet er det ønskelig at dataen blir brukt videre i fremtiden, men at alle data skal lagres i anonymisert form.

Hva gir oss rett til å behandle personopplysninger om deg?
Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Handelshøgskolen (HHN) ved Nord Universitet har Sikt – Kunnskapssektorens tjenesteleverandør vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Dine rettigheter
Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke opplysninger vi behandler om deg, og å få utlevert en kopi av opplysningene
- å få rettet opplysninger om deg som er feil eller misvisende
- å få slettet personopplysninger om deg
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Hvis du har spørsmål til studien, eller ønsker å vite mer om eller benytte deg av dine rettigheter, ta kontakt med:
Jakob Grønmo, +47 476 21 228.
Karianne P. Sunde, +47 486 06 192
Camilla Christoffersen, +47 483 04 325
Handelshøgskolen i Bodø, Nord universitet, Anatoli Bourmistrov, +47 909 56 042
Vårt personsvernombud: Toril Irene Kringen, personvernombud@nord.no, +47 740 22 750

Hvis du har spørsmål knyttet til vurderingen som er gjort av personverntjenestene fra Sikt, kan du ta kontakt via:

- Epost: personverntjenester@sikt.no eller telefon: 73 98 40 40.

Med vennlig hilsen

Anatoli Bourmistrov	Jakob Grønmo Karianne P. Sunde Camilla Christoffersen
(Forsker/veileder)	Studenter

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet cyber sikkerhet, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- å delta i intervju

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

---

(Signert av prosjektdeltaker, dato)

Vedlegg 3: Informasjonsskriv til ansatte i case-bedriftene

Vil du delta i forskningsprosjektet «Cybersikkerhet»?

Dette er et spørsmål til deg om å delta i et forskningsprosjekt. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål
I dette forskningsprosjektet ønsker vi undersøke hvordan bedrifter håndterer cyberangrep ulikt. Videre avdekke nødvendige suksessfaktorer for å lykkes i sin strategi opp mot cybersikkerhet.

Hvem er ansvarlig for forskningsprosjektet?
Forskningsprosjektet er en del av TRANSACT, og Handelshøgskolen (HHN) ved Nord Universitet er ansvarlig. Veileder for masteroppgaven er Anatoli Bourmistrov, og oppgaven skrives av Jakob Severinsen Grønmo, Karianne Pettersen Sunde og Camilla Fleines Christoffersen.

Hvorfor får du spørsmål om å delta i spørreskjema?
Du har fått tilbudet om å delta på spørreskjema, fordi du er ansatt i en av de bedriftene som deltar i prosjektet.

Hva innebærer det for deg å delta?
Metoden som kommer til å brukes i prosjektet er intervju og spørreskjema. Relevant for deg vil være spørreskjema.

Spørreskjema
Spørreskjemaet sendes ut til flest mulig ansatte i de utvalgte bedriftene. Hvis du velger å delta i prosjektet innebærer det at du fyller ut et spørreskjema. Det vil ta deg ca. 5 minutter. Spørsmålene vil omfatte cybersikkerhet.

Spørreskjemaet blir registrert elektronisk hos nettskjema.no, hvor man kan innhente statistikk etter endt forskning. Oppbevaring av materiale skal følges i henhold til prosjektet TRANSACT.

Det er frivillig å delta
Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.
Dette kommer ikke til å påvirke deg i noen sammenheng ved din arbeidsgiver eller i fremtiden.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger
Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

- Det er kun studentene og veileder som kommer til å ha tilgang til dataen som blir hentet.
- All informasjon som kommer fram kommer til å bli anonymt behandlet, og for å skille mellom bedriftene blir det laget nummer for å anonymisere bedriftene.
- Dataen kommer til å bli lagret hvor det er kun veileder og studentene kommer til å ha tilgang.
- Dataen vil samles inn hos Nettskjema.

Hva skjer med personopplysningene dine når forskningsprosjektet avsluttes?
Ettersom prosjektet er en del av TRANSACT til Nord Universitet er det ønskelig at dataen blir brukt videre i fremtiden, men at alle data skal lagres i anonymisert form.

Hva gir oss rett til å behandle personopplysninger om deg?
Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Handelshøgskolen (HHN) ved Nord Universitet har Sikt – Kunnskapssektorens tjenesteleverandør vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Dine rettigheter
Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke opplysninger vi behandler om deg, og å få utlevert en kopi av opplysningene
- å få rettet opplysninger om deg som er feil eller misvisende
- å få slettet personopplysninger om deg
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Hvis du har spørsmål til studien, eller ønsker å vite mer om eller benytte deg av dine rettigheter, ta kontakt med:
Jakob Grønmo, +47 476 21 228.
Karianne P. Sunde, +47 486 06 192
Camilla Christoffersen, +47 483 04 325
Handelshøgskolen i Bodø, Nord universitet, Anatoli Bourmistrov, +47 909 56 042
Vårt personsvernombud: Toril Irene Kringen, personvernombud@nord.no, +47 740 22 750

Hvis du har spørsmål knyttet til vurderingen som er gjort av personverntjenestene fra Sikt, kan du ta kontakt via:

- Epost: personverntjenester@sikt.no eller telefon: 73 98 40 40.

Med vennlig hilsen

	Jakob Grønmo
Anatoli Bourmistrov	Karianne P. Sunde
	Camilla Christoffersen
(Forsker/veileder)	Studenter

Samtykkeerklæring
Jeg har mottatt og forstått informasjon om prosjektet cyber sikkerhet, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- å delta i intervju

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

---

(Signert av prosjektdeltaker, dato)

Vedlegg 4: Intervjuguide til ekspertinformanter

Bakgrunn

Navn, nåværende posisjon og selskap?

Fortell om din bakgrunn og erfaring knyttet til cybersikkerhet.

Cybersikkerhet og cyberangrep

Hva er cybersikkerhet?

Hva er den vanligste måten å bli hacket på?

Kan du trekke frem ulike typer svindelmetoder? Hvor utbredt er disse?

Er dette et tabu tema? Hvorfor? Vil du anbefale at bedrifter går ut med denne typen informasjon?

Hva er den største feilen bedrifter gjør når det kommer til cybersikkerhet? Hvor ligger oftest svakheten til bedriftene?

Opplever du at folk generelt ikke tar cybersikkerhet på alvor? Eller ser man en endring de siste året/årene?

Hva ønsker hackerne å få ut av et angrep?

Hvis man allerede har blitt hacket, hva burde man gjøre?

Små og mellomstore bedrifter

Små og mellomstore bedrifter har som regel mindre ressurser, hvilke tiltak vil du anbefale disse å iverksette for å forebygge et cyberangrep?

Har du noen tanker om hva som er den beste måten å lære sine ansatte rundt cybersikkerhet? Noen eksempler?

Hva er viktige elementer i opplæring og oppfølging? Noen eksempler?

Ser man tendenser til at noen bedrifter er mer utsatt for å bli angrepet enn andre? F.eks. bransje, sektor og størrelse. Hvorfor? Noen eksempler?

Vedlegg 5: Intervjuguide til ledere/IT i case-bedriftene

Bakgrunn

Navn, nåværende posisjon og selskap?

Fortell om din bakgrunn og erfaring knyttet til cybersikkerhet.

Bedrift

Kan du fortelle om bedriften? Bransje, størrelse og virksomhet?

Hvor mange ansatte?

Hva er bedriftens visjon?

Har dere verdier i bedriften? Er det godt implementert i de ansatte?

"Angrepet"

Har bedriften blitt utsatt for cyberangrep?

Eventuelt: Hvordan skjedde angrepet og hvordan oppdaget dere det?

Hvis dere hadde noen retningslinjer og prosedyrer, fulgte dere de?

Hvor lang tid tok det før dere hadde kontroll på angrepet?

Informerte dere de ansatte?

Cybersikkerhet

Når du hører ordet cybersikkerhet, hva tenker du på da?

Hadde dere egen avdeling knyttet arbeid med cybersikkerhet?

Hvilken strategi / plan hadde dere i forhold til håndtering av eventuelle angrep? Eksempel? Var de ansatte informert og klare over hva denne strategien gikk utpå?

Praktiserer dere tilbakemelding og måling av ytelse på de ansatte? F.eks i form av testing, kontinuerlig opplæring, oppfølging av kunnskap relatert til cybersikkerhet.

I forhold til systemer, har dere rutiner eller funksjoner som sørger for at systemet fungerer? F.eks en test (etisk hacking) eller kontroll

Hadde dere tydelige regler og prosedyrer i forhold til cybersikkerhet? Hva var disse?

Opplæring i bedriften

Hvordan har dere implementert regler og prosedyrer for de ansatte?

Hvilke begrensninger er satt for de ansatte i forhold til avgjørelser?

Praktiserer dere hjemmekontor, og hvilke forholdsregler blir gjort i forhold til cybersikkerhet?

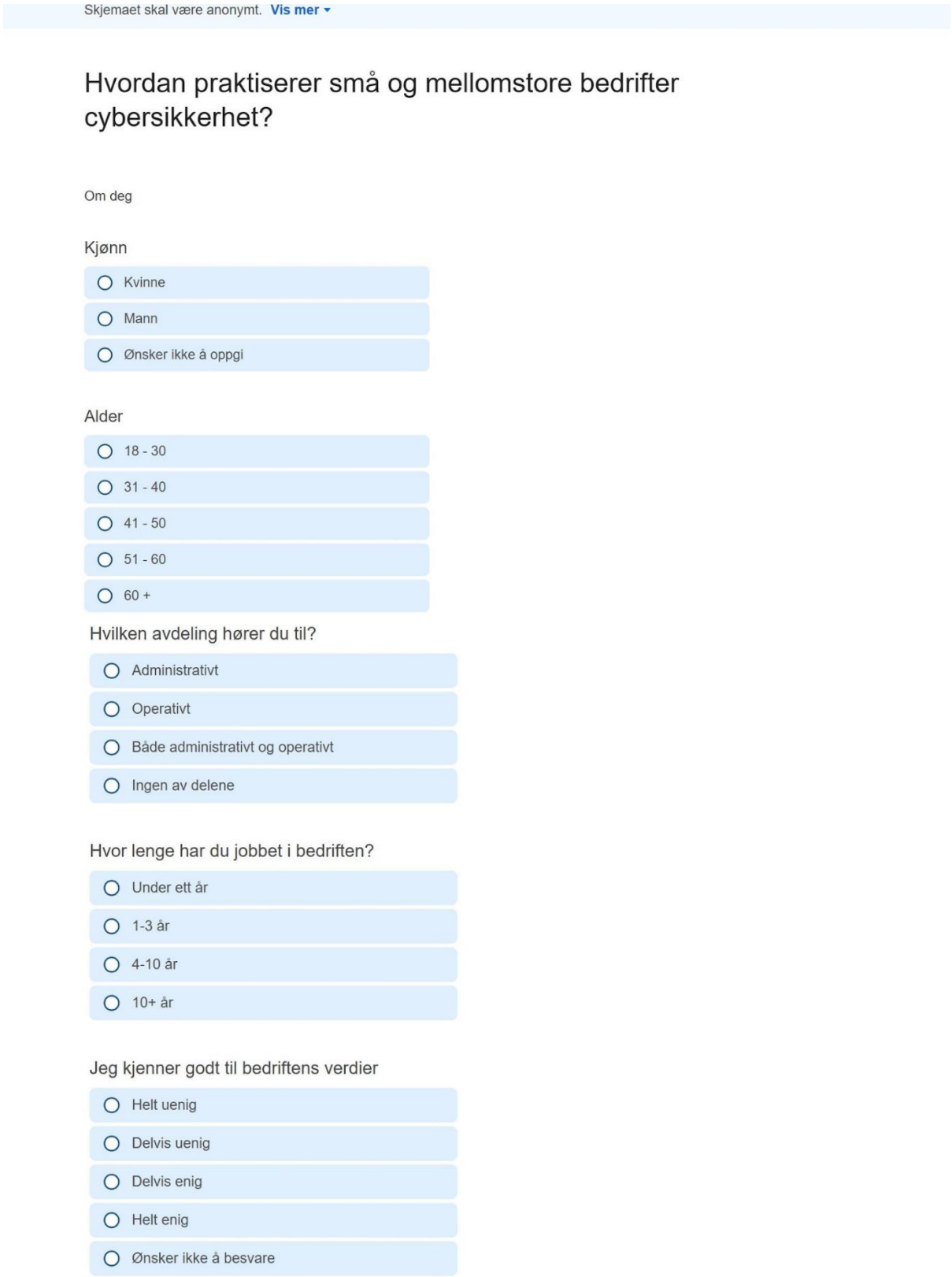
Har dere opplæring og oppfølging av disse reglene og prosedyrene?

Hvordan er kommunikasjonen mellom de ansatte, avdelingene og ledere? Informasjonsflyt i form av? Personlig kontakt / ikke personlig kontakt?

Gir dine ansatte beskjed dersom de mottar en mistenkelig mail?

Hvorvidt har dere kontroll på de ansatte avgjørelser? Får de arbeide selvstendig eller blir de tett fulgt opp av leder / teamleder?

Vedlegg 6: Spørreundersøkelse til ansatte i case-bedriftene



Skjemaet skal være anonymt. Vis mer

Hvordan praktiserer små og mellomstore bedrifter cybersikkerhet?

Om deg

Kjønn

- Kvinne
- Mann
- Ønsker ikke å oppgi

Alder

- 18 - 30
- 31 - 40
- 41 - 50
- 51 - 60
- 60 +

Hvilken avdeling hører du til?

- Administrativt
- Operativt
- Både administrativt og operativt
- Ingen av delene

Hvor lenge har du jobbet i bedriften?

- Under ett år
- 1-3 år
- 4-10 år
- 10+ år

Jeg kjenner godt til bedriftens verdier

- Helt uenig
- Delvis uenig
- Delvis enig
- Helt enig
- Ønsker ikke å besvare

Hva er din oppfatning av cybersikkerhet?

Min bedrift gjør at jeg har god oversikt over trusselbilde rundt cybersikkerhet

- Helt uenig
- Delvis uenig
- Delvis enig
- Helt enig
- Ønsker ikke å besvare

Min bedrift har satt større fokus på cybersikkerhet de siste årene

- Helt uenig
- Delvis uenig
- Delvis enig
- Helt enig
- Ønsker ikke å besvare

Opplæring i bedriften

Jeg har fått tilstrekkelig opplæring på jobb om cybersikkerhet

- Helt uenig
- Delvis uenig
- Delvis enig
- Helt enig
- Ønsker ikke å besvare

Jeg kjenner godt til bedriftens regler og prosedyrer i forhold til å bevare cybersikkerheten

- Helt uenig
- Delvis uenig
- Delvis enig
- Helt enig
- Ønsker ikke å besvare

Jeg følger alltid reglene og prosedyrene som er satt av bedriften

- Helt uenig
- Delvis uenig
- Delvis enig
- Helt enig
- Ønsker ikke å besvare

Hvor ofte får du oppfrisket kunnskapen rundt cybersikkerhet

- Hver uke
- Hver måned
- Hvert halvår
- Hvert år
- Har ikke fått oppfrisket kunnskap

Jeg skulle ønske bedriften satte mer fokus på cybersikkerhet

- Ja
- Nei
- Ønsker ikke å besvare

Kultur i bedriften

Jeg får arbeide selvstendig på jobb

- ○ Helt uenig
- ○ Delvis uenig
- ○ Delvis enig
- ○ Helt enig
- ○ Ønsker ikke å besvare

Jeg får ta avgjørelser på egen hånd på jobb

- ○ Helt uenig
- ○ Delvis uenig
- ○ Delvis enig
- ○ Helt enig
- ○ Ønsker ikke å besvare

Jeg føler frykten for cyberangrep hemmer evnen min til å jobbe selvstendig

- ○ Helt uenig
- ○ Delvis uenig
- ○ Delvis enig
- ○ Helt enig
- ○ Ønsker ikke å besvare

Jeg kan spørre lederne om hjelp hvis jeg er usikker på om noe er trygt

- ○ Helt uenig
- ○ Delvis uenig
- ○ Delvis enig
- ○ Helt enig
- ○ Jeg spør heller andre feks IT-avdelingen eller andre kollegaer om hjelp
- ○ Ønsker ikke å besvare

Jeg melder alltid i fra til ledelsen/IT-avdeling, hvis jeg mottar en mistenkelig mail som kan minne om et cyberangrep

- ○ Helt uenig
- ○ Delvis uenig
- ○ Delvis enig
- ○ Helt enig
- ○ Ønsker ikke å besvare

Jeg melder alltid i fra til ledelsen/IT-avdeling, hvis jeg mottar en mistenkelig mail som kan minne om et cyberangrep

- ○ Helt uenig
- ○ Delvis uenig
- ○ Delvis enig
- ○ Helt enig
- ○ Ønsker ikke å besvare

Har du blitt utsatt for svindel forsøk i jobbsammenheng?

- ○ Ja
- ○ Nei
- ○ Jeg vet ikke hvilke tegn jeg skal se etter for å identifisere et svindelforsøk
- ○ Ønsker ikke å svare

Om du har blitt utsatt for svindel i jobbsammenheng tidligere, meldte du ifra til ledelsen eller IT avdelingen?

- ○ Ja
- ○ Nei
- ○ Ikke relevant

Føler du at du har nok kompetanse til å ha hjemmekontor med tanke på cybersikkerheten

- ○ Helt uenig
- ○ Delvis uenig
- ○ Delvis enig
- ○ Helt enig
- ○ Ønsker ikke å besvare

Er det noe mer du ønsker å tilføye?

Send

Vedlegg 7: Spørreundersøkelse til Alumni

Nettskjema

Hvordan praktiserer små og mellomstore bedrifter cybersikkerhet? Alumni

Kort om prosjektet
Denne spørreundersøkelsen er relatert til TRANSACT-prosjektet, som er et samarbeid mellom Handelshøgskolen (HHN) ved Nord universitet samt nasjonale og internasjonalepartnere. Spørreundersøkelsen tar ca. 3-5 minutter å gjennomføre. For mer informasjon om prosjektet, se https://www.nord.no/transact.
Du mottar dette spørreskjema i anledning masteroppgaven "Cybersikkerhet". Forskningen baserer seg på små og mellomstore bedrifter sin håndtering av cyberangrep. Målet er å avdekke nødvendige suksessfaktorer innenfor bedriftens strategi rundt cybersikkerheten.
Vi ønsker å takke deg for at du bidrar med viktig informasjon til vår forskning. Ved fullførelse av spørreundersøkelsen er du med på å skape økt forståelse og kunnskap om temaet.
Personvern
Det er frivillig å delta i prosjektet. Det vil naturligvis ikke ha noen negative konsekvenser for deg hvis du ombestemmer deg senere og ønsker å trekke deg fra undersøkelsen. Spørreskjemaet inneholder spørsmål som er relatert til cybersikkerhet, og har som formål å finne ut hvilke holdninger ansatte har til temaet.
Dine svar vil bli registrert og lagret elektronisk og det vil ikke være mulig å identifisere deg i undersøkelsen. Vi behandler opplysningene kofidensielt og i samsvar med gjeldene personvernlovverk.
Hvis du har spørsmål til studiene, om prosjektet, eller ønsker å vite mer om dine rettigheter. Ta kontakt med:

Nord Universitet ved Professor Anatoli Bourmistrov, anatoli.bourmistrov@nord.no, telefon 755 17 673

Vårt personvernombud: Toril Irene Kringen, personvernombud@nord.no, telefon 74 02 27 50

Del A: Om deg

A01: Kjønn

Kvinne
Mann
Annet
Ønsker ikke å oppgi

A02: Alder

18 - 30
31 - 40
41 - 50
51 - 60
60 +

Del B: Bedrift

B01: Hvilken avdeling hører du til?

Administrativt
Operativt

Både administrativt og operativt
Ingen av delene

B02: Hvor lenge har du jobbet i bedriften?

Under ett år
1-3 år
4-10 år
10+ år

B03: Jeg kjenner godt til bedriftens verdier

Helt uenig
Delvis uenig
Nøytral
Delvis enig
Helt enig
Ønsker ikke å besvare

Del C. Cybersikkerhet

C01: Hva er din oppfatning av cybersikkerhet?

I hvilken grad er du uenig eller enig med følgende påstander?

C02: Min bedrift gjør at jeg har god oversikt over trusselbilde rundt cybersikkerhet

Helt uenig
Delvis uenig
Nøytral
Delvis enig
Helt enig
Ønsker ikke å besvare

C03: Min bedrift har satt større fokus på cybersikkerhet de siste årene

Helt uenig
Delvis uenig
Nøytral
Delvis enig
Helt enig
Ønsker ikke å besvare

Del D: Opplæring i bedriften

I hvilken grad er du uenig eller enig med følgende påstander?

D01: Jeg har fått tilstrekkelig opplæring på jobb om cybersikkerhet

Helt uenig
Delvis uenig
Nøytral

Delvis enig
Helt enig
Ønsker ikke å besvare

D02: Jeg kjenner godt til bedriftens regler og rutiner i forhold til å bevare cybersikkerheten

Helt uenig
Delvis uenig
Nøytral
Delvis enig
Helt enig
Ønsker ikke å besvare

D03: Jeg følger alltid reglene og rutinene som er satt av bedriften

Helt uenig
Delvis uenig
Nøytral
Delvis enig
Helt enig
Ønsker ikke å besvare

D04: Jeg vet hva jeg skal gjøre hvis bedriften blir utsatt for et cyberangrep

Helt uenig
Delvis uenig
Nøytral
Delvis enig
Helt enig
Ønsker ikke å besvare

D04: Hvor ofte får du oppfrisket kunnskapen rundt cybersikkerhet i regi av bedriften

Hver uke
Hver måned
Hvert halvår
Hvert år
Har ikke fått oppfrisket kunnskap

D05: Jeg skulle ønske bedriften satte mer fokus på cybersikkerhet

Ja
Nei
Ønsker ikke å besvare

Del E: Kultur i bedriften

I hvilken grad er du uenig eller enig med følgende påstander?

E01: Jeg får arbeide selvstendig på jobb

Helt uenig

Delvis uenig
Nøytral
Delvis enig
Helt enig
Ønsker ikke å besvare

E02: Jeg får ta avgjørelser på egen hånd på jobb

Helt uenig
Delvis uenig
Nøytral
Delvis enig
Helt enig
Ønsker ikke å besvare

E03: Jeg føler frykten for cyberangrep hemmer evnen min til å jobbe selvstendig

Helt uenig
Delvis uenig
Nøytral
Delvis enig
Helt enig
Ønsker ikke å besvare

E04: Jeg kan spørre lederne om hjelp hvis jeg er usikker på om noe er trygt

Helt uenig
Delvis uenig
Nøytral
Delvis enig
Helt enig
Ønsker ikke å besvare

E05: Jeg melder alltid i fra til ledelsen/IT-avdeling, hvis jeg mottar en mistenkelig mail som kan minne om et cyberangrep

Helt uenig
Delvis uenig
Nøytral
Delvis enig
Helt enig
Ønsker ikke å besvare

E06: Jeg syns at kommunikasjonen mellom ansatte og ledere er god

Helt uenig
Delvis uenig
Nøytral
Delvis enig

Helt enig
Ønsker ikke å besvare

E07: Kommunikasjonen mellom ansatte og ledere inneholder personlig kontakt (ansikt til ansikt)

Helt uenig
Delvis uenig
Nøytral
Delvis enig
Helt enig
Ønsker ikke å besvare

E08: Jeg føler jeg har nok kompetanse til å ha hjemmekontor med tanke på cybersikkerheten

Helt uenig
Delvis uenig
Nøytral
Delvis enig
Helt enig
Ønsker ikke å besvare

E07: Hvor ofte blir du utsatt for svindelforsøk

Hver dag
Hver uke
Hver måned
Har ikke blitt utsatt for svindelforsøk
Ønsker ikke å svare

E08: Om du har blitt utsatt for svindel i jobbsammenheng tidligere, meldte du ifra til ledelsen eller IT avdelingen?

Ja
Nei
Ikke relevant

E09: Er det noe mer du ønsker å tilføye?

Fyll inn e-post i feltet under hvis du ønsker å få tilsendt den ferdige oppgaven.

Generert: 2023-05-16 16:02:50.