Masteroppgave

NTNU
Norges teknisk-naturvitenskapelige universitet
Fakultet for ingeniørvitenskap
Institutt for vareproduksjon og byggteknikk

Edvard Listøl

Perspektiver på digital sikkerhet i byggenæringen

En studie av byggenæringens holdninger til BIM-sikkerhet i lys av ISO 19650-5

Masteroppgave i Bygg- og miljøteknikk / Digitale byggeprosesser
Veileder: Eilif Hjelseth
Juni 2022

NTNU
Kunnskap for en bedre verden

Edvard Listøl

Perspektiver på digital sikkerhet i byggenæringen

En studie av byggenæringens holdninger til BIM-sikkerhet i lys av ISO 19650-5

Masteroppgave i Bygg- og miljøteknikk / Digitale byggeprosesser
Veileder: Eilif Hjelseth
Juni 2022

Norges teknisk-naturvitenskapelige universitet
Fakultet for ingeniørvitenskap
Institutt for vareproduksjon og byggteknikk

NTNU
Norwegian University of
Science and Technology

Sammendrag

I risikovurderingen til Nasjonal sikkerhetsmyndighet (NSM, 2021) trekkes det frem hvordan store samfunnsverdier i større grad legges over i det digitale domenet. Ny teknologi og bruksmønstre tilknyttet dette skaper derfor nye muligheter i det digitale rom som trussel-aktører kan utnytte. Bygningsinformasjonsmodeller (BIM) står allerede sentralt i dagens byggeprosjekter, samtidig som teknologien konstant er under utvikling. Mange av Norges kritiske infrastrukturer har tilknytning til bygg- og anlegg som allerede bruker, eller kommer til å bruke BIM i fremtiden. Selv om BIM gir mange positive effekter, er det også en økt risiko for misbruk av informasjonen BIM tilgjengeliggjør eller gjennom delingsgraden slik teknologi fremskaper.

Standarden ISO 19650 gir et felles rammeverk for informasjonsforvaltning gjennom hele livssyklusen til et byggverk ved bruk av BIM, hvor ISO 19650 del 5 fokuserer på sikkerhet. Det finnes i dag lite forskning omhandlende ISO 19650 del 5 og BIM-sikkerhet, likevel hevder (NSM, 2022a) at næringslivet generelt mangler sikkerhetsfokus. Til sammenligning har fokuset på HMS i byggenæringen økt de siste årene. Dette har resultert i systemer og rutiner som reduserer risikoen for ulykker. Kan erfaringer fra HMS overføres til digital sikkerhet? Denne studiens formål er å undersøke hvordan den digitale sikkerhetskulturen for Norsk byggenæring kan bedres ved hjelp av ISO 19650-5. Følgende problemstilling og forskningsspørsmål er valgt: *På hvilken måte kan ISO 19650-5 bidra til å bedre den digitale sikkerhetskulturen i Norske byggeprosjekter?*

1. Hvordan er den digitale sikkerhetskulturen blant aktører i byggenæringen i dag?
2. Hva kan man lære av HMS?
3. Hvilke tiltak kan gjøres i praksis basert på ISO 19650-5?

Studiens metodikk er kvalitativ og fortolkende, med grunnlag i litteraturstudie og intervjuer. Litteraturstudiens søk på Scopus, Google scholar og Oria resulterte i 8 artikler fra ulike deler av verden. I tillegg ble totalt 7 intervjuer gjennomført med aktører fra byggenæringen. Aktørene representerte byggherre, rådgiver, arkitekt, entreprenør og produsent.

Tidligere forskning viser at det generelt mangler kunnskap om BIM-sikkerhet hos aktører i dag. Denne studien bekrefter at dette også gjelder den norske byggenæringen, noe som kan skyldes digitaliseringens dilemmaer og fremtidens usikkerheter. HMS erfaringer viser at et tydelig lovverk, gode systemer/rutiner og tilpasset opplæring har hatt god effekt, noe intervjuene viser at mangler innen digital sikkerhet. Rammeverket ISO 19650-5 viser seg å ha mange prinsipielle likhetstrekk med HMS-prosessene, noe som gir grunnlag for å tro at tilsvarende metoder kan brukes for å bedre den digitale sikkerheten. Ved å kombinere tiltak fra ISO 19650-5 med etablerte HMS-rutiner, kan byggenæringen bli mer bevisst på sikkerhetsrisikoer og hvordan disse bør forebygges eller håndteres.

Basert på studiens funn anbefales 5 tiltak for å bedre sikkerhetskulturen: (1) Krav til BIM-sikkerhet, (2) Sensitivitetsvurdering i alle ledd, (3) Etablere systemer og rutiner tilsvarende HMS, (4) Innføre tilpassede opplæringskurs, (5) Øke lederengasjementet. Ettersom prinsippene bak sikkerhetshåndteringen er svært like, kan et tettere samarbeid mellom HMS-avdelingen som har erfaringen, BIM-avdelingen som kan det byggetekniske og IT-avdelingen som kan det datatekniske, skape bedre sikkerhetsløsninger for byggenæringen i fremtiden.

Abstract

In the risk assessment from Norwegian National authority of security (NSM, 2021) it is brought forward how great values of society is transferred to the digital domain. The new technology and its possibilities come with added risk due to how external actors can access and misuse this data. Building information models (BIM) is already a key element in today's construction projects, while technology related to this is rapidly advancing. Several of the critical infrastructures in Norway today is related to building and construction, which is already, or will be using BIM models in the future. Although there are great advantages with BIM models, it also comes with added risk of exploitation of the information made available from the model.

ISO 19650 is a standard that gives a common framework for how information is managed throughout the lifecycle of a building structure using BIM, where ISO 19650 part 5 focuses on security. There is currently little research around ISO 19650-5, and BIM security, yet (NSM, 2022a) claims that businesses are in general lacking focus on security. In comparison, the focus on Health and Safety has increased in recent years. This has resulted in systems and routines that reduce the risk of accidents at construction sites. Can the experience seen from Health and Safety be transferred to the aspect of data security? This study will investigate whether the digital security culture within Norwegian construction work can be improved with ISO 19650-5. The following problem and research question has been chosen: *In what way can ISO 19650-5 contribute to improving the digital security culture within Norwegian construction projects?*

1. How is the digital security culture among actors in construction work today?
2. What can be learned from Health and Safety?
3. What measures can be done based on ISO 19650-5?

The method of the study is qualitative and interpreting, based on literature studies and interviews. The literature studies from Scopus, Google Scholar, and Oria resulted in 8 articles from various parts of the world. In addition, 7 interviews were conducted with workers in construction, representing builders, consultants, architects, contractors, and producers.

Previous research shows that there is a general lack of knowledge around BIM-security among actors today. This study confirms that this also applies to the Norwegian construction industry, which might come from the dilemmas of digitalization and uncertainties of the future. Experience from Health and Safety shows how a clear legal framework, good systems/routines, and adapted training has had a good effect, which according to the interviews are missing in digital security today. The ISO 19650-5 is apparent to have principal similarities with the Health and Safety processes, which gives reasons to believe some of the same methods can be used for digital security in construction. By combining measures from ISO 19650-5 and the established Health and Safety routines, the construction industry can become more aware of the risks and how they should be prevented or handled.

Based on this study's findings, 5 measures are recommended to improve the security culture: (1) demand BIM-security, (2) conduct sensitivity assessments at all stages, (3) establish systems and routines like what is seen in Health and Safety, (4) implement specialized training, (5) increase the engagement from senior parts of the organization. As the principles behind the security management are similar, a closer collaboration between the Health and Safety department with the experience, the BIM department with the constructional knowledge, and the IT department who knows the IT-technical, can yield improved security solutions for the construction industry in the future.

Forord

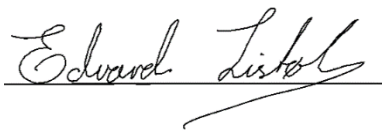
Denne masteroppgaven er skrevet våren 2022 og tilsvarer 30 studiepoeng. Oppgaven representerer det avsluttende arbeidet på studieretningen Digitale byggeprosesser, underlagt masterprogrammet Bygg- og miljøteknikk ved Norges teknisk-naturvitenskapelige universitet (NTNU).

Masteroppgaven er en studie av den Norske byggenæringens digitale sikkerhetskultur. Tematikken fanget min interesse allerede høsten 2021. Likevel har jeg gått mange blindveier før jeg havnet på denne oppgavens avgrensing. Ettersom det finnes svært lite forskning på området har prosessen vært vanskelig, men også svært spennende og lærerik. Mitt ønske er at kunnskapen fra denne oppgaven skal bli nyttig for byggenæringens videre utvikling og i nasjonalt sikkerhetsarbeid. Dette er samtidig bare starten på det jeg tror kommer til å bli mye viktigere i fremtiden. Derfor håper jeg også at oppgaven kan gi et bedre utgangspunkt for videre forskning.

Jeg ønsker å rette en stor takk til min veileder Eilif Hjelseth for gode innspill og tanker rundt oppgaven. Dette har vært til stor hjelp i stunder hvor jeg har stått fast. Videre ønsker jeg å takke alle involverte aktører som har tatt seg tid til å stille opp i intervjuene! Deres ærlighet og videreformidling har vært helt avgjørende for oppgavens resultat. Videre ønsker jeg å takke studieprogrammet på Gjøvik, og spesielt Erling Onstein og Ole Jonny Klakegg for deres engasjement og tilretteleggelse. Studiet har lært oss å tenke helhetlig, og samtidig gitt rom for å utforske det vi selv har hatt interesse for.

Jeg ønsker også å rette en stor takk til min gode venn Olve Aaberg, for gode diskusjoner, tilbakemeldinger og innspill. Det har betydd svært mye å ha deg som sparringspartner gjennom hele prosessen. Til slutt ønsker jeg å takke min nærmeste familie og venner for støtten og hjelpen jeg ellers har fått.

Gjøvik, juni 2022



Edvard Listøl

Innhold

Figurer

Tabeller

Forkortelser

NTNU	Norges teknisk-naturvitenskapelige universitet
BIM	Bygningsinformasjonsmodell/modellering
IT	Informasjonsteknologi
NSM	Nasjonal sikkerhetsmyndighet
HMS	Helse, miljø og sikkerhet
SHA	Sikkerhet, helse og arbeidsmiljø

1 Introduksjon

1.1 Bakgrunn

Den store utviklingen innen teknologi de siste årene vil også sette høyere krav til informasjonssikkerhet. Datamaskiner har blitt en naturlig del av hverdagen til svært mange og bidratt til å forenkle arbeidsoppgaver i flere deler av næringslivet. Selv om byggenæringen generelt har vært på etterskudd innen digitalisering, har det skjedd en utvikling av teknologi også her. (Statsbygg, 2021) beskriver blant annet bygningsinformasjonsmodeller (BIM) som en av de sentrale tiltakene i digitaliseringen av byggenæringen. Tradisjonelt sett har tegninger blitt benyttet til å formidle informasjon i byggeprosjekter. Utfordringen med dette er at tegningene raskt blir utdaterte etter hvert som endringer gjøres. BIM modeller skiller seg fra 3D modeller ved at bygningskomponentene (dør, vindu, ventilasjon, etc.) også er tilknyttet informasjon. BIM bidrar til at endringer kan oppdateres umiddelbart via skyløsninger, noe som reduserer risikoene for å bygge etter utdaterte tegninger. En av BIM-modellens store fordel er måten modellene tilgjengeliggjør et helhetsbilde for alle parter. Dette gjør samhandling og gjensidig forståelse på tvers av fagfelt enklere i prosjekteringen. Disse faktorene kan skape bedre arbeidsflyt, mindre feil og økt effektivitet for de involverte. Som en konsekvens av teknologien, blir uante mengder informasjon tilgjengelig i langt større grad. Dette fører til at nye ukjente trusler og sårbarheter vokser frem. På hvilken måte kan dette skape utfordringer?

I risikovurderingen for 2021 fremhever (NSM, 2021) hvordan store samfunnsverdier i større grad legges over i det digitale domenet. Ny teknologi og bruksmønstre tilknyttet dette skaper derfor nye muligheter i det digitale rom som trussel-aktører kan utnytte. I risikovurderingen for 2022 beskriver (NSM, 2022a) hvordan trusselen i økende grad rettes mot leverandørkjeder, og virksomheter som indirekte har med nasjonale verdier å gjøre fremfor direkte angrep.

> *«Det er i mange tilfeller enklere å få tilgang til en virksomhets teknologi, bedriftshemmeligheter eller annen sensitiv informasjon gjennom å utnytte en leverandør eller underleverandør enn ved å ramme en virksomhet direkte. Verdikjedene utnyttes på mange måter.» (NSM, 2022a)*

Mange av Norges kritiske infrastrukturer har tilknytning til bygg og/eller anlegg som allerede bruker, eller kommer til å bruke BIM i fremtiden. Dette kan være demninger, kraftverk, veier, sykehus, flyplasser, forsvarsbygninger etc. Som en følge av den store mengden informasjon som BIM-modeller og annen teknologi tilgjengeliggjør, er det en økt risiko for at sikringstiltak, materialvalg, bygningers oppbygning og svake punkter avsløres dersom informasjonen blir tilgjengelig for trusselaktører.

«A simple Ctrl+F could be enough for people to know where the Achillies´heel of a project or facility is.» (Piazzi, 2022)

(Piazzi, 2022) uttrykker hvordan sensitiv informasjonen «enkelt» kan søkes opp. Dette er ikke nødvendigvis så enkelt som det høres ut, ettersom det forutsetter at en vet hva det søkes etter. På en annen side er det en mulighet, og kan derfor utgjøre en trussel. Én av flere utfordringer med BIM og sikkerhet er balansegangen mellom skjerming av informasjon, og deling av informasjon. For å kunne unngå at verdifull informasjon blir delt med uvedkommende mener (NSM, 2022a) at vi trenger økt årvåkenhet. De uttrykker tydelig hvordan digital sikkerhet er et felles ansvar, og ikke et ansvarsområde for en liten gruppe mennesker, slik IT-avdelinger ofte har vært. Ifølge ((al, 2021), s. 243) viser digitalisering til organisering av samfunnet på måter som ikke har vært mulig tidligere ved å koble mennesker, organisasjoner, systemer og teknologier sammen på enkle måter. Digitalisering handler derfor ikke bare om hvilken teknologi som finnes, men hvordan den blir anvendt. Dette gjør at menneskene og prosessene rundt også må kunne spille på lag med teknologien.

Både Covid-19 pandemien og den pågående Ukraina krigen viser hvor raskt verdensbilde kan endre seg, og hvor avhengig samfunnet er av hverandre og teknologien. Som følge av blant annet teknologi har verdenssamfunnet blitt mer globalisert, noe som også fører til at internasjonale virksomheter etablerer seg i norsk næringsliv. Bygg- og anleggsbransjen består i større grad av utenlandsk arbeidskraft sammenlignet med tidligere. Utenlandske entreprenørselskap er også i ferd med å etablere seg i det norske markedet. (Strømmen, 2019) beskriver hvordan Kinesiske entreprenører ser på Norge som et springbrett for å etablere seg i det europeiske anleggsmarkedet. (Asgeir Leine Pedersen, 2020) gjorde en studie på hvorfor Kinesiske entreprenører etablerer seg i blant annet Norge sett fra et økonomisk og markedsorientert perspektiv. Få har imidlertid stilt spørsmål til om Norge bør overlate byggingen av infrastruktur og nasjonale verdier til utenlandske virksomheter.

(Standard-Norge, 2021) beskriver ISO 19650-serien som en standard som gir et felles rammeverk for informasjonsforvaltning gjennom hele livssyklusen til et byggverk ved bruk av BIM. ISO 19650 består av 5 deler, hvor del 5 kalles *«Security minded approach to information management»* og ble publisert i 2020. Artikkelen til (Piazzi, 2022) beskriver hvorfor ISO 19650-5 er en svært relevant standard for byggenæringen som få har benyttet i dag. ISO 19650-5 viser til hvilke prinsipper og prosedyrer en organisasjon bør benytte for å ivareta sikkerheten i informasjonsforvaltningen med BIM gjennom alle ledd. Kan denne bidra til å bedre sikkerhetskulturen i byggenæringen?

1.2 Formål og Problemstilling

Formålet med denne studien er å kaste lys over dagens digitale sikkerhetskultur i den norske byggebransjen. Basert på studiens resultater og egen fortolkning skal oppgaven komme med anbefalinger som kan bidra til å øke fokuset på sikkerhet. Med et økt fokus, god kultur og gode prosesser øker sannsynligheten for å forebygge uheldige informasjonsdelinger. Med bakgrunn i oppgavens tematikk, er ISO 19650-5 et sentralt rammeverk å se i sammenheng med digital sikkerhet i byggenæringen. Spørsmålet er imidlertid om den vil gjøre sikkerhetskulturen bedre? Oppgavens hovedproblemstilling er derfor:

På hvilken måte kan ISO 19650-5 bidra til å bedre den digitale sikkerhetskulturen i Norske byggeprosjekter?

For å besvare problemstillingen, er det utarbeidet tre forskningsspørsmål:

Hvordan er den digitale sikkerhetskulturen blant aktører i byggenæringen i dag?

Første forskningsspørsmål handler om å kartlegge dagens sikkerhetskultur i den norske byggenæringen. Tanken bak forskningsspørsmålet er å gi en tydeligere pekepinn på hvordan den digitale sikkerhetskulturen faktisk er i dag. Det er først når en vet hvordan dagens situasjon er, at en eventuell ny kurs kan pekes ut.

Hva kan man lære av HMS?

Selv om det er gjort lite forskning på digital sikkerhetskultur i byggebransjen, vet mange likevel at sikkerhetskulturen innen HMS har hatt en positiv utvikling gjennom årene. Derfor er det interessant å undersøke om det finnes erfaringer og metoder fra HMS-siden som kan være overførbare til digital sikkerhet.

Hvilke tiltak kan gjøres i praksis basert på ISO 19650-5?

Det siste forskningsspørsmålet skal bidra til å trekke frem hvilke konkrete tiltak fra standarden som er relevante for norske forhold. En standard kan virke overveldende og diffus for enkelte, derfor er det ønskelig å presentere noen av standardens tiltak på en mer konkretisert måte. Dette skal også bidra til å besvare hovedproblemstillingen.

1.3 Avrensninger og rammer

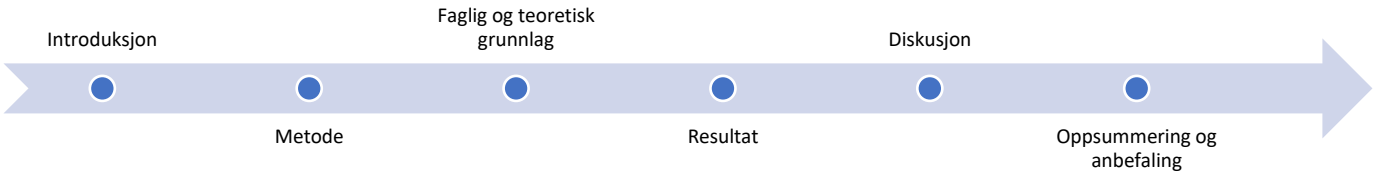
Flere av artiklene som er innhentet gjennom litteraturstudiet og presentert i forprosjektet (Listøl, 2021a) viser at teknologien for å løse informasjonssikkerhetsutfordringer i byggeprosesser allerede finnes, selv om den ikke nødvendigvis er tilpasset byggebransjen. Med bakgrunn i dette har denne studien i større grad rettet seg mot aktørers holdninger og fokus på sikkerhet under Norske forhold.

Følgende avgrensninger og rammer er satt for oppgaven:

- Studiet fokuserer på menneskers holdninger til digital sikkerhet og HMS i byggebransjen og sammenligner dette.
- Oppgaven sammenligner likheter og forskjeller mellom ISO 19650-5 og HMS prosesser.
- Det er intervjuet ulike deler av byggenæringen for å danne et bredere bilde av problemstillingen. Det er ikke avgrenset til ett perspektiv, men det helhetlige bildet vektlegges.
- Studiet er ikke tilknyttet et spesifikt prosjekt.
- Det er ikke gått i dybden på detaljerte arbeidsoppgaver, hverken på ISO 19650-5 eller HMS-siden. Dette hadde ført til at viktige sammenhenger uteble.

Studien er begrenset av tid i tillegg til at alle intervjuer, litteraturstudie, analyse og diskusjon gjøres av én person. Flere intervjuer, perspektiver og synspunkt kunne blitt inkludert dersom det hadde vært mer tid tilgjengelig. Ettersom det finnes minimalt med forskning på området er det er valgt å se det store bildet i oppgaven. intervjuene er derfor gjort med både byggherrer, rådgiver, arkitekt, produsent og entreprenører. Oppgaven har kun valgt å inkludere del 5 av ISO 19650 serien som følge av oppgavens omfang og tidsaspekt. Både del 1, 2 og 3 er imidlertid svært relevante å se i sammenheng med del 5 ved videre forskning (Se videre arbeid, kapittel 6.3).

1.4 Oppgavens oppbygning



Figur 1: Oppgavens oppbygning

1. **Introduksjon** presenterer oppgavens tematikk, underbygger behovet for kunnskap på området og viser til kunnskapsgapet i forskningen. Dette danner grunnlaget for oppgavens problemstilling og forskningsspørsmål. Til slutt legges rammene og avgrensningene for oppgaven.
2. **Forskningsmetode** beskriver hvordan det er gått frem for å løse problemstillingen. Dette starter med en begrunnelse av forskningsmetodene som brukes. Videre beskrives planleggingen, gjennomføringen og analysen av litteraturstudien og intervjuene, før det til slutt blir gjort en evaluering av metoden i lys av pålitelighet, troverdighet, overførbarhet og bekreftbarhet.
3. **Teoretisk og faglig rammeverk** legger frem basiskunnskap som er relevant for å forstå oppgaven. Først presenteres lovverket (sikkerhetsloven), grunnleggende sikkerhetsbegreper og definisjoner, deretter en modell for sikkerhetshåndtering, til slutt beskrives ISO 19650-5 og HMS prosesser i grove trekk.
4. **Resultat** presenterer intervjuresultatene. Holdninger og erfaringer med HMS og digital sikkerhet er det som legges frem. Til slutt sammenlignes ISO 19650-5 med vanlige HMS-aktiviteter for å danne et bilde av likheter og forskjeller.
5. **Diskusjon** trekker frem årsaker og perspektiver til dagens sikkerhetskultur med grunnlag i resultat, teori og tidligere forskning. Erfaringer og utfordringer med HMS blir diskutert i lys av usikkerheter og dilemmaer.
6. **Oppsummering og anbefaling** skal samle trådene og komme med svar på både forskningsspørsmålene og problemstillingen. Anbefalte tiltak basert på funn og diskusjon presenteres til slutt.

2 Forskningsmetode

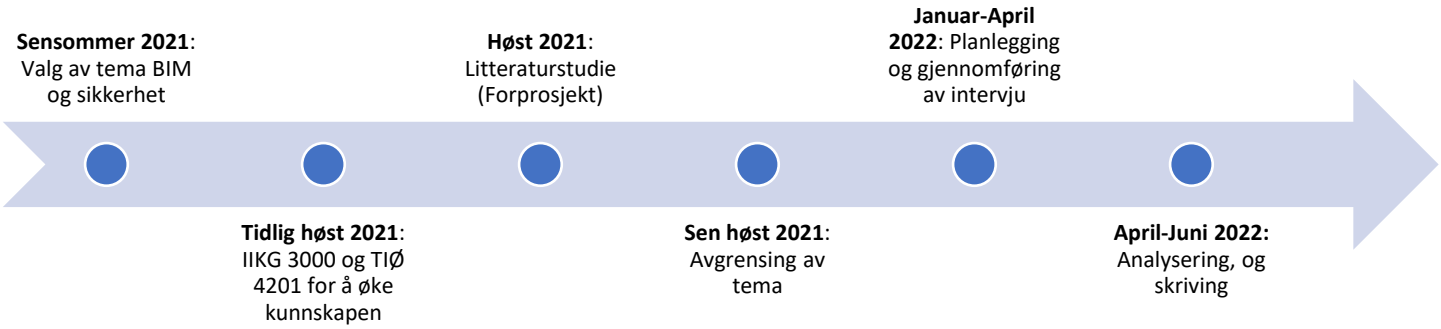
I dette kapittelet blir oppgavens metode presentert. Målet med kapittelet er å redegjøre for valgene som er tatt og hvorfor de er tatt. En beskrivelse av forfatters lærdom av prosessen blir utdypet i egenevalueringen sammen med en vurdering av metodens troverdighet, pålitelighet, overførbarhet og bekreftbarhet.

2.1 Valg av metode

Valg av forskningsmetode er basert på oppgavens problemstilling og formål. De vanligste forskningsmetodene er kvalitativ, kvantitativ eller en kombinasjon av begge. ((Asbjørn Johannessen, 2021), s. 23) beskriver kvantitativ tilnærming som der man eksempelvis gjør en spørreundersøkelse, teller opp fenomener og kartlegger utbredelsen gjennom et tallbasert resultat. Hvis man er ute etter mer detaljert og utfyllende informasjon for å belyse et bestemt tema skriver ((Asbjørn Johannessen, 2021), s. 23) at en dialog med et utvalg av personer kan gjøres gjennom for eksempel intervjuer. Dette kan være hensiktsmessig når en skal undersøke fenomener vi ikke kjenner spesielt godt, og som det finnes lite forskning på.

I denne oppgaven er det gjort en kvalitativ tilnærming. Dette er med grunnlag i studiens fokus på menneskelige holdninger og prosesser, som i mindre grad er kvantifiserbare. Resultatene baseres i større grad på synspunkter som avdekkes gjennom ulike intervjuer. For å kartlegge dagens digitale sikkerhetskultur, er det valgt å gjennomføre intervjuer av personer med ulikt utgangspunkt og perspektiv. Representanter for byggherre, entreprenør, rådgiver, arkitekt og produsent ble intervjuet for å omfavne en stor del av bransjen. Litteraturstudiet gjennomført i forprosjektet (Listøl, 2021a) bidro til valg av oppgavens fokus og ledet til valget av metode.

Det er bevisst valgt å vektlegge metodikken til bøkene *«Introduksjon til samfunnsvitenskapelig metode»* (Asbjørn Johannessen, 2021) og *«Det kvalitative forskningsintervju»* (Steinar Kvale, 2021). Hensikten med konsekvent bruk av disse bøkene er å skape bedre sammenheng og flyt i den metodiske tilnærmingen. Ved å benytte mange ulike tilnærminger, kan metoden fremstå mer rotete. Likevel skal det nevnes at boken *«Hvordan gjennomføre undersøkelser?»* (Jacobsen, 2022) også var aktuell til formålet.



Figur 2: Tidslinje arbeidsprosess

Interessen for sikring av bygg har vært tilstede allerede fra studiets begynnelse og vokst ytterligere i løpet av de siste to årene, ettersom dette har virket meningsfylt og viktig. Sommeren 2021 ble det fattet større interesse for digitale trusler og samfunnssikkerhetsperspektivet. Sensommeren 2021 var tanken å gå mer teknisk inn på løsninger som skulle sikre mot deling av sensitiv informasjon. Denne tankegangen viste seg utover høsten 2021 å være i overkant utfordrende, da mange av løsningene allerede eksisterte, eller ikke var gjennomførbare innenfor de gitte rammene for tid og personlig ferdighetsnivå. For å øke eget kunnskapsnivå på tematikken, ble det besluttet å ta tilleggsfagene *TIØ 4201 – Risikohåndtering, Samfunnssikkerhet og kritisk infrastruktur*, og *IIKG 3000 – Introduksjon til informasjonssikkerhet og personvern*. Kunnskapen som ble tilegnet gjennom disse fagene har vært til stor hjelp i det videre arbeidet. Fordypningsprosjektet som ble gjennomført parallelt, handlet i stor grad om å finne tidligere litteratur på tematikken. Det var også i dette faget forfatter ble introdusert for ISO 19650-5 som omhandlet sikkerhetsperspektivet.

Etter mange gode råd fra venner, lærere, veileder og ved hjelp av litteraturstudiets resultat, ble det derfor besluttet å gå vekk fra tekniske løsninger ettersom behovet i større grad pekte mot manglende fokus og bevissthet. Dette ble derfor det interessante å studere videre utover våren 2022. Alle disse faktorene førte til oppgavens forskningsspørsmål som videre har blitt utviklet gjennom arbeidsprosessen.

2.2 Litteraturstudier

Ifølge (Aveyard, 2010) er litteraturstudie en omfattende studie og tolkning av litteratur som relaterer seg til et bestemt emne. I denne studien har relevant litteratur blitt innhentet og analysert høsten 2021 i forprosjektet (Listøl, 2021a). Målet med litteraturstudien var å skape oversikt over tidligere forskning på tematikken, samt avdekke kunnskapsgap.

Det er innhentet litteratur fra ulike deler av verden (UK, Kina, Brasil og Australia), noe som gir et bredere bilde av hva som er gjort og hva som ikke er gjort på området. Majoriteten av litteraturen er av nyere dato, noe som er naturlig ettersom dette er et fremvoksende problem i takt med den teknologiske utviklingen. Det har generelt vært utfordrende å finne informasjon tilknyttet temaet BIM og sikkerhet (security). Spesielt finnes det lite forskning omhandlende ISO 19650-5. Litteraturstudiens resultater presenteres i kapittel 3.4.

2.2.1 Valg av søkemotorer

Det er valgt å benytte søkemotorene «Scopus», «Oria» og «Google Scholar» som er kjente og veletablerte databaser for forskningsartikler. Valget er basert på erfaring fra tidligere prosjektarbeid gjennom studiet i tillegg til at de ble presentert i faget TVB4500-fordypningsprosjekt som pålitelige søkemotorer. Noen av artiklene har vært mulig å finne via flere av søkemotorene. Dette har bidratt til å øke troverdigheten til søketreffene som er gjort, og artiklene som er innhentet.

Scopus

Ifølge (Scopus, 2022) er Scopus en omfattende abstrakt- og siteringsdatabase som kombinerer berikede data med vitenskapelig litteratur på tvers av et bredt spekter av disipliner. Scopus identifiserer eksperter og gir tilgang til pålitelige data, beregninger og analytiske verktøy.

Oria

Søketjenesten Oria er en felles portal til det samlede materialet som finnes ved de fleste norske fag- og forskningsbibliotek. Supplert med en mengde elektronisk materiale fra åpne kilder, gir Oria en enhetlig tilgang til materiale som bøker, elektroniske bøker, tidsskrifter, elektroniske tidsskrifter, dokumenter, artikler, musikk og filmer. (UNIT, 2022)

Google Scholar

Google Scholar er en database for å søke etter vitenskapelig litteratur. Fra ett sted kan en søke på tvers av mange disipliner og kilder som artikler, avhandlinger, bøker, sammendrag og rettsuttalelser, fra akademiske forlag, profesjonelle foreninger, nettarkiver, universiteter og andre nettsteder. Google Scholar hjelper med å finne relevant arbeid over hele verden av vitenskapelig forskning. (Google-scholar, 2022)

2.2.2 Litteraturstudiens fremgangsmåte

Under selve søkeprosessen ble det benyttet søkeord som inneholdt «BIM» og «security» i flere ulike kombinasjoner med bindeordet «AND». Disse søkeordene ga alt fra få til mange treff. Søkeordene som gav flest resultater var de som hadde ordene «BIM» og «security» i seg. Det ble også gjort flere søk med «ISO 19650 part 5» og «ISO 19650-5». Det ble i enkelte databaser gjort flere treff på disse søkeordene. Artiklene som dukket opp omhandlet likevel ikke part 5, men fokuserte ofte på de andre delene av ISO 19650-serien. Part 5 ble likevel nevnt i oppgaven som en tilhørende del av serien, noe som forklarer mengden treff, spesielt i Google scholar. Blant de relevante artiklene som ble funnet, var det kun én som konkret omhandlet ISO 19650-5.

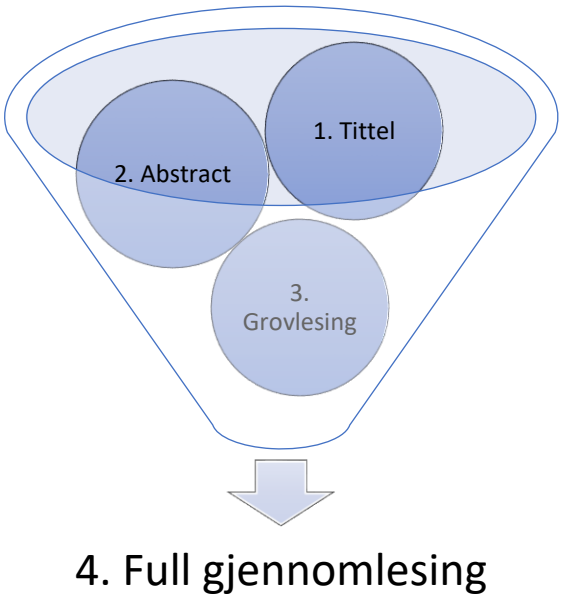
Tabell 1 viser de ulike søkeordene og kombinasjonene som ble benyttet. Enkelte søk viser svært mange treff, noe som ikke har vært mulig å gjennomgå fullstendig på grunn av den begrensede tiden med denne oppgaven. Det ble derfor gjennomført en seleksjonsprosess for å sile ut de mest relevante artiklene. Dette er gjennomgått i kap. 2.2.3.

Tabell 1: Søkeord og treff

Søkeord	Oria	Google Scholar	Scopus
«BIM» AND «security»	9332	51800	274
«BIM security»	9332	52400	1
«ISO 19650 part 5»	0	1700	1
«ISO 19650-5»	4	104	1
«ISO 19650» AND «part 5»	5	59	0

2.2.3 Seleksjonsprosess

Tabell 1 viser at enkelte søkeord har gitt svært mange treff. Det har ikke vært hensiktsmessig å gå gjennom alt dette, derfor var det nødvendig å gjøre et utvalg. Utvelgelsesprosessen tok utgangspunkt i tittel, sammendrag, grovlesing og full gjennomlesing. Prosessen er illustrert i figur 3:



Figur 3: Illustrasjon av seleksjonsprosessen

Steg 1 – Tittel

Steg 1 gikk ut på å lese gjennom titlene til om lag 100 artikler. De titlene som i størst grad ble ansett som relevante og interessante for oppgaven ble satt til side for lesing av sammendraget. Selv om enkelte søkeord har gitt tilsynelatende mange treff, har det imidlertid vist seg at svært få har vært av direkte relevans for oppgaven. Denne grovutvelgelsen har vært mest effektiv for søkeord med svært mange treff.

Steg 2 – Sammendrag

Neste steg i seleksjonsprosessen handlet i større grad om å få en helhetlig oversikt over oppgaven ved å gå igjennom oppgavens abstract (sammendrag). Her ble det raskt avdekket hvorvidt oppgaven nevnte nøkkelbegreper som «Security», «ISO 19650-5» og tilsvarende i en aktuell kontekst, eller som en bisetning. Overraskende mange omhandlet ikke søkeordene i den konteksten som var interessant for denne oppgaven. Kun de som gjorde dette ble med videre for en grov gjennomlesing.

Steg 3 – Grovlesing

Grovlesningen i seleksjonsprosessen skulle skape et bedre bilde av de mest interessante artiklene. Dette ble gjort ved å identifisere artikkelens metodikk, resultat og konklusjon i en mer detaljert grad enn ved sammendraget.

Steg 4 – Full gjennomlesing

Steg 4 i seleksjonsprosessen er det siste steget i utvelgelsen av litteraturstudiets forskningsartikler. Dette steget handlet om å lese gjennom de gjenværende 8 artiklene fra steg 3. De 8 artiklenes viktigste elementer er fremstilt i tabell 5 i kapittel 3.4.

2.2.4 Vurdering av litteraturens kvalitet

Etter utvelgelsen av artiklene var gjennomført, ble de aktuelle gjenværende artiklene vurdert etter T-O-N-E prinsippet slik (NTNU-Universitetsbibliotek, 2017) beskriver. Dette var for å sikre artiklenes troverdighet, objektivitet, nøyaktighet og egnethet. Tabell 2 gir et bilde over hvordan artiklene er vurdert.

Tabell 2: Vurdering etter TONE-prinsippet

Vurderings-kriterier	**Spørsmål forfatteren bør stille seg Hentet fra: (NTNU-Universitetsbibliotek, 2017)**	**Beskrivelse av vurdering**
Troverdighet	Hvem er ansvarlig for artikkelen? Hva er forfatterens utdanning og institusjonstilknytning? Er artikkelen publisert i et fagfellevurdert tidsskrift?	Artiklene er publisert i databasene Scopus, Google scholar og Oria. De 3 mest brukte artiklene dukket opp i både scopus og google scholar. Dette bidrar til å øke troverdigheten til artiklene. Samtlige artikler er publisert via store universiteter fra ulike deler av verden. Majoriteten av artiklene er publisert etter 2019.
Objektivitet	Hvordan er dataene i artikkelen presentert? Er dataene i samsvar med tidligere forskning, eller ikke? Er forfatterens hensikt å overtale eller å informere leseren? Er flere sider av saken belyst?	Ettersom tematikken er såpass ny, bærer samtlige artikler preg av å være informative eller har foreslått et «proof of concept». Dette har ført til diskusjoner rundt behov, mangler, muligheter og risikoer.
Nøyaktighet	Er den brukte forskningsmetoden godt forklart? Hvor oppdaterte er dataene? Kan informasjonen bekreftes av minst to andre kilder?	8 artikler har en grundig metodikk i forskningen. Selv om det finnes svært få artikler på tematikken, har flere av artiklene gjort samsvarende observasjoner, som peker i retning av behovet denne studien undersøker.
Egnethet	Er dataene relevante for egen studie? Vil de kaste nytt lys over problemstillingen? Hvem er artikkelen skrevet for?	Kun 2 artikler er direkte relevante for egen studie. Likevel er de 8 utvalgte artiklene indirekte relevante på flere måter, ved at de beskriver behovet og gir informasjon om andre deler av tematikken.

2.2.5 Styrker og svakheter

Selv om søkene og funnene som ble gjort i dette litteraturstudiet tyder på at det finnes lite forskning på området, kan det likevel finnes forskningsartikler som er unntatt offentligheten. Ettersom BIM-security er et tema som kan omhandle anlegg med sensitiv informasjon, er det sannsynlig at disse ikke vil ligge offentlig tilgjengelig. Samtidig kan det være forskningsartikler som ikke er avdekket blant de store søketreffene fra Google scholar som kunne inneholde interessant informasjon. Det vil derfor være en svakhet med disse søkeresultatene og litteraturen som er innhentet.

Det er imidlertid gjort søk i tre ulike søkedatabaser og funnet flere av de utvalgte forskningsartiklene i alle tre databasene. Dette kan ansees som en styrke i litteraturutvelgelsen. Samtidig kan en også stille seg kritisk til søkeordene som er benyttet. Dersom flere søkeord hadde blitt benyttet, er det mulig at flere relevante treff hadde vært funnet. Dersom oppgaven skulle vært foretatt på ny, ville også en litteraturstudie på HMS være aktuelt å utforske. På en annen side kan en i lys av oppgavens tidsramme vurdere hvorvidt dette ville bli for omfattende.

Litteraturstudien har som tidligere beskrevet bidratt til valget av oppgavens fokus – Digital sikkerhetskultur. Selv om få artikler omhandler sikkerhetskulturen spesifikt, kan det likevel ansees som en styrke at artiklene omfavner det teknologiske perspektivet ved temaet BIM-sikkerhet. På den måten bidrar litteraturen til å danne et bedre bilde over tematikken og samtidig fremheve behovet for mennesket og prosess vinklingen. Vurderingen av litteraturens kvalitet med hjelp av TONE-prinsippet bidrar også til å styrke utvelgelsen av litteraturen.

2.3 Intervjuer

For å kunne besvare forskningsspørsmål 1: *«Hvordan er den digitale sikkerhetskulturen blant aktører i byggenæringen i dag?»*, er det ansett som hensiktsmessig å foreta intervjuer av aktører i næringen. Dette vil gi et bilde av holdninger og oppfatninger av digital sikkerhetskultur under norske forhold. I tillegg er det interessant å høre hva aktørers syn på HMS-kulturen er til sammenligning.

2.3.1 Intervjumetodikk

(Steinar Kvale, 2021) beskriver en metode for gjennomføring av kvalitative forskningsintervju. Denne benyttes i gjennomføringen av studiens intervjuer. ((Steinar Kvale, 2021), s. 137) deler forskningsintervjuet inn i syv faser. Disse illustreres i figur 4.

Figur 4: Intervjuprosessens syv faser

2.3.2 Planlegging av intervju

Intervjuobjekter

Intervjuenes hensikt er å bidra til å besvare FS1 og FS2. Det er laget to ulike intervjuguider, som har to ulike formål. Planleggingsprosessen har vært lik, men innholdet og spørsmålene har vært ulike.

Hensikten med FS1 er å kartlegge dagens situasjon rundt holdninger og fokus til sikkerhet i byggenæringen. For å kartlegge dette på en god måte ble det valgt å intervjue et bredt spekter av bransjen. Dette skulle danne et større helhetsbilde enn ved intervju av personer i samme type rolle. Det ble derfor intervjuet representanter fra både byggherrerollen, rådgiverrollen, arkitektrollen, entreprenørrollen og produsentrollen.

For å besvare FS2 er det også nødvendig å snakke med folk i bransjen om deres inntrykk av kulturen, hva de synes fungerer og ikke, samt hva de selv tror er årsaken til at HMS fokuset har endret seg de siste tiårene. På samme vis som FS1 er det valgt å intervjue et tilsvarende bredt spekter av bransjen. Alle de 7 intervjuobjektene har fått spørsmål som kan knyttes til både FS1 og FS2. 4 av 7 intervjuer har hatt hovedfokus på digital sikkerhet, mens 3 av 7 intervjuer har hatt hovedfokus på HMS.

Det er bevisst valgt å ikke knytte intervjuene til spesifikke prosjekter, for å unngå prosjekter med særegne og spesielle sikkerhetskrav. Baktanken med å gjennomføre intervjuer med så forskjellige deler av byggenæringen er å danne et grovt bilde av hvordan dagens sikkerhetskultur generelt er i bransjen, og høre ulike perspektiv. De utvalgte intervjuobjektene ble funnet ved hjelp av offentlige nettsider og via kontaktpersoner. ((Steinar Kvale, 2021), s. 148) beskriver hvordan antallet intervjupersoner avhenger av formålet med undersøkelsen. Hvis formålet er å forstå verden slik den oppleves av en bestemt person, er det nok med den ene personen. Hvis intensjonen er å undersøke å gi en grundig beskrivelse av en gruppe kan man gjennomføre intervjuer inntil meningspunket nås, hvor flere intervjuer ikke tilfører noen ny informasjon. I intervjuene var formålet å undersøke «byggebransjens» holdninger. Byggebransjen er imidlertid stor og har mange ulike perspektiver og vinklinger, derfor ville en grundig kartlegging av kun dette blitt veldig omfattende. Intervjuobjektenes synspunkter vil samtidig gi en indikasjon på deres personlige meninger. Derfor kan en til en viss grad oppleve 7 ulike syn på verden likevel.

De 7 intervjuobjektenes rolle i byggenæringen og deres stillingstitler er presentert i tabell 3. Av hensyn til intervjuobjektenes anonymitet, er det valgt å ikke oppgi navn på intervjuobjektene. Stillingstittel er likevel tatt med da dette kan være interessant i forhold til resultatene.

Tabell 3: Intervjuobjektenes rolle i byggenæringen

Rolle i byggenæringen	Stillingstittel
Byggherre 1	BIM-koordinator
Byggherre 2	Prosjektleder
Rådgiver	Fagspesialist
Arkitekt	BIM-koordinator
Produsent	Konstruktør
Entreprenør 1	VDC-manager
Entreprenør 2	Prosjektleder

Intervjuguide

I forkant av intervjuene ble det utarbeidet to intervjuguider. Én med hovedfokus på å besvare FS1, og én med hovedfokus på å besvare FS2. For å danne et sammenligningsgrunnlag mellom de to ulike sidene av sikkerhet (digital sikkerhet og HMS) er det fulgt samme oppbygning i begge intervjuguidene;

- Hvordan oppleves dagens (digitale sikkerhetskultur)/(HMS kultur)
- Hvilke erfaringer har aktører med (digital sikkerhet)/(HMS)
- Hva mener aktører at kan bedres i fremtiden? (digital sikkerhet)/(HMS)

Det er også stilt mer individuelle spørsmål under hver inndeling, se vedlegg 1 og 2. Intervjuguidene har styrt tematikken i samtalene, men avhengig av intervjuobjektenes interesse, fokusområde og kunnskap har det blitt stilt oppfølgingsspørsmål som har ledet samtalene i ulike retninger.

2.3.3 Gjennomføring av intervju

Intervjuet

Etter intervjuforberedelsene ble selve intervjuene gjennomført i perioden 1. mars 2022 til 12. april 2022. Intervjuene ble gjennomført med intervjuguiden som utgangspunkt. Det ble valgt å gjøre semi-strukturerte intervjuer, noe som ledet til at alle intervjuobjektene fikk ulike oppfølgingsspørsmål basert på svarene deres. Dette førte i flere tilfeller til et bedre bilde av deres perspektiv på tematikken, men kan også ha ledet samtalen vekk fra annen interessant informasjon. Med intervjuobjektenes samtykke ble det gjort opptak av intervjuene for å gjøre transkriberingen lettere. Den planlagte lengden på intervjuene var satt til 40 minutter, men i praksis varte intervjuene i gjennomsnitt 50 minutter, hvor det korteste intervjuet varte omlag 35 minutter og det lengste varte omlag 65 minutter.

Transkribering

Transkriberingsprosessen ble gjennomført umiddelbart etter hvert intervju. Hensikten med dette var å utnytte hukommelsen i størst mulig grad. Ut ifra opptakene ble intervjuene skrevet ned i sin helhet og senere analysert ved hjelp av analyseverktøyet Nvivo (Se kapittel 2.4).

2.3.4 Styrker og svakheter

En styrke med å velge intervju som forskningsmetode er at representantene fra bransjen i større grad får uttrykt sine meninger, opplevelser og erfaringer om tematikken. Det gjør det mulig å stille oppfølgingsspørsmål som kan lede til andre viktige funn.

Ved å intervjue aktører fra ulike deler av bransjen vil det dannes et mer generelt bilde av holdninger og fokus i dag. Dette anses som en styrke i forhold til å besvare oppgavens problemstilling, til sammenligning med å intervjue aktører med samme perspektiv. Dette ville på en annen side gi et bedre bilde av det aktuelle perspektivet. Aktørene som er intervjuet er store og representerer viktige deler av norsk byggenæring. Samtlige intervjuobjekter fortalte at de har erfaring med graderte prosjekter, noe som på en side kan styrke deres oppfatning av dagens bransje, men samtidig påvirkes av intervjuobjektets opplevelse av erfaringen. Intervjuguidenes likheter i oppbygning og struktur gjør det enklere å sammenligne HMS med den digitale sikkerhetskulturen, noe som kan styrke sammenligningen.

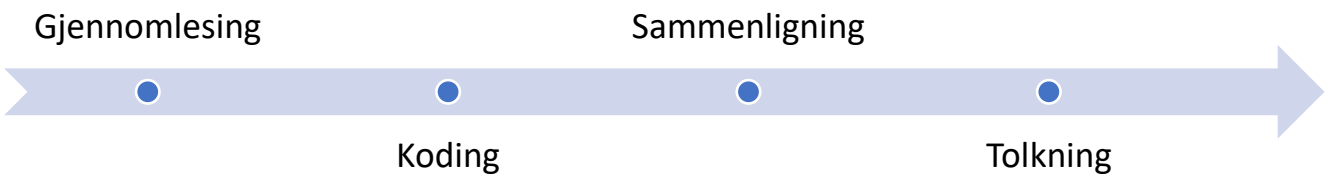
Ifølge (Grønmo, 2020) innebærer bias i forskning at resultater eller slutninger i en studie er skjeve eller feilaktige. Dette kan oppstå som følge av en begrenset forståelse og utnytting av tidligere relevant forskning, snevert valg av kilder, datatyper eller kontekster for studien, samt ledende spørsmål til respondenter. Med oppgavens tematikk, manglende kunnskap hos både intervjuobjekter og i forskningen generelt vil faren for bias være tilstede. Det er imidlertid tilstrebet å stille objektive spørsmål uten å ta parti i intervjuprosessen. Likevel kan dette være en aktuell svakhet.

En kan stille seg kritisk til å trekke slutninger basert på intervjuresultatene i denne studien. En svakhet med at intervjuene brukes som en del av grunnlaget for å omtale dagens sikkerhetskultur i byggenæringen på generelt grunnlag er at det kun er gjort 7 intervjuer. Dette er i seg selv kan virke for lite til å kunne gi et presist bilde, og vil i større grad fungere som en «stikkprøve» av dagens situasjon. I tillegg ble lærdom høstet ettersom intervjuerfaringen økte, noe som kan utgjøre en svakhet i utførelsen av de første intervjuene til sammenligning med de siste. Spesielt oppfølgingsspørsmålene kan ha båret preg av liten intervjuerfaring i de første intervjuene. Det vil også være en fare for misforståelser i forbindelse med formuleringen av intervjuspørsmålene, noe som kan ha ledet samtalene deretter. Samtidig har de samme hovedspørsmålene blitt stilt til alle aktørene, noe som likevel kan gjøre svarene sammenlignbare.

2.4 Analyse og tolkning av funn

Både ((Asbjørn Johannessen, 2021), s. 152) og ((Steinar Kvale, 2021), s. 219) beskriver analysering som å dele noe opp i biter eller elementer. Etter at store mengder informasjon og datamateriale er samlet inn, kan det være utfordrende å hente ut essensen av innholdet og fremstille det på en god måte. Ved å dele datamengden inn i mindre deler, blir denne jobben betraktelig enklere. I de neste delkapitlene blir fremgangsmetoden benyttet i denne studien beskrevet.

2.4.1 Fremgangsmåte



Figur 5: Analyseprosessen

Gjennomlesning

Før selve analysearbeidet startet ble alt datamaterialet lest gjennom for å ha innholdet friskt i minnet. Datamaterialet har i tillegg vært lest gjentatte ganger i løpet av prosessen. Undertegnede erfarte hvordan mer og mer informasjon sank inn ved gjentatte gjennomlesninger. Dette anses derfor som en viktig del av analysemetoden.

Koding (Tverrsnittbasert og kategorisk inndeling av data)

((Asbjørn Johannessen, 2021), s. 153) beskriver hvordan kvalitative data kan organiseres og deles inn gjennom *tverrsnittbasert og kategorisk inndeling av data*. Når data er samlet inn, består analysen i å finne en meningsfull inndeling på tvers av materialet. Ifølge ((Asbjørn Johannessen, 2021), s. 154) betyr tverrsnittbasert inndeling å konstruere et system for å indeksere datamengden, dvs. at det settes merkelapper på setninger eller avsnitt som gjør det mulig å identifisere og finne igjen spesielle temaer i datamaterialet.

Denne fremgangsmetoden ble ansett som hensiktsmessig for å strukturere og kategorisere datamaterialet i denne studien. Dataverktøyet «NVivo» (Alfasoft, 2022) ble anvendt som hjelpemiddel i denne prosessen. Dette har bidratt til å få frem datamengdens essensielle faktorer sett i lys av problemstillingen.

Sammenligning

Diagrammer og tabeller kan ifølge ((Asbjørn Johannessen, 2021), s. 159) brukes for å sortere, organisere eller fungere som hjelpemiddel ved tverrsnittbasert og kategorisk inndeling av data. Når datamaterialet var kodet gjennom NVivo, ble resultatene fremstilt i tabeller slik ((Asbjørn Johannessen, 2021), s. 160) beskriver for å synliggjøre sammenhenger som ellers ville være vanskelig å få frem ved hjelp av tekst (se kapittel 4). Dette ble gjort for å gi en oversikt over funn, meninger, likheter og forskjeller mellom ulike aktører, men også mellom ISO 19650-5 og HMS aktiviteter.

Tolkning

Å tolke betyr ifølge ((Asbjørn Johannessen, 2021), s. 152) å sette noe inn i en større ramme eller sammenheng. Dette kan gjøres ved å se på hvilke konsekvenser analyse og konklusjon har for studiens tematikk. For den digitale sikkerhetskulturen i byggebransjen har det også vært viktig å fremheve usikkerheten rundt teknologien og verdensbildet. Videre vil det være viktig å se datamaterialet fra ulike sider og perspektiver for å belyse ulike situasjoner og utfordringer. Tolkningens hensikt handler også om å komme med anbefalinger til tiltak og videre forskning.

2.5 Rapportering

Det syvende steget av intervjuundersøkelsen handler ifølge ((Steinar Kvale, 2021), s. 137) om å formidle funn og fortolkninger i en form som overholder vitenskapelige kriterier og resulterer i et lesbart produkt. I denne oppgaven har rapporteringen fulgt (NTNU, 2022) sine krav til rapportering av masteroppgaver, som på mange måter er tilsvarende det ((Steinar Kvale, 2021), s. 305) foreslår. Denne oppgaven består derfor av følgende steg:

1. Introduksjon
2. Metode
3. Faglig og teoretisk grunnlag (teori)
4. Resultat
5. Diskusjon
6. Oppsummering og anbefalinger (konklusjon)
7. Referanser

I tillegg til disse stegene er det forside, sammendrag og innholdsfortegnelse i forkant av introduksjonen, samt vedlegg i etterkant av referanselisten. Kildehenvisningen er gjort i henhold til (NTNU, 2022) sin foretrukne Harvard stil. Resultatene er presentert med utgangspunkt i tabeller da dette raskt vil gi leseren oversikt over hovedinnholdet, etterfulgt av mer utfyllende og beskrivende tekst.

2.6 Etikk

Studien er gjort uten tilknytning til en bedrift/arbeidsgiver, og har dermed ingen økonomisk støtte eller fordeler som kan påvirke resultatet eller diskusjonen. Gjennom intervjuprosessen har samtlige intervjuobjekter gitt samtykke til å delta og til å bli gjort opptak av for å gjøre transkriberingsprosessen lettere og mer korrekt. Det er bevisst valgt å ikke oppgi navn på hverken personene eller organisasjonene som har deltatt for å bevare informantenes anonymitet.

Gjennom studiens arbeid er det forsøkt å være så nøytral som mulig, uten å ta parti med noen av perspektivene som trekkes frem. Det er samtidig gjort en rekke fortolkninger i oppgaven. Dette kan medføre feil som følge av undertegnedes oppfattelser og tolkninger av informasjonen. På en annen side kan det også være feil å ikke fortolke eller bruke egen innsikt til å forstå resultatet. Kvalitative studier gir i utgangspunktet rom for tolkning og ulike perspektiver. Det er likevel forsøkt å være så konkret som mulig for å støtte utviklingen i næringen.

2.7 Evaluering

((Asbjørn Johannessen, 2021), s. 255) beskriver evalueringsprosessen til kvalitative undersøkelser til å omfatte fire hovedpunkter:

1. Pålitelighet (reliabilitet)
2. Troverdighet (intern validitet)
3. Overførbarhet (ekstern validitet)
4. Bekreftbarhet (objektivitet)

2.7.1 Pålitelighet

Ifølge ((Asbjørn Johannessen, 2021), s. 256) er reliabiliteten knyttet til forskningens data. I kvantitative undersøkelser er dette kritisk, og det finnes en rekke metoder for å etterprøve slike resultater. I kvalitativ forskning er ofte datamaterialet basert på tolkbare synspunkter og meninger gjennom blant annet intervjuer. Dette vil ifølge ((Asbjørn Johannessen, 2021), s. 256) være svært kontekstavhengig og kan ikke etterprøves på samme måte av en annen forsker. Tolkningen i seg selv er også unik for den aktuelle forskers resultater. Ettersom alle har ulik bakgrunn og erfaring, vil følgelig svar oppfattes og tolkes forskjellig.

I denne oppgaven er det tilstrebet å gi en god beskrivelse av fremgangsmåten, metodikken og tankene underveis. Ved å begrunne hvorfor og hvordan ulike valg er tatt mener ((Asbjørn Johannessen, 2021), s. 256) dette bidrar til å styrke påliteligheten i kvalitative undersøkelser. Likevel er alle funn og tolkninger i denne rapporten gjort av én forfatter, noe som ikke gir samme rom for diskusjon underveis og ulike perspektiver av resultatene kan mistes eller misforstås. Dette vil på denne måten bidra til å svekke studiens pålitelighet.

2.7.2 Troverdighet

((Asbjørn Johannessen, 2021), s. 256) mener validitet i kvalitative undersøkelser dreier seg om i hvilken grad forskerens fremgangsmåter og funn på en riktig måte reflekterer formålet med studien og representerer virkeligheten. Det vises til to teknikker som frembringer troverdige resultater: vedvarende observasjon og triangulering.

«Metodetriangulering» handler ifølge ((Asbjørn Johannessen, 2021), s. 256) om å gjennomføre flere ulike metoder for å undersøke et fenomen. I denne studien har det blitt gjennomført både litteraturstudie og intervjuer. Studiens validitet kunne vært styrket ytterligere ved å inkludere flere fremgangsmetoder slik som casestudier, spørreundersøkelser, etc. På en annen side ville en casestudie skapt mer kontekstbaserte svar, og spørreundersøkelser ville ikke tillate og gå i dybden på samme måte. Dette ville også krevd mer tid, noe som villr ført til at oppgavens tidsramme måtte utvides.

Den andre teknikken ((Asbjørn Johannessen, 2021), s. 256) mener frembringer troverdige resultater er «vedvarende observasjoner» som handler om å investere nok tid til å bli godt kjent med feltet, og på den måten lettere kunne skille mellom relevant og ikke-relevant informasjon. Mye kunnskap har blitt tilegnet over en tidsperiode på et år, både gjennom studering, men også gjennom observasjoner av menneskers holdninger i byggebransjen og i dialog med flere ulike mennesker innen relevante deler av sikkerhetssektoren. Høsten 2021 tok forfatter to relevante tilleggsfag (TIØ 4201 - Risikohåndtering, samfunnssikkerhet og kritisk infrastruktur, og IIKG 3000 – Introduksjon til informasjonssikkerhet og personvern) for å gi et bedre kunnskapsmessig utgangspunkt. Dette anses å ha styrket troverdigheten til studiens fortolkninger.

2.7.3 Overførbarhet

Ved kvalitative undersøkelser ønsker man gjerne å avdekke kunnskap som kan overføres til flere tilfeller. ((Asbjørn Johannessen, 2021), s. 257) eksemplifiserer overførbarhet med: «Kan resultater fra en casestudie av reinsdyr på Finnmarksvidda overføres til sauehold i Gudbrandsdalen?».

En studies overførbarhet styrkes ifølge ((Asbjørn Johannessen, 2021), s. 258) gjennom fyldige beskrivelser av detaljer som inngår i en kultur eller et fenomen. Gjennom denne studien har noe av formålet vært å se sammenhenger og overførbarhet mellom sikkerhetskulturen innen teknologi og HMS. I lys av dette vil studien ha en god og svært relevant overførbarhet. På en annen side kan også prinsippene være overførbare til andre bransjer.

2.7.4 Bekreftbarhet

Med bekreftbarhet menes det ifølge ((Asbjørn Johannessen, 2021), s. 258) at forskningen skal være nøytral og upartisk. Det finnes også her en rekke strategier som styrker bekreftbarheten i en studie. Det pekes først på hvordan forskeren må vektlegge beskrivelser av forskningsprosessen og beslutninger som er tatt underveis. Slik kapittel 2.7.1 beskriver er det tilstrebet å gi en god beskrivelse av metodikken og beslutninger underveis i prosessen. ((Asbjørn Johannessen, 2021), s. 259) beskriver videre hvordan forskeren må være selvkritisk til hvordan prosjektet er gjennomført, og kommentere hvordan blant annet fortolkninger, fordommer og oppfatninger kan påvirke resultatet. Bekreftbarheten kan også styrkes dersom fortolkningene støttes av annen litteratur, eventuelt av informantene i undersøkelsen. I denne studien har blant annet litteraturstudiet, forprosjektet (Listøl, 2021a), samt risikovurderingen til (NSM, 2021) vært viktige faktorer som førte til at tematikken ble valgt i utgangspunktet. Funnene i denne studien peker i stor grad samme retning som tidligere forskning, i tillegg til overførbarheten til HMS. Dette gjør at bekreftbarheten styrkes. Samtidig er det en svakhet at få forskningsartikler finnes på området, spesielt i Norge. Dette gjør at det er lite kunnskap å lene seg på, eller sammenligne mot.

3 Faglig og teoretisk grunnlag

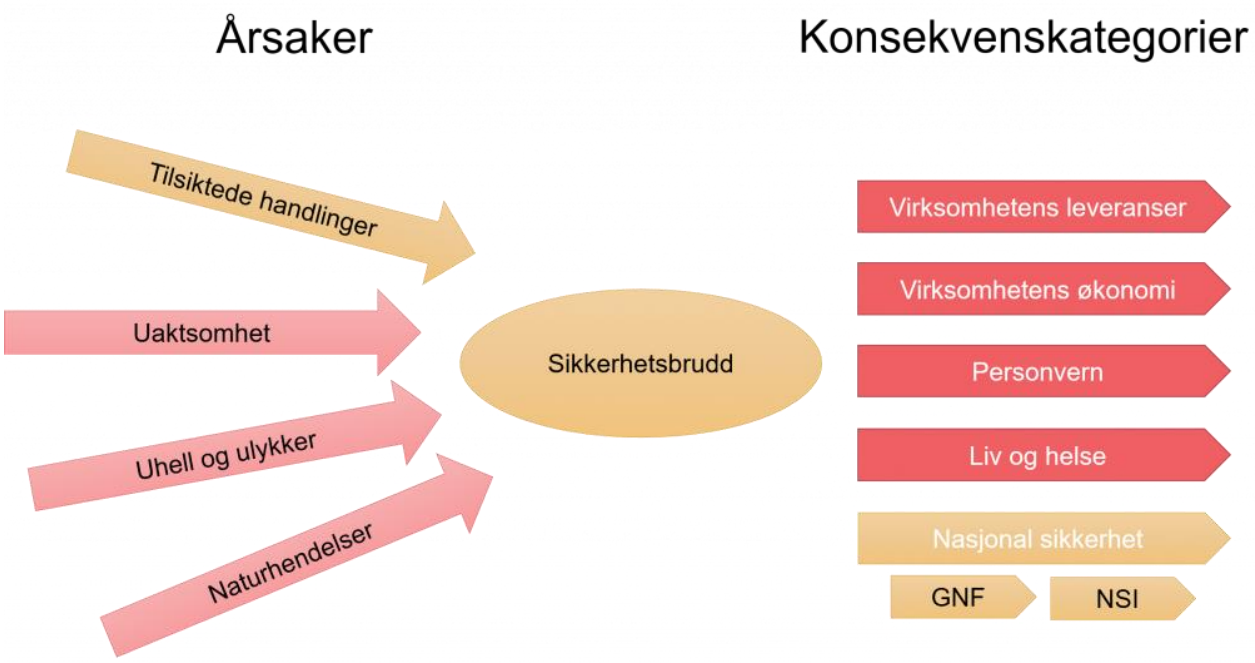
Dette kapittelet tar for seg sentrale begreper og definisjoner innen sikkerhet, samt et rammeverk for håndtering av sikkerhetsproblematikk (IRGC-modellen). Videre beskrives ISO 19650-serien, med hovedvekt på del 5. HMS prosessen introduseres i grove trekk med utgangspunkt i (Proactima, 2016). Til slutt presenteres en oversikt over tidligere forskning som er funnet gjennom litteraturstudiet høst 2021. Innholdet i kapittelet er strukturert som følger:

3.1 Sikkerhet

3.1.1 Sikkerhetsloven

Lov om nasjonal sikkerhet (sikkerhetsloven) har ifølge (Lovdata, 2019) som formål å trygge Norges suverenitet, territorielle integritet og demokratiske styreform og andre sikkerhetsinteresser. I tillegg skal den forebygge, avdekke og motvirke sikkerhetstruende virksomhet og bidra til at sikkerhetstiltak gjennomføres i samsvar med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn. Kravene skal blant annet bidra til å beskytte skjermingsverdige verdier gjennom informasjonssikkerhet, informasjonssystemsikkerhet og objekt- og infrastruktursikkerhet. For mer informasjon om sikkerhetsloven henvises det til (NSM, 2022b).

(Digitaliseringsdirektoratet, 2022) beskriver hvordan sikkerhetsbrudd kan oppstå som følge av ulike årsaker som direkte eller indirekte kan få konsekvenser for grunnleggende nasjonale verdier. Dette er illustrert i figur 6.



Figur 6: Konseptuell forståelse av årsaker og konsekvenser (Digitaliseringsdirektoratet, 2022). GNF=Grunnleggende nasjonale funksjoner, NSI=Nasjonale sikkerhetsinteresser

Skjermingsverdig informasjon

Skjermingsverdig informasjon defineres som følger:

> *«Informasjon er skjermingsverdig dersom det kan skade nasjonale sikkerhetsinteresser at informasjonen blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig.» ((Lovdata, 2019), §5-1)*

Skjermingsverdig informasjonssystem

Skjermingsverdig informasjonssystem defineres som følger:

> *«Et informasjonssystem er skjermingsverdig dersom det behandler skjermingsverdig informasjon, eller dersom det i seg selv har avgjørende betydning for grunnleggende nasjonale funksjoner.» ((Lovdata, 2019), §6-1)*

Skjermingsverdig objekt og infrastruktur

Skjermingsverdige objekter og infrastrukturer defineres som følger:

> *«Objekter og infrastruktur er skjermingsverdige dersom det kan skade grunnleggende nasjonale funksjoner om de får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse.» ((Lovdata, 2019), §7-1)*

3.1.2 Begreper og definisjoner

Boken *«Perspektiver på samfunnssikkerhet»* (al, 2021) er en sentral kilde i denne oppgaven. Mye av det teoretiske grunnlaget som brukes vil, i tillegg til forskningsartikler, være forankret i denne boken. Et utvalg av sentrale begreper og definisjoner blir beskrevet i dette delkapittelet, ellers henvises det videre til (al, 2021).

Safety og security

I Norge brukes kun ordet «sikkerhet» om alle typer sikkerhetsbetydninger og kun sammenhengen kan skille betydningene. På engelsk deles sikkerhetsbegrepet inn i «safety» og «security». Ifølge ((al, 2021), s. 27) er det i Skandinavia vanlig å tenke at «safety» handler om ulykker, og «security» om sikkerhet mot ondsinnede handlinger slik som krig og terrorisme. Videre beskrives det hvordan «safety» igjen kan ha flere betydninger på norsk. Det skilles mellom sikkerhet (safety) som tilstand, og sikkerhet (safety) som følelse. «Sikkerhet som tilstand sikter til det å være i sikkerhet rent faktisk, mens sikkerhet som følelse sikter til det å føle seg sikker eller trygg» ((al, 2021), s. 27)

ISO 19650-5 definerer imidlertid «safety» og «security» som følger:

Safety: *«State of relative freedom from threat or harm caused by random, unintentional acts or events». ((Standard-Norge, 2020), kap. 3.6)*

Security: *«State of relative freedom from threat or harm caused by deliberate, unwanted, hostile or malicious acts». ((Standard-Norge, 2020), kap. 3.7)*

Risiko

Ifølge ((al, 2021), s. 96) refererer Terje Aven og Ortwin Renn risiko til usikkerheten om og alvorlighetsgraden av hendelser og konsekvenser (eller resultater) av en aktivitet med hensyn til det mennesket verdsetter. En kan tallfeste en slik risiko ved å regne sannsynlighet mot konsekvens. Dette påstås å være et effektivt verktøy, selv om det alltid vil være en usikkerhet med risikoen man regner seg fram til.

Risikopersepsjon

Risikopersepsjon defineres i ((al, 2021), s. 96) som enkeltindividets oppfatning av risiko. Dette kan påvirkes av enkeltpersoners kognitive egenskaper, personlige erfaringer, individuelle verdier og personlig virkelighetsoppfatning.

Sett fra det psykologiske perspektivet beskriver ((al, 2021), s. 108) følgende:

> *«Risikopersepsjon er både et spørsmål om hvordan vi fysisk oppfatter vår verden, men også hvordan vi selekterer, vurderer og utveksler informasjon om usikkerhet knyttet til hendelser og konsekvenser.» ((al, 2021), s. 108)*

Restrisiko

Med restrisiko menes den gjenværende risikoen etter at risikoreduserende tiltak er implementert. ISO 19650-5 (Standard-Norge, 2020) definerer det som følger:

«Risk that remains after controls have been implemented» ((Standard-Norge, 2020), kap. 3.12)

Kritisk infrastruktur

Kritisk infrastruktur defineres av (beredskapsdepartementet, 2021) som følger:

> *«Kritisk infrastruktur er de anlegg, og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner som igjen dekker samfunnets grunnleggende behov og befolkningens trygghetsfølelse.» ((beredskapsdepartementet, 2021), del 1, kap. 3)*

Sensitiv informasjon

ISO 19650-5 ((Standard-Norge, 2020), kap. 3.11) definerer sensitiv informasjon som informasjon der tap, misbruk, endring eller uautorisert tilgang kan:

- Påvirke personvernet, sikkerheten (både «safety» og «security») for en eller flere personer på en uheldig måte;
- Kompromittere en organisasjons intellektuelle eiendom eller handelshemmeligheter;
- Forårsake kommersiell eller økonomisk skade på en organisasjon eller et land, og/eller;
- Sette nasjonens sikkerhet, innenriks- og utenrikssaker på spill.

Phishing

(Datatilsynet, 2020) beskriver phishing som en form for sosial manipulering hvor en angriper forsøker å lure noen til å utføre en handling, for eksempel ved å åpne et e-postvedlegg, klikke på en lenke eller betale en falsk regning. Via vedlegg kan det installeres skadevare slik som løspengevirus som kan spres til andre datamaskiner i samme nettverk, eller det kan drives spionasje. Via lenker kan også angriperen be om passord til systemløsninger og benytte disse til å stjele informasjon som er konfidensielle.

Phishing kan komme fra både kjente og ukjente avsendere. Jo mer troverdig avsenderen er, jo lettere er det å bli lurt. Phishing kan ifølge (Datatilsynet, 2020) forekomme gjennom ulike kommunikasjonsformer, men e-post er det vanligste.

Collingridges dilemma

((al, 2021), s. 254) omtaler «collingridges dilemma» som sentralt innen digitalisering og sikkerhetstenkning.

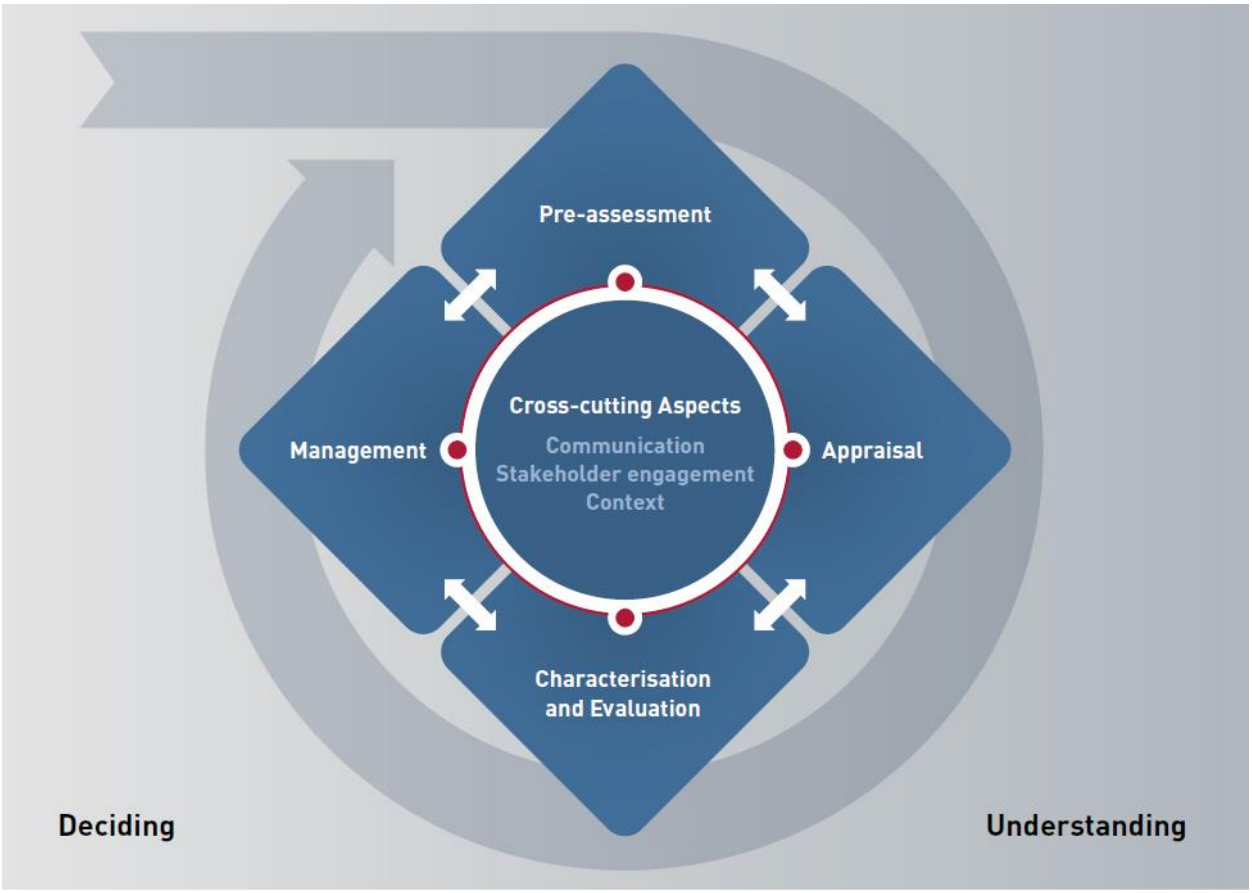
> *«Dilemmaet viser til hvordan den teknologiske utviklingen vanskelig kan styres i en tidlig fase, fordi omfanget av konsekvensene ikke kommer klart frem før i en senere fase når kunnskapen og teknologien er tatt i bruk. Da er det gjerne for sent å prøve å styre eller reversere utviklingen og trekke tilbake teknologien» ((al, 2021), s. 254)*

3.1.3 IRGC – modellen

I faget TIØ 4201 jobbet undertegnede med en semesteroppgave om risikohåndtering, hvor en del av det teoretiske grunnlaget (IRGC-modellen) også anses som relevant for denne studien. Derfor er denne delen hentet fra tidligere arbeid (Listøl, 2021b).

IRGC – modellen utviklet av «International Risk Governance Council» (IRGC, 2021) er et relevant rammeverk for håndtering av sikkerhetsaspekter i et samfunnsperspektiv. Boken «perspektiver på samfunnssikkerhet» ((al, 2021), s. 387) beskriver hvordan modellen kombinerer tekniske risikoanalyser med ulike politiskinstitusjonelle beslutningsprosesser og foreskriver en aktiv strategi for å avdekke, analysere og evaluere risiko. Deretter skal det bestemmes om risikoen oppfattes som akseptabel, tolererbar eller ikke-tolererbar. Poenget er at ulike fakta, meninger og synspunkter på risiko skal veies opp mot hverandre gjennom diskusjoner mellom interessenter og enkeltaktører for å finne frem til en løsning.

Ifølge (IRGC, 2021) gir IRGC rammeverket veiledning for tidlig identifisering og håndtering av risiko, og involverer flere interessenter. IRGC anbefaler en inkluderende tilnærming til å etablere rammer, vurdere, evaluere, håndtere og kommunisere viktige risikospørsmål, som ofte er preget av kompleksitet, usikkerhet og tvetydighet. (IRGC, 2021) beskriver rammeverket som generisk og tilpasningsdyktig, noe som gjør at det kan skreddersys for ulike risikoer og organisasjoner. Rammeverket består av fire hovedfaser, og et tversgående aspekt. Figur 7 viser rammeverkets faser:



Figur 7: IRGC-modellen (IRGC, 2021)

Fase 1: Førvurderingsfase (pre-assessment)

Førvurderingsfasen skal identifisere og etablere rammer for risikoen. Rammene som etableres her kan påvirke hvordan risikoen blir håndtert til slutt. En risiko kan se veldig ulik ut avhengig av hvor stort man velger å se på den (se (IRGC, 2017)).

Fase 2: Risikovurderingsfase (Risk appraisal)

Fasen består av å gjøre en risikovurdering av de potensielle farene ved en sannsynlighet og konsekvensvurdering. Fasen deles videre opp i to hovedpunkter:

- Risikoevaluering
- Bekymringsevaluering

Detaljert informasjon om fasen finnes i ((IRGC, 2017), s. 14).

Fase 3: Risiko karakterisering og evaluering (Characterisation and evaluation)

Fasen handler om å karakterisere og evaluere den identifiserte risikoen. Det pekes på hvordan en risiko kan karakteriseres som enkle, komplekse, usikre, tvetydige eller en blanding. Dette påvirker utfallet til evalueringen og hvilken ledelsesstrategi som velges (se. ((IRGC, 2017), s. 17)).

Fase 4: Risikoledelse (Risk management)

Risikoledelsesfasen handler om å velge riktig ledelsesstrategi basert på funnene som er identifisert i de foregående fasene for å håndtere risikoen. Fasen deles gjerne inn i to hovedpunkter:

- Ta en beslutning om risikoledelsesstrategier
- Implementering, monitorering og evaluering

Detaljert informasjon om fasen finnes i ((IRGC, 2017), s. 23).

Fase 5: Tversgående aspekter (Cross-cutting aspects)

De tversgående aspektene som er viktige gjennom alle faser beskrives som

- Kommunikasjon
- Interessent engasjement for risikostyring
- Viktigheten av kontekst

For mer detaljert informasjon henvises det til ((IRGC, 2017), s. 27).

3.2 ISO 19650-serien

3.2.1 Standarder i ISO 19650-serien

ISO 19650-serien består av 6 deler, hvorav kun 4 er tilgjengelige via Standard Norge. Del 4 og 6 er fremdeles under utvikling.

Del 1: *Organisering og digitalisering av informasjon om byggverk, inkludert bygningsinformasjonsmodellering (BIM) — Informasjonsforvaltning med BIM — Del 1: Begreper og prinsipper (NS-EN ISO 19650-1:2018)*

Del 2*:* *Organisering og digitalisering av informasjon om byggverk, inkludert bygningsinformasjonsmodellering (BIM) — Informasjonsforvaltning med BIM — Del 2: Prosjektfasen (NS-EN ISO 19650-2:2018)*

Del 3: *Organisering og digitalisering av informasjon om byggverk, inkludert bygningsinformasjonsmodellering (BIM) — Informasjonsforvaltning med BIM — Del 3: Driftsfasen (NS-EN ISO 19650-3:2020)*

Del 4: *Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) — Information management using building information modelling — Part 4: Information exchange (ISO 19650-4: under development) (ISO, 2022b).*

Del 5: *Organisering og digitalisering av informasjon om byggverk, inkludert bygningsinformasjonsmodellering (BIM) — Informasjonsforvaltning med BIM — Del 5: Informasjonsforvaltning med fokus på sikkerhet (NS-EN ISO 19650-5:2020)*

Del 6: *Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) – Information management using building information modelling – Part 6: Health and Safety (ISO 19650-6: under development) (ISO, 2022a).*

3.2.2 NS-EN ISO 19650-5: 2020

Ifølge (Standard-Norge, 2021) spesifiserer NS-EN ISO 19650-5 prinsipper og krav for sikker forvaltning av sensitiv informasjon i et byggeprosjekt. Dette innebærer informasjon som innhentes, opprettes, behandles og lagres i et pågående prosjekt, produkt, ferdig byggverk, eller tjeneste.
Formålet med standarden er å være et rammeverk som skal hjelpe organisasjoner til å forstå de viktigste sårbarhetene, og hva som kreves for å håndtere risiko slik at et akseptabelt sikkerhetsnivå på forvaltning av informasjon blir oppnådd. Dette gjelder alle relevante parter i et byggeprosjekt og i alle faser av byggets levetid. Samtidig påpekes det at standarden ikke skal være til hinder for fordelene med BIM.

> *«Its purpose is not in any way to undermine collaboration or the benefits that BIM, other collaborative work methods and digital technologies can generate.» (Standard-Norge, 2021)*

Tiltakene i standarden kan også benyttes til beskyttelse mot tap, tyveri eller utlevering av verdifull kommersiell informasjon og personopplysninger.

ISO 19650-5 er del 5 i serien av standarder som omhandler informasjonsforvaltning med BIM. Dette er en sikkerhetsstandard som er laget med hensyn på byggenæringen og utfordringene her. Standarden skiller seg fra tradisjonelle konstruksjonsfokuserte standarder, ved at den ikke omhandler matematiske formler og naturlover, men tar for seg sikkerhetsaspektet av en teknologi som ikke er ferdigutviklet. Dette gjør at standarden kan virke lite konkretisert ved første øyekast. Da det er en internasjonal standard, er den utformet for å kunne tilpasses enhver nasjons lovgivning og systemer.

I introduksjonsbeskrivelsen av (Standard-Norge, 2020) omtales det hvordan informasjonssikkerhetskrav for en enkelt organisasjon, avdeling eller system er beskrevet i NS-ISO/IEC 27001, men at denne ikke kan anvendes på tvers av organisasjoner. BIM og andre teknologier innen digitalt samarbeid vil som regel føre til samarbeid og deling av informasjon på tvers av en lang rekke uavhengige organisasjoner innen sektoren for bebygde områder. Derfor oppmuntrer ISO 19650-5 (Standard-Norge, 2020) til innføring av en risikobasert metode med sikkerhetsfokus som både kan anvendes på tvers av organisasjoner, i tillegg til innad.

ISO 19650-5 består totalt av 9 kapitler hvor kap. 1-3 er introduksjon, definisjoner og begreper. Kapittel 4-9 formidler standardens viktigste steg. Disse stegene kan grovt sett deles inn i kategoriene:

1. Sensitivitetsvurdering
2. Sikkerhetsstrategi
3. Sikkerhetsstyringsplan
4. Plan for håndtering av uønskede hendelser/sikkerhetsbrudd
5. Arbeid med tredjeparter

3.3 Helse, miljø og sikkerhet (HMS)

I tillegg til lovverket, tar denne studien utgangspunkt i veilederen for HMS i byggeprosjekter som er publisert og kvalitetssikret av (Proactima, 2016).

Ifølge (Arbeidstilsynet, 2021a) omfatter begrepet HMS helse, miljø og sikkerhet i all arbeidssammenheng. Arbeidsgiver er pålagt å arbeide systematisk med HMS for å forebygge helseskade på arbeidstakere. Arbeidstakere er pliktige til å medvirke i HMS arbeidet. Det blir videre beskrevet at HMS også omfatter vern av ytre miljø og andre sikkerhetsaspekter enn arbeidstakernes sikkerhet, helse og velferd. (Proactima, 2016) beskriver at HMS er et begrep de aller fleste arbeidsgivere og arbeidstakere er kjent med.

Byggherreforskriften

Byggherreforskriftens formål er ifølge ((Lovdata, 2010), §1) å verne arbeidstakerne mot farer ved at det tas hensyn til sikkerhet, helse og arbeidsmiljø på bygge- eller anleggsplasser i forbindelse med planlegging, prosjektering og utførelse av bygge- eller anleggsarbeider. Forskriften stiller blant annet konkrete krav til plikter for byggherre, prosjekterende, arbeidsgivere og enkeltmannsforetak. I tillegg har arbeidstilsynet laget en informativ side med utgangspunkt i byggherreforskriften. For mer informasjon henvises det til (Arbeidstilsynet, 2022).

Sikkerhet, Helse og Arbeidsmiljø (SHA)

Begrepet «SHA» ble ifølge (Proactima, 2016) introdusert i den første utgaven av forskrift mot sikkerhet, helse og arbeidsmiljø på bygge- eller anleggsplassen som ble utgitt i 1995.

Byggherreforskriften beskriver hvordan byggherre skal ivareta arbeidstakernes sikkerhet, helse og arbeidsmiljø gjennom prosjektering og gjennomføring av bygge- og anleggsarbeider. I henhold til byggherreforskriften §7 (Arbeidstilsynet, 2021b) skal byggherren før oppstart av arbeidet på bygge- eller anleggsplassen sørge for at det utarbeides en skriftlig plan for sikkerhet, helse og arbeidsmiljø (SHA-plan).

Byggherreforskriften §8 (Lovdata, 2010) stiller krav til innholdet i planen for sikkerhet, helse og arbeidsmiljø (SHA-plan) til å være:

a) Et organisasjonskart som beskriver rollefordelingen og entrepriseformen
b) En fremdriftsplan som beskriver når og hvor de ulike arbeidsoperasjoner skal utføres, hvor det tas hensyn til koordinering av de forskjellige arbeidsoperasjonene.
c) En beskrivelse av de spesifikke tiltakene som er nødvendige for å redusere fare for liv og helse forbundet med; (se. (Arbeidstilsynet, 2021b)).
d) En rutine for behandling av endringer og oppdatering av planen.

Sikker Jobb Analyse (SJA)

Ifølge (UiB, 2021) er SJA en metode for å systematisk gjennomgå en arbeidsoppgave eller aktivitet. Dette gjøres ved å dele den aktuelle oppgaven inn i mindre deloppgaver, og gjennomgå deloppgavene for å vurdere risikoen knyttet til disse. På denne måten kan man også innføre tiltak for å redusere eller fjerne risikoen.

HMS-kultur

((Proactima, 2016), s. 21) beskriver ulike kjennetegn på en god HMS kultur. Det vesentligste kjennetegnet beskrives å være **velinformert**. Dette betyr at den er preget av gode rapporteringssystemer, hvor medlemmene kan lære av erfaringer. For å få til en god HMS-kultur er det også viktig å gi rom for kritiske refleksjoner og dialoger rundt arbeidet som gjøres. Dette vil bidra til at medlemmer føler de bidrar, noe som igjen kan øke fokuset.

3.4 Tidligere forskning

Resultatet av litteraturstudiet som ble gjennomført høsten 2021 (Listøl, 2021a) (se kapittel 2.2 for fremgangsmåte) illustreres i tabell 5. I tillegg gis en oversikt over artiklenes opprinnelse og publiserings år i tabell 4.

Tabell 4: Forskningsartiklenes publiserings år og land

	Tittel	Publisert	Land
1	BIM-enabled facilities management (FM): a scrutiny of risks resulting from cyber-attacks (Nikdokht Ghadimina, 2021)	2021	UK
2	Management procedure for sensitive projects in the context of a BIM adoption in a public organization (Giuseppe Miceli Junior, 2020)	2020	Brazil
3	Management of Collaborative BIM Data by Federating Distributed BIM Models (Thomas Beach, 2017)	2017	UK
4	BIM security: A critical review and recommendations using encryption strategy and blockchain (Moumita Das, 2020)	2021	Kina
5	Breaking into BIM: Performing static and dynamic security analysis with the aid of BIM (Stuart Porter, 2014)	2014	Australia
6	Challenges to BIM-cloud integration: Implication of security issues on secure collaboration (Abdul-Majeed Mahamadu, 2013)	2013	UK
7	Sensing network security prevention measures of BIM smart operation and maintenance system (Yu Peng, 2020)	2020	Kina
8	bcBIM: A Blockchain-Based Big Data Model for BIM Modification Audit and Provenance in Mobile Cloud (Rongyue Zheng, 2019)	2019	Kina

Tabell 5: Forskningsartiklenes innhold og konklusjon

	Tittel	Beskrivelse	Konklusjon/mangler
1	"BIM-enabled facilities management (FM): a scrutiny of risks resulting from cyber-attacks" (UK, 2021)	Utarbeidet en risikomatrise som fremhever fasilitetsstyrings-områdene som vil bli kompromittert som følge av et nettangrep.	Studien ønsker å øke fokuset til menneskene og prosessaspektene ved cybersikkerhet i BIM-fasilitetsstyring.
2	"Management Procedure for Sensitive Projects in the Context of a BIM Adoption in a Public Organization" (Brazil, 2020)	Foreslår prosesser for prosjektplanleggingsledelse, og hvordan dette kan brukes for en offentlig organisasjon som har egne prosjektteam for utvikling av militære prosjekter. Resultatet er basert på ISO19650 part 1, 2 og 5	Generelt er sikkerhetsproblemer i BIM-modeller svært ukjente for designere, og forholdet til andre prosessgrupper er fortsatt ukjent.
3	"Management of Collaborative BIM Data by Federating Distributed BIM Models" (UK, 2017)	Foreslått løsning gir en datamodell som automatisk forener og styrer distribuerte BIM-data. Bruken av dette gir en integrert BIM-modell som er fysisk fordelt på tvers av interessentene i et byggeprosjekt. Løsningen ble testet i et motorveiprosjekt.	Ytterligere validering må utføres for å sikre at modellen er fullt moden. Framtidig validering bør inkludere presentasjon av styringsmodell, sammen med nødvendige forbedringer, til et bredere spekter av byggebransjens interessenter, samt et større prosjekt som case-studie med flere disipliner.
4	"BIM-security: A critical review and recommendations using encryption strategy and blockchain" (Kina, 2021)	**1**-Identifiserer viktige komponenter innen «BIM security». **2**-Viser til tre ulike datasikkerhetskriterier som settes i sammenheng med de syv sikkerhetskomponentene fra første del. **3**-Tar for seg ulike cybersikkerhetsteknikker og teknologier **4**-Handler om implementering av rammeverk for «BIM-security»	Denne studien viser at teknologiene for å støtte BIM-sikkerhet er tilgjengelige på markedet, men de er ikke tilpasset eksisterende BIM-plattformer for samarbeid
5	"Breaking into BIM: Performing static and dynamic security analysis with the aid of BIM" (Australia, 2014)	Målet var å utvikle et BIM basert simuleringsverktøy som støtter fysisk sikkerhetsvurdering av bygg. Artikkelen viser en statisk og dynamisk tilnærming for å vurdere fysisk sikkerhet som krever mindre teknisk kompetanse og sikkerhetskompetanse enn ved å leie inn en ekspert.	Det utviklede simuleringsverktøyet er ifølge artikkelen fremdeles sett på som et «proof of concept» og har svakheter som blant annet å estimere innbrudds tid dersom en inntrenger løper.
6	"Challenges to BIM-cloud integration: Implication of security issues on secure collaboration" (UK, 2013)	Artikkelen kategoriserer fire nivåer av beskyttelsesløsninger, og diskuterer utfordringer og løsninger til disse: ***1. Infrastruktur og teknisk*** ***2. Informasjonsoppdeling og beskyttelse*** ***3. Juridisk og kontraktsmessig forvaltning*** ***4. Tillitbasert***	Artikkelen peker på at det fortsatt er generell mangel på forståelse for konsekvensene ved datatap, og rollen/ansvaret for nettskyleverandører ved av tap av data.
7	"Sensing network security prevention measures of BIM smart operation and maintenance system" (Kina, 2020)	Den foreslåtte metoden er basert på Bayesianske nettverksalgoritmer for å evaluere nettverksrisikoen til et BIM-intelligent drift og vedlikeholdssystem av en bro.	Det pekes på at den største risikoen med et nettverksangrep på en BIM er at inntrengere kan få tilgang til dataen og gjøre endringer.
8	"bcBIM: A Blockchain-Based Big Data Model for BIM Modification Audit and Provenance in Mobile Cloud" (Kina, 2019)	Målet var å lage en BIM-systemmodell som takler informasjonssikkerhetsutfordringer i skyløsninger. Artikkelen foreslo en metode for BIMdata-organisering basert på blokkjeder.	Artikkelen mener bruken av blokkjede vil fremme utviklingen av BIM-teknologi.

4 Resultater

Resultatene presenterer funnene fra intervjuene. Først presenteres holdninger og opplevelser aktører har innen digital sikkerhet, deretter for HMS. Siste del av resultatet sammenligner ISO 19650-5 med «typiske» HMS-aktiviteter slik de beskrives av (Proactima, 2016). Kapittelet er strukturert i samme rekkefølge som forskningsspørsmålene.

- Den digitale sikkerhetskulturen i byggenæringen
- Erfaringer fra HMS arbeid
- Sammenligning av ISO 19650-5 og HMS-aktiviteter

4.1 Den digitale sikkerhetskulturen i byggenæringen

Nasjonal sikkerhetsmyndighet (NSM) beskriver i (NSM, 2022a) at ansatte i næringslivet har for dårlig sikkerhetsfokus og sikkerhetsforståelse. For å finne ut hvordan dette er for byggenæringen og eventuelt hvordan det kan forbedres, skal oppgaven først kartlegge hvordan byggenæringens sikkerhetsfokus er i dag og holdningene rundt dette. Dette gjøres gjennom følgende punkter:

- Hvordan oppleves den digitale sikkerhetskulturen blant aktører i bransjen i dag?
- Hvilke erfaringer har aktører med digital sikkerhet?
- Hva tenker aktører at kan gjøres bedre i fremtiden?

Hovedspørsmålene har fulgt intervjuguide 1 (se vedlegg 1). Svarene fra de tre hovedspørsmålene skal bidra til å besvare første forskningsspørsmål; *Hvordan er den digitale sikkerhetskulturen blant aktører i byggenæringen i dag?*

4.1.1 Opplevelse av digital sikkerhetskultur i byggenæringen

Alle intervjuobjektene ble spurt om deres oppfatning av dagens holdninger til digital sikkerhet og informasjonssikkerhet i byggebransjen. Det har vært varierende formuleringer og svar blant de ulike aktørene og deres perspektiv. Noen fellestrekk har imidlertid utpekt seg. De ulike rollenes svar illustreres i tabell 6 og 7 og beskrives videre.

Tabell 6: Digital sikkerhetskultur beskrevet av aktører

Den digitale sikkerhetskulturen beskrevet av aktører i bransjen i dag					
	Stort fokus	Variabelt fokus	Lite fokus	Lite bevissthet	Manglende kunnskap
Produsent					
Entreprenør 1					
Entreprenør 2					
Rådgiver					
Arkitekt					
Byggherre 1					
Byggherre 2					
Oppsummering:	1 av 7	3 av 7	3 av 7	6 av 7	6 av 7

1 av 7 forklarer at de har stort fokus på sikkerhet. De mener dette er på grunn av deres rolle som forvaltere av kritisk infrastruktur. De påpeker imidlertid at andre deler av bransjen ikke har samme fokus. De forteller at dette heller ikke er nødvendig, da ikke alle har ansvar for kritisk infrastruktur.

3 av 7 aktører formidlet hvordan fokuset på digital sikkerhet og informasjonssikkerhet i stor grad varierte med type prosjekt, og at forskjellene var store. Flere fortalte at de hadde deltatt i graderte prosjekter, hvor det var så strengt at det kunne være utfordrende å gjøre jobben deres. Dette i stor kontrast til «ordinære» prosjekter hvor fokuset er lite, og det i større grad handler om å dele mest mulig.

3 av 7 beskriver at de ikke har spesielt fokus på digital sikkerhet og informasjonssikkerhet.

6 av 7 aktører omtaler at konsekvenstenkning rundt deling av bygningsinformasjon ikke er noe ansatte tenker på. De nevnte aktørenes inntrykk er at byggenæringen har en generelt lav bevissthet, selv om det i strengt graderte prosjekter er en større bevissthet rundt tematikken. Én av byggherrene og én av entreprenørene relaterte digital sikkerhet og informasjonssikkerhet kun til personvern og personopplysninger, og forklarte at sensitivitet i forhold til bygningsinformasjon ikke var blitt reflektert rundt.

6 av 7 intervjuobjekter mener det mangler kunnskap om temaet.

Tabell 7: Hva aktørene ønsker å beskytte i dag

Hva aktører er bevisste på å beskytte i bransjen i dag					
	Økonomi	Personvern	Data-systemer	Bygnings-informasjon	Bedrifts-hemmeligheter
Produsent	■		■		
Entreprenør 1	■	■	■		
Entreprenør 2		■	■		
Rådgiver	■		■		■
Arkitekt	■		■		■
Byggherre 1			■	■	
Byggherre 2	■	■	■		
Oppsummering:	5 av 7	3 av 7	7 av 7	1 av 7	2 av 7

5 av 7 aktører beskrev at informasjon tilknyttet økonomi ble regnet som sensitiv informasjon, og dette var derfor ansett som viktig å beskytte.

3 av 7 aktører fortalte at fokuset på personopplysninger og har økt kraftig de siste årene, og at dette var informasjon som ikke ble delt uten videre.

7 av 7 fortalte at de var opptatt av datasikkerhet, og hadde systemer for dette. Ofte var det IT-selskaper eller IT-avdelingen som hadde dette ansvaret.

1 av 7 opplevde bygningsinformasjon som sensitivt.

2 av 7 beskrev hvordan bedriftshemmeligheter og løsninger ble ansett som sensitiv informasjon, og dermed beskyttes.

Produsent

På spørsmål om hvordan fokus og holdninger til digital sikkerhet og informasjonssikkerhet oppfattes, svarte produsent at det generelt var veldig lite fokus og kunnskap om dette. Deres erfaring pekte mot enten/eller. Det kunne være veldig sikkerhetsfokus i noen prosjekter (eks. regjeringskvartalet), men til daglig var det lite fokus på denne typen sikkerhet. Produsenten fremhevet imidlertid at det var sjeldent det var sensitiv informasjon som ble sendt, og at det derfor ikke var «krise» om noen fikk tak i deres tegninger. De fortalte likevel at pristilbud og informasjon tilknyttet økonomi ikke var noe de ønsket å distribuere unødig.

På oppfølgingsspørsmål om hva de trodde årsaken til at det var lite fokus og kunnskap, ble det fortalt at gamle arbeidsrutiner og vaner var en av årsakene. Spesielt trekkes den eldre generasjonen frem, som over mange år har jobbet ut ifra gamle vaner. Godt innarbeidede rutiner kunne derfor være utfordrende å endre uten videre. En annen årsak produsenten trakk frem var at det hadde vært lite fokus på digital sikkerhet generelt i verden, spesielt for 10-20 år siden. Rutinene som ble innarbeidet da, har ikke nødvendigvis blitt oppdatert siden, forteller produsenten.

Det ble stilt spørsmål om de hadde opplevd at andre aktører hadde delt informasjon med dem som de kanskje ikke burde gjort. Svaret var først nei, men ved nærmere ettertanke ble et eksempel beskrevet. Produsent forklarte at de hadde sendt informasjon om blant annet et pristilbud til en aktør, og fått returnert den samme informasjonen med forespørsel fra en tredjepart. For det spesifikke tilfellet utgjorde ikke dette noen fare for bedriften, men det var et tydelig brudd på regler ved at informasjon hadde blitt delt uten samtykke. Det har imidlertid ikke blitt delt tegninger uønsket så vidt produsenten kjente til.

Entreprenør

Entreprenør 1 forteller hvordan informasjonen styres etter type bygg, og fokuset byggherren har på informasjonen som distribueres. Regjeringskvartalet blir igjen eksemplifisert som et byggeprosjekt med høyt fokus på sikkerhet, hvor mye er svært lukket. Samtidig forklarer de at et kontorbygg som skal stilles ut for markedet, ikke fokuserer like mye på sikkerhet (security), da det ikke er like viktig her. Entreprenør 1 presiserer at de forholder seg til kontrakter, og dersom det er spesifisert hva som skal deles og hva som er gradert, så følges dette. Dette mener de at er opp til byggherre og valg av kontraktsform.

På spørsmål om folk internt reflekterer rundt sensitiviteten til informasjonen de besitter svarer entreprenør 1 at det heller er motsatt. De er et større fokus på å dele mest mulig, ha større åpenhet og at de jobber for en bedre delingskultur. Dette mener de fører til mindre feil og dermed større fremdrift i prosjektene. Entreprenør 1 nevner likevel at det kan være utfordrende å få originalfiler fra spesielt arkitekter. Disse oppfattes som mer beskyttende enn andre aktører. Dette tror de er fordi arkitektene ikke ønsker at løsningene deres skal bli stjålet. Entreprenør 1 på sin side mener at en av fordelene med å dele BIM-modeller offentlig er at det gir dem som entreprenør god markedsføring av prosjekter, noe som kan lede til et konkurransefortrinn senere.

Entreprenør 2 mener at bransjen generelt er veldig uviten og har lite kunnskap om denne type sikkerhet. De forteller imidlertid at det er enkelte personer innad i organisasjonen

som prøver å skape en bedre sikkerhetskultur. Dette eksemplifiseres ved at de relativt ofte må gjennomføre mindre nettkurs. På spørsmål om hva disse kursene inneholder svarer entreprenør 2 at dette er veldig generelle informasjonssikkerhetskurs hvor man rådes til å ikke trykke på linker uten videre. Det ble stilt oppfølgingsspørsmål på om disse kursene var rettet mot byggebransjen, til dette var svaret nei.

Rådgiver/arkitekt

Det ble gjennomført intervju med en rådgiver og en arkitekt fra to ulike bedrifter på prosjekteringssiden. Arkitekten beskriver dette som en såpass ny problemstilling at de oppfatter at svært få tenker spesielt på bygningsinformasjon som sensitivt. Deres erfaring så langt er at alle løser slike problemer på sin egen måte, noe som fører til store variasjoner mellom ulike firmaer. Dette skaper relativt store forskjeller fra prosjekt til prosjekt. Dersom det ikke stilles spesifikke krav til hva som ikke skal deles, oppfatter arkitektens at få reflekterer over det.

Rådgiveren opplever også at svært få personer i byggebransjen tenker på dette av seg selv. De forteller likevel at deres bedrift har dette i bakhodet når det kommer inn en ekstern part. Fokuset beskrives som prosjektavhengig. Rådgiveren sier at enkelte prosjekter er så strenge at de ikke er tilkoblet nettverk og sitter eksternt. Noen prosjekter har litt fokus på det ved at de må signere papirer som gir de tillatelse til å produsere på prosjektet og som binder de til og ikke distribuere eller snakke om prosjektet. Andre prosjekter blir kjørt uten noe spesielt fokus på sikkerhet (security).

Byggherre

Det er intervjuet to ulike byggherrerepresentanter i denne studien. Begge byggherrene er store på nasjonalt nivå. Byggherre 1 beskriver deres sikkerhetsfokus som bra. Dette mener de skyldes deres ansvar for kritisk infrastruktur. De forteller imidlertid at få andre virksomheter (entreprenører, rådgivere, etc.) i byggenæringen har spesielt fokus på dette før de hyres inn av dem og blir bevisstgjort på det. Samtidig peker de på at det ikke er nødvendig for alle å ha dette sikkerhetsfokuset, ettersom ikke alle har ansvar for kritisk infrastruktur. De har gitt uttrykk for en stor interesse for temaet og mener holdningsendrende arbeid er svært viktig.

Byggherre 2 forteller at de ikke gjør noen sikkerhetsvurderinger (security) i forkant av deres prosjekter. Informasjonen de beskytter handler hovedsakelig om deres konkurransefortrinn og det økonomiske perspektivet. Til sammenligning forteller de at sikkerhetsfokuset til HMS har kommet veldig langt de siste årene. Informasjonssikkerhet tilknyttet personvern blir også mer fokusert på nå enn tidligere. Sikkerheten (security) rundt det tekniske på selve bygget blir ikke vurdert. Byggherre 2 forteller at det som oftest er entreprenøren som organiserer delingsplattformer med andre underentreprenører og underleverandører (Det er verdt å merke seg at dette gjelder totalentreprise, ettersom dette er mest brukt av byggherre 2). Samtidig er deres erfaring at dagens BIM modeller ikke er modne nok til å inneholde informasjon som er sensitiv.

På oppfølgingsspørsmål om hva de anså som sensitiv bygningsinformasjon i et byggeprosjekt, var respondenten usikker. Dette var noe intervjuobjektet forklarte at ikke var reflektert rundt. Ved å stille et bredere spørsmål om hvilke typer byggeprosjekter de anså som sensitive ble regjeringskvartalet, og generelt forsvarsprosjekter nevnt.

4.1.2 Hvilke erfaringer har aktører med digital sikkerhet?

Et interessant aspekt å kartlegge er hvilke erfaringer aktører i byggebransjen har med digital sikkerhet i dag. Har aktørene gjort forebyggende tiltak for å forhindre at sensitiv bygningsinformasjon kommer på avveie? De viktigste erfaringene som trekkes frem er presentert i tabell 8:

Tabell 8: Erfaringer med digital sikkerhet i byggebransjen

Erfaringer med digital sikkerhet i byggebransjen					
	Usikkerhet rundt hva som er sensitivt	Ulike tiltak fra bedrift til bedrift	Stor tillit til hverandre	BIM er ikke moden nok	Generell datasikkerhets-opplæring praktiseres
Produsent					
Entreprenør 1					
Entreprenør 2					
Rådgiver					
Arkitekt					
Byggherre 1					
Byggherre 2					
Oppsummering:	6 av 7	3 av 7	4 av 7	6 av 7	6 av 7

Ut ifra intervjuresultatene er det varierende hva aktørene anser som sensitiv informasjon i et byggeprosjekt. Felles for de fleste er at økonomi, personopplysninger og bedriftshemmeligheter ses på som sensitiv informasjon, og har følgelig måter å beskytte denne informasjonen.

Slik flere av intervjuobjektene beskriver, er det veldig ulikt hvordan aktører løser digitale sikkerhetsutfordringer. I forhold til BIM, fokuserer arkitekten og rådgiveren på å dele IFC-filer fremfor arbeidsfiler, men hovedhensikten er først og fremst å beskytte egne løsninger. Byggherre 1 er nøye på avtaler og kontrakter, og har i tillegg to ulike nettverk for å beskytte deres sensitive informasjon. Byggherre 2 har tatt grep rundt e-poster ved at de merkes med «begrenset», «beskyttet» eller «strengt beskyttet». Dette betyr ikke at de er kryptert, men kun merket. Hensikten er ifølge byggherre 2 å få mottaker til å tenke seg om før e-posten evt. deles med andre. Produsenten forteller at alt med økonomi generelt ikke skal deles.

I 4 av 7 intervjuer står tillit sentralt. Entreprenør 1 forteller at deres selskap er tuftet på kjerneverdier som blant annet tillit. Disse kjerneverdiene blir alle nyansatte introdusert for med en gang de starter. I tillegg er de opptatt av ansvar og etikk, og diskuterer dette internt. Dette mener de skaper en god kultur innad i selskapet og gjør alle mer opptatt av å være lojale. Til nå har de ikke opplevd at noen har vært illojale. Byggherre 1 på sin side forteller at de må stole på aktørene som jobber på prosjektet, og at de kommuniserer seg imellom på en fornuftig måte. Selv om de stiller krav til sikkerhet, har de i dag ikke kontroll på hva som deles videre mellom underentreprenører, rådgivere etc. Arkitekten forteller også at folk i bransjen har høy tillit til hverandre på dette området, og at mange avtaler gjøres muntlig i deres prosjekter. Blant annet tilgangsstyringer sendes gjerne med link via e-post. Byggherre 2 overlater det meste av ansvaret til entreprenøren og stoler på at de sørger for at informasjon ikke kommer på avveie.

6 av 7 intervjuobjekter peker på BIM og sikkerhet som et fremtidig problem. Flere mener at BIM modellene i dag ikke er modne nok til å inneholde spesielt sensitiv informasjon. Samtidig forteller enkelte at bransjen generelt ikke har kunnskap nok til å vite hvordan dette kan utnyttes.

6 av 7 aktører beskriver at de har nettkurs i informasjonssikkerhet og digital sikkerhet. Disse kursene beskrives som generelle, og ikke spesifikt bygg-rettet. Tabell 9 viser hvilke erfaringer intervjuobjektene har med digitale angrep i deres organisasjon.

Tabell 9: Opplevelser med digitale sikkerhetshendelser

Opplevelser med digitale angrep/ informasjon på avveie i byggebransjen				
	«phishing» mails	Større hacking angrep	Uønsket deling av informasjon	Ingen kjente opplevelser
Produsent				
Entreprenør 1				
Entreprenør 2				
Rådgiver				
Arkitekt				
Byggherre 1				
Byggherre 2				
Oppsummering:	5 av 7	1 av 7	4 av 7	1 av 7

Produsent

Produsenten forteller at de har opplevd uønskede delinger av økonomisk informasjon mellom aktører, men ikke bygningsinformasjon. Produsenten forteller videre at det er begrenset med informasjon å hente fra deres modeller og at det derfor ikke er «krise» om noen får tilgang til dette. I de prosjektene det er mye sensitiv informasjon, sitter man som regel på en ekstern plass uten tilkobling til internett, og klare regler. Det er i praksis lite man får gjort i de tilfellene. Intervjuobjektet uttrykker også at denne måten å jobbe på kan være slitsom, og fører ofte til at selv enkle ting blir krevende. På spørsmål om produsenten har blitt forsøkt svindlet eller angrepet av en trusselaktør, var svaret nei. De blir imidlertid jevnlig utsatt for «phishing mails», men ikke noe annet utover det som vedkommende husket.

Entreprenør

På spørsmål om entreprenørene har opplevd at andre aktører har delt informasjon med dem som de ikke burde, ble det fortalt om jevnlige «phishing» mails. De hadde ikke opplevd uheldig deling av bygningsinformasjon. Entreprenør 2 utelukket imidlertid ikke at det kunne ha skjedd andre steder i bedriften. Det var sjeldent tilfeller av hacking og uheldige delinger ble informert om til resten av virksomheten dersom dette ikke direkte hadde påvirkning eller konsekvenser for videre arbeid. Begge entreprenørene forteller at de også har jobbet i strengt graderte prosjekter hvor de har vært uten tilkobling til internett. De forteller at det er langt fra samme bevissthet og fokus i vanlige prosjekter. Entreprenør 2 beskriver dette som en såpass ny problemstilling, og mener dette sannsynligvis vil få et større fokus i fremtiden.

Rådgiver og Arkitekt

Både rådgiver og arkitekt jobber ut ifra web-hoteller som de får tilgang til av entreprenøren (som oftest). Rådgiveren forteller at de ofte bruker to-faktor løsninger for å logge seg på webhotellet. Både rådgiver og arkitekt deler hovedsakelig IFC-filer, og ikke arbeidsfiler hvor det er mulig å gjøre endringer. Grunnen til dette er ifølge arkitekten at det ofte tegnes og kladdes løsninger på siden av modellen i arbeidsfilene som de ikke ønsker å dele med andre av konkurransehensyn.

Arkitektens inntrykk er forskjellige bedrifter løser sikkerhet på sin egen måte, noe som skaper store variasjoner fra bedrift til bedrift, og prosjekt til prosjekt. I tillegg bruker mange bedrifter ulike programmer, verktøy og filformater, noe som også bidrar til store variasjoner i utførelse. Det ble stilt spørsmål om hvordan kommunikasjonen mellom aktørene foregår uten at den blir tilgjengelig for alle i web-hotellet. Til dette svarer rådgiveren at det finnes egne kommunikasjonssystemer for dette i noen skyløsninger. Arkitekten forteller at dette stort sett foregår på mail, eller ved deling av dropbox mapper. Dette er avhengig av prosjektet og systemene til de som oppretter web-hotellet.

Både arkitekten og rådgiveren forteller også om jevnlige «Phishing» mails. I forhold til større hacking angrep forteller arkitekten at deres bedrift har vært utsatt for et hackerangrep for noen år siden. Ingen har ellers opplevd tilfeller i senere tid. På spørsmål om det i dag blir gjennomført opplæring i informasjonssikkerhet og digital sikkerhet svarte rådgiver at de har generelle e-læringskurs de må gjennom med jevne mellomrom. Arkitekten forteller at dette ikke praktiseres i deres bedrift, men at det meste av digital sikkerhet blir tatt hånd om av et eksternt IT-selskap.

Byggherre

Byggherre 1 forteller at det har vært tilfeller av informasjon på avveie og BIM modeller som har ligget på steder hvor byggherre 1 ikke har hatt kontroll på den. Byggherre 2 forteller om hendelser hvor de har mottatt interne e-post samtaler fra eksterne bedrifter som ved en feil har blitt delt. Begge byggherrene sier de må gjennom generelle opplæringskurs i datasikkerhet og informasjonssikkerhet. Begge var imidlertid usikre på om alle aktørene som jobbet for dem i prosjekter måtte gjennom tilsvarende.

4.1.3 Hva tenker aktører at kan gjøres bedre i fremtiden?

I forbindelse med kartleggingen av holdninger rundt digital sikkerhet er det nå beskrevet hva aktører i bransjen tenker om tematikken. En annen relevant side å undersøke er hva intervjuobjektene selv tenker kan bli bedre i fremtiden. Tabell 10 oppsummerer de viktigste tiltakene aktører mener kan forbedres i fremtiden.

Tabell 10: Hva aktørene mener bør forbedres

Hva tenker aktører at kan gjøres bedre i fremtiden?			
	Øke bevisstheten og kunnskapen	Standardisering	Utvikle bedre delingsplattformer
Produsent			
Entreprenør 1			
Entreprenør 2			
Rådgiver			
Arkitekt			
Byggherre 1			
Byggherre 2			
Oppsummering:	7 av 7	2 av 7	1 av 7

7 av 7 aktører peker på at økt kunnskap og bevisstgjøring bør bli bedre i fremtiden. Flere av intervjuobjektene mener de selv har for liten kunnskap om tematikken.

2 av 7 peker i tillegg på standardisering som en viktig faktor. Dette er med bakgrunn i erfaringen om at mange aktører i dag løser sikkerhetsutfordringer forskjellig.

Produsenten fremhever at delingsplattformene bør forbedres og tilpasses. De forteller om mange ulike webhoteller, formater og lignende som fører til mye manuelt arbeid. Produsenten forteller at bedre delingsplattformer som er mer integrert med modelleringsprogrammene fører til mindre manuelt arbeid. Dette mener de kan redusere menneskelig feil og igjen øke sikkerheten.

4.2 Erfaringer fra HMS arbeid

De fleste som har vært på en byggeplass i dag er kjent med Helse- miljø og sikkerhet (HMS). Byggherreforskriften stiller en rekke krav til HMS, noe som gjør at mange også har dette i baktankene når de foretar seg ulike arbeidsoppgaver i bygg- og anleggsarbeid. De fleste er også klar over at bransjen har kommet en lang vei innen HMS de siste tiårene. Spørsmålet er hvordan byggenæringen har klart å skape et økt fokus og til en viss grad endret holdninger blant ansattes forhold til HMS? Er det noe ved dette som kan overføres til arbeidet med digital sikkerhet? Kapittel 4.2 skal undersøke hvordan aktørene opplever HMS-kulturen, samt hvilke tiltak de selv mener har hatt effekt. Hensikten med kapittel 4.2 er å besvare studiens andre forskningsspørsmål; «*Hva kan man lære av HMS?*».

I likhet med digital sikkerhet er det valgt å dele opp kapittelet i tre underkategorier som skal bidra til å besvare forskningsspørsmålet:

- Hvordan oppleves HMS kulturen blant aktører i byggenæringen i dag?
- Hvilke erfaringer har man fra HMS arbeid?
- Hva mener aktører at kan gjøres bedre i fremtiden?

4.2.1 Hvordan oppleves HMS kulturen blant aktører i byggenæringen i dag?

Selv om de fleste vet at HMS har blitt bedre de siste årene, er det likevel interessant å høre hva aktørenes inntrykk av holdningene til dette er i dag. Er man kommet dit man ønsker med HMS? Tabell 11 illustrerer hva aktørene mener om dagens HMS kultur.

Tabell 11: Hvordan HMS kulturen oppleves i byggebransjen

Hvordan oppleves HMS kulturen i byggebransjen?					
	Svært bra	Dårlig	Påvirkes av størrelse på bedrift	Påvirkes av by/distrikt	Påvirkes av kulturforskjeller
Produsent					
Entreprenør 1					
Entreprenør 2					
Rådgiver					
Arkitekt					
Byggherre 1					
Byggherre 2					
Oppsummering:	5 av 7	1 av 7	2 av 7	1 av 7	3 av 7

5 av 7 aktører opplever HMS i dag som svært bra. Flere mener at HMS generelt snakkes mye om og tas seriøst. 1 av 7 opplever HMS kulturen som «skremmende dårlig», spesielt hos de eldre generasjonene av ansatte.

Arkitekten opplever at fokuset og holdningene til HMS varierer med størrelsen på bedriften. Store entreprenørselskaper har oftere bedre systemer og samtidig en bedre kultur for dette, sammenlignet med mindre bedrifter. I de mindre bedriftene kan HMS i større grad bli ansett som en kostnad og et hinder. Opplevelsen til entreprenør 2 er at holdningene er bedre i større byer sammenlignet med distriktene.

3 av 7 forteller at kulturforskjeller, som følge av økt utenlandsk arbeidskraft også påvirker HMS.

Produsent

På spørsmål om hvordan fokuset og holdningene rundt HMS oppleves, forteller produsenten at den oppleves som bra. De mener det er et stort fokus på HMS hos de som produsent, både i selve produksjonen, men også under dimensjonering og modellering på kontoret. De beskriver hvordan HMS ofte tar en del plass i møter og at det brukes mye tid på det. Dette opplever produsenten som positivt.

Det ble også stilt mer konkrete spørsmål om hvordan de tar hensyn til dette, hvor de forteller at det gjøres flere forebyggende HMS tiltak allerede på kontoret ved å regne på løft, planlegge og tilrettelegge for håndtering av produktene på byggeplassen. De ønsker å fremheve det som veldig positivt at HMS får så mye oppmerksomhet, da det er et veldig viktig tema. På spørsmål om eventuelle negative sider med dagens HMS prosess, kommer ikke intervjuobjektet på noe spesifikt.

Entreprenør

Entreprenør 1 forteller at de opplever en kjempeforbedring når det kommer til fokuset på HMS de siste 20 årene. De forteller at sikkerhetskulturen (safety) er med helt fra tidligfasen i utviklingen av et prosjekt. I tillegg til dem selv, ber de også premissfagene om å identifisere typiske faremomenter og risikoer for deres område, som videre blir fulgt opp.

De ønsker å trekke frem bevisstheten bransjen har fått på sikkerhet og helse gjennom ulike systemer og prosesser som veldig positivt. De forteller likevel at det kan være utfordrende å få aksept ute i produksjon for at man ønsker å ta vare på egen eller andres helse. De mener en årsak til dette er alle de ulike personlighetene. Entreprenør 2 beskriver i tillegg at holdninger til HMS ofte påvirkes av om prosjektet er lokalisert ute i distriktet eller om det bygges i byen. I tillegg mener entreprenør 2 at holdningene også påvirkes av kulturforskjellene hos utenlandske arbeidere.

Rådgiver/Arkitekt

Både rådgiver og arkitekt forteller at HMS er et tema som det i dag fokuseres mye på. Spesielt på byggeplasser, men også innenfor prosjektering. Begge forteller at det er langt flere tiltak i dag, enn det var for bare noen få år siden. Personer uten HMS-opplæring slipper i dag ikke inn på en byggeplass, noe som tidligere ikke var like strengt. De fremhever imidlertid at HMS ofte er strengere hos de utførende (entreprenører), ettersom denne delen av byggeprosessen er mer direkte utsatt for ulykker.

Arkitekten forteller at deres erfaring tyder på at mindre selskaper synes å ha mindre fokus på HMS, og noen har også en mer negativ holdning til dette. De forteller at en mulig årsak til dette kan være at et godt system for rapportering og avvikshåndtering utgjør en større kostnad for et mindre selskap enn for et stor, og at de gjerne arbeider for mindre byggherrer som ikke stiller like strenge krav til HMS. Et SHA-dokument som en større byggherre utarbeider, stiller ofte strengere krav til aktørene i prosjektet om hvilke HMS-tiltak som må tilfredsstilles. Dette gjelder også for de prosjekterende.

Byggherre

Byggherre 2 opplever dagens HMS prosess som veldig bra og mener HMS-kulturen generelt står sterkt i Norge. De forteller at systemene som brukes gir god oversikt og dokumentasjon på sikkerheten i et prosjekt. I dagens store byggeprosjekter forteller byggherre 2 at gode HMS prosesser har blitt et konkurransefortrinn, noe de mener kan være en faktor som fører til at flere ønsker å etablere bedre systemer og skape god kultur for dette. En annen faktor som trekkes frem er at det er andre typer folk som er med å lede byggeprosjektene nå, sammenlignet med før. Tidligere var det flere «cowboy-typer». Byggherren opplever også at utenlandske arbeidere har andre holdninger til HMS og at de er helt avhengig av gode ledere som kan språket og kulturen.

4.2.2 Hvilke erfaringer har aktører fra HMS arbeid?

For å kunne høste kunnskap og erfaringer fra HMS og undersøke om noe av dette kan være overførbart til den digitale sikkerhetskulturen er det relevant å høre med aktørene i bransjen om hvilke tiltak og systemer de selv mener har hatt størst effekt i praksis. I tabell 12 presenteres det aktørene erfarer er de viktigste faktorene som har påvirket fokuset og holdningene til HMS:

Tabell 12: Faktorer som har påvirket HMS-kulturen

Faktorer aktører mener har påvirket HMS kulturen i byggenæringen					
	Lovverk og krav	Systemer og rutiner	Økonomi	Læring av feil	Utenlandsk arbeidskraft
Produsent					
Entreprenør 1					
Entreprenør 2					
Rådgiver					
Arkitekt					
Byggherre 1					
Byggherre 2					
Oppsummering:	4 av 7	6 av 7	3 av 7	3 av 7	2 av 7

4 av 7 opplever lovverk og krav som viktige faktorer som ligger til grunn for HMS arbeidet. Det pekes på byggherreforskriften og spesifikke krav som byggherre stiller gjennom blant annet SHA-planen.

6 av 7 mener gode systemer og rutiner er en viktig faktor som har økt bevisstheten til ansatte i bransjen. Mange av rutinene og systemene er relativt like hos aktører i bransjen, men entreprenør 2 forteller at det likevel kan være en utfordring når aktørene benytter ulike digitale plattformer for registrering og gjennomføring av HMS rutinene. Dette beskrives som en utfordring som følge av den digitale utviklingen og at det stadig utvikles nye programmer og digitale verktøy.

3 av 7 trekker frem økonomiske insentiver som en viktig årsak for HMS arbeidet. De økonomiske årsakene beskrives som både positive og negative. 3 aktører forteller hvordan gode HMS rutiner kan gi et konkurransefortrinn i større byggeprosjekter. Dette kan dermed være en motivasjon for andre bedrifter til å utvikle gode HMS-systemer. Samtidig peker flere på at det i mindre byggefirmaer fokuseres mindre på HMS da byggherren ofte er mindre, har lavere kunnskap og stiller mindre krav til HMS. I disse tilfellene vil derfor ikke HMS utgjøre et konkurransefortrinn og derfor kan ofte HMS oppleves som en negativ kostnad blant enkelte.

3 av 7 mener at læring er et viktig nøkkelord i HMS arbeidet. Rådgiver forteller at bransjen har vært gode på å lære av feil, noe som har ført til utvikling.

2 av 7 beskriver den økende utenlandske arbeidskraft som en stadig viktigere faktor. Flere aktører mener Norge er i en særklasse når det kommer til å fokusere på god HMS. Her kan kulturforskjeller skape utfordringer, og de mener det er avgjørende med gode prosjektledere som kan språket og kulturen.

Produsent

Produsenten beskriver at større møter alltid åpnes med HMS som første punkt. De mener at når dette til stadighet får oppmerksomhet så blir man også mer bevisst og det blir en naturlig del av hverdagen. Produsenten forteller at tydelige regler og krav fører til at man skal ta seg tid til å tenke på HMS. Da er gode systemer og rutiner veldig viktig.

Entreprenør

Entreprenør 1 mener at så mye som mulig risiko bør prosjekteres bort på forhånd. Det som da ikke er mulig å prosjektere bort (restrisikoen) blir da tatt hånd om gjennom en sikker jobb analyse (SJA) på byggeplass. De forteller også at 3D modeller i større grad brukes for å illustrere fareområder og 4D planlegging for å gjøre logistikken lettere i forhold til bevegelse og transport ut og inn på byggeplassen. Entreprenør 1 mener dette er systemer som fungerer bra og bidrar til økt bevissthet hos alle på byggeplassen. Rapport om uønsket hendelse (RUH) blir også snakket frem som et viktig virkemiddel for læring. Alt fra små til store ulykker vil registreres og danne statistikk og erfaringsgrunnlag.

Entreprenør 2 forteller at de følger byggherreforskriften og kravene som kommer i SHA-planen fra byggherre. I SHA-planen fremkommer det mange føringer for hvordan sikkerheten skal ivaretas. I tillegg har de rutiner som i noen tilfeller går ut over forskriftskravene. Mange av sikkerhetstiltakene er prosjektspesifikke, i tillegg til å ivareta det generelle. Entreprenør 2 forteller imidlertid at en utfordring er alle de ulike systemene og plattformene som forskjellige bedrifter jobber ut ifra. Selv om systemene i seg selv er gode, kan det være utfordrende å samarbeide med underentreprenører som har andre systemer. På spørsmål om hvilke deler av HMS entreprenør 2 tenker fungerer bra, svarer entreprenør 2 som eneste aktør at psykisk helse har fått større plass. Når det kommer til utfordringer med HMS, forteller de at kommunikasjon ofte kan være vanskelig. For mange på byggeplassen kan det være vanskelig å forstå hvorfor alle reglene og tiltakene finner sted og hindrer fremdriften i prosjektet.

Rådgiver/prosjekterende

På spørsmål om hvilke faktorer prosjekterende tenker er avgjørende for at byggebransjen fokuserer mer på HMS i dag, sammenlignet med tidligere blir lovverk og krav, dokumentasjon og læring av feil pekt ut som spesielt viktige faktorer.

Dokumentasjon på gode HMS-rutiner kan gi et konkurransefortrinn i anbudsfaser, mener arkitekten. Et SHA dokument som en større byggherre utarbeider, stiller krav til aktørene i prosjektet om hvilke HMS-tiltak som må tilfredsstilles. Dette gjelder også for de prosjekterende. For dem kreves det at en HMS tankegang skal ligge i bakhodet til alle som tegner og prosjekterer. Under prosjekteringsmøter, arrangert av for eksempel en entreprenør er det derfor viktig for utførende å få oversikt over eventuelle endringer som kan få følge for HMS. Dette er derfor et punkt som alltid blir tatt opp i prosjekteringsmøter. Eksempelvis vil store tunge elementer og krevende løfteoperasjoner være noe av det de prosjekterende må tenke på i forhold til HMS for å hindre unødvendig risiko ved bygging.

Arkitekten mener at ledelsen har den største påvirkningen til å skape gode systemer og prosesser ved å stille krav. Som konkrete tiltak, trekkes SHA-plan, sjekklister og avviksmeldinger frem som HMS prosedyrer det er lett å se fungerer, ettersom det er dokumentasjon som fylles ut. Samtidig er det også en del folk, spesielt i mindre bedrifter som synes dette er et ork. Intervjuobjektet tror selv at dersom det hadde vært opp til arbeiderne, ville det vært mye mindre fokus på HMS. Rådgiveren mener HMS er flinke på å lære av feil etter ulykker og nesten-ulykker.

Byggherre

Byggherre 2 tror at noen av faktorene til at det fokuseres mer på HMS i dag sammenlignet med tidligere er at det er andre typer folk som er med på å lede prosjektene. I dagens byggebransje er det flere yngre folk med høyere utdannelse som kommer inn i prosjekter med en annen bevissthet og holdning. En annen faktor som nevnes er de økonomiske insentivene. I større prosjekter i dag, beskrives det som et stort konkurransefortrinn å ha gode systemer for HMS. Den tredje faktoren er nettopp systemene i seg selv. De har blitt svært mye bedre de siste årene, noe som gjør HMS dokumentering og rutiner for dette enklere i praksis.

Byggherre trekker frem et system hvor alle som skal inn på en byggeplass må gjennom en sikkerhetskontroll hvor dokumentasjon på gjennomført HMS kurs og andre kurs blir kontrollert. Her blir arbeidere på forhånd introdusert for hvor HMS konteinere befinner seg og hvor det er farlige soner på byggeplassen. Byggherre 2 opplever at når ledere på toppnivå snakker om HMS og vektlegger dette, så påvirker det holdningene til hele bedriften.

4.2.3 Hva tenker aktører at kan gjøres bedre i fremtiden?

I dette delkapittelet har aktørene blitt spurt hva de tenker kan bli bedre i HMS arbeidet. Dette er interessant å kartlegge da det kan indikere hvilke type prosesser og systemer som fungerer i praksis og ikke. Tabell 13 oppsummerer aktørenes meninger:

Tabell 13: Hva som kan gjøres bedre innen HMS i fremtiden

Hva aktører mener kan gjøres bedre i fremtiden				
	Fungerer bra i dag	Mer fokus på mental helse	Bedre holdninger ute i produksjon	Vet ikke
Produsent				
Entreprenør 1				
Entreprenør 2				
Rådgiver				
Arkitekt				
Byggherre 1				
Byggherre 2				
Oppsummering:	2 av 7	1 av 7	2 av 7	2 av 7

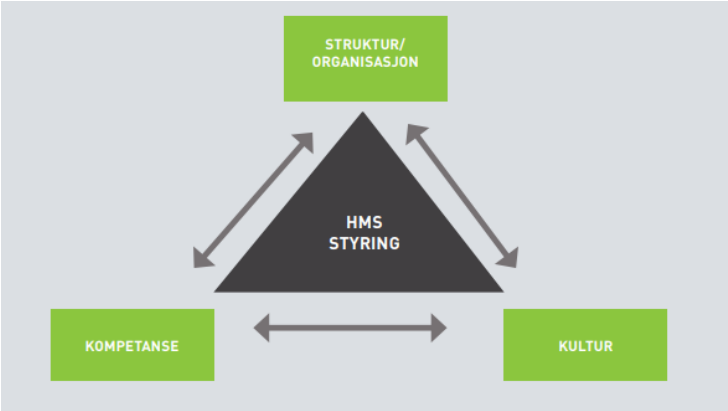
4.3 Sammenligning av NS-EN ISO 19650-5:2020 og HMS

Intervjusvarene presentert i kapittel 4.1 og 4.2 tegner et bilde av hvordan holdninger til både digital sikkerhet og HMS er i dag. Formålet med dette delkapittelet er å sammenligne ISO 19650-5 med de prosesser som i dag finnes for HMS. Sammenligningen er en fortolkning basert på intervjuresultatene, analysering av ISO 19650-5 og typiske HMS aktiviteter beskrevet i veilederen (Proactima, 2016). Hvilke likhetstrekk er det mellom ISO 19650-5 og HMS prosessene i byggenæringen? Delkapittelet skal bidra til å besvare det tredje forskningsspørsmålet; «*Hvilke tiltak kan gjøres i praksis basert på ISO 19650-5?*».

Selv om betydningen av sikkerhet i en HMS sammenheng er ulik digital sikkerhet og informasjonssikkerhet, er det fremdeles likheter i måten farer og risikoer håndteres. Gjennom å etablere systemer, rutiner og kunnskap, har HMS allerede gått opp en sti i byggenæringen. Denne sammenligningen har derfor kun fokusert på de viktigste overordnede punktene, da en grundig gjennomgang ville blitt for tidkrevende for denne studien.

Struktur, kultur og kompetanse

((Proactima, 2016), s. 6) beskriver kjennetegnene for god HMS styring til å være sammensatt av struktur/organisasjon, kultur og kompetanse. Dette har de illustrert i figur 8.



Figur 8: Kjennetegn for god HMS-styring (Proactima, 2016)

Det kan trekkes sammenhenger mellom figur 8 og tabellene i kapittel 4.1 som viser intervjuobjektenes inntrykk av sikkerhetskulturen i byggenæringen. Det ((Proactima, 2016), s. 6) omtaler som kjennetegn for god HMS styring, er blant faktorene intervjuobjektene trekker frem som mangler innen digital sikkerhet.

> *«I tillegg sier vi at kultur er brillene du ser på omgivelsene dine med, og som er med på å bestemme hva du ser som riktig og galt og hvordan vi bedømmer andres og egen atferd og valg. Det betyr at kulturen virker som en norm for hvordan vi skal utføre arbeidet på en «sikker» måte». ((Proactima, 2016), s. 19)*

Denne beskrivelsen er også relevant for digital sikkerhet, hvor (NSM, 2022a) har poengtert betydningen av bevissthet. Ved å plassere det (Proactima, 2016) omtaler som typiske HMS aktiviteter i bygge- og anleggsprosjekter ved siden av hoved stegene i ISO 19650-5, finnes det en rekke likhetstrekk. Dette blir presentert i de videre kapitlene.

4.3.1 Struktur

(Proactima, 2016) omtaler struktur som én av tre viktige faktorer for god HMS styring. For å få frem sammenhengen mellom ISO 19650-5 og HMS, er det valgt å sette hoved stegene i ISO 196505-5 ved siden av HMS-aktivitetene fra (Proactima, 2016). Resultatet presenteres i tabell 14.

Tabell 14: Hovedsteg i ISO 19650-5 og HMS-aktiviteter

Likhetstrekk mellom ISO 19650-5 og HMS aktiviteter	
ISO 19650-5	**HMS aktiviteter**
Sensitivitetsvurdering	HMS Risikovurdering
Sikkerhetsstrategi	HMS Strategi
Sikkerhetsstyringsplan	SHA-plan
Plan for håndtering av sikkerhetsbrudd	Beredskapsplan og avviksrapportering
Arbeid med tredjeparter	Samarbeid og Kommunikasjon
Rammeverk, lover og forskrifter	Rammeverk, lover og forskrifter

Vurderingsprosess

((Proactima, 2016), s. 8) beskriver hvordan HMS-risiko tradisjonelt har blitt håndtert gjennom det de omtaler som hendelsesbasert HMS-styring. Dette går ut på at risiko håndteres basert på tidligere uønskede hendelser og erfaring. Etter hvert som utviklingstakten har økt, har denne metoden i dag blitt utvidet ved at det også må gjennomføres risikovurderinger i alle faser av et prosjekt. Alle tiltak og planer baseres på disse vurderingene. ((Proactima, 2016), s. 8) skriver at denne type HMS styring har vokst frem i industrier som blant annet luftfartssektoren og offshore industrien, hvor det har vært for farlig og dyrt å gjøre seg erfaringer i full skala uten å ha noen formening om hva som kan gå galt på forhånd, og hvordan det kan håndteres.

Denne teknikken har likhetstrekk med det ISO 19650-5 beskriver. Første del av ISO 19650-5 handler om å gjennomføre en prosess for sensitivitetsvurdering. Hensikten er ifølge ((Standard-Norge, 2020), Kap. 4) å identifisere sårbarheter man ellers ikke ville vært klar over, både innad i organisasjonen og for samfunnet ellers. Dersom digitale sikkerhetshendelser oppstår, kan dette få svært store følger. Til forskjell fra HMS vil digitale sikkerhetshendelser påvirke organisasjonen og samfunnet på andre måter enn ved HMS.

Tabell 15: Vurderingsprosesser

ISO 19650-5	**HMS**
Sensitivitetsvurdering	HMS Risikovurdering
• Prosess for sensitivitetsvurdering • Registrere resultatet • Bestemme hvorvidt det er behov for metode med fokus på sikkerhet	• Planlegging • Risikovurdering • Risikohåndtering

Sikkerhetsstrategi

På bakgrunn av risikovurderingene som identifiseres, blir det utarbeidet en HMS strategi. Her utarbeides en HMS-policy som ifølge ((Proactima, 2016), s. 17) baserer seg på byggherrens overordnede visjon og verdier, samt en risikovurdering som kartlegger overordnede faremomenter. HMS-policyen beskrives som drivende for etablering av HMS-mål. I tillegg til en god policy er innhenting av erfaringer fra andre tilsvarende prosjekter et viktig grunnlag for HMS målene. HMS målsettinger og strategiene for å oppnå disse etableres i denne fasen. I strategifasen er det i HMS også sentralt å legge grunnlaget for ønsket HMS-kultur og organisasjonskultur generelt. Dette handler blant annet om å ha en felles forståelse for hvordan farer kan reduseres, og hva man ser på som farer.

ISO 19650-5 presenterer en lignende struktur innen informasjonsforvaltning med fokus på sikkerhet. Problemstillingene er imidlertid noe ulike. Når HMS fokuserer på enkeltindividets helse, fokuserer ISO 19650-5 på informasjonsflyten i et prosjekt og i større grad samfunnets sikkerhet. Det er likevel mange av de samme prinsippene som ligger til grunn i prosessen. Tabell 16 viser sikkerhetsstrategien til ISO 19650-5 sammenlignet med HMS strategien slik ((Proactima, 2016), s. 17) beskriver.

Tabell 16: Sikkerhetsstrategier

ISO 19650-5	**HMS**
Sikkerhetsstrategi	HMS strategi
• Vurdere sikkerhetsrisikoene som er identifisert • Utvikle risikodempende tiltak • Dokumentere restrisiko og tolererte sikkerhetsrisikoer	• HMS policy • Identifisere erfaring fra tidligere prosjekt • Utvikle HMS mål • Etablere grunnlag for ønsket HMS-kultur

Sikkerhetsstyringsplan

(Arbeidstilsynet, 2022) beskriver at byggherren er ansvarlig for utarbeidelsen av en plan for sikkerhet, helse og arbeidsmiljø (SHA-plan). Denne skal være tilpasset det bestemte byggearbeidet. SHA-planen skal beskrive strategien og tiltakene som ble utarbeidet i strategi-fasen.

Tilsvarende sikkerhetsstyringsplan er beskrevet i ISO 19650-5. Denne planen kan tolkes på tilsvarende vis til å beskrive hvordan strategien skal gjennomføres. I tabell 17 er beskrivelsene fra (Arbeidstilsynet, 2022) og ((Standard-Norge, 2020), kap. 7) presentert.

Tabell 17: Styringsplaner for sikkerhet

ISO 19650-5	**HMS**
Sikkerhetsstyringsplan	SHA-plan
• En registrering av resultatet av anvendelsen av den behovsprøvde prosessen. • Ordninger for styring, ansvar og ansvarlighet for metoden med fokus på sikkerhet. • Vurdering av de spesifikke sikkerhetsrisikoene for organisasjonen(e) som oppstår fra større tilgjengelighet til informasjon, integrering av tjenester og systemer og økt avhengighet av teknologibaserte systemer. • Potensielle risikodempende tiltak for å ta hensyn til de aktuelle sikkerhetsrisikoene og tiltakene som skal implementeres. • En oppsummering av de tolererte sikkerhetsrisikoene og gjenværende tolererte sikkerhetsrisikoer. • Mekanismene for å gjennomgå og oppdatere sikkerhetsstrategien.	• Beskrivelse av bygge- og anleggsplassens organisering, roller, ansvarsfordeling og entrepriseform • Framdriftsplan for anlegget som viser når og hvor de ulike arbeidsoperasjoner skal finne sted. • Beskrivelser av de spesifikke tiltakene knyttet til arbeid som kan innebære fare for liv og helse • Rutine for behandling av endringer og oppdatering av planen

Plan for håndtering av sikkerhetsbrudd

HMS har systemer for å håndtere ulykker, både små og store. På byggeplasser finner en ofte en HMS-tavle hvor blant annet en beredskaps og varslingsplan står, samt ansvarlige personer. En viktig del av håndteringen av uønskede hendelser er at folk vet hva som skal gjøres. Derfor beskriver ((Proactima, 2016), s. 42) at dette løses ved opplæring og jevnlige øvelser på ulike hendelser.

ISO 19650-5 stiller også krav til en plan for håndtering av sikkerhetsbrudd. Digitale sikkerhetshendelser skiller seg fra HMS ved at konsekvensene ofte er usikre og ikke like håndfaste som ved en brekt hånd, eller brann. Prinsippene har samtidig likhetstrekk ved at sikkerhetshendelsens omfang må kartlegges, deretter gjøre skadebegrensende tiltak for så å ta stilling til følgene. Tabell 18 lister opp prinsippene fra ((Standard-Norge, 2020), kap. 8) og HMS aktivitetene beskrevet i ((Proactima, 2016), s. 38).

Tabell 18: Plan for håndtering av sikkerhetsbrudd

ISO 19650-5	**HMS**
Håndtering av sikkerhetsbrudd	Håndtering av uønskede hendelser
• Avdekke • Oppbevare og gjenvinne • Gjennomgå følger	Avviksrapportering Etablering av beredskap • Identifisering • Etablering • Evaluering Opplæring og trening

Arbeid med tredjeparter

((Proactima, 2016), s. 35) beskriver viktigheten av å etablere tydelige HMS-krav i anbuds- og kontraktsdokumentasjon. Videre blir det antydet at det kan ha stor betydning for prosjektets HMS prestasjoner å stille tilsvarende krav til kulturdimensjonen.

> *«Det å stille gode og spesifikke krav i forhold til HMS ovenfor underleverandører er avgjørende for å oppnå gode HMS-resultater i et bygge- og anleggsprosjekt» ((Proactima, 2016), s. 35)*

ISO 19650-5 ((Standard-Norge, 2020), kap. 9) stiller krav til opprettelse av informasjonsdelingsavtaler i arbeid som foregår uten andre formelle avtaler. I øvrige tilfeller skal informasjon om hva som skal deles omfattes av andre avtaledokumenter. Tabell 19 illustrerer sammenhengen mellom ISO 19650-5 og HMS ved arbeid med tredjeparter.

Tabell 19: Krav til arbeid med tredjeparter

ISO 19650-5	HMS
Arbeid med tredjeparter	Arbeid med tredjeparter
• Avtaler om informasjonsdeling	• Etablere tydelige HMS-krav i anbuds- og kontraktsdokumentasjon

Rammeverk, lover og forskrifter

Et viktig fundament i etablering av rutiner og systemer er rammeverk, lover og forskrifter. Dette tvinger på mange måter frem en endring, og gjør at sikkerhet ikke kan neglisjeres. Tabell 20 viser relevante rammeverk, lover og forskrifter. For HMS henvises det til (Proactima, 2016) samt de oppramsede lovverk. Lovverkene som er satt opp i venstre kolonne er lovverk som er antatt relevante av forfatter. ISO 19650-5 er en internasjonal standard som må tilpasses lover og regler for det aktuelle landet.

Tabell 20: Antatte relevante lovverk for ISO 19650-5 og HMS-lovverk

ISO 19650-5	HMS
Rammeverk, lover og forskrifter	Rammeverk, lover og forskrifter
• Datatilsynet • Lov om nasjonal sikkerhet (sikkerhetsloven) • Personopplysningsloven	• Arbeidstilsynet • Arbeidsmiljøloven • Byggherreforskriften • Internkontrollforskriften

4.3.2 Kultur

Det er en rekke multifaktorelle årsaker til hvorfor kulturen i en organisasjon er som den er. ((Proactima, 2016), s. 25) beskriver 10 faktorer for å påvirke HMS-kulturen i en positiv retning. Det er valgt å presentere disse ettersom det er med på å synliggjøre årsaker, likhetstrekk og overførbarhet til en digital sikkerhetskultur.

Mange av punktene kan trekkes tilbake til strukturen for HMS-aktivitetene presentert i kap. 4.3.1. Ut ifra punktene kan blant annet kunnskap, rutiner, læring sammenlignes med svarene fra intervjuobjektene i kapittel 4.1. Tabell 21 viser sammenhengen mellom planen for etablering og bygging av HMS-kultur som ifølge kapittel 4.2 blir ansett som god, og manglene identifisert gjennom intervjuresultatene i kapittel 4.1.

Tabell 21: 10 punkter for bygging av HMS-kultur, sammenlignet med intervjusvarene

	Plan for etablering og bygging av HMS-kultur	**Intervjuresultat kapittel 4.1**
1.	Kunnskap og praktisk ferdighet i HMS arbeid	Mangel på kunnskap om digitale trusler for byggebransjen (Se kapittel 4.1.1)
2.	Felles mål om sikker arbeidsplass	Liten bevissthet rundt risiko (Se kapittel 4.1.1)
3.	Anerkjenne dilemmaet mellom HMS og effektivitet/fremdrift	Produsenten uttrykker at arbeidsmåten i strengt hemmelige prosjekter i dag kan være slitsom, og fører ofte til at selv enkle ting blir krevende. (Se kapittel 4.1.2)
4.	Forvente etterlevelse av prosedyrer, regler og rutiner	I liten grad prosedyrer og rutiner (Se kapittel 4.1.2)
5.	Insentiver/belønninger for sikkert arbeid	Ikke omtalt
6.	Kontinuerlig forbedring og læring	Overlates til ekstern/intern IT-avdeling (Se kapittel 4.1.2)
7.	Et arbeidsmiljø som er årvåkent for risiko	Lav bevissthet (Se kapittel 4.1.1)
8.	Feiltolerante organisasjoner	«Ikke krise om noen får tak i våre tegninger» (Se kapittel 4.1.2)
9.	Synlig lederengasjement i HMS-arbeidet	Lite bevissthet. Flere intervjuobjekter i lederroller (Se kapittel. 4.1.1 og 2.3.2)
10.	Arenaer for informasjonsdeling og kommunikasjon	E-post og skytjenester blir oftest brukt (Se kapittel 4.1.2)

4.3.3 Kunnskap

For å kunne håndtere risikoer innen HMS og digital sikkerhet er ansatte avhengig av å vite hva som skal ses etter, og ha kunnskap om hvordan dette kan håndteres. Intervjuresultatene i kapittel 4.1.1 trakk frem kunnskapsmangel på området som en sentral årsak til hvorfor det ikke var fokus på dette området. Samtidig fortalte 6 av 7 at de hadde jevnlige kurs i generell informasjonssikkerhet og digital sikkerhet.

> *«HMS-faglig kompetanse vil aldri være nok i seg selv, det må alltid settes i sammenheng med fagkunnskap ift. Bygg og anlegg.» ((Proactima, 2016), s. 10)*

Ifølge ((Proactima, 2016), s. 9) dreier HMS-faglig kompetanse seg om forståelse for alt fra praktiske HMS-tiltak på byggeplassen, men også HMS-ledelse og risikostyring. Det å ha et helhetsperspektiv på HMS som er i henhold til lovgivningen er viktig. Samtidig vil ikke HMS kompetanse generelt være nok for å skape god nok effekt. Det vil ikke bli gjort gode nok risikovurderinger innen HMS, dersom fagkunnskapen mangler.

5 Diskusjon

5.1 Den digitale sikkerhetskulturen i byggenæringen

Resultatene presentert i kapittel 4.1 antyder at aktørene i Norsk byggenæring opplever den digitale sikkerhetskulturen som dårlig. Hvorfor det er slik? Aktørene selv mener årsakene til dette blant annet skyldes lite kunnskap og varierende fokus på området. Aktørene beskriver i intervjuene hvordan noen prosjekter har et stort fokus, mens de fleste andre prosjekter har lite eller ingen fokus. Finnes det andre forklaringer på hvorfor sikkerhetskulturen er slik den er i dag?

5.1.1 Hva kan årsakene til dagens sikkerhetskultur skyldes?

«Digital divide»

7 av 7 aktører påpekte manglende kunnskap som en sentral faktor for hvordan dagens digitale sikkerhetskultur i byggenæringen er. Entreprenør 1 forteller at deres fokus i stor grad dreier seg om å øke delingskulturen i byggebransjen, noe som står i stor kontrast til hvordan prosjekter med høy sikkerhet omtales. 3 av 7 aktører beskrev også hvordan sikkerhetsfokuset er preget av hvilke krav byggherren stiller. Som følge av dette kan fokuset i dag bli enten veldig stort, eller veldig lite. Dette kan blant annet skyldes varierende kunnskap hos byggherrer, men også aldersforskjeller.

((al, 2021), s. 245) omtaler et fenomen kalt «digital divide» som viser til ujevnheter eller kontraster som følge av digital teknologi. Dette blir blant annet eksemplifisert gjennom at unge og eldre behersker digital teknologi forskjellig, noe som kan stemme bra med intervjuobjektenes beskrivelser av unge og eldre i byggebransjen. I tillegg er ikke dette et fenomen begrenset til byggenæringen. Kontrastene mellom unge og eldre er allerede stort når det kommer til teknologi. De fleste yngre mennesker i dag har på et tidspunkt hjulpet sine foreldre eller besteforeldre med et teknologisk problem, for eksempel telefon, tv eller data. Spørsmålet er derfor hvordan «digital divide» eventuelt har påvirket byggenæringen?

I ((al, 2021), kap. 5.6, s. 174) «*kultur og sikkerhet i organisasjoner*» omtales kultur som et sentralt begrep når det gjelder organisasjoners sårbarhet og problemer. Det blir fremhevet hvordan delte antagelser og normer styrer den kollektive oppmerksomheten og atferd tilknyttet risiko og sikkerhet i organisasjoner. Som ung og fersk i en byggebedrift har en gjerne en tendens til å forholde seg til hva de eldre og mer erfarne ansatte gjør og sier. Deres holdninger og synspunkt kan ofte være innarbeidet over mange år. Likevel har verden forandret seg med årene, spesielt innen teknologi. Spørsmålet er om den eldre generasjons holdninger har bidratt til å farge kulturen som utspiller seg hos ulike organisasjoner i byggenæringen?

Vel, den eldre generasjonen vil sannsynligvis ha såpass innflytelse på bedriften at deres holdninger kan gjenspeiles i enkelte tilfeller. Dette kan blant annet føre til at utviklingen og utprøving av nye metoder går tregere enn ellers, men også skape en negativ holdning

til forandring. På den andre siden vil den yngre generasjonen likevel oppdage og bruke teknologi utenom arbeid, og på denne måten bli bedre til å benytte digitale verktøy og se andre løsninger enn det som ble etablert da forrige generasjon startet. Dette kan slikt sett øke skillet mellom unge og eldre i bruk av teknologi, men også føre til at yngre begrenses av den eldre generasjons erfaringer.

Dersom den eldre generasjonen i utgangspunktet har vanskeligheter med å tilegne seg ferdigheter og kunnskap innen digital teknologi, vil antageligvis sikkerhets- og konsekvenstenkningen være enda mer krevende. Er dette en del av forklaringen på hvorfor den digitale sikkerhetskulturen og holdningene til dette er slik det er?

Er generell sikkerhetsopplæring nok?

Basert på intervjuresultatet og de ulike aktørenes perspektiver, er usikkerhet noe som preger definisjonene av sensitiv bygningsinformasjon og potensielle konsekvenser rundt dette per dags dato. (NSM, 2020) viser til en rekke generelle sikkerhetsråd som anbefales for virksomheter uavhengig av bransjetilknytning. Spørsmålet er likevel om generell sikkerhetsopplæring alene er tilstrekkelig for byggenæringen?

6 av 7 intervjuobjekter forteller at deres virksomhet jevnlig gjennomfører digitale sikkerhetskurs, men likevel er intervjuobjektene usikre på hva som er potensielle konsekvenser med BIM. Intervjuobjektenes beskrivelser av lav kunnskap om digital sikkerhet, tross generell digital sikkerhetsopplæring, er derfor tydelige tegn på at opplæringen må bli mer tilpasset aktørenes arbeidssituasjoner. Dette omtales som effektivt i HMS-sammenheng, noe som gir grunn til å tro at det også vil være effektivt innen digital sikkerhet. En mer spesifikk opplæring vil kanskje skape mer interesse og forståelse rundt potensielle farer og konsekvenser som er relevant for de ansattes daglige arbeid. Samtidig vil dette kreve mer ressurser å gjennomføre, noe som fører til en større økonomisk kostnad. Basert på inntrykket av dagens byggenæring, er ikke dette en kostnad aktørene frivillig kommer til å ta.

Blant annet arkitekten forteller at de har egne IT-selskaper som i stor grad har ansvaret for den digitale sikkerheten til virksomheten. Flere gir også uttrykk for at disse hovedsakelig skal sørge for den digitale sikkerheten til bedriften. Samtidig kan en spørre seg; hva vet et IT-selskap/avdeling om hva som er sensitiv informasjon i et byggeprosjekt? IT-selskaper er gode på deres fagfelt som innebærer datasikkerhet, og vil i stor grad sørge for den tekniske systemsikkerheten. Likevel hjelper det lite med god teknisk sikkerhet, dersom ikke menneskene bak forstår hva de beskytter. Så, er generell sikkerhetsopplæring nok?

For mye fokus på tekniske løsninger?

(Moumita Das, 2020) konkluderer med at tekniske systemer for å ivareta sikkerheten med BIM allerede eksisterer, men at disse ikke er tilpasset byggenæringen. (Nikdokht Ghadimina, 2021) gjorde en studie med mål om å kartlegge konsekvensene av et cybersikkerhetsbrudd for ulike arbeidsområder innen fasilitetsstyring med BIM. Deres funn peker også mot en overavhengighet av teknologi innen BIM fasilitetsstyring i tillegg til manglende cybersikkerhetsbevissthet blant ansatte. De mener fokuset bør skiftes til menneske- og prosessaspektene ved cybersikkerhet innen BIM. Allerede i 2013 konkluderer (Abdul-Majeed Mahamadu, 2013) med at det var mangel på forståelse rundt

konsekvensene ved datatap i forbindelse med BIM samarbeid over skyløsninger. Likevel har utviklingen av skytjenester og webhoteller for BIM fortsatt, og aktørene i denne studien forteller om både positive og negative sider ved dette. Produsenten mener skytjenestene er for lite kompatible med modelleringsprogrammene, noe som fører til mer manuelt arbeid. De uttrykker det som et ork å måtte logge på en rekke forskjellige web-hoteller for å starte dagen. Rådgiveren beskriver skytjenestene de benytter på en mer positiv måte, og forteller om egne kommunikasjonsløsninger innad i skytjenestene. Likevel var også rådgiveren skeptisk til skytjenestenes serverlokasjoner, ved at arbeid ligger på en server i utlandet. Den tekniske sikkerheten er likevel av liten betydning dersom menneskene ikke har kunnskap om risiko og riktig bruk av teknologien. Det er generelt mange tegn som peker i retning av et høyere fokus på de positive sidene ved teknologien sammenlignet med de negative.

((al, 2021), s. 245) beskriver hvordan dagens samfunn har en tendens til å fremheve teknologiens positive sider i større grad enn konsekvensene. Dette kan også relateres til byggebransjens måte å omtale teknologi, for eksempel ved hvordan ulike bedrifter reklamerer for deres bruk av ny teknologi. Flere aktører beskriver likevel BIM-modellene som lite utviklet med tanke på innhold av informasjon. Dette gjør at mange har problemer med å forstå hvordan modellene kan bli misbrukt. Har de rett i dette? Så langt finnes det lite informasjon som underbygger tidligere uønskede hendelser som følge BIM deling. En årsak til dette kan være at det ikke er nok informasjon å hente fra modellene slik aktørene beskriver, men også at trusselaktørene har lite kunnskap. Samtidig er det grunn til å tro at BIM utviklingen vil fortsette i tiden fremover, noe som gjør dette til en større fremtidig problemstilling.

((al, 2021), s. 55) omtaler en rekke generelle aspekter og usikkerheter i forhold til digitalisering og risiko. Ifølge ((al, 2021), s. 245) er det i det gjensidige avhengighetsforholdet mellom mennesker og maskiner at det kan oppstå nye risikoer og sårbarheter i samfunnssikkerheten. Slik byggenæringen, og verden ellers utvikler seg, er en i ferd med å skape et stadig større gjensidig avhengighetsforhold til teknologien. Det er svært få arbeidsplasser i dag som ikke påvirkes av digitale angrep, men hvor mange tenker egentlig på det?

Kan hemmelighold virke mot sin hensikt?

Enkelte prosjekter (for eksempel regjeringskvartalet) preges likevel av stort hemmelighold til sammenligning med andre prosjekter, noe flere intervjuobjekter forteller. Produsenten beskriver at de i slike prosjekter i praksis ikke får gjort feil som følge av menneskelig uvørenhet ettersom deres handlingsrom på mange måter er «låst». Likevel er produsenten, i likhet med flere andre aktører at de er usikre på hva som er sensitiv bygningsinformasjon. Selv forteller de at det ikke er noen «krise» dersom noen får tak i deres tegninger. ((Giuseppe Miceli Junior, 2020)) beskriver i sin konklusjon hvordan sikkerhetsproblemer med BIM-modeller generelt sett er svært ukjente for designere. Dette kan tyde på at det er lite kunnskap om konsekvensene ved digitale angrep. Likevel kan en spørre seg om et slikt hemmelighold virker mot sin hensikt? Ved at kunnskapen om sikkerhetsrisikoer blir holdt tilbake av aktører som i dag har høyt fokus og bevissthet rundt dette, begrenses også muligheten for læring. Er dette ønskelig?

Menneskelige feil vil i mindre grad få mulighet til å lekke ut gjennom et slikt system, da de i praksis er frakoblet alle kommunikasjonsmidler. Det er en vanlig tankegang å skjule informasjonen som er sensitiv. Dette kan også være en bevisst strategi fra disse byggherrenes side. På en annen side vil de involverte aktørene ikke være like klar over hva som er sensitiv informasjon og ikke ved senere prosjekter.

Spørsmålet er om sikkerheten totalt sett kan bli bedre ved å dele mer informasjon med involverte aktører? Kanskje de involverte på denne måten ville tatt til seg mer kunnskap om risikoer og potensielle konsekvenser? Selv om byggherren opererer med en veldig lukket sikkerhetsløsning, kan en trussel aktør likevel skaffe seg en del informasjon om et prosjekt ved å innhente informasjon fra underleverandørene, hvis de til daglig har et dårlig sikkerhetsfokus. Det er jo naturlig å tenke at arbeidsmetodene er relativt like uavhengig av prosjekt.

5.1.2 Perspektiver, roller og verdi

((al, 2021), s. 96) omtaler hvordan det kan være store forskjeller på enkeltindividets oppfattelse av risiko. Dette kan være påvirket av enkeltpersonenes kognitive egenskaper, erfaringer, individuelle verdier og virkelighetsoppfatning. Dette kalles risikopersepsjon og er definert i ((al, 2021), s. 108). Kan dette bidra til å forklare hvorfor den digitale sikkerhetskulturen er som den er i dag?

Både produsent og entreprenør 1 uttrykte det å arbeide i sikkerhetsgraderte prosjekter som mer krevende som følge av alt ekstraarbeidet dette medførte. De beskrev det som vanskelig å gjøre jobben de var satt til som følge av alle sikkerhetsrestriksjonene. Entreprenør 1 gav imidlertid uttrykk for at det var negativt de gangene de ikke fikk tillatelse til å dele informasjon om et prosjekt offentlig. Dette kan samtidig være intervjuobjektets egen oppfattelse, og behøver ikke å gjelde de andre ansatte hos entreprenør 1.

På en annen side kan også intervjuobjektene være påvirket av rollene de har som entreprenør, arkitekt, byggherre, etc. og eventuelle sub-kulturer skapt internt i virksomhetene. Intervjuobjektet som representerte byggherre 2 har imidlertid påpekt at vedkommende har majoriteten av sin arbeidserfaring fra entreprenørbransjen. På hvilken måte kan dette ha påvirket svarene?

Avhengig av om intervjuobjektet hadde rolle som entreprenør, byggherre eller prosjekterende, er svarene noe ulike. Selv om mange aktører ser ut til å ha en viss grad av sikkerhetstenkning, er det oftest sett i et konkurranseperspektiv for deres egen situasjon og egen bedrift. Det er imidlertid lite som peker i retning av at det gjøres andre refleksjoner rundt eventuelle konsekvenser i et større samfunnsmessig perspektiv. Aktørene prioriterer gjerne utfordringer som hovedsakelig rammer deres egen bedrift direkte. Men hvilke utfordringer kan dette være? Hvordan vektlegger aktørene verdifull informasjon for deres virksomhet? De ulike rollenes syn på verdi vil sannsynligvis påvirke fokuset deres rundt sikkerhet.

Byggherrens verdi

For byggherren som eier vil det være naturlig at bygget som objekt og behovet det skal dekke, utgjør selve verdien. Sett ut ifra måten byggherrene omtaler sikkerhet og verdi, kan det tyde på at de fokuserer mer på byggets verdiskapning i et større perspektiv sammenlignet med entreprenører og prosjekterings bedrifter. Byggherren er samtidig nødt til å foreta mange vurderinger og prioriteringer når et nytt bygg skal settes opp, både i forhold til verdiskapning, løsninger, kostnad- og tidsrammer. Ikke minst bør byggherrer ha en formening om behovet for det som bygges ut ifra et lengre tidsperspektiv. Dette kan gjøre at helhetsvurderinger og virkninger over tid allerede er et trekk som kjennetegner en byggherre i større grad enn entreprenører og prosjekterende bedrifter.

For byggherrer som er ansvarlig for kritisk infrastruktur vil i tillegg angrep (både digitale og fysiske) derfor kunne skape store konsekvenser for samfunnet. Dette gjør at byggherrer ofte kan ha et større fokus på hvilke konsekvenser (både positive og negative) prosjektet utgjør for samfunnet, sammenlignet med aktørene som utfører prosjektering og bygging. Byggherre 1 som ble intervjuet i denne studien, viste et stort engasjement til sikkerhetsaspektet og hvilken rolle de hadde i samfunnet. Byggherre 2, som ikke var ansvarlig for kritisk infrastruktur, hadde ikke samme engasjement eller kunnskap om sikkerhetstematikken (security). Den utarbeidede figur 9 illustrerer det forfatter tolker som byggherres største verdi i et byggeprosjekt.

Figur 9: Tolkning av byggherres verdi

Prosjekterendes verdi

Entreprenør 1 omtalte at de i flere tilfeller gjerne ønsket å få tak i originalfiler til et prosjekt, og oppfattet ofte arkitektene som spesielt tilbakeholdene. For prosjekterings-siden (i dette tilfellet rådgiver, arkitekt og produsent) svarte både rådgiver og arkitekt hvordan de var opptatt av å ikke dele originalfiler, ettersom de ikke ønsket å dele verdifull informasjon om hvordan de laget ulike løsninger, helt gratis.

Ut ifra intervjubeskrivelsene kan en forstå hvordan markedsverdien og konkurransefortrinnet til de prosjekterende i stor grad ligger i kunnskapen og løsningene de besitter. Dette gjør det derfor naturlig for dem å implementere tiltak for å beskytte sine løsninger i større grad enn entreprenører. Likevel forteller de at disse tiltakene ikke er av hensyn til sikkerhetsperspektivet, men for å beholde sitt eget konkurransefortrinn i markedet. Generelt sett ser man hvordan prosjekteringsbedrifter ofte sitter på mer teoretisk kunnskap, og det er i praksis denne kunnskapen de selger. Den utarbeidede figur 10 illustrerer undertegnedes fortolkning av prosjekterendes største verdi.

Figur 10: Tolkning av prosjekterendes verdi

Entreprenørens verdi

For entreprenøren som utførende i et byggeprosjekt, vil verdien i større grad ligge i tids- og kostnadsperspektivet, spesielt i totalentrepriser. For at entreprenører skal tjene penger er de nødt til å levere det utførende arbeidet innen en gitt tidsramme samtidig som de klarer å holde seg innenfor et gitt budsjett, både for byggherren sin del, men også for å skape egen fortjeneste. Dette betyr at hendelser som gjør at produksjonen og fremdriften i prosjektet stanser, kan føre til store konsekvenser for entreprenøren.

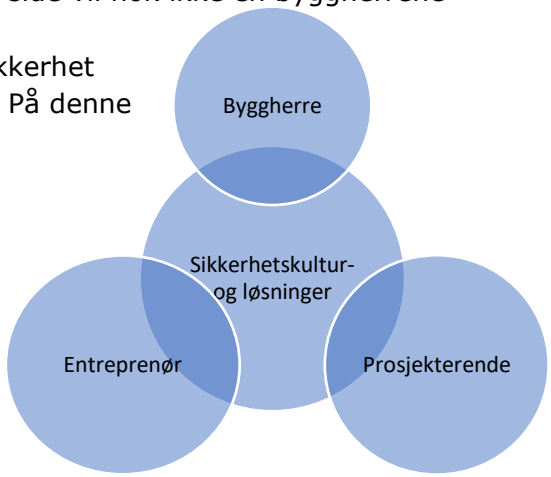
Selv om konsekvensene i stor grad vil være økonomiske, kan også forsinkelser være ugunstig for bedriftens omdømme dersom prosjektet ikke fullføres innen tidsfristen. I kapittel 4.1 beskrev entreprenør 1 hvordan de jobbet for å ha en større åpenhet og bedre delingskultur. Sett fra entreprenør-perspektivet i lys av deres verdi i markedet (tid og penger) er dette gunstig, ettersom dette kan bidra til å øke fremdriften, som igjen kan skape større fortjeneste. Slikt sett vil generelt digitale verktøy som bidrar til økt fremdrift og/eller lavere kostnader, være svært interessante for entreprenører. Tanken oppsummeres i figur 11 og representerer det forfatter tolker som entreprenørenes største verdi.

Figur 11: Tolkning av entreprenørens verdi

Er det for lite samarbeid mellom aktører i lys av digital sikkerhet?

Med utgangspunkt i svarene og fortolkningen av de ulike rollenes interesser, kan konkurransefortrinn og egeninteresse påvirke aktørenes sikkerhetstankegang og syn på sensitiv informasjon. Kunne sikkerheten totalt sett blitt enda bedre dersom det var et tettere samarbeid mellom aktørene?

Foruten byggherre 1 er det få som trekker frem potensielle konsekvenser for prosjektet eller samfunnet, og knytter det tilbake til sitt eget arbeid. Men er det dette viktigst for byggherren? De utførende aktørene vil jo ikke påvirkes direkte av at informasjon om et bygg blir tilgjengelig for andre i etterkant? På en annen side vil nok ikke en byggherrene tenke på en entreprenørs økonomiske situasjon heller.
Spørsmålet er imidlertid om det kunne blitt en bedre sikkerhet dersom aktørene delte sine perspektiver og synspunkt? På denne måten kan kanskje alle få et grundigere helhetsbilde?



Figur 12: Samarbeid om felles sikkerhetskultur?

5.2 Erfaringer fra HMS i lys av digital sikkerhet

Intervjuobjektene forteller at holdningene til HMS jevnt over er mye bedre enn hva det var for bare noen år siden. 5 av 7 omtaler dagens HMS kultur som «svært bra». Likevel forteller enkelte at det fremdeles er en del negativitet til HMS blant enkelte. Aktørene i denne studien mener dette påvirkes av en rekke faktorer, hvor dette delkapittelet diskuterer tre av disse faktorene i lys av digital sikkerhet; lovverk, systemer/rutiner og økonomi. Kan disse utfordringene også oppstå innen digital sikkerhet?

5.2.1 Faktorer aktørene mener har påvirket HMS-kulturen

Lovverk og krav

4 av 7 aktører trekker frem hvordan lovverk, forskrifter og krav ligger til grunn for dagens tiltak og utvikling innen HMS. De forteller at dette har presset bransjen til å gjøre flere tiltak rundt HMS. Byggherreforskriften (Lovdata, 2010) viser blant annet til byggherrens plikter når det kommer til sikkerhet, helse og arbeidsmiljø (SHA). Byggherreforskriften er veldig konkret utformet for bygg- og anleggsvirksomhet, sammenlignet med for eksempel sikkerhetsloven. Lite tyder på at det finnes tilsvarende forskrifter innen digital sikkerhet for byggebransjen. Burde dette vært en del av byggherreforskriften?

Å vurdere sensitiv informasjon i en BIM kan være svært vanskelig ettersom det er så komplekst og sammensatt. I tillegg vil det være store variasjoner avhengig av type prosjekt og virksomhet. Dette blir ikke enklere når aktørene forteller at dette enda ikke er sett på som en sikkerhetsutfordring. ((Lovdata, 2019), §5-1) definerer skjermingsverdig informasjon som følger;

> *«Informasjon er skjermingsverdig dersom det kan skade nasjonale sikkerhetsinteresser at informasjonen blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig.» ((Lovdata, 2019), §5-1)*

Denne loven kan tolkes til å gjelde bygningsinformasjonsmodeller (BIM), men dette forutsetter at det faktisk gjøres en vurdering. En god vurdering forutsetter igjen kunnskap om BIM som en sikkerhetsrisiko, noe flere aktører trekker frem som en mangel i dag. Kan dette forklare de store variasjonene mellom sikkerhetsgraderte prosjekter og «ordinære» prosjekter?

På en annen side kan en spørre seg hvor grensen går på hva som er skjermingsverdig, eller sensitiv informasjon? (NSM, 2022a) beskriver hvordan trusselaktører i større grad angriper leverandørkjeder. I et byggeprosjekt hvor for eksempel en dør, rørsystem, strøm etc. isolert sett ikke kan klassifiseres som skjermingsverdig, kan det likevel bli skjermingsverdig når det settes i sammenheng med resten. Dette gjør det også vanskelig å definere en tydelig lov. For dagens lov dekker jo alt dersom den tolkes riktig? Dette hjelper likevel lite dersom kunnskapen og bevisstheten til å gjennomføre en god nok vurdering ikke er tilstede. Hva bør derfor gjøres med dette i lys av lovverk og krav? Ut ifra aktørenes erfaringer har byggherreforskriften fungert på HMS-siden, burde problemstillingene innen BIM og digital sikkerhet implementeres her?

Sikkerhetsloven krever derfor gode vurderinger for å dekke alle trusler slik den er utformet i dag. For å gjøre en god vurdering av lovverket er en avhengig av å ha kunnskap om sikkerhetstruslene tilknyttet BIM og digitalisering i byggenæringen. Uten dette, kan lovverket tolkes svært forskjellig. Dette kan føre til at det blir gjort gode tiltak, men også føre til at mange risikofaktorer uteblir. Aktørene har beskrevet HMS lovverket som en viktig faktor som har «presset» bransjen til å gjøre tiltak. Uten tydelige sikkerhetskrav fra byggherren, er det lite sannsynlig at dette gjøres frivillig av aktørene.

Figur 13 illustrerer fortolkningen av sikkerhetsloven i lys av BIM-sikkerhet for dagens byggenæring. Fortolkningen er basert på aktørenes beskrivelser av HMS og digital sikkerhet. Dette er en generell betraktning, og det vil derfor være lokale forskjeller.

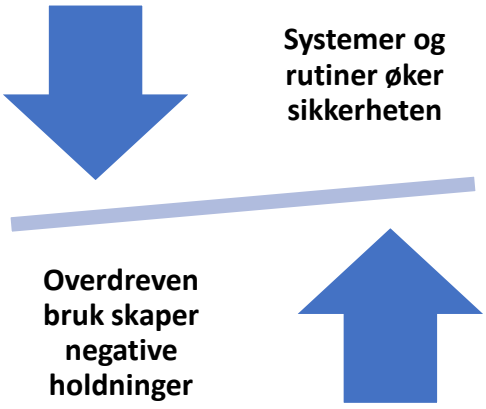
Figur 13: Tolkning av sikkerhetsloven i lys av BIM for dagens byggenæring (egenprodusert)

Systemer og rutiner

6 av 7 intervjuobjekter fremhever systemer og rutiner i HMS arbeid som positivt. Den teknologiske utviklingen gjør også systemene bedre og mer effektive for aktørene. Slikt sett kan disse systemene og rutinene bidra til å holde fokuset og bevisstheten på HMS oppe over tid. På en annen side kan også sikkerhetsrutiner og systemer bli overdrevne i enkelte tilfeller.

På HMS siden i dagens byggenæring beskrives «overdrevne» sikkerhetsrutiner som en negativ konsekvens av systemer og rutiner. Entreprenør 2 forteller at flere av HMS-tiltakene kan være vanskelige for ansatte å se betydningen av, spesielt blant håndverkere. Det er forståelig at det kan være frustrerende for en håndverker å sette opp en lift ettersom det ikke er tillatt å benytte en 2-trinns gardintrapp, da dette medfører en god del ekstraarbeid. I slike tilfeller kan en undres på om sikkerhetstiltakene har gått for langt? På en annen side kan også frustrasjonen komme som et resultat av dårlig eller mangelfull informasjon. Kanskje frustrasjonen er mindre hos aktører med bedre dialog mellom ledere og arbeidere? Uansett kan strenge sikkerhetstiltak og/eller dårlig kommunikasjon også lede til negative holdninger rundt HMS. Entreprenør 2 uttrykte: *«det er forskjell på å barbere seg, og å skjære av seg hodet».* Når det er sagt, beskriver likevel 5 av 7 intervjuobjekter at HMS-kulturen generelt sett er bra! Betyr det at tiltakene har fungert bra totalt sett? Er det dette som må til innen digital sikkerhet også?

Allerede i dag uttrykker aktørene hvordan det kan være frustrerende å logge seg på en rekke systemer bare for å starte arbeidet. Ved overdrevne og tilsynelatende «meningsløse» sikkerhetstiltak på dette området, kan nok tilsvarende holdninger oppstå her også. På en annen side vil en vurderingsprosess øke sikkerheten ved at det blir reflektert rundt potensielle konsekvenser, samtidig som vurderingen tillater personene å veie positive og negative sider mot hverandre og på den måten unngå overdrevne tiltak. Figur 14 illustrerer poenget med å ha en balansegang rundt systemer og rutiner.



Figur 14: Balansegangen mellom få/mange systemer og rutiner (Egenprodusert)

Økonomisk perspektiv

Sikkerhetstiltak og prosedyrer gir i seg selv lite økonomisk gevinst for bedrifter, enten det er digital sikkerhet eller HMS. Når det ikke stilles spesifikke krav til sikkerhet fra en byggherre, blir det sjeldent prioritert hos de utførende. Slik beskriver blant annet arkitekten at det ofte er hos mindre bedrifter som jobber på prosjekter hvor byggherren ikke stiller like strenge krav.

Flere intervjuobjekter forteller at større byggeprosjekter hvor byggherrenes krav til sikkerhet er tydelige, skapes det et konkurransefortrinn for virksomheter som kan vise til gode HMS systemer. Både byggherre 2 og entreprenør 2 forteller at bedrifter som i dag ikke kan dokumentere og vise til et godt HMS system (spesielt i større prosjekter), ikke engang er kandidater til å få jobben. Dette kan slikt sett skape økonomiske forskjeller hos de med gode sikkerhetssystemer, og de som har valgt å nedprioritere dette. Kan dette også bli tilfelle for digital sikkerhet i fremtiden?

En av utfordringene med digital sikkerhet og BIM er at dette i praksis er et lite problem i dag. Likevel kan dette bli et stort problem i fremtiden når BIM-modeller blir mer detaljerte. Med den teknologiske utviklingen som skjer i verden, kan også dette gå raskere enn man er klar over (se kapittel 6.3 – videre arbeid). Dette betyr at sikkerhetstiltak må implementeres før eller siden uansett. Økonomisk kan det være lønnsomt å starte utviklingen av slike systemer allerede nå, da dette kan være en tidkrevende prosess. HMS-erfaringen viser hvordan lovverket kan presse frem en endring innen sikkerhet. Når dette skjer, kan det være lønnsomt å ha på plass et slikt system allerede fremfor å starte utviklingen da. Kanskje dette kan bli en motivasjonsfaktor for å skape endring relativt raskt i byggenæringen? På en annen side, er det knyttet stor usikkerhet til denne problemstillingen. Når kommer dette til å bli et problem? Blir det et problem? Vil problemet endre seg? Disse usikkerhetene gjør denne utfordringen vanskelig å forholde seg til.

5.3 Sammenligning av HMS aktiviteter og ISO 19650-5

Ifølge (Giuseppe Miceli Junior, 2020) mangler det generelt kunnskap om BIM sikkerhet hos designere i dag. Denne studiens funn bekrefter at dette også gjelder det norske bygg- og anleggsmarkedet. Flere av intervjuobjektene mener dette er en viktig årsak til hvorfor det er lite fokus og få tiltak på dette området. I tillegg har tilpassede kurs og opplæring vist seg å ha god effekt på HMS-siden, noe som totalt sett gir grunnlag for å tro at dette også vil fungere for å øke den digitale sikkerheten.

(Moumita Das, 2020) har gjort en studie på teknologien BIM i et sikkerhetsperspektiv og konkluderte med at teknologien som trengs for å gjøre BIM sikrere allerede eksisterer, men ikke er tilpasset byggebransjen. Dette gjør imidlertid den menneskelige faktoren ekstra viktig. ISO 19650-5 foreslår en prosess for vurdering av sensitivitet i byggeprosjekter, både internt i ulike bedrifter, men også i et helhetsperspektiv. Fra HMS-siden ser en hvordan en rekke systemer og rutiner har blitt etablert på en relativt lik måte som ISO 19650-5 foreslår.

5.3.1 Likheter og forskjeller

Forskjellig betydning og hensikt

Avhengig av perspektivet en velger å se HMS og digital sikkerhet fra, kan de to være svært forskjellig, men også svært like. Ved å se på BIM og HMS i praksis, er det relativt ulike fokusområder, og de som jobber med dette har sannsynligvis et ulikt syn på verden. Dette kan gjøre det vanskelig å se likhetene mellom de to fagfeltene. I tillegg skiller en gjerne mellom «Safety» som er hovedfokuset til HMS, og «security» som er hovedfokuset til ISO 19650-5. Et inntrykk en fort kan få som skiller disse perspektivene er hvordan «safety» ofte blir delt og snakket opp på en helt annen måte enn «security» som ofte preges mer av hemmelighold. Dette kan eksemplifiseres blant annet gjennom hvordan HMS i byggeprosjekter angår samtlige, mens digitale trusler og utfordringer overlates til en IT-avdeling eller et eksternt IT-selskap slik blant annet arkitekten fortalte i intervjuene. HMS-siden reklamerer stort med ulike systemer og programmer som bidrar til å gjøre sikkerheten bedre i byggeprosjekter, hører man slikt om digital sikkerhet?

Prinsipielt svært like

Dersom en velger å fjerne betydningene «security» og «safety», og kun ser på hvordan HMS og ISO 19650-5 er bygget opp, ser en hvordan prinsippene som ligger til grunn er svært like. I tillegg til å være svært like hverandre, er de også lik prinsippene til IRGC-modellen (IRGC, 2017) som er et kjent og veletablert rammeverk for identifisering og håndtering av risiko. Hva betyr dette? Vel, tross en rekke ulikheter mellom HMS og ISO 19650-5 er det kanskje ikke nødvendig å jobbe så ulikt? Ettersom HMS prosedyrene allerede er implementert i byggenæringen, er det nærliggende å anta at tiltak fra ISO 19650-5 kunne utvidet de allerede eksisterende HMS-rutinene. Kanskje betydningen av sikkerhet i HMS også kunne vært utvidet til å gjelde «security»? En slik implementering ville samtidig medført en rekke usikkerheter og dilemmaer. Et utvalg av disse vil diskuteres i kapittel 5.3.2.

5.3.2 Usikkerheter og dilemmaer

BIM bruk i byggebransjen byr på flere usikkerheter, og selv om standarder som ISO 19650-5 implementeres og sikkerhetsfokuset blir bedre, vil det likevel være usikkerhetsmomenter som ikke kan kontrolleres.

Digitalisering og standardisering

Standardisering gir ifølge ((al, 2021), s. 256) en rekke fordeler i form av et felles språk, metoder og effektivitet. Samtidig reduserer digitale standarder mulighetsrommet for alternative perspektiver og løsninger. Det er grunn til å tro at ISO 19650-5 vil bidra til å forbedre det digitale sikkerhetsfokuset sett ut ifra dagens perspektiv. Likevel vil det alltid ligge en usikkerhet i fremtiden. Utviklingen av digitale teknologier har hatt en betydelig økning de siste årene, og man vet ikke hvilke muligheter som ligger i teknologien 5-10 år frem i tid. De siste par årenes erfaringer minner i tillegg på hvor dynamisk verdensbildet er. Ukraina-krigen og covid-19 pandemien viser hvor raskt verdenssituasjonen og trusselbildet kan endres på svært kort tid. Dette er usikkerheter som kan gjøre standardiserte løsninger til en begrensning på utfordringer vi i dag ikke klarer å forutse. Det er nemlig ingen som vet sikkert hvilken løsning eller hvilke teknologier som vil være aktuelle for fremtiden.

På en annen side er ISO 19650-5 utformet svært åpent. Dette gir blant annet rom for vurderinger av enkelttilfeller, noe som i en usikker fremtid gir et godt utgangspunkt. Det er kanskje det verden trenger i første omgang?

Collingridges dilemma

Når en snakker om digitalisering og sikkerhet vil det dukke opp flere dilemmaer. I en ideell verden ville det beste og mest effektive være å ikke ha sikkerhetstiltak, og ingen ville vært ute etter å utnytte digitale sårbarheter. Dessverre finnes ikke dette, og konsekvensene av å ikke ha sikkerhetstiltak kan bli større enn man kanskje er klar over. Likevel kan sikkerhetstiltak i enkelte tilfeller også skape motsatt effekt.

Et dilemma tilknyttet digitalisering og sikkerhet som omtales i boken ((al, 2021), s. 254) er «Collingridges dilemma». Dilemmaet viser til hvordan den teknologiske utviklingen vanskelig kan styres i en tidlig fase, fordi omfanget av konsekvensene ikke kommer tydelig nok frem før i en senere fase når kunnskapen og teknologien er tatt i bruk. Problemet er ofte at det da er for sent å styre eller reversere utviklingen og trekke tilbake teknologien. Basert på samfunnets utvikling og aktørenes beskrivelser av BIM er det liten tvil om at BIM har kommet for å bli. Ut ifra dette kan det tyde på at byggenæringen befinner seg i en midt-fase av «collingridges dilemma». Det er for sent å reversere bruken av BIM, samtidig er ikke BIM-teknologien ferdigutviklet, og inneholder ifølge aktørene lite informasjon i dag. Dette betyr at det fremdeles er muligheter til å påvirke bruken av BIM i fremtiden. Dette frembringer imidlertid en rekke nye problemstillinger.

Hva bør deles, hva bør begrenses?

En sentral problemstilling med BIM-sikkerhet er hvor linjen går på hva som skal/bør deles og ikke. Er det i det hele tatt noen klar grense for hva som skal deles og ikke? ISO 19650-5 er tydelig på at formålet med standarden ikke er å begrense mulighetene og fordelene som ligger i teknologien med BIM, samtidig som den tilrettelegger for et større sikkerhetsfokus. Er det mulig å få til dette i praksis?

Det finnes en rekke bygg- og anlegg som inneholder informasjon som åpenbart ikke bør være allment tilgjengelig, slik som forsvarsinstallasjoner, sykehus, flyplasser og annen kritisk infrastruktur. Samtidig kan man spørre seg; Hva er sensitivt? Er det selve bygget, eller er det virksomheten som gjør bygget og ulike bygningskomponenter sensitive? Sikkerhetsorganisasjoner generelt har ofte en tankegang som handler om å begrense og å holde tilbake informasjon, og det er fort å tenke at all informasjon bør begrenses og hemmeligstemples, kanskje fordi det rår en usikkerhet rundt nettopp hva som er sensitivt og hva informasjonen potensielt kan brukes til. Men er dette nødvendig?

Et rør er kun et rør og har liten verdi isolert sett? Det er først når røret settes i sammenheng med resten av bygget og virksomheten at det kan skape interesse for en trusselaktør. Dette er en utfordring med byggenæringens kompleksitet og avhengighet av samarbeid mellom fag. Hver for seg, vil ikke fagene nødvendigvis være spesielt interessante, men utgjøre «brikker i et puslespill». Likevel forteller flere intervjuobjekter i dag at det ikke bare deles informasjon de ulike fagene trenger, men de fleste får tilgang til et prosjekthotell hvor hele modellen tilgjengeliggjøres.

Intervjuobjektene fremhever hvordan de store fordelene med BIM i dag er muligheten til å forstå andres arbeid gjennom det visuelle. Det er for øvrig også hit BIM-utviklingen sies å ha kommet. Det finnes ifølge intervjuobjektene svært liten informasjon foruten om geometri i dagens BIM-modeller. Flere forteller også at det er geometrien som er viktig å se for fagene, ikke nødvendigvis informasjonen om hvor mye for eksempel røret tåler, eller andre kapasiteter. På den andre siden vil geometrien også kunne utgjøre en risiko i visse prosjekter. Ved bygging av tuneller, undergrunnsbaner eller lignende skulle man tro at også geometrien ville utgjøre en viktig risikofaktor? Dersom delingen av informasjon begrenses i for stor grad kan imidlertid dette skape konsekvenser for andre viktige områder ved byggeprosjekter. Noen typer informasjon må deles av hensyn på miljø/gjenbruk, kostnadskalkyler, brannsikkerhet, etc. For beregning av både kostnader og CO2-utslipp er man avhengig av å vite en god del informasjon om produktene i bygget. Samtidig er arbeidet med gjenbruk svært viktig med tanke på en større global trussel, nemlig klimakrisen.

I forhold til brannsikkerhet vil også ulike brannrådgivere være avhengig av mye informasjon rundt sammensetningen av vegger, planløsninger for rømningsveier og branndører, vinduer etc. Dette er derfor ikke nødvendigvis noen god løsning å begrense all informasjon. Noen typer informasjon må deles, og avhengig av prosjektets sensitivitet må dette vurderes for hvert prosjekt.

Sikkerhetstiltak på bekostning av digital utvikling?

Et av de store ankepunktene med sikkerhet i en HMS sammenheng, er faktumet at det påvirker effektiviteten til prosjektet. Flere av intervjuobjektene har trukket frem dette som en negativ faktor som følge av sikkerhetstiltakene. (Proactima, 2016) beskriver også at man må erkjenne at sikkerhetstiltak går ut over effektiviteten. Samme utfordring vil sannsynligvis oppstå i forbindelse med BIM og sikkerhetsaspektet. BIM er som tidligere nevnt under utvikling og har et stort potensial for effektivisering av byggeprosjekter. Ved implementering av sikkerhetstiltak, kan mye av denne utviklingen begrenses. Er dette ønskelig?

Selv om ISO 19650-5 hevder deres formål ikke er å skape et hinder for alle de positive sidene med BIM kan en derfor undres på om dette vil være mulig i praksis. Slik (Proactima, 2016) beskrev innen HMS vil fremdriften påvirkes av sikkerhetstiltak. I en HMS sammenheng vil imidlertid alternativet være en høyere ulykkesstatistikk. Ettersom BIM ikke er ferdigutviklet, og samtidig ikke rammer virksomheten på samme måte, vil alternativene være mer usikre. Fra dette perspektivet kan det være vanskelig å se nytten av sikkerhetstiltak med BIM dersom konsekvensene er så usikre at en ikke vet hvorfor det gjøres. I lys av BIM, sikkerhetstiltak og effektivitet kan en også spørre seg; er det noen poeng å benytte BIM dersom sikkerhetstiltakene utligner fordelene?

6 Oppsummering og anbefalinger

6.1 Oppsummering

Denne studien har hatt som formål å belyse den digitale sikkerhetskulturen i byggenæringen, med hovedvekt på BIM-bruk. Det ble først gjort en litteraturstudie for å undersøke hva som er gjort tidligere innen tematikken. Videre har NS-EN ISO 19650-5 (2020) *«security minded approach to information management»* vært en sentral standard å utforske i lys av den norske byggenæringens digitale sikkerhetskultur, men også i verden ellers ettersom standarden viser til prinsipper som bidrar til sikker informasjonsforvaltning med BIM.

7 aktører fra byggenæringen har blitt intervjuet, med representanter fra både byggherre, entreprenør, rådgiver, arkitekt og produsent. Hensikten med intervjuene var å besvare forskningsspørsmål 1 og 2 ved å gi en pekepinn på hvordan holdninger til digital sikkerhet oppfattes i den norske byggenæringen i dag. I tillegg skulle intervjuobjektenes erfaringer med holdninger og kulturbygging fra HMS-siden kartlegges, samt hvordan prosesser, systemer og rutiner er løst her.

For å besvare forskningsspørsmål 3 har denne studien valgt å sammenligne ISO 19650-5 med konkrete HMS-aktiviteter for å synliggjøre likheter, forskjeller og undersøke hvordan en slik standard potensielt kan brukes som et rammeverk i Norsk byggenæring.

Den digitale sikkerhetskulturen i dag

Det første forskningsspørsmålet er: *«Hvordan er den digitale sikkerhetskulturen blant aktører i bransjen i dag?».* Resultatene viser at det er lite fokus og bevissthet rundt sikkerhetsrisikoer knyttet til bygningsinformasjon og digital teknologi i byggenæringen. Flere aktører begrunner dette med at det er svært lite kunnskap på området. Likevel beskriver aktørene at enkelte prosjekter i stor grad er preget av hemmelighold, slik som byggingen av det nye regjeringskvartalet. Dette mener aktørene skaper store kontraster mellom prosjektene hvor det er høyt fokus, og lite fokus på digital sikkerhet.

6 av 7 forteller at det gjennomføres generelle digitale sikkerhetskurs internt i bedriften, for å gjøre ansatte mer årvåken, spesielt for «phishing mails» og tilsvarende e-post bedrageri. Til tross for disse sikkerhetskursene er det ulike oppfatninger og usikkerhet rundt hva som regnes som sensitiv bygningsinformasjon. Aktørene forteller at det i dag ikke gjøres noen konkrete sensitivitetsvurderinger av ansatte som kunne avdekket slike sikkerhetsrisikoer. Entreprenørene forteller imidlertid at de forholder seg til kontrakter og avtaler, noe som gjør byggherrens vurdering enda viktigere. Likevel varierer det fra byggherre til byggherre om denne typen kunnskap finnes og om krav til BIM-sikkerhet stilles. Intervjuresultatene peker i tillegg mot at aktørene tenker sikkerhet ut ifra egen situasjon, fremfor helhetsperspektivet til bygget.

Erfaringer fra HMS

Det andre forskningsspørsmålet er: *«Hva kan vi lære av HMS?»*.

Aktørene beskriver jevnt over et godt inntrykk av dagens HMS prosesser, og majoriteten mener fokuset har utviklet seg i positiv retning de siste årene. Likevel uttrykker enkelte at det fremdeles er dårlige holdninger hos noen. Intervjuobjektene tror dette blant annet skyldes kulturforskjeller som følge av utenlandsk arbeidskraft, men også interne kulturforskjeller som følge av by eller distrikt. I tillegg uttrykker entreprenør 2 at også overdrevne HMS-tiltak generelt kan føre til negative holdninger. Sett i et lengre tidsperspektiv, beskriver aktørene flere faktorer de mener har påvirket HMS-kulturen i positiv retning. De mest gjentakene faktorene er lovverk, gode systemer/rutiner og økonomiske fordeler.

4 av 7 mener lovverket har presset bransjen til å utvikle løsninger for å håndtere sikkerhet (safety) bedre. Den teknologiske utviklingen har på den måten stadig skapt mer effektive systemer som gjør rutinene for HMS mer effektive. Flere forteller også at bedrifter med gode systemer og rutiner for HMS har et konkurransefortrinn, spesielt i større prosjekter. Dette gjør derfor at HMS-systemene som i utgangspunktet var kostbare å implementere, nå har fått en positiv økonomisk fordel.

Digital sikkerhet kan derfor lære mye av HMS generelt, men spesielt i forhold til etablering og tilpassing av systemer/rutiner for byggenæringen. Blant annet skreddersydde opplæringskurs og risikovurderinger på tvers av involverte aktører.

Tiltak basert på ISO 19650-5

Det tredje forskningsspørsmålet er: *«Hvilke tiltak kan gjøres i praksis basert på ISO 19650-5?».*

Selv om «safety» og «security» har noe ulik betydning, er likevel prinsippene bak veldig like. Resultatet (i kapittel 4.3) sammenligner kapitlene til ISO 19650-5 med «typiske» HMS-aktiviteter, noe som viser svært mange likheter. Blant fellestrekkene er risikovurderingen, sikkerhetsstyringsplanen, håndtering av uønskede hendelser og avtaler.

Med utgangspunkt i at intervjuobjektene beskriver dagens HMS-prosesser som bra, er det muligheter for at også tilsvarende prinsipper kan fungere for å heve den digitale sikkerhetskulturen i byggenæringen. Basert på sammenligningene gjort i kapittel 4.3 er det derfor svært mange tiltak som kan gjøres i praksis basert på ISO 19650-5. For å fremheve noen tiltak er det i kapittel 6.2 tabell 22 illustrert 5 tiltak undertegnede anser som spesielt viktige, i tillegg til antatte effekter etter implementering. Disse er basert på sammenligningen i kapittel 4.3, men også intervjuresultatene fra kapittel 4.1 og 4.2.

Hovedproblemstilling

Denne oppgavens hovedproblemstilling er: *«På hvilken måte kan ISO 19650-5 bidra til å bedre den digitale sikkerhetskulturen?»*.

Ifølge (Giuseppe Miceli Junior, 2020) mangler det generelt kunnskap om BIM sikkerhet hos designere i dag. Denne studiens funn bekrefter at dette også gjelder det norske bygg- og anleggsmarkedet. Flere aktører mener mangel på kunnskap er en viktig årsak til hvorfor det er lite fokus og få tiltak på dette området. I tillegg har tilpassede kurs og opplæring vist seg å ha god effekt på HMS-siden, noe som totalt sett gir grunnlag for å tro at dette også vil fungere for å øke den digitale sikkerheten. ISO 19650-5 i seg selv er ikke nødvendigvis løsningen, men kan fungere som et rammeverk som legger til rette for en bedre digital sikkerhetskultur. Prinsippene om å gjennomføre en sensitivitetsvurderingsprosess, etablere en sikkerhetsstyringsplan og plan for håndtering av uønskede hendelser som ISO 19650-5 presenterer kan gjøre byggenæringen mer årvåken og bevisst på hvilke sikkerhetsrisikoer som kan oppstå, og hvordan de kan forebygges/håndteres.

For at disse anbefalingene skal bli iverksatt, bør det i likhet med HMS stilles krav til dette av byggherrene. Lovverket og kravene stilt av byggherre har ifølge intervjuobjektene hatt stor effekt på HMS-siden. I tillegg beskrives lederengasjement som en viktig faktor som har fremmet en positiv HMS kultur. Dette kan også bli et viktig punkt i arbeidet med en bedre digital sikkerhetskultur.

6.2 Anbefalinger

Intervjuresultatene i kapittel 4.1 indikerer hvordan den digitale sikkerhetskulturen i byggenæringen er i dag. Intervjuene i kapittel 4.2 viser at HMS-kulturen generelt sett har blitt mye bedre enn tidligere, og gir en pekepinn på hvilke faktorer aktørene mener har hatt positiv effekt, og hva de mener kan forbedres. Sammenligningen i kapittel 4.3 viser likhetstrekkene mellom HMS-aktiviteter og ISO 19650-5.

Denne studien viser at det er svært mange tiltak som kan gjøres innen BIM-sikkerhet. Tematikken er imidlertid ny og relativt lite utforsket, og for å begynne i en ende, ønsker denne studien å trekke frem fem viktige punkter som anbefalte fokusområder. Disse punktene er hentet fra både ISO 19650-5 og HMS-erfaringer. Tabell 22 illustrerer effektene som kan oppstå som følge av anbefalingene.

Tabell 22: Anbefalte tiltak og effekter basert på ISO 19650-5 og HMS-erfaringer

Anbefalinger og effekter				
Anbefaling	**Direkte effekt**	**Indirekte effekt**	**Avledede**	**Potensielle**
Stille krav til BIM-sikkerhet	Legger press på aktører i næringen	Skaper utvikling av systemer og rutiner	Kan lede til Konkurransefortrinn	Økt sikkerhetsfokus Negative holdninger Mindre effektivitet
Sensitivitets-vurdering i alle ledd	Ekstra arbeid Identifisering av sårbarheter.	Utvidet forståelse av risikoer	Forebyggende tiltak	Kunnskapsbygging Bedre beskyttelse Bedre avgjørelser
Etablere systemer og rutiner	Økte kostnader i startfasen. Påvirker fremdriften	Struktur Trygghet Samarbeid Mindre feil	Konkurransefortrinn Økt sikkerhetsfokus	Utvikling og forbedring Overdrevne tiltak
Tilpassede opplæringskurs	Økt interesse Ekstra arbeid	Økt bevissthet og risikoforståelse.	Økt kunnskap om sikkerhet	Økt årvåkenhet
Leder-engasjement	Større mulighet for å påvirke	Holdningene påvirker resten av hierarkiet.	Skape felles målsettinger	Bedre kultur

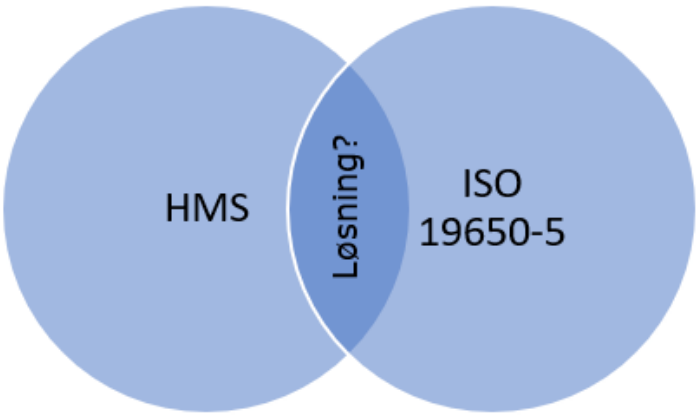
Dersom byggherrene stiller strengere krav til BIM-sikkerhet, vil det legges et press på aktører i byggenæringen til å utvikle løsninger for å få jobben, spesielt i store prosjekter hvor byggherren er attraktiv å jobbe for. Dette vil da virke som en indirekte effekt av BIM-kravene som stilles. Dette kan igjen føre til at mange aktører utvikler ulike systemer, hvor det beste systemet får jobben slik HMS-erfaringene viser. Dette blir sannsynligvis en kostnad i startfasen, slik det har vært for HMS, men kan på lengre sikt skape et konkurransefortrinn på samme måte som for HMS.

Aktørene har gjennom intervjuene presisert stor mangel på kunnskap om sikkerhetsaspekter med BIM, det til tross for datasikkerhetsopplæring. Til sammenligning har HMS-siden klart å nå ut til ansatte ved å lage svært tilpassede kurs for hver bedrift, prosjekt etc. Aktørene forteller at dette gjør det mye enklere å se relevansen, og på den måten absorberer de informasjonen lettere. Ved å implementere tilsvarende opplæringskurs innen digital sikkerhet og BIM tilpasset virksomheten, er det sannsynlig at både interessen, bevisstheten og forståelsen rundt dette øker. Det kan igjen bidra til å øke årvåkenheten som (NSM, 2022a) etterlyser.

6.2.1 Hvordan kan anbefalte tiltak implementeres?

Ofte møter en utfordringer ved implementering av nye tiltak og systemer. Denne studien ønsker likevel å understreke at prinsippene som ligger til grunn for både HMS og ISO 19650-5 er svært like, noe som gir grunn til å anta at HMS-avdelingen og BIM-avdelingen kan ha mer til felles enn man kanskje er klar over. En samordnet løsning hvor både digital sikkerhet og HMS blir vurdert i samme prosess kan være en implementeringsløsning som ikke behøver å medføre for mye ekstra arbeid eller kostnader, sammenlignet med å jobbe hver for seg.

En ser gjennom dagens SHA-plan (Sikkerhet, Helse og Arbeidsmiljø) hvordan «safety» er det som ligger i betydningen av «sikkerhet». Sikkerhet er handler imidlertid om mer enn «safety», og bør kanskje også ta hensyn til «security» slik ISO 19650-5 viser til? En fremtidig løsning på sikkerhet i byggenæringen kan derfor ligge i dette grensesnittet. Figur 15 illustrerer tanken.



Figur 15: Prinsipielle likheter mellom ISO 19650-5 og HMS

6.3 Videre arbeid

Tematikken omhandlende bygningsinformasjonssikkerhet er som denne oppgaven viser, et stort og omfattende tema. Denne studien synliggjør kun toppen av isfjellet når det kommer til andre sikkerhetsutfordringer med digital teknologi i byggenæringen. For videre arbeid finnes det derfor svært mange interessante områder å utforske videre. Denne rapporten er avgrenset til menneske- og prosessaspektene rundt sikkerhet med digital bygningsinformasjon, et tema som i seg selv bør forskes videre på. Samtidig er det stor utvikling på teknologi-siden i byggenæringen, og slik denne oppgaven har forsøkt å få frem, er det behov for sikkerhetsvurderinger og refleksjoner rundt all ny teknologi.
Det er vanskelig å sette fingeren på ett forslag til videre arbeid, derfor vil neste delkapittel omfatte trender som er observert gjennom denne studiens arbeid som kan være aktuelle å forske videre på.

6.3.1 Trender i næringen

Digital tvilling

Digitale tvillinger vil antagelig bli mer vanlig fremtiden. En digital tvilling er definert på ulike måter, hvor (Sintef, 2022) definerer det følgende:

> *«En virtuell representasjon av en fysisk virkelighet gjort mulig gjennom data og simulatorer for sanntidsberegninger, optimalisering, overvåking, kontroll og forbedret beslutningsstøtte.» (Sintef, 2022)*

I sammenheng med bygg- og anleggsbransjen kan en digital tvilling gi en rekke positive fordeler. (DigitalNorway, 2021) beskriver dette som potensielt svært kostnadsbesparende, ettersom samspillet mellom byggherre, entreprenører og prosjekterende går mer sømløst. I tillegg til de positive sidene ved dette, er også dagens fokus i stor grad rettet mot nettopp de positive sidene ved dette. Likevel vil en digital tvilling tilgjengeliggjøre enorme mengder informasjon om et bygg som vil gjøre det helt nødvendig å sikre informasjonen mot misbruk. Spørsmålet her er imidlertid hvordan dette skal gjøres?

Plattformer/skyløsninger

Stadig flere plattformer for samarbeid benyttes i byggeprosjekter. Hvilke skyløsninger som benyttes varierer fra prosjekt til prosjekt, og virksomhet til virksomhet. Det er imidlertid forskjellig hvor den geografiske plasseringen av serverne er, noe som også kan by på sikkerhetsutfordringer. Bør det stilles krav til hvilke skyløsninger som kan brukes? Hvordan kan dette påvirke sikkerheten?

Allerede i dag beskrives det som utfordrende å samarbeide som følge av ulike programvarer og plattformer. I lys av sikkerhetsperspektivet er spørsmålet hvordan alle de ulike løsningene bør håndteres/sikres? Bør det stilles krav til en type plattform? Dette kan kanskje føre til at god teknologi ikke kan tas i bruk under Norske forhold som følge av «feil» produksjonsland? I sammenheng med bygg, er dette et sentralt område å forske videre på.

Kryptering og Blokkjede-teknologi

Artikkelen (Rongyue Zheng, 2019) gjorde en studie på blokkjede basert metode for BIM-data som skulle sikre en sikker overføring av bygningsinformasjon. (Rongyue Zheng, 2019) konkluderer med at blokkjede teknologien forbedrer sikkerheten til BIM-data betydelig, noe som i stor grad fremmer utviklingen av BIM-teknologien. I tillegg gjorde (Moumita Das, 2020) en omfattende studie av både krypteringsløsninger og blokkjede teknologi. Rammene som den artikkelen foreslo gir eksempler på hvordan eksisterende cybersikkerhetsteknologier på best måte kan distribuere visse komponenter av BIM. Likevel beskriver (Moumita Das, 2020) at det finnes en rekke dokumenter, mediefiler, etc. i tillegg til de store BIM-modellene som ikke er dekt av deres studie.

I lys av den tidligere forskningen på teknologiske aspekter, er det stort potensiale i cybersikkerhetsmetoder for å skape en sikker overføring av bygningsinformasjon. Samtidig skal en være klar over at selv om blokkjede og krypterings-teknologi tilrettelegger for sikker informasjonsoverføring, sjekker ikke teknologien innholdet. Dette er likevel et svært relevant område å forske videre på.

Produktdokumentasjon

Produktdokumentasjon blir stadig mer aktuelt i takt med digitaliseringsutviklingen. Fokuset på klimavennlige løsninger, gjenbruk og mer nøyaktige kostnadsestimeringer er eksempler på temaer som krever mye dokumentasjon og informasjon. For å gjøre mer korrekte kostnadsestimeringer og CO_2-kalkulasjoner er en avhengig av å vite mange detaljer om hver komponent av et byggverk. Dette kan derfor skape konflikter med sikkerhetsperspektivet. For å løse disse utfordringene i fremtiden, bør det derfor etableres en gjensidig forståelse mellom disse som forhåpentligvis kan føre til en passelig balansegang. Likevel er dette i seg selv en komplisert prosess som utvilsomt bør forskes mer på i fremtiden.

Referanser

Abdul-Majeed Mahamadu, L. M., Colin Booth (2013) Challenges to BIM-cloud integration: Implication of security issues on secure collaboration. Tilgjengelig fra: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6735420.

al, O. A. E. e. (2021) Perspektiver på samfunnssikkerhet 2. utgave.

Alfasoft (2022) What is Nvivo? Tilgjengelig fra: https://www.alfasoft.com/no/produkter/statistikk-og-analyse/nvivo.html.

Arbeidstilsynet (2021a) HMS og SHA. Tilgjengelig fra: https://www.arbeidstilsynet.no/hms/hms-i-bygg-og-anlegg/forskjellen-pa-hms-og-sha/.

Arbeidstilsynet (2021b) Byggherreforskriften. Tilgjengelig fra: https://www.arbeidstilsynet.no/regelverk/forskrifter/byggherreforskriften/2/7/.

Arbeidstilsynet (2022) HMS i bygg og anlegg. Tilgjengelig fra: https://www.arbeidstilsynet.no/hms/hms-i-bygg-og-anlegg/.

Asbjørn Johannessen, P. A. T., Line Christoffersen (2021) Introduksjon til samfunnsvitenskapelig metode.

Asgeir Leine Pedersen, S. U. (2020) Usikkerhet ved involvering av utenlandske entreprenører. Tilgjengelig fra: https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2779420.

Aveyard, H. (2010) Doing a literature review in health and social care. Tilgjengelig fra: https://ebookcentral.proquest.com/lib/ntnu/detail.action?docID=771406&query=Doing+a+literature+review+in+health+and+social+care+%3A+a+practical+guide.

beredskapsdepartementet, J.-o. (2021) NOU 2006: 6. Tilgjengelig fra: https://www.regjeringen.no/no/dokumenter/nou-2006-6/id157408/sec3.

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

Digitaliseringsdirektoratet (2022) Informasjonssikkerhet for skjermingsverdige verdier etter sikkerhetsloven. Tilgjengelig fra: https://www.digdir.no/informasjonssikkerhet/informasjonssikkerhet-skjermingsverdige-verdier-etter-sikkerhetsloven/2283.

DigitalNorway (2021) Digitale tvillinger: slik brukes det i dag. Tilgjengelig fra: https://digitalnorway.com/digitale-tvillinger-slik-brukes-det-i-dag/.

Giuseppe Miceli Junior, P. C. P. a. M. C. R. (2020) Management Procedure for Sensitive Projects in the Context of a BIM Adoption in a Public Organization. Tilgjengelig fra: https://www.researchgate.net/profile/Giuseppe-Junior/publication/343723321_Management_Procedure_for_Sensitive_Projects_in_the_Context_of_a_BIM_Adoption_in_a_Public_Organization/links/5f3cd70fa6fdccc43d3283d/Management-Procedure-for-Sensitive-Projects-in-the-Context-of-a-BIM-Adoption-in-a-Public-Organization.pdf.

Google-scholar (2022) About google scholar. Tilgjengelig fra: https://scholar.google.com/scholar/about.html.

Grønmo, S. (2020) Bias i forskning. Tilgjengelig fra: https://snl.no/bias_i_forskning.

IRGC (2017) Introduction to the IRGC Risk Governance Framework. Tilgjengelig fra: https://irgc.org/risk-governance/irgc-risk-governance-framework/.

IRGC (2021) IRGC Risk Governance Framework. Tilgjengelig fra: https://irgc.org/risk-governance/irgc-risk-governance-framework/.

ISO (2022a) ISO/AWI 19650-6. Tilgjengelig fra: https://www.iso.org/standard/82705.html.

ISO (2022b) ISO/FDIS 19650-4. Tilgjengelig fra: https://www.iso.org/standard/78246.html.
Jacobsen, D. I. (2022) Hvordan gjennomføre undersøkelser? . Tilgjengelig fra: https://www.norli.no/hvordan-gjennomfore-undersokelser-1?gclid=CjwKCAjwyryUBhBSEiwAGN5OCIdogFT95LDEwPF8Pvvg2LvRvpo2OxwoygNH32Feb0i7zTVLAuoyZRoCbNsQAvD_BwE.
Listøl, E. (2021a) BIM og sikkerhet - ISO 19650-5.
Listøl, E. (2021b) BIM og samfunnssikkerhet.
Lovdata (2010) Forskrift om sikkerhet, helse og arbeidsmiljø på bygge- eller anleggsplasser (byggherreforskriften). Tilgjengelig fra: https://lovdata.no/dokument/SF/forskrift/2009-08-03-1028.
Lovdata (2019) Lov om nasjonal sikkerhet (sikkerhetsloven). Tilgjengelig fra: https://lovdata.no/dokument/NL/lov/2018-06-01-24.
Moumita Das, X. T., Jack C.P. Cheng (2020) BIM security: A critical review and recommendations using encryption strategy and blockchain. Tilgjengelig fra: https://www.sciencedirect.com/science/article/pii/S0926580521001333.
Nikdokht Ghadimina, M. M., Sharon Cox and Jan Krasniewicz (2021) BIM-enabled facilities management (FM): a scrutiny of risks resulting from cyber attacks. Tilgjengelig fra: https://www.emerald.com/insight/content/doi/10.1108/JFM-01-2021-0001/full/pdf?title=bim-enabled-facilities-management-fm-a-scrutiny-of-risks-resulting-from-cyber-attacks.
NSM (2020) Grunnprinsipper for IKT-sikkerhet. Tilgjengelig fra: https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/grunnprinsipper-ikt.
NSM (2021) Risiko 2021 - Helhetlig sikring mot sammensatte trusler. Tilgjengelig fra: https://nsm.no/getfile.php/136419-1616673370/Demo/Dokumenter/Rapporter/NSM_Risiko_2021_web_enkeltside_1203.pdf.
NSM (2022a) Risiko 2022 - Økt risiko krever økt årvåkenhet. Tilgjengelig fra: https://nsm.no/getfile.php/137798-1644424185/Filer/Dokumenter/Rapporter/NSM_rapport_final_online_enekeltsider.pdf.
NSM (2022b) Sikkerhetsloven og forskrifter. Tilgjengelig fra: https://nsm.no/regelverk-og-hjelp/sikkerhetsloven-og-forskrifter/.
NTNU-Universitetsbibliotek (2017) Kildekritikk av artikler: T-O-N-E prinsippet. Tilgjengelig fra: https://www.youtube.com/watch?v=rs5PFX5SIHc.
NTNU (2022) Masteroppgave. Tilgjengelig fra: https://i.ntnu.no/masteroppgave.
Piazzi, M. (2022) Why do we need ISO 19650-5. Tilgjengelig fra: https://www.bimplus.co.uk/why-do-we-need-iso-19650-5/.
Proactima (2016) Veileder - HMS i byggeprosjekter. Tilgjengelig fra: http://v1.prosjektnorge.no/site-content/uploads/2016/hms.pdf.
Rongyue Zheng, J. J., Xiaohan Hao, Wei Ren, Feng Xiong, Yi Ren (2019) bcBIM: A Blockchain-Based Big Data Model for BIM Modification Audit and Provenance in Mobile Cloud. Tilgjengelig fra: https://www.hindawi.com/journals/mpe/2019/5349538/.
Scopus (2022) Scopus - Ekspert kuratert abstrakt- og siteringsdatabase. Tilgjengelig fra: https://www.elsevier.com/solutions/scopus.
Sintef (2022) Digital tvilling. Tilgjengelig fra: https://www.sintef.no/ekspertise/digital/anvendt-matematikk/digital-tvilling/.
Standard-Norge (2020) NS-EN ISO 19650-5. Tilgjengelig fra: https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=1143866.
Standard-Norge (2021) Organisering og digitalisering av informasjon om byggverk - ISO 19650-serien. Tilgjengelig fra: https://www.standard.no/fagomrader/bygg-anlegg-og-eiendom/digital-byggeprosess/iso-19650-serien/.
Statsbygg (2021) BIM. Tilgjengelig fra: https://www.statsbygg.no/bim.
Steinar Kvale, S. B. (2021) Det kvalitative forskningsintervju 3. utgave.

Strømmen, K. (2019) Kinesiske entreprenører ser på Norge som et springbrett. Tilgjengelig fra: https://www.nrk.no/urix/kinesiske-entreprenorer-vil-bygge-og-investere-i-norge-1.14765938.
Stuart Porter, T. T., Tele Tan, Geoff West (2014) Breaking into BIM: Performing static and dynamic security analysis with the aid of BIM. Tilgjengelig fra: https://www.sciencedirect.com/science/article/pii/S0926580513002148.
Thomas Beach, L. P., Yacine Rezgui, Omer Rana (2017) Management of Collaborative BIM Data by Federating Distributed BIM Models. Tilgjengelig fra: https://ascelibrary.org/doi/pdf/10.1061/%28ASCE%29CP.1943-5487.0000657.
UiB (2021) Sikker jobbanalyse (SJA). Tilgjengelig fra: https://www.uib.no/hms-portalen/136754/sikker-jobbanalyse-sja.
UNIT (2022) Oria. Tilgjengelig fra: https://www.helsebiblioteket.no/databaser/alle-databaser/bibsys?lenkedetaljer=vis.
Yu Peng, X. L., Ming Li, Zheng Li, Tao Hu, Yangjun Xiao, Sheng Zhang, Luyu Zhang, Pengwei Wang, Chengwu Ming, Xiaobo Mi (2020) Sensing network security prevention measures of BIM smart operation and maintenance system. Tilgjengelig fra: https://www.sciencedirect.com/science/article/pii/S014036642031851X.

Vedlegg

Rapporten har følgende vedlegg:

Vedlegg 1: Intervjuguide digital sikkerhet

Vedlegg 2: Intervjuguide HMS

Vedlegg 1:

Intervjuguide digital sikkerhet

Mitt navn Edvard Listøl. Jeg skriver masteroppgave ved studieretningen Bygg- og miljøteknikk (Digitale byggeprosesser) ved NTNU Gjøvik. Oppgaven tilsvarer 30 studiepoeng og skal leveres juni 2022.

Formålet med oppgaven er å belyse den digitale sikkerhetskulturen i byggebransjen. Som følge av den digitale utviklingen innen bygg- og anleggssektoren, dagens risikobilde og fremtidens usikkerhet er det relevant å fremheve dette temaet. Jeg ønsker å få frem hvordan holdningene og fokuset til digital sikkerhet hos aktører i byggenæringen i dag, og sammenligne dette med det tilsynelatende positive holdningsfremmende arbeidet innen HMS-kulturen i byggebransjen. Kan vi lære noe av dette?

Den internasjonale serien av standarder for informasjonsforvaltning med BIM (ISO 19650-serien) har nylig laget en del 5 (informasjonsforvaltning med fokus på sikkerhet). Hvordan kan denne anvendes som rammeverk for å heve fokuset på sikkerhet i byggeprosjekter? For å belyse dette er det utarbeidet tre forskningsspørsmål:

1) Hvordan er den digitale sikkerhetskulturen blant aktører i byggenæringen i dag?
2) Hva kan vi lære av HMS?
3) Hvilke tiltak kan gjøres i praksis basert på ISO 19650-5?

For å danne et generelt overordnet bilde skal det intervjues personer med ulike roller i byggenæringen (byggherre, rådgiver, arkitekt, entreprenør og produsent). I intervjuene vil spørsmålene omhandle intervjuobjektets inntrykk av bransjens holdninger til sikkerhet, hvordan de kommuniserer og deler bygningsinformasjon og hvor de tenker det eventuelt er forbedringspotensial.

Intervjuet skal vare rundt 45 min. Jeg vil ta notater underveis, og dersom dere godtar det, vil alle intervjuene bli gjort opptak av. Opptakene er kun ment for å gjøre transkriberingsprosessen lettere, og vil ikke bli delt. Intervjuet vil gjennomføres på en semi-strukturert måte, noe som gjør at oppfølgingsspørsmål kan bli stilt. Dere står fritt til å svare så utfyllende eller kort som dere ønsker.

Generelle spørsmål

Navn:

Organisasjon/firma:

Type organisasjon:

Stilling/rolle:

Spørsmål i intervju:

Hvordan oppleves den digitale sikkerhetskulturen blant aktører i byggenæringen i dag?

Hvilke fordeler og ulemper medfører informasjonsdeling gjennom BIM i dine øyne?

Hvordan oppfatter du generelt fokus og holdninger til informasjonssikkerhet og digital sikkerhet i norsk bygge- og anleggsbransje?

Opplever du at folk i byggenæringen reflekterer rundt sensitiviteten til informasjonen de deler?

Har dere opplevd at andre aktører har delt informasjon med dere som de kanskje ikke burde gjort?

Hvilke erfaringer har man fra digital sikkerhet og prosessene rundt disse i dag?

Har dere opplevd å bli hacket, eller forsøkt svindlet på noen måte? I så fall hvordan?

Har dere opplæring i informasjonssikkerhet internt?

Pleier dere å sette av tid til å vurdere hva som er sensitiv informasjon i hvert enkelt byggeprosjekt?

Pleier dere å benytte informasjonsdelings-avtaler i byggeprosjekter?

Hvordan sørger dere for at sensitiv bygningsinformasjon ikke kommer på avveie?

Hva gjør dere hvis dere oppdager at bygningsinformasjon (som ikke burde deles) har kommet på avveie?

Hva tenker aktørene kan gjøres bedre i fremtiden i forhold til digital sikkerhet?

Hva mener du at byggenæringen kan bli bedre på i forhold til sikring/deling av bygningsinformasjon?

Vedlegg 2:

Intervjuguide HMS

Mitt navn Edvard Listøl. Jeg skriver masteroppgave ved studieretningen Bygg- og miljøteknikk (Digitale byggeprosesser) på NTNU i Gjøvik. Oppgaven tilsvarer 30 studiepoeng og skal leveres i juni 2022.

Formålet med oppgaven er å belyse den digitale sikkerhetskulturen i byggebransjen. Som følge av den digitale utviklingen innen bygg- og anleggssektoren, dagens risikobilde og fremtidens usikkerhet er det relevant å fremheve dette temaet. Jeg ønsker å få frem hvordan holdningene og fokuset til digital sikkerhet hos aktører i byggenæringen i dag, og sammenligne dette med det tilsynelatende positive holdningsfremmende arbeidet innen HMS-kulturen i byggebransjen. Kan vi lære noe av dette?

Den internasjonale serien av standarder for informasjonsforvaltning med BIM (ISO 19650-serien) har nylig laget en del 5 (informasjonsforvaltning med fokus på sikkerhet). Hvordan kan denne anvendes som rammeverk for å heve fokuset på sikkerhet i byggeprosjekter? For å undersøke dette er det utarbeidet tre forskningsspørsmål:

1) Hvordan er den digitale sikkerhetskulturen blant aktører i byggenæringen i dag?
2) Hva kan vi lære av HMS?
3) Hvilke tiltak kan gjøres i praksis basert på ISO 19650-5?

For å danne et generelt bilde skal det intervjues personer med ulike roller i byggenæringen (byggherre, rådgiver, arkitekt, entreprenør og produsent). I intervjuene tilknyttet HMS vil spørsmålene omhandle intervjuobjektets inntrykk av bransjens holdninger til HMS, hvordan prosessen er i dag og eventuelle forbedringspotensialer.

Intervjuet skal vare rundt 45 min. Jeg vil ta notater underveis, og dersom dere godtar det, vil alle intervjuene bli gjort opptak av. Opptakene er kun ment for å gjøre transkriberingsprosessen lettere, og vil ikke bli delt. Intervjuet vil gjennomføres på en semi-strukturert måte, noe som gjør at oppfølgingsspørsmål kan bli stilt. Dere står fritt til å svare så utfyllende eller kort som dere ønsker.

Generelle spørsmål

Navn:

Organisasjon/firma:

Type organisasjon:

Stilling/rolle:

Spørsmål i intervju:

Hvordan oppleves HMS kulturen blant aktører i byggenæringen i dag?

Hvordan vil du beskrive og vurdere dagens HMS prosess?

Hvilke faktorer tenker du er årsaken til at aktører i byggenæringen fokuserer mer på HMS i dag, sammenlignet med tidligere?

Hvordan oppfatter du holdninger til HMS i norsk bygg- og anleggsbransje i dag?

Hvilke erfaringer har man fra HMS arbeid og prosessene rundt disse?

Kan du tenke deg til et prosjekt du i nyere tid har vært med på hvor HMS spilte en spesielt viktig rolle?

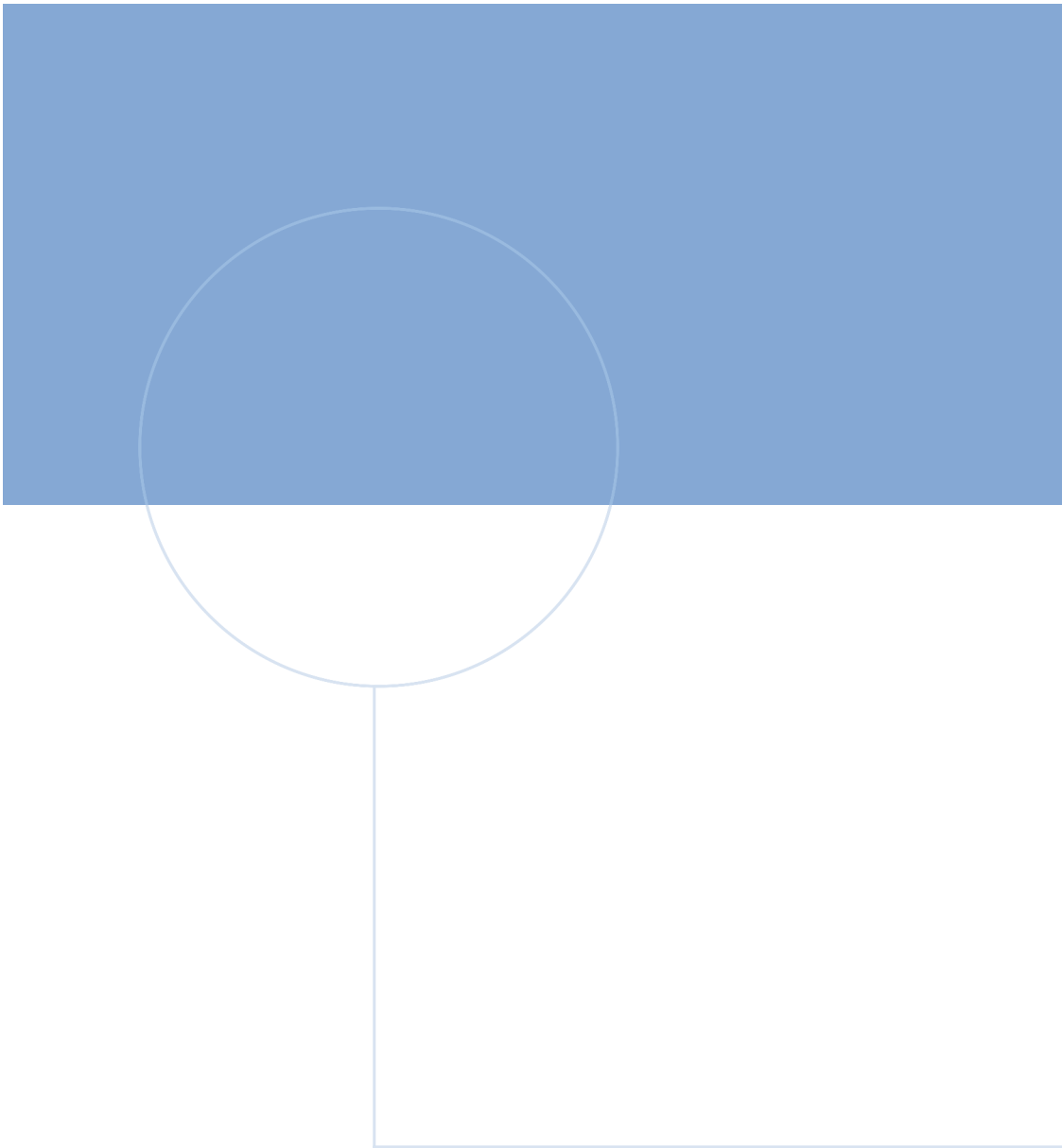
Hvilke deler av HMS-prosedyrene synes du fungerte spesielt godt? Hvorfor?

Møtte dere på noen utfordringer tilknyttet HMS?

Hvilke tiltak tror du har hatt størst betydning for de ansattes holdninger til HMS de siste 30 årene?

Hva tenker aktører at kan gjøres bedre i fremtiden?

Hva tenker du at bør gjøres annerledes for å oppnå en enda bedre HMS-prosess i fremtiden?



NTNU

Kunnskap for en bedre verden