Etablering av beredskap for Cyberhendelser

Hvordan kan Glencore Nikkelverk etablere god beredskap for cyberhendelser?

Helgeland, Stian

MASTERGRADSSTUDIUM I

RISIKOSTYRING OG SIKKERHETSLEDELSE

MASTEROPPGAVE

SEMESTER:

VÅREN 2023

FORFATTER:

STIAN HELGELAND

VEILEDER:

MORTEN SOMMER

TITTEL PÅ MASTEROPPGAVE:

ETABLERING AV BEREDSKAP FOR CYBERHENDELSER

EMNEORD/STIKKORD:

IKT-sikkerhet, cyberhendelser, cyberangrep, beredskap, krisehåndtering, sårbarhet, kritiske produksjonssystemer, hendelseshåndtering, trusselbilde og risikostyring.

SIDETALL: 82 (inkludert litteraturliste og vedlegg)

KRISTIANSAND **05.06.2023**

DATO/ÅR

Forord

Denne masteroppgaven markerer slutten på min utdanning i risikostyring og sikkerhetsledelse ved Universitetet i Stavanger (UiS). Det har vært en spennende og lærerik tid som har gitt meg solid kunnskap.

Utdanningen jeg har tatt ved UiS har vært viktig for min faglige utvikling og hjulpet meg med å utforske nye karriereveier. Jeg er veldig takknemlig for alt jeg har lært.

Jeg vil gjerne takke arbeidsgiveren min for den økonomiske støtten og fleksibiliteten som har gjort det mulig for meg å fullføre dette prosjektet. Jeg er sikker på at den nye kunnskapen kommer til å være nyttig på jobben framover.

En spesiell takk går til min veileder, Morten Sommer, som har gitt meg gode råd og konkrete tilbakemeldinger underveis. Hans hjelp har vært viktig for å heve kvaliteten på prosjektet.

Jeg vil også takke min fantastiske kone, som har støttet meg hele veien og tatt på seg ekstra ansvar når jeg har vært opptatt med å skrive. Uten hennes tålmodighet og støtte hadde det vært mye vanskeligere å fullføre oppgaven.

Til slutt vil jeg takke informantene ved Glencore Nikkelverk som har stilt opp på intervjuer til tross for travle hverdager. Deres bidrag har vært uvurderlige for oppgaven, og jeg setter stor pris på deres åpenhet og at de delte sin tid med meg.

Stian Helgeland

Kristiansand, 05.06.23

Sammendrag

Etablering av beredskap for cyberhendelser.

Denne masteroppgaven analyserer cybersikkerhetsstrategier og -praksis hos Glencore Nikkelverk, med fokus på forberedelse og håndtering av cyberhendelser. Med økende digitalisering og endrede trusselbilder, avdekker oppgaven at det er behov for forbedring knyttet til beredskapen mot digitale trusler.

Kvalitative metoder ble benyttet for datainnsamling, gjennom intervjuer av ledere og sikkerhetsansvarlige er det funnet at Nikkelverket har en moderat grad av beredskap for cyberhendelser. Selskapet har tatt i bruk teorier og rammeverk for cybersikkerhet, men risikoforståelsen relatert til det digitale domenet krever forbedring.

Økende digitalisering av samfunnet, inkludert viktige samfunnsfunksjoner og industriell produksjon, har endret trusselbildet. Det kreves beredskap mot digitale trusler på linje med fysisk beredskap i dagens samfunn. Dette er et relativt nytt fagområde, og mange bedrifter mangler erfaring med etablering av beredskap for cyberhendelser.

Denne masteroppgaven har adressert følgende tiltak for å styrke beredskapen for cyberhendelser ved Glencore Nikkelverk:

- Etablering av bedre dialog mellom forskjellige funksjoner i bedriften, eksempelvis IT-avdelingen, beredskapsstaber, industrivernledelsen og ledergruppen.
- Risikoanalyser bør gjennomføres og oppdateres regelmessig.
- Det bør utarbeides en beredskapsanalyse basert på resultatene fra risikoanalysene.
- Beredskapsplaner, tiltakskort for cyberhendelser og en plan for kompetanseutvikling, trening og øving bør etableres ut fra resultatene i beredskapsanalysen.
- Samarbeidsavtalen med det eksterne IT-sikkerhetsselskapet bør revideres for klarhet om ansvarsfordeling ved en cyberhendelse.

Opprettholdelse av konkurranseposisjonen i et trusselutsatt, digitalisert landskap vil kreve kontinuerlig forbedring, bevissthet og kompetanseheving blant ansatte. Implementeringen av teorier og rammeverk for håndtering av cyberhendelser er en pågående prosess hos Glencore Nikkelverk. Ved å adressere de identifiserte svakhetene, kan bedriften styrke sin beredskap og evne til å håndtere cyberhendelser.

Innholdsfortegnelse

1. Innledning

Den 8. mai 2021 ble det kjent at en av USAs viktigste oljeledninger, Colonial Pipeline, var stengt som følge av et dataangrep utført av hackergruppen "DarkSide" (Reuters, 2021). Oljeledningen som strakte seg over 8000 km langs hele Østkysten fra Texas til New York, transporterte ca. 2,5 millioner fat med drivstoff daglig og leverte drivstoff til en rekke grunnleggende samfunnsfunksjoner, herunder flere av landets største flyplasser. Nyheten om angrepet førte til at mange innbyggere begynte å hamstre drivstoff, noe som resulterte i lange køer ved bensinstasjonene og erklæring av "unntakstilstand" i flere delstater (CNN, 2021).

Hackerne fikk tilgang til selskapets IT-nettverk ved å bruke et gammelt brukernavn og passord fra en tidligere ansatt, og tok etter hvert over Active Directory-serveren, noe som ga dem tilgang til tusenvis av selskapets datamaskiner (WSJ, 2021). Selv om hackerne ikke fikk tilgang til operasjonell teknologi-nettverket, som styrer flyten i rørledningene, krevde de løsepenger for å gi tilbake kontrollen over selskapets datamaskiner. Colonial Pipeline bekreftet senere at de betalte ut 4,4 millioner dollar i løsepenger til hackerne (WSJ, 2021).

Hendelsen viser hvor sårbar kritisk infrastruktur er for dataangrep, og hvor alvorlige konsekvensene kan bli når de rammes. Mens mange mennesker tidligere så på dataangrep som et abstrakt problem, viser denne hendelsen at det kan ha en direkte påvirkning på deres daglige liv. Dette understreker viktigheten av å ha robuste og pålitelige systemer for cybersikkerhet, og å ha gode beredskapsplaner for å håndtere slike angrep.

Dataangrep har vært en trussel mot bedrifter og enkeltpersoner siden det første kjente angrepet i 1989, og det har blitt stadig mer vanlig i dagens digitale samfunn. Colonial Pipeline-angrepet i USA og flere vellykkede angrep i Norge i 2021, har vist at angrepene kan ha alvorlige konsekvenser for virksomheter og samfunnsfunksjoner. Med stadig flere bransjer og verdikjeder som er avhengige av digitale systemer, er det viktig å være forberedt på slike angrep. Likevel mangler mange virksomheter erfaring med å håndtere cyberhendelser, og det er derfor viktig å legge en plan for å etablere beredskap. Den raske utviklingen av informasjons- og kommunikasjonsteknologi kan gi økt sårbarhet i komplekse systemer og dermed øke behovet for å teste systemer før lansering. Det er derfor viktig å lære av erfaringene og forbedre beredskapen for å håndtere dataangrep (Digi.no, 2016; NRK, 2021; Njå m. fl, 2020).

1.1 Problemstilling

Denne studien fokuserer på etablering av beredskap for cyberhendelser ved en spesifikk industribedrift, Glencore Nikkelverk AS. Selv om studien tar utgangspunkt i en bestemt bedrift, antas funnene å være overførbare til andre virksomheter i lignende sektorer. For å undersøke hvordan Glencore Nikkelverk kan etablere beredskap for cyberhendelser og vurdere betydningen av dette, er følgende problemstilling utformet:

Hvordan kan Glencore Nikkelverk etablere god beredskap for cyberhendelser?

For å svare på problemstillingen vil et utvalg av ledergruppen i bedriften, IKT- drifts -og sikkerhetsledere, samt beredskapsrådgivere bli intervjuet. Følgende forskningsspørsmål vil bli undersøkt:

1. Hvilke sårbarheter og trusler er mest fremtredende for IKT-verdiene ved Glencore Nikkelverk, og hvordan kan disse potensielt påvirke bedriften?
2. I hvilken grad er teorier og rammeverk for cyberhendelser implementert i praksis hos Glencore Nikkelverk, og hvilke utfordringer og muligheter kan identifiseres i forbindelse med dette?
3. Hvordan utformer og evaluerer Glencore Nikkelverk trening- og øvelsesprogrammer for å forberede de ansatte på å håndtere cyberhendelser, og hvilke prosesser og metoder benyttes for systematisk forbedring av beredskapen mot cyberhendelser?

Ved å utforske disse spørsmålene, vil studien bidra til en bedre forståelse av hvordan virksomheter som Glencore Nikkelverk kan utvikle effektiv beredskap for å håndtere og redusere risikoen forbundet med cyberhendelser.

1.2 Avgrensninger

Cybersikkerhet i virksomheter er et bredt fagfelt som omfatter både teknologi, mennesker og organisasjon. Tradisjonelt forbinder mange datasikkerhet med antivirusprogrammer, kryptering, brannmurer og andre tekniske systemer. Denne teknologien er i stadig utvikling og endres hyppig på grunn av endringer i trusselbildet, eller avdekkede sårbarheter. Det antas at disse spiller en viktig rolle for å forebygge og håndtere dataangrep mot virksomheter. Fordi teknologien endres så hyppig at beskrivelser fort kan være utdaterte, og i lys av omfanget på oppgaven, vil det ikke studien gå i dybden på teknologiske tiltak eller barrierer.

I verdikjeden knyttet til cybersikkerhet inngår eksterne samarbeidspartnere og underleverandører. Disse vil kun omtales i den grad de direkte sees på som en del av beredskapen knyttet til bedriften.

Fysisk sikring er også en viktig barriere for å hindre tilgang til digital infrastruktur og analoge dokumenter. Dette vil heller ikke diskuteres i oppgaven.

Virksomheten som undersøkes er underlagt en rekke tilsynsmyndigheter som påser at regulatoriske krav oppfylles og at sikkerhetsarbeidet utføres tilfredsstillende. Som ansatt i virksomheten har jeg sett en trend hvor fokuset de senere år i større grad også omfatter cybersikkerhet. Det samme gjelder for internkontroll. Lovregulering og tilsynsmyndigheter spiller en viktig rolle i sikkerhetsarbeidet, men deres rolle vil heller ikke belyses i studien.

Fokuset i denne oppgaven vil være på de organisatoriske og menneskelige faktorene (de ikke-tekniske barrierene) knyttet til etablering av beredskap for cybersikkerhet. I relasjon til dette vil det sees på sårbarheter, trusler og etablering av beredskap for cyberhendelser.

2. Bakgrunn og kontekst

I dette kapittelet vil bakgrunnen og konteksten for studien presenteres. Det vil bli redegjort for digitalisering av industrien. Deretter vil sentrale begreper innen cybersikkerhet forklares, før det sees på hvilke trusler dagens industribedrifter står ovenfor. Til slutt vil det sees på beredskap knyttet til respons på cyberhendelser.

2.1 Glencore Nikkelverk

Glencore Nikkelverk AS er den største produsenten av nikkel i den vestlige verden. Selskapet har en lang historie som strekker seg tilbake til starten av 1900-tallet, da det ble etablert som en del av den norske industriveksten som fant sted på den tiden (nikkelverk.no, 2023).

I dag er Glencore Nikkelverk en del av det multinasjonale selskapet Glencore, som har virksomhet over hele verden. Nikkelverket ligger i Kristiansand og produserer årlig rundt 100 000 tonn nikkel. Bedriften er også en stor produsent av kobber og kobolt (nikkelverk.no, 2023).

Nikkel er et viktig metall som brukes i en rekke forskjellige industrielle applikasjoner, som for eksempel i produksjonen av rustfritt stål. Kobber og kobolt er også viktige metaller i industrien, og brukes blant annet i elektronikk og batteriproduksjon (nikkelverk.no, 2023).

Glencore Nikkelverk har gjennom årene blitt anerkjent for sin innovative tilnærming til produksjon og sitt fokus på bærekraft. Selskapet har gjort store investeringer i ny teknologi og har som mål å redusere miljøpåvirkningen fra sin virksomhet. Nikkelverket har også engasjert seg i samfunnsprosjekter i lokalsamfunnet, og har en sterk forpliktelse til å skape arbeidsplasser og bidra til økonomisk vekst i regionen (nikkelverk.no, 2023).

Glencore Nikkelverk er en såkalt storulykkevirksomhet. Storulykkevirksomheter er bedrifter som har potensiale for alvorlige konsekvenser for mennesker og miljø hvis det skulle skje en ulykke. Andre eksempler på slike virksomheter kan være petrokjemiske fabrikker, anlegg for produksjon av farlige kjemikalier, eller industrianlegg som håndterer farlig avfall. Slike bedrifter har et stort ansvar for å sikre at ansatte og samfunnet rundt dem er trygge, og en viktig del av dette ansvaret er å ha et godt industrivern.

Industrivernet er industriens egen beredskap som raskt kan håndtere branntilløp, personskader og lekkasjer av gass og farlige kjemikalier før nødetatene kommer. Industrivern er et lovpålagt krav om egenbeskyttelse som gjelder for de fleste store og mellomstore industrivirksomheter (NSO, 2023).

Industrivern er en kombinasjon av tiltak en virksomhet har til rådighet for å håndtere en beredskapssituasjon. Dette inkluderer for eksempel utstyr og materiell som brannbiler og røykdykkerutstyr, beredskapsplaner for å håndtere beredskapssituasjoner og opplæring av mannskapene som har funksjoner som beredskapspersonell. Dette inkluderer også samarbeid med nødetater som brannvesen, politi og helsevesen, samt øvelser for å trene på beredskapen. I den etablerte beredskapen ved Glencore Nikkelverk inngår 2 staber: Redningsstab og Krisestab. Disse er sammensatt av personer fra bedriftens ledergruppe og ledere for ulike fag- og ansvarsområder.

2.2 Glencore Nikkelverks organisering

Glencore Nikkelverk AS, også referert til som bedriften, er en del av det internasjonale konsernet Glencore International PLC, som har sitt hovedkontor i Sveits. Konsernet opererer innenfor en rekke sektorer, inkludert utvinning og foredling av mineraler og metaller, produksjon av kull, olje og gass, resirkulering av metaller og salg av disse produktene.

Glencore Nikkelverk er en integrert del av Glencore-konsernets nikkeldivisjon og mottar hovedsakelig råstoffet fra konsernets gruver i Canada. Dette bidrar til en effektiv og koordinert verdikjede innen nikkelproduksjon.

På lokalt nivå styres Glencore Nikkelverk av en administrerende direktør og en ledergruppe som består av direktører med ansvar for ulike fagområder. Denne organiseringen sikrer en strukturert tilnærming til beslutningstaking og styring av bedriftens ulike funksjoner, og bidrar til å opprettholde en klar linje med ansvar og rapportering til det overordnede konsernet.

2.3 Beredskapsplanverk

Glencore Nikkelverk har i dag et omfattende beredskapsplanverk som tar for seg ulike typer hendelser, inkludert prosess-sikkerhetshendelser, brann, personskader og miljøutslipp. Bedriften har utarbeidet vaktinstrukser og sikringsplaner for å håndtere sikkerhetshendelser, og har også utviklet detaljerte kontinuitetsplaner for å håndtere uforutsette utfall i produksjonsprosessen.

For å identifisere og håndtere risiko benytter bedriften et risikoregister som lister opp potensielle farer og tilhørende kontrolltiltak. Cybersikkerhet er inkludert i dette risikoregisteret, og behovet for å utføre en risikoanalyse og utarbeide en beredskapsplan for IKT-hendelser er identifisert. Selv om det har vært forsøk på å utvikle en slik plan, har ulike hindringer ført til at dette arbeidet ennå ikke er fullført.

På nåværende tidspunkt har Glencore Nikkelverk ikke et spesifikt planverk for cyberhendelser. Dette betyr at risikoen er identifisert, men eventuelle hendelser håndteres ad hoc og etter beste evne.

2.4 Digitalisering av industrien

Digitalisering av industrien refererer til bruk av digitale teknologier og løsninger for å forbedre og automatisere ulike produksjonsprosesser og arbeidsoppgaver. Dette kan inkludere bruk av roboter, sensorer, dataanalyse, kunstig intelligens og annen avansert teknologi.

I Norge har digitaliseringen av industrien blitt en stadig viktigere faktor i økonomien. Mange bedrifter har tatt i bruk digital teknologi for å øke effektiviteten og produktiviteten i produksjonsprosessene, og for å møte kravene til en stadig mer konkurransedyktig global økonomi.

Digitaliseringen av industrien har også muliggjort en større grad av tilpasning og fleksibilitet, som har ført til at industrien kan tilby mer skreddersydde produkter og tjenester til kundene sine.

Likevel er det også en del utfordringer knyttet til digitaliseringen av industrien, blant annet knyttet til sikkerhet og personvern, samt tilpasning av arbeidsstokken til de nye teknologiene.

Det er derfor viktig å ta hensyn til disse faktorene når man tar i bruk digital teknologi i industribedrifter.

I mars 2017 la den norske regjeringen, for første gang på 37 år, frem Industrimeldingen (Nærings- og handelsdepartementet, 2017). Her lanserte de sin visjon for en aktiv industripolitikk: *"Norge skal være en ledende industri- og teknologinasjon"* (Nærings- og handelsdepartementet, 2017, s. 9).

Norge har en lang og stolt industrihistorie, og mange industribedrifter har vært viktige for både lokalsamfunn og nasjonen som helhet. Landets konkurransefortrinn har i stor grad vært knyttet til tilgangen på naturressurser, som har forsynt industrien med fornybar og rimelig kraft. Høy kompetanse hos bedriftene og effektiv drift har veid opp for det forholdsvis høye lønnsnivået i norske bedrifter (NHD, 2017).

Norsk olje- og gassvirksomhet har sørget for høy sysselsetting og store inntekter. Selv om denne virksomheten fortsatt vil være viktig i mange år fremover, forventes det at etterspørselen fra næringen vil svekkes på lengre sikt. For å opprettholde verdiskapning må det utvikles ny næringsvirksomhet og legges til rette for gode rammevilkår for eksisterende industri (NHD, 2017).

Digitalisering, automatisering og teknologiutvikling trekkes frem som nøkkelfaktorer for å lykkes i denne omstillingen. Som en følge av dette vil hele produksjonskjeder kunne digitaliseres, noe som vil bidra til økt effektivitet, fleksibilitet og muligheter for tilpasning.

For å realisere regjeringens visjon om en ledende industri- og teknologinasjon må Norge investere i forskning, utvikling og kompetanseheving, samt legge til rette for samarbeid mellom forskningsinstitusjoner, næringsliv og offentlige aktører (Nærings- og handelsdepartementet, 2017). Dette vil være avgjørende for å sikre en vellykket overgang til en mer digitalisert, innovativ og konkurransedyktig industri i Norge.

I 2011 ble begrepet «Industri 4.0» lansert i Tyskland som en del av en nasjonal strategi for å fremme digitaliseringen av industrien (Kagermann, Wahlster, & Helbig, 2013). Industri 4.0 kan beskrives som et reformprogram for å digitalisere industrien gjennom blant annet automatisering og digitalisering av hele verdikjeder, inkludert bruk av tingenes internett (IoT), kunstig intelligens (AI) og avansert dataanalyse (Ghobakhloo, 2018). Hensikten er å opprettholde konkurransekraft og innovasjon i en globalisert og stadig mer teknologidrevet økonomi.

Begrepet Industri 4.0 og lignende konsepter har siden blitt tatt i bruk i mange land rundt om i verden (Ghobakhloo & Iranmanesh, 2021). I Norge har blant annet «Norsk Industri», som er den største landsforeningen i Næringslivets Hovedorganisasjon, omfavnet begrepet og fremmet det som en del av sin strategi for å styrke norsk industri (NHO, 2023). Mange beskriver digitaliseringen industrien står ovenfor som «den fjerde industrielle revolusjon» (Schwab, 2016).

Industri 4.0 handler om å bruke teknologien til å fundamentalt endre måten produksjon foregår og hele verdikjeden samhandler, noe som kan skape økt effektivitet, fleksibilitet og kundetilpasning (Ghobakhloo & Iranmanesh, 2021). Når man introduserer nye og avanserte teknologier i eksisterende produksjon, må man også sette i verk tiltak for å sikre disse mot cyberangrep. Enhver virksomhet som har et ønske om å digitalisere bør derfor ha omfattende cybersikkerhetstiltak på plass, inkludert risikovurdering, implementering av sikkerhetsteknologier og kontinuerlig overvåking og respons på potensielle trusler (Ghobakhloo & Iranmanesh, 2021).

2.5 IKT-sikkerhet

Informasjons- og kommunikasjonsteknologi-sikkerhet, heretter IKT-sikkerhet, referer til prinsippene, teknologiene og prosessene som brukes for å beskytte digitale enheter, nettverk, systemer, data og informasjon mot uautorisert tilgang, endring, ødeleggelse, forstyrrelser eller annen form for skade.

IKT-sikkerhet er avgjørende for å beskytte sensitive og konfidensielle data, inkludert personlige opplysninger, forretningshemmeligheter og andre former for digital informasjon som kan være verdifull eller sensitiv for en organisasjon eller enkeltperson.

Noen av de vanlige tiltakene som brukes i IKT-sikkerhet inkluderer brannmur, antivirusprogramvare, kryptering, passordbeskyttelse, autentisering, tilgangskontroll, overvåkning og sikkerhetskopiering. IKT-sikkerhet omfatter også implementering av beste praksis for datasikkerhet, for eksempel å begrense tilgangen til sensitive data og trene ansatte på cybersikkerhet (Store norske leksikon, 2022).

I en tid hvor stadig mer av våre personlige og forretningsmessige liv spiller seg ut digitalt, blir IKT-sikkerhet stadig viktigere for å beskytte mot cyberkriminalitet og digitale trusler.

Det er vanskelig å finne en entydig definisjon av begrepet IKT-sikkerhet. Selve forkortelsen IKT står for *«Informasjons- og kommunikasjonsteknologi»* Dette er en samlebetegnelse for teknologi som innhenter, overfører, bearbeider, lagrer eller presenterer informasjon (Store norske leksikon, 2022).

Hva den enkelte legger i begrepet IKT-sikkerhet vil kunne variere og endre seg over tid, i takt med den digitale utviklingen. I denne studien er det valgt å legge til grunn definisjonen fra det regjeringsoppnevnte IKT-sikkerhetsutvalget sin utredning- *«IKT-sikkerhet i alle ledd»* (NOU 2018:14). Historisk har mange forbundet IKT-sikkerhet med beskyttelse av nettverk og systemer. I de senere år har det vært større fokus på informasjonen som behandles i nettverk og systemer, og hvilke typer tjenester disse systemene leverer. Utvalget beskriver IKT-sikkerhet som *«beskyttelse av IKT-systemene, tjenestene som leveres av systemene, eller informasjon som behandles i systemene»* (NOU 2018:14).

Begrepet IKT-sikkerhet er assosiert med en rekke synonymer og tilgrensende felt, som inkluderer uttrykk som «cybersikkerhet» (også kjent på engelsk som «Cybersecurity»), «digital sikkerhet» og «informasjonssikkerhet». Disse betegnelsene anvendes av forskjellige aktører innen feltet. I denne sammenhengen er det verdt å merke seg at IKT-sikkerhet, slik det er definert her, omfatter alle disse begrepene. I denne studien benytter vi uttrykket "cyberhendelser" for å beskrive alle former for angrep, sikkerhetsbrudd, eller andre uønskede hendelser som er relatert til IKT-systemer.

Tidligere snakket man ofte isolert om IT-sikkerhet og så på K'en (kommunikasjon) som en egen gruppe. Utviklingen over mange år har derimot ført disse sammen. For eksempel er TV og telefoni, som tidligere gikk via separate analoge systemer, i dag erstattet med digitale løsninger. På den andre siden skal informasjonen som finnes i IT-systemene i større grad deles, det vil si kommunisere med andre nettverk og systemer (SNL, 2022). Det er derfor naturlig å bruke informasjons- *og* kommunikasjonsteknologi når man snakker om dagens digitale systemer.

IKT-sikkerhetsutvalget presenterer også sikkerhetsmål for IKT-sikkerhet. Tre nøkkelbegreper de trekker frem i sine sikkerhetsmål er: tilgjengelighet, integritet og konfidensialitet. Hva sikkerhetsmålene innebærer er beskrevet som (NOU 2018:14, s. 14):

- tilgjengelighet, dvs. at IKT-systemene, informasjonen som behandles i systemene, og tjenestene tilknyttet systemene er tilgjengelig der og når det trengs for brukerne

- integritet, dvs. at IKT-systemene, informasjonen som behandles i systemene, og tjenestene tilknyttet systemene ikke endres utilsiktet eller uautorisert
- konfidensialitet, dvs. at IKT-systemene, informasjonen som behandles i systemene, og tjenestene tilknyttet systemene kun er tilgjengelige for dem som rettmessig skal ha.

For å nå sikkerhetsmålene ser man at det er behov for barrierer som omfatter både det menneskelige, teknologiske og organisatoriske nivået i en virksomhet. Hensikten med disse barrierene er at de skal *«motvirke uønskede digitale hendelser, evne til å oppdage slike hendelser og påfølgende reaksjon for å gjenopprette en sikker tilstand for IKT-systemene»* (NOU 2018:14, 2018, s. 14).

2.6 Digitale trusler

«Norske bedrifter og offentlige virksomheter vil bli utsatt for datainnbrudd og datatyveri. Det er vurdert at virksomheter med samfunnskritiske funksjoner vil bli utsatt for datatyveri eller datamanipulasjon som følge av datainnbrudd» Politiets trusselvurdering 2022 (POD, 2022).

Digitale trusler refererer til potensielle farer eller sikkerhetsproblemer som kan oppstå når man bruker digitale enheter og teknologier. Disse truslene kan omfatte en rekke ulike angrep og farer, som for eksempel:

1. Malware: Dette er en form for skadelig programvare som er laget for å skade datamaskinen eller mobiltelefonen din. Malware kan inkludere virus, trojanere og spyware.
2. Phishing: Svindler sender deg en falsk e-post eller tekstmelding som ser ut som om den kommer fra en legitim kilde, som en bank eller et selskap. Målet er å lure deg til å gi fra deg personlig informasjon, som passord eller kredittkortnummer.
3. Identitetstyveri: Noen stjeler personlig informasjon, som navn, personnummer, adresse eller kredittkortnummer, og bruker det til å åpne kontoer, ta opp lån eller kjøpe varer og tjenester.
4. Cyberstalking: Dette er når noen følger og trakasserer deg på nettet, for eksempel gjennom sosiale medier eller e-post.

5. DDoS-angrep: Når en gruppe hackere sender en stor mengde trafikk til en nettside for å overbelaste serverne og gjøre nettsiden utilgjengelig.
6. Ransomware: Dette er når en hacker tar kontroll over datamaskinen eller mobiltelefonen din og krypterer filene dine. Deretter krever de at man betaler løsepenger for å få tilbake tilgangen til filene.
7. Skimming: En hacker installerer en enhet på en minibank eller betalingsterminal for å stjele kredittkortinformasjonen din når du bruker kortet.
8. Uautorisert tilgang: En uautorisert person får tilgang til datamaskinen eller mobiltelefonen din, enten gjennom en svakhet i sikkerheten eller ved å stjele passordet ditt.

Digitalisering av industrien har skapt nye muligheter for virksomhetene, men også nye muligheter for kriminelle aktører. I motsetning til tradisjonell kriminalitet kan datakriminalitet utføres uten fysisk kontakt. Utenlandske kriminelle trenger ikke en befinne seg på norsk jord for å kunne utføre alvorlige dataangrep mot norske virksomheter. De som utfører datakriminalitet, spenner fra enkeltindivider til organiserte kriminelle og statlige aktører. Kriminalitet mot datasystemer begås først og fremst for å oppnå økonomisk vinning, men også for å få tilgang til sensitiv informasjon eller skade digitale tjenester og maskinvare. Ved å ha tilgang på dette kan de kriminelle presse virksomhetene for penger ved å true med å publisere data. De kan selge informasjon til konkurrenter eller andre kriminelle aktører, eller de kan utsettes for løsepengevirus. Denne type virus krypterer virksomhetens data og de kriminelle krever penger for å låse opp data. Løsepengevirus anses som den største trusselen mot bedrifter og virksomheter i det digitale rom (POD,2022).

3. Teori

I følgende kapittel vil det teoretiske rammeverket oppgaven baserer seg på bli presentert. Først presenteres det en oversikt over de sentrale begrepene risiko, risikostyring, sikkerhet og sårbarhet. Deretter dykker vi dypere inn i teoriene som er knyttet til etablering av beredskap, inkludert relevante aspekter som opplæring, øvelser og systematisk forbedring. Ved å koble sammen disse teoretiske elementene, vil det bygges en teoretisk ramme for resten av oppgaven.

3.1 Risiko

Risiko er en uunngåelig del av livet og påvirker mange av beslutningene vi tar hver dag, både i arbeidslivet, samfunnet og i våre personlige liv. For å ta informerte valg må vi vurdere risiko, og det finnes ulike perspektiver på hva risiko innebærer. Innen sikkerhetstenkning er forståelsen og betydningen av begrepet vesentlig for å forstå hvordan man kan vurdere og styre risiko (Renn, 1998).

I denne sammenhengen defineres risiko som «*kombinasjon av konsekvensene av aktiviteten med tilhørende usikkerhet*» (Aven, 2015, s. 6). Dette betyr at risiko ikke bare handler om de potensielle konsekvensene av en gitt aktivitet, men også om hvor usikre vi er på hva disse konsekvensene faktisk vil være (Aven, 2015).

I denne definisjonen handler risiko om en fremtidig aktivitet, for eksempel et dataangrep mot bedriften. Dersom bedriften utsettes for dataangrep, kan dette få konsekvenser for produksjon og påføre økonomiske tap. Med andre ord kan aktiviteten (dataangrep) få konsekvenser for våre økonomiske verdier. Det man ikke kan si på forhånd er om man blir utsatt for et angrep og hvor alvorlige konsekvensene av et slikt angrep vil være, altså tilhørende usikkerhet.

Ved å inkludere usikkerhet i definisjonen av risiko, blir begrepet mer nyansert og relevant (Aven, 2015). Risiko blir ikke lenger bare en beskrivelse av potensielle konsekvenser, men også graden av usikkerhet rundt disse konsekvensene. Dette gjør det lettere å vurdere om en aktivitet er verdt å utføre, og hvordan man best kan håndtere risikoen som følger med (Aven & Renn, 2009).

Det er viktig å merke seg at risiko ikke nødvendigvis er negativt. Selv om risiko ofte blir assosiert med farer og trusler, kan risiko også være knyttet til muligheter og potensielle gevinster. Å investere i aksjemarkedet innebærer for eksempel risiko, men også potensiale for høy avkastning (Lunde, 2019). Dette illustrerer at risiko kan ha både positive og negative aspekter, og at det er viktig å ta hensyn til begge sider når man vurderer og styrer risiko i ulike sammenhenger.

3.2 Risikostyring

Formålet med risikostyring er å systematisk anvende ulike strategier for å styre fremtidig utvikling, og kan defineres som «*alle tiltak og aktiviteter som gjøres for å styre risiko*» (Aven, 2015). Risikostyring er en kritisk komponent i beslutningsprosessene for mange organisasjoner og virksomheter, da det bidrar til å balansere verdiskaping og unngå skader og tap (Aven & Renn, 2009).

Etablering av en systematisk tilnærming til risikostyring gir organisasjoner verktøy for å identifisere, analysere og håndtere risiko på en effektiv måte (Renn, 1998). For å skape verdier er det nødvendig å akseptere en viss grad av risiko, siden fullstendig unngåelse av risiko vil hindre vekst og utvikling. Samtidig er det viktig å vurdere om det er et uakseptabelt misforhold mellom risikoen og verdiene en aktivitet genererer, og om det er forsvarlig å opprettholde aktiviteten (Aven & Renn, 2009).

Ved å identifisere, analysere og håndtere risiko på en systematisk måte, kan organisasjoner redusere sannsynligheten for uønskede hendelser og minimere konsekvensene dersom de skulle oppstå (Lunde, 2019). Gjennom dette arbeidet kan organisasjoner utvikle en mer robust og bærekraftig drift, samtidig som de skaper muligheter for vekst og innovasjon (Aven, 2015).

3.3 Sikkerhet

Sikkerhet er en sentral verdi i alle samfunn og kan betraktes som et av menneskets mest grunnleggende behov (Maslow, 1943, snl.no). Opplevelsen av sikkerhet, trygghet og stabilitet er avgjørende for menneskers velvære og kognitive funksjoner. For å sikre et trygt samfunn, har vi utviklet ulike metoder for å beskytte oss mot potensielle trusler mot våre verdier.

Sikkerhet kan defineres som *"evnen til å unngå skader og tap som følge av uønskede hendelser, enten disse skyldes tilfeldige eller bevisste handlinger"* (Aven, 2006). Dette innebærer at sikkerhet innebærer kontroll og tiltak for å beskytte mot uønskede hendelser. Definisjonen skiller mellom tilfeldige (ikke-intenderte) og bevisste (intenderte) handlinger. På engelsk deler man begrepet "sikkerhet" mellom "safety" og "security". "Safety" refererer til ikke-intenderte hendelser, mens "security" omhandler tiltak for å hindre intenderte handlinger. Aven's definisjon dekker begge begreper (Aven, 2006).

Sikkerhet kan omfatte både individ- og samfunnsnivå og omhandler det menneskelige, politiske og fysiske plan (Renn, 1998). Dette inkluderer personlig sikkerhet, nasjonens sikkerhet mot ytre trusler og cyber-sikkerhet for å beskytte digitale ressurser og infrastruktur.

For å ivareta sikkerheten i samfunnet er det viktig med en helhetlig tilnærming som inkluderer tiltak for å forebygge, identifisere og håndtere trusler (Aven & Renn, 2009). Dette innebærer blant annet samarbeid mellom offentlige og private aktører, investeringer i infrastruktur og teknologi, og opplæring og utdanning av befolkningen i sikkerhetsspørsmål (Renn, 1998)

For å ivareta sikkerheten i samfunnet er det viktig med en helhetlig tilnærming som inkluderer tiltak for å forebygge, identifisere og håndtere trusler (Aven & Renn, 2009). Dette innebærer blant annet samarbeid mellom offentlige og private aktører, investeringer i infrastruktur og teknologi, og opplæring og utdanning av befolkningen i sikkerhetsspørsmål (Renn, 1998).
I en stadig mer globalisert verden, er det viktig å forstå at sikkerhet ikke bare er et nasjonalt anliggende, men også et internasjonalt samarbeidsområde. Felles innsats for å bekjempe trusler, som terrorisme og cyberangrep, er avgjørende for å ivareta sikkerheten i en stadig mer sammenkoblet verden.

3.4 Sårbarhet

Sårbarhet er et begrep som beskriver tilstanden av å være utsatt for risiko og fare. Dette kan være på individuelt, organisatorisk eller samfunnsnivå, og kan skyldes ulike faktorer som for eksempel fysiske, økonomiske eller sosiale forhold.

Sårbarhet er en viktig faktor å ta hensyn til når man utfører risikoanalyser og risikostyring, da sårbarhetene kan gjøre det vanskelig å hindre uønskede hendelser eller forverre konsekvensene av disse hendelsene. Derfor er det viktig å identifisere og analysere sårbarheter som kan påvirke oss for å kunne implementere barrierer som kan øke vår motstandsdyktighet (Lunde, 2019).

Videre kan sårbarhet bli ekstra utfordrende å håndtere hvis andre med vilje ønsker å utnytte dem mot oss. Slike tilsiktede handlinger kan være alt fra kriminelle handlinger som tyveri og vold til mer alvorlige handlinger som sabotasje og terror. Innenfor arbeidet med informasjonssikkerhet er det spesielt viktig å beskytte seg mot tilsiktede handlinger, spesielt fordi sårbarhetene knyttet til cyberangrep ofte kan være svært alvorlige (Lunde, 2019).

Å håndtere sårbarhet krever en helhetlig tilnærming til risikostyring og kan kreve tiltak på flere nivåer. Dette kan inkludere tekniske og organisatoriske tiltak som å øke sikkerheten på et bygg, eller implementere sikkerhetsprosedyrer for ansatte. Å øke bevisstheten omkring sårbarhetene kan også bidra til å redusere risikoen, ved at man identifiserer og tar tak i sårbarheter på et tidlig stadium og sørger for at de er en del av risikostyringen på en kontinuerlig basis (ISO, 2018).

Eriksen et al. (2021, s. 171)(Aven, 2015) definerer sårbarhet som *«Et systems evne til å motstå en uønsket handling eller uønsket hendelse, samt manglende evne til å gjenoppta sin funksjon.»*

Videre beskriver Eriksen et al. (2021) sårbarhet som en tilstand der et system har begrensninger i sin evne til å tåle påkjenninger eller stress som kan føre til uønskede situasjoner og konsekvenser med verditap. For å identifisere sårbarhetene til et system, kan man utføre sårbarhetsanalyser. Dette er et velkjent verktøy som brukes for å vurdere konsekvensene av uønskede situasjoner og sannsynligheten for at disse situasjonene kan oppstå. Sårbarhetsanalyser gir oss en bedre forståelse av systemets tåleevne og hjelper oss med å implementere tiltak for å redusere sannsynligheten for uønskede hendelser og minimere konsekvensene av dem hvis de likevel skulle skje (Eriksen et al. 2021).

«I beredskapssammenheng vil sårbarhet være et utrykk for at beredskapen svekkes, eller svikter når en aktuell definert situasjon inntreffer» (Eriksen et al. 2021, s. 171).

Sheila Jasanoff (2018) sin studie presentert i boken «Vulnerability in technological cultures» utforsker hvordan teknologi og samfunn er sammenkoblet og påvirker hverandre gjensidig. Studien viser hvordan teknologi og samfunn ikke kan sees som to distinkte enheter, men heller som komponenter i et komplett system. Dette perspektivet kan anvendes på alle elementer i krisesituasjoner og kriseberedskap, da alt er i samproduksjon.

Studien utforsker spesielt konseptet sårbarhet og hvordan dette kan brukes til å forstå hvordan teknologi og samfunn påvirker hverandre. Sårbarhet kan sees som et resultat av en økende avhengighet av teknologi og systemer, og hvordan dette gjør oss sårbare for feil, mangler og manglende ressurser.

Jasanoff (2018) bruker eksempler fra ulike sammenhenger for å illustrere hvordan sårbarhet kan oppstå. Et eksempel er naturkatastrofer, der samfunnets respons og evne til å håndtere krisen er sterkt avhengig av teknologi og systemer. Et annet eksempel er menneskeskapte katastrofer som oljeutslipp og atomulykker, der teknologi og samfunn er gjensidig påvirkende faktorer.

Studien viser videre hvordan sårbarhet og samproduksjon også er relevante for kriseberedskap og respons. Jasanoff (2018) argumenterer for at kriseberedskap må være en integrert del av samfunnets planlegging og ressursallokering, og ikke bare en reaksjon på en krise. Videre må kriseberedskap ta hensyn til kompleksiteten og samproduksjonen mellom teknologi og samfunn, og hvordan dette kan føre til økt sårbarhet.

Studien har viktige implikasjoner for norsk krisehåndtering og beredskapsplanlegging. Norge har i det siste opplevd flere naturkatastrofer, som flom, ras og skogbranner. Disse katastrofene har vist at samfunnets respons er avhengig av teknologi og systemer, og at sårbarheten øker når teknologien og samfunnet ikke fungerer sammen.

Norge er også et land med høy risiko for menneskeskapte katastrofer, som for eksempel oljeutslipp. Studien viser at kriseberedskap må ta hensyn til samproduksjonen mellom teknologi og samfunn, og at dette krever en integrert tilnærming til planlegging og ressursallokering.

3.5 Beredskap

Beredskap handler om å være både forberedt på og i stand til å håndtere uønskede situasjoner på en best mulig måte. Selv om vi ikke kan planlegge for alle mulige uønskede situasjoner, er det viktig å ha et mål om å kunne iverksette beredskap når slike situasjoner oppstår (Eriksen et al., 2021).

I denne studien defineres beredskap som *«Beredskap er forberedelse og utøvelse av konsekvenshåndtering ved uønskede situasjoner»* (Eriksen et al., 2021).

Beredskap er et begrep som beskriver evnen til å håndtere uønskede hendelser og situasjoner. Dette kan være alt fra naturkatastrofer og ulykker, til dataangrep og pandemier. Beredskap handler om å være forberedt på det uforutsette, og å ha planer og tiltak på plass for å håndtere uønskede hendelser når de inntreffer.

Perry og Lindell (2003) er to forskere som har bidratt mye til studiet av beredskap og katastrofepsykologi. De beskriver beredskap som en prosess som omhandler forebygging, forberedelse, respons og gjenoppbygging.

Perry og Lindell mener at beredskap ikke kun handler om å være forberedt på en krise, men også om å kunne tilpasse seg situasjonen og gjenopprette normalfunksjonene så raskt som mulig etter en krise. De understreker også at beredskap ikke bare handler om tekniske og operative tiltak, men også om psykologiske og sosiale faktorer som kan påvirke hvordan folk reagerer i en krisesituasjon.

Perry og Lindell (2003) identifiserer en rekke faktorer som kan påvirke beredskapen, blant annet tidligere erfaringer med katastrofer, tillit til myndigheter, kultur og sosiale normer, og tilgjengeligheten av informasjon. De påpeker også viktigheten av å involvere lokalsamfunnet i beredskapsplanlegging og -gjennomføring, og å ta hensyn til behovene til sårbare grupper som eldre og funksjonshemmede.

Perry og Lindell (2003) argumenterer også for at beredskap bør betraktes som en kontinuerlig prosess, og at det er viktig å lære av tidligere erfaringer og kontinuerlig evaluere og forbedre beredskapsplanene. De mener at god kommunikasjon, koordinering og samarbeid mellom ulike aktører er avgjørende for å oppnå en effektiv beredskap.

3.5.1 Prinsipper for beredskap

Både på nasjonalt nivå og i ulike organisasjoner er det etablert prinsipper for beredskap.

De nasjonale beredskapsprinsippene er retningslinjer som benyttes i oppbygningen av nasjonale beredskapsorganisasjoner. De fire grunnleggende nasjonale prinsippene er i dag *likhetsprinsippet, ansvarsprinsippet, nærhetsprinsippet* og *samvirkeprinsippet.*

1. Ansvarsprinsippet: Dette innebærer at den organisasjonen som har ansvar for et fagområde i en normalsituasjon, også har ansvaret for nødvendige beredskapsforberedelser og for å håndtere ekstraordinære hendelser på området. Dette prinsippet sikrer at ansvarlige instanser har en klar rolle i arbeidet med samfunnssikkerhet og kan ta nødvendige beslutninger for å redusere risiko og håndtere kriser.

2. Likhetsprinsippet: Betyr at den organisasjonen man opererer med under kriser, i utgangspunktet skal være mest mulig lik den organisasjonen man har til daglig. Dette sikrer at organisasjonen er godt forberedt på å håndtere kriser, da de allerede har erfaring med hvordan organisasjonen fungerer til daglig.

3. Nærhetsprinsippet: Dette innebærer at kriser organisatorisk skal håndteres på lavest mulige nivå. Dette sikrer at beslutninger kan tas raskt og effektivt, og at ressursene kan utnyttes på en best mulig måte. Det betyr også at lokalkunnskap og -ressurser kan tas i bruk for å håndtere situasjoner på en mest mulig hensiktsmessig måte.

4. Samvirkeprinsippet: Dette prinsippet vil si at myndigheter, virksomheter eller etater har et selvstendig ansvar for å sikre et best mulig samvirke med relevante aktører og virksomheter i arbeidet med forebygging, beredskap og krisehåndtering. Dette sikrer at samarbeidet mellom ulike aktører fungerer best mulig og at ressurser og kompetanse kan deles på tvers av organisasjoner og sektorer.

Disse prinsippene danner grunnlaget for arbeidet med samfunnssikkerhet i Norge og sikrer en helhetlig og koordinert tilnærming til beredskapsarbeidet. Prinsippene anbefales benyttet også av private virksomheter (Meld. St. 5, 2020) (Lunde, 2019).

Mange private organisasjoner følger de nasjonale beredskapsprinsippene, men noen velger å utvikle sine egne prinsipper for beredskap. Disse kan ofte finnes i et eget policy-dokument for risikostyring eller sikkerhet og beredskap. Det er likevel viktig å tydeliggjøre og beskrive

hvem som i organisasjonen skal utarbeide, følge opp og forbedre rammeverket for beredskap (Eriksen et.al, 2021).

3.6 Etablering av og modeller for beredskap

For å være forberedt på og i stand til å håndtere uønskede situasjoner må det etableres beredskap i virksomheten, eller organisasjonen. Det finnes flere tilnærminger i litteraturen som tar for seg prosessen med å etablere beredskap. I denne studien tas det utgangspunkt i Eriksen et al., (2021), Lunde (2019) og Perry og Lindell (2003).

En vanlig tilnærming til å planlegge for beredskap er å utføre en risikoanalyse for å kartlegge potensielle farer. Imidlertid går mange organisasjoner direkte fra risikoanalysen til å utvikle en beredskapsplan som beskriver hvordan de skal håndtere slike situasjoner. Selv om risikoanalyser er en viktig del av beredskapsplanlegging, gir de ofte bare informasjon om hva som kan gå galt og hvor ille det kan bli. De gir sjelden svar på hvordan man best kan håndtere disse situasjonene og hva som trengs for å gjøre det. En beredskapsanalyse kan gi svar på dette og hjelpe organisasjoner å ta steget fra risikokartlegging til valg av beredskapsstrategier. Beredskapsanalysen kan også hjelpe til med å identifisere sårbarheter og uønskede situasjoner som ikke ble avdekket i risikoanalysen (Eriksen et al., 2021).

Etableringen av beredskap kan variere betydelig mellom ulike virksomheter. Mens noen organisasjoner har en fast beredskapsorganisasjon som regelmessig trener og øver, har andre organisasjoner et kortvarig behov for beredskap i en begrenset tidsperiode. Til tross for ulike behov, kompleksiteter og risikobilder kan virksomheter følge samme prosess for å etablere beredskap. Lunde (2019) hevder at for å oppnå en planlagt, effektiv og tilpasset beredskap til en akseptabel kostnad, bør beredskapsetableringen gjennomgå følgende overordnede aktiviteter:

- Identifisering:
    - Hva skal beredskapen etableres for?
    - Hvilke krav skal den oppfylle?
    - Hvilke tiltak og ressurser skal benyttes for å oppfylle kravene?
- Etablering:
    - Implementering, organisering og dokumentering av tiltak og ressurser

- Opplæring, trening og øving av beredskapsressurser.

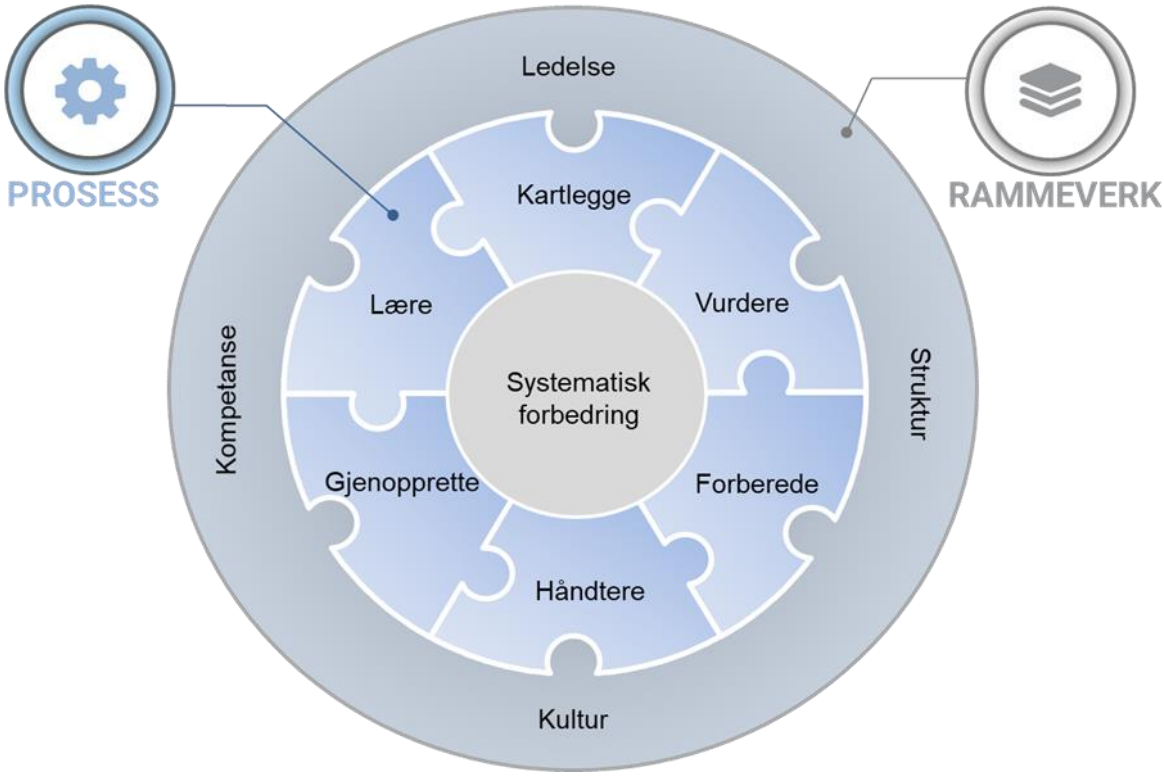
- Evaluering:
    - Tilfredsstiller den etablerte beredskapen eksisterende krav?
    - Hvordan kan den etablerte beredskapen kontinuerlig forbedres?

Beredskapsetablering kan defineres som *"en systematisk prosess som har som mål å planlegge og implementere egnede beredskapstiltak for den aktuelle virksomheten, basert på en gjennomført risiko- og sårbarhetsanalyse"* (Lunde, 2019, s. 58).

Perry og Lindell (2003) presenterer ti retningslinjer for god beredskap i deres artikkel. Den første av disse er at beredskapen bør baseres på nøyaktig kunnskap om trusselen. For å kartlegge trusselen gjennomføres risiko- og sårbarhetsanalyser (ROS-analyser). Sommer, Rake, og Botnen (2018) påpeker at norske kommuner og brannvesen i varierende grad legger ROS-analyser til grunn for deres etablering av beredskap.

3.6.1 Modell for beredskapsarbeid

Eriksen et al. (2021, s. 40) presenterer sin modell for beredskapsarbeid.



Denne modellen tar utgangspunkt i NS-ISO 31000:2018, Risikostyring. Standarden NS-ISO 31000 for risikostyring gir retningslinjer for håndtering av risiko og omfatter tre elementer: prinsipper, rammeverk og prosess for risikostyring. Eriksen et al. (2021) argumenterer for at det er fornuftig at beredskapsarbeid også følger denne inndelingen.

De nasjonale beredskapsprinsippene som ble beskrevet i det foregående delkapittelet, kan integreres som prinsipper. Forskjellige virksomheter kan også ha sine egne prinsipper som kan anvendes. Disse kan være knyttet til styringsmodeller, risikohåndtering, strategi, beslutningstaking, kommunikasjon, etikk og læring. Prinsipper for beredskap er ikke direkte tatt med i modellen (Eriksen et al., 2021). Modellen tar for seg rammeverk og prosess.

3.6.2 Rammeverk

Et systematisk rammeverk for beredskapsarbeid skal legge til rette for en effektiv arbeidsprosess innen beredskap ved å integrere beredskap med andre sentrale aktiviteter og funksjoner i en organisasjon. Rammeverket for beredskap inkluderer elementene ledelse, struktur, kultur og kompetanse (Eriksen et al., 2021).

Ledelse

For å lykkes med beredskap, er det essensielt at ledelsen aktivt engasjerer seg i arbeidet. Det er viktig at ledelsen anerkjenner beredskap som et strategisk virkemiddel, tar ansvar og eierskap, og legger til rette for og deltar i beredskapsarbeidet. En passiv ledelse som ikke prioriterer beredskap, vil føre til et utilstrekkelig beredskapsarbeid (Eriksen et al., 2021).

For å bestemme organisasjonens nødvendige beredskapsnivå, er det avgjørende at ledelsen etablerer og forankrer målsettinger og krav knyttet til beredskap. Dette vil sikre at organisasjonen har en solid beredskap som er tilpasset organisasjonens behov og risikoprofil (Eriksen et al., 2021).

Ledelsens engasjement i beredskapsarbeidet innebærer blant annet å sikre:

- at beredskapen er i tråd med organisasjonens strategi
- klare mål og krav til beredskapens kvalitet
- tilpasning av beredskapen til organisasjonens omgivelser
- en vedvarende og autentisk forpliktelse til å prioritere beredskapsarbeid

- tillit til ledelsens evne til å håndtere beredskap
- styring og støtte for å nå mål og intensjoner innen beredskap
- motivasjon og kommunikasjon om viktigheten og fordelene ved beredskap
- en organisasjonskultur som fremmer beredskapstenkning
- integrasjon av beredskap i organisasjonens øvrige prosesser
- ressurser tilgjengelige for beredskapsarbeidet
- tydelig fordeling av ansvar og oppgaver innen beredskapsarbeidet
- systematisk forbedring av beredskapen

(Eriksen et al., 2021).

Struktur

Strukturen bør legge til rette for et smidig og effektivt beredskapsarbeid, både internt og eksternt. Sentrale komponenter i strukturen for beredskapsarbeidet kan omfatte:

- krav og mål
- roller, ansvar og myndighet
- retningslinjer for engasjement, informasjon og kommunikasjon
- arbeidsprosesser og metoder
- fasiliteter og verktøy
- rutiner for kvalitetssikring, kontroll og forbedring
- nødvendig dokumentasjon.

Strukturen må også sikre hensiktsmessig integrering av beredskapsarbeidet i andre aktiviteter og prosesser, som virksomhetsstyring, risikostyring, kvalitetsstyring, kommunikasjon, interessenthåndtering, IKT, HR, osv (Eriksen et al.,2021).

Kultur

Uønskede situasjoner kan ofte oppstå på grunn av flere latente faktorer som kombineres på en uheldig måte. Hvis man identifiserer disse uheldige latente faktorene tidlig nok, øker

mulighetene for å håndtere konsekvensene. Det er derfor viktig for beredskapen å ha en kultur som oppfordrer til å rapportere kritikkverdige forhold og bekymringer tidlig. En organisasjonskultur som fremmer risikoforståelse, vil også være gunstig for beredskapen. Dette innebærer en kultur preget av individer som prioriterer å identifisere risiko og som er i stand til å bruke et bredt spekter av kompetanse for å forstå risiko. Med økt bevissthet og forståelse av risiko kan vi også identifisere uønskede situasjoner tidligere. Tidlig oppmerksomhet på uønskede situasjoner og en proaktiv tilnærming vil forbedre mulighetene for å håndtere situasjonene på en vellykket måte. Videre vil det være fordelaktig at organisasjonskulturen er preget av en positiv holdning til beredskapens betydning for å ivareta organisasjonens verdier. Dette innebærer blant annet en kultur som kjennetegnes av en positiv holdning til redundans og resiliens (Eriksen et al.,2021).

Kompetanse

Svak kompetanse kan resultere i betydelige mangler i beredskapen. Derfor bør rammeverket inneholde klare retningslinjer og rutiner for å etablere, vedlikeholde og videreutvikle kompetanse innen beredskap. Dette inkluderer blant annet:

- bevissthet, kunnskap, ferdigheter og holdninger innen beredskap på individ-, team- og organisasjonsnivå, samt mellom organisasjoner
- bruk av metoder og verktøy for kompetansestyring innen beredskap
- systematiske prosesser og metoder for gjennomganger og læring innen beredskap
- organisatorisk læring som et virkemiddel for systematisk forbedring av beredskapen.

Et godt rammeverk for beredskapsarbeidet bidrar til en strukturert og systematisk arbeidsprosess (Eriksen et al.,2021).

3.6.3 Prosess

Beredskapsarbeidsprosessen inneholder seks hovedaktiviteter. Disse aktivitetene kan betraktes som nødvendige puslespillbrikker for å sikre en solid beredskap. Bortsett fra aktivitetene "håndtere" og "gjenopprette", utføres de jevnlig. De seks aktivitetene i beredskapsarbeidsprosessen er kort beskrevet nedenfor, sammen med systematisk forbedring, som er kjernen i figuren og påvirker alle aktivitetene og rammeverket (Eriksen et al.,2021).

Kartlegge

Et risikobilde er en viktig grunnstein for beredskapen ettersom det gir innsikt i potensielle problemer og konsekvensene av uønskede situasjoner. Flere metoder kan benyttes for å identifisere uønskede situasjoner og deres konsekvenser, som risiko- og sårbarhetsanalyser, HAZID/HAZOP-analyser, sikringsrisikoanalyser, kontinuitetsanalyser og strategiske analyser. Det er også fornuftig å identifisere risiko basert på analyser og rapporter fra eksterne kilder. Identifisering handler ikke bare om å få oversikt over mulige uønskede situasjoner. Det er også viktig å etablere en solid risikoforståelse. Dette innebærer å forstå svakheter, styrker og særegenheter ved omgivelser og interessenter, organisasjon og kompetanse, anlegg og tekniske systemer, osv. Det kan finnes sårbarheter relatert til ulike risikoer som gjensidig påvirker hverandre og øker den samlede risikoen. Et annet eksempel kan være styrken i vår kompetanse og dermed vår evne til å forstå ulike risikoer. I tillegg vil det alltid være rammebetingelser, usikkerhet, forutsetninger og antagelser som danner grunnlaget for et risikobilde. Uten en solid risikoforståelse blir verdien av identifiseringen sterkt redusert (Eriksen et al.,2021).

Risiko, risikostyring, som diskutert i kapittel 3.1 og 3.2, og kartlegging er tett sammenvevd i beredskapsarbeidet, og er sentrale elementer for effektiv håndtering av IKT-relaterte trusler og sårbarheter. Dette inkluderer vurdering av organisatoriske sårbarheter og trusler, spesielt de som kan påvirke IKT-verdiene, og en grundig analyse av usikkerheten knyttet til potensielle konsekvenser - for eksempel et mulig cyberangrep mot Glencore Nikkelverk.

Risikostyring, som er definert som en integrert tilnærming til identifisering, analyse og håndtering av risiko (Aven, 2015), gir en strategisk ramme for organisasjoner å utføre en systematisk og grundig kartlegging av slike risikoer. Dette innebærer en gjennomgående prosess som identifiserer potensielle sårbarheter og trusler, forstår deres potensielle konsekvenser og den usikkerheten som er knyttet til dem, noe som gir en solid grunnmur for utvikling av effektive beredskapsplaner og strategier.

Vurdering

Målet med å vurdere beredskapen er å skape et fundament for valg av passende beredskapstiltak. Disse tiltakene kan variere i både omfang og kvalitet. Det er nødvendig å klargjøre hvilke aspekter av beredskapen som bør vurderes, slik som ulike beredskapsfaser,

nivåer i beredskapsorganisasjonen, spesifikke beredskapssituasjoner eller ressurser, osv. Vurderingsaktiviteter kan inkludere granskning, temamøter og beredskapsanalyser (Eriksen et al.,2021).

Flere organisasjoner utfører ikke nødvendige beredskapsvurderinger og -analyser, og går i stedet direkte fra risiko- og sårbarhetsanalyser til utforming av beredskapsplaner. Dette fører ofte til utilstrekkelig beredskapsforståelse og suboptimale løsninger (Eriksen et al.,2021).

Bruken av beredskapsvurderinger og -analyser ble blant annet fremhevet som en viktig lærdom i koronakommisjonens rapport fra 2021 (Koronakommisjonen, 2021). En grundig vurdering av beredskapen omfatter tre trinn: identifisering, analyse og evaluering.

Det er i denne hovedaktiviteten det gjennomføres en beredskapsanalyse.

Identifiseringsfasen begynner med å velge uønskede situasjoner som krever beredskap, basert på risikokartleggingen. Deretter bestemmer vi hvilke beredskapssituasjoner som skal danne grunnlaget for vurdering av beredskapstiltak, og beskriver dem.

Det andre trinnet i vurderingsprosessen innebærer å utføre planlagte aktiviteter for å samle informasjon og undersøke alternative beredskapsløsninger. Beredskapsanalyser er et effektivt verktøy for å evaluere ulike løsninger innen beredskap. Behovet vil avgjøre hvilke typer beredskapsanalyser som utføres (Eriksen et al., 2021).

Lunde (2019) understreker også betydningen av identifiseringsfasen, som har som mål å klargjøre virksomhetens ambisjoner og mål for beredskapen. Han oppfordrer til å stille spørsmål som: Er virksomheten underlagt spesifikke lover og forskrifter? Hva slags ressurser og tiltak er nødvendige for at virksomheten skal nå sine beredskapsmål? For å svare på disse spørsmålene, foreslår han en beredskapsanalyse som tar hensyn til definerte risiko- og ulykkessituasjoner, krav til beredskap og nødvendige tiltak (Lunde, 2019).

Evaluering er det siste trinnet i vurderingsprosessen. Her evalueres beredskapstiltak og anbefalinger gis til beslutningstakerne. Flere hensyn må tas i betraktning, som ønsket risikonivå, mål innen risikostyring og beredskap, overholdelse av regelverk, kvaliteten på beredskapsløsningene, usikkerhet, helse, miljø og sikkerhet (HMS), samt økonomiske faktorer. Det er ledelsen som bestemmer hvilke beredskapsløsninger organisasjonen skal implementere. Vurderingene må derfor inneholde relevant og solid informasjon, slik at de danner et kunnskapsgrunnlag som gjør ledelsen i stand til å forstå problemstillingene og ta informerte beslutninger (Eriksen et al.,2021).

Forberede

Etter at beredskapsløsningene er besluttet, er neste trinn å forberede implementeringen. Hvis organisasjonen ikke allerede har beredskap på plass, må dette først etableres. Dette kan innebære å utarbeide planer, finne personell til ulike beredskapsroller, gjennomføre opplæring, anskaffe nødvendig utstyr, etablere arbeidsprosesser, etablere samarbeidsrutiner med eksterne aktører og identifisere passende verktøy som skal brukes. Hvis organisasjonen allerede har en beredskap, må den justeres for å tilfredsstille de besluttede løsningene (Eriksen et al.,2021).

Når beredskapen er etablert og justert, er neste trinn å sikre vedlikehold. Dette innebærer å etablere administrative rutiner, som å gjennomgå og oppdatere beredskapsvurderinger og planverk. Andre viktige forberedelsesaktiviteter inkluderer opplæring, trening og øvelser for å sikre at beredskapen fungerer som den skal og at alle involverte parter er forberedt på potensielle kriser (Eriksen et al.,2021).

Håndtering

Når en beredskapssituasjon oppstår, enten gradvis eller plutselig, er det nødvendig å iverksette en tilpasset beredskapsrespons. I slike situasjoner er det essensielt å handle raskt, og vår evne til å forstå situasjonen blir kritisk for en vellykket håndtering. Det vil alltid være nødvendig å justere og tilpasse responsen til den aktuelle situasjonen, og derfor er det viktig at beredskapen er fleksibel og robust (Eriksen et al.,2021).

En sentral oppgave i håndteringen er å etablere og opprettholde en god forståelse av situasjonen, inkludert hva som har skjedd, hva som skjer og en vurdering av potensielle konsekvenser. Deretter må vi utforme og implementere en plan som er spesifikk for den aktuelle situasjonen, som adresserer potensielle utfordringer og trusler. Planen kan inneholde ulike elementer, som varsling og mobilisering av involverte parter og ressurser, evakuering og sikring av områder, håndtering av krisen, omsorg for berørte personer, krisekommunikasjon og opprettholdelse av drift (Eriksen et al.,2021).

Etter hvert som planen iverksettes, må vi evaluere om den oppnår ønsket effekt og justere den ved behov for å sikre en effektiv respons på den pågående situasjonen (Eriksen et al.,2021).

Gjenopprette

Uønskede hendelser kan ha betydelig innvirkning på organisasjoner og kan ofte kreve omstilling. Organisasjonen må tilpasse seg endrede forhold og en ny risikooppfatning. Det

kan også bli nødvendig med langvarige endrings- og læringsprosesser. Når krisen avtar, vil det ofte være ulike aspekter som må håndteres og avklares, for eksempel driftskontinuitet, juridiske spørsmål, ansvars- og strafferettslige forhold, tillit, omdømme og medieoppmerksomhet, støtte til berørte personer, gjenopprettelse av tjenester, fasiliteter og infrastruktur, og lignende (Eriksen et al.,2021).

Gjenopprettelsesfasen innebærer også å utnytte muligheter og skape gevinster for organisasjonen, som nye markeder, innovative løsninger, nye arbeidsprosesser og metoder, samt nye samarbeidspartnere. Slike faktorer kan ha betydelig strategisk innflytelse og kreve betydelige ressurser. Det kan derfor være nødvendig å organisere gjenopprettelsesarbeidet som en prosjektgruppe med relevant personell. Uten en solid struktur og tilstrekkelige ressurser kan gjenopprettelsesprosessen bli tilfeldig og utilstrekkelig (Eriksen et al.,2021).

Læring

Selv om organisasjoner heldigvis opplever et begrenset antall krisesituasjoner, betyr dette også at erfaringene innen beredskap er begrensede. Dette gjelder selv for nødetater, som dermed må lære av andre. Læring er en vesentlig del av beredskapsprosessen, både fra andre og fra egen organisasjon (Eriksen et al.,2021).

For å lære av andre må det settes av tid til å innhente informasjon og erfaringer. Dette innebærer å lese dokumenter og snakke med personer som kan dele sine opplevelser fra krisesituasjoner. Disse situasjonsspesifikke erfaringene må deretter generaliseres for å kunne brukes i nye sammenhenger og overføres til varige endringer i egen organisasjon (Eriksen et al.,2021).

Læring bør tilrettelegges på individ-, team- og organisasjonsnivå, samt mellom organisasjoner. Læring er relevant for alle aspekter av beredskapsarbeidet, inkludert prinsipper, rammeverk og prosesser. Spesielt i forbindelse med opplæring, trening og øvelser er det viktig å sikre læring, men læring foregår kontinuerlig i alle deler av beredskapsarbeidet.

En vellykket læreprosess i organisasjoner krever en langvarig forpliktelse og engasjement fra alle involverte (Eriksen et al.,2021).

Ifølge Lunde (2019) har dokumentert beredskap liten verdi dersom man ikke samtidig etablerer en reell beredskapsevne ved å lære opp, trene og øve mannskapene som skal utøve beredskapen i virksomheten. Dette bør skje på individ-, gruppe-, og organisasjonsnivå.

Perry og Lindell (2003) understreker også viktigheten av trening og samhandling i deres retningslinjer for god beredskap. Når en krise oppstår vil det vanligvis involvere flere interessenter, eller såkalte stakeholders. Disse kan være kommuner, nødetater, eller nabobedrifter. Det er viktig at disse interessentene kjenner hverandres oppdrag, organisasjon, og strukturer for å kunne dra nytte av hverandre og samarbeide effektivt. Viktigheten av trening som en komponent i beredskapsplanlegging blir også understreket av Perry og Lindell (2003). Trening vil være en effektiv måte å få tilbakemelding på om planene faktisk fungerer og gjøre «dokumentene levende».

Øvelser og evne til læring spiller en viktig rolle i beredskapskontekst. Som en nøkkelkomponent i beredskapsprosessen, bidrar trening og øving betydelig til å forbedre kriserespons og styrke samfunnssikkerheten. Forskningslitteraturen bekrefter entydig at øvelser forsterker folks evne til å takle utfordrende og krevende situasjoner på en effektiv måte (Sommer et al.,2020).

Samtidig peker flere studier på en utfordring i beredskapsorganisasjoner – deres vanskeligheter med å trekke lærdom fra erfaringer og feil som oppstår under håndtering av hendelser (Sommer et al.,2020). Dette aspektet belyser at det er et særlig behov for kontinuerlig forbedring og systematisk læring i disse organisasjonene.

Organisasjonslæring er et bredt begrep med ulike definisjoner (Sommer et al., 2020). Argyris og Schon (1978, 1996), referert i Sommer et al. (2020), presenterer en fremtredende definisjon av organisasjonslæring. De argumenterer for at organisasjonslæring skjer når individer innad i en organisasjon står overfor en problematisk situasjon og gransker disse problemene for organisasjonens del. For at denne læringen skal betraktes som organisatorisk, må resultatene fra disse undersøkelsene inkorporeres i medlemmenes kollektive kunnskapsbase og forståelse, og/eller i organisasjonens prosedyrer, rutiner og lignende.

Denne forståelsen av organisasjonslæring korresponderer med Garvins (1993) syn, også sitert i Sommer et al. (2020), på hva som utgjør en lærende organisasjon. Han definerer en lærende organisasjon som *"en organisasjon som er flink til å skape, anskaffe og formidle kunnskap, og til å endre sin adferd basert på ny innsikt og informasjon."*

Dette innbefatter to hovedelementer av organisasjonslæring i beredskapskontekst: kunnskap og handling. Læring blir sett på som en prosess som fører til endringer i praksis (Sommer et al., 2020). Det innebærer å transformere tilegnet kunnskap til handling som bidrar til å forbedre beredskap og krisehåndtering, dermed skaper organisasjonen en forbedret og mer

effektiv responsstrategi. Denne kontinuerlige læringsprosessen er sentral for beredskapsarbeid, hvor organisasjonen aktivt søker å lære fra tidligere erfaringer og hendelser for å øke sin kapasitet til å håndtere fremtidige beredskapssituasjoner (Sommer et al., 2020).

Systematisk forbedring

Beredskap er et dynamisk fagfelt som stadig utvikler seg, med flere nye perspektiver og har mye å lære fra andre disipliner som organisatorisk læring, digitalisering, risikostyring og samfunnssikkerhet. Beredskapen vår er også basert på forutsetninger, antagelser, risikoforståelse og forventninger som er etablert i samfunnet. Siden disse forholdene kontinuerlig endres, vil det påvirke kravene til beredskapens kvalitet.

Som en del av et systematisk beredskapsarbeid, er det nødvendig å gjennomføre regelmessige gjennomganger for å sikre at både beredskapen og arbeidsmetodene er tilfredsstillende. Det er spesielt viktig å vurdere om endringer i omgivelsene, som for eksempel risiko og forventninger til beredskapen, krever justeringer.

Organisasjoner må derfor etablere og opprettholde rutiner for kontinuerlig forbedring av beredskapen, slik at de kan tilpasse seg endringer og opprettholde en høy kvalitet på sitt beredskapsarbeid (Eriksen et al.,2021).

Prinsippet om kontinuerlig forbedring er ifølge Lunde (2019) en sentral del av modellen for etablering av beredskapsplaner, hvor det anerkjennes at selv om en tilfredsstillende beredskap er etablert, må dette sees på som en gjentakende prosess (Lunde, 2019).

Perry og Lindell (2003) understreker også at arbeidet med beredskapsplaner bør være en pågående prosess, og at det aldri er et tidspunkt hvor planleggingen er fullført. *«There is never a time when planning is completed»* (Perry og Lindell 2003: 346). Manglende verifikasjon kan få store konsekvenser, selv om en tilsynelatende tilfredsstillende beredskap er dokumentert skriftlig. Planer som ikke blir revidert og testet i praksis, kan gi et urealistisk bilde av virkeligheten å bli brukt som en falsk forsikring om at situasjonen er under kontroll. Clarke og Perrow (1996) betegner denne typen planer som «fantasy documents».

Organisatorisk læring er ikke en selvgående prosess. Det krever et fastsatt system som sikrer at læring foregår systematisk og regelmessig i organisasjonen. Et læringssystem kjennetegnes av organisatoriske strukturer og aktiviteter som legger til rette for vurdering og dialog om tidligere erfaringer, og som fremmer spredning og deling av informasjon, så vel som endringer i kunnskap og praksis (Sommer et al., 2020).

En effektiv metode for å implementere dette i praksis er å etablere en såkalt lukket styringssløyfe, et konsept innen kvalitetsledelse som sikter mot kontinuerlig forbedring. En lukket styringssløyfe er en tilbakevendende prosess hvor organisasjonen fastsetter mål, utfører handlinger for å nå disse målene, måler resultater, og foretar justeringer basert på disse resultatene. Denne syklusen gjentas deretter kontinuerlig for å sikre vedvarende forbedring og læring (Sommer et al., 2020).

Å fokusere på erfaringslæring, det vil si læring fra direkte eller indirekte erfaring, er også viktig i denne sammenheng. Erfaringslæring kan fremme innsikt og forståelse som går ut over det som kan oppnås gjennom formell opplæring, og kan dermed bidra til å styrke organisasjonens evne til å håndtere fremtidige beredskapssituasjoner. Kombinasjonen av en lukket styringssløyfe og erfaringslæring kan derfor bidra til å sikre systematisk og kontinuerlig læring innad i organisasjonen (Sommer et al., 2020).

3.7 Oppsummering av teori

Teorikapittelet presenterer anerkjente tilnærminger til beredskapsarbeid og etablering av beredskap. Selv om tilnærmingene er presentert forskjellig, er det flere likheter mellom dem. Alle de nevnte teoriene fokuserer på beredskapsplanlegging og understreker viktigheten av kontinuerlig forbedring og en systematisk tilnærming.

De fremhever alle viktigheten av trening og samhandling for å sikre effektiv beredskap. Dette omfatter opplæring og øvelser på individ-, gruppe- og organisasjonsnivå, samt samarbeid mellom interessenter og aktører for å sikre en koordinert og effektiv respons i krisesituasjoner. Teoriene vektlegger også nødvendigheten av å evaluere og verifisere beredskapsevnen ved hjelp av øvelser og tester. Dette sikrer at planene er praktiske og effektive, og bidrar til å identifisere eventuelle svakheter og forbedringsområder.

Når vi vender oss mot våre forskningsspørsmål, kan vi se at den presenterte teorien gir et godt fundament for å utforske disse problemstillingene.

3.7.1 Sårbarheter og trusler

Forskningsspørsmål 1, om hvilke sårbarheter og trusler som er mest fremtredende for IKT-verdiene ved Glencore Nikkelverk og hvordan disse kan påvirke bedriften, er relevant for å vurdere risikoen knyttet til informasjons- og kommunikasjonsteknologien som brukes i virksomheten. Det er viktig å identifisere og forstå disse sårbarhetene og truslene for å kunne utvikle effektive tiltak for å beskytte bedriftens IKT-verdier og sikre kontinuitet i virksomheten.

Teknologisk utvikling og avhengighet av digitale systemer, som sett i sammenheng med Industri 4.0, har ført til økt sårbarhet og trussel for dataangrep (Ghobakhloo & Iranmanesh, 2021). For å beskytte seg mot slike angrep er det nødvendig med omfattende cybersikkerhetstiltak, inkludert risikovurdering og implementering av sikkerhetsteknologier (Ghobakhloo & Iranmanesh, 2021). Dette er relevant for å vurdere sårbarheter og trusler mot IKT-verdiene ved Glencore Nikkelverk, da industrien stadig blir mer avhengig av digitale systemer for å oppnå økt effektivitet og fleksibilitet (Ghobakhloo & Iranmanesh, 2021). Politiets trusselvurdering (POD, 2022) understreker også behovet for å beskytte seg mot datainnbrudd og datatyveri, spesielt for virksomheter med samfunnskritiske funksjoner.

Sårbarhetsbegrepet er relevant for å forstå konsekvensene av dataangrep og behovet for å redusere sannsynligheten for uønskede hendelser og minimere konsekvensene av dem (Lunde, 2019). Eriksen et al. (2021) definerer sårbarhet som *«et systems evne til å motstå uønskede hendelser og manglende evne til å gjenoppta sin funksjon.»* Sårbarhetsanalyser kan brukes til å identifisere og vurdere sårbarheter i et system (Eriksen et al., 2021). Dette er relevant for å analysere hvilke sårbarheter og trusler som er mest fremtredende for IKT-verdiene ved Glencore Nikkelverk og hvordan de kan påvirke bedriften.

Sheila Jasanoff (2018) sin studie om sårbarhet i teknologiske kulturer bidrar til å forstå hvordan teknologi og samfunn påvirker hverandre gjensidig. Studien viser hvordan økt avhengighet av teknologi og systemer kan gjøre samfunnet sårbart for feil, mangler og manglende ressurser. Dette er relevant for å forstå konsekvensene av sårbarheter og trusler knyttet til digitale systemer og teknologi i Glencore Nikkelverk, da sårbarhetene kan påvirke samhandlingen mellom teknologi og samfunn og føre til økt sårbarhet (Jasanoff, 2018).

For å håndtere sårbarheter og redusere risiko er en helhetlig tilnærming til risikostyring nødvendig (ISO, 2018). Dette kan innebære tekniske og organisatoriske tiltak, som økt

sikkerhet og implementering av sikkerhetsprosedyrer (ISO, 2018). Lunde (2019) understreker viktigheten av å beskytte seg mot tilsiktede handlinger, spesielt når det gjelder cyberangrep, da sårbarhetene knyttet til slike angrep kan være alvorlige. En bevisstgjøring om sårbarhetene og implementering av kontinuerlig risikostyring kan bidra til å redusere risikoen (Lunde, 2019).

For å svare på forskningsspørsmålet om hvilke sårbarheter og trusler som er mest fremtredende for IKT-verdiene ved Glencore Nikkelverk og hvordan de kan påvirke bedriften, er det nødvendig å analysere sårbarhetene knyttet til digitalisering og avhengighet av IKT-systemer. Dette inkluderer identifisering av potensielle trusler og konsekvensene de kan ha for bedriftens drift og verdikjede.

Det er også viktig å ta hensyn til kompleksiteten og samproduksjonen mellom teknologi og samfunn, som Sheila Jasanoff (2018) påpeker. Hennes studie viser hvordan sårbarhet og samproduksjon er relevante for kriseberedskap og respons, og at en integrert tilnærming til planlegging og ressursallokering er nødvendig. Dette er relevant for å forstå hvordan sårbarheter og trusler kan påvirke Glencore Nikkelverk, da bedriften er avhengig av teknologi og samfunnsmessige faktorer for sin drift.

Ved å kombinere perspektiver fra Ghobakhloo & Iranmanesh (2021), Politiets trusselvurdering (POD, 2022), Eriksen et al. (2021), Lunde (2019), Jacobsen & Repstad (2004) og Jasanoff (2018), kan man få en helhetlig forståelse av sårbarheter og trusler knyttet til IKT-verdiene ved Glencore Nikkelverk. Dette kan danne grunnlaget for å utvikle tiltak og strategier for å redusere sårbarheter og håndtere potensielle trusler på en effektiv måte.

3.7.2 Teori og rammeverk

Forskningsspørsmål 2 tar for seg teorier, rammeverk, utfordringer og muligheter for Glencore Nikkelverk. Teorier og rammeverk for håndtering av cyberhendelser, som utformet av Eriksen et al. (2021), er høyst relevante for å adressere forskningsspørsmålet om i hvilken grad slike teorier og rammeverk er implementert i praksis hos Glencore Nikkelverk. De fungerer som et nyttig verktøy for evaluering av virksomhetens nåværende tiltak, samt for å identifisere muligheter for forbedring.

Disse teoriene og rammeverkene kan fungere som et mål eller standard for å evaluere i hvilken grad Glencore Nikkelverk har implementert passende tiltak for å håndtere cyberhendelser. Ved å sammenligne virksomhetens nåværende praksis med anbefalingene i teorien, kan man vurdere effektiviteten av virksomhetens strategier og identifisere potensielle områder for forbedring.

Teorier og rammeverk kan også være nyttige for å identifisere potensielle utfordringer som kan hindre effektiv implementering. Forståelse av disse utfordringene, som kan være av organisatorisk, teknisk eller kulturell natur, kan hjelpe virksomheten med å utvikle strategier for å overvinne dem.

På samme måte kan disse teoriene og rammeverkene bidra til å identifisere muligheter for forbedring. Dette kan omfatte potensielle tiltak for å forbedre teknologiske løsninger, opplæring og trening, eller organisatoriske strukturer.

Til slutt kan teorier og rammeverk for håndtering av cyberhendelser gi veiledning til Glencore Nikkelverk om hvordan de kan forbedre implementeringen av tiltak for å håndtere slike hendelser i fremtiden. De kan tilby innsikt i beste praksis, effektive strategier og potensielle fallgruver å unngå.

Dermed bidrar teorien av Eriksen et al. (2021) til å forstå og evaluere implementeringen av tiltak for å håndtere cyberhendelser ved Glencore Nikkelverk, samtidig som den understreker viktige områder for potensiell forbedring.

3.7.3 Evaluering og organisatorisk læring

Når det gjelder forskningsspørsmål 3, er det teorier om organisatorisk læring, trening og øvelser som er mest relevante. Her aktualiseres begreper som erfaringslæring, lukket styringssløyfe og systematisk forbedring av beredskap (Argyris & Schon, 1978; Sommer et al., 2020). Disse konseptene hjelper organisasjoner med å utvikle, implementere og evaluere trening- og øvelsesprogrammer, samt med å integrere lærdom fra disse programmene i deres fremtidige beredskapsarbeid.

Sammen bidrar disse teoriene til en forståelse av hvordan organisasjoner som Glencore Nikkelverk kan bygge en robust beredskap mot cyberhendelser. Fra identifisering og vurdering av sårbarheter og trusler, til implementering av passende beredskapsrammeverk og

systematisk forbedring av organisatorisk læring, gir disse teoriene veiledning om hvordan organisasjoner kan forberede seg på, reagere på, og gjenopprette fra cyberhendelser.

Mens Perry & Lindell gir generelle retningslinjer og prinsipper for god beredskap, tilbyr Lunde (2019) og Eriksen et al. (2021) mer detaljerte modeller og faser knyttet til etablering av beredskap. Selv om alle teoriene inkluderes i studien, vil datainnsamling og drøfting hovedsakelig basere seg på Eriksen et al. (2021).

4. Design og metode

I dette kapittelet beskrives forskningsdesignet og metodikken som ligger til grunn for oppgaven. For å sikre studiens troverdighet vil det også reflekteres over både styrker og svakheter ved valgene som er gjort, samt vurdere i hvilken grad kvalitet er ivaretatt.

4.1 Forskningsdesign

Forskningsdesign refererer til prosessen som knytter sammen forskningsspørsmål, empirisk data og forskningskonklusjoner (Blaikie & Priest, 2019). Forskningsdesignet innebærer å ta ulike valg og overveielser før og under gjennomføringen av forskningen, inkludert å besvare spørsmål som hva som skal studeres, hvorfor det skal studeres, og hvordan det skal studeres. I dette tilfellet er hensikten med studien å undersøke hvordan Glencore Nikkelverk kan etablere god beredskap for cyberhendelser.

Teorier som er valgt ut for denne studien er nøye vurdert for å bidra til å besvare problemstillingen, som krever en forståelse av hva beredskap er og teorier knyttet til etablering av beredskap. For å samle data som kan belyse problemstillingen, benyttes en kvalitativ metode med semistrukturerte intervjuer av seks informanter. Informantene er valgt ut basert på deres stilling og ansvarsområder i bedriften.

Funnene fra intervjuene vil bli drøftet i lys av den valgte teorien. Det er viktig å merke seg at studien fokuserer på informantenes utsagn om hvordan de håndterer problemstillingen, og det foretas ingen direkte observasjon av arbeidet som utføres. Imidlertid har forskeren, som ansatt ved virksomheten, innsikt i deler av problemstillingen og kan i noen grad verifisere informasjonen som kommer frem i intervjuene.

For å utforske problemstillingen: «Hvordan kan Glencore Nikkelverk etablere god beredskap for cyberhendelser?», er en kvalitativ forskningsmetode valgt som den mest hensiktsmessige tilnærmingen. Kvalitative metoder er særlig egnet når forskningsspørsmålene søker å utforske komplekse fenomener i dybden, der kontekst og prosesser er avgjørende for å forstå de observerbare fenomenene (Blaikie & Priest, 2019).

Dette gjelder særlig for problemstillingen i denne studien, som krever en forståelse av den organisatoriske konteksten, inkludert individers holdninger, erfaringer, kunnskaper og oppfatninger rundt cyberhendelser. I tillegg er problemstillingen sammensatt og flerdimensjonal, noe som innebærer at den ikke kan undersøkes effektivt gjennom enkle målinger.

Videre kan den kvalitative tilnærmingen tillate forskeren å belyse potensielle tiltak og strategier for å forbedre cyberberedskapen ved Glencore Nikkelverk, noe som er et sentralt mål for studien. Dette kan oppnås ved å trekke på informantenes kunnskap og erfaring, samt å diskutere og drøfte funnene i lys av relevant teori.

Samlet sett er den valgte kvalitative metoden relevant og hensiktsmessig for problemstillingen i denne studien, da den gir mulighet for en dyp, kontekstspesifikk forståelse av temaet for forskningen.

Forskningsdesignet er dermed tilpasset problemstillingen og forskningsspørsmålene. Ved slutten av studien vil det presenteres en konklusjon, inkludert forslag til videre forskning.

4.2 Metodevalg

Denne oppgaven bygger på en kvalitativ forskningsmetode. Som en primær metode for datainnsamling har semistrukturerte intervjuer blitt benyttet. I tillegg til disse intervjuene, har dokumentanalyse tjent som et supplement.

Dokumentanalyse gir mulighet for å undersøke eksisterende dokumenter og arkiverte data, i dette tilfellet relatert til bedriftens eksisterende beredskapssystemer, rapporteringskjede, sikkerhetspolicyer, prosedyrer og hendelsesrapporter.

Hensikten med denne kombinerte tilnærmingen er å utnytte dokumentanalysen til å danne et bilde av hva bedriften har dokumentert og etablert, for deretter å supplere dette med innsikt

fra intervjuer med nøkkelinformanter for å dekke eventuelle kunnskaps gap. Kvalitative metoder gir en fleksibel tilnærming, der de ulike fasene i forskningsprosessen kan overlappe og gi en mer helhetlig forståelse (Halvorsen, 2008, s. 131).

Studiet adresserer problemstillingen: "Hvordan kan Glencore Nikkelverk etablere god beredskap for cyberhendelser?" Med tanke på kompleksiteten og potensielle utfordringer ved å adressere denne problemstillingen direkte, har det vært nødvendig å plassere problemstillingen i en kontekst. Denne konteksten hjelper til med å bryte ned problemstillingen i mer håndterbare deler og sammenligne dataene samlet inn gjennom intervjuene med relevant teori og dokumentanalyse (Blaikie & Priest, 2019).

Semistrukturerte intervjuer med seks informanter tillater en fleksibel tilnærming der oppfølgingsspørsmål kan stilles for å oppnå dypere forståelse og avklaring av eventuelle misforståelser. Ifølge Johannessen et al. (2016), er kvalitative metoder godt egnet for å samle mer detaljert og nyansert informasjon, noe som er nødvendig i dette studiet.

Forskningsspørsmålene har blitt utviklet for å tydeliggjøre og presisere problemstillingen:

1. "Hvilke sårbarheter og trusler er mest fremtredende for IKT-verdiene ved Glencore Nikkelverk, og hvordan kan disse potensielt påvirke bedriften?"

   Dette forskningsspørsmålet sikter mot å kartlegge og forstå det unike landskapet av cyber-risikoer som Glencore Nikkelverk står overfor. Det er avgjørende å identifisere og analysere disse spesifikke sårbarhetene og truslene for å kunne utforme en robust og effektiv beredskapsplan. Dermed blir forståelsen av disse potensielle risikoene grunnlaget for å utvikle passende og målrettede beredskapsstrategier.

2. "I hvilken grad er teorier og rammeverk for cyberhendelser implementert i praksis hos Glencore Nikkelverk, og hvilke utfordringer og muligheter kan identifiseres i forbindelse med dette?"

   Hensikten her er å evaluere hvordan Glencore Nikkelverk har omfavnet og implementert beredskapsplaner for cyberhendelser, i samsvar med etablerte teorier og beste praksis på feltet. Videre søkes det å identifisere eventuelle hindringer som kan hemme effektiv implementering, samt å avdekke potensielle muligheter for forbedring og optimalisering av disse beredskapsstrategiene.

3. "Hvordan utformer og evaluerer Glencore Nikkelverk trenings- og øvelsesprogrammer for å forberede de ansatte på å håndtere cyberhendelser, og hvilke prosesser og metoder benyttes for systematisk forbedring av beredskapen mot cyberhendelser?"

   Dette forskningsspørsmålet retter seg mot bedriftens innsats for å bygge og opprettholde sin interne kapasitet for å møte cyberhendelser effektivt. Det gir muligheten til å bedømme hvordan disse programmene er konstruert, implementert, og evalueres, samtidig som det avdekker metoder og prosesser for kontinuerlig forbedring av beredskapen mot cyberhendelser. Dette vil gi grunnlag for å foreslå potensielle forbedringer og optimalisering av disse prosessene.

Disse forskningsspørsmålene gir mulighet til å utforske den større problemstillingen, samtidig som de skaper en struktur for datainnsamling og analyse.

Dokumentanalyse og semistrukturerte intervjuer er valgt som forskningsmetoder i dette studiet av en rekke årsaker. Disse metodene gir dybde, detalj og kontekst, som er vesentlig for en omfattende tilnærming til problemstillingen. Dette reflekteres i Halvorsens (2008) betraktninger om kvalitative metoders evne til å lede til en mer helhetlig forståelse, da forskningsprosessen er fleksibel og tillater overlapp mellom ulike faser.

Dokumentanalyse fungerer som en kunnskapsbase, som gir forskeren en inngående forståelse av beredskapen for cyberhendelser ved Glencore Nikkelverk. Denne kunnskapsbasen benyttes som fundament for å analysere og tolke funnene fra de semistrukturerte intervjuene.

Valget av semistrukturerte intervjuer tillater forskeren å dykke dypere inn i informantenes perspektiver, oppfatninger og erfaringer. I dette studiet er det spesielt viktig å forstå hvordan eksisterende beredskapssystemer brukes for å håndtere cyberhendelser, da det krever innsikt i informantenes personlige oppfatninger og fortolkninger. Metoden gir forskeren fleksibilitet til å stille oppfølgingsspørsmål, noe som bidrar til en dypere forståelse av temaet, og muligheten til å avklare eventuelle uklarheter (Johannessen et al., 2016).

I denne konteksten kan observasjon være en mindre egnet metode, ettersom cyberberedskap er et komplekst felt som ikke alltid er synlig eller lett å observere. Beredskapen er forankret i rammeverk, prosedyrer, systemer og holdninger, som ikke nødvendigvis kan observeres direkte.

Når det gjelder utvalg av informanter, er det anvendt en bevisst utvalgsstrategi for å sikre relevans og variasjon. Informantene har forskjellige roller og ansvarsområder knyttet til sikkerhet og beredskap, også ved cyberhendelser. Dette sikrer et bredt spekter av perspektiver og kunnskaper, som er avgjørende for å svare på forskningsspørsmålene på en balansert og omfattende måte (Johannessen et al., 2016).

Dette studiet fokuserer på problemstillingen: «Hvordan kan Glencore Nikkelverk etablere god beredskap for cyberhendelser?». For å adressere denne problemstillingen på en effektiv måte er det nødvendig å plassere den i riktig kontekst. Det innebærer å forstå virksomhetskulturen hos Glencore Nikkelverk, de aktuelle sikkerhetsutfordringene og de beredskapssystemer som er på plass. Metodevalgene – dokumentanalyse og semistrukturerte intervjuer – støtter denne tilnærmingen ved å tillate forskeren å innhente informasjon fra et bredt spekter av kilder og perspektiver.

Forskningsspørsmålene bidrar til å konkretisere og presisere problemstillingen ved å dele den inn i mindre, mer håndterbare enheter. Disse forskningsspørsmålene er konstruert for å styre datainnsamlingen og analysen mot å belyse de spesifikke aspektene av problemstillingen. De inkluderer spørsmål om hvilke sårbarheter og trusler som er mest fremtredende for IKT-verdiene ved Glencore Nikkelverk, og hvordan teorier og rammeverk for cyberhendelser er implementert i praksis.

For å svare på forskningsspørsmålene og adressere problemstillingen er det nødvendig å sammenligne data samlet inn under intervjuene med den valgte teorien og de analyserte dokumentene. Dette kan gi en dypere forståelse av hvordan Glencore Nikkelverk håndterer cyberberedskap, inkludert deres tilnærming til risikovurdering, opplæring og øvelser, samt forbedringsprosesser.

Ved å sette problemstillingen i en spesifikk kontekst og ved å bruke forskningsspørsmålene til å guide datainnsamling og analyse, sikres det at metodevalget bidrar til en relevant undersøkelse av problemstillingen.

4.3 Datainnsamling

Valget av datainnsamlingsmetode i denne studien er basert på hva som best kan belyse de problemstillingene og temaene oppgaven søker å utforske (Jacobsen, 2018). Kvalitative metoder legger vekt på informantenes perspektiver og erfaringer, noe som kan være spesielt verdifullt for å forstå komplekse problemstillinger og kontekster. Begrensninger knyttet til tid og ressurstilgjengelighet innenfor oppgavens rammer har også vært avgjørende faktorer ved valget av metode.

Valget av informanter er basert på en bevisst utvalgsstrategi, der hver informant anses som relevant og innsiktsfull i henhold til studiens mål. Alle informantene har roller som innebærer ansvar eller oppgaver knyttet til sikkerhet og beredskap mot cyberangrep. Informantene har en variert og relevant bakgrunn, noe som sikrer en betydelig grad av variasjon, da de besitter ulik kunnskap og erfaring (Johannessen et al., 2016, s. 113).

Tabellen gir en oversikt over informantenes erfaring og deres funksjoner i virksomheten.

Informant	**Funksjon i virksomheten**	**Antall år i virksomheten**	**Dato**
A	Direktør- har rolle i krisestab	>20 år	24.04.23
B	Direktør- har rolle i krisestab	>20 år	26.04.23
C	Direktør- har rolle i krisestab	<10 år	02.05.23
D	Beredskapsrådgiver	<5 år	25.04.23
E	Leder ved IT-avdelingen	>25 år	27.04.23
F	Leder ved IT-avdelingen	<5 år	03.05.23

Intervjuene ble gjennomført på en semistrukturert måte, noe som innebærer at spørsmålene som ble stilt var relativt åpne og ga informantene mulighet til å reflektere rundt temaene som ble tatt opp. Hensikten med en semistrukturert tilnærming var å la informantene selv komme med relevant informasjon, også rundt temaer og forhold som falt utenfor de direkte spørsmålene som ble stilt, men som likevel var relevante. Dette valget ble også gjort for å unngå å avsløre sårbarheter som kunne utnyttes ved publikasjon eller avsløre klassifisert informasjon som ikke kunne deles.

Ved å tillate informantene å snakke fritt, kunne oppfølgingsspørsmål stilles basert på informasjon som fremkom underveis. I tillegg kunne informasjon gitt av andre informanter brukes til å stille spørsmål om en informant kjente seg igjen i en annen informants refleksjoner rundt et tema, noe som bidro til en mer helhetlig forståelse av problemstillingen.

Intervjuguiden var strukturert i fem deler for å organisere intervjuene på en systematisk måte. Hver av disse delene var nøye knyttet til forskningsspørsmålene.

1. Den første delen av intervjuguiden fokuserte på bakgrunnsinformasjon, samt informantenes erfaring og oppfatning av beredskapssystemer. Dette ga et grunnlag for å forstå informantenes perspektiver og erfaringer.

2. Den andre delen av intervjuguiden omhandlet forståelsen av cyberhendelser, samt trusler og sårbarheter knyttet til dette. Dette bidro til å gi innsikt i hvordan informantene oppfattet og vurderte cybertrusler og deres potensielle konsekvenser.

3. Den tredje delen fokuserte på bedriftens prosesser knyttet til risiko- og beredskapsanalyser for cyberhendelser og tilhørende planverk. Her ble muligheten for å tilpasse eller benytte eksisterende systemer for også å gjelde cyberhendelser belyst.

4. Del fire handlet om i hvilken grad bedriften gjennomfører trening eller øvelser knyttet til cyberhendelser, samt hvordan disse eventuelt evalueres og blir en del av et system for kontinuerlig forbedring. Dette ga innsikt i bedriftens praksis og fokus på opplæring og øvelser.

5. Del fem oppsummerte og syntetiserte informasjonen fra de fire første delene. Her ble informantene bedt om å komme med anbefalinger for fremtidige tiltak for å etablere eller forbedre et effektivt beredskapssystem for cyberhendelser, samt hva de mente skulle til for å opprettholde et slikt system. Informantene fikk også anledning til å komme med innspill om det var noen temaer de mente var viktige i forbindelse med etablering av beredskap for cyberhendelser, som ikke hadde blitt diskutert tidligere i intervjuet.

Etter avslutningen av hvert intervju, ble notater nøye gjennomgått og svarene strukturert skriftlig. Målet med denne umiddelbare gjennomgangen var å sikre at informasjonen var fersk i minnet, slik at alle detaljer og sitater ble presist og korrekt registrert. I tillegg var det viktig å unngå forvirring mellom informantenes svar. Dette skrittet var viktig for å beholde klarheten og integriteten i dataene samlet inn gjennom intervjuene.

Under studien ble det klart at Glencore Nikkelverk hadde begrenset dokumentasjon direkte relatert til cyberhendelser. Dette førte til at dokumentanalysen ikke spilte en så fremtredende rolle i forskningen som først antatt. De tilgjengelige dokumentene fungerte primært som bekreftelse på hva bedriften selv hadde identifisert, knyttet til cyber-risiko. Det ble også pekt på nødvendige dokumenter som ennå ikke var blitt implementert. Gitt denne situasjonen, ble det vurdert som lite hensiktsmessig å gjennomføre en detaljert analyse av dokumentene i forhold til manglende implementering. Dermed ble dokumentanalysen tilpasset de faktiske forholdene og begrenset i omfang til tross for sin opprinnelige forventede betydning.

4.4 Datainnsamlingens utfordringer

Forskerens rolle som ansvarlig for sikkerhet og beredskap ved Glencore Nikkelverk kan medføre både fordeler og utfordringer knyttet til dataanalysen. På den ene siden kan engasjement og endringslyst knyttet til beredskap og problemstillingen bidra til en dypere forståelse av temaet (Jacobsen & Repstad, 2004). Forskerens kjennskap til bedriften og ønsket om å bidra til at bedriften følger beste praksis kan også være en fordel.

På den andre siden kan engasjementet medføre en mulig feilkilde ved at det fungerer styrende for konklusjonen, samt at forskeren kan påvirkes av forutfattede meninger og fordommer (Jacobsen & Repstad, 2004). En annen utfordring kan være å gjengi en usminket sannhet, da det kan stilles spørsmål ved om forskeren klarer å fremstille data på en korrekt måte eller om negative funn begrenses.

Alle informantene i studien er ansatt i stillinger med strategisk, overordnet eller teknisk ansvar for sikkerhet og beredskap knyttet til cyberhendelser. Derfor kan det også være utfordringer knyttet til om informantene svarer det de oppriktig mener eller om de forsøker å glatte over eventuelt forbedringspotensiale (Jacobsen & Repstad, 2004). Informantenes ærlighet og åpenhet er viktig for å sikre validitet i studien.

Ved en kvalitativ tilnærming er det rom for feiltolkning, ettersom subjektive oppfatninger blir kommunisert (Jacobsen & Repstad, 2004, s. 239). For å minimere risikoen for feiltolkning har forskeren tatt hensyn til dette ved å oppsummere det informantene har sagt og kontrollere at informasjonen er forstått riktig.

Forskerens rolle i bedriften kan også være en fordel ved intervju av informanter, da det vil være vanskelig å glatte over sannheten, og det vil være lettere å få fram et eventuelt skille mellom ord og handling (Jacobsen & Repstad, 2004, s. 240). Forskeren vil også være bedre rustet til å stille utdypende spørsmål, da han kjenner hverdagsspråket og pågående prosesser i bedriften (Jacobsen & Repstad, 2004). Dette har vært en fordel i forhold til samtlige informanter i studien og har bidratt til en mer kvalitetssikret prosess for utvalg og intervju av informanter.

4.5 Studiens troverdighet

I dette kapittelet vil det bli reflektert over valgene som er gjort angående forskningsdesign og metode, med fokus på å vurdere troverdigheten av den presenterte empirien samt fordeler og ulemper ved den anvendte metoden. Det er viktig å reflektere over og evaluere kvaliteten på en studie, uavhengig av hvilke metoder som er benyttet (Johannessen et al., 2016, s. 231). I kvantitativ forskning benyttes ofte begrepene reliabilitet og validitet for å vurdere kvaliteten i studien. Imidlertid vil Lincoln og Guba sine kvalitetsbegreper bli lagt til grunn i denne diskusjonen, da de gir et bedre grunnlag for å vurdere kvalitative undersøkelser som er anvendt i denne studien (Lincoln & Guba, 1985).

Begrepet "trustworthiness" er sentralt, med de fire kvalitetsbegrepene troverdighet, overførbarhet, pålitelighet og bekreftelse (Lincoln & Guba, 1985). Videre vil vi gå gjennom hvert av de fire kvalitetsbegrepene og reflektere over hvorvidt de er ivaretatt på en tilfredsstillende måte.

4.5.1 Troverdighet

Troverdighet innebærer i hvilken grad det man skulle undersøke faktisk har blitt undersøkt, og at leseren etablerer tillit til at resultatene som presenteres samsvarer med virkeligheten. For å fremme troverdighet kan det gjøres på flere måter, og Johannessen et al. (2016) trekker fram det å sette seg godt inn i feltet som skal studeres, involvere flere forskere til å vurdere prosjektet, samt benytte seg av flere metoder ved innhenting av data.

I denne studien har målet vært å undersøke hvordan Glencore Nikkelverk kan etablere beredskap for å håndtere cyberhendelser. Problemstillingen og forskningsspørsmålene har vært sentrale, og på bakgrunn av dette ble det utarbeidet en intervjuguide med temaer. Temaene og spørsmålene ble utviklet og avgrenset direkte mot problemstillingen og tilhørende forskningsspørsmål, for å sikre at intervjuene faktisk ga svar på dette (Bryman, 2016). Informantene fikk tilsendt problemstilling og en beskrivelse av de ulike delene intervjuguiden tok for seg i forkant, slik at de kunne forberede seg og gi mest mulig utfyllende svar. Dette kan ha bidratt til å redusere sannsynligheten for improviserte svar (Kvale & Brinkmann, 2009).

Studien har benyttet kvalitative intervjuer som metode for å innhente viktige data, noe som har vært nødvendig for å kunne dokumentere status og hvordan de ulike ansvarshavende reflekterer rundt problemstillingen. Spørreundersøkelser ville eksempelvis ikke gitt den samme kvaliteten eller grunnlaget for å kunne besvare problemstillingen (Creswell, 2014). Intervjuene har gjort at informantene har kunnet gi grundige forklaringer, og forskeren har kunnet stille oppfølgingsspørsmål dersom noe har vært uklart. Temaet for oppgaven er krevende og bredt, og det å stille oppfølgingsspørsmål har vært avgjørende for å sikre kvalitet i studien (Bryman, 2016).

Seks informanter er intervjuet, noe som utgjør et godt grunnlag for å kunne svare på problemstillingen og ivareta troverdigheten, spesielt ettersom studien tar utgangspunkt i en enkelt bedrift. Dersom studien hadde vært utvidet til å gjelde flere virksomheter, kunne antallet informanter med fordel økes. Begrensning av antall informanter gir også mulighet til å bruke mer tid på hver enkelt og gå i dybden (Creswell, 2014). Etter hvert intervju har forskeren gitt en oppsummering av hvordan svarene er forstått og tolket, for å kvalitetssikre at innhentet materiale er riktig oppfattet (Kvale & Brinkmann, 2009).

De innhentede dataene viser ulik tilnærming og kunnskap, noe som indikerer at forskeren har fått frem flere perspektiver enn forventet gjennom intervjuene. Dette styrker troverdigheten til studien (Creswell, 2014).

Ettersom forskeren er en student, er det ikke naturlig å involvere flere forskere i prosjektet. Det har heller ikke vært mulig eller hensiktsmessig å benytte seg av flere metoder. Det har imidlertid vært god dialog med veileder, som dermed har fungert som en kontroll av kvaliteten i prosjektet fortløpende (Bryman, 2016). Blant annet har veileder vurdert

intervjuguiden før intervjuene ble gjennomført, og dialog med veileder har medført justeringer underveis (Kvale & Brinkmann, 2009).

Forskeren er som tidligere nevnt selv ansatt ved bedriften og har et ansvar for øvrig beredskap. Dette kan føre til spørsmål om hvorvidt det svekker troverdigheten. Forskeren har vurdert at dette ikke har påvirket studien i negativ retning. Av informantene er det kun én som rapporterer til forskeren, og denne informanten har ikke ansvar for fagfeltet, noe som gir vedkommende mulighet til å snakke fritt om sin kjennskap til problemstillingen (Creswell, 2014). Noen av informantene ligger i rapporteringslinjen over forskeren, noe som kan medføre en risiko for at forskeren reserverer seg i spørsmålsstillingen eller at informantene kan forsøke å påvirke eller pynte på svarene som gis. Forskeren har vært oppmerksom på dette og svarene som er gitt gir inntrykk av stor åpenhet rundt forbedringspotensialet (Bryman, 2016). Dette tyder på at svarene som er gitt gir en ærlig beskrivelse av forhold knyttet til problemstillingen (Creswell, 2014).

Kjennskap til informantene har gitt tilgang til deres tid og kunnskap, noe som har vært viktig for studien. Det har også bidratt til at forskeren lettere kunne etablere en trygg ramme rundt intervjuene, noe som er en viktig faktor for å sikre åpenhet og ærlighet fra informantene (Kvale & Brinkmann, 2009).

4.5.2 Overførbarhet

Overførbarhet refererer til i hvilken grad funnene fra en studie kan overføres til andre sammenhenger (Lincoln & Guba, 1985). Dette innebærer en vurdering av om resultatene og metoden er gyldige i en annen setting. I denne studien er det benyttet kvalitativ metode, nærmere bestemt semistrukturerte intervjuer, noe som begrenser antallet informanter sammenlignet med kvantitative metoder som spørreundersøkelser (Creswell, 2014).

Det er likevel gjort et nøye utvalg av informanter som er godt egnet til å bidra med data for å besvare problemstillingen. Det er beskrevet hvilke kriterier informantene er valgt ut på, slik at leseren selv kan vurdere overførbarheten basert på resultatene og den øvrige litteraturen (Bryman, 2016). Informantene har ulike stillinger der de har ansvar for sikkerhet og beredskap i virksomheten på forskjellige nivåer. Antallet informanter er høyt sett ut fra antall

personer som har et slikt ansvar i bedriften, og de representerer et bredt spekter av ledergruppe og IT-teknisk kompetanse (Kvale & Brinkmann, 2009).

Mange industribedrifter og øvrige virksomheter i Norge er organisert på en tilsvarende måte som Glencore Nikkelverk. Forskeren kan ikke selv trekke konklusjonen, men leseren bør kunne vurdere om resultatene er overførbare til lignende virksomheter (Lincoln & Guba, 1985). Forskerens tolkninger av resultatene er av betydning for å vurdere graden av overførbarhet (Bryman, 2016).

Som tidligere nevnt, har flere norske og internasjonale virksomheter vært utsatt for ulike cyberhendelser de siste årene, og fokus på håndtering av slike hendelser har økt. Problemstillingen kan derfor ikke sies å være unik for Glencore Nikkelverk, noe som styrker overførbarheten av funnene til andre sammenhenger (Creswell, 2014).

Ved å gi en utvidet beskrivelse av prosessen i studien, kan leseren bedre vurdere overførbarheten til andre sammenhenger (Lincoln & Guba, 1985). Forskeren vurderer at resultatene som er presentert er relevante for arbeidet med etablering av beredskap for cyberhendelser også i andre virksomheter. Det antas at tilsvarende resultater kunne fremkomme ved å benytte et annet utvalg av informanter. Forskeren mener at de vurderinger og valg som er gjort fremkommer tydelig i metodekapittelet og at det dermed vil være egnet og mulig dersom andre ønsker å gjenta prosjektet i samme målestokk eller større omfang (Bryman, 2016).

I hvilken utstrekning en annen forsker vil kunne gjenta prosjektet påvirker graden av pålitelighet i studien (Lincoln & Guba, 1985). Måten spørsmålene blir stilt i intervjuet vil påvirke graden av pålitelighet til studien, og Lincoln og Guba (1985) trekker frem åpne eller lukkede spørsmål som eksempel. For å reflektere over påliteligheten av egen studie vil dermed intervjuguiden og de spørsmål som er stilt i intervjuene stå sentralt (Kvale & Brinkmann, 2009). Intervjuguiden er nøye vurdert i forhold til hvordan spørsmålene kan bidra til å besvare problemstillingen på en objektiv måte og unngå lukkede spørsmål som begrenser muligheten til å fortolke dataene (Creswell, 2014).

Forskeren har bakgrunn fra politiet og er kjent med viktigheten av å presentere åpne spørsmål og la informanter forklare seg fritt uten avbrytelser. Forskerens egen erfaring og bakgrunn har dermed bidratt til å styrke påliteligheten av studien (Bryman, 2016). Den samme intervjuguiden er benyttet i alle intervjuene, og spørsmålene har i størst mulig grad blitt stilt

på samme måte, noe som øker muligheten for at andre forskere kan gjennomføre intervjuene på samme måte.

Før intervjuene startet ble det presisert overfor informantene at de skulle uttrykke eventuell usikkerhet rundt forståelsen av spørsmålene som ble stilt, for å sikre klar kommunikasjon og korrekt tolkning. Selv om intervjuguiden og spørsmålene er tilgjengelige, må det erkjennes at en annen forsker kan komme frem til et annet resultat, ettersom det ikke vil være mulig å legge til rette for at spørsmålene blir stilt på nøyaktig samme måte (Kvale & Brinkmann, 2009). Sitater fra intervjuene er benyttet i både resultat- og drøftingsdelen for at leseren skal forstå hvordan resultatet er fortolket og hva som ligger til grunn for de ulike konklusjoner.

4.5.3 Pålitelighet

Pålitelighet innebærer å etablere tillit til studien som er gjennomført (Lincoln & Guba, 1985). For å styrke påliteligheten og tilliten til studien er det, som tidligere nevnt, viktig å gi en detaljert og omfattende beskrivelse av prosjektets rasjonale, fremgangsmåte og metodiske valg (Bryman, 2016). Dette gir andre forskere muligheten til å spore dokumentasjon av data, metoder og avgjørelser gjennom hele prosjektet (Johannessen et al., 2016).

I denne studien har forskeren nøye vurdert og beskrevet metodevalg, utvalg av informanter, datainnsamling og analyseprosessen (Creswell, 2014; Kvale & Brinkmann, 2009). Dette bidrar til å styrke studiens pålitelighet og tilliten til resultatene. Videre har forskeren også reflektert over egen rolle, potensielle bias og begrensninger i studien (Bryman, 2016). Dette er viktige aspekter for å øke troverdigheten og påliteligheten av forskningen (Lincoln & Guba, 1985).

For å ytterligere styrke tilliten til studien, er det også viktig å vise hvordan resultatene er i tråd med tidligere forskning og teori (Creswell, 2014). Dette innebærer å sammenligne og sette resultatene i kontekst av eksisterende litteratur, noe som kan bidra til å bekrefte, utfordre eller utvide vår forståelse av fenomenet som studeres (Bryman, 2016).

Med den grundige argumentasjonen og beskrivelsen av metodiske valg og prosesser, samt refleksjon over forskerens rolle og sammenligning med tidligere forskning, legges det til grunn at tilliten til studien er ivaretatt. Dette gjør studien mer pålitelig og nyttig for andre forskere og praktikere som ønsker å forstå og arbeide med beredskap for cyberhendelser i

ulike virksomheter (Johannessen et al., 2016).

4.5.4 Bekreftbarhet

Bekreftbarhet innebærer at de presenterte funnene er reelle og samsvarer med virkeligheten, og at forskerens egne synspunkter ikke utelukkende legges til grunn (Lincoln & Guba, 1985). For å fremme bekreftbarheten bør prosessen og fremgangsmåten i studien beskrives nøye og i sin helhet, slik at leseren kan settes inn i beslutningene og valgene som er gjort (Johannessen et al., 2016). Forskeren må også reflektere over de forholdene som kan påvirke subjektive tolkninger og tilnærminger i studien (Creswell, 2014).

I denne studien har forskeren reflektert over subjektive meninger, spesielt innen kvalitative studier, og har tydelig beskrevet de forholdene som er forskerens egen oppfattelse eller vurdering. Samtidig erkjennes det at det kan være krevende å fristille seg på en helt objektiv måte, særlig i en bedrift og et fagområde man har kjennskap og kunnskap om. Bekreftbarheten ivaretas ved at forskeren er kritisk til egen objektivitet og kommuniserer tydelig de forholdene som er subjektive forståelser, noe som er gjort i størst mulig grad i denne studien (Lincoln & Guba, 1985).

Lincoln og Guba (1985) påpeker at for at en studie skal være bekreftbar, bør den inneha gjennomsiktighet i form av en rød tråd gjennom prosessen i sin helhet. Med rød tråd menes at forskeren må reflektere og kommunisere de valgene som blir gjort gjennom hele prosjektet, fra problemstilling, metodiske valg, og til resultat. I denne studien er dette ivaretatt ved at fremgangsmåten skal være gjennomsiktig ved disse forholdene (Bryman, 2016).

Det er likheter mellom kriteriene for pålitelighet og bekreftbarhet, der sistnevnte skiller seg fra førstnevnte ved at det essensielle er at resultatet utelukkende er basert på fremskaffet data, og ikke forskerens subjektive oppfattelser (Lincoln & Guba, 1985). I dette kapittelet er det reflektert og argumentert over de fire kvalitetskriteriene, og med bakgrunn i dette kan det konkluderes med at disse kriteriene er ivaretatt på en god måte i studien. Dette styrker studiens troverdighet og bidrar til at funnene kan anses som bekreftbare og pålitelige (Johannessen et al., 2016).

4.6 Etiske hensyn

Etiske hensyn er av stor betydning i forskning, spesielt når det gjelder intervjuer og publisering av utsagn eller deler av utsagn, ettersom det kan oppleves som et inngrep i informantenes privatliv (Kvale & Brinkmann, 2015). For å ivareta informantenes interesser og vise respekt, er det viktig å handle i tråd med gjeldende forskningsetiske retningslinjer. Dette forskningsetiske perspektivet bør være til stede gjennom hele forskningsprosessen og oppgaveskrivingen (Blaikie & Priest, 2019).

Selv om denne studien ikke stiller private eller følsomme spørsmål, eller inneholder sensitiv data, har det vært viktig å utarbeide oppgaven profesjonelt og med etiske retningslinjer i fokus. Dette har vært et sentralt element i oppgaveskrivingen.

Blaikie og Priest (2019) fremhever fire hovedpunkter innenfor forskningsetikk som bør tas i betraktning: frivillig deltakelse, informert samtykke, beskyttelse av deltakernes interesser og forskning med integritet. Disse prinsippene har blitt nøye fulgt i denne studien.

Før intervjuene ble gjennomført, fikk alle informanter skriftlig informasjon om studien og deres deltakelse. Informantene ble også informert om anonymisering av navn, men at det kunne være mulig å knytte utsagn eller sitater til deres stilling og ansvarsområde. Alle informantene ga sitt samtykke til dette. Videre ble informantene informert om at de kunne trekke seg fra studien når som helst i prosessen, noe som ivaretar prinsippet om frivillig deltakelse (Creswell, 2014).

Gjennom hele forskningsprosessen har det vært fokus på å beskytte deltakernes interesser og forske med integritet. Dette innebærer blant annet å være ærlig og nøyaktig i fremstillingen av data, samt å unngå potensielle skader eller ulemper for informantene (Bryman, 2016).

I denne studien har forskningsetiske hensyn blitt ivaretatt ved å følge prinsippene om frivillig deltakelse, informert samtykke, beskyttelse av deltakernes interesser og forskning med integritet (Blaikie & Priest, 2019). Dette har bidratt til å skape en profesjonell og etisk forsvarlig oppgave, som respekterer og beskytter informantenes interesser og privatliv.

5 Empiri

Dette kapittelet presenterer funnene som har fremkommet gjennom intervjuene, og empirien vil bli strukturert og presentert i tråd med forskningsspørsmålene og intervjuguiden. Temaene som blir behandlet vil være basert på empirisk materiale og vil bidra til å besvare forskningsspørsmålene på en grundig og systematisk måte.

5.1 Beskrivelse av status og eksisterende beredskapssystemer

Basert på intervjuer med informanter fra Glencore Nikkelverk, presenterer dette kapittelet en beskrivelse av bedriftens nåværende status, eksisterende beredskapssystemer og den enkeltes erfaring og kompetanse, med fokus på cyberhendelser. Sitater og ulike svar fra informantene er inkludert for å illustrere deres synspunkter og erfaringer.

Informantene ved Glencore Nikkelverk har ulik og variert erfaring med beredskapsarbeid innen både fysiske og operasjonelle hendelser. Noen av informantene har erfaring fra arbeid i kommunal kriseledelse, mens andre har mange års erfaring med overordnet ansvar for beredskap i industrien. Flere informanter har håndtert situasjoner som brann, eksplosjoner og alvorlige personskader. Imidlertid har de begrenset erfaring med cyberhendelser.

En av informantene, informant F, har tidligere erfaring med å håndtere cyberhendelser og har hatt øverste ansvar for IT-sikkerhet i en annen selvstendig bedrift. Informanten beskriver at deres beredskapsplan og tilhørende tiltakskort omfattet de syv mest sannsynlige scenarioer. Denne planen var tilgjengelig både digitalt og i trykt format og ble regelmessig testet minst to ganger årlig gjennom bordøvelser.

Informant F: *"Vi hadde en beredskapsplan og lagde tiltakskort knyttet til dette. [...] Sikkerhetsfokuset var på topp hos alle som jobbet på IT-avdelingen. Noen ganger valgte vi sikkerhet over brukervennlighet."*

Informanten deler sine erfaringer med å ha opplevd cyberhendelser "på kroppen" og nevner en hendelse i 2017, der han jobbet i et konsern som ble rammet av en kryptolocker, spesifikt en Viper. Denne angrepet førte til et estimert tap på 2 milliarder kroner og påvirket konsernets sentrale infrastruktur. Informanten understreker at deres egen bedrift klarte seg bedre på grunn av de forberedelsene som var gjort i henhold til konsernets retningslinjer.

Informant F: *"I 2017 jobbet jeg i et konsern som ble rammet av krypto locker, eller strengt tatt en Viper, som rammet konsernet og tok ned all sentral infrastruktur. Estimert tap ble beskrevet som 2 milliarder kroner. [...] All e-post og filservere ble borte, men vi kunne fortsatt kjøre produksjonen, for der hadde vi vårt eget system som ikke var styrt fra konsernet, men bare var vårt."*

Denne informanten bidrar med verdifull innsikt om hvordan en solid beredskapsplan og et sterkt fokus på sikkerhet kan redusere konsekvensene av cyberhendelser. Det understreker også viktigheten av å finne en balanse mellom sikkerhet og brukervennlighet, samt å skape aksept for nødvendige kompromisser innen organisasjonen.

Alle informantene fremhever eksisterende forebyggende tiltak mot cyberhendelser. De beskriver at det årlig gjennomføres obligatorisk nettbasert compliance-trening for alle ansatte, samt phishing-kampanjer og holdningskampanjer knyttet til årvåkenhet og passordbruk.

Informantene fra IT-avdelingen påpeker at mesteparten av systemenes sikkerhet styres fra konsernets hovedkontor i Sveits og ligger på et høyt sikkerhetsnivå. Informant B fra ledergruppen trekker også frem dette, men poengterer at selv om dette er på plass så er det mennesket, de som bruker systemene, som er det svakeste leddet i sikkerhetskjeden.

IT-avdelingens informanter har begrenset kjennskap til beredskapen for operasjonelle eller fysiske hendelser i bedriften. De er klar over at det finnes en beredskap, men kjenner ikke til deltakerne eller strukturen. Representantene fra ledergruppen, som alle innehar stabsfunksjoner knyttet til beredskapsorganisasjonen, beskriver bedriften som godt forberedt, med solide prosedyrer og rammeverk for eksisterende beredskap. Informant C (ledergruppen) påpeker imidlertid at dokumentasjonen for beredskap er god, men tilgjengeligheten er dårlig på grunn av papirbasert og permbasert arkivering. Samme informant mottok heller ikke opplæring eller informasjon om beredskap før en øvelse ble gjennomført et halvt år etter at denne startet i jobben.

Når det gjelder beredskap for cyberhendelser, er informantene enige om at det er rom for forbedring. Informant A vil ikke være kategorisk, men erkjenner at diskusjoner om risiko og gjennomførte revisjoner har avdekket svakheter i bedriftens beredskap knyttet til cyberhendelser. Informant B uttrykker at de ennå ikke har nok på plass for å håndtere cyberhendelser og foreslår å utnytte eksisterende kunnskap og overføre noe av systematikken fra den etablerte, ordinære beredskapen til dette området. *«På cyber så har vi ikke så mye på plass, enda. Så der ser jeg for meg at vi kan bruke den kunnskapen som finnes og overføre noe av systematikken som finnes i den etablerte ordinære beredskapen».*

5.2 Risikoforståelse

Alle informantene uttrykker at de anser cyberhendelser som en reell trussel for bedriften. Informanter fra ledergruppen beskriver at cyberhendelser er inkludert i bedriftens risikoregister, og at det de siste årene har vært økt fokus på dette området, samt identifisert behov for å styrke arbeidet. Informant A fremhever at *"et målrettet og vellykket angrep vil utgjøre en eksistensiell risiko for bedriften."*

Informantene er enige om at cyberhendelser som fører til produksjonsstans over tid utgjør en av de største risikoene. Flere av dem påpeker også at hvis bedriften mister kontroll, eller styring over prosessen, kan dette i ytterste konsekvens få betydning for liv, helse og ytre miljø.

Noen av informantene trekker også frem tap av sensitive personopplysninger som en høyt rangert risiko ved cyberhendelser.

Informantene fra IT-avdelingen beskriver ransomware, eller kryptolocker, som den mest alvorlige trusselen i forbindelse med cyberhendelser. Utfordringen med denne typen hendelser er at alt ofte "går i svart", og man mister oversikten over egne systemer. Dette skaper utfordringer når det gjelder å fastslå hvor langt tilbake man må gå for å gjenopprette eventuelle sikkerhetskopier.

Samlet sett erkjenner informantene ved Glencore Nikkelverk at cyberhendelser utgjør en betydelig risiko for bedriften, og det er enighet om at det er nødvendig å styrke arbeidet med å beskytte bedriften mot slike hendelser.

5.3 Beredskapsanalyser og planverk

Når det gjelder utformingen og implementeringen av beredskapsplanverket for cyberhendelser hos Glencore Nikkelverk, opplyser informantene fra ledergruppen at det ikke finnes et slikt planverk, i alle fall ikke et de er kjent med. De opplyser at behovet for å gjennomføre risikoanalyse knyttet til cyberhendelser er «flagget», men at det gjenstår en del arbeid knyttet til dette. På spørsmål om man kan si at cyberhendelser i dag "håndteres etter beste evne", svarer informantene bekreftende.

Informantene fra IT-avdelingen gir et noe mer nyansert svar. De opplyser at det er påbegynt et arbeid med å kartlegge og identifisere risiko, men at dette arbeidet har stoppet opp da den ansvarlige byttet stilling. De er ikke kjent med om det er gjort en sårbarhets- eller verdivurdering av de ulike datasystemene bedriften benytter, og de mangler også full oversikt over hvilke programmer som benyttes i dag.

Når det gjelder beredskap, beskriver en informant fra IT-avdelingen at selv om de ikke har en formalisert beredskapsplan eller tiltakskort for cyberhendelser, har de likevel en form for beredskap. IT-avdelingen har en vakttelefon som skal være bemannet døgnet rundt, året rundt. Den som har vakt, skal kunne gi råd over telefon, logge seg inn fra hjemmekontor eller rykke ut. Det nevnes også at bedriften nylig har inngått en avtale med et eksternt IT-sikkerhetsselskap som skal kunne bistå bedriften før, under og etter et cyberangrep. Det understrekes imidlertid at rammeverket knyttet til denne avtalen ennå ikke er på plass.

Når det gjelder spørsmålet om informantene tror eksisterende beredskapssystemer kan tilpasses for også å kunne håndtere cyberhendelser, er informantene i stor grad positive til dette. De ser fordelene ved å benytte kjent metodikk og struktur, spesielt når det gjelder etablering av krisestaben på strategisk nivå. Flere av informantene understreker at det må inngå eller tilføyes IT-faglig ekspertise ved en cyberhendelse. Informantene trekker også frem at en beredskapsplan for cyberhendelser bør være et eget planverk, hvor innholdet tydelig skiller seg fra operasjonelle og fysiske hendelser.

5.4 Trening, øvelser og systematisk forbedring

Informantene understreker betydningen av både phishing-kampanjer og obligatoriske compliance-treninger innen IKT-sikkerhet som sentrale elementer i opplæring og trening. De påpeker også at det legges vekt på IKT-sikkerhet i introduksjonskursene som alle nyansatte må gjennomgå.

Informant A bemerker at bedriften har en egen Enterprise Risk Management (ERM)-komité, bestående av nøkkelpersoner som møtes minst hvert halvår for å vurdere de mest betydningsfulle risikoene for bedriften. Cybersikkerhet har vært et gjennomgående tema på møtene de siste årene, noe som beskrives som et viktig bidrag for å opprettholde fokus på temaet.

En informant fra IT-avdelingen forteller at han har jobbet der i 25 år, men aldri deltatt eller hørt om øvelser knyttet til cyberhendelser før nylig. Denne øvelsen var en tabletop i forbindelse med en revisjon fra IT-personell fra hovedkontoret. Han beskriver øvelsen som en «øyenåpner» for seg selv og sine kolleger. «*For eksempel, i tilfelle av en cyberhendelse, er responsen ofte helt motsatt av hvordan man ville håndtere andre akutte situasjoner. I en brannsituasjon er målet å umiddelbart starte slokking og skadebegrensning. Men når man oppdager et pågående cyberangrep, er den beste taktikken ofte å observere og avvente for å se hva angriperen gjør videre. Dette er en utfordrende tilnærming, ettersom det kan være vanskelig å avgjøre når det er riktig tidspunkt å gripe inn. Når er det nok?".*

Informantene forklarer at det i phishing-kampanjer gis tilbakemelding til de som mottar e-postene, og at man kan se en synkende trend i antallet som trykker på mistenkelige lenker etter slike kampanjer. Totalt antall som trykker på neste test, går også ned.

Når det gjelder compliance-trening og holdningskampanjer, erkjenner en av informantene fra ledergruppen at det er vanskelig å måle effekten av dette. Likevel oppfatter informantene at det har en positiv effekt, da slike kampanjer ofte blir diskutert i møter, rundt lunsjbordet eller tatt opp som sikkerhetsbudskap i såkalte sikkerhetsmøter.

En av informantene påpeker at det følges opp at alle som skal gjennomføre obligatorisk nettbasert trening faktisk gjennomfører dette. Bedriften har også en kultur for å gjennomføre mange granskninger hvert år, noe som bidrar til systematisk læring fra hendelser og hvordan man kan unngå at de gjentar seg. Denne metodikken mener informanten også kan og vil benyttes etter en cyberhendelse.

En informant fra IT-avdelingen beskriver at konsernet har en egen standard for IKT-sikkerhet, Glencore Security Framework (GSF), som i stor grad bygger på den internasjonale standarden for informasjonssikkerhet, ISO-27001. Informanten mener at det å oppfylle og opprettholde dette rammeverket vil være et godt eksempel på systematisk forbedring.

5.5 Anbefalinger og fremtidige tiltak

På bakgrunn av hva som kom frem i intervjuene ble også informantene spurt om hvilke tiltak de hadde identifisert, eller anbefalte for å tilpasse og forbedre eksisterende beredskapssystemer for å håndtere cyberhendelser.

Informant B, fra ledergruppen, understreket at det er viktig å definere hvilket sikkerhetsnivå bedriften bør strebe etter. Dette innebærer en grundig analyse av dagens situasjon og fastsetting av fremtidige mål. Informanten mente at en omstrukturering av IT-avdelingen var nødvendig og nevnte at bedriften for tiden var i prosessen med å rekruttere en ny direktør for informasjon og digitalisering. Informanten ser for seg en IT-avdeling med et grunnleggende kompetansenivå blant fast ansatte, supplert med spesialistkompetanse. Denne kombinasjonen, sammen med tilgang til ekstern støtte, vil ifølge informanten gjøre bedriften bedre rustet til å forebygge og håndtere cyberhendelser.

Informant F, fra IT-avdelingen, uttrykte at organisasjonen allerede har flere viktige elementer på plass, men at det er behov for systematisering og dokumentasjon av disse. Informanten oppfordret til utvikling, testing og forbedring av beredskapsplaner. Viktigheten av å ha kontroll over IT-infrastrukturen, hvor kjernesystemer må kartlegges og deres kritikalitet identifiseres, ble også trukket frem. Avtaler med eksterne aktører ble sett på som en forsikring, men nevnte også at kostnadene ofte er høye, og han var usikker på effektiviteten av slike avtaler. Han foreslo derfor en risikoanalyse som grunnlag for beslutninger rundt hvilke avtaler organisasjonen trenger.

Informant E fra IT-avdelingen listet opp tre sentrale tiltak: utvikling av en egen beredskapsplan for cyberhendelser, gjennomføre verdivurdering og prioritering av systemer og programmer, samt dokumentasjon av eget nettverk. Han fremhevet betydningen av samarbeid med ledergruppen for å sikre at de forstår alvoret knyttet til cyberhendelser.

Informant C fra ledergruppen påpekte at ledergruppen nå har en mye bedre forståelse av situasjonen enn for noen år siden. De har blitt mer bevisst på temaet og tar trusselen seriøst. Informanten fremhevet viktigheten av øvelser knyttet til cyberhendelser, betydningen av en avtale med et eksternt firma, samt å legge til rette for kontinuerlig oppdatering av kompetanse i IT-avdelingen.

Informant D anbefalte at det først og fremst bør gjøres en kartlegging av ansattes kompetanse, og det samme for beredskapsstaben. I samarbeid med industrivernet, som har kompetanse på beredskapsplanlegging, bør IT-avdelingen utvikle en beredskapsplan for cyberhendelser, hvor kritiske systemer blir identifisert. Informanten understreket viktigheten av å øve på håndtering av cyberhendelser og fortsatt arbeid med økt årvåkenhet hos alle ansatte. Informanten snakket også om betydningen av samarbeid med eksterne aktører, men advarte mot å være for

avhengig av denne støtten. I en cyberhendelse-situasjon, påpekte han, er det viktig at informasjonen kommer fra ledelsen, som de ansatte allerede er kjent med.

5.6 Opprettholdelse av beredskapssystemer

Intervju av informantene avdekket at det var lite sammenhengende planverk knyttet til beredskap for cyberhendelser. Informantene ble derfor bedt om å svare med utgangspunkt i at dette kommer, eller er på plass.

Informant F understreker at vedlikehold av et effektivt beredskapssystem krever konstant innsats, ettersom nye trusler konstant oppstår og krever tilpasninger. Informanten påpeker at mennesket ofte er det svakeste leddet i sikkerhetskjeden, og tok opp dynamikken mellom forskjellige generasjoner. Selv om de yngre generasjonene ofte er mer dyktige med digitale verktøy, fremhever F at deres forventning om "full tilgjengelighet" kan føre til en mer avslappet holdning til sikkerhetstiltak som skal beskytte data. Informant F beskriver dette med et sitat: "Brukere er som vann, de finner alltid en vei".

Tre informanter fra ledergruppen, A, B, og C, understreker alle viktigheten av å definere nye roller, få de riktige personene på plass, bruke tilstrekkelig med tid og ressurser, samt å ha støtte fra ledergruppen. Informant A fremhever også behovet for å øke ledergruppens forståelse av cyberhendelser, beskriver temaet som "en ullen elefant som vi kan for lite om", og påpeker viktigheten av å lære av tidligere hendelser for fremtidig forebygging og beredskap.

Informant C understreker nødvendigheten av regelmessige øvelser for å opprettholde effektive beredskapssystemer, og uttrykker: "Vi må trene for å holde det levende".

Informant D fremhever behovet for at ledelsen forstår den alvorlige trusselen som cyberhendelser kan utgjøre. For å opprettholde effektive beredskapssystemer, foreslår informanten at det bør benyttes nye metoder, og at arbeidet med beredskap er en kontinuerlig prosess. Informant D peker også på potensialet som ligger i bruk av kunstig intelligens for å forebygge og håndtere cyberhendelser.

5.7 Oppsummering av hovedfunn

Basert på intervjuene med informantene ble det fastslått at bedriften allerede har en del elementer på plass for å håndtere cyberhendelser. Likevel ble det uttrykt behov for en mer strukturert tilnærming og grundigere dokumentasjon av disse komponentene, samt økt innsats for å fastsette bedriftens ambisjoner knyttet til cyberhendelser.

Bevisstheten om og forståelsen for risikoen knyttet til cyberhendelser beskrives som stigende blant informantene. Som et resultat av dette foreslo informantene risikoanalyser som et sentralt verktøy som beslutningsgrunnlag for videre tiltak.

Flere strategier for å styrke bedriftens beredskap mot cyberhendelser ble foreslått av informantene. Disse inkluderte utvikling av en spesifikk IT-beredskapsplan, gjennomføring av verdivurderinger, prioritering av systemer og programmer, samt en grundig dokumentasjon av organisasjonens nettverksinfrastruktur. Det ble også uttrykt et behov for å vurdere de ansattes kompetansenivåer og identifisere virksomhetskritiske systemer.

Informantene understreket viktigheten av regelmessige øvelser for å forberede seg på potensielle cyberhendelser. Det ble lagt vekt på at alle ansatte, inkludert ledelsen, bør delta i disse på ulike nivå. Kontinuerlig forbedring og oppdatering av IT-avdelingens kompetanse ble også sett på som avgjørende for å opprettholde effektive beredskapssystemer.

Det ble anbefalt en restrukturering av IT-avdelingen, inkludert ansettelse av en ny direktør for informasjon og digitalisering. Informantene påpekte viktigheten av samarbeid med eksterne aktører, men uttrykte samtidig bekymring for å bli for avhengig av slik støtte. Fremtidige foreslåtte tiltak innebar også bruk av nye metoder og teknologier, som kunstig intelligens, for å bekjempe cyberhendelser.

Funnene tilsier en enighet om at opprettholdelse av effektive beredskapssystemer krever kontinuerlig innsats og tilpasning til nye trusler. Informantene anerkjente behovet for økt støtte fra ledergruppen, definering av nye roller, og tildeling av tilstrekkelige ressurser for å opprettholde og forbedre organisasjonens beredskap for cyberhendelser.

Ledergruppens engasjement og forståelse av cybertrusler ble spesielt fremhevet. Det ble understreket at det er viktig at ledelsen anerkjenner alvoret og tar nødvendige tiltak for å møte disse truslene. Videre ble det pekt på viktigheten av kontinuerlig læring og forbedring, som inkluderer læring fra tidligere hendelser og fra andre organisasjoner.

Vedlikehold av beredskapssystemene innebærer også jevnlige øvelser for å simulere reelle situasjoner. Det ble uttrykt at dette hjelper organisasjonen til å forberede seg på mulige trusler og til å reagere raskt og effektivt når de oppstår.

6 Drøfting

Som en del av denne studien vil det nå gås videre til å diskutere teori og empiri i lys av den valgte problemstillingen. Problemstillingen det tas utgangspunkt i, lyder som følger: "Hvordan kan Glencore Nikkelverk etablere god beredskap for cyberhendelser?"

For å kunne drøfte teori og empiri i forhold til denne problemstillingen, vil vi ta utgangspunkt i de tre forskningsspørsmålene som ble presentert i kapittelet om metode.

6.1 Mest fremtredende sårbarheter og trusler

Hvilke sårbarheter og trusler er mest fremtredende for IKT-verdiene ved Glencore Nikkelverk, og hvordan kan disse potensielt påvirke bedriften?

6.1.1 Digitalisering av industrien, IKT-sikkerhet og digitale trusler

Informantene erkjenner at cyberhendelser utgjør en betydelig risiko for bedriften, som er i tråd med Aven's definisjon av risiko som "kombinasjonen av konsekvensene av aktiviteten med tilhørende usikkerhet". De potensielle konsekvensene av et cyberangrep, som produksjonsstans, tap av sensitive personopplysninger og fare for liv og helse, er tydelig identifisert (Aven, 2015, s. 6).

Informantenes svar gir gode betraktninger om hvordan teorien om digitalisering i industrien forholder seg til praktiske aspekter av IKT-sikkerhet. Fokuset på digitalisering og teknologisk innovasjon har åpnet opp for fordeler som økt effektivitet, fleksibilitet og kundetilpasning (Ghobakhloo & Iranmanesh, 2021; Nærings- og handelsdepartementet, 2017). Informantenes utsagn bekrefter disse fordelene, men de fremhever også IKT-sikkerhetens sentrale rolle i den pågående digitaliseringen.

Blant de truslene informantene identifiserer, kommer ransomware (kryptolocker) frem som en hovedbekymring. I en industriell sammenheng kan denne type cyberangrep være særlig skadelig, ettersom digitalisering og automatisering har ført til økt sårbarhet (Ghobakhloo & Iranmanesh, 2021). Slike angrep kan begrense tilgangen til kritiske produksjonsdata eller systemer, noe som igjen kan stanse hele produksjonslinjer.

Informantene fremhever også betydningen av opplæring og økt bevissthet rundt IKT-sikkerhet blant ansatte. Dette er spesielt relevant i en stadig mer digitalisert industri, der arbeidsstyrken må tilpasse seg nye teknologier. Denne vektleggingen av opplæring er i tråd med det norske Nærings- og handelsdepartementets (2017) fokus på kompetanseheving som en kritisk faktor i industriens digitaliseringsprosess.

Informantenes tilbakemeldinger gjenspeiler også behovet for å balansere mellom innovasjon og sikkerhet. Selv om digitalisering kan medføre betydelige forbedringer i effektivitet og produktivitet, fremhever informantene de iboende risikoene ved økt digitalisering. Denne balansen er et tilbakevendende tema i litteraturen rundt digitalisering av industrien (Nærings- og handelsdepartementet, 2017; Ghobakhloo & Iranmanesh, 2021).

Et annet viktig poeng fra informantene er at trusler mot IKT-sikkerhet kan representere en betydelig barriere for videre digitalisering av industrien. Dette spørsmålet berører den norske regjeringens mål om å bli en ledende industri- og teknologinasjon, noe som kan være utfordrende å oppnå uten en mer omfattende innsats innen IKT-sikkerhet.

Ved Glencore Nikkelverk uttrykker informantene flere synspunkter som direkte korresponderer med prinsippene for IKT-sikkerhet. De anerkjenner viktigheten av å beskytte bedriftens digitale systemer, data og informasjon mot uautorisert tilgang, endring, ødeleggelse, forstyrrelser og skade, noe som er kjernen i IKT-sikkerhet (Store norske leksikon, 2022; NOU 2018:14).

I intervjuene fremhever informantene både tekniske og menneskelige tiltak for å oppnå IKT-sikkerhet. På den tekniske siden peker informantene på behovet for å styrke IT-infrastrukturen, for eksempel ved å opprette et dedikert IT-sikkerhetsteam og implementere en beredskapsplan for cyberhendelser. De fremhever også viktigheten av teknologier og prosesser som sikrer IKT-systemer, som kryptering, passordbeskyttelse, autentisering, tilgangskontroll og overvåkning (NOU 2018:14).

På den menneskelige siden, vektlegger informantene betydningen av økt bevissthet og opplæring i cybersikkerhet blant ansatte. Implementering av beste praksis for datasikkerhet er avgjørende for IKT-sikkerhet, og det er her den menneskelige faktoren kommer inn (NOU 2018:14). Gjennom opplæring kan ansatte lære å oppdage og unngå potensielle sikkerhetsrisikoer, noe som til syvende og sist kan styrke organisasjonens samlede IKT-sikkerhet.

Informantenes tilbakemeldinger underbygger viktigheten av en dynamisk og robust tilnærming til IKT-sikkerhet, som omfavner både menneskelige og tekniske aspekter. En slik tilnærming vil være avgjørende for å sikre den pågående digitaliseringen av industrien, og bidra til å oppnå den norske regjeringens mål om å bli en ledende industri- og teknologinasjon (NOU 2018:14).

Når det kommer til å opprette barrierer på menneskelig, teknologisk og organisatorisk nivå for å forhindre uønskede digitale hendelser, fremhever informantene behovet for å omstrukturere IT-avdelingen, ansette en ny direktør for informasjon og digitalisering, samt øke bevissthet og opplæring rundt cybersikkerhet blant de ansatte. Dette illustrerer en proaktiv innsats for å etablere disse nødvendige barrierene, som foreslått i NOU 2018:14.

Samlet sett indikerer de samlede dataene at informantene har en forståelse av truslene knyttet til cyberhendelser, og de har tenkt gjennom hvordan disse kan håndteres, både gjennom tekniske tiltak og økt bevissthet og opplæring blant ansatte. Deres tilnærming reflekterer til en viss grad prinsippene i teorien om IKT-sikkerhet, samtidig som den også viser en forståelse for det stadig skiftende digitale trusselbildet og behovet for kontinuerlig evaluering og oppdatering av IKT-sikkerhetstiltak. Samtidig erkjenner informantene at lite av dette er dokumentert gjennom risikoanalyser, beredskapsanalyser eller beredskapsplan for cyberhendelser.

6.1.2 Sårbarheter

Drøftingen av informantenes data mot den valgte teorien om sårbarhet vil bygge på rammene om sårbarhet som et resultat av økt teknologisk avhengighet, og også rollen som menneskelige og organisatoriske faktorer spiller i dette bildet.

Informantenes refleksjoner og perspektiver understreker tydelig at sårbarheter i bedriften ikke bare er tekniske, men også påvirkes av menneskelige og organisatoriske faktorer. Dette er i tråd med teorien som beskriver sårbarhet som et bredt begrep som inkluderer fysiske, økonomiske, sosiale og teknologiske aspekter. Når det gjelder den teknologiske komponenten, opplever informantene at bedriften er svært sårbar for digitale trusler, noe som er i samsvar med Lundes (2019) og Jasanoff's (2018) argument om økt sårbarhet i et høyteknologisk samfunn.

På samme måte er informantenes forslag om å restrukturere IT-avdelingen, ansette en ny direktør for informasjon og digitalisering, og øke bevisstheten og opplæringen rundt cybersikkerhet blant ansatte i tråd med Lundes (2019) og ISO's (2018) anbefalinger om en helhetlig tilnærming til risikostyring som omfatter både tekniske og organisatoriske tiltak.

Videre understreker informantene viktigheten av å være forberedt på uønskede hendelser og å ha en plan for å gjenoppta normal drift etter slike hendelser. Dette reflekterer Eriksen et al.'s (2021) definisjon av sårbarhet som et systems evne til å motstå en uønsket handling eller hendelse, samt manglende evne til å gjenoppta sin funksjon.

Med hensyn til Jasanoff's (2018) perspektiv på sårbarhet i teknologiske kulturer, viser informantenes erfaringer at både teknologi, produksjon og mennesker er sterkt sammenvevd. De påpeker at sårbarhetene knyttet til cyberangrep ofte kan være svært alvorlige og krever en tilnærming til risikostyring som tar hensyn til kompleksiteten og produksjonen ved bedriften.

Til slutt, i lys av Jasanoff's (2018) påpekning av det innbyrdes forholdet mellom teknologi og samfunn, tyder informantenes innspill på at en sterkere kobling og samordning mellom teknologiske og menneskelige faktorer kan være nødvendig for å håndtere organisatorisk sårbarhet mer effektivt. Dette understreker behovet for en integrert tilnærming til risikostyring, som tar hensyn til den komplekse og gjensidig påvirkende naturen av teknologi og samfunn i konteksten av organisatorisk sårbarhet og IKT-sikkerhet.

6.2 Implementering av beredskap for cyberhendelser, utfordringer og muligheter

«I hvilken grad er teorier og rammeverk for cyberhendelser implementert i praksis hos Glencore Nikkelverk, og hvilke utfordringer og muligheter kan identifiseres i forbindelse med dette?»

Basert på informantenes svar synes det som om Glencore Nikkelverk har utfordringer når det kommer til implementeringen av et effektivt rammeverk for beredskapsarbeid, slik det er beskrevet i Eriksen et al. (2021). Rammeverket inkluderer elementene ledelse, struktur, kultur, og kompetanse.

Ledelse:

Fra svarene fremgår det at ledelsen er klar over behovet for risikoanalyse for cyberhendelser, men det er tydelig at det ikke er blitt tatt klare og besluttsomme tiltak for å sikre at denne analysen er gjennomført. Intervjuene avdekket også at arbeidet med en beredskapsplan for cyberhendelser også har stoppet opp. Dette kan gi et inntrykk av at ledelsen ser ut til å mangle aktivt engasjement, og anerkjenner ikke beredskap som et strategisk virkemiddel, noe Eriksen et al. (2021) understreker som vesentlig for suksessfull beredskap.

På den andre side uttrykker informanter fra ledergruppen at arbeidet knyttet til IKT-sikkerhet vil være et satsingsområde fremover og at det allerede er tatt grep for å bedre dette. Det opplyses at det vil stilles ressurser tilgjengelig for dette arbeidet. Informanter fra ledelsen utrykker også at arbeid med systematisk forbedring er en viktig del av bedriftens kultur og at denne metodikken også brukes for IKT-området.

Bedriftsledelsens erkjennelse av behovet for forbedring i håndtering av cyberhendelser viser en bevissthet om dagens digitale trusler. Denne bevisstheten og ønsket om forbedring er i tråd med Aven (2015) og Renn (1998) sin forskning, som fremhever usikkerheten rundt risiko og behovet for å håndtere og tilpasse seg denne usikkerheten på en systematisk og informert måte.

Struktur:

Når det kommer til struktur, har bedriften har et visst nivå av struktur for å håndtere cyberhendelser, inkludert en vakttelefon for IT-avdeling og en avtale med et eksternt IT-sikkerhetsselskap.

På den annen side, avslører informantenes tilbakemeldinger en betydelig mangel på formalisering rundt dette arbeidet. Det er ingen klar definert beredskapsplan eller rammeverk for håndtering av cyberhendelser. Det er heller ikke fastsatt klare krav, mål, eller definerte roller, ansvar og myndigheter i denne sammenhengen. Disse elementene er avgjørende for en effektiv struktur for beredskapsarbeid, ifølge Eriksen et al. (2021).

I tillegg, indikerer dataene at bedriften har utfordringer med å integrere beredskap for cyberhendelser i organisasjonens øvrige prosesser og aktiviteter. Dette er en viktig del av en effektiv struktur for beredskapsarbeid, som understreket av Eriksen et al. (2021).

Kort sagt, selv om det er noen strukturelle elementer på plass hos Glencore Nikkelverk, er det vesentlige mangler i implementeringen av en omfattende og formalisert struktur for å håndtere cyberhendelser. Dette utgjør betydelige utfordringer, men også potensielle muligheter for forbedring.

Kultur:

Basert på svarene virker det som om det er en erkjennelse av behovet for å forbedre håndtering av cyberhendelser, noe som kan tyde på en viss grad av risikoforståelse og en kultur for å rapportere kritikkverdige forhold og bekymringer.

På den andre siden så beskriver informantene at bedriften har gjennomført risikoanalyser for alle produksjonsområder knyttet til prosessikkerhet. Det beskrives at alle som skal utføre en jobb på Nikkelverket er forpliktet til å utføre en risikovurdering i forkant av utførelsen. Jo mer komplisert jobben er, jo strengere krav stiller bedriften til risikovurderingen som fortas. Også innenfor fysisk sikring og beredskap beskrives at det er gjennomført sikrings- og sårbarhetsanalyser, beredskapsanalyse og at det foreligger et omfattende planverk. Med andre ord, det ser ut til at bedriften har en kultur som fremmer risikoforståelse, som ikke bare oppfordrer til rapportering av kritikkverdige forhold og bekymringer, men også prioriterer å identifisere risiko gjennom en systematisk tilnærming som involverer omfattende risiko- og sårbarhetsanalyser.

Rapporteringen av over 3000 saker årlig i avvikssystemet vitner om en kultur som oppfordrer til å rapportere kritikkverdige forhold. Dette er i tråd med teoriens påstand om at beredskapen er tjent med en kultur som oppfordrer til å rapportere bekymringer tidlig.

En av de viktigste delene av effektiv risikostyring, ifølge Aven & Renn (2009), er å identifisere, analysere og håndtere risiko på en systematisk måte. Dette synes å være en del av kulturen i bedriften, som viser at de på mange områder har implementert solid risikostyring.

Samlet sett tyder informasjonen som informantene gir på at bedriften har en organisasjonskultur som fremmer en solid forståelse av risiko, en proaktiv tilnærming til uønskede situasjoner, og en verdsetting av beredskapens betydning for å ivareta organisasjonens verdier. Disse observasjonene er stort sett i tråd med teorien til Eriksen et al., (2021), og tyder på at bedriften har en effektiv kultur for beredskapsarbeid.

Kompetanse:

Når det gjelder kompetanse, gir informantenes svar inntrykk av at Glencore Nikkelverk står overfor noen utfordringer. IT-avdelingen påpeker at det har vært et forsøk på å utføre en risikoanalyse for cyberhendelser, men at dette initiativet har stagnert. En mulig tolkning kan være en mangel på nødvendig ekspertise for å utføre en slik analyse og for å håndtere cyberhendelser på en adekvat måte. Dette kan også reflektere en mangel på prioritering av slike oppgaver.

Så vidt det kommer frem av svarene, ser det ikke ut til å være etablert klare retningslinjer eller rutiner for å bygge opp og vedlikeholde kompetanse på IT-avdelingen, noe Eriksen et al. (2021) fremhever som sentralt.

Når det er sagt, må det nevnes at informantene synes å ha betydelig erfaring innen beredskapsarbeid for fysiske og operasjonelle hendelser. Dette er i tråd med Eriksens et al. (2021) betydning av bevissthet, kunnskap og ferdigheter på individ- og organisasjonsnivå.

Likevel er det en tydelig mangel på erfaring når det gjelder cyberhendelser blant informantene. Gitt den økende trusselen fra cyberangrep, kan dette utgjøre en betydelig svakhet i organisasjonens beredskapskompetanse. Her kan Eriksens et al. (2021) oppfordring til kontinuerlig utvikling og vedlikehold av beredskapskompetanse være særlig relevant.

Organisatorisk læring, et annet sentralt komponent av kompetanse i henhold til Eriksen et al. (2021), vil bli diskutert mer detaljert i et senere kapittel.

6.3 Cyberberedskapstrening hos Glencore Nikkelverk, metoder og forbedringsprosesser

Hvordan utformer og evaluerer Glencore Nikkelverk trening- og øvelsesprogrammer for å forberede de ansatte på å håndtere cyberhendelser, og hvilke prosesser og metoder benyttes for systematisk forbedring av beredskapen mot cyberhendelser?

Beredskapsarbeid for cyberhendelser i Glencore Nikkelverk fremstår som omfattende og inkluderer flere viktige elementer. Informantene trekker frem phishing-kampanjer og obligatoriske compliance-treninger i IKT-sikkerhet som sentrale tiltak. Disse tiltakene, sammen med fokus på IKT-sikkerhet i introduksjonskursene, gir en indikasjon på at bedriften ser alvorlig på cybertrusler, noe som samsvarer med anbefalingene fra Eriksen et al. (2021).

Den nevnte Enterprise Risk Management (ERM)-komiteen bidrar til å sikre at risiko for cyberhendelser blir diskutert regelmessig. Dette fokuset på risiko og beredskap på toppledernivået er også anerkjent som viktig i litteraturen (Eriksen et al., 2021).

Imidlertid gir en av informantenes erfaringer innblikk i en potensiell svakhet i bedriftens beredskap: Mangel på praktiske øvelser. Erfaringen fra den nylige tabletop-øvelsen viser at slike øvelser kan gi verdifull læring og endring i perspektiv. Dette er i tråd med Eriksen et al. (2021), som fremhever viktigheten av både teoretisk kunnskap og praktisk erfaring i beredskap.

Resultatene fra phishing-kampanjene indikerer en positiv utvikling, mens effekten av compliance-trening og holdningskampanjer oppleves som mer usikker. Selv om det kan være utfordrende å måle direkte effekt av slike tiltak, er det flere metoder som kan benyttes, for eksempel gjennom regelmessige tester av ansattes atferd og holdninger (Eriksen et al., 2021).

Informantene forteller også om systematisk oppfølging av obligatorisk trening, samt en kultur for granskninger for å lære fra hendelser. Dette er i tråd med teorien om organisatorisk læring, som understreker viktigheten av å analysere og lære av både vellykkede og mislykkede hendelser (Eriksen et al., 2021).

Den beskrevne Glencore Security Framework (GSF), som bygger på ISO-27001, gir også en tydelig indikasjon på at bedriften har en systematisk tilnærming til forbedring av IKT-

sikkerhet. ISO-27001 er en anerkjent standard for informasjonssikkerhet og inkluderer krav om kontinuerlig forbedring.

Samlet sett ser det ut til at Glencore Nikkelverk har tatt flere positive skritt i arbeidet med beredskap for cyberhendelser. Likevel er det områder, som for eksempel praktiske øvelser og måling av effekt av tiltak, hvor det kan være rom for ytterligere forbedringer.

Kulturen i en organisasjon er en avgjørende faktor i beredskapsarbeidet. Informantene fra Glencore Nikkelverk fremhever viktigheten av organisasjonskultur for effektiv IKT-sikkerhet. Diskusjoner om IKT-sikkerhet ved lunsjbordet og i møter indikerer en kultur der sikkerhet er viktig, og det er åpenhet rundt disse temaene.

Samlet sett tyder informantenes svar på at kulturen i Glencore Nikkelverk støtter beredskapsarbeid for cyberhendelser, men at det også kan være utfordringer knyttet til hvordan praktisk erfaring vektlegges. Det kan være nødvendig å utforske dette aspektet nærmere for å fullt ut forstå betydningen av organisasjonskultur for beredskap mot cyberhendelser i Glencore Nikkelverk.

6.3.1 Trening, øvelser og systematisk forbedring

Basert på informantenes tilbakemeldinger, er det klart at læring og forbedring er sentrale elementer i Glencore Nikkelverks helhetlige beredskapsstrategi, og dette korresponderer godt med teoriene presentert.

Eriksen et al. (2021) understreker betydningen av læring på individ-, team- og organisasjonsnivå, samt mellom organisasjoner. Dette resonnerer med funnene fra intervjuene, hvor informantene påpeker betydningen av læring både innenfor og utenfor organisasjonen. Glencore Nikkelverk har demonstrert sin evne til å lære på flere nivåer. For eksempel blir læringsmulighetene fra phishing-kampanjene brukt til å forbedre ansattes evne til å identifisere og håndtere potensielle cybertrusler. Den synkende trenden i antallet ansatte som trykker på mistenkelige lenker etter slike kampanjer indikerer at organisasjonen opplever læring fra denne form for øvelse.

Det kan også argumenteres for at Enterprise Risk Management (ERM)-komiteen fremmer organisatorisk læring. Ved å møtes regelmessig for å vurdere risikoer, inkludert cybersikkerhet, inkorporerer organisasjonen kontinuerlig nye innsikter i sin kollektive

kunnskapsbase, noe som er i tråd med Argyris og Schon's (1978, 1996) definisjon av organisasjonslæring. Ved å holde regelmessige møter for å vurdere risikoer, inkludert cybersikkerhet, sikrer organisasjonen en kontinuerlig dialog og læring rundt viktige temaer.

Perry og Lindell (2003) fremhever viktigheten av trening og samhandling. I likhet med dette, er trening, øvelser og simuleringer blitt identifisert av informantene som viktige aspekter av Glencore Nikkelverks beredskapsarbeid. Når det gjelder samhandling, nevner informantene også behovet for samarbeid på tvers av organisasjonen, noe som understreker viktigheten av å forstå og dra nytte av hverandres organisatoriske strukturer og kompetanser.

Det er imidlertid en utfordring å lære fra feil og hendelser, som nevnt av Sommer et al., (2020). Ifølge informanter fra IT-avdelingen, har Glencore Nikkelverk startet en prosess for å kartlegge og identifisere risiko, men denne har blitt avbrutt. Dette antyder et område for forbedring i Glencore Nikkelverks tilnærming til læring og forbedring.

Å ta i bruk øvelser som et verktøy for læring er anerkjent som et viktig element i beredskapskontekst (Sommer et al., 2020). Fra informantenes tilbakemeldinger, er det klart at dette er et område hvor Glencore Nikkelverk har potensial til forbedring. En informants kommentar om at en øvelse var en "øyenåpner" for ham og hans kolleger, viser verdien av denne typen trening. En økt satsing på slike øvelser kan bidra til å styrke organisasjonens beredskap og håndtering av potensielle cyberhendelser.

På samme måte understreker Lunde (2019) viktigheten av å etablere reell beredskapsevne ved å lære opp, trene og øve mannskapene. Fra intervjuene fremgår det at Glencore Nikkelverk legger vekt på å trene de ansatte, særlig når det gjelder prosess-sikkerhet og operasjonell beredskap knyttet til dette.

På den annen side, er det tydelig at det er behov for økt fokus på øvelser knyttet til cyberhendelser. At det tok 25 år før en informant fra IT-avdelingen opplevde en slik øvelse, indikerer at dette er et område som har blitt nedprioritert. Gitt at øvelser er sentrale for å forberede organisasjonen på potensielle hendelser bør det vurderes å øke fokus på dette.

Ved å implementere og etterleve Glencore Security Framework (GSF) - et rammeverk for IKT-sikkerhet som hovedsakelig er basert på den internasjonale standarden for informasjonssikkerhet, ISO-27001 - kan organisasjonen oppnå en systematisk forbedring. Denne implementeringen vil også sikre at bedriften er i samsvar med anerkjente beste praksiser og standarder innen cybersikkerhet.

Samlet sett tyder informantenes svar på at Glencore Nikkelverk arbeider med å fremme læring og kontinuerlig forbedring i sitt beredskapsarbeid. Dette er i tråd med teorien og indikerer at organisasjonen har tatt viktige skritt mot å forbedre sin beredskapskapasitet. Imidlertid, som mange organisasjoner, er det rom for forbedring. Dette er særlig tilfellet når det gjelder øvelser og simuleringer knyttet til cyberhendelser.

7 Konklusjon

Denne oppgaven har søkt å belyse den overordnede problemstillingen: *Hvordan kan Glencore Nikkelverk etablere god beredskap for cyberhendelser?*

Hensikten med denne studien var å undersøke en stadig økende tematikk i industrien, cyberhendelser og etablering av beredskaps knyttet til dette. Studien har undersøkt hvilke suksesskriterier som skal til for å etablere og opprettholde en god beredskap for cyberhendelser, og gjennom en kvalitativ datainnsamling har denne tematikken blir analysert og drøftet i lys av valgt teori.

Før det gis oppsummerende konklusjon og anbefaling, vil det presenteres kortfattede konklusjoner knyttet til de forskjellige forskningsspørsmålene.

1. Hvilke sårbarheter og trusler er mest fremtredende for IKT-verdiene ved Glencore Nikkelverk, og hvordan kan disse potensielt påvirke bedriften?

Basert på informantenes svar, relevant teori, og egen analyse, kan vi trekke følgende konklusjoner:

Det ble identifisert flere sårbarheter og trusler som påvirker IKT-verdiene ved Glencore Nikkelverk. Blant de mest fremtredende truslene var cyberangrep som ransomware og datainnbrudd med påfølgende tap av personopplysninger eller andre immaterielle verdier. Sårbarhetene omfattet blant annet mangel på rammeverk, begrenset bevissthet og kunnskap om cybersikkerhet blant ansatte, og avhengighet av eksterne tjenesteleverandører.

Disse truslene og sårbarhetene kan ha alvorlige konsekvenser for bedriften. Cyberangrep kan føre til tap av eller uautorisert tilgang til sensitiv informasjon, driftsstans, og økonomisk tap. På samme måte kan sårbarheter som utilstrekkelig teknisk sikkerhet og begrenset bevissthet om cybersikkerhet blant ansatte øke risikoen for vellykkede cyberangrep.

2. I hvilken grad er teorier og rammeverk for cyberhendelser implementert i praksis hos Glencore Nikkelverk, og hvilke utfordringer og muligheter kan identifiseres i forbindelse med dette?

Etter å ha analysert informasjonen fra informantene og utført en gjennomgang av praksis hos Glencore Nikkelverk, fremkommer det at bedriften for øyeblikket ikke har implementert spesifikke teorier eller rammeverk for å håndtere cyberhendelser på en strukturert måte. Selv om enkelte prinsipper og tiltak innenfor cybersikkerhet kan synes å være til stede, mangler det en formell og systematisk beredskapsplan som er dedikert til å håndtere slike hendelser.

3. Hvordan utformer og evaluerer Glencore Nikkelverk trening- og øvelsesprogrammer for å forberede de ansatte på å håndtere cyberhendelser, og hvilke prosesser og metoder benyttes for systematisk forbedring av beredskapen mot cyberhendelser?

Data indikerer at Glencore Nikkelverk har rom for forbedring i hvordan de forbereder de ansatte på å håndtere cyberhendelser. Det anbefales at bedriften øker sitt fokus på opplæring i cybersikkerhet og styrking av de ansattes kompetanse på dette området. Et viktig tiltak vil være å utvikle en sterkere kultur for cybersikkerhet hvor alle ansatte spiller en aktiv rolle i beskyttelsen av selskapets IKT-verdier. Økt samarbeid med eksterne aktører, inkludert andre industriaktører, rådgivningsfirmaer og offentlige organer, kan også bidra til å forbedre selskapets beredskap.

Oppsummerende konklusjon

Denne studien har vist at Glencore Nikkelverk står overfor flere sårbarheter og trusler, som potensielt kan påvirke bedriftens IKT-verdier negativt. Blant de mest fremtredende truslene er cyberangrep som ransomware og datainnbrudd. Usikkerhet knyttet til cybersikkerhetsbevissthet blant ansatte, utilstrekkelige rammeverk og avhengighet av eksterne tjenesteleverandører er sentrale sårbarheter.

Bedriften har ennå ikke fullt ut implementert spesifikke teorier eller rammeverk for å håndtere cyberhendelser på en strukturert måte. Selv om visse cybersikkerhetstiltak er på plass, mangler det en dedikert, systematisk beredskapsplan for å håndtere slike hendelser.

Når det gjelder trening og forberedelse av ansatte på cyberhendelser, viser dataene at det er betydelig rom for forbedring ved Glencore Nikkelverk. Bedriften bør styrke fokus på øvelser relatert til cyberhendelser og utvikle en sterkere kultur for cybersikkerhet. Økt samarbeid med eksterne aktører kan også bidra til å forbedre bedriftens beredskap mot cyberhendelser.

Ved å adressere disse utfordringene kan Glencore Nikkelverk styrke sin beredskap og evne til å håndtere fremtidige cyberhendelser, og dermed bedre beskytte sine IKT-verdier.

7.1 Anbefaling

Bedriftens beredskap og evne til å respondere på cyberhendelser er av stor betydning. Rask og effektiv håndtering av slike hendelser kan redusere skadeomfanget, sikre kontinuitet i virksomheten og beskytte bedriftens omdømme. Denne studien har belyst at mens det er en god generell forståelse av hva beredskap er og hva den skal inneholde, er det samtidig flere svakheter når det gjelder IKT-sikkerhet og beredskap. Selv om det er økende fokus på cyberhendelser, er det mange som mangler erfaring på dette området, og mange mangler også tilstrekkelig kompetanse og kunnskap. For å være godt forberedt bør bedriften øke fokus på beredskap for cyberhendelser på lik linje med fysisk beredskap. Dette inkluderer å fremme bedre dialog mellom IT-avdelingen, beredskapsstaber, industrivernledelsen, de ansvarlige for risikostyring og ledergruppen. Risikoanalyser bør gjennomføres og oppdateres i takt med det endrede trusselbilde. På bakgrunn av dette bør det planlegges og gjennomføres en beredskapsanalyse. Beredskapsløsninger bør evalueres og deretter må valgt beredskap dokumenteres. Dette innebærer blant annet en konkret beredskapsplan og tilhørende tiltakskort for cyberhendelser. Det bør også utarbeides en plan for kompetanseutvikling, trening og øving knyttet til cyberhendelser. Krav, lærings- og øvingsmål bør utarbeides. Samarbeidsavtalen med det eksterne IT-sikkerhetsselskapet bør konkretiseres slik at bedriften og selskapet har en plan på hvordan de skal forholde seg til hverandre, inkludert fordeling av ansvar og myndighet ved en cyberhendelse.

Fremover vil trusler og sårbarheter knyttet til IKT fortsette å være en stor utfordring for Glencore Nikkelverk. En vedvarende innsats for å forbedre beredskapen og systematisk forbedring vil være avgjørende for å beskytte selskapets IKT-verdier og opprettholde sin konkurranseposisjon. Studien viser at implementeringen av teorier og rammeverk for håndtering av cyberhendelser hos Glencore Nikkelverk er et pågående arbeid, der fremskritt

er gjort, men der det også gjenstår viktig arbeid. Med læring fra både egne og andres erfaringer kan Glencore Nikkelverk fortsette å styrke sin beredskap og evne til å håndtere cyberhendelser.

Glencore Nikkelverk har et solid fundament for å kunne etablere robust beredskap for cyberhendelser, men det kreves fortsatt betydelige anstrengelser for å styrke cybersikkerheten ytterligere. Det krever kontinuerlig forbedring, oppdatering, økt bevissthet og kompetanse blant ansatte, samt et økt samarbeid med eksterne aktører. Ved å ta disse stegene, kan Glencore Nikkelverk sikre en robust beredskap mot cyberhendelser, beskytte sine IKT-verdier og opprettholde sin konkurranseposisjon i et stadig mer digitalisert og trusselutsatt landskap.

7.2 Videre forskning

Denne studien har bidratt til forståelsen av hvordan Glencore Nikkelverk kan etablere en effektiv beredskap for cyberhendelser. Gjennom denne prosessen har det imidlertid blitt identifisert flere områder som kan undersøkes videre.

For det første kan det være verdifullt å utvide omfanget av undersøkelsen ved å inkludere andre industribedrifter i studien. Dette vil gi muligheten til å sammenligne ulike tilnærminger til beredskap mot cyberhendelser, og dermed gi en dypere forståelse av feltet. En slik studie kan omfatte både større og mindre virksomheter, noe som kan gi et mer nyansert bilde av hvor modne forskjellige organisasjoner er i forhold til cybersikkerhet.

Videre kan det være nyttig å utforske hvordan teoriene Normal Accident Theory (NAT) (Perrow, 1984) og High Reliability Organizations (HRO) (La Porte & Consolini, 1991, Weick & Sutcliffe, 2001) kan anvendes i praksis innen cybersikkerhet. Disse teoriene gir unike perspektiver på håndtering av risiko og uforutsigbarhet i komplekse teknologiske systemer.

NAT framhever at systemulykker er uunngåelige i komplekse systemer, og oppfordrer organisasjoner til å være forberedt på uventede hendelser. På den andre siden fokuserer HRO på hvordan organisasjoner kan oppnå høy pålitelighet og sikkerhet, selv i de mest utfordrende og farlige situasjoner. Sammenligning av disse to teoriene kan gi innsikt i hvilke strategier og praksiser som er mest effektive for å forhindre, håndtere og lære av cyberhendelser.

For eksempel, det kan være av interesse å utforske hvordan prinsippene for HRO kan anvendes for å minimere risikoen for "tight coupling" og "interactive complexity" som er

identifisert av NAT. Hvordan kan organisasjoner balansere behovet for å forutse og forhindre systemulykker (som foreslått av NAT) med behovet for å være fleksible og adaptive (som foreslått av HRO)? Slike spørsmål kan være gjenstand for fremtidig forskning.

Disse forslagene til videre forskning gir bare et utvalg av mulige retninger. Den økende avhengigheten av digital teknologi i dagens samfunn gjør at studier innen cybersikkerhet og beredskap for cyberhendelser blir stadig mer relevant. Det er håp om at denne studien vil bidra til en dypere forståelse og videre diskusjon om hvordan vi som bedrift kan sikre våre digitale systemer mot trusler og hvordan man best kan etablere beredskap for cyberhendelser.

8. Litteraturliste

Argyris, C. (1978) Organizational learning. Reading, Massachusetts: Addison-Wesley.

Aven, T. (2015). Risikostyring (2. utg.). Oslo, Norge: Universitetsforlaget.

Aven, T. (2006) Pålitelighets- og risikoanalyse. 4. utg. Oslo: Universitetsforl.

Aven, T. and Renn, O. (2009) "On risk defined as an event where the outcome is uncertain," Journal of risk research, 12(1), pp. 1–11.

Berman, J. (2021, 14. mai). The Colonial Pipeline Hack Is a New Extreme for Ransomware. The Wall Street Journal. https://www.wsj.com/articles/the-colonial-pipeline-hack-is-a-new-extreme-for-ransomware-11620935401

Blaikie, N. and Priest, J. (2019) Designing social research: the logic of anticipation. Third. Cambridge, UK: Polity Press.

Bryman, A. (2016) Social research methods. 5th edn. Oxford: Oxford University Press.

CNN. (2021, May 11). Colonial Pipeline hack: A 'wake up call' about the need for cybersecurity standards in the energy industry. https://www.cnn.com/2021/05/11/politics/colonial-pipeline-cybersecurity-standards-energy-industry/index.html

Creswell, J.W. (2014) Research design: qualitative, quantitative, and mixed methods approaches. 4th ed.; International student. Los Angeles, Calif: SAGE.

Digi.no. (2016, 19. oktober). The AIDS Trojan – tidenes første ransomware-angrep. Hentet 14. mai 2021, fra https://www.digi.no/artikler/the-aids-trojan-tidenes-forste-ransomware-angrep/339375

Eriksen, J., Rake, E.L. and Sommer, M. (2021) Beredskapsanalyse. 1. utgave. Oslo: Cappelen Damm akademisk.

Ghobakhloo, M. (2018) "The future of manufacturing industry: a strategic roadmap toward Industry 4.0," Journal of manufacturing technology management, 29(6), pp. 910–936.

Ghobakhloo, M. and Fathi, M. (2020) "Corporate survival in Industry 4.0 era: the enabling role of lean-digitized manufacturing," Journal of manufacturing technology management, 31(1), pp. 1–30.

Ghobakhloo, M. and Iranmanesh, M. (2021) “Digital transformation success under Industry 4.0: a strategic guideline for manufacturing SMEs,” Journal of manufacturing technology management, 32(8), pp. 1533–1556.

Halvorsen, K. (2008) Å forske på samfunnet : en innføring i samfunnsvitenskapelig metode. 5. utg. Oslo: Cappelen akademisk forl.

Hommels, A. et al. (2014) Vulnerability in Technological Cultures. Cambridge: MIT Press (Inside Technology).

Industrivern - Næringslivets sikkerhetsorganisasjon. (n.d.). Retrieved from https://www.nso.no/

ISO. (2018). ISO 31000:2018 Risk management - Guidelines. International Organization for Standardization.

Jacobsen, D.I. and Repstad, P. (2004) Dugnadsånd og forsvarsverker: tverretatlig samarbeid i teori og praksis. 2. utg. Oslo: Universitetsforl.

Johannessen, A., Christoffersen, L. and Tufte, P.A. (2016) Introduksjon til samfunnsvitenskapelig metode. 5. utg. Oslo: Abstrakt.

Kagermann, H., Wahlster, W., & Helbig, J. (2013). Recommendations for implementing the strategic initiative INDUSTRIE 4.0: Securing the future of German manufacturing industry; final report of the Industrie 4.0 Working Group. Forschungsunion.

Kull, H. (2015) “References,” in Mass Customization. Berkeley, CA: Apress, pp. 125–128.

Koronakommisjonen. (2021). NOU 2021: 1, Beredskap mot pandemier. Hentet fra https://files.nettsteder.regjeringen.no/wpuploads01/blogs.dir/421/files/2021/04/Koronakommisjonens_rapport_NOU.pdf

Kvale, S. and Brinkmann, S. (2009) Interviews: learning the craft of qualitative research interviewing. 2nd edn. Los Angeles, Calif: Sage.

LaPorte, T.R. and Consolini, P.M. (1991) “Working in Practice But Not in Theory: Theoretical Challenges of ‘High-Reliability Organizations,’” Journal of public administration research and theory, 1(1), pp. 19–48.

Lincoln, Y.S. and Guba, E.G. (1985) Naturalistic inquiry. Beverly Hills, Calif: Sage.

Lunde, I.K. (2019) Praktisk krise- og beredskapsledelse : etablering av beredskap : potensialbasert beredskapsledelse : proaktiv stabsmetodikk. 2. utgave. Oslo: Universitetsforlaget.

Regjeringen. (2021). Meld. St. 5 (2020–2021). En helhetlig integrert sikkerhetspolitikk. Hentet fra https://www.regjeringen.no/contentassets/eb05d43fc14e4682a1ee156d8f9ee9ce/no/pdfs/stm202020210005000dddpdfs.pdf

Regjeringen. (2017). Meld. St. 27 (2016–2017). Nasjonal sikkerhet i en ny tid. Hentet fra https://www.regjeringen.no/contentassets/3fda224cc2824e5790ca9c9e40d8b0e8/no/pdfs/stm201620170027000dddpdfs.pdf

Nikkelverk. (u.å.). Hentet fra https://www.nikkelverk.no/

Njå, O. et al. (2020) Samfunnssikkerhet : analyse, styring og evaluering. Oslo: Universitetsforlaget.

NRK. (2021, 13. mai). Disse store norske selskapene ble angrepet av hackere i 2021. Hentet 14. mai 2021, fra https://www.nrk.no/norge/disse-store-norske-selskapene-ble-angrepet-av-hackere-i-2021-1.15477026

Norges offentlige utredninger 2018: 14, hentet fra 26968_NOU_2018_XX_JD.book (regjeringen.no)

Politiets trusselvurdering 2023. (2022). Politiets sikkerhetstjeneste. Retrieved from https://pst.no/globalassets/dokumenter/politiets-trusselvurdering/politiets-trusselvurdering-2023.pdf

Renn, O. (1998) “Three decades of risk research: accomplishments and new challenges,” Journal of risk research, 1(1), pp. 49–71.

Reuters. (2021, May 9). Explainer: How hackers closed the US's biggest fuel pipeline. Reuters. https://www.reuters.com/business/energy/how-hackers-closed-us-biggest-fuel-pipeline-2021-05-09/

Schwab, K. (2016) “Shaping the Fourth Industrial Revolution,” pp. Project Syndicate, 2016.

Schwab, K. (2017) The Fourth Industrial Revolution. First. Westminster: Crown/Archetype.

Sommer, M., Pollestad, B. and Steinnes, T. (2020) Beredskapsøving og -læring. 1. utgave. Bergen: Fagbokforlaget.

Sommer, M., Rake, E. L., Botnen, D. (2018) *Emergency preparedness analysis*. Paper presentert ved Nordic Fire Safety Days 2018. NTNU, Trondheim.

Steinar Kvale and Svend Brinkmann (2009) Interviews: learning the craft of qualitative research interviewing : pbk. 2nd edn. Sage.

Store norske leksikon. (2022). IKT. I Store norske leksikon. Hentet fra https://snl.no/IKT

Store norske leksikon. (2023) Maslows behovspyramide. Hentet fra Abraham Maslow – Store norske leksikon (snl.no)

The Wall Street Journal. (2021, May 13). Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers. The Wall Street Journal. https://www.wsj.com/articles

Weick, K.E. and Sutcliffe, K.M. (2001) Managing the unexpected. 1. edn. San Francisco: Jossey-Bass (University of Michigan Business School management series).

Weick, K.E. and Sutcliffe, K.M. (2007) Managing the Unexpected. 2. Aufl. Hoboken: Jossey-Bass (J-B US non-Franchise Leadership).

Perry, R.W. and Lindell, M.K. (2003) "Preparedness for Emergency Response: Guidelines for the Emergency Planning Process," Disasters, 27(4), pp. 336–350.

9. Vedlegg

Vedlegg 1. Intervjuguide

Intervjuguide til masteroppgave: Hvordan kan Glencore Nikkelverk etablere god beredskap for cyberhendelser?

Introduksjon:

1. Presenter deg selv og formålet med intervjuet.
2. Forklar problemstillingen for intervjuobjektet.
3. Informer intervjuobjektet om grad av konfidensialitet og at de kan trekke seg fra intervjuet når som helst.

Del 1: Bakgrunnsinformasjon og organisasjonskultur

1. Hva er din rolle ved Glencore Nikkelverk og din erfaring med beredskapssystemer?
2. Hvordan vil du beskrive selskapets nåværende beredskapssystemer for håndtering av fysiske og operasjonelle hendelser?
3. Hvordan karakteriserer du Glencore Nikkelverks tilnærming til IKT-sikkerhet og beredskap for cyberhendelser?

Del 2: Forståelse av cyberhendelser, sårbarheter og trusler

1. Hvor godt kjent er du med cyberhendelser og deres mulige konsekvenser for bedriften?
2. Hvilke cyberhendelser ser du på som de mest alvorlige truslene mot Glencore Nikkelverk?
3. Hvilke tiltak har selskapet iverksatt for å beskytte seg mot cyberhendelser?

Del 3: Beredskapsanalyser, planverk og tilpasning av eksisterende systemer

1. Hvordan utføres (risiko- og) beredskapsanalyser hos Glencore Nikkelverk for å identifisere og prioritere risiko knyttet til cyberhendelser?
2. Hvordan er beredskapsplanverket for cyberhendelser utformet og implementert hos Glencore Nikkelverk?

3. Tror du eksisterende beredskapssystemer kan tilpasses for å håndtere cyberhendelser? Hvis ja, hvilke aspekter ved de nåværende systemene kan være direkte overførbare?

Del 4: Trening, øvelser og systematisk forbedring

1. Hvilke trening- og øvelsesprogrammer finnes for å forberede de ansatte på å håndtere cyberhendelser, og hvordan evalueres effektiviteten av disse programmene?
2. Hvordan evaluerer Glencore Nikkelverk beredskapen for cyberhendelser og læringspunktene fra tidligere hendelser eller øvelser?
3. Hvilke prosesser og metoder benyttes for systematisk forbedring av beredskapen mot cyberhendelser?

Del 5: Anbefalinger og fremtidige tiltak

1. Hvilke tiltak anbefaler du for å tilpasse og forbedre eksisterende beredskapssystemer for håndtering av cyberhendelser?
2. Hvordan tror du Glencore Nikkelverk bør koordinere med eksterne aktører, som myndigheter og leverandører som tilbyr tjenester for håndtering, for å styrke selskapets evne til å håndtere cyberhendelser?
3. Hva tror du vil være den største utfordringen i fremtiden når det gjelder å opprettholde et effektivt beredskapssystem for håndtering av cyberhendelser?

Avslutning: Takk intervjuobjektet for deltakelsen og tiden deres