Masteroppgave i samfunnssikkerhet

Universitetet i Stavanger

Våren 2022

Hvordan kan anvendelse av resiliens styrke cyber-beredskap i virksomheter

Av

Anurag Shukla og Even Andre Solbakken

UNIVERSITETET I STAVANGER

MASTERGRADSSTUDIUM I

RISIKOSTYRING OG SIKKERHETSLEDELSE

MASTEROPPGAVE

SEMESTER: Våren 2022

FORFATTER: Anurag Shukla og Even Andre Solbakken

VEILEDER: Riana Steen

TITTEL PÅ MASTEROPPGAVE:

Hvordan kan anvendelse av resiliens styrke cyber-beredskap i virksomheter

EMNEORD/STIKKORD:

Risiko, risikostyring, risikobilde, risikopersepsjon, resiliens, Resilience Engineering, RAG, sosiotekniske systemer, sikkerhetskultur, beredskap, beredskapsanalyser, cyber-beredskap, cyber-hendelse og cybersikkerhet

SIDETALL: 91 uten vedlegg (med vedlegg 169 sider)

Skedsmokorset / Moss

DATO/ÅR: **15.10.2022**

Innholdsfortegnelse

Sammendrag ..... *V*

Summary ..... *VI*

Forord ..... *VII*

1 Innledning ..... *- 1 -*

1.1 Bakgrunn ..... **- 1 -**

1.2 Problemstilling ..... **- 6 -**

1.3 Avgrensninger ..... **- 8 -**

1.4 Masteroppgavens utforming ..... **- 8 -**

2 Kontekst – cyber ..... *- 9 -*

2.1 Hva er en cyber-hendelse? ..... **- 13 -**

2.2 Nasjonal beredskap og organisering ..... **- 16 -**

2.3 Ansvarsfordeling for nasjonal cyber-beredskap ..... **- 18 -**

2.4 Nasjonalt cyber-risikobilde ..... **- 20 -**

3 Teori ..... *- 22 -*

3.1 Risiko ..... **- 24 -**

3.1.1 Risikokonsept ..... - 24 -

3.1.2 Risikopersepsjon ..... - 25 -

3.1.3 Risikostyring ..... - 26 -

3.2 Sikkerhetskultur og sikkerhet i dybden ..... **- 28 -**

3.3 Cyber-beredskap ..... **- 32 -**

3.3.1 Systematisk - tradisjonell tilnærming ..... - 32 -

3.3.2 Systemisk tilnærming for å etablere cyber-beredskap ..... - 38 -

4 Metode ..... *- 48 -*

4.1 Forskningsdesign ..... **- 48 -**

4.2 Forskningsprosessen ..... **- 50 -**

4.3 Datainnsamling ..... **- 50 -**

4.3.1 Kvantitativ datainnsamling ..... - 54 -

4.3.2 Kvalitativ datainnsamling ..... - 57 -

4.4 Validitet og relabilitet ..... **- 60 -**

4.5 Fordeler og ulemper ved valgt metode ..... **- 61 -**

5 Empiriske funn ..... *- 62 -*

5.1 FS1 Hva kjennetegner at Cyber -beredskap i virksomheter er resilient? ..... **- 62 -**

5.2 FS2 På hvilken måte kan virksomheter øke graden av sin Cyber-beredskap? ..... **- 63 -**

5.3 Kategorisering av funn fra informanter, fageksperter og sekundærdata ..... - 63 -
5.3.1 Cyber-hendelse ..... - 63 -
5.3.2 Risikopersepsjon ..... - 64 -
5.3.3 Sikkerhetskultur og beredskap ..... - 65 -
5.3.4 Risikostyring ..... - 66 -
5.3.5 Risikobilde ..... - 67 -
5.3.6 Resiliens og cyber-beredskap ..... - 68 -
5.4 Presentasjon av tematisk analyse for semistrukturerte intervjuer ..... - 69 -
6 Diskusjon..... - 70 -
6.1 Behov for resilient tilnærming for å kunne håndtere cyber-hendelser..... - 70 -
6.2 Bruk av Resilience Engineering for å oppnå bedre cyber-beredskap ..... - 73 -
7 Konklusjon ..... - 91 -
8 Referanser:..... - 92 -
Figur - 98 -
Tabell 99
Forkortelser 100

Vedlegg

Vedlegg 1 – NSDs vurdering av masteroppgaven - godkjent 103
Vedlegg 2 – Informasjonsskriv til informantene 105
Vedlegg 3 – Informasjonsskriv til informantene - purring 107
Vedlegg 4 – Spørreundersøkelsen 108
Vedlegg 5 – Informasjonsskriv til fagekspertene ifm. intervju 125
Vedlegg 6 – Intervjuguide 126
Vedlegg 7 – Intervju med Gøran Tømte 130
Vedlegg 8 – Intervju med Roar Thon 140
Vedlegg 9 – Dokumentanalyse 152
Vedlegg 10 – Tematisk analyse av intervju med fageksperter 157

Sammendrag

Ser man cyber-, risiko- og beredskapsfagene under ett, har disse noen fellestrekk. Disse fagene er relativt unge, og har utviklet seg gjennom de siste 40-50 årene. Utviklingstakten er fortsatt økende. Følgende problemstilling innleder til vårt arbeid med denne masteroppgaven.

Hvordan kan anvendelse av resiliens styrke cyber-beredskap i virksomheter?

For å besvare denne problemstillingen har vi to forskningsspørsmål [FS1] *Hva kjennetegner at Cyber -beredskap i virksomheter er resilient?* [FS2] *På hvilken måte kan virksomheter øke graden av sin Cyber-beredskap*. I denne masteroppgaven har vi benyttet triangulerings-metoden (MMA). Vi har gjennomført spørreundersøkelse med 26 informanter, to semistrukturerte intervjuer med fageksperter og benyttet sekundærdata.

Våre funn viser at det er en ubalanse knyttet til cyber-beredskapen i virksomheter, og ønsket tilstand. Endringer i den sikkerhetspolitiske situasjonen nasjonalt og internasjonalt, har medført økt fare for cyber-trusler, og derav økt behovet for å styrke cyber-beredskap og cyber-sikkerhet i virksomheter. I kombinasjon med grenseoverskridende kriminalitet, hvor kriminelle aktører med onde hensikter tar i bruk samme teknologi for egen vinning, er dette noe som må tas på alvor.

Funnene i masteroppgaven viser på flere områder at det finnes gode muligheter for å utvikle cyber-beredskap i virksomhetene videre. Vi mener at prinsippene i resiliens teorien kan bidra til å styrke cyber-beredskap i virksomheter. Vi mener at økt bevissthet og kompetanse om hva som kjennetegner mennesker i organisasjoner med god sikkerhetskultur er en viktig faktor for å utvikle en resilient sikkerhetskultur.

Datagrunnlaget i denne masteroppgaven viser at noen av virksomhetene i ulik grad er resiliente, og at graden av resiliens er avhengig av hvor mye virksomheten benytter seg av egenskapene som de fire hjørnesteinene representerer (jfr. lære, respondere, overvåke og forutse). Vi mener å ha funnet at virksomheter ved å øke sin bevissthet og kompetanse om resiliens, på denne måten kan forbedre sin cyber-beredskap. Vi mener også at økt bevissthet og kompetanse om NSMs grunnprinsipper for IKT-sikkerhet er en viktig faktor for å bidra til større grad av resiliens i virksomheter.

Nøkkelord: Risiko, risikostyring, risikobilde, risikopersepsjon, resiliens, Resilience Engineering, RAG, sosiotekniske systemer, sikkerhetskultur, beredskap, beredskapsanalyser, cyber-beredskap, cyber-hendelse og cybersikkerhet

Summary

If you look at the cyber, risk, and preparedness, these have some common features. These subjects are relatively young and have developed over the past 40-50 years. The pace of development is still increasing. The following research question begins our work on this master's thesis.

How can the application of resilience strengthen cyber preparedness in businesses?

To answer this question, we have two research questions [FS1] *What characterizes cyber preparedness in resilient businesses?* [FS2] *In what way can companies increase the level of their Cyber readiness*? In this master's thesis, we have used the triangulation method (MMA). We conducted a survey with 26 informants and two semi-structured interviews with experts and used secondary data.

Our findings show an imbalance in related to cyber preparedness and the desired state of affairs. Changes in the security policy situation nationally and internationally have led to an increased risk of cyber-threats, and hence the increased need to strengthen cyber-preparedness and cyber-security in businesses. In combination with cross-border crime, where criminal actors with malicious intent use the same technology for their own gain, this is something that must be taken seriously.

The findings in the master's thesis show in several areas that there are good opportunities for developing cyber preparedness in enterprises further. We believe the principles of resilience theory can strengthen cyber preparedness in businesses. We believe that increased awareness and competence in what characterizes people in organizations with a good safety culture is essential in developing a resilient safety culture.

According to this master's thesis data, some informants use different degrees of resilience with the four cornerstones of their work (cf. learning, responding, monitoring, and anticipating). We believe that increased awareness and expertise about resilience and helping businesses become more resilient will strengthen cyber preparedness in the companies. We also believe that increased awareness and competence about NSM's basic principles for ICT security is an essential factor in contributing to a greater degree of resilience in the business.

Key words: Risk, risk management, risk picture, risk perception, resilience, Resilience Engnieering, RAG, socio-technical systems, security culture, preparedness, preparedness analyses, cyber preparedness, cyber incident and cyber security

Forord

Arbeidsprosessen med å skrive masteroppgaven med en kollega har vært veldig givende og lærerik. I tillegg har det gitt oss en unik mulighet til å gå i dybden innenfor flere fagområder som vi arbeider med til daglig, og som vi har stor egeninteresse av. Vårt interne samarbeid og vår felles arbeidsgiver har også gitt oss muligheten til drøfting og refleksjon gjennom hele arbeidsprosessen. Dette har bidratt til å forbedre arbeidsprosessene knyttet til oppgave-skrivingen, samt til å stille krav til og kvalitetssikre hverandres bidrag.

Vi vil rette en stor takk til våre informanter og fageksperter som utelukkende stilte seg positive til å dele sin kunnskap og erfaring med oss. Videre vil vi takke våre informanter og fageksperter for deres engasjement knyttet til vår problemstilling, og for hvordan de motiverte oss til videre arbeid. Vi vil også takke våre ektefeller (Merethe og Cathrine) for deres støtte fra vi startet på masterutdanningen i 2019 og frem til i dag, samt for alt de har bidratt med underveis i arbeidet med masteroppgaven.

Til slutt, vil vi takke vår veileder Riana Steen for hennes entusiasme og engasjement gjennom hele prosessen. Hennes entusiasme og klare tale var ikke til å misforstå, og vi har satt stor pris på at hun alltid var tilgjengelig når vi hadde behov for veiledning. En stor takk til henne for tydelige og konstruktive tilbakemeldinger.

Skedsmokorset/Moss, 15. oktober 2022

Anurag Shukla og Even Andre Solbakken

1 Innledning

I denne masteroppgaven ønsker vi å undersøke om resiliens kan styrke cyber-beredskap i virksomheter. Bakgrunnen for at vi valgte denne tematikken er at vi har god kjennskap til hvordan egen virksomhet har etablert beredskap for å håndtere krise- og beredskapssituasjoner. I tillegg har vi arbeidserfaring innenfor fagfeltene teknologi, telekom og teknisk kybernetikk, i kombinasjon med interesse for digital sikkerhet og beredskap. Idag er det mange virksomheter som har etablert beredskap basert på en systematisk og tradisjonell risikotenkning, hvor operasjonelle driftsorganisasjoner har ansvaret for å dimensjonere og håndtere den forebyggende beredskapen. Mens beredskap knyttet til å håndtere ekstraordinære situasjoner i noen tilfeller blir dimensjonert av driftsorganisasjoner, kan den også, i andre tilfeller, bli håndtert av en *egen* beredskapsorganisasjon.

På sikkerhetskonferansen 2022, i regi av Nasjonal sikkerhetsmyndighet (NSM), ble resilient cyber-beredskap omtalt av flere foredragsholdere. Statsminister Jonas Gahr Støre, sjef for NSM, Sofie Nystrøm, sjef for E-tjeneste, viseadmiral Nils Andreas Stensønes og tidligere sjef for PST, Hans Sverre Sjøvold, uttrykte alle «at det er nødvendig å gjøre cyber-beredskapen mer resilient» (NSM, 2022b).

Cyber-beredskap skal inngå i virksomhetens etablerte beredskap, men samtidig er det mye læring i å forstå hvordan andre virksomheter dimensjonerer og etablerer cyber-beredskap. I 2021 ble totalt 38 virksomheter i Norge rammet av cyberangrep, og disse er utgangspunktet for vår masteroppgave.

1.1 Bakgrunn

I 2003 utarbeidet Norge, som et av de første land i verden, en nasjonal strategi for digital sikkerhet. I takt med endringer av trusselbildet, har nasjonal strategi for digital sikkerhet blitt revidert tre ganger. I det siste nasjonale strategidokumentet kunngjorde tidligere statsminister Erna Solberg at «strategien skulle møte utfordringene som følger av en rask og gjennomgående digitalisering av det norske samfunnet» (Departementene, 2019, forord). Utviklingen innen informasjons- og kommunikasjonsteknologi (IKT) har også bidratt til store endringer i samfunnet (Departementene, 2012, s.8) og følger teknologitrendene (NOU 2018: 14, s. 22).

Den globale digitale infrastrukturen omtales ofte som «Internett», og eies hovedsakelig av private virksomheter. Dette private eierskapet bidrar til innovasjon og utvikling, en utvikling

som i all hovedsak foregår i forsknings- og utviklingsmiljøer, samt i private selskaper (Meld. St. 38 (2016-2017), s. 20).

Fra vi står opp til vi legger oss produserer og konsumerer vi ulik grad av digitale tjenester; når vi ser eller hører nyheter, er på skole, arbeid eller hjemmekontor, ved aktiviteter på sosiale medier mfl. Tilsvarende samfunnsutvikling ser vi også i virksomheter som benytter digital teknologi og digitale tjenester til en rekke formål. For nesten alle virksomheter er tjenestene tilkoblet et nettverk med tilgang til internett for å oppnå en effektiv samhandling og kostnadsbesparende løsninger. Internett har mange fordeler, og mange digitale tjenester hadde ikke vært mulig uten internett. Det er en høy grad av digitalisering av samfunnet globalt, og ifølge FN er Norge rangert på 13. plass i verden og på 8. plass i Europa når det gjelder å ta i bruk ny teknologi (United Nation, 2020, s. 12-14).

Tabell 1 - Landene med høyest grad av digitalisering (United Nation, 2020, s.12)

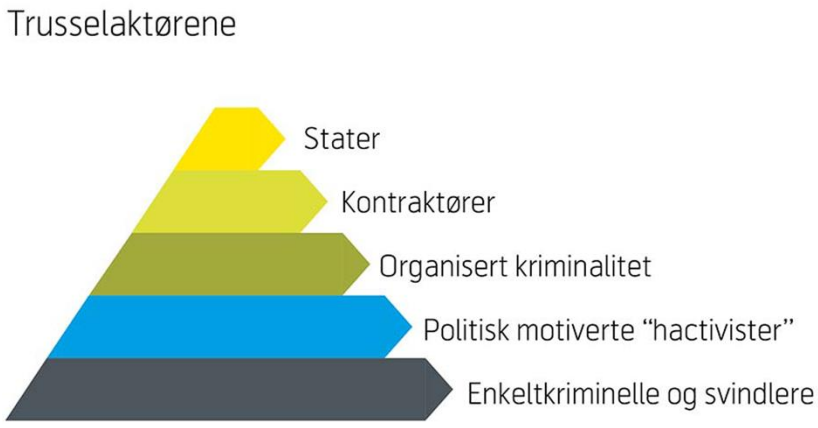
Rank	Country	Rating class	Region	OSI value	HCI value	TII value	EGDI value (2020)	EGD value (2018)
1	Denmark	VH	Europe	*0.9706*	*0.9588*	*0.9979*	*0.9758*	*0.9150*
2	Republic of Korea	VH	Asia	*1.0000*	*0.8997*	*0.9684*	*0.9560*	*0.9010*
3	Estonia	VH	Europe	*0.9941*	*0.9266*	*0.9212*	*0.9473*	*0.8486*
4	Finland	VH	Europe	*0.9706*	*0.9549*	*0.9101*	*0.9452*	*0.8815*
5	Australia	VH	Oceania	*0.9471*	*1.0000*	*0.8825*	*0.9432*	*0.9053*
6	Sweden	VH	Europe	*0.9000*	*0.9471*	*0.9625*	*0.9365*	*0.8882*
7	United Kingdom of Great Britain and Northern Ireland	VH	Europe	*0.9588*	*0.9292*	*0.9195*	*0.9358*	*0.8999*
8	New Zealand	VH	Oceania	*0.9294*	*0.9516*	*0.9207*	*0.9339*	*0.8806*
9	United States of America	VH	Americas	*0.9471*	*0.9239*	*0.9182*	*0.9297*	*0.8769*
10	Netherlands	VH	Europe	*0.9059*	*0.9349*	*0.9276*	*0.9228*	*0.8757*
11	Singapore	VH	Asia	*0.9647*	*0.8904*	*0.8899*	*0.9150*	*0.8812*
12	Iceland	VH	Europe	*0.7941*	*0.9525*	*0.9838*	*0.9101*	*0.8316*
13	Norway	**VH**	**Europe**	***0.8765***	***0.9392***	***0.9034***	***0.9064***	***0.8557***
14	Japan	VH	Asia	*0.9059*	*0.8684*	*0.9223*	*0.8989*	*0.8783*

Resultatene fra FN-rapporten understøttes av Lysne I-utvalgets oppsummering om den teknologiske utvikling av samfunnet og hvordan det forandrer og påvirker livene våre.

> *«De siste tiårene har digitaliseringen ført til gjennomgripende samfunnsmessige endringer. Den har effektivisert arbeidshverdagen for de fleste av oss, slik at det samme arbeidet nå kan utføres av langt færre hender. Den har forandret måten vi styrer prosesser på, slik at komplekse operasjoner og infrastrukturer nå kan kontrolleres fra ett eller noen få sentrale steder. Den har gitt befolkningen en lang rekke nye tjenester, som kontantløs handel og finansielle tjenester på mobil,*

elektronisk samhandling med det offentlige og sanntids trafikkinformasjon som lar oss finne den mest hensiktsmessige reiseveien mellom to steder. Videre har den revolusjonert måten vi kommuniserer på, ved at mobiltelefoner, sosiale medier og samarbeidsstøtteverktøy er blitt dagligdags. Norge ligger i verdenstoppen når det gjelder bruk av IKT. Dette gjør norsk næringsliv mer konkurransedyktig, og øker samfunnets totale produktivitet og innovasjonsevne. En videreføring av denne situasjonen forutsetter at samfunnet har tillit til at teknologien er trygg å ta i bruk.» (NOU 2015: 13, s. 15)

Digitalisering av samfunnet bidrar også til økt risiko for å bli utsatt for digitale trusler, hvor enkeltpersoner eller virksomheter kan bli utsatt for sosial manipulasjon, løsepengevirus (utpressing), datainnbrudd mm. Trusselaktørenes motivasjon er forskjellig. Enkeltkriminelle og svindlere kan ha intensjon om å få anerkjennelse gjennom hærverk eller gjennom økonomisk vinning. Andre trusselaktører han være alt fra politisk motiverte, til kriminelle organisasjoner, kontraktører og stater (se *Figur 1 under*). Eksempler på dette kan være alt fra uskyldige rampestreker fra ungdommer til de mest avanserte trusselaktører som har tilgang til store mengder ressurser (bl.a. mennesker, penger, teknologi, infrastruktur mm.). Sistnevnte kan også ha god tid (i måneder og år) for å oppnå sine målsetninger. Videre har de evne og kapasitet til å drive skjulte operasjoner som er vanskelige å oppdage (Telenor, 2020, s. 18-19; NOU 2015: 13, s. 15-17; NOU 2017: 11, s. 48-49).

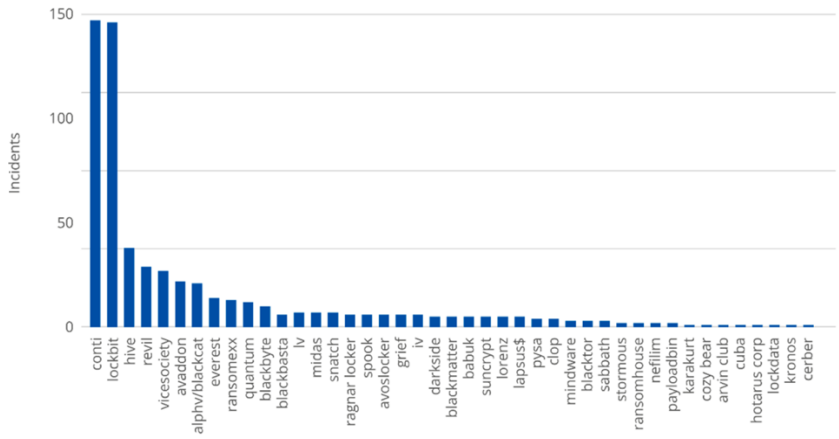


Figur 1 - Trusselpyramiden (Telenor, 2020, s. 19)

Ifølge NSM er det vesentlig forskjell i intensjon og kapasitet mellom kriminelle (organisert kriminalitet og kontraktører) og stater eller kontraktører tilknyttet stater, og de utdyper det på følgende måte:

«[...] målet for en kriminell aktør kan være økonomisk vinning, kan det ramme viktige samfunnsfunksjoner. Kraftforsyning, teleinfrastruktur, helsetjenester og matforsyning – digital utpressing og sabotasje kan treffe hvem som helst. Det er kun et spørsmål om tid før slike hendelser får alvorlige konsekvenser for samfunnsfunksjoner og nasjonal sikkerhet.» (NSM, 2022a, s. 17-19)

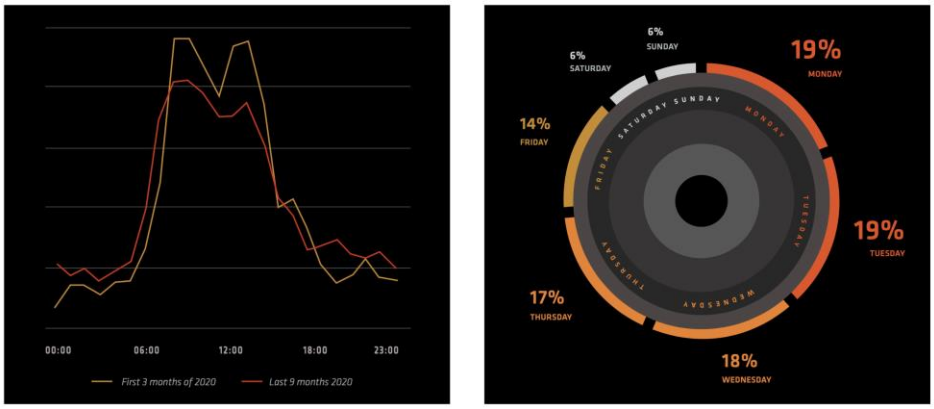
Tidligere i år publiserte European Union Agency for Cybersecurity (ENISA) en rapport som omhandlet dybdeanalyse av 623 cyberhendelser i tidsrommet mai 2021 til juli 2022 (se Figur 2 under). Av disse cyberhendelsene klarte ENISA å identifisere 603 trusselaktører, dvs. 97 % av tilfellene, se illustrasjon i Figur 2 under. Det er ikke overraskende at de tre største trusselaktørene står for mer enn 345 (57 %) av de analyserte cyberhendelsene (ENISA 2022, s. 25-26). Sikkerhetsselskapet Trend micro har fulgt med på trusselaktørene over flere år, og de publiserer et oppdatert trusselaktørbilde hvert kvartal. Ut fra deres rapporter kan vi lese at trusselaktørene Conti, Lockbit og Hive har profesjonalisert sin virksomhet og utviklet en forretningsmodell hvor de bl.a. selger løsepengevirus som et eget produkt/tjeneste (Ransomware as a Service) (Trend micro, 2022).



Figur 2 – oversikt over cyberhendelser knyttet til trusselaktører (ENISA 2022, s. 26)

Alle som er tilkoblet internett kan bli rammet av uønskede digitale hendelser, og det er noen ganger tilfeldig hvem som rammes. Andre ganger er det målrettede digitale angrep mot enkeltpersoner eller virksomheter. Ifølge det største cybersikkerhets-selskapet i Norge (Mnemonic), som årlig utgir en sikkerhetsrapport, og har analysert nesten 7 billioner sikkerhetshendelser i mer enn 38.000 virksomheter i 2021, finnes det indikasjoner på at trusselaktørene lever sitt daglige liv som folk flest. De er på jobben fra mandag kl. 7:00 til

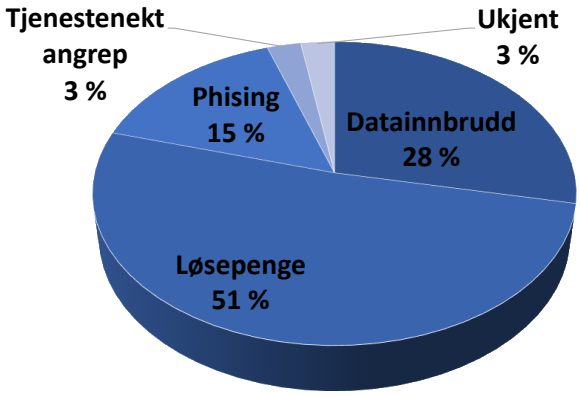
fredag kl. 15.00, se Figur 3. De har de samme utfordringene i hverdagen som andre folk, med kjøring og henting av barn til og fra barnehage og skole etc. Ved at de driver hverdagslige og legitime aktiviteter på en profesjonell og strukturert måte, slik som «vanlige» folk, gjør dette at den *trusselaktør-virksomheten* de driver lettere kan holdes skjult. (Mnemonic 2021, s 28-29).



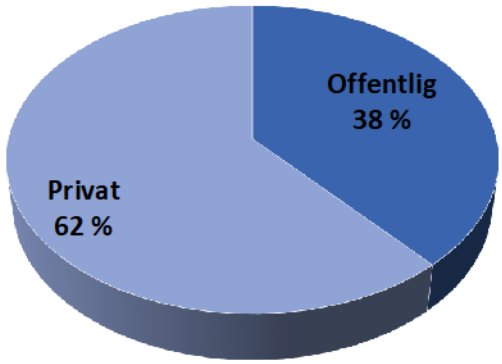
Figur 3 – Cyber-hendelser. V. - tidspunkt på døgnet, H. - aktivitet i ukedagene (Mnemonic, 2021, s. 28-29)

I slutten av 2019 ble hele verden satt på prøve med COVID-19 pandemien. Den 12. mars 2020 ble det iverksatt strenge smittevernstiltak i Norge, noe som førte til at vi bl.a. måtte begrense kontakt mellom mennesker for å redusere smittespredningen. Samfunnet ble mer eller mindre stengt ned, og arbeidsgivere ble tvunget til å sende sine ansatte på hjemmekontor (Regjeringen Solberg, 2020). Norge var generelt langt fremme innen digitalisering av samfunnet, bl.a. når det gjaldt offentlige tjenester, finansielle tjenester, helsesektoren mfl. Noen virksomheter hadde allerede lagt til rette for bruk av hjemmekontor, mens andre raskt måtte implementere løsninger for dette.

Pandemien bidro til at samfunnets digitaliseringstakt økte drastisk, noe som ga samfunnet nye muligheter og utfordringer gjennom nye digitale sårbarheter. Kriminelle med ondsinnede hensikter utnyttet i 2021 dette sårbarhetspotensialet. I Norge ble minst 38 virksomheter utsatt for cyberhendelser av ulik karakter, og noen av disse cyberhendelsene har fått alvorlige konsekvenser for enkeltpersoner (personopplysninger på avveie), og enkelte virksomheter har måttet stenge ned sin produksjon. Analyser viser at løsepenge-virus dominerer med 51 %, samt at det er flest (62 %) private virksomheter som er rammet (Seglsten, 2022a, 2022b).



Figur 5 - Type cyber-hendelser (Seglsten, 2022a, 2022b)



Figur 4 - Kjente cyber-hendelser offentlig og privat sektor

I desember 2021 oppdaget sikkerhetssystemene til en av Norges største matprodusenter mistenkelig aktivitet på servere som senere viste seg å være en cyberhendelse. Det ble oppdaget krypto-virus i Norturas kritiske infrastruktur, noe som gjorde at denne ble utilgjengelig. Dette medførte bl.a. at forbrukere ikke fikk handlet mat (Vogt et al., 2022). For å sikre leveranser av kjøttprodukter til butikkene i forkant av julehøytiden i Norge, ble det iverksatt tiltak for å importere kjøttprodukter fra andre land (Figur 6 og Figur 7).

Figur 6 - Bilde av Kiwis ferskvarehylle med produkter fra Nortura (Haraldsen, 2021)

Figur 7 - Bilde av Coops ferskvarehylle med produkter fra Nortura (NSM, 2022a)

1.2 Problemstilling

Vårt hovedmål med denne masteroppgaven er å få mer kunnskap om forebyggende og ekstraordinær cyber-beredskap i virksomheter som har vært utsatt for kriminelle cyber-hendelser.

Vi vil ta utgangspunkt i de tidligere nevnte 38 virksomhetene og andre relevante virksomheter som har vært utsatt for cyber-hendelser. Med bakgrunn i dette har vi følgende problemstilling som vi ønsker å utrede nærmere:

Hvordan kan anvendelse av resiliens styrke cyber-beredskap i virksomheter?

Forskningsspørsmål (FS):

FS1: Hva kjennetegner at Cyber -beredskap i virksomheter er resilient?

FS2: På hvilken måte kan virksomheter øke graden av sin Cyber-beredskap.

Vår hypotese er at virksomhetene ikke har et klart skille mellom den forebyggende beredskapen og den beredskapen som er etablert for å håndtere ekstraordinære cyberhendelser etter at de har inntruffet. Dersom en virksomhet ikke etablererer beredskap basert på sitt helhetlige risikobilde, vil det være økt risiko for at virksomheten ikke oppnår sine forretningsmål dersom det skulle inntreffe en ekstraordinær cyberhendelse. Gjennom vårt arbeid med masteroppgaven skal vi undersøke om prinsipper og tenkning knyttet til *Resiliens* kan være en metodikk for å forbedre cyber-beredskap i virksomheter.

Mens vi bruker oppgavens teoretiske fundament til å besvare det første forskningsspørsmålet, bruker vi en triangulering av data til å besvare det andre. I denne masteroppgaven vil vi benytte kvalitative og kvantitative metoder. I den kvalitative delen vil vi gjennomføre semi-strukturerte intervjuer med to fageksperter. Disse fagekspertene har lang erfaring fra en rekke roller og funksjoner i offentlige og private virksomheter, og de har hatt betydning for utvikling innen cybersikkerhet i mer enn de siste ti årene. Begge har aktive roller med å påvirke cybersikkerhet, og har stor innflytelse på mange virksomheter i Norge. De er, med andre ord, ressurssterke personer som har kunnskap og erfaring til å belyse en sak eller et fenomen (Andersen, 2006, s. 282). Dette vil bidra til å skape et virkelighetsbilde av virksomhetenes cyber-beredskap som gir grunnlag for å diskutere og drøfte problemstillingene med de underliggende forskningsspørsmålene.

1.3 Avgrensninger

Tid og kapasitet gjør det nødvendig med avgreninger i denne masteroppgaven.

Med referanse til retningslinjer for masteroppgaven i erfaringsbasert master i risikostyring og sikkerhetsledelse (5. februar 2016) kap. 4.2 Omfang «masteroppgaven skal være i størrelsesorden 80 skrevende sider», vår masteroppgave har totalt 91 sider (pluss vedlegg).

Den empiriske primærdata er avgrenset til spørreundersøkelsen og to semistrukturerte intervjuer med fageksperter, dette var nødvendig på grunn av tidskapasitet.

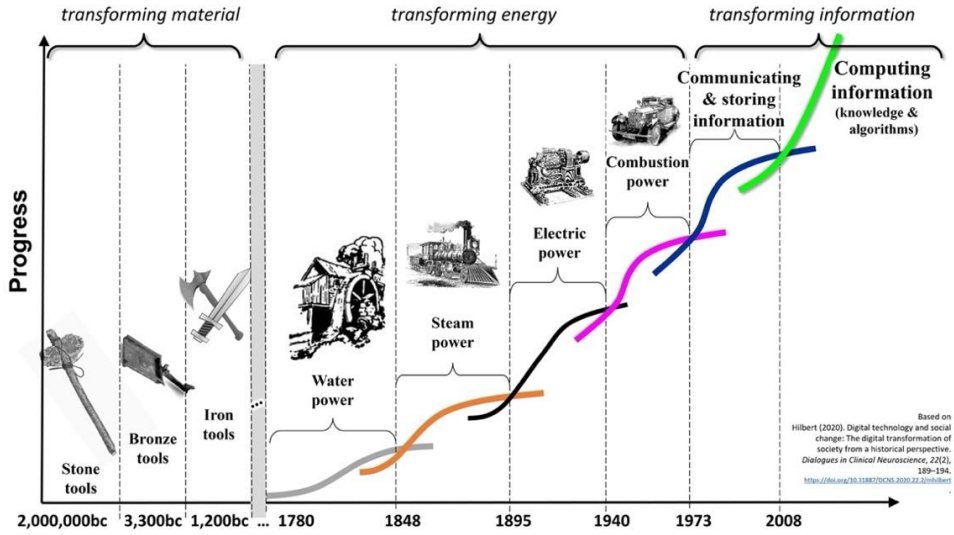
1.4 Masteroppgavens utforming

Tabell 2 - Oversikt over masteroppgavens utforming

Kapitel	Oppsummering
1 – Innledning	Bakgrunn og tema for oppgaven, problemstilling, formål og problemstilling som masteroppgaven søker å gi svar på. Oppgavens utforming, faser og avgrensninger er nærmere beskrevet.
2 - Kontekst	Her presenteres cyber, historisk tilbakeblikk, hva er en cyberhendelse, nasjonalt beredskap og totalforsvaret med ansvarsfordeling og nasjonalt risikobilde fra sikkerhetstjenesten i perioden 2020 - 2022
3 – Teori	Her presenteres relevant teori opp mot oppgavens problemstilling. Her vil vi se nærmere på risikofaget, historisk utvikling, risikopersepsjon, tradisjonell tilnærming, klassisk beredskap, sikkerhetskultur og sikkerhet i dybden, systemisk tilnærming og sosiotekniske systemer.
4 – Metode	I dette kapittelet tar vi for oss studiens metodiske valg, gjennomføring av studien, bakgrunn for valgene, spørreundersøkelse, semi-strukturert intervju, spørreskjema, samt analyse av data
5 – Empiri	I dette kapittelet presenteres de sentrale funnene fra vår spørreundersøkelse, fra semi-strukturerte intervjuer med fagekspertene og sekundærdata.
6 – Diskusjon	Her besvares masteroppgavens problemstilling basert på empiridata opp imot teori og kontekst.
7 - Konklusjon	I det avsluttende kapittelet presenteres konklusjoner, anbefaling på hvordan man kan anvende funnene i studien i praksis og forslag til videre forskning.
Vedlegg	Vedlegg til masteroppgaven, NSD søknad og godkjenning, informasjon til informantene, spørreundersøkelse, intervjuguide og intervju med fagekspertene, dokumentanalyse og tematisk analyse.

2 Kontekst – cyber

Mennesket har i all tid utforsket og utviklet seg selv ved å ta i bruk nye verktøy med tilhørende risikoer. Vi vil først starte med et kort historisk tilbakeblikk, og man beskriver ofte ovennevnte påstand med tre paradigmeskifter.



Figur 8 - Tre paradigmer med informasjonseraen (Wikipedia, 2022; Hilbert, 2022)

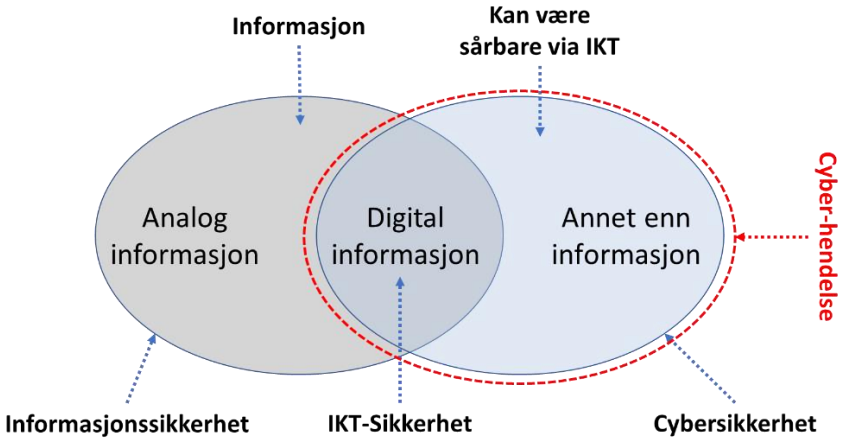
Det første paradigmet blir omtalt som «transforming material» og innebefatter stein-, bronse- og jernalderen. Her var verktøyene primitive, men mennesket kunne utnytte materialet til å lage mer avanserte verktøy og redskaper. Det andre paradigmet, strekker seg fra midten av 1700 tallet frem til 1973, og blir omtalt som «transforming energy». Dette paradigmet innebefatter vannkraft, damp, elektrisitet og forbrenningsmotorer**.**

Tidlig på 1800-tallet begynte man å bygge store høytrykks-dampmotorer som ga mange nye muligheter i industrien, men bruk av disse store maskinene førte til uønskede hendelser som i ytterste konsekvens medførte tap av menneskeliv. På denne tiden ble også Davey Safety Lamp (en lampe med «lukket» flamme) oppfunnet, og denne bidro til å redusere farene for metangasseksplosjoner i gruver. Sikkerhet ble satt på dagsorden for å redusere sannsynligheten for uønskede hendelser, og for å redusere alvorlige konsekvenser dersom disse skulle inntreffe.

Det tredje paradigmet er omtalt som «Transforming information», og omfatter kommunikasjon, lagring, og databehandling av informasjon. Dette paradigmet skiller seg ut fra de to foregående på flere områder. I løpet av de siste 50 år har informasjonsæraen vokst til å bli avgjørende for samfunnet. Revolusjonen har fortsatt i en eksponennsiell hastighet – ingen teknologi har nådd flere mennesker på så kort tid som internett og digitale tjenester – og den er **ikke** ferdig utviklet ennå. Digitalisering av samfunnet fikk ytterligere taktskifte med de tiltak som ble implementert

ifm. COVID-19 pandemien, slik som f.eks. hjemmekontor. Hjemmekontor var mulig fordi teknologien og tilhørende infrastruktur var tilgjengelig for en større del av befolkningen. Om COVID-19 pandemien hadde inntruffet ti år tidligere, ville denne digitaliseringen av samfunnet ha tatt vesentlig lengre tid, og ville kanskje ha vært nesten umulig. For ti år siden ville ikke hjemmekontor ha vært like tilgjengelig pga. datidens begrensninger med internett-kapasitet og -hastigheter. På den tiden var mange av samhandlings-applikasjonene som Microsoft Teams, Zoom mfl. i en tidlig fase av utviklingen, og sky-plattformer var ikke like tilgjengelige. I tillegg var datidens utstyr på hjemmekontor mer begrenset. Fordi det var mer normalt å ha arbeidsstasjoner på arbeidsplassene var f.eks. webkamera mindre tilgjengelig, og bærbare PCer var lite utbredt.

Begrepene informasjons-, IKT- og cybersikkerhet har ikke en entydig definisjon. Det har grenseflater mot, eller oppfattes som synonymt med, informasjonssikkerhet, cybersikkerhet og digital sikkerhet, se Figur 9 under. Ulik forståelse av og ulik bruk av begrepet IKT-sikkerhet har også endret seg noe over tid. Fra å knytte IKT-sikkerhet til beskyttelse av nettverk og systemer, knytter man det nå i større grad til de tjenestene som systemene leverer, samt til den informasjonen som behandles i systemene i NOU 2018: 14 (s. 13-14).



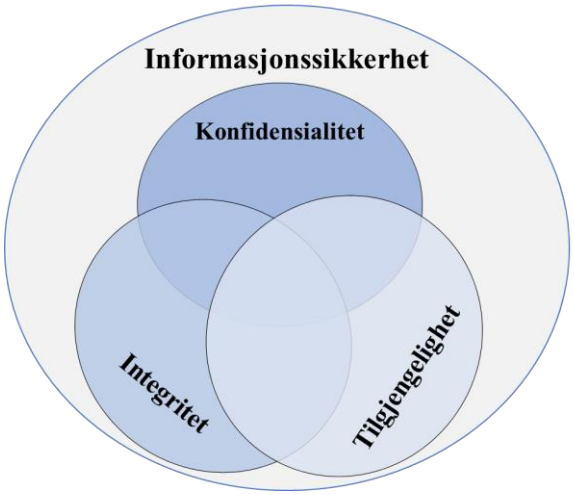
Figur 9 - Basert på Informasjons-, IKT- og Cybersikkerhet (Hagen et al.,2017, s. 15)

I den første stortingsmeldingen for IKT-sikkerhet benytter en begrepet IKT-sikkerhet synonymt med cybersikkerhet (Meld. St. 38 (2016-2017), s. 14). Vi legger dette til grunn, og vi vil benytte begrepet cybersikkerhet videre i denne masteroppgaven, men vi vil også benytte IKT begrepet der det er hensiktsmessig. Det er mange utfordringer knyttet til cybersikkerhet. For det første vil den teknologiske utviklingen fortsette å øke pga. økt bruk av skyløsninger, mer utstyr tilkoblet internett, samt mer globale og integrerte systemer. For det andre utvikler utfordringene

seg raskere enn det virksomhetene klarer å respondere på. Krav knyttet til lønnsomhet medfører behov for kostnadsbesparelser, noe som bidrar til at flere virksomheter setter ut cyber-funksjoner til en tredjepart. Disse sikkerhetsutfordringene bidrar til at det oppstår flere sårbarheter, og det skaper også flere avhengigheter på tvers av landegrenser og mellom virksomheter. Eksempel på en slik sårbarhet kan være ulike internasjonale lover og forskrifter som regulerer Cybersikkerhet forskjellig fra hvordan vi gjør det i Norge. Videre er det en utfordring at IKT-kriminalitet kan være uten et fysisk gjerningssted og/eller den kan være grenseoverskridende.

> *«Det vil si at de kriminelle kan oppholde seg i ett land, men bruker programvare som er plassert i et annet land, for å begå den kriminelle handlingen i et tredje land. Et annet typisk trekk er at det er mulig å angripe mange mål samtidig, ofte med lav oppdagelsesrisiko» (NOU 2017: 11, s. 49).*

Uavhengig av om informasjon er på papir eller er lagret digitalt, så handler informasjonssikkerhet om å beskytte informasjon. Sikkerhetsutfordringene bidrar også til at det er behov for at nettverk og systemer er stabile og sikre til enhver tid. Det er flere definisjoner på informasjonssikkerhet og felles for disse er at følgende tre begreper danner fundamentet: konfidensialitet, integritet og tilgjengelighet (NOU 2016: 19, s. 165-166) se Figur 10.



- **Konfidensialitet** – sikkerhet for at kun autoriserte personer får tilgang til følsom eller gradert informasjon og at det på forhånd er foretatt en gyldig identifisering og autentisering av personen
- **Integritet** – sikkerhet for at informasjon og informasjonsbehandling er fullstendig, nøyaktig og gyldig, og et resultat av autoriserte og kontrollerte aktiviteter
- **Tilgjengelighet** – sikkerhet for at en tjeneste oppfyller bestemte krav til stabilitet, slik at aktuell informasjon er tilgjengelig ved behov.

Figur 10 - basert på definisjon av informasjonssikkerhet (Daler et al., 2014, s. 35-36)

Ifølge Traavik-utvalget, er konfidensialitet, integritet og tilgjengelighet, faktorer som er viktige for å ivareta informasjonssikkerheten i virksomheter.

Dagens industri benytter ulike typer teknologier i fremstilling av produkter eller tjenester, og disse teknologiene omtales ofte med et felles begrep - operasjonell teknologi (OT). OT er kritiske systemer som gjennomsyrer livene våre både direkte og indirekte, og de overvåker og kontrollerer automatiserte prosesser og maskiner, som er for farlige eller for krevende for oss mennesker å overvåte og kontrollere manuelt. Videre er OT definert som en teknologi som har et grensesnitt med den fysiske verden og inkluderer bl.a. programmerbare logiske systemer eller kontrollsystemer (PLS/PLC), industrielle kontrollsystemer (ICS), Supervisory Control and Data Acquisition (SCADA) og Distributed Control Systems (DCS) mfl. Tradisjonelt har OT vært spesialisert på systemer og innretninger som er laget for et bestemt formål med fokus på kvalitet, funksjonalitet og driftssikkerhet, dvs. «oppetid».

Historisk sett har det ikke vært fokus på cybersikkerhet i disse OT infrastrukturene. Dette fordi disse har vært i et lukket nettverk eller i et lukket system, der behovet eller muligheten for å kommunisere med andre infrastrukturer har vært begrenset. Dette er i ferd med å endre seg dramatisk, og vi ser to hovedtrender. Den ene er den teknologiske utviklingen, hvor produsenter av OT-teknologi har gått fra å benytte spesiallagde enheter og komponenter, til å ta i bruk mer standard IKT komponenter som f.eks. PC, servere, nettverkskomponenter, programvare, operativsystemer mm. Den andre trenden at det er større behov for samhandling eller informasjonsdeling fra OT-infrastruktur ifm. drift, forvaltning eller samhandling mm. Dette gjør at det blir et behov for å koble IKT- og OT-infrastrukturene sammen. Det finnes mange sikre måter å koble disse infrastrukturene sammen på, med formål om å redusere sårbarhetene. Felles for disse er at OT, direkte og indirekte, blir eksponert for helt nye typer sårbarheter. Figur 11 under på neste side illustrerer kompleksiteten i virksomhetens cybersikkerhetsperspektiv, hvor mennesker er avhengig av prosesser, som igjen er avhengig av komplekse og sammensatte teknologier jf. IKT og OT med tilhørende funksjoner.

Figur 11 - Cyber-perspektiver i virksomheter, informasjon, IKT og OT. (Shariff, 2020)

2.1 Hva er en cyber-hendelse?

Det er flere definisjoner og perspektiver på hva en cyber-hendelse kan være. De er forskjellige i ulike bransjer, sektorer og ikke minst forskjellige fra land til land. Felles for disse er at man forsøker å kategorisere og beskrive ulik grad av konsekvenser knyttet til en cyber-hendelse, alt fra forsøk på inntrenging, rekognosering, sabotasje, krenkende innhold og til faktisk innbrudd eller sabotasje. Noen av disse er godt definert, mens andre er beskrevet på et overordnet nivå.

I 2018 publiserte en arbeidsgruppe, bestående av 37 fageksperter og myndighetspersoner i regi av ENISA (European Union Agency for Network and Informasjon Security), en felles definisjon av begrepet *cyber-hendelse* i EU. Denne er inndelt i 11 kategorier med flere nyanser av alvorlighetsgrad (ENISA, 2018, s. 4, 9-10, s. 19). NSMs definisjoner og kategoriseringer er basert på ENISAs definisjon av cyber-hendelse (NSM, 2017a, s. 18-20, 2017b, s. 1-2). I denne masteroppgaven har vi lagt NSMs definisjon og kategorier av cyber-hendelser til grunn, og vi har oppsummert dette i Tabell 3 på neste side:

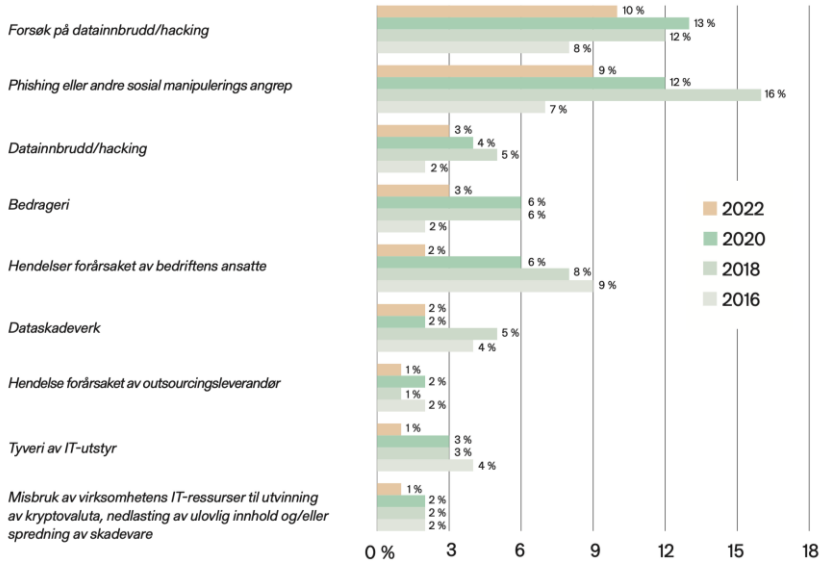
Tabell 3 – NSMs kategorisering av cyber-hendelser (NSM, 2017b, s.1-2)

Klassifisering	Eksempler	Beskrivelse
A. Uautorisert tilgang til informasjon (*Information Content Security*)	• Uautorisert tilgang til informasjon • Uautorisert endring av informasjon	Vellykket uautorisert tilgang til informasjon eller funksjoner på systemer eller tjenester. Resultatet kan være kompromittering av konfidensialitet, integritet og/eller tilgjengelighet. Dette dekker også tilgang til informasjon under overføring.
B. Kompromit-tering (*Intrutions*)	• Kompromiss med privilegert konto og uten privilegrert • Applikasjons-kompromiss	Vellykket uautorisert tilgang til system eller tjeneste. Ingen tegn til aktivitet på målet.
C. Forsøk på kompromittering (*Intrusion Attempts*)	• Utnytte kjente sårbarheter • Påloggingsforsøk • Ny angrepssignatur	Forsøk på kompromittering av systemer eller tjenester ved for eksempel å lure autorisasjonssystemet, gjette passord, utnytte sårbarheter i systemet eller feil i oppsett. En metode som er mye brukt er også å lure legitime brukere til å starte skadelig programvare på interne systemer.
D. Tjenestenekt (*Availability*)	• DoS • DdoS	I denne typen angrep blir systemet bombardert med så mye trafikk at tjenester går ned eller blir mindre responsive.
E. Svindel (*Fraud*)	• Uautorisert bruk av ressurser • Opphavsbeskyttet • Phishing	Bruk av ressurser for å tjene penger, for eksempel misbruk av domenenavn eller epostadresser. Salg eller installasjon av materiale beskyttet av copyright. Bruk av andres identitet.
F. Rekognosering/ informasjonsinnsamling (Info. Gathering)	• Scanning • Avlytting • Sosial manipulasjon	Informasjonsinnsamling om målet via åpne kilder, skanning av infrastruktur og tjenester som er åpne mot Internett, sniffing av trafikk, sosiale nettverk eller telefon.
G. Støtende innhold (Abusive Content)	• Spam • Skadelig tale • Barn, vold, seksueltinnhold mfl.	Spam eller reklame fra parter som ikke har innhentet tillatelse til utsendelse. Plaging, trusler eller forfølgelse via digitale kanaler. Distribusjon av barnepornografi eller forherligelse av vold.

IKT-kriminalitet

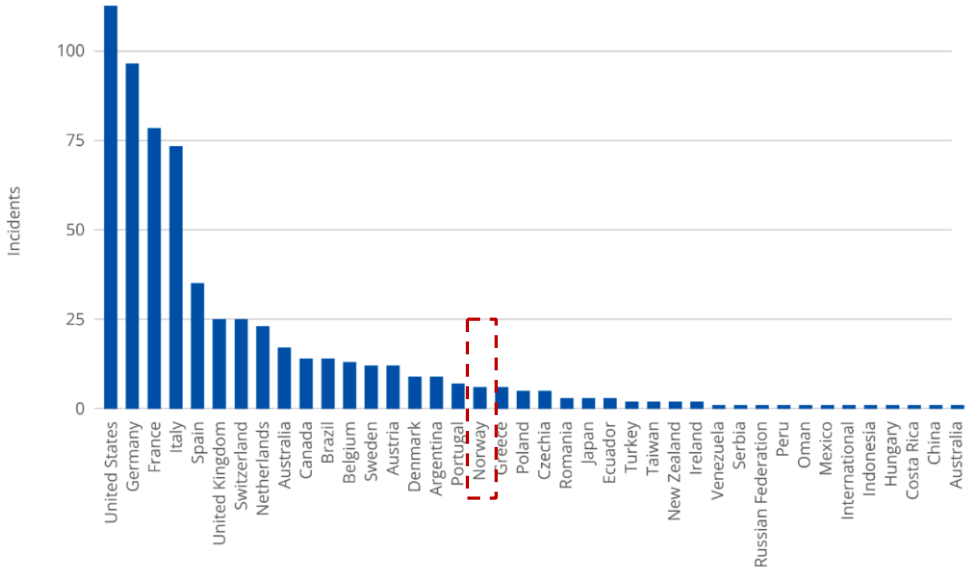
Når vi benytter begrepene IKT-kriminalitet, cyber-kriminalitet eller datakriminalitet, er det heller ikke en entydig internasjonal definisjon for disse begrepene, og de blir ofte også sidestilt med hverandre. Lovverket skiller mellom to typer IKT-kriminalitet, hvor den ene typen er rettet mot datasystemer, mens den andre er knyttet til at det skjer et hendelsesforløp ved hjelp av datasystemer, nettverk eller utstyr (NOU 2017: 11, s. 48-49). Cyber-kriminaliteten øker stadig i omfang, og det er en utfordring for politi og påtalemyndigheter at det digitale rommet begrenser deres mulighet til å pågripe, tiltale og irettesette (Meld. St. 38 (2016-2017), s. 31). Ifølge NSM er det et taktskifte i cyber-domenet, hvor antall cyberhendelser fra 2019 til 2021 har tredobbelt seg, og det er en klar indikasjon på at fremmede stater står bak flere av angrepene (NSM, 2022b, s. 26-27).

Næringslivets sikkerhetsråd (NSR) bidrar med årlige undersøkelser om sikkerhetstilstanden i norsk næringsliv og i noen offentlige virksomheter. NSR har undersøkt sikkerhetstilstanden for virksomhetene over lang tid og deres «mørketallsrapport» påvirker det pågående og forebyggende sikkerhetsarbeidet i vårt næringsliv. Ifølge NSR er de mest vanlige cyber-hendelsene forsøk på datainnbrudd eller hacking og phishing eller andre manipuleringsangrep. Figur 12 nedenfor viser at det fremkommer flere typer av cyber-hendelser for perioden 2016-2022 (NSR, 2022, s. 16).



Figur 12 – Mørketalls undersøkelse 2022 (Næringslivets sikkerhetsråd, 2022, s.16)

ENISA har publisert en rapport som viser et trussel-landskap for løsepenge-virus, der de har analysert 623 løsepengevirus-hendelser i tidsrommet mai 2021 t.o.m. juni 2022. Rapporten viser at Norge ligger på 18. plass i verden og på 13. plass i Europa antall registrerte cyber-hendelser, se Figur 13 på neste side (ENISA, 2022, s. 22-23). Ifølge ENISA har mer enn 60 % av virksomhetene betalt løsepenger. I samme periode identifiserte ENISA 47 forskjellige trussel-aktører (ENISA, 2022, s. 24-26).



Figur 13 – Oversikt over cyber-hendelser fordelt på land (ENISA, 2022, s. 22-23)

2.2 Nasjonal beredskap og organisering

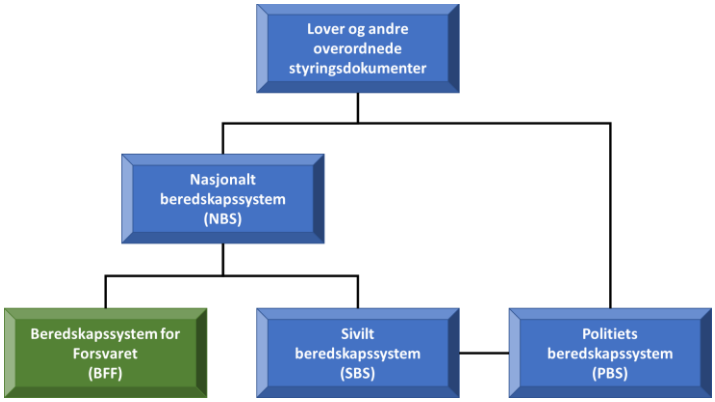
Totalforsvaret og beredskap

Totalforsvaret ble etablert etter andre verdenskrig, og var i hovedsak basert på et militært forsvar med bred sivil beredskap. Videre utvikling av totalforsvarskonseptet har fulgt den sikkerhetspolitiske, teknologiske og samfunnsmessige utviklingen, og har bidratt til at samfunnets forsvarsbehov har blitt endret. Totalforsvarskonseptet var ikke dekkende nok, og det ble innført et nytt begrep, *sivil-militært samarbeid*, for å utdype dette nærmere. Sivil-militært samarbeid gjenspeiler den faktisk balanserte avhengigheten i et sammensatt komplekst system med mange avhengigheter (Forsvarsdepartementet og Justis- og beredskapsdepartementet, 2018, s. 9 og 15). Norge har kommet langt i utviklingen av det sivil-militære samarbeidet, og flere land, bl.a. England, ser på den norske modellen for hvordan totalforsvarskonseptet kan utvikles med sivil-militært samarbeid. (Omand, 2022).

Norges totalforsvar er bygget opp av flere systemer og bygger på sivil-militært samarbeid i fred, krise og krig. Figur 14 under på neste side, illustrerer strukturen mellom de ulike beredskaps-systemene. Totalforsvarskonseptet innebærer gjensidig støtte og samarbeid mellom det militære og det sivile samfunn, og da i hele krisespekteret fra fred til sikkerhetspolitisk krise og krig.

Sivilt Beredskapssystem (SBS), sammen med Beredskapssystem for Forsvaret (BFF) og Politiets Beredskapssystem (PBS), utgjør et helhetlig Nasjonalt Beredskapssystem (NBS).

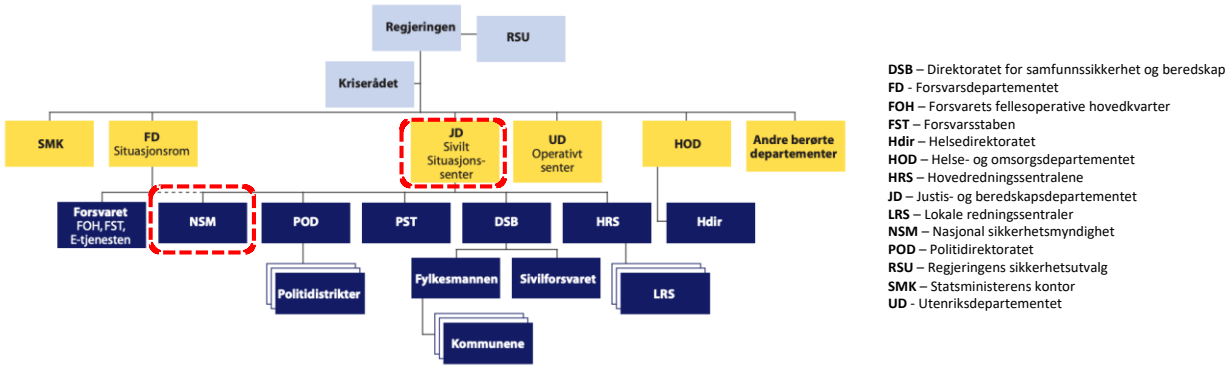
Disse ulike systemene inneholder forhåndsplanlagte prosedyrer og tiltak som kan benyttes for å forebygge og redusere skadeomfang ved kriser, katastrofer, terroranslag og krig. NBS er basert på NATOs krise- og beredskapsrammeverk (Forsvarsdepartementet og Justis- og beredskapsdepartementet, 2018, s. 26-27; Politidirektoratet, 2020, s. 18-19).



Figur 14 - Oversikt over nasjonalt beredskapssystem (Politidirektoratet, 2020, s. 18)

Samfunnssikkerhet og beredskap

Samfunnssikkerhet er et begrep som benyttes for å beskrive sikkerhet i forskjellige kontekster. I Norge er det regjeringen som har det øverste ansvaret for samfunnssikkerhet og beredskap (Forsvarsdepartementet og Justis- og beredskapsdepartementet, 2018, s. 67). I Figur 15 under vises myndighetenes organisering av sentral krisehåndtering ved sivile nasjonale kriser.



Figur 15 - Organisering av sentral krisehåndtering ved sivile nasjonale kriser (NOU 2021: 6, s.210)

I kapittel IV i Samfunnssikkerhetsinstruksen settes det krav til departementenes samfunnssikkerhets -og beredskapsarbeid. Her fremkommer det at departementene har det overordnede ansvaret for å kartlegge risiko innfor sitt ansvarsområde, og at de er ansvarlige for å ivareta beredskap innenfor egen sektor. Videre har departementene etablert forskjellige

direktorater som har myndighets-oppgaver og ansvar for å ivareta samfunnssikkerhet og beredskap innenfor eget ansvarsområde (Samfunnsikkerhetsinstruksen, 2017, kap. IV).

I dag er det 15 departementer i Norge, og det er derfor behov for en helhetlig forståelse og koordinering av samfunnssikkerhet og beredskap. Justis- og beredskapsdepartementet (JD) har et overordnet samordningsansvar for alle departementene i sivil sektor, og skal sikre at det utføres et nasjonalt og helhetlig samfunnssikkerhetsarbeid, se Figur 15 på forrige side. Videre har JD også et samordningsansvar for planlegging av Norges sivile beredskap (Meld. St. 17 (2001-2002), s. 100; Meld. St. 10 (2016-2017), s. 25).

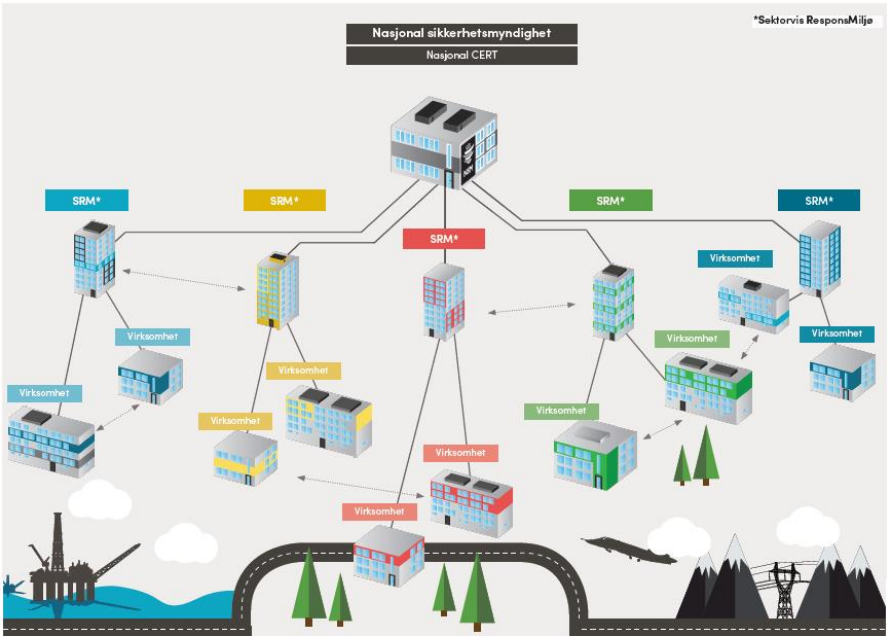
JDs samordningsansvar omfatter IKT-sikkerheten for alle sivile virksomheter. I tillegg har JD også ansvaret for å utarbeide nasjonale krav og anbefalinger innenfor IKT-sikkerhets-området for private og offentlige virksomheter (Meld. St. 38 (2016-2017), s. 19).

I regjeringens første stortingsmelding innenfor IKT-sikkerhet (Meld. St. 38 (2016-2017), s. 11) er IKT-ansvaret beskrevet. Ved å ta utgangspunkt i en tidligere stortingsmelding, hvor en tydeliggjorde at virksomheter og enkeltpersoner har et medansvar for egen sikkerhet, samt at alle må ta et ansvar for hvordan egne handlinger kan påvirke andres sikkerhet (Meld. St.10 (2016-2017), s. 7), ble medansvaret tydeliggjort for virksomheter og enkeltpersoner til å også omfatte IKT-sikkerhet. Videre ble det tydeliggjort at det er virksomhetene som har ansvaret for å ivareta egen IKT-sikkerhet (Meld. St. 38 (2016-2017), s. 19).

2.3 Ansvarsfordeling for nasjonal cyber-beredskap

Nasjonal sikkerhetsmyndighet (NSM) er et direktorat og er administrativt underlagt Justis- og beredskapsdepartementet som ble etablert i 2003. Forsvarsdepartementet (FD) har instruksrett overfor NSM, innenfor sitt ansvarsområde. NSM har et bredt ansvarsområde. Innen cyberdomenet har NSM ansvaret som rådgivende og kontrollerende organ, samt at de har ansvaret for å utarbeide et digitalt risikobilde som omfatter statssikkerhet, samfunnssikkerhet og individsikkerhet. JD har sammen med NSM det overordnede samordningsansvaret for å understøtte og bidra til cybersikkerhet i sivil sektor. Nasjonalt cybersikkerhetssenter (NCSC) er en del av NSM og de har ansvaret for alvorlige cyber-angrep eller cyber-hendelser i Norge. I tillegg har NCSC samordningsansvar for de sektorvise responsmiljøene (SRM) sammen med Felles cyber-koordineringssenter (FCKS). FCKS, som ledes av NSM, og består av Kripos, Etterretningstjenesten og PST, har som formål å styrke nasjonal evne til effektivt forsvar mot, og håndtering av, alvorlige hendelser eller kriminalitet i det digitale rom.

Responsmiljøet er også omtalt som CERT (Computer Emergency Response Team), NorCERT er en avdeling i NCSC og har nasjonalt ansvar for responsmiljøene slik som vist i Figur 16 under. De sektorvise responsmiljøene er typisk HelseCERT med virksomheter i helsesektoren, EkomCERT med teleoperatørene, FinansCERT med virksomheter i finanssektoren, KraftCERT med kraftprodusenter, transportører og distributører i kraftsektoren mfl. (JD og FD, 2019, s. 3-5, NSM, 2017a, s. 3-19).



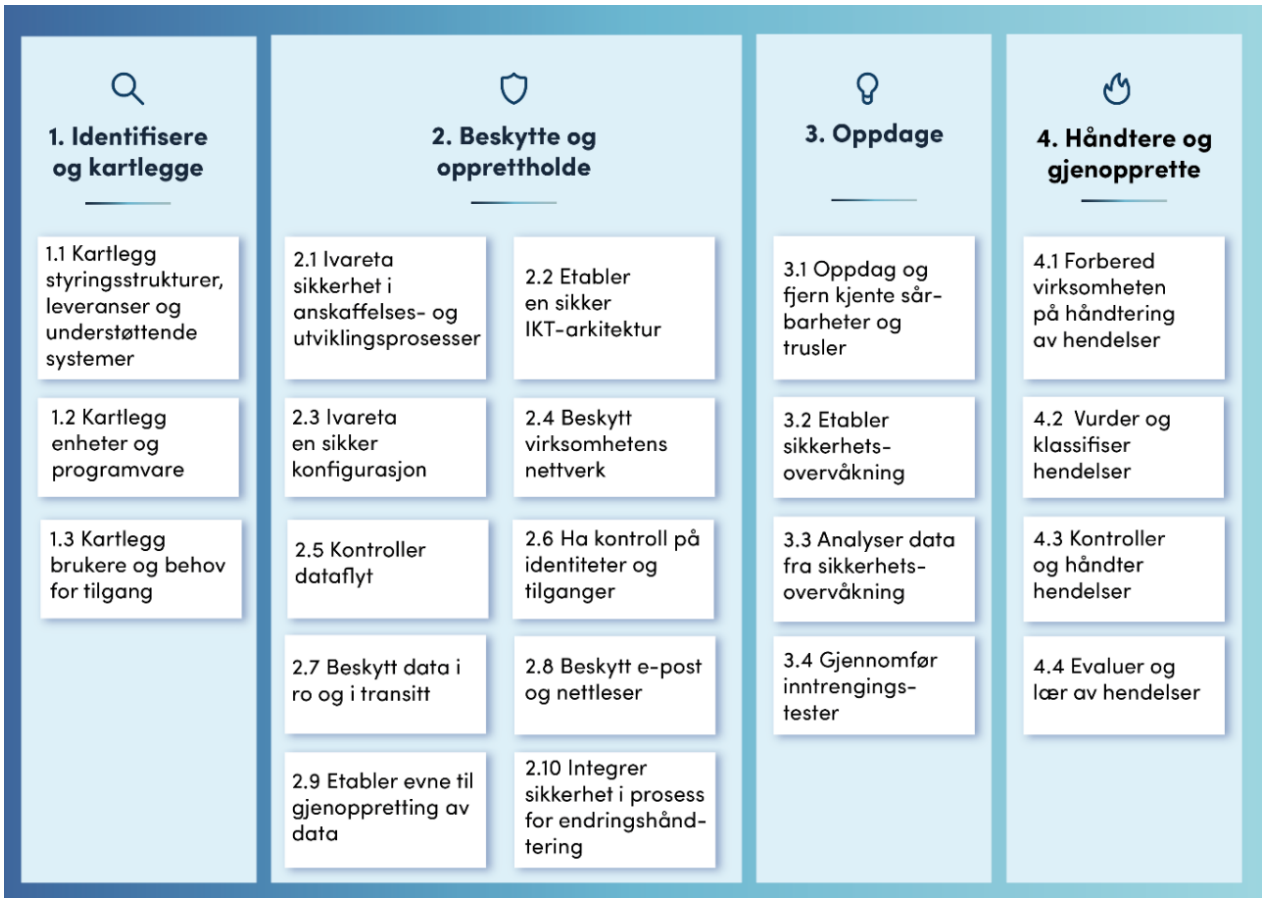
Figur 16 - Samhandling mellom NSM, SRM og virksomheter (NSM, 2017a, s. 12)

NSMs grunnprinsipper for IKT-sikkerhet

I 2018 utga NSM sin første utgave av grunnprinsippene for IKT-sikkerhet. Denne er basert på flere anerkjente standarder og rammeverk, blant annet fra International Organization for Standardization og The International Electrotechnical Commission (ISO/IEC 27001 og 27002), Center for Internet Security (CIS Critical Security Controls for Effective Cyber Defense), National Institute of Standards and Technology (NIST), Information Technology Infrastructure Library (ITIL) mfl. (NSM, 2020, s. 7-8).

Revidert versjon av Grunnprinsipper for IKT-sikkerhet ble utgitt i 2020, og NSM har videreutviklet grunnspinnsippene for å hensynta teknologisk utvikling. Grunnprinsippene har fire hovedkategorier, og de skal bidra til at virksomhetene etablerer en praksis som fungerer

som en forebyggende «grunnmur» for cybersikkerhet. Rammeverket med de fire hovedkategoriene med tilhørende sikkerhetsaktiviteter er vist i Figur 17 nedenfor:



Figur 17 - Oversikt over NSMs grunnprinsipper for IKT-sikkerhet (NSM, 2020a, s. 6)

Dersom en cyber-hendelse skulle inntreffe, skal man ha tiltak og erfaring for å normalisere situasjonen. Eksempel kan være som følger: Virksomheten har etablert tiltak som tar jevnlig sikkerhetskopier av sin digitale informasjon og IKT systemer. Men hvis man ikke øver og tester om sikkerhetskopien fungerer, vil det ta lenger tid før man får normalisering etter et evt. angrep, og i ytterste konsekvens vil sikkerhetskopien være ubrukelig (NSM, 2020a, s. 34-35).

2.4 Nasjonalt cyber-risikobilde

Sikkerhetstjenesten i Norge utarbeider årlig rapporter innenfor sitt ansvarsområde, og disse danner grunnlaget for nasjonalt cyber-risikobilde. *Fokus-rapporten* utgis av Etterretningstjenesten (Etterretningstjenesten, 2020, 2021 og 2022), *Nasjonal trusselvurdering*

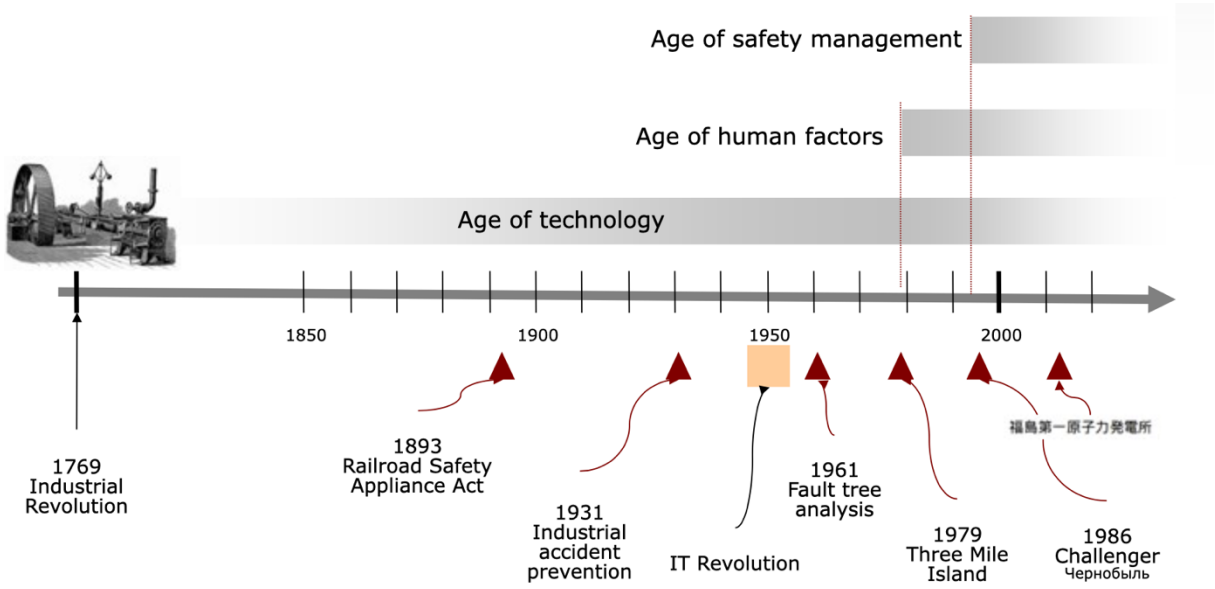
utgis av PST (PST, 2020, 2021 og 2022) mens *Risiko* utgis av NSM (NSM, 2020b, 2021 og 2022a). I Tabell 4 under har vi oppsummert de aktuelle fokusområdene i de ulike rapportene fra 2020 til 2022.

Tabell 4 - Overordnet risikobilde fra sikkerhetsmyndighetene fra 2020 og 2021

	2020	2021	2022
Fokus av E-tjenesten	Etterretning, påvirkning og trusler i det digitale domenet Mot nye våpenkappløp Internasjonal terrorisme Regionale konflikter og stormaktsrivalisering Fremmede stater: Kina og Russland	Etterretning, påvirkning og trusler i det digitale rom Internasjonal terrorisme Regionale konflikter og stormaktsrivalisering Fremmede stater: Kina og Russland Stormaktsrivalisering og opprustning	Et sammensatt trusselbilde Russlands åpne maktbruk Xi Jinpings Kina Internasjonal terrorisme Regionale konflikter
Nasjonal trussel -vurdering av PST	Terrorfinansiering Hvitvasking Kriminalitet som genererer utbytte [...]	Statlig etterretnings-virksomhet Politisk motivert vold – ekstremisme Trusselen mot myndighetspersoner	Statlig etterretnings-virksomhet Politisk motivert vold – ekstremisme Trusselen mot myndighetspersoner
Risiko av NSM	Avhengigheter mellom samfunnsfunksjoner Trusselaktører utnytter sårbarhetene våre Sårbarheter i et digitalt samfunn Informasjon og kompetanse i forebyggende sikkerhetsarbeid	Risikobildet Verdier av betydning for risikobildet Nasjonale sårbarheter på strategisk nivå Sårbarheter i virksomheter og samfunnsfunksjoner Sårbarheter ved systemer, infrastruktur og objekter Anbefalte tiltak	Vi må beskytte nasjonens viktigste verdier Våre viktigste nasjonale verdier må kartlegges Risikobildet Viktige samfunnsfunksjoner kan rammes Trusselaktører utnytter sårbare verdikjeder Lav sikkerhetsbevissthet svekker nasjonal sikkerhet Et taktskifte i cyberdomenet Tiltak for å styrke sikkerheten Sikkerhetsbevisstheten hos ledere og ansatte må heves Ta ansvar for sikkerhetsarbeidet Sikkerheten i IKT-systemene må styrkes

3 Teori

Sikkerhetsproblemet i moderne industri dukket opp fra den industrielle revolusjonen i 1769. I forbindelse med effektivisering og utvikling av transport og masseproduksjon har det blitt mulig å øke graden av mekanisk og elektrisk kraftutvikling. Dette har vært helt avgjørende å få teknologi- og produksjonsnivået raskt forbedret. Bakteppet av den utviklingen av industrialiseringen har det hatt en negativ effekt på arbeiderenes helse, miljø og sikkerhet med tanke på farlige og risikofylte arbeidsoppgaver: Age of technologies, Age of human factors og Age of safety management, se Figur 18. De primære bekymringene i hver tidsepoke har blitt endret i henhold til innovasjonsperspektivet (Hollnagel, 2014, s.21 - 32).



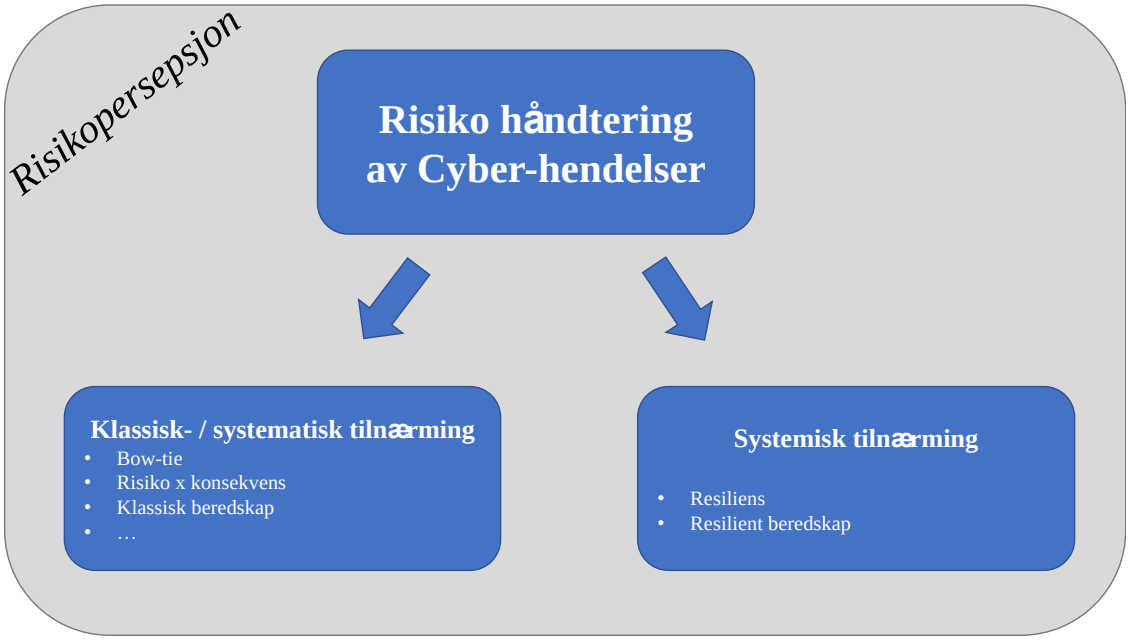
Figur 18 – Tre tidsaldere av sikkerhets perspektiver (Hollnagel, 2014)

Erik Hollnagel har oppsummert risikostyrings-historien som vist i Figur 18 over. **Den første tidsalderen** startet i ca. 1769 med den industrielle revolusjon, og den varte omtrent i 200 år. Den største trusselen i denne perioden var knyttet til bruk av dampkjeler. Upålitelig teknologi resulterte i mange eksplosjoner som var direkte farlige for menneskene og omgivelsene. Dette medførte at risikoforståelsen måtte tilpasses for å gjøre dampkjeler mer driftssikre.

Den andre tidsperioden startet i 1979 og var knyttet til katastrofen på kjernekraftverket på Three Mile Island. Før denne hendelsen var det en felles enighet om at de risikoanalyse-metodene som var i bruk, f.eks. HAZOP, FMEA, feiltre mfl. ville være tilstrekkelig for å sikre

sikkerhet ved kjernekraftverk. Etter selve katastrofen ble det smertelig klart at noe manglet i de eksisterende risikoanalyse-tilnærmingene, og det var *den menneskelige faktoren*. **Den tredje tidsalderen**, også kalt Age of the safety management, startet i 1986 med to ulykker, mislykket oppskyting av romfergen Challenger, og nedsmelting av reaktor fire ved kjernekraftverket i Tsjernobyl. En konsekvens av disse ulykkene var at sikkerhetsstyringssystemer ble satt på dagsorden (Hollnagel, 2014, s. 24-32).

Samfunnsutviklingen har bidratt til at myndigheter og virksomhetseiere idag stiller høyere krav til sikkerhet og forsvarlig drift, samt til større grad av risikostyring. Formålet med dette er å «sikre den riktige balansen mellom det å utvikle og skape verdier, og det å unngå ulykker, skader og tap» (Aven, 2015, s. 14; Lunde, 2019, s. 28). Stor grad av digitalisering i alle typer virksomheter har medført at klassisk systematisk risikostyring ikke lenger er tilstrekkelig for å håndtere dagens cyber-risiko. Flere forskere mener at en systemisk tilnærming (resiliens) kan bidra til å håntere ukjente og plutselige cyber-hendelser bedre enn en klassisk systematisk risikostyring (Nemeth og Hollnagel, 2021, s. 2-3; Woods, 2019, s. 52-54), ref. Figur 19.



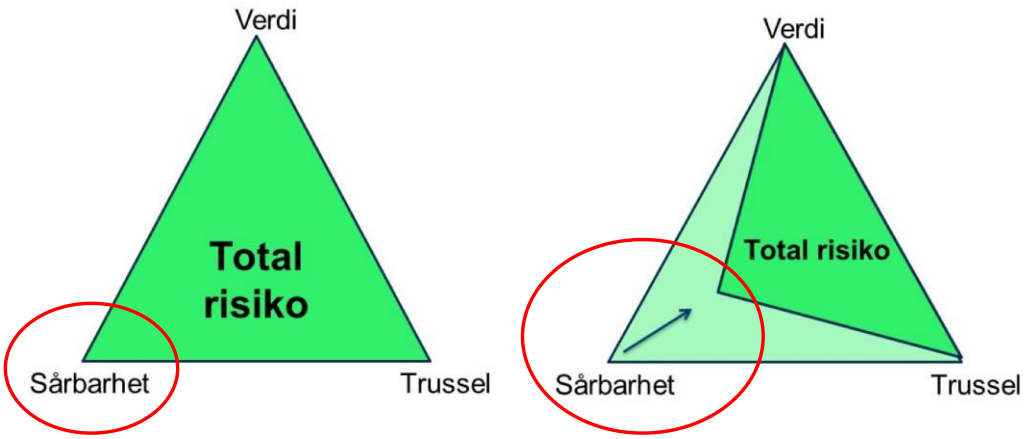
Figur 19 – Skisse av teori kapittel

3.1 Risiko

3.1.1 Risikokonsept

Risikoanalyse – Verdi, trussel og sårbarhet

Ifølge faglitteraturen er ikke sannsynlighet og konsekvenser i en sikkerhets- og beredskaps-kontekst alltid egnet for å beskrive risiko. Eksempel på dette kan være tilsiktede hendelser som cyber-angrep eller insider-problematikk. Istedenfor å vurdere sannsynlighet og konsekvenser, kan en benytte en sikringsrisikoanalyse for å identifisere og vurdere virksomhetens verdier (V), trusler (T) og sårbarheter (S). Denne analysemetoden omtales ofte som risikotrekanten, og når disse tre faktorene sammenstilles utgjør de til sammen sikringsrisikoen, se i Figur 20 (Njå et al., 2021, s. 259).



Figur 20 – Risikotrekanten (Busmundrud et al., 2015, s. 34)

Risikoanalyser er subjektive vurderinger, og er basert på bakgrunnskunnskapen til de som er involvert i analysearbeidet, samt tilgjengelig informasjon (Aven, 2015, s. 55-56). En sikringsrisikoanalyse kan, som andre risikoanalyser, utføres på ulike måter, og de metodiske valgene og forståelsen av begreper er avgjørende for hvordan en analyserer og presenterer sikringsrisiko (Standard Norge, 2014b).

ROS-analyse er et begrep som kan forstås som en «samlebetegnelse for en rekke systematiske fremgangsmåter for å identifisere, beskrive og/eller beregne risiko og sårbarhet» (Rausland og Utne, 2014, s. 369).

I tillegg til å ha forskjellig tilnærming til risiko, kan risikoanalyser utføres på ulike måter. Ifølge Terje Aven kategoriseres risikoanalysene i tre hovedkategorier (Aven et al., 2017, s. 16): Disse er forenklet risikoanalyse, standard risikoanalyse og modellbasert risikoanalyse som oftes er benyttet og omtalt.

3.1.2 Risikopersepsjon

Risikopersepsjon handler om hvordan vi mennesker forstår, opplever og håndterer risiko og farer (Aven et al., 2019, s. 40; Njå et al., 2020, s. 47)). Det finnes mye litteratur om hva som påvirker vår risikooppfatning, og om hvordan dette påvirker våre beslutninger (Engen at el., 2016, s.94). Ifølge Marit Boysen er det en sammenheng mellom opplevd risiko og hvordan en forholder seg til risiko (Boysen, 2003, s. 4). Risikopersepsjon tilhører, ifølge Boysen, det psykologiske perspektivet på risiko, mens risikoforståelse og opplevd risiko er tema innenfor de kulturelle og sosiologiske perspektivene på risiko (Boysen, 2003, s. 9).

I faglitteraturen beskriver en at det er mulig å skille risikopersepsjon fra risiko. I en slik betraktning baserer risikopersepsjon seg på enkeltpersoners kognitive egenskaper, individuelle verdier, og personlige erfaringer, som forklares med at enkeltpersonen blir isolert i sin egen virkelighetsoppfatning. Når en eller flere personer skal vurdere risiko eller usikkerhet, er resultatene avhengig av dem som vurderer dette, og vurderingen er også avhengig av at man benytter felles kunnskap om metoder og teorier. Risiko- og usikkerhetsbildet baseres ofte på kunnskap «*sett gjennom øynene»* til de som vurderer, og i en slik betraktning er disse knyttet sammen med risikopersepsjon. Dersom en klarer å skille mellom risiko- og usikkerhetsdefinisjoner basert på egne oppfatninger og verdivurderinger, kan risikopersepsjonen likevel holdes adskilt fra risiko (Engen et al., 2020, s. 82).

Men ifølge Boysen er det vanskelig for de fleste mennesker å vekte sannsynlighet og konsekvens opp mot hverandre. Hun hevder at risikoopplevelse eller risikopersepsjon antas å påvirke adferd, og derfor også sannsynligheten for at mennesker gjør feil. Dette kan skje innenfor flere forhold, mellom atferd og situasjon, mellom situasjon og risikoopplevelse, samt mellom risikoopplevelse og adferd (Boysen, 2003, s. 9-10). Innenfor psykologifaget beskrives flere faktorer som har betydning for risikopersepsjon. Risikoforståelsen er, ifølge

faglitteraturen, i stor grad individuell og endrer seg over tid. Det betyr at folk kan vurdere noe som risikabelt på et tidspunkt, men så kan risikoforståelsen endre seg dersom en har vært eksponert for risikoen i en lengre tidsperiode (Boysen, 2003, s. 3). Et annet perspektiv knyttet til risikopersepsjon handler om hva som skjer når informasjon som beskrives som viktig, er mottatt. På bakgrunn av den mottatte informasjonen vurderer man sannsynligheten for at en uønsket hendelse skal inntreffe. Dette beskrives som fornuftsreaksjoner som normalt trer i kraft for å behandle, systematisere og selektere sanseinntrykkene våre (Engen et al., 2020, s. 82-95). Ifølge Boysen underestimerer folk risiko som man selv forventer å ha kontroll over, og man underestimerer risikoen for at sjeldne hendelser skal ramme nettopp en selv (Boysen, 2003, s. 16).

Innenfor psykologifagfeltet er det flere enn de ovennevnte faktorene som har betydning for risikopersepsjon. Når f.eks. personer får presentert informasjon som utfordrer deres oppfatninger om sannsynlighet eller mulighet for at hendelser oppstår, vil de ofte «tone ned» eller overse informasjonen. I tillegg er det slik at man vurderer at sannsynligheten er høyere for at hendelser som man betrakter som alvorlige skal inntreffe.

Når en skal bestemme hvilket risikonivå som er akseptabelt, er det ikke et teknisk spørsmål, men et verdispørsmål, og følgelig vil det måtte omfatte både politiske og etiske overveielser (Aven et al., 2003, s. 18-22).

3.1.3 Risikostyring

I faglitteraturen beskrives risikostyring som et systematisk forsøk på å styre fremtids-utviklingen, hvor risikostyring da kan forståes som «*alle tiltak og aktiviteter som gjøres for å styre risiko*» (Lunde, 2019, s.27; Aven, 2015, s. 13).

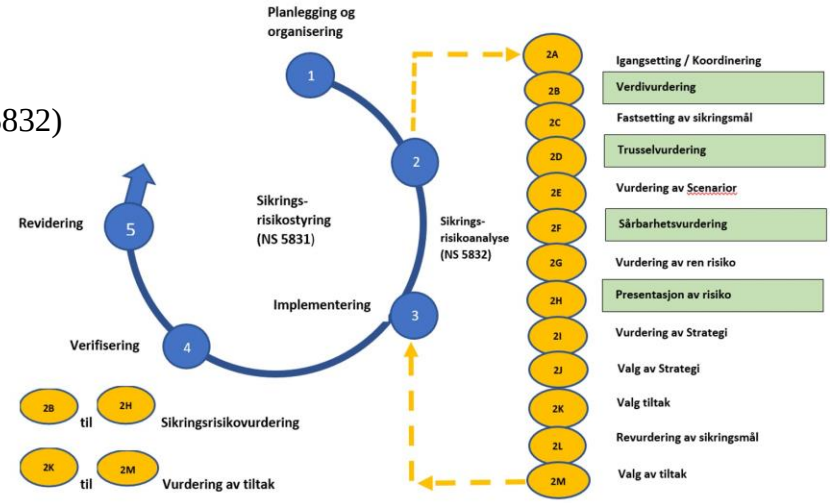
Det finnes mange metoder for, og mye teori om, hvordan risikostyring og beslutningsprosesser bør operasjonaliseres (Aven, 2015, s. 145).

Risikostyring kan innebære beslutningstaking i situasjoner med store usikkerheter og høy risiko, og det kan da være utfordrende å forutsi konsekvensene av beslutninger (Aven, 2015, s. 17). En utfordring en beslutningstager kan forvente når en beslutning skal tas, er at beslutningsunderlaget ikke gir all den informasjon som ansees som viktig før beslutning skal tas (Aven, 2015, s. 18). Videre kan beslutninger omfatte vanskelige avveininger i forhold til

verdier og usikkerhet. I tillegg kan ulike beslutningssituasjoner kreve forskjellige beslutningsstrategier (Aven, 2015, s. 20).

For de fleste er beslutningstaking i hverdagslige situasjoner, hvor det er risiko knyttet til beslutningen, velkjent. Når man har foretatt en beslutning, har man, ifølge Aven, da også definert risikoen som akseptabel (Aven, et al., 2003, s. 20). For folk flest høres dette fornuftig ut, men det er mange utfordringer knyttet til bruk av risikoanalyser før en beslutning tas. Dette fordi det ikke er opplagt for alle hva risiko betyr. Upresise og uklare begrepsdefinisjoner begrunnes som en av årsakene til at risiko er vanskelig å forstå (Aven et al., 2017, s. 198; eget arbeid, 2021, s. 8). Vår problemstilling handler om Cyber-beredskap, og ifølge faglitteraturen bør det være problemstillingen som styrer hvilke metoder en skal benytte når en skal analysere risiko. Med bakgrunn i ovennevnte, kan noen fagmiljøer som vanligvis arbeider med sikringsrisiko, benytte seg av risikostyringsmodellen Norsk Standard 5831 (Standard Norge, 2014a), hvor en benytter sikringsrisikoanalysen i risikostyringsprosessen. Sikringsrisikomodellen i Figur 21 under har følgende 5 steg (Njå et al., 2020, s. 320; Standard Norge, 2012, 2014a og 2014b).

(1) Planlegging og organisering
(2) Sikringsrisikoanalysen (NS5832)
(3) Implementering av tiltak
(4) Verifisering
(5) Revidering



Figur 21 – Illustrasjon av sikringsmodell iht. NS5831 (Njå et al., 2020, s. 320)

Risikostyring i kontekst av safety eller security har samme målsetting knyttet til å finne frem til tiltak som skal håndtere risiko. Det er to vitenskapelige retninger som kan benyttes når en skal dimensjonere sikringstiltak som skal fungere i lang tid fremover, systematisk og systemisk tilnærming.

Flere forskere er kritiske til bruk av systematisk risikostyring, fordi tradisjonell scenariotenkning, sannsynlighetstilnærming og konsekvenstenkning, i for stor grad blir knyttet opp mot historiske data og kunnskap, slik at en mister fremtidsperspektivet når en skal dimensjonere sikringstiltak. Trusler innenfor security er vanskelig å forutse, og den andre vitenskapelige retningen, den systemiske, er knyttet til at en isteden legger til grunn tanker og ideer om fremtiden. Ved å benytte systemisk tilnærming vil en tilrettelegge for mer fleksibilitet, samt tilpasse seg nye og uventede situasjoner, som ifølge faglitteraturen åpner opp for å vektlegge bruk av resiliens (Njå et al., 2020, s. 320).

Sikkerhetsbegrepet

Det finnes ingen entydig akademisk definisjon på Security (Jore, 2019, s. 159). Både «security» og «safety» betyr sikkerhet på norsk, og dette kan være forvirrende. Videre benyttes disse ordene på forskjellige måter, avhengig av kontekst og språk.

La oss se på et eksempel relatert til en nødutgang for et datasenter. Hvis det oppstår en brann, slik at personell inne i datasenteret må evakuere seg selv, må nødutgangen være åpen eller lett kunne åpnes, slik at evakueringen kan skje raskest mulig. På den andre siden skal det være mekanismer på den samme nødutgangsdøren som sikrer datasenteret mot innbrudd, oppdager forsøk på innbrudd eller sabotasje, og evt. varsler dette videre til relevante enheter. Dette betyr at nødutgangen må designes og dimensjoneres med sikringstiltak som hensyntar begge perspektivene (Steen et al., 2021, s. 6). Det er en pågående diskusjon i fagmiljøene om likheter og ulikheter innen safety- og security-områdene.

3.2 Sikkerhetskultur og sikkerhet i dybden

I et kulturperspektiv kan sikkerhet betraktes som delte tankemønstre og forestillingsevne knyttet til trusler og farer. (Engen, 2016, s. 158).

Det finnes flere og ulike kultur-aspekter, hvor psykologer, sosiologer, antropologer bidrar ut ifra sine respektive fagområder, og hvor adferd, verdier og kognitive systemer beskrives som fasetter i en kultur (Westrum og Adamski, 2009, s. 67-104).

Ifølge Ranveig Kviseth Tinmannsvik er adferd i arbeidssituasjoner et resultat av ulike påvirkninger. Selv om en virksomhet etablerer et ledelsessystem eller styringssystem med styrende dokumenter som beskriver ansvarsforhold, og etablerer prosedyrer og

kommunikasjonslinjer for hvordan arbeid i virksomheten skal utføres, så er ikke dette alltid tilstrekkelig for at arbeidet blir utført som planlagt. Ifølge Tinmannsvik må menneskene i organisasjonen også ha en kultur for å tenke og handle i henhold til gjeldende arbeidspraksis. Kultur er normer, verdier og forståelsesrammer som bidrar til handling. Kultur bygges og utvikles gjennom samhandling i et fellesskap, og beskrives som et felleseie, og omfatter også alt som ikke kan formaliseres i et styringssystem (Tinmannsvik, 2008, s. 134). Sikkerhets-kultur er et begrep som handler om verdier, oppfatninger, holdninger og kommunikasjon og samspill mellom mennesker (Rausand og Utne, 2014, s. 232). Det finnes ikke *en* definisjon eller forklaring i den norske faglitteraturen på hva som menes med sikkerhetskultur som det er felles enighet om. Derimot finnes det flere måter å beskrive sikkerhetskulturen til en organisasjon på. I tillegg finnes det mange eksempler på hva som kjennetegner en organisasjon med dårlige eller gode sikkerhetskulturer. Når vi skal beskrive en organisasjon med god sikkerhetskultur i denne masteroppgaven, velger vi følgende beskrivelse:

> *«At den er kjennetegnet ved at menneskene:*
>
> - *alltid er rede til å forvente det uventede*
> - *til enhver tid er i stand til å forstå hva de skal gjøre*
> - *er åpne for forslag, og*
> - *er i stand til å tro på at egne handlinger har en virkning på dem selv og andre» (Tinmannsvik, 2008, s. 134)*

I tillegg til ovennevnte beskrivelse av hva som kjennetegner mennesker i en organisasjon med god sikkerhetskultur, finnes det beskrivelser på at sikkerhetskultur kan bli gradert på ulike nivåer. I faglitteraturen til Resilience Engineering (RE) som vi beskriver i kapitel 3.3.2 blir sikkerhets-kulturen delt opp i fem nivåer, hvor typisk karakteristikk og adferd eller respons for hvert nivå beskrives. I et slikt tankesett legges det som en viktig forutsetning at organisasjoner som ønsker å forbedre seg, har en målsetting om å utvikle seg fra ett nivå til nivået over, se eksempel i Tabell 5 på neste side (Nemeth og Hollnagel, 2014, s. 181):

Tabell 5 – Fem nivåer av sikkerhetskultur (Nemeth og Hollnagel, 2014, s. 181, egen oversettelse)

Nivå	Karakteristikk	Typisk respons etter hendelse
Resilient	Sikker adferd er intergrert i alt organisasjonen utfører	Gjennomføre en revurdering av sikkerhetspolicier og praksis
Proaktive	Vi arbeider med problemer som vi oppdager	Felles oppfølging eller undersøkelse
Kalkulativ	Utfører alltid styrende dokumente	Standard måte å følge opp hendelser på
Reeaktiv	Sikkerhet er viktig og gjør mye etter at det har skjedd en hendelse	Begrenset med oppfølging eller undersøkelse
Patalogisk	Organisasjonen er mer opptatt av å ikke få skylden, og mindre opptatt av sikkerhet	Ingen oppfølging eller undersøkelse

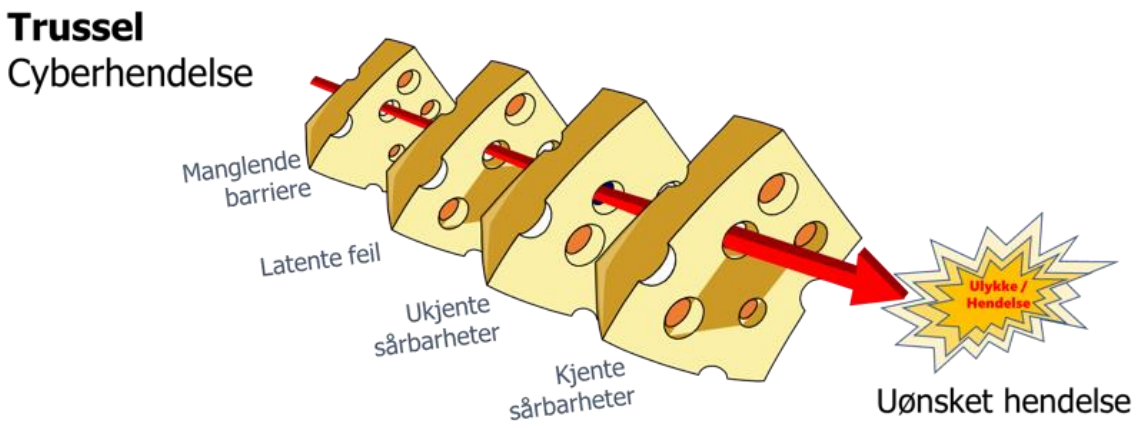
Det er mange som har forsøkt å operasjonalisere sikkerhetskultur (Engen, 2016, s. 157), men det er få begrep som er så lite forstått som sikkerhetskultur (Reason, 2016, s. 191). Ifølge James Reason består sikkerhetskultur av flere underkulturer, og han understreker viktigheten av å ha et effektivt informasjonssystem for sikkerhet som bla. består av følgende underkulturer (Reason, 2016, s. 194-196):

> *"en rapporterende kultur, en "bry seg" kultur, en fleksibel kultur og en lærende kultur" (Reason, 2016, s. 194-196, egen oversettelse)*

Sikkerhet i dybden

«*Sikkerhet i dybden*» eller «*beskyttelse i dybden*» er begreper som tradisjonelt benyttes i fysisk sikkerhet i kombinasjon med positivt tidsregnskap. Hovedhensikten er å ha tilstrekkelig med barrierer, slik at en evt. inntrengning tar lengre tid enn sikringsstyrkenes responstid, og formålet er å forhindre eller begrense tap av verdier (Forsvarsbygg, 2017, s. 17-22 og 195-196).

James Reason har forsket på ulykker og bakenforliggende årsaker til hvorfor ulykker eller uønskede hendelser oppstår i virksomheter med sammensatte komplekse systemer. Hans teori handler om at når uønskede hendelser eller ulykker oppstår, er dette oftest utløst av handlinger utført av oss mennesker. Den bakenforliggende årsaken derimot, er ikke mennesket i seg selv, men ulike typer sårbarheter i barrierer i systemer. Videre forklarer Reason at uønskede hendelser ikke oppstår bare på grunn av tilfeldigheter. Han introduserer to sentrale begreper som kan knyttes til årsaken til at uønskede hendelser inntreffer; 1) aktive feil og 2) latente feil.



Figur 22 – Illustrasjon basert på Sveitserostmodellen (Reason, 1997, s.12)

Reason har illustrert dette gjennom sveitserostmodellen (se Figur 22), hvor menneskelige, tekniske og organisatoriske innretninger ikke skal ha svakheter. En barriere er en komponent som enkeltvis, eller sammen med flere, skal bidra til å redusere sannsynligheten for at en bestemt uønsket hendelse skal oppstå. Hullene som er illustrert i sveitserosten i Figur 22 over, oppstår med bakgrunn i aktive eller latente feil (Reason 1997, s. 12). I et styringssystem kan det for eksempel være feil bruk av det tekniske utstyret, feil design på det tekniske utstyret, svakheter ved utstyret etc. For å unngå uønskede hendelser, er det viktig at slike hull som beskrevet over tettes igjen.

Tidlig på 1990-tallet utviklet Stephen Paul Marsh et konsept for sikkerhet for logiske systemer. Han hevder at det må være tillit mellom IT-systemer på tilsvarende måte som det er tillit mellom mennesker. Det sentrale bak Marshs modell for «Zero Trust» er å *«aldri stole på og alltid kontrollere»*. Med dette mener han at ingen mennesker må gis tilgang til noen enheter eller applikasjoner før de er klarert og autorisert for *hver enkelt* av disse. Dette betyr at en person som tidligere er klarert, autorisert og har hatt tilgang til enheter eller applikasjoner på generell basis, vil miste sine tidligere tildelte rettigheter (Marsh, 1994, s. 199-200). Det må i stedet gis ny tilgang og nye rettigheter til *hver enkelt* enhet, applikasjon eller tjenester, og ikke på generell basis. Zero Trust har videre utviklet seg sammen med den teknologiske utviklingen og prinsippene benyttes i de fleste moderne virksomhetsnettverk. Disse virksomhetsnettverkene består som regel av mange sammenkoblede IT-systemer, som deles inn i *interne*, de som er kontrollert av virksomheten selv med stor grad av kontroll og styring, og *eksterne*, de som eies og forvaltes av andre aktører, og hvor virksomheten selv har lav grad av kontroll og styring.

På grunn av at kompleksiteten i sammenkoblede IT-systemer er høy, kan man ha ulike sikkerhets-soner (bygger på samme prinsippet som *sikkerhet i dybden*), ulike typer skytjenester

og sammensatt infrastruktur mm. En Zero Trust-tilnærming tar til orde for at tilgang til programmer og tjenester ikke gis før det er foretatt gjensidig godkjenning, inkludert kontroll av identiteten og integriteten til IT komponenter. Det tas ikke hensyn til fysisk eller logisk plassering. (Rose et al., 2020, s. 1-3).

Zero Trust er ikke kun en tradisjonell tilnærming, men den har flere prinsipper og egenskaper som kan ligne på en systemisk risikobasert tilnærming for sosiotekniske systemer. Dette kommer vi nærmere inn på i neste kapittel.

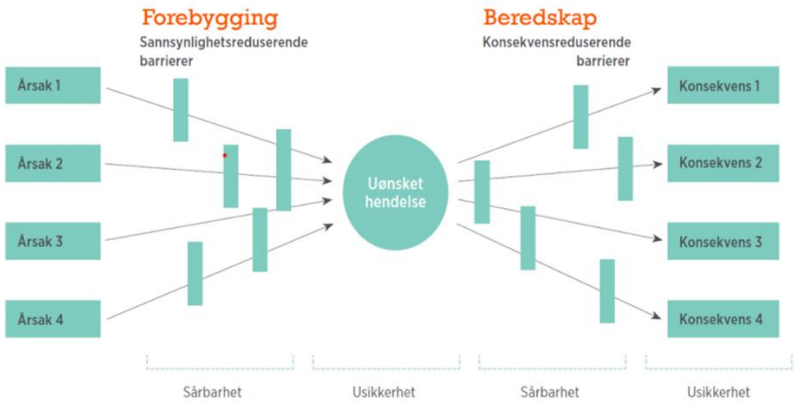
3.3 Cyber-beredskap

3.3.1 Systematisk - tradisjonell tilnærming

Formålet med beredskap

Det er flere formål med beredskap. Innenfor petroleumssektoren har man definert følgende hovedformål med beredskap: «å forhindre eller begrense konsekvenser av ulykker og tilløp til ulykker» (Meld. St. 12 (2006-2006), s. 46-47; Meld. St. 12 (2017-2018), s. 53-54). I forrige kapittel beskrev vi hvordan beredskap kan være et tiltak og en del av en risikobasert styring, når virksomhetene forholder seg til sine verdier knyttet til sannsynligheter med tilhørende konsekvenser. I dette perspektivet er formålet med beredskap å kunne iverksette risikoreduserende tiltak, og å forhindre at en uønsket cyber-hendelse inntreffer etter at det er oppdaget en fare eller en trusselsituasjon.

Ifølge Ivar Lunde handler formålet om å ivareta sannsynlighets- og konsekvensreduserende barrierer. Det første handler om å sikre opprettholdelse av etablerte sannsynlighetsreduserende barrierer, samt opprette nye sannsynlighetsreduserende tiltak eller barrierer når det er et akutt behov. Sannsynlighets- reduserende tiltak og barrierer blir ofte også benyttet som forebyggende tiltak. Videre, og etter at en hendelse er inntruffet, er målsettingen å redusere konsekvensene ved å iverksette planlagte- og «nye» konsekvensreduserende tiltak eller barrierer (Lunde, 2019, s. 41-42). I Figur 23 på neste side benytter vi et sløyfediagram (bow-tie) for å vise sannsynlighets- og konsekvensreduserende barrierer før og etter at en hendelse inntreffer:



Figur 23 – Sløyfediagram (DSB, 2017)

I et virksomhetsperspektiv er formålet med beredskap å etablere tiltak for å opprettholde og iverksette barrierer, å ivareta menneskene og verdiene, samt virksomhetens omdømme. Dersom en alvorlig hendelse inntreffer, er det viktig at beredskapsressursene utfører handlinger i en rekkefølge som ivaretar menneskene, verdiene og virksomhetens omdømme. Det er derfor viktig at virksomhetene er godt kjent med hva som er deres verdier, slik at en gjør en prioritering av disse. Slike verdier omtales i faglitteraturen ofte som beredskapsverdier, og en prioritering av disse skal bidra til at beredskapsressursene ivaretar de verdiene som til enhver tid har høyest prioritet i virksomheten (Lunde, 2019, s. 132).

Systematisk prosess for etablering av beredskap

I faglitteraturen finnes det flere metodiske tilnærminger som kan benyttes som verktøy når en virksomhet skal etablere beredskap. Ivar Lunde har utarbeidet en praktisk tilnærming i sin metodikk for beredskapsetablering, som han beskriver som en «systematisk prosess for å planlegge og implementere egnede beredskapstiltak» (Lunde, 2019, s. 58). Den systematiske prosessen er delt opp i følgende overordnede arbeidsprosesser (Lunde, 2019, s. 58-59).

A) Identifiseringsarbeidet handler om å beskrive hvilke ambisjoner virksomheten har til beredskap, utføre ROS-analyser, avklare ytelsesrammer og ytelseskrav, samt gjennomføre beredskapsanalyser for å dimensjonere tiltakene som er nødvendige for å ivareta de ulike beredskapsbehovene
B) Etablerings-arbeidet handler om etableringsarbeidet for å utarbeide nødvendig beredskapsplan og beredskapsdokumentasjon, samt gjennomføre nødvendig opplæring i egen organisasjon

C) Evaluerings-arbeidet handler om å kontrollere at virksomheten har etablert en tilfredsstillende beredskapsevne gjennom øvelser, læring og kontinuerlig forbedring

Flere forfattere beskriver i sin faglitteratur at ROS-analyser må benyttes på flere områder enn i dag, og de argumenterer for at det må være en sterk kobling mellom forståelsen og nytteverdien mellom analyse, system, tiltak og barrierer (Njå et al., 2020, s. 230). De introduserer en systematisk modell, Beredskapsplanleggingshjulet, for etablering av beredskap. Beredskapsplanleggingshjulet består av totalt 6 steg, og er en metodisk fremgangsmåte som kan brukes i arbeidet med å få etablert et beredskapsplanverk, hvor beredskapsøvelser og læring inngår. Virksomhetsledelsen blir tidlig involvert for å avklare ambisjoner og målsettinger knyttet til etablering av beredskap. Deretter skal virksomheten kartlegge og gjennomføre ROS-analyser for å ivareta virksomhetens sikkerhet. Hensikten med ROS-analysene er å få et kunnskapsgrunnlag, slik at virksomheten kan gjennomføre tiltak for å oppnå akseptabel risiko. Slike tiltak beskrives også som forebyggende tiltak, og blir utført før hendelser inntreffer, for å redusere risiko. Eksempel på dette kan være å redusere risiko for at en cyber-hendelse inntreffer, samt for å begrense konsekvensene dersom cyber-hendelsen likevel skulle inntreffe (NOU 2015: 13, s. 257). I tillegg er hensikten med å gjennomføre kunnskapsbaserte ROS-analyser, å kunne redusere konsekvensene av en ekstraordinær hendelse dersom den likevel oppstår (NOU 2021: 6, s. 56). Etter å ha gjennomført ROS-analysene og definert sikkerhetsnivået, vil det alltid være en restrisiko (NOU 2015: 13, s. 35-36), og det er denne restrisikoen som legges til grunn når en skal etablere beredskap for å kunne håndtere alvorlige cyber-hendelser.

I Figur 24 nedenfor vises de ulike stegene i Beredskapsplanleggingshjulet. (Njå et al., 2020, s. 231).

(1) Beskrive ambisjoner, mål, rammer, ressurser, budsjett og tidsplan for etablering av beredskap.

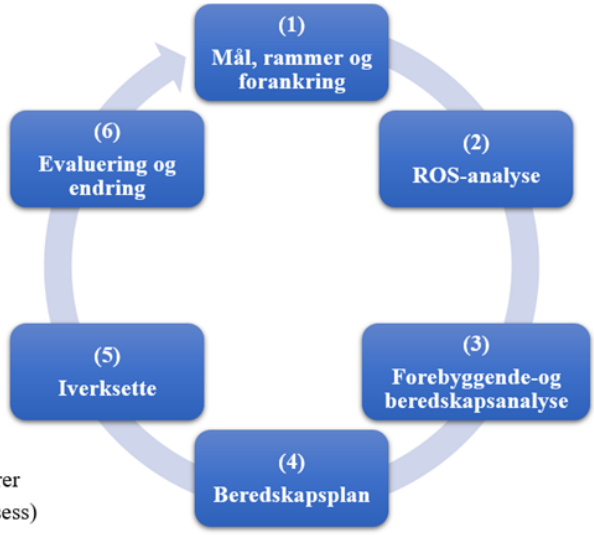
(2) Gjennomføre ROS-analyse

(3) Utføre forebyggende beredskapsanalyse for etablering av forebyggende beredskap, og utføre beredskapsanalyse for etablering av beredskap

(4) Utarbeide beredskapsplan og plandokumenter. Omfatter både forebyggende- og beredskapsplaner. Utarbeide planer for kompetanse, opplæring, trening og øvingsplaner,

(5) Iverksette og implementere beredskapsplanene fra steg 4

(6) Utføre evalueringer og vurdere om etablert beredskap fungerer som planlagt, deretter regelmessig, steg 1-6 (forbedringsprosess)



Figur 24 - Beredskapsplanleggingshjul med 6 steg (Njå et al., 2020, s. 230)

Flere tilnærminger for beredskap

Vi har ikke en omforent definisjon av hva som menes med beredskap i det norske samfunnet (NOU 2021: 6, s. 55). Likevel er felles forståelse av begreper eller kunnskap en forutsetning for hvordan begrepet *beredskap* benyttes for å kunne samhandle effektivt (St.meld. 10 (2016-2017), s. 25) i ulike beredskapssituasjoner. I denne Stortingsmeldingen er beredskap definert som «planlagte og forberedte tiltak som gjør oss i stand til å håndtere uønskede hendelser slik at konsekvensene blir minst mulig» (St.meld. 10 (2016-2017), s. 26). Vi har lagt til grunn følgende definisjon av beredskap i denne masteroppgaven da denne er mer utfyllende og kriseperspektivet er inkludert. Ivar Konrad Lunde definerer beredskap i sin faglitteratur som «*tiltak for å forebygge, begrense eller håndtere uønskede hendelser og kriser*» (Lunde, 2019, s. 38).

Beredskap omfatter alle «menneskelige, tekniske og organisatoriske tiltak som kan hindre at en faresituasjon utvikler seg til en uønsket hendelse, eller som kan bidra til å redusere skadevirkningene av inntrufne hendelser» (Njå et al., 2020, s. 272). Vår tilnærming til beredskap i denne masteroppgaven handler om «å være beredt», dvs. være forberedt på å håndtere uønskede hendelser som kan være ekstraordinære eller uforutsette. Etablert beredskap

omfatter de planlagte og forberedte tiltakene som er nødvendige for å håndtere det beredskaps-behovet som oppstår når de uønskede hendelsene inntreffer (Njå et al., 2020, s. 280).

Daglig beredskap kan beskrives som den beredskapen som er etablert for å håndtere dagligdagse uønskede cyber-hendelser. Noen virksomheter etablerer, i tillegg til sin driftsorganisasjon, en *sideorganisasjon*, og denne kan beskrives som virksomhetens beredskapsorganisasjon, som har som oppgave å håndtere *ekstraordinære* uønskede cyber-hendelser. Etablering av en egen beredskapsorganisasjon kan være basert på en strategisk ledelsesbeslutning fordi uønskede hendelser kan være så akutte, komplekse, omfattende eller spesielle, at den daglige beredskapen ikke har kapasitet eller kompetanse til å håndtere en cyber-hendelse innenfor forsvarlige rammer. I tillegg vil organisasjonen som skal håndtere ekstraordinær beredskap, ha tilgang til ekstra ressurser (interne og eksterne) og nødvendige fullmakter for å kunne håndtere *ekstraordinære* uønskede hendelser (Lunde, 2019, s. 40).

Terje Aven beskriver at en «risikoanalyse er en analyse av risiko, samt at sårbarhet er et aspekt av risiko». Innenfor samfunnssikkerhets-fagfeltet i dag, er det flere bransjer og fagfelt som har lovkrav til at det skal utføres ROS-analyser. Eksempel på dette er kommunal beredskapsplikt, hvor kommunene er forpliktet til å utføre ROS-analyser. I en ROS-analyse er sårbarhetsanalysen en del av risikoanalysen, hvor en vektlegger sårbarhet i analysearbeidet. (Aven, 2015, s. 48).

Flere av virksomhetene som ble rammet av cyber-hendelser i 2021 var norske kommuner. Til tross for forskriftskrav, er det ikke opplagt for kommunene, eller for de som utfører praktisk arbeid knyttet til ROS-analysen, hva kravene til risiko- og sårbarhetsanalyser egentlig innebærer. Ifølge Ove Njå og Kirsti Russell Vastveit, som har forsket på hvordan norske kommuner gjennomfører ROS-analyser, er det utfordrende at forskriften inneholder flere begreper som er vanskelige å forstå eller å tolke, og at dette bidrar til at det stilles kompetansekrav til de som skal operasjonalisere det praktiske arbeidet knyttet til ROS-analysen. I tillegg har en helhetlig ROS-analyse, ifølge Njå og Vastveit, en tendens til å bli for «altomfattende», og dette bidrar til at flere kommuner opplever at slike analyser gir dem liten verdi (Njå og Vastveit, 2016, s. 9).

Videre hevder de at flere kommuner også beskriver analyseprosessen mer som en skriveeksersis enn som et verktøy for å styre sikkerheten (Njå et al., 2020, s. 110-111).

Ifølge Terje Aven har kunnskapsdimensjonen blitt for lite vektlagt under utviklingen av ROS-modellen. I tillegg er han kritisk til at risikomatriser blir presentert med «trafikklys-metaforen»,

her bruker man farger for å illustrere risikonivå: rødt, gult, grønt (Aven og Renn, 2010, s. 107). Han mener at bruk av farger kan gi et feilaktig bilde av hva som er akseptabel risiko. Videre argumenterer han med at en ikke kan benytte seg av tankesett som ble introdusert på 1970-tallet for å møte nåtidens farer og trusler (Engen et al., 2016, s. 352-354).

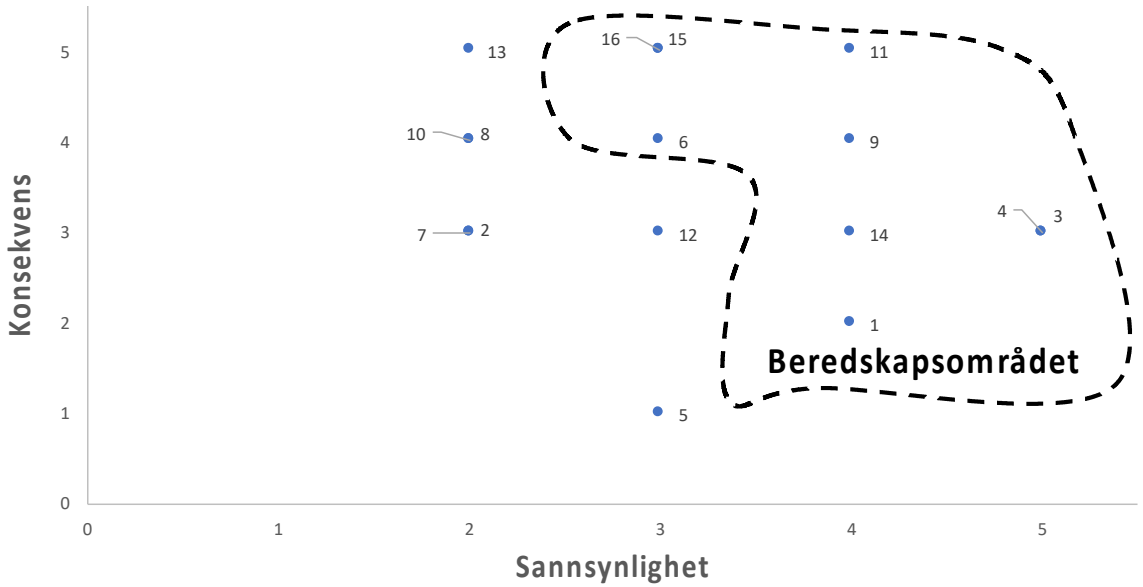
Folk har ofte et syn på risiko som tilsier at risiko er lik deres oppfattelse av situasjonen, eller at de blander sammen risikobegreper som usikkerhet og sannsynlighet. I et scenario der en beslutningstager kommuniserer om risiko med lekfolk, vil deres risikoforståelse være avhengig av om en stoler på eller har tillit til den en kommuniserer med (Veland og Aven, 2013, s. 34-39).

Beredskapsanalyse

Når Ivar Lunde beskriver hvordan en virksomhet skal etablere en beredskap som er tilpasset virksomheten til en akseptabel kostnad, så er han tydelig på at dette bør planlegges og gjennomføres som en prosess. Dette skal bidra til en praktisk og analytisk tilnærming (Lunde, 2019, s. 58). Ifølge faglitteraturen finnes det flere beskrivelser av hva som er formålet med en beredskapsanalyse (Njå et. al., 2020, s. 347) (Engen et al., 2016, s. 280), og vi benytter Lundes definisjon i denne masteroppgaven (Lunde, 2019, s. 60):

> *"en analyse som omfatter etablering av definerte fare- og ulykkes-situasjoner (DFU), herunder dimensjonerende ulykkessituasjoner, etablering av funksjonskrav til beredskap og identifisering av tiltak for å dimensjonere beredskapen".* (Lunde, *2019, s. 60)*

Arbeidet med beredskapsanalyse vises i trinn 3 i Beredskapsplanleggingshjulet, ref. Figur 24, og ifølge faglitteraturen er det de dimensjonerende hendelsene en skal etablere beredskap for å håndtere, og disse er basert virksomhetens styrende risikoer. Dette er visualisert i risikomatrisen i Figur 25 på neste side, hvor de styrende risikoene er plassert innenfor "*beredskapsområdet*" (Njå et al., 2020, s. 346-348):



Figur 25 - Beredskapsområdet

Ovennevnte Figur 25 viser hvilke risikoer en ikke skal etablere beredskap for (*tallene* utenfor beredskapsområdet), og hvilke risikoer som skal være styrende når virksomheten skal dimensjonere sin beredskap (*tallene* innenfor beredskapsområdet).

Beredskapsplanverk

I dag finnes det mange håndbøker og veiledere, samt mye informasjonsmateriell tilgjengelig i Norge for å beskrive hva en beredskapsplan kan inneholde. Ifølge Lunde er formålet med en beredskapsplan å beskrive "*hvem gjør hva, hvor, når, hvordan og til hvilken effekt*". En beredskapsplan som beskriver alt dette vil, ifølge Lunde (Lunde, 2019, s. 114), bidra til at alle involverte vil benytte denne aktivt i håndteringen av en evt. beredskapssituasjon i virksomheten?

3.3.2 Systemisk tilnærming for å etablere cyber-beredskap

Sosiotekniske systemer

I dagens moderne samfunn benytter virksomheter mennesker og teknologi for å levere tjenester og produkter innenfor for eksempel service- og industrinæringen. I et slikt perspektiv kan virksomheter betraktes som sosiotekniske systemer, hvor disse kjennetegnes ved at de er bygget opp av mennesker som produserer tjenester eller produkter ved hjelp av en eller annen form for

teknologi. I faglitteraturen beskrives et sosioteknisk system som to delsystemer som er tett sammenkoblet. Det første delsystemet består av det tekniske utstyret, det som er nødvendig for at systemet oppnår et resultat (output), og som er basert på systemets inngangsfaktorer (input). Det andre delsystemet består av det sosiale aspektet, som er de menneskene som er involvert i organisasjonsarbeidet. Sistnevnte kan være enkeltpersoner på forskjellige nivåer, som ledere og ansatte, samt innleide personer (Patriarca et al., 2018b, s. 265).

I komplekse sosiotekniske systemer er det ikke nødvendigvis noen direkte interaksjon mellom årsak og virkning for å kunne håndtere kjente eller ukjente hendelser. Dette kan skyldes at antallet ikke-lineære kombinasjoner er mange, samt at det er sterke interaksjoner mellom organisasjoner, teknologi, mennesker og regulatoriske aspekter. Komplekse sosiotekniske systemer kjennetegnes også ved at de har en målrettet struktur som kan bestå av innbyrdes relaterte, og gjensidig avhengige, sosiale og tekniske elementer som påvirker hverandre, indirekte eller direkte, for at systemet skal oppnå sitt mål. Et sosioteknisk system kan også bestå av flere sosiotekniske delsystemer som har tette sammenkoblinger med hverandre (Patriarca et al., 2018b, s. 265-266).

I et moderne samfunn som i dag, kan sosiotekniske systemer knyttes til det som omfattes av cyber-relaterte faktorer. I et slikt perspektiv kan en tenke seg at det tekniske delsystemet består av cyber-delsystemer, hvor intelligente og adaptive programvarer har interaksjoner og tette koblinger med sosial-ledelsessystemer, samt med maskinvare og annet utstyr. Eksempler knyttet til dette er arbeidsprosesser innenfor digitalisering og automatisering i sosiotekniske systemer. Slike sosiotekniske systemer kan være sammenvevd av sosiale- og tekniske aktører med forskjellige formål. Til tross for dette, kan de involverte aktørene, i fellesskap, bidra med interaksjoner slik at sosiotekniske systemer fungerer under forventede og uventende situasjoner eller hendelser.

Når arbeidsprosesser og delsystemer også inkluderer det som omfattes av cyber-funksjonaliteter beskrives dette i faglitteraturen som Cyber-sosiotekniske systemer (Patriarca et al., 2021, s. 1).

Resiliens

Resiliens-begrepet stammer fra det latinske ordet *resilire* og beskrives som *«en evne til å komme tilbake til en normaltilstand etter en påkjenning»* (Stavland og Bruvoll, 2019, s. 10).

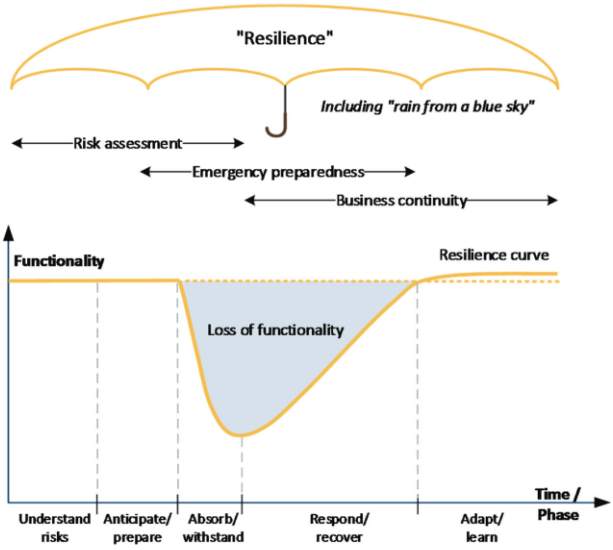
Resiliens har mange definisjoner (Aven, 2017, s. 536; Stavland og Bruvoll, 2019, s. 33), og ulike aktører, praktikere og teoretikere, benytter begrepet forskjellig. Dette skyldes blant annet at resiliens-begrepet er tilpasset ulike formål, samt at resiliens benyttes i et stort omfang. I dag beskrives resiliens i en rekke ingeniørrelaterte fagdisipliner, samt innenfor psykologi fagområdet (Nemeth og Hollnagel, 2014, s. 3). Stavland og Bruvoll har forsket på resiliens-begrepet, og har gjennomført undersøkelser for å kartlegge tolkninger og forståelser knyttet til resiliens, samt studert ulike resiliens-definisjoner. De oppsummerte i sin forskningsrapport i 2019 at det var et mangfold på over 300 sprikende definisjoner (Stavland og Bruvoll, 2019, s. 10-11). Som eksempel kan nevnes at regjeringen beskriver resiliens på følgende måte (Meld. St. 10 (2016-2017), s. 31):

> *«et samfunns evne til å tåle og håndtere store hendelser, gjenopprette viktige funksjoner etter at hendelser har funnet sted, og om nødvendig tilpasse seg til endrede forutsetninger» (Meld. St. 10 (2016-2017), s. 31)*

Det eksisterer mye litteratur om resiliens, og det kommer mer og mer litteratur om dette temaet (Aven, 2017). I faglitteraturen fremkommer det at kunnskapen om resiliens har et abstrakt preg. Dette forklares med manglende forståelse av organisasjoner som er, eller har vært, resiliente, samt at det er vanskelig å kontekstualisere generelle teorier som knyttes til begrepet resiliens (Engen et al., 2020, s. 153-154).

Flere forskere innenfor samfunnssikkerhet og beredskap ønsker imidlertid å benytte analyser basert på resiliens-begrepet, hvor gode «praksiser» analyseres fremfor at en fokuserer på uønskede hendelser og/eller på feil i systemer (Njå el al., 2020, s. 227).

Resiliens omtales også som et konsept som kan illustreres som en «*paraply-betegnelse*», og som forklares som en mekanisme som gjør noe, og er en evne og en kapasitet som bidrar til at systemer eller organisasjoner som har blitt utsatt for forstyrrelser spretter tilbake til utgangspunktet (Nemeth og Hollnagel, 2014, s. 3; Steen og Ferreira, 2021, s. 1), se Figur 26 på neste side:



Figur 26 – Resiliensparaplyen (Øien et al.2017)

Resiliens-paraplyen i ovennevnte Figur 26 skal illustrere at resiliens omfatter risikovurderinger, beredskapsplanlegging og gjenopprettelse av funksjonalitet. Resiliens handler om prosesser som gjør noe, ikke om hva systemer eller organisasjonen er (Nemeth og Hollnagel, 2014, s. 186).

Erik Hollnagel har, sammen med andre forfattere, bidratt med en rekke fagbøker om resiliens over en lengre tidsperiode. I disse fagbøkene er det flere ulike definisjoner på resiliens. Ifølge Hollnagel var definisjonen som de bidro med i 2006 basert på datidens industrielle sikkerhets-(safety) tenkning, om systemers iboende evne til å begynne å fungere igjen etter å ha vært utsatt for ulike påkjenninger. På den tiden hadde definisjonen ikke med noen betraktninger knyttet til trussel og risiko. Når Hollnagel i 2022 presenterer sin siste resiliens-definisjon (se nedenfor), omtaler han definisjonen som en «arbeids-definisjon», og med dette mener han at også denne definisjonen vil endres i fremtiden (Nemeth og Hollnagel, 2022, s. 3):

> *«Evne til å lykkes under varierende forhold, slik at antall tiltenkte og akseptable resultater er så høyt som mulig» (Nemeth og Hollnagel, 2022, s. 3, egen oversettelse)*

Videre beskriver Hollnagel i sist nevnte fagbok at resiliens er helt nødvendig i alle virksomheter (Nemeth og Hollnagel, 2022, s. 25), og at resiliens handler om hvordan systemer presterer, men ikke nødvendigvis i kontekst til sikkerhet. I tillegg har definisjonen endret seg fra å handle om

selve resiliens-begrepet, til nå mer å fokusere på resiliens-prestasjonskarakteristikker (Nemeth og Hollnagel, 2022, s. 4).

Resilience engineering (RE)

Erik Hollnagel blir omtalt som en av pionèrene innenfor RE (Stavland og Bruvoll, 2019, s. 30) og han har bidratt med mye forskning innenfor fagområdet, samt at han har utgitt en rekke RE-fagbøker og artikler knyttet til å forstå RE. Ifølge Hollnagel er RE knyttet til risiko-styring og sikkerhetsforståelse, og kan forstås som å ha fokus på å designe eller utvikle resiliente sosiotekniske systemer (Hollnagel et al., 2011, prolog) Begrepet Resilience Engineering (RE) omtales som et merkenavn innenfor resiliens-tenkningen. Videre fremkommer det i faglitteraturen for RE at resiliens både omfatter det en kan forvente kan inntreffe, og det som tilfeldig, plutselig og uventet kan inntreffe (Hollnagel et al., 2011, s. 26-27). RE omtales også som et velkjent konsept, og representerer en ny måte å tenke på når det gjelder sikkerhet og sikkerhetsstyring (Stavland og Bruvoll, 2019, s. 18).

RE som fagområde har utviklet seg mye fra det ble introdusert på det første Resilience Association (REA) Symposiet i 2004 (Patriarca et al., 2018, s. 79). Innenfor RE har mye av fokuset vært rettet mot sosiotekniske systemer (Nemeth og Hollnagel, 2014, s. 3). RE beskriver sikkerhet helt overordnet som *en evne til å lykkes under varierende tilstander*. Denne beskrivelsen legger til grunn at det er tilstrekkelig å observere normaltilstanden for å forstå hvordan sosiotekniske systemer feiler (Hollnagel et al., 2016, prologue). RE som forskningsfelt har endret seg fra Resilience Association (REA) Symposet i 2004, og vi nevner en av flere resiliens definisjoner fra RE-faglitteraturen (Hollnagel et al., 2016, s. XXXVI):

> *«den iboende evnen et system har til å justere sine funksjoner i forkant av, under, eller etter endringer og forstyrrelser, slik at det kan opprettholde nødvendige funksjoner under både forventede og uventede forhold» (Hollnagel et al., 2016, s. XXXVI, egen oversettelse).*

Etter å ha forsket flere år på RE, er fokuset nå endret til at en forsker mer på det å *forstå* RE, samt hvordan en kan *måle* resiliens for å kunne beskrive *grad av* resiliens eller om det *i det hele tatt er* resiliens, som nevnt over. Ifølge faglitteraturen er Resilience Engineering (RE) en

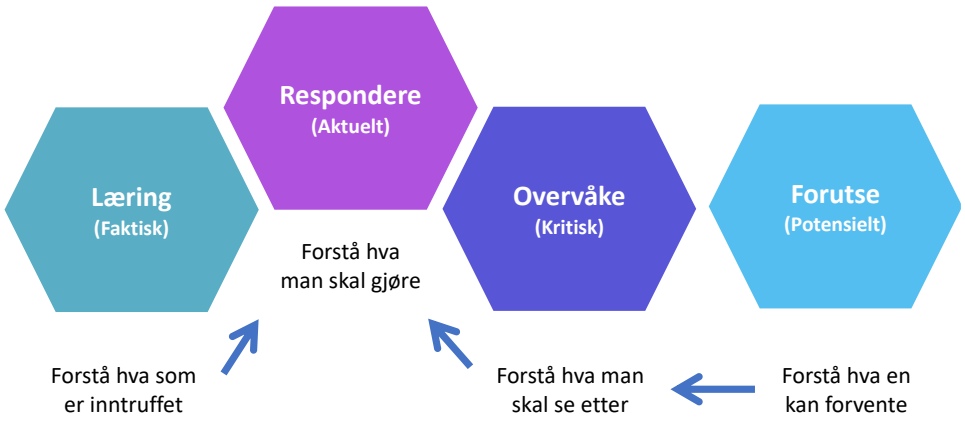
metode man kan benytte når en skal designe resiliens og en kan benytte Resilience Analysis Grid- (RAG-) metoden for å gjøre dette.

Resilience Analysis Grid (RAG): en metode for å designe resiliens

Innenfor RE beskriver flere forskere at metoden «Resilience Analysis Grid (RAG)» kan benyttes for å avgjøre om systemer er resiliente eller ikke, og metoden er egnet for å finne ut om noen av de fire hjørnesteinene, som resiliens består av, kan forbedres.

I RE -teorien knyttes det å bli resilient opp imot fire grunnleggende egenskaper:

1) Overvåke 2) Respons 3) Lære og 4) Forutse (se *Figur 27*) må være til stede for at organisasjonen skal være resilient (Hollnagel et al., 2011, s. 279):



Figur 27 – Basert på de fire grunnleggende egenskapene for resiliens (Hollnagel, 2011, s. 279)

Figuren over beskriver de fire hjørnesteinene innenfor resiliens (Hollnagel et al., 2016, xxxvii) og til sammen beskriver disse hvor resilient organisasjoner eller systemer er (Nemeth og Hollnagel, 2014, s. 283).

Evne til å forutse

Egenskapen med å forutse beskrives som den første hjørnesteinen knyttet til resiliens (Nemeth og Hollnagel, 2014, s. 5). For å vite hva en kan forvente eller forstå, for eksempel endringer av trusler, muligheter eller forstyrrelser, så vil denne egenskapen bidra til å forutse potensialet av hva for eksempel forstyrrelser kan medføre i en konkret situasjon. I et resilient system er

egenskapen forutse nødvendig for å kunne respondere på en hensiktsmessig måte. I tillegg fremkommer det fra RE-teorien at det er en målsetting å støtte de kognitive prosessene i en organisasjon, og å forutse hvilke tiltak en skal utvikle for respons-funksjonen, før det oppstår en hendelse, samt under håndteringen av hendelsen (Wood, 2019, s. 24).

Evne til å overvåke

Egenskapen med å overvåke beskrives som den andre hjørnesteinen knyttet til resiliens. For å vite hva en skal se etter, trenger en å overvåke for eksempel endringer, trusler eller forstyrrelser for å kunne respondere på en hensiktsmessig måte. Overvåknings-egenskap bidrar til at en også kan overvåke resiliens-prestasjon som respons-funksjonen bidrar med. (Nemeth og Hollnagel, 2014, s. 5). Ifølge David Wood bør overvåkningen bidra at en får justert den adaptive kapasiteten som er nødvendig etter hvert som endringer pågår (Wood, 2019, s. 22-23)

Evne til å respondere

Egenskapen knyttet til å kunne respondere beskrives som den tredje hjørnesteinen knyttet til resiliens (Nemeth og Hollnagel, 2014, s. 6). Når en forstår hva som skal utføres, kan en respondere på en hensiktsmessig måte (kapasitet og responstid) for å kunne håndtere for eksempel forstyrrelser eller trusler effektivt.

Evne til å lære

Den siste og fjerde hjørnesteinen er knyttet til læring (Nemeth og Hollnagel, 2014, s. 6). Det å kunne overvåke og forutsi hva som skjer når det for eksempel oppstår en forstyrrelse eller trussel, samt hvordan man responderer, og hvordan man lærer av denne prosessen, vil bidra til at man i resiliente systemer vil utføre aktiviteter og oppgaver på en bedre og bedre måte.

I tillegg til ovennevnte beskrivelse av RE-egenskaper (de fire hjørnesteinene) mener David Woods, som har forsket på resiliens-konseptet og studert hvordan en kan designe komplekse adaptive systemer, at andre folk som jobber innenfor andre fagområder, som for eksempel reguleringsteknikk, er godt kjent med hvordan en kan designe adaptive reguleringssystemer som kan håndtere mange komplekse forstyrrelser samtidig (Wood, 2015, s. 4)

Risikostyring og resiliens

Krisehåndtering vil alltid være en kombinasjon av planlegging og improvisasjon, fordi ingen kriser vil oppstå eller vil utvikle seg slik en tenkte når en etablerte beredskap. Til tross for at virksomheter etablerer helhetlig beredskap basert på tradisjonell risikotenkning, betyr ikke dette at all risiko de omgir seg med kan vurderes som akseptabel. I dagens moderne samfunn er det flere som hevder at den tradisjonelle måten å vurdere og håndtere risiko i sosiotekniske systemer på, ikke er tilstrekkelig for å møte de nye risikoene vi møter i dag, uavhengig av om risiko er kjent eller ukjent. Flere argumenterer for at risikobegrepet bør sees i samheng med resiliens, fordi de vurderer at den tradisjonelle risiko-tenkningen ikke er i stand til å håndtere de nye risikoene eller endringer av risiko (Nemeth og Hollnagel, 2021, s. 2-3; Stavland og Bruvoll, 2019, s. 7; Woods, 2019, s. 52-54;).

Vi har tidligere beskrevet at risikostyring handler om risikovurdering knyttet til å redusere skadeomfang for kjente risikokilder dersom de inntreffer, mens resiliens handler om å opprettholde funksjoner for kjente og ukjente risikoer. En annen forskjell er knyttet til at risikostyring har et avgrenset tidsrom når det gjelder risikoanalyse, mens resiliens i større grad handler om langvarige og kontinuerlige prosesser.

Det er flere aspekter innenfor risikostyringsteorier hvor man mener at resiliens-begrepet blir en viktigere del av fremtidig risikostyring. Dette fordi resiliens har elementer som bidrar til at risikostyringen blir forbedret. Resiliens-styring og den tradisjonelle risikostyringen har også noen likheter. Begge har en prosesstilnærming der formålet er å redusere negative konsekvenser av uønskede hendelser. En annen likhet er at både risikostyring og resiliens søker etter metoder for å redusere sårbarhetene i systemene (Stavland og Bruvoll, 2019, s. 14).

Ifølge Terje Aven er resiliens-tenkningen spesielt relevant for komplekse sammensatte systemer, der det er stor usikkerhet knyttet til håndtering av ukjente og usikre hendelser. Videre mener han at resiliens også kan styrkes i prosesser uten at risikobegrepet benyttes (Aven, 2017, s. 536)

Resilience Engineering (RE) er et fagområde som på mange måter er en alternativ tilnærming til risikostyring. Ifølge Riana Steen og Terje Aven er det tradisjonelle risikoperspektivet basert på historisk «etterpåklokskap», mens RE har fokus på dagligdagse aktiviteter. Eksempel på historisk «etterpåklokskap» kan være basert på «lagging»-faktorer som ulykkesstatistikker eller avviksrapportering. I et slikt risikoperspektiv er risiko definert på bakgrunn av en sannsynlighetsfordeling, eller av en sannsynlighet som uttrykker stokastiske usikkerheter.

Resiliens derimot, handler om konsekvensene. Ifølge Steen og Aven er det et fundamentalt problem å sannsynlighets beregne ved hjelp av historisk data (dvs. den frekvensbaserte sannsynlighetstilnærmingen) i sosiotekniske systemer når en skal beskrive risiko (Steen og Aven, 2011, s. 292-297).

Det finnes flere måter å beskrive risiko på, og det finnes også flere måter å beskrive forholdet mellom resiliens og risiko på. I sitt forskningsarbeid, og i samsvar med Hollnagel, benyttet de usikkerhet som hovedkomponent istedenfor å benytte sannsynlighet når de skulle beskrive risiko i et cyber-angrep.

Resiliens sett fra et cyber-angrep

Innenfor tradisjonell risikotenking, gitt et cyber-angrep, hvor sannsynlighet er hovedkomponent, ble «feil eller handlingssvikt» erstattet med uventede, ikke lineære kombinasjoner av handlinger, når Steen og Aven ønsket å beskrive utvikling av risiko. Basert på sin forskning, argumenterer de for en utvidet risikovurdering, hvor usikkerhet og kunnskap sees i sammenheng. Videre argumenterer de for at utvidet risikovurdering vil bidra mer innenfor RE og risikostyring, enn kun RE-analyser som er basert på isolerte prosesser. (Steen og Aven, 2011, s. 295-298). I et risikoperspektiv vil resiliens-begrepet dermed bidra til en alternativ tilnærming, og flere forskere mener at risiko og resiliens kan utfylle hverandre dersom de sees i sammenheng (Stavland og Bruvoll, 2019, s. 37).

Resiliens og beredskap

I beskrivelser knyttet til robusthet og organisatoriske beredskapsresponser på kriser, har resiliens blitt et sentralt begrep (Engen et al., 2020, s. 153). I et slikt perspektiv er det flere som er enige med Terje Aven om at robusthet og motstandsdyktighet har en tilnærmet lik betydning.

Erik Hollnagel mener derimot at robusthet skiller seg fra resiliens fordi resiliens også inkluderer ukjente hendelser, mens robusthet kun er basert på kjente hendelser (Stavland og Bruvoll, 2019, s. 34). Resiliens-tenkning i krise- og beredskapssituasjoner gir helt nye muligheter innenfor beredskapsfagfeltet fordi en resiliens-tilnærming tar utgangspunkt i normalsituasjoner, mens tradisjonell beredskapstenkning tar utgangspunkt i at risiko er basert på historiske kunnskapsbaserte negative hendelser.

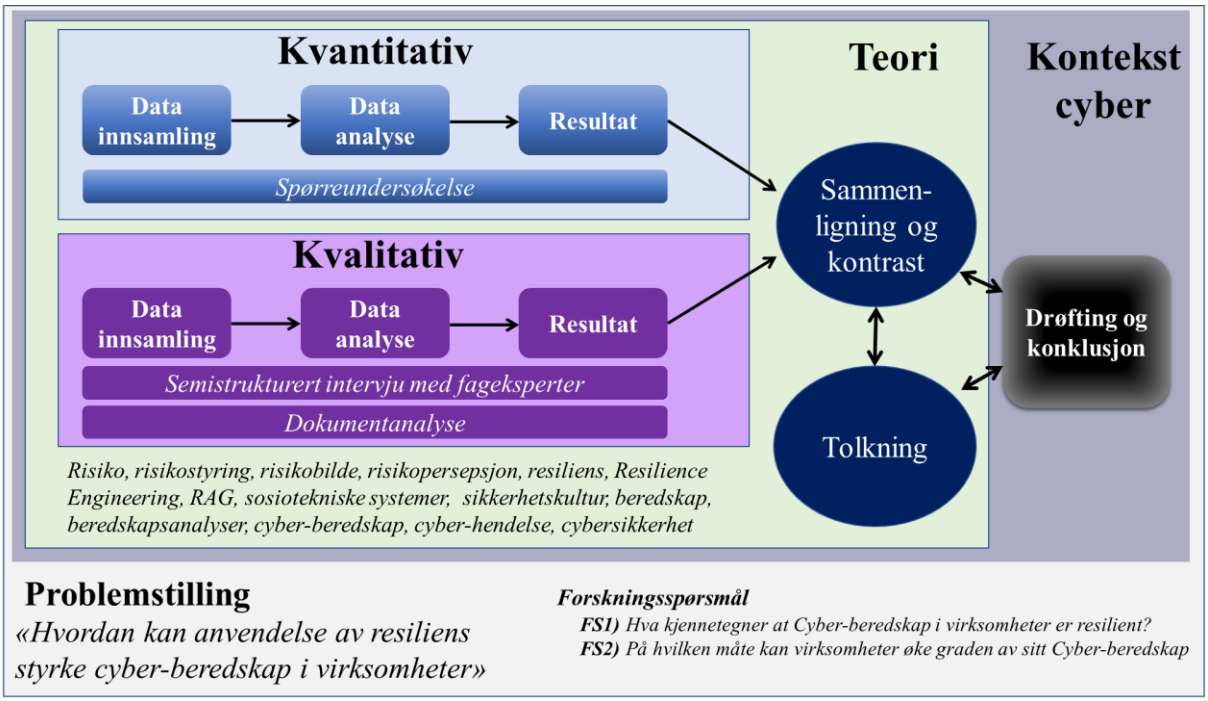
Istedenfor å bare fokusere på negative hendelser som sjelden skjer, som ulykker og kriser, fokuserer man mer på verdier som forbindes med noe som er positivt og som man kan observere kontinuerlig. Denne dreiningen skal gi en klarere forståelse av sammenhengen mellom måloppnåelse og tilhørende virkemidler innenfor samfunnssikkerhets-feltet (Njå et al., 2020, s. 143).

4 Metode

I dette kapittelet skal vi presentere masteroppgavens forskningsmetode og redegjøre for hvordan vi har gått frem for å gjennomføre datainnsamlingen. I de neste avsnittene beskriver vi valget av den metoden som skal kunne bidra til å gi svar på masteroppgavens problemstilling og forskningsspørsmålene. Videre skal vi presentere prosessen med forskningsdesign hvor vi beskriver valg av metode, forskningsprosess med den tilhørende datainnsamlingsmetoden som vi har benyttet, samt hvordan valgt metode oppfyller kravene til reliabilitet og validitet for denne masteroppgaven. I tillegg har det vært viktig for oss å vise til objektivitet, ivareta informantenes personvern ved å anonymisere de og deres virksomheter, samt å ivareta god etisk standard og kvalitet.

4.1 Forskningsdesign

For å besvare oppgavens problemstilling med tilhørende forskningsspørsmålene, har vi valgt å samle inn empirisk data gjennom spørreundersøkelse, dokumentanalyse og semistrukturert intervju med fageksperter. Denne fremgangsmåten er omtalt som et metodisk design basert på Mixed Method Approach (MMA), også omtalt som metodetriangulering. Metodetriangulering kan beskrives som en kombinasjon av kvalitative og kvantitative metoder. John W. Creswell og J. David Creswell mener at benyttelse av denne metoden legger til rette for bruk av kvalitativ og kvantitativ innsamling av data. Fordelen med MMA metoden vil bidra til å innhente informasjon, data og nyttig informasjon (Creswell og Creswell, 2017, s. 187-189). Vi har valgt semistrukturert intervju med fageksperter for å belyse problemstillingen på balansert måte og få frem bakenforliggende utfordringer. Ifølge William Adams er semistrukturert intervju en ressurskrevende aktivitet. Denne intervju formen setter større krav til oss. (Adams, 2015, s. 492 – 495). I Figur 28 på neste side har vi illustrert hvordan masteroppgavens forskningsdesign er strukturert. For å besvare masteroppgavens problemstilling med tilhørende forskningsspørsmål, blir kvantitative og kvalitative data triangulert basert på relevant teori og kontekst,



Figur 28 - Forskningsdesign

Figuren nedenfor viser vår tilnærming knyttet til struktur for oppbygging av oppgaven, samt relevant teori og empiri fordelt under tradisjonell beredskap og resilient beredskap.

Tabell 6 – Overordnet plan og struktur på relevant teori og emperi

Cyberberedskap			
Tradisjonell beredskaps-tilnærming		Resilient beredskaps-tilnærming	
Tema	Relevant teori / Rapporter	Tema	Relevant teori /Rapporter
3.1.1 Risikokonsept 3.1.2 Risikopersepsjon 3.1.3 Risikostyring 3.2 Sikkerhetskultur og sikkerhet i dybden 3.3.1 Systematisk – tradisjonell tilnærming	Teori: Aven Aven, Røed og Wiencke Engen, Kruke, Lindøe, Olsen, Olsen og Pettersen Lunde Njå, Sommer, Rake og Braut Rausand og Utne Reason Rapporter: NOU Stortingsmelding Publikasjon	3.3.2 Systemisk tilnærming for å etablere cyber-beredskap - Sosiotekniske systemer - Resiliens - Resilience Engineering (RE) - Resilience Analysis Grid (RAG)	Teori: Hollnagel, Paries, Woods og Wreathall Nemeth og Hollnagel Rapporter: NOU Stortingsmelding Publikasjon

4.2 Forskningsprosessen

Prosessen med å diskutere tema knyttet til masteroppgaven har utviklet seg parallelt med vårt arbeid med å levere oppgaver på to tidligere kurs innenfor dette masterstudiet. Den første oppgaven handlet om planlegging og etablering av beredskap i virksomheter, mens den andre oppgaven handlet om hvordan kommuner kan øke kvaliteten i sitt arbeid for etablering av kommunal beredskap. Inspirert av pågående forbedringsprosesser knyttet til cyber-beredskap hos vår arbeidsgiver ved Institutt for energiteknikk (IFE), fant vi et tema som vi begge er genuint opptatt av og ønsket å skrive om. Da vi har god erfaring med å benytte Microsoft Teams fra tidligere studier og arbeidslivet, bestemte vi oss for å fortsette å bruke Microsoft Teams i arbeidet med denne masteroppgaven. Det har fungert veldig bra. I tillegg har vi hatt fysiske møter på Kjeller og i Halden hvor IFE er lokalisert, og vi har benyttet telefon ved behov.

I arbeidet med masteroppgaven har vi videreført samme arbeidspraksis og rutiner som vi benyttet i arbeidet med ovennevnte prosjektoppgaver. Vi har hatt faste arbeidsmøter hver lørdag og søndag morgen, samt hver onsdag kveld. Denne møtestrukturen bidro til at vi fikk god fremdrift i skrivearbeidet, samt felles forståelse og læring frem mot innleveringen.

Etter å ha deltatt på obligatorisk metodekurs, leverte vi inn prosjektskisse for godkjenning til Universitetet i Stavanger (UiS) og fikk tildelt Riana Steen som veileder. Vi fikk til et raskt møte med veilederen, hvor både problemstilling og forskningsspørsmål ble justert. Deretter startet vi med å skrive kontekst og teori. Vi har deltatt på flere konferanser, og vil spesielt fremheve Sikkerhetskonferansen 2022 som ble arrangert av NSM, med mange interessante foredrag med bl.a. fokus på «alt vi ikke ser». Vi hadde store forventninger til sikkerhetskonferansen, og vi ønsket å få innspill og nye perspektiver for bl.a. etablering av cyberberedskap. Årets sikkerhetskonferanse hadde et spesielt bakteppe, hvor krig i Europa naturligvis fikk mye oppmerksomhet. Med dagens sikkerhetspolitiske situasjon i Europa, ble viktigheten av å ha god cybersikkerhet i Norge spesielt satt på dagsorden.

4.3 Datainnsamling

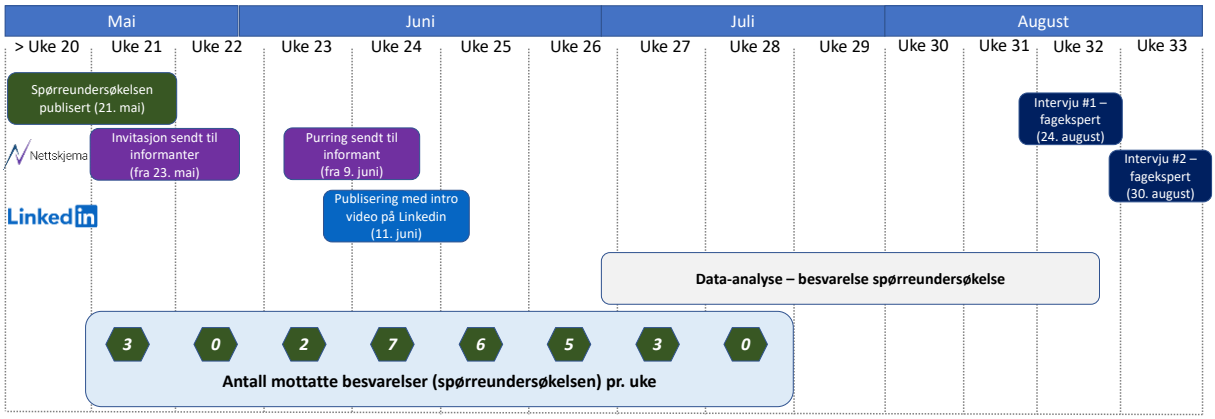
Det er i hovedsak to ulike former for datakilder (Halvorsen K., 2014, s. 114-115):

1) Primærdata – data som først og fremst samles inn av forskeren selv
2) Sekundærdata – data som samles inn av andre, og er tilgjengelige for andre forskere.

I denne masteroppgaven er primærdata avgrenset til spørreundersøkelsen (vedlegg 4) og semistrukturert intervju med fageksperter (vedlegg 7 og 8).

Sekundærdata i denne masteroppgaven er Stortingsmeldinger, NOU, lover, trusselvurderinger, rapporter, mfl., se Tabell 9 for oversikt over sekundærdata.

Med bakgrunn i at resiliens-fagområdet er i kontinuerlig utvikling, har det blitt gitt ut flere nye publikasjoner i den perioden vi har jobbet med vår masteroppgave. Ved å lese disse har vi fortløpende fått mer innsikt og ny kunnskap, noe som har vært nyttig i vårt arbeid med denne masteroppgaven.



Figur 29 - Tidslinje datainnsamling

Informasjonsskriv om masteroppgaven, spørreskjema og intervjuguide

I samråd med veileder, og etter at store deler av teorien var skrevet, ble metodevalg for masteroppgaven bestemt. Med bakgrunn i oppgavens problemstilling, som inkluderer tre fagområde; resiliens, beredskap og cyber, valgte vi i første omgang å jobbe med spørsmålene knyttet til hvert fagområde hver for seg. Spørsmålene ble kategorisert pr. fagområde knyttet til de tidligere nevnte resiliens-hjørnesteinene, og for å ha god oversikt valgte vi å strukturere disse ved hjelp av fargekoder.

Da vi testkjørte spørreskjemaet oppdaget vi at dette var for omfattende. Vi hadde mer enn 50 spørsmål, og noen av disse spørsmålene var overlappende. Dette resulterte i at vi reduserte antall spørsmål, og endret spørsmålene flere ganger. Til slutt endte vi opp med 25 hovedspørsmål som dannet grunnlaget for spørreundersøkelsen. Spørreskjemaet er bygget opp med en kombinasjon av nedtrekksliste, avkrysningsbokser og en matrise med skala fra 1 - 7

(helt uenig, uenig, litt uenig, litt enig, enig, helt enig og vet ikke). Flere av spørsmålene er adaptive, som betyr at vi har lagt inn oppfølgingsspørsmål basert på informantenes svar. I tillegg har vi hatt åpne spørsmål som gir informantene muligheten til å utdype sine svar i en fritekst-boks. I spørreskjemaet har vi lagt opp til at informantene har anledning til å gi oss tilbakemelding eller kommentar underveis, slik at informantens perspektiver blir ivaretatt i besvarelsen.

Når spørreskjemaet var ferdig, utarbeidet vi et informasjonsskriv om masteroppgaven for å rekruttere informanter til spørreundersøkelsen (vedlegg 2), og et tilsvarende skriv til fagekspertene (vedlegg 5). Vi laget også en intervjuguide for semistrukturert intervju med fageksperter (vedlegg 6).

Utvalg og informanter og fageksperter

I den kvalitative delen av masteroppgaven har vi benyttet systematiske og strategiske utvalgsprinsipper for å identifisere informantene (Dalland, 2021, s. 59-60). Vårt valg av strategisk utvalg er gjort med ønske om å få kunnskap om cyberberedskapen i virksomheter som har blitt rammet av cyber-hendelser. NSM har siden 2019 registrert en tredobling i antall cyberhendelser som har fått alvorlige konsekvenser for norske virksomheter 2019 (Prop. 78S (2021-2022), s. 17), men det var uklart for oss hvilke virksomheter som hadde vært rammet. Dette fordi informasjonen ikke er offentlig tilgjengelig. Vi tok utgangspunkt i Per Helge Seglstens artikkelserie hvor han skrev om virksomheter som hadde blitt rammet av cyberhendelser i 2021. Her identifiserte han 38 virksomheter som hadde blitt rammet av cyberhendelser som fikk alvorlige konsekvenser for dem (Seglsten, 2022a og 2022b).

Tabell 7 – Utvalg av data (oppdatert 2. oktober 2022)

Utvalg	Antall virksomheter / personer	Eksponert
Strategisk	38 virksomheter	
Systematisk	LinkedIn gruppe – Sikkerhet og sårbarhet	83
Systematisk	LinkedIn gruppe – IT sikkerhetsgruppen	119
Systematisk	LinkedIn gruppe – Norsk Informasjonssikkerhetsforum ISF	431
Systematisk	LinkedIn gruppe – Industriell cybersikkerhet – Norge	79
Systematisk	LinkedIn gruppe – CSA Norway Chapter Members Group	266
Systematisk	LinkedIn gruppe – Scandinavian Security and Preparedness – Skandinavisk sikkerhet og beredskap	95
Strategisk	Utvalgte fageksperter som har tung erfaring fra cyber- og teknologi-området	2

I Tabell 7 på forrige side vises relevante LinkedIn grupper som vi har publisert innlegget i, og gruppemedlemmene består typisk av fagpersoner, ledere, beredskapsrådgivere, beredskapssjefer, informasjonssikkerhetsledere, sikkerhetsrådgivere, sikkerhetssjefer, personvernombud mfl.

Olav Dalland mener at fremgangsmåten for å velge eller rekruttere informanter til kvantitative undersøkelser eller kvalitativt orienterte metoder er viktig å belyse. Han forteller at «kravet om systematisk utvalg av data står helt sentralt, og reglene tar sikte på å hindre at data blir valgt på en slik måte at det påvirker resultatet av undersøkelsen». For strategisk utvalg er det spesialister, fageksperter, eller nøkkelinformanter med god dybde-kunnskap, som kan bidra med å belyse et fenomen (Dalland, 2020, s. 59; Andersen, 2006, s. 281-282).

Utdanning, kompetanse og arbeidserfaring

Med de innledende spørsmålene i spørreundersøkelsen ønsket vi å kartlegge informantenes utdanning, kompetanse, arbeidserfaring, samt sektor og størrelse på virksomhetene. (Spørsmål 1a) 83 % av informantene har mer enn 3 års høyere utdanning og (spørsmål 1b) i tillegg har flere av informantene mange relevante kurs og sertifiseringer. Alle informanter har mer enn 10 års erfaring og 77 % av informantene har mer enn 20 års erfaring (spørsmål 4). 80 % av informantene jobber i virksomheter som har mer enn 50 ansatte, og 58 % jobber i virksomheter som har mer enn 250 ansatte (spørsmål 5). Informantene jobber i mange ulike sektorer og ca. 30 % av dem er ansatt i offentlig sektor (spørsmål 6a).

Valg av de to fagekspertene er basert på vår kunnskap om deres erfaring og brennende engasjement for cybersikkerhet. Begge er aktive foredragsholdere og etterspurt av alle sektorer. Roar Thon er en viktig pådriver for å øke bevissthet og sette fokus på dagsaktuelle problemstillinger med cybersikkerhet gjennom sin rolle som fagdirektør for sikkerhetskultur i NSM. Han har erfaring fra Forsvaret og fra Politiet, før han i 2003 begynte i NSM. Roar Thon er en prisbelønnet foredragsholder og han har holdt mer enn 1500 foredrag i NSM. Gøran Tømte har mer enn 26 års erfaring fra teknologi-bransjen, hvor han har jobbet for et av de største og ledende sikkerhetsselskapene i verden (Palo Alto Network). Han har deltatt i håndtering av en rekke cyber-hendelser nasjonalt og internasjonalt, og innførte begrepet «VG-testen» for å effektivt teste cybersikkerhet i virksomheter. Videre er Gøran Tømte en forkjemper for Zero Trust konseptet, for å øke cybersikkerhet i alle virksomheter nasjonalt og internasjonalt.

Tidslinjen i Figur 29 viser når og hvilke aktiviteter som ble gjennomført, samt besvarelse av spørreundersøkelsen og intervju med fageksperter.

4.3.1 Kvantitativ datainnsamling

Valg av teknisk plattform og meldeskjema til Norsk senter for forskningsdata

Vi hadde begge erfaring med bruk av flere ulike typer tekniske plattformer som Microsoft Forms, Questback, SurveyMonkey mfl. Fordi vi hadde best kjennskap og mest erfaring med Microsoft Forms, begynte vi først å lage spørreundersøkelsen i dette programmet. Etter noen test-kjøringer, oppdaget vi noen begrensninger som primært var knyttet til anonymisering. F.eks. var det begrensninger til å være informant dersom man ikke hadde en gyldig bruker hos Microsoft Forms med tilgang til spørreskjemaet. Vi fikk etter hvert løst flere av begrensningene som vi hadde identifisert med Microsoft Forms, men var likevel ikke helt fornøyde med resultatet. Derfor måtte vi finne en annen løsning, og valgte å bruke Nettskjema.no, som var godt egnet for utarbeidelse av med flervalgs-muligheter, nedtrekks-menyer og adaptive spørsmål.

Adaptiv spørreundersøkelse

Spørreundersøkelsen er basert på hovedspørsmål og delspørsmål. De fleste spørsmålene er obligatoriske, men noen av spørsmålene er adaptive. De adaptive spørsmålene vil bli synlige for informantene etter hvert som de svarer på de obligatoriske spørsmålene, og er avhengig av hva de svarer på disse, ref. vedlegg 4.

Utsendelse av spørreundersøkelsen

Spørreundersøkelsen ble ferdigstilt den 18. mai 2022, men ble ikke publisert før den 23. mai 2022. Vi hadde utfordringer knyttet til samtykke i spørreundersøkelsen i Nettskjema.no-plattformen, jfr. Personvernforordningen og vilkår fra Norsk senter for forskningsdata. Utfordringen var i hovedsak at vi ikke fikk benytte funksjonaliteten for å anonymisere informantene uten å benytte BankID, ref. nettskjema for tjenester for sensitive data. Vi vurderte at BankID ville være en god løsning, der informantenes identitet ville vært anonymisert av plattformen, og ikke være synlig for oss. En evt. tilbaketrekking av samtykke ville også ha blitt håndtert på en effektiv måte av Nettskjema.no-plattformen. Vår vurdering var at identifisering med bruk av BankID, for å få besvart spørreskjemaet, ville ha vært tungvint for informantene.

Basert på avklaringen om at det ikke fantes noen gode løsninger for samtykke uten bruk av TSD skjema den 20. mai 2022, valgte vi å lage en løsning i spørreundersøkelsen hvor informantene kunne benytte flere alternativer for å identifisere seg. Dette for å ivareta eventuell tilbaketrekking av samtykke fra informantene på et senere tidspunkt. Dette løste vi med at informantene kunne benytte privat- eller jobb e-post adresse eller en kode som kun informantene kjente til (altså nøkkel for å koble sammen informanten med deres besvarelse.)

Etter at informasjonsskriv (vedlegg 2) og spørreundersøkelse (vedlegg 4) var sendt ut til virksomhetene, overvåket vi kontinuerlig antall besvarelser vi fikk på spørreundersøkelsen, se tidslinjen i **Feil! Fant ikke referansekilden.** over. Spørreundersøkelsene ble sendt til virksomhetenes postmottak. Vi var i utgangspunktet optimistiske på utsendelsestidspunktet, og hadde nok regnet med relativt rask respons fra flere informanter, men vi fikk kun inn tre besvarelser i løpet av de to første ukene. Vi ble overrasket over lav respons, og bestemte oss for å finne ut hvorfor responsen var så lav. Vi hadde en mistanke om at informasjonsskrivet ikke kom frem til riktige fagpersoner, og tok kontakt med virksomhetene for å undersøke hvordan vårt informasjonsskriv hadde blitt håndtert hos dem, samt spurte om å få snakke med ledelsen, beredskapsrådgivere eller ledere som hadde ansvaret for IKT. Dette var en tidkrevende prosess. Til vår overraskelse kunne personene vi tok kontakt med å fortelle at de ikke hadde mottatt noen e-post fra oss. Vi informerte dem da om vår masteroppgave og spørreundersøkelse. Personene vi snakket med var godt kjent med utfordringer knyttet til å ivareta cybersikkerhet, og flere ble nysgjerrige og interesserte når vi snakket med dem på telefonen. Deretter avklarte vi hvilken person i virksomheten som skulle få tilsendt en ny e-post med informasjonsskriv fra oss. Når nye e-poster var mottatt i virksomhetene, fikk vi raskt tilbake flere besvarelser. Videre var det ofte at kontaktpersonen vi fikk oppgitt ikke var tilgjengelig, og når vi først fikk kontakt, så hendte det at vi ble henvist videre til en ny kontaktperson. Med en mer målrettet tilnærming bidro dette til at svarprosenten økte, men vi hadde fortsatt fått inn for få besvarelser. Vi sendte purringer pr. e-post i uke 23 og 24 og forlenget da svarfristen.

For å øke oppslutningen i spørreundersøkelsen, besluttet vi å utvide med flere informanter, og benyttet LinkedIn plattformen for å rekruttere disse. Vi identifiserte relevante grupper som vi var medlem i fra tidligere (noen av disse gruppene er private), se Figur 30 - Utdrag fra LinkedIn innlegg. Vi laget et innlegg med en kort animert videofilm (19 sekunder) med følgende budskap: «Vi trenger din hjelp for å øke cyber-beredskap i Norge»», «risiko og cyber», «Hvordan kan anvendelse av resiliens styrke cyber-beredskap i virksomheter» og «cyber-beredskap». I løpet av noen uker hadde innlegget blitt eksponert til flere hunder personer og pr. 2. oktober var det 1033 personer som hadde sett innlegget. LinkedIn gruppene som ble vurdert til å være relevante er bl.a. cyber, industriell sikkerhet, informasjonssikkerhet og beredskap.

Figur 30 - Utdrag fra LinkedIn innlegg

Det var totalt 26 besvarelser, og informantene benyttet i gjennomsnitt 25 minutter på å besvare hele undersøkelsen. I analysen av spørreundersøkelsen presenteres resultatene i prosent, og er basert på informantenes besvarelser. På de spørsmålene der det er flere valgmuligheter for informantene vil resultatene også vise hvor mange informanter som valgt tilhørende spørsmål.

4.3.2 Kvalitativ datainnsamling

Intervju med fageksperter

Semistrukturert intervju med fagekspertene ble gjennomført med utgangspunkt i intervjuguiden (vedlegg 6). Vi har redegjort for valg av informantene i kap. 4.3

Tabell 8 - Gjennomføring av intervju med fageksperter (informanter)

Nr.	Navn	Stilling	Dato, sted	Lengde
Inf. 1	Gøran Tømte	Field Security (Zero Trust)	24.08.22, Kjeller	120 min
Inf. 2	Roar Thon	Fagdirektør sikkerhetskultur	30.08.22, Kjeller og Teams	90 min

I tabellen over har fagekspertene fått tildelt et informantnummer som benyttes i tematisk analyse av de semistrukturerte intervjuene ved bruk av [Inf.1, sitat #nr] og [Inf.2, sitat #nr]» i vedlegg 10.

Dokumentanalyse

I en dokumentanalyse skaffer man til veie data gjennom analyse av det mest aktuelle og relevante kildemateriale i forhold til masteroppgavens problemstilling, og utarbeider en form for kilde hierarki. Videre må man være oppmerksomme på at de finnes godt og mindre godt arbeid innenfor de ulike sjangre. (Dalland, 2020, s. 144-145). I denne masteroppgaven bygges dokumentanalysen på dokumenter nevnt i Tabell 9 under.

Tabell 9 - Dokumentoversikt sekundærdata

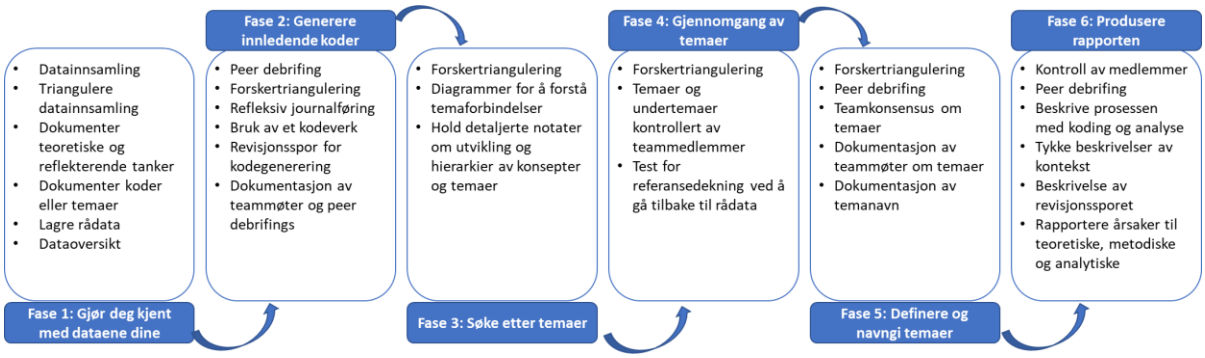
Nr.	Tittel sekundærdata / kilder	Fokusområde	Sider
1	DSB (2003) Risikopersepsjon – en innføring i fagfeltet	Risikopersepsjon, om hvordan risikopersepsjon påvirker adferden til mennesker	19
2	Etterretningstjenesten (2020), Fokus 2020	E-tjenestens årlige trusselvurdering, kunnskap om trusselbilde for Norge 2020 og utviklingstrekk	127
3	Etterretningstjenesten (2021), Fokus 2021	E-tjenestens årlige trusselvurdering, kunnskap om trusselbilde for Norge 2021 og utviklingstrekk	99
4	Etterretningstjenesten (2022), Fokus 2022	E-tjenestens årlige trusselvurdering, kunnskap om trusselbilde for Norge 2022 og utviklingstrekk	38

5	Forsvarets forsknings-institutt (2019), Resiliens – hva er det og hvordan kan det integreres i risikostyring?	Resiliens og risikostyring	44
6	Forsvarsdepartementet, JD (2018), Støtte og samarbeid. En beskrivelse av totalforsvaret i dag	Norges totalforsvar, sivil-militært samarbeid, det nasjonale beredskaps-systemet og beredskapsansvar	99
7	Meld. St. 17 (2001-2002), Samfunnssikkerhet. Veien til et mindre sårbart samfunn.	Stortingsmeldingen er på 151 sider og vi har fokusert på side 100, hvor Justis-departementets samordnings-ansvar for planleggingen av den sivile beredskapen beskrives	151
8	Meld. St. 12 (2005-2006), HMS i petroleumsvirksomheten	Beredskaps defininsjoner, fra petroleumssektoren	71
9	Meld. St. 10 (2016-2017), Risiko i et trygt samfunn – samfunnssikkerhet	Cybersikkerhet og ansvar, og resiliens definisjon og sentrale begreper	192
10	Meld. St. 38 (2016-2017), IKT-sikkerhet. Et felles ansvar	Cyber/IKT- sikkerhet og ansvar på ulike nivåer	85
11	Meld. St. 12 (2017-2018), HMS i petroleumsvirksomheten	Beredskaps definisjoner, fra petroleumssektoren	75
12	Mnemonic (2021), Cyber Security Report 2021	Trusselaktørenes arbeidsdag, fokus på døgn og ukedager	59
13	NOU (2015:13), Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker og samfunn (JD)	Hvordan digitalisering påvirker oss (Lyseutvalget)	329
14	NOU (2016:19). Samhandling for sikkerhet. Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid	Informasjonssikkerhet, hva som menes med konfidensialitet, integritet og tilgjengelighet	297
15	NOU (2017:11), Bedre bistand. Bedre beredskap. Fremtidig organisering av politiets særorganer (JD)	Hva er cyber- / IKT-kriminalitet	313
16	NOU (2018:14), Organisering og regulering av nasjonal IKT-sikkerhet (JD)	Begrepet cyber-/ IKT-sikkerhet og grenseflater /synonymer knyttet til informasjonssikkerhet, cybersikkerhet og digital sikkerhet	147
17	NOU (2021:6), Myndighetenes håndtering av koronapandemien - Rapport fra Korona-kommisjonen	Organiseringen av sentral krisehåndtering ved sivile nasjonale kriser	452
18	NSM (2020),Risiko 2020	Risikobilde 2020, og kompetanse og forebyggende sikkerhetsarbeid	30
19	NSM (2021) Risiko 2021	Risikobilde 2021, og kompetanse og VTS- risiko og sikkerhetsarbeid	
20	NSM (2022), Risiko 2022	Risikobilde 2022, og taktskifte i cyberdomene, helhetlig risikostyringsprosesser, NSM grunnprinsipper	38
21	NSM (2022), Den digitale sikkerhetskonferansen 2022	Sikkerhetskonferanse (3,5t), det globale risikobildet, sikkerhetspolitiske utfordringer og cybersikkerhet	Møte
22	NSR (2022), Mørketallsundersøkelsen 2022	Næringslivets sikkerhetsråd (NSR), belyser den digitale sikkerhetstilstanden i Norge.	62
23	Regjeringen (2020), strakstiltak for å dempe de økonomiske virkningene av koronaviruset	Strakstiltak, bruk av hjemmekontor	Presse-melding

24	Politidirektoratet (2020), Politiets beredskapssystem Del I, Retningslinjer for politiets beredskap	Rapporten er på 255 sider og vi har benyttet kunnskap knyttet til det nasjonale beredskapssystemet, samt om politiets beredskaps-system beskrevet på side 18-19.	254
25	Seglsten, Per Helge (2022a), Lei årskavalkade: 39 kjente dataangrep rammet norske virksomheter i 2021	Digi reportasje 15. januar 2022 om de 38 Cyber-angrepene som rammet Norge i 2021, omfattet navngitte virksomheter som hadde blitt rammet av cyber-angrep, samt informasjon om type angrep	Nett-side
26	Seglsten, Per Helge (2022b), Norske IT-angrep i 2021: Året endte med en bølge av løsepengevirus	Digi reportasje 16. januar 2022 (årskavalkade), med fokus på data-angrep på Toten kommune og Stortinget og de 36 andre kjente Cyber-angrepene, samt hvordan cyber-kriminelle arbeider	Nett-side
27	Telenor (2020), Digital sikkerhet	Kunnskap om trusselforståelse, trussel-bilde og trusselaktører	58
28	Trend micro (2022),	Trend micro rapport, "ransonware in" Q1 2022	Nett-side
29	PST (2020), Nasjonal trusselvurdering 2020	PST redegjørelse for det sammensatte trusselbildet som det norske samfunnet står overfor i 2020	73
30	PST (2021), Nasjonal trusselvurdering 2021	PST redegjørelse for det sammensatte trusselbildet som det norske samfunnet står overfor i 2021	36
31	PST (2022), Nasjonal trusselvurdering 2022	PST redegjørelse for det sammensatte trusselbildet som det norske samfunnet står overfor i 2022	28
32	UN (2020), UN E-Government Survey 2020	Hvordan Norge er rangert i forhold til andre land når det gjelder å ta i bruk teknologi og digitalisering	323
33	Njå, O. & Vastveit, K.R. (2016)	Norske kommuners planlegging, gjennomføring og bruk av risiko- og sårbarhetsanalyser i forbindelse med samfunns-sikkerhetsarbeidet	173

Tematisk analyse

Tematisk analyse-metode benyttes for å strukturere data ved bl.a. å identifisere og tyde vesentlig informasjon fra store datamengder (Clarke og Braun, 2017, s. 297; Dalland, 2020, s. 246-249). Ifølge Olav Dalland kan funnene man gjør ved en slik analyse være godt egnet til tematisk presentasjon og drøfting (Dalland, 2020, s. 247). Victoria Clarke og Virginia Braun beskriver også at en tematisk analyse-metode gir fleksibilitet opp imot forskningsspørsmålene. De mener bl.a. mengde data, har mindre betydning (Clarke og Braun, 2017, s. 297). Ifølge Lorelli Nowell et al. er det noen fallgruver som man bør passe seg for ved økt grad av fleksibilitet som kan resultere i inkonsistens og mangel på sammenheng. I Figur 32 har de vist hvordan dette kan gjøres i seks steg (Nowell et al., 2017, s. 2, 4-5).



Figur 31 - Steg en til seks ifm. etablering av tematisk analyse (Nowell et al., 2017, s. 4)

4.4 Validitet og relabilitet

Validitet

Ifølge Olav Dalland dreier validitetsbegrepet seg om hvorvidt en metode er egnet til å undersøke det den skal undersøke (Dalland, 2020, s. 245-246). Svein S. Andersen mener at «nøkkelinformanter er interessante fordi de er ressurssterke personer som kan belyse en sak eller et fenomen» (Andersen, 2006, s. 282). Videre utdyper han «*ofte at man benytter nøkkelinformanter til å få kunnskap om saker og hendelser som er uvanlige, og som ofte oppleves som kompliserte og vanskelig å forstå*» (Andersen, 2006, s. 292-293). Vi har benyttet spørreundersøkelse, dokumentanalyse av sekundærdata og semistrukturert intervju av fageksperter for å belyse masteroppgavens problemstilling ved hjelp av MMA, slik vi har redegjort for i kap. 4.1 og 4.2. Cyber-begrepet omfattes av, og består av, sammensatte komplekse systemer som har mange løse bindinger, bl.a. eksplosiv teknologi-utvikling, samt mange brukere og bruksområder, ref. kap. 2. Vi mener at fagekspertene har stor betydning for å belyse en sak eller et fenomen som i tillegg er komplisert og vanskelig å forstå.

Reliabilitet

Ifølge Olav Dalland dreier begrepet reliabilitet seg om forskningsresultatenes konsistens og troverdighet, ved blant annet å vise hvordan man har gått frem for å innhente eller skape datagrunnlaget. Dette med det formål om at andre forskere eller studenter kan benytte samme fremgangsmåte for å gjenskape resultatene. Gjennom denne masteroppgaven har vi arbeidet åpent og systematisk, samt redegjort for fremgangsmåtene vi har benyttet. På bakgrunn av dette vil det være mulig å kontrollere eller gjenskape det samme resultatet i ettertid, og det vil være mulig å vurdere masteroppgavens resultater som konsistente og troverdige (Dalland, 2020, s.

246). Vi ser det som en styrke å være to studenter som jobber sammen, fordi vi da har hatt muligheten til å ha gode diskusjoner underveis i arbeidet med masteroppgaven.

4.5 Fordeler og ulemper ved valgt metode

Vi har valgt å benytte Nettskjema.no for vår kvantitative spørreundersøkelse. Dette IT-systemet har flere fordeler, og en av disse er knyttet til innhenting av data som i dette tilfellet, håndteres av Nettskjema.no Dette systemet strukturer innsamlet data i flere formater, noe som bidrar til at etterarbeid blir mindre ressurskrevende. Ulempen med slike spørreundersøkelser er at det er en viss usikkerhet knyttet til om vi når alle informantene. Dette var også en utfordring vi opplevde med denne masteroppgaven. Til å begynne med var det svært få som hadde besvart spørreskjemaet, og vi hadde ikke kunnskap om hvem disse var. Vi var nødt til å ringe alle de 38 virksomhetene for å få riktig kontaktinformasjon slik at spørreskjemaet kom frem til rett person. Dette var meget ressurskrevende, da vi måtte ringe flere ganger til noen av virksomhetene for å identifisere riktig person og få etablert kontakt. Etterpå startet prosessen med å rekruttere potensielle informanter til vår spørreundersøkelse.

Det har vært en fordel for oss og ha benyttet dokumentanalyse som sekundærdata for å få dybdeforståelse knyttet til vår datainnsamling. Sekundærdata som er benyttet har bidratt til å gi oss innsikt, kunnskap og bakgrunnsinformasjon som er relevant for denne masteroppgavens problemstilling med tilhørende forskningsspørsmål.

Fordelen med å benytte semistrukturert intervju med fagekspertene, er at vi får belyst flere sider av den kompleksiteten som cyber har. Fagekspertene har, med sin erfaring og spisskompetanse innen fagområdet cyber, belyst flere sider som fungerer godt, men også det som fungerer mindre godt. Ulempen med å benytte semistrukturert intervju, er at denne metoden er meget ressurskrevende mht. at det krever mye av oss i selve gjennomføringen og i etterarbeidet.

5 Empiriske funn

I empiridelen av masteroppgaven vil vi presentere utvalg av data som er samlet inn og analysert.

Vi vil innlede med følgende problemstilling:

Hvordan kan anvendelse av resiliens styrke cyber-beredskap i virksomheter?

Empirikapittelet er delt inn i forskningsspørsmål FS1 «Hva kjennetegner at Cyber -beredskap i virksomheter er resilient?» og FS2 «På hvilken måte kan virksomheter øke graden av sin Cyber-beredskap». Disse to sprømålene blir drøftet i kap. 6 i lys av valgt teoretisk rammeverk.

Videre vil vi presentere utvalgte funn basert på data fra tre valgte hovedpilarer; 1) Funn fra spørreundersøkelsen, 2) Funn fra semistrukturerte intervjuer med fra fagekspertene, 3) Funn fra sekundærdata som er benyttet i dokumentanalysen som er relevante for å belyse masteroppgavens problemstilling. Vi har strukturert vårt arbeid ved hjelp av tematisk analyse, hvor vi har knyttet våre funn til seks ulike tema; cyber-hendelse, risikopersepsjon, sikkerhetskultur og beredskap, risikostyring, risikobilde, samt resiliens og cyber-beredskap. ref. kap. 4.3.2 ovenfor

5.1 FS1 Hva kjennetegner at Cyber -beredskap i virksomheter er resilient?

For å besvare forskningsspørsmål FS1 har vi analysert dokumenter beskrevet i vedlegg 9. Eksempler på dokumenter vi har analysert er FFI-rapport, Etterretningstjenestens trusselvurdering, PSTs nasjonal trusselvurderinger, NSMs risikovurderinger og NSR mørketallsundersøkelse 2022, for detaljer se vedlegg 9. Hovedfunn fra dette analysearbeidet, blir presentert i kap. 5.3 nedenfor, for de seks utvalgte temaene, hvor vi også har med funn fra spørreundersøkelsen og funn fra fagekspertene.

5.2 FS2 På hvilken måte kan virksomheter øke graden av sin Cyber-beredskap?

For å besvare forskningsspørsmål FS2 har vi analysert dokumenter beskrevet i vedlegg 9. Eksempler på dokumenter vi har analysert er FFI-rapport, Etterretningstjenestens trusselvurdering, PSTs nasjonal trusselvurderinger, NSMs risikovurderinger og NSR mørketallsundersøkelse 2022, for detaljer se vedlegg 9. Hovedfunn fra dette analysearbeidet, blir presentert i kap. 5.3 nedenfor, for de seks utvalgte temaene, hvor vi også har med funn fra spørreundersøkelsen og funn fra fagekspertene.

5.3 Kategorisering av funn fra informanter, fageksperter og sekundærdata

5.3.1 Cyber-hendelse

Funn fra spørreundersøkelse

Spørsmål 22a - Hvilken/hvilke metode/metoder benyttet trusselaktørene for å bryte seg inn i IT systemene?

Svar	Antall	Prosent
Innbrudd via e-post	7	**26,9 %**
Innbrudd via vannhull (lurer brukeren til å installere et program)	0	**0 %**
Innbrudd via skyleverandører	0	**0 %**
Innbrudd via gammelt utstyr	1	**3,8 %**
Innbrudd via Internet of Things (IoT)	0	**0 %**
Innbrudd via nettsider og databaser	2	**7,7 %**
Innbrudd via brukernavn og passord (innlogging detaljer på avveie eller lett passord å gjette)	5	**19,2 %**
Innbrudd via ved bruk av innsider	0	**0 %**
Direktørsvindel og klassisk svindel	2	**7,7 %**
Innbrudd gjennom avlytting og tilgang til trafikk	0	**0 %**
Vet ikke	3	**11,5 %**
Annet (vennligst spesifiser under)	3	**11,5 %**

Funn fra fageksperter

> *«Jeg tror det er viktig å dele erfaring og kunnskap om forsøkt på cyber-angrep som blir stoppet, og ikke bare dele etter at det har skjedd en katastrofe» (Inf.1, sitat #130)*

Funn fra Sekundærdata

> *«Det virker å være tilnærmet allmenn konsensus om at dataangrep har hatt sterk fremvekst de seneste år – både i omfang og alvorlighet. Flere estimater anslår at økonomisk motiverte organiserte kriminelle står bak det store flertall (opp mot 75-80 %) av registrerte dataangrep forrige år. Det er med andre ord profittmotiverte kriminelle som utgjør den mest sannsynlige cybertrusselen mot alle typer organisasjoner og virksomheter» (NSR, 2022, s. 47)*

5.3.2 Risikopersepsjon

Spørreundersøkelse:

Spørsmål 14a – Hvor ofte oppdateres cybersikkerhet risikoer?

Svar	Antall	Prosent
Mindre enn gang pr. år	1	4,2 %
En gang pr. år	6	25 %
To ganger pr. år	1	4,2 %
Hvert kvartal	5	20,8 %
En gang pr. måned	2	8,3 %
Flere ganger pr. måned	3	12,5 %
Kun ved alvorlig hendelse eller større endringer	0	0 %
Flere gang pr. år og ved alvorlig hendelse eller større endringer	5	20,8 %
Annet (vennligst spesifiser under)	1	4,2 %

Fageksperter:

> *«De har ikke oversikt over hvor mange forsøk bedriften deres stanser daglig, ukentlig og månedlig»* (Inf.2, sitat #2)

Sekundærdata

«Blant de som har opplevd hendelser er det 61 prosent som mener årsaken var tilfeldigheter eller uflaks, mens 37 prosent mener det skyldes menneskelige feil» (NSR, 2022, s. 21)

5.3.3 Sikkerhetskultur og beredskap

Spørreundersøkelse:

Spørsmål 15 – Hvor enig er du i følgende påstander?

Svar fordelt på prosent

	Helt uenig	Uenig	Litt uenig	Litt enig	Enig	Helt enig	Vet ikke
Vi har en felles risikoforståelse i vår virksomhet	0 %	0 %	23,1 %	26,9 %	30,8 %	15,4 %	3,8 %
Vi oppmuntrer til å rapportere negative hendelser	3,8 %	0 %	3,8 %	3,8 %	34,6 %	53,8 %	0 %
Vi oppmuntrer til å rapportere positive hendelser	3,8 %	3,8 %	26,9 %	23,1 %	15,4 %	23,1 %	3,8 %

Fageksperter:

«Det er viktig å bygge god sikkerhetskultur ved å få de ansatte med på laget» (Inf.1, sitat #112)

Sekundærdata

«Det er nødvendig med gode prosesser i virksomheten og god sikkerhetskultur hos brukere av systemer og hos virksomhetens ansatte. Dette øker robusthet, men også bevissthet og forståelse for sikkerhet hos den enkelte» (NSR,2022, s. 42)

5.3.4 Risikostyring

Spørreundersøkelse

Spørsmål 9a – Hvilken av følgende risikometodikk, analyser eller rammeverk har du kjennskap til?

Svar	Antall	Prosent
Trefaktor modellen - Verdi, trusel og sårbarhet (VTS)	16	61,5 %
Forventningsverdi (sannsynlighet x konsekvens = forventningsverdi)	11	42,3 %
Feiltreanalyse (FTA)	8	30,8 %
Hendelsestreanalyse (ETA)	9	34,6 %
Sikkerjobbanalyse (SJA)	10	38,5 %
Failure modes and effect analysis (FMEA)	5	19,2 %
Hazard and operability analysis (HAZOP)	8	30,8 %
ISO 27005 - Information security risk management	13	50 %
ISO 31000 – Risikostyring	12	46,2 %
Norsk Standard 5814 – Risikovurdering	12	46,2 %
Norsk Standard 5832 – Sikringsrisiko	7	26,9 %
NIST Risk Management Framework (RMF)	8	30,8 %
Committee of Sponsoring Organizations of the Treadway Commission (COSO)	3	11,5 %
Annet (vennligst spesifiser under)	2	7,7 %

Fageksperter

> *«Six serving men» i Zero Trust tilnærmingen som går på at man må ha kontroll på: Hvem skal ha tilgang? Hva skal man ha tilgang til? Hvor skal man ha tilgang fra? Når trenger man tilgang? Hvordan skal det kommuniseres? Hvorfor trengs denne tilgangen? Hvis man tar med disse seks kontrollene ifm. tilgangsstyring, vil man har god kontroll og sikkerhet» (Inf.1, sitat #139)*

Sekundærdata

> *«Resiliens har utvilsomt elementer som kan styrke en helhetlig risikostyring» (Stavland og Bruvoll, 2019, s. 139).*

5.3.5 Risikobilde

Spørreundersøkelse

Spørsmål 13 – Vi har risikobilde knyttet til cybersikkerhet i vår virksomhet

Svar	Antall	Prosent
Ja	24	92,3 %
Nei	2	7,7 %
Vet ikke / usikker	1	3,8 %

Fageksperter

> *«Jeg tror ikke de fleste virksomhetene har god nok oversikt over sine verdier» (Inf.2, sitat #2)*

Sekundærdata

> *«Den mest alvorlige utviklingen i det nasjonale risikobildet kan oppsummeres i tre hovedpunkter.*
>
> *For det første øker gapet mellom trusselen og sikkerhetsnivået i norske virksomheter og samfunnsfunksjoner. Det skyldes blant annet at bevisstheten og kompetansen om trussel- og risikobildet og hva som utgjør god nok sikkerhet, er for svak. […]*
>
> *For det andre ser vi at sårbarheter i verdikjeder utnyttes mer målrettet. Gjennom stadig nye metoder og virkemidler, som cyberoperasjoner, investeringer og oppkjøp, utnytter trusselaktørene at virksomhetene er knyttet sammen i lange og komplekse verdikjeder […]*
>
> *For det tredje ser vi at taktskiftet i cyberaktivitet mot Norge skjerper den digitale risikoen. Fra 2019 til 2021 har NSM sett en tredobling i antall alvorlige hendelser og cyberoperasjoner. […] I tillegg ser vi en kraftig økning i digital utpressing og sabotasje, såkalte løsepengevirus eller ransomware.» (NSM, 2022a, s. 8-9)*

5.3.6 Resiliens og cyber-beredskap

Spørreundersøkelse

Spørsmål 18 - Gradering «helt uenig» til «helt enig». Hvis du ikke føler at du kan svare på spørsmålet velger du «vet ikke»

	Helt uenig	Uenig	Litt uenig	Litt enig	Enig	Helt enig	Vet ikke
Vi forbedrer vår beredskap basert på erfaringer fra cyberøvelser	0 %	7,7 %	11,5 %	26,9 %	26,9 %	11,5 %	15,4 %
Vi kan tilføre flere beredskapsressurser for å håndtere beredskapshendelser	0 %	0 %	7,7 %	19,2 %	53,8 %	15,4 %	3,8 %
Vi har etablert en beredskap som er basert på det reelle trusselbildet	3,8 %	3,8 %	11,5 %	23,1 %	34,6 %	19,2 %	3,8 %
Vi er kjent med hva som er vårt beredskapsbehov dersom det oppstår en alvorlig cyberhendelse	3,8 %	0 %	7,7 %	26,9 %	38,5 %	23,1 %	0 %
Vi er kjent med hva som er viktig å beskytte dersom det oppstår en alvorlig cyberhendelse	3,8 %	0 %	3,8 %	26,9 %	34,6 %	30,8 %	0 %
Våre sikkerhetstiltak inneholder krav knyttet til responstid, utstyr og kompetanse	3,8 %	7,7 %	7,7 %	30,8 %	26,9 %	19,2 %	3,8 %

Fageksperter

> *«Zero Trust handler det om å gjøre smarte ting, som er relatert til beredskap, krisehåndtering, og rask gjenoppretting» (Inf.1, sitat #113)*

Sekundærdata

> *«det er nødvendig å gjøre cyber-beredskapen mer resilient [Sitat tidligere PST sjef Hans Sverre Sjøvold]» (NSM, 2022b).*

5.4 Presentasjon av tematisk analyse for semistrukturerte intervjuer

Utdrag fra tematisk analyse (vedlegg 10) er presentert i tabellen under

Tabell 10 - Utdrag fra tematisk analyse (vedlegg 10)

Nr	Utdrag fra intervju med fageksperter (ref. Vedlegg 7 og 8)	Kode gruppering	Tema/kategori
Inf. 2	(1) Det å ha oversikt over systemer, verdier, avhengigheter av andre er viktig for å lage god planer.	**A. Læring**	**Cyberhendelse**
Inf. 2	(2) De har ikke oversikt over hvor mange forsøk bedriften deres stanser daglig, ukentlig og månedlig.	50, 52, 76, 77	J, K, L, M
Inf. 2	(3) Ha oversikt over verdiene, jeg tror ikke de fleste virksomhetene har god nok oversikt over sine verdier	**B. Respondere**	**Resiliens og Cyberberedskap**
Inf. 2	(4) Det å ha oversikt over systemer, verdier, avhengigheter av andre er viktig for å lage god planer	1, 4, 5, 17, 34, 41, 52, 59, 75, 110	A, B, C, D, E, O, P, N
Inf. 2	(5) Planene tåler aldri virkeligheten	**C. Overvåking**	**Risikopersepsjon**
Inf. 2	(6) Hvor CFOen sier at du kommer til oss og snakker om dette her	41, 48, 74, 75	F, G, M, P,
Inf. 2	(7) ikke invitert fra teknisk side, altså CISO eller teknologiske del av virksomheten, men fra finans delen	**D. Forutse**	**Sikkerhetskultur og beredskap**
Inf. 2	(8) Det som er interessant er, da jeg snakker om risiko og det som kan ramme dem	8, 17, 26, 41, 102	A, B, C, D, E, O, P
Inf. 2	(9) Så snur konsernsjefen seg til den som er CISO eller teknisk ansvarlig og spør «skjer det oss også»?	**E. Ansvar**	**Risikobilde**
Inf. 2	(10) For meg betyr resiliens motstandsdyktighet og hva er da vi snakker om i beredskaps sammenheng?	9, 20	J, G, M, P

6 Diskusjon

I dette kapittelet vil vi diskutere de funnene som er presentert i empiridelen. Vi sammenstiller funnene belyst med relevant teori angående om resiliens kan bidra til å styrke cyberberedskap i virksomheter.

Vi har strukturert diskusjonen inn i to delkapitler med utgangspunkt i forskningsspørsmålene.

Her sammenstilles funnene fra kvantitative og kvalitative metoder opp imot relevant teoretisk grunnlag med kontekst.

6.1 Behov for resilient tilnærming for å kunne håndtere cyber-hendelser

For å svare på det første forskningsspørsmålet i masteroppgaven FS1, *«Hva kjennetegner at cyber-beredskap i virksomheter er resilient?»*, begynner vi med å belyse cyber-historikken fra 1950 og frem og utvikling av risikofaget fra 1769 (industrielle revolusjonen) til i dag. Videre vil vi si litt om hva som kjennetegner cyber-hendelser, og til slutt knytte dette opp mot våre primær-data (spørreundersøkelse og semistrukturert intervju med fageksperter), samt mot relevante sekundær-data, teori og kontekst.

Cyber-historikk

Datamaskiner gjorde sitt inntog på starten av informasjonsæraen, dvs. for omtrent 50 år siden. Gjennom 1970- og 1980-tallet ble selskaper som Microsoft og Apple mfl. etablert. Mange teknologiske utviklinger, deriblant Internett, hadde sitt opphav fra Forsvaret. Internett ble gradvis tilgjengelig for sivilbruk fra 1980-tallet. På den tiden var det stort fokus på cybersikkerhet i den sivile delen av samfunnet. Likevel var det flere som jobbet med ulike perspektiver på cybersikkerhet. Et av sikkerhetskonseptene som omhandler logisk sikkerhet mellom datamaskiner som ble utviklet av Stephen Paul Marsh (Marsh, 1994), og det sentrale bak modellen for «Zero Trust» er å *«aldri stole på og alltid kontrollere»*. Med dette mener han at ingen mennesker må gis tilgang til noen enheter eller applikasjoner før de er klarert og autorisert for *hver enkelt* av disse (kapitel 3.6). Gjennom 1990 tallet tar internett mer fart og blir mer tilgjengelig for flere virksomheter, og blir også tilgjengelig i private hjem. Gjennom 2000-tallet øker takten av tilkoblede enheter på internett, og selskaper som Google, Twitter og Facebook mfl. (som er helt avhengig av internett) ser dagens lys. En teknisk revolusjon

fortsetter i en eksponentiell hastighet frem til 2020 og COVID-19 pandemien tvinger hele samfunnet til hjemmekontor og hjemmeskole. COVID-19 gir et ytterligere taktskifte i digitaliseringen av samfunnet. Ifølge FN (2020) er Norge rangert på 13. plass i verden og 8. plass i Europa, når det gjelder grad av digitalisering i ulike nasjoner. Ifølge Lysne I utvalget er alt rundt oss digitalisert og påvirker våre liv døgnet rundt (NOU 2015: 13). OT har i større grad standardisert sine systemer ved hjelp av standard IT-komponenter som i de senere årene også benyttes i samfunnet generelt. Dette bidrar bl.a. til at man har høy grad av synergi mellom IT og OT, og dette gir OT mulighet for å ta i bruk produkter fra IT utviklingen (kapittel 2).

Ifølge Erik Hollnagel er sikkerhetsstyrings-historie tett knyttet til den industrielle revolusjonen som startet i 1769 med dampkjeler. Utvikling og effektivisering av transport og masseproduksjon var i fokus, noe som medførte en negativ sikkerhetseffekt på menneskene og samfunnet rundt. For å skape tillit til arbeiderene og samfunnet generelt, ble sikkerhetsstyring introdusert. Hollnagel har oppsummert dette i tre tidsperioder «age of technology», «age of human factors» og «age of safety management», ref. Figur 18. Ifm. katastrofen med nedsmelting av Three Mile Island kjernekraftverket i 1979, oppdaget man til stor overraskelse at risikovurderinger som ble benyttet ikke var tilstrekkelige. Risikoanalysene hensyntok ikke den menneskelige faktoren, og dette ble starten på neste periode «age of human factors». I 1986 oppstår det to alvorlige hendelser, reaktor fire ved kjernekraftverket i Tsjernobyl eksploderer, og romfergen Challenger eksploderer kort tid etter oppskytning. Styringssystem ble satt på dagsorden, og styringssystem i virksomheter ble viktigere enn menneskelige faktorer (Hollnagel, 2014). Fra risikostyring ble introdusert i 1769, med fokus på tekniske risikoanalyser for å redusere negative konsekvenser av ny teknologi og å skape tillit i samfunnet, så har større hendelser (Challenger og Tsjernobyl) bidratt til økt fokus og kunnskap, noe som igjen har medført et taktskifte i videreutvikling av risiko- og beredskapsfagene de siste 40 år.

Fagekspert Thon [Inf. 2, sitater #12; #15] og Ove Njå og Kirsti Russell Vastveit (Njå og Vastveit, 2016), mener at fagområdene cyber og risiko er ungt og umodent, og at man benytter begrepene ulikt eller i forskjellige kontekster.

Cyber-hendelse i senere tid

De store teknologiske fremskrittene gir oss også utfordringer, nye sårbarheter blir introdusert, og de skaper muligheter for de som ikke vil oss vel, trusselaktørene. Disse kan være alt fra de som utfører uskyldige «guttestreker» til store statlige aktører. Ifølge NSM (2022a) er det en

vesentlig forskjell mellom kriminelle og statlige aktører mht. intensjon og kapasitet. De kriminelle utnytter sårbarheter i cyberdomenet med mål om økonomisk vinning. Rapportene fra ENISA, Telenor, Trend micro og Mnemonic viser at cyber-hendelser øker i takt med den teknologiske utviklingen, og denne økningen får store konsekvenser for virksomhetene og samfunnet (ENISA, 2022; Mnemonic, 2021; NSM, 2022a). Ifølge Etterretningstjenesten ble det gjennomført cyberangrep av statlige aktører, og dette var en vellykket etterretningsoperasjon mot Stortinget i 2020 (Etterretningstjenesten, 2021).

Per Helge Seglsten (2022) publiserte to artikler i IT-bransjens tidsskrift Digi.no, som omhandler 38 cyberhendelser som berørte norske virksomheter i 2021 (Seglsten, 2022a, 2022b). En av disse hendelsene var knyttet til løsepenge-virus hos Nortura og konsekvensene av dette kunne vi se i kjøledisken i de lokale dagligvarebutikkene. Det som møtte oss i butikken var tomme ferskvarehyller med en informasjons-lapp med følgende budskap «Til våre kunder. Grunnet dataangrep hos Nortura kan vi være tomme for enkelte produkter fra Gilde, Prior og Folkets. Med vennlig hilsen Kiwi», ref. Figur 6. Det er mange sårbarheter som kan utnyttes for å få tilgang til virksomhetenes cyber- / IKT-systemer, og når vi undersøkte dette i vårt spørreskjema (spørsmål 22a), «*Hvilken/hvilke metode/metoder benyttet trusselaktørene for å bryte seg inn i IT systemene»,* så svarte informantene *at innbrudd via e-post* (27 %), og *innbrudd via brukernavn og passord* (19 %), mens 11 % svarte «*vet ikke*» og 11 % svarte «*annet*». Funn fra intervju med fagekspertene viser at en bør være mer opptatt av hvordan en deler kunnskap og erfaring om forsøk på cyber-angrep, og de argumenterer for at en ikke bare børe dele *etter* at det har skjedd en katastrofe, men også *dele* erfaring og kunnskap når cyber-angrepet faktisk har blitt oppdaget og stoppet (Inf.1, sitat #130).

Ifølge Mørketallsundersøkelsen 2022 viser NSRs undersøkelse at «*40% av de som utsettes for hendelser, oppdager det ved en tilfeldighet*» (NSR,2022, s.6). Den samme undersøkelsen viser at trenden på type hendelser er i endring, og Datatilsynet har «*sett en økning i antall sikkerhetsbrudd som var forårsaket av eksterne aktører med onde hensikter.» (NSR,2022, s.44).*

Daler (2014) beskriver en definisjon på informasjonssikkerhet og cybersikkerhet med KIT modellen (K – Konfidensialitet, I – Integritet og T – Tilgjengelighet), se Figur 10. Ifølge Roar Thon [Inf. 2, sitat #53] og Traavik-utvalget er det tilstrekkelig å benytte disse hovedkategoriene selv om det finnes flere kategorier. Vi legger KIT-modellen til grunn, for å se nærmere på hva som kjennetegner en Cyber-hendelse. Dette blir ofte kategorisert som følger: løsepengevirus, datainnbrudd, phishing, tjenestenekt-angrep. I spørsmål 23 spør vi informantene om hvilken av disse typene cyber-hendelse de ble berørt av. 23 % av informantene svarer da at de var berørt

av løsepenge-virus, 23 % var berørt av phishing mens 15 % var berørt av datainnbrudd. Gøran Tømte utdyper at det er bakenforliggende årsaker til at et cyber-angrep oppstår med følgende:

> *[...] et angrep er ikke en ting, det består av mange steg. Når det sies at phishing tok ned Østre Toten kommunens IT-systemer, er vel dette noe upresist. Ting som kan være bidragsytere til hendelsen er: manglende to-faktor autentisering, manglende sikkerhetsoppdatering, manglende segmentering av infrastruktur, manglende logging, manglende alarmering, manglende menneskelig interaksjon, manglende utgående kontroll på datatrafikken og mer. Dvs. den listen som de kriminelle måtte gjennom for å gjøre suksess, inneholder 10 – 15 momenter som Østre Toten ikke hadde forberedt seg godt nok på. Å skylde på at brukernavn og passord er en risiko når man mangler to-faktor. Da blir det for enkelt å skylde på phishing. [...] (vedlegg 7)*

Gøran Tømte mener at det meste innen cybersikkerhet handler om ««principle of least privilege», altså tilgangskontroll [Inf. 1, sitat # 121]. Selv om man kan følge gode råd og anbefalinger om å ha lange passord blir disse ikke alltid fulgt [Inf. 1, sitat #104]. Dette er et Paradoks. *Er gode råd gode, hvis ingen følger disse?* [Inf.1, sitat #105]. En god tilnærming for å øke graden av cybersikkerhet vil være å benytte Zero Trust perspektivet, som *handler om å gjøre smarte ting som er relatert til beredskap, krisehåndtering og rask gjenopprettelse* [Inf. 1, sitater #113 og #117].

6.2 Bruk av Resilience Engineering for å oppnå bedre cyber-beredskap

For å svare på det andre forskningsspørsmålet i masteroppgaven, «*På hvilken måte kan virksomheter øke graden av sin cyber-beredskap?*», så diskuterer vi først risiko-persepsjon (risiko-opplevelse), sikkerhetskultur og kunnskapsdeling. Videre diskuterer vi hvordan vi ved å øke graden av resiliens med Resilience Analysis Grid (RAG)-metoden, kan øke graden av cyber-beredskap i en IT-avdeling.

Risikopersepsjon

Risikopersepsjon handler om hvordan vi mennesker forstår, opplever og håndterer cyber-risiko (Aven 2019). Ifølge Boysen (2003) er resultatene som utarbeides gjennom risikoarbeidet også avhengig av menneskene som vurderer risiko, samt av deres felles kunnskap om metoder og

teorier som benyttes i risikoarbeidet. Det fremkommer også fra faglitteraturen at risiko ofte baseres på kunnskap «*sett gjennom øynene til de involverte»*.

Begrepet cybersikkerhet har ikke en entydig definisjon, begrepet har grenseflater mot, og omfatter alt fra IKT-nettverk og systemer, samt de tjenestene som systemene leverer og den informasjonen som behandles i systemene i (NOU 2018: 14)

Funn fra intervju med Roar Thon, belyser at cyber-fagområdet er ungt, umodent og at mange benytter begreper som de selv ikke forstår [Inf. 2, sitater #12 og #15]. Dette er i samsvar med funnene til Ove Njå og Kirsti Russell Vastveit som har forsket på hvordan norske kommuner utfører og presenterer risiko og sårbarhetsanalyser. Njå og Vastveit beskriver at de kommunale virksomhetene opplever at forskrifter også er vanskelige å forstå eller å tolke, og at dette bidrar til at det bør stilles kompetansekrav til de som skal operasjonalisere det praktiske ROS-analysearbeidet. Ifølge Njå og Vastveit er det også en utfordring at ROS-analysene ofte blir for «*altomfattende*», og at dette bidrar til at de mindre kommunene opplever at ROS-analyser gir dem liten verdi (Njå og Vastveit, 2016).

Funn fra intervjuet med fagekspertene gir indikasjoner på at virksomhetene ikke forstår hva som er viktigst for dem, at de mangler oversikt [Inf.2, sitater #2 og #74], og at beredskapsplanene i mange virksomheter «*tåler aldri virkeligheten*» [Inf.2, sitat #5]. Fagekspertisen har et annet ståsted, og deres vurdering stemmer ikke med det informantene svarer i spørreundersøkelsen når de besvarte spørsmål nr.15, knyttet «*til at deres virksomhet har et oppdatert risikobilde»*. På dette spørsmålet svarer 23 % at de er *litt enig*, men 35 % svarer *enig* og 38 % svarer at de er *helt enig* i at de har et oppdatert risikobilde for cybersikkerhet.

Når vi analyserte informantenes svar om risikobildet knyttet til spørsmål 14a, om «*hvor ofte oppdateres cybersikkerhet risikoer*», svarte 20 % av informantene at dette utføres en gang pr. kvartal, mens noen virksomheter oppdaterte risikobildet årlig (25 %). Ifølge Boysen (2003) vil menneskers risikoforståelse endres over tid. Dersom vi knytter manglende oppdatering av risikobilde for cybersikkerhet til et sårbarhetsperspektiv for cybersikkerhet, og at denne sårbarheten på et tidspunkt ble vurdert som risikabel, så vil risikoforståelsen for denne sårbarheten endre seg over tid. Hun forteller også at personer har en tendens til å underestimere risiko på områder som de selv forventer å ha kontroll på. Dette kan være faktorer som påvirker risikopersepsjonen, og som kan bidra til en adferd som påvirker hvor ofte risikobildet for cybersikkerhet blir oppdatert. Ifølge NSM er det et generelt behov for å øke forståelsen for trussel- og risikobildet, og de hevder at det er et lederansvar å sørge for nødvendig

kompetanseheving i virksomhetene (NSM, 2022, s. 8-9). Ifølge Mørketallsundersøkelsen 2022, som har undersøkt hvordan virksomheter investerer i opplæring, fremkommer det at virksomheter med mer enn 20 ansatte investerer mer i opplæring enn virksomheter med færre ansatte (NSR, 2022, s. 26). I spørreundersøkelsen har 90 % av virksomhetene mer enn 20 ansatte, og av disse igjen er det 65 % som har mer enn 100 ansatte. Funn knyttet til spørsmål 1 i spørreundersøkelsen vår viser at 75 % av alle som besvarte spørreundersøkelsen hadde mer enn ti års arbeidserfaring, at de kom fra virksomheter med mer enn 100 ansatte, samt at alle disse informantene har mer enn 3 års høyere utdanning. Videre viser funn fra spørsmål 2 at 90 % av informantene er ledere eller rådgivere. Ifølge Roar Thon er cybersikkerhet og beredskap fortsatt umodent [Inf. 1, sitater #12 og #15]. Det er ikke lenge siden myndighetene understreket viktigheten av ledelsesforankring og ledelsens forpliktelser knyttet til å avsette nødvendige ressurser for å ivareta deres cybersikkerhet (Meld. St. 38 (2016-2017), samt at etablering av cyber-kompetanse er et viktig sikringstiltak for å bygge god cybersikkerhetskultur (Hagen el al., 2017). Vi er kjent med at krav og kompetanse knyttet til cybersikkerhet og beredskap begynte å materialisere seg med Nasjonal strategi for digital sikkerhet i 2003, og dette har resultert i at flere lovverk har blitt endret (f.eks. Sikkerhetsloven, 2018; Personopplysningsloven, 2018). På den ene siden, er det nå flere år side våre informanter har avsluttet sin høyre utdannelse. På den andre siden ser vi at kompetanse-bygging foregår på ulike arenaer som f.eks. NSMs sikkerhetskonferanse, NSMs grunnprinsipper for IKT-sikkerhet, kurs, publikasjoner mfl. Et annet viktig aspekt er knyttet til om ledelsen har handlingskraft når det gjelder å etablere et ledelsessystem for sin virksomhet. NSR beskriver at store virksomheter har et etablert ledelsessystem i større grad enn mindre virksomheter (NSP, 2022, s. 13), og at virksomhetene som har et etablert ledelsessystem, i større grad oppdager cyber-hendelser enn mindre virksomheter (NSR, 2022, s.22). Samme undersøkelse viser samtidig at det systematiske arbeidet med styringssystem for digital sikkerhet har stagnert, og dette er ifølge NSR bekymringsfullt (NSR, 2022, s. 37). I virksomheter som omfattes av sikkerhetsloven er det krav om at sikkerhet og beredskap er integrert i virksomhetens styringssystem. Mørketallsundersøkelsen 2022viser at virksomheter som har et etablert ledelsessystem for informasjonssikkerhet, etterlever det som er beskrevet i ledelsessystemet (NSR, 2022, s. 13). En slik etterlevelse er en viktig forutsetning for at virksomhetens cybersikkerhet blir ivaretatt.

Når Norges Teknisk-naturvitenskapelige universitet (NTNU) undersøkte om virksomheter har gjennomført lærings-aktiviteter det siste året, for å øke sine ansattes bevissthet knyttet til sikkerhet, så viser Mørketallsundersøkelsen 2022 at det er stor forskjell på om det er gjennomført tiltak for å øke bevissthet knyttet til cyber-sikkerhet eller ikke. 84 % av de store

virksomhetene har gjennomført tiltak, mens kun 47 % av de små har gjort dette (NSR, 2022, s. 31). Mørketallsundersøkelsen (NSR, 2022, s. 22) viser også at virksomheter som har etablert et styringssystem eller et rammeverk, bidrar mer for å øke ansattes bevissthet knyttet til å oppdage en cyber-hendelse ved rutine kontroll (47 %,) enn de som ikke har etablert dette (28 %). På NSMs sikkerhetskonferanse i 2022 blir det kommunisert at sikkerhetstiltakene i virksomheter ikke er dimensjonert for det virkelige trusselbildet. Sikkerhetstiltakene blir heller ikke etablert raskt nok når nye sårbarheter oppstår. Nasjonale sikkerhetsmyndigheter beskriver også et taktskiftet knyttet til cyberaktivitet mot Norge, noe som har bidratt til at den digitale risikoen for at antall alvorlige cyber-hendelser er tredoblet i perioden 2019 til 2021. Det er bekymringsfullt når økt bevissthet om digital risiko ikke bidrar til at ledelsen i virksomhetene utfører nødvendige handlinger (NSM, 2021, s. 5). Ifølge Marit Boysen er det grunn til å anta at risikoopplevelse påvirker adferd når man knytter dette til å gjøre feil. Det er ifølge faglitteraturen mye som kan påvirke vår risikooppfatning (Engen at el., 2016, s. 94). Marit Boysen beskriver hva som påvirker vår risikooppfatning ut ifra psykologifaget, og som vi eksemplifiserer med ledere som blir presentert en risiko for at en cyber-hendelse kan inntreffe, og som utfordrer ledelsens risiko-oppfatning. I slike tilfeller vil ledelsen tone ned eller overse cyber-risikoen. Dette stemmer godt med funn fra intervju med Roar Thon (vedlegg 8), som forklarte om ledere som ikke trodde at det kunne oppstå en cyber-hendelse i deres virksomhet. Han utdyper dette med følgende eksempel:

> *«Vi er to stykker som har invitert oss selv ut i utvalgte miljøer, hvor vi har hatt spesielt fokus på finansdirektører eller CFOer i virksomheter. Fordi de lever med en risikoforståelse som er mye breiere, de ser på helhetlig risiko for virksomheten med målsetning for at finansdirektører forstår konsekvensene og hva vi snakker om at virksomhetene ikke klarer å produsere noe ting. Og hva om dette varer i 14 dager og hva tenker dere om det? Min erfaring er at ikke alle har tenkt på denne senario til tross for at det ikke har vært mangel på historiserer i media om løsepengevirus. Men da er vi tilbake til at, at denne skjer ikke dem, fordi de holder til på Vestlandet og driver bare med oppdrett laks. [...]*
>
> *Fordi jeg har en opplevelse av at, når jeg blir invitert inn til konsernleder gruppe og det kanskje etter jeg har snakket til en CFO forsamling. Hvor CFOen sier at du kommer til oss og snakker om dette her, så er jeg ikke invitert fra teknisk side, altså CISO eller den teknologiske del av virksomheten, men fra finans delen.*

Fordi jeg føler i disse situasjonene at nå kommer det noen fra sidelinja og ledere med tekniskansvar blir nervøse og syns det er ekkelt i seg selv. Det som er interessant er, da jeg snakker om risiko og det som kan ramme dem. Så snur konsernsjefen seg til den som er CISO eller teknisk ansvarlig og spør «skjer det oss også?» I det øyeblikket forstår man at det ikke er et tema på det nivået i virksomheten. De har ikke oversikt over hvor mange forsøk bedriften deres stanser daglig, ukentlig og månedlig. Når de stiller spørsmål på denne måten internt. Det er også uttrykt mål for oss å få toppledere til å stille noen av de riktige spørsmålene og de vi også opplever til tider er at disse blir også avspist av fagmenneskene. Nei, vi krypterer [...] Jeg hører hva du sier, men er det kryptologi fra Donald eller hva slags krypto er det vi snakker om her?» (Vedlegg 8)

Et annet eksempel knyttes til motivasjon og evne. Både motivasjon og evne påvirker hvordan en selekterer og behandler mottatt informasjon om risiko for cyber-hendelser på, og at dette kan påvirke ledelsens handlinger.

Det er vanskelig for de fleste mennesker å vekte sannsynlighet og konsekvens opp mot hverandre. Risikoforståelsen er også i stor grad individuell og endrer seg over tid, noe som betyr at selv om mennesker vurderer noe som risikabelt på et tidspunkt, så kan risikoforståelsen endre seg dersom en har vært eksponert for cyber-risiko i en lengre tidsperiode. Et annet perspektiv knyttet til risikopersepsjon handler om hva som skjer når informasjon som beskrives som viktig er mottatt. På bakgrunn av den mottatte informasjonen vurderer man sannsynligheten for at en uønsket hendelse skal inntreffe.

Sikkerhetskultur og beredskap

Sikkerhetskultur handler, ifølge Rausand og Utne (2014), om verdier, oppfatninger, holdninger og kommunikasjon og samspill mellom mennesker.

En av våre fageksperter er tydelig på at en bør dele informasjon og kunnskap når cyber-angrep blir stoppet (Vedlegg 7):

«Jeg tror det er viktig å dele erfaring og kunnskap om forsøkt på cyber-angrep som blir stoppet, og ikke bare dele etter at det har skjedd en katastrofe» [Inf. 1, sitat #130].

Østre Toten kommune blir derimot trukket frem som et godt eksempel på hvordan en deler informasjon og kunnskap knyttet til cyber-angrepet som rammet deres kommune [Inf. 1, sitater #130, #131 og #132; Inf. 2, sitat #29]. Dette har ifølge fageksertene bidratt mye for å øke bevisstheten i norske kommuner.

Ifølge NSM (NSM, 2022a) er de helt avhengig av samhandling og varsling fra virksomheter om avvik fra normalen for å bygge et nasjonalt cyber-risikobilde. NSM oppfordrer virksomhetene til å gå gjennom sine varslingsrutiner. Ifølge NSM har varslings- og informasjonsdelingskulturen i virksomhetene et forbedringspotensial. Dette sammenfaller med våre observasjoner ifm. virksomhetenes deltagelse i spørreundersøkelsen. I intervju med Roar Thon, utdyper han åpenhetskulturens dilemmaer med følgende utsagn (vedlegg 8):

> *«[...] virksomheter som er helt åpne som f.eks. Østre Toten kommune. Hvor jeg har berømt de ved flere anledninger på hvordan Østre Toten har stilt opp i enhver tenkelig anledning om ganske ubehagelig ting å snakkes om. Opplæringseffekten av det, bl.a. i kommune Norge har vært enorm og oppvåkning på hva som faktisk kan ramme en virksomhet og en kommune. Det er forståelig at på et eller annet tidspunkt begynner noen av disse personen å bli ganske lei også, f.eks. å besvare på spørreundersøkelse fra dere eller alltid stå på scenen å snakke om disse tingene.» (Vedlegg 8)*

Gøran Tømte utdyper ytterligere dilemmaene som Østre Toten kommune har med tanke på informasjonsdeling [Inf.1, sitat #30; Inf. 2, sitat #40]:

> *«Så åpenhet er veldig sammensatt av forskjellige grunner, noen avstår fra å være åpne fordi det er tidskrevende. Se hvor mange timer som er medgått for at Østre Toten kommune har stått på ulike scener og eventer, hvor både ordføreren og kommunedirektøren har vært delende, men de har samtidig høstet mye skryt for å dele sine erfaringer» (Vedlegg 7)*

Våre data fra spørreundersøkelsen (spørsmål 19) viser at 12 % av informantene ikke ønsker å dele informasjon og dette skyldes at cyberhendelsen er under politietterforskning eller at virksomheten er underlagt lovbestemt taushetsplikt (jf. Sikkerhetsloven, 2018).

På den andre siden, kan virksomhetene komme til å bruke mye ressurser på å dele informasjon om cyberhendelser. Disse virksomhetene må prioritere, og kanskje si nei til å delta på spørreundersøkelser. Det er naturlig å stille spørsmål ved om dette er en begrenset utfordring eller en større utfordring som gjelder flere virksomheter og sektorer.

Det finnes mange forskjellige beskrivelser av en organisasjons sikkerhetskultur, og det er mange som har forsøkt å operasjonalisere og forbedre sikkerhetskulturen i sine virksomheter. James Reason (2016) mener at det er mange som mangler en grunnleggende forståelse for sikkerhetskultur, eller at sikkerhetskultur-begrepet kan være misforstått. Reason beskriver også viktigheten av å ha etablert et informasjonssystem for sikkerhet, samt at en sikkerhetskultur består av flere underkulturer:

«*en rapporterende kultur, en "bry seg" kultur, en fleksibel kultur og en lærende kultur"*
(Reason, 2016, s. 194-196, egen oversettelse)

Når Ranveig Kviseth Tinmannsviks (2008) beskriver en organisasjon med god sikkerhetskultur, så handler beskrivelsen om hva som kjennetegner mennesker i organisasjoner med *god sikkerhetskultur*. Hun trekker frem følgende:

> *«at menneskene til enhver tid er i stand til å forstå hva de skal gjøre, samt at menneskene alltid er klar til å forvente noe som er uventet. I tillegg trekker hun frem to kjennetegn, det ene er at en er åpen for nye forslag, mens det andre handler om at mennesker har tro på at egne handlinger, at det de utfører har en virkning på seg og andre» (Tinmannsviks, 2008).*

Vi er enige med Tinmannsviks beskrivelse knyttet til hva som kjennetegner menneskene i organisasjoner med god sikkerhetskultur. Utvikling av mennesker i et kulturperspektiv skjer i samspill med andre. Slik vi forstår James Reasons teori så mener han at sikkerhetskultur består av flere underkulturer, og at disse har innvirkning på hvor *effektive informasjonssystemene* blir,

og hvordan organisasjoner håndterer en sikkerhetshendelse. Ifølge Reason er det utfordrende å bygge en god sikkerhetskultur som kjennetegnes slik Tinmannsviks beskriver. Vi tenker derfor at det er behov for å begrense sikkerhetsomfanget, og å tydeliggjøre sikkerhetskontekst i en organisasjon, fordi det er utfordrende å beskrive hva sikkerhetskultur egentlig er, og hva det betyr for enkeltmennesker. For en IT-avdeling kan en begrensning for eksempel være knyttet til å omfatte Security, mens konteksten kan knyttes til cybersikkerhet. For en større organisasjon, så mener vi at en benytter samme tankesett, slik at andre relevante fagdisipliner oppnår samme forståelse som IT-avd. Tilført kunnskap til IT-avd. skal bidra til økt forståelse for sikkerhetskultur, og til adferdsendring, hvor IT-avdelingens målsetting er å få en sikkerhetskultur som Tinmannsviks beskriver. Underkulturene som Reason beskriver handler f.eks. om hvordan personer og interessenter skal bidra for å få etablert et *effektivt informasjonssystem* for sikkerhet. Underkulturene han beskriver handler om hvordan en skal *bry seg* når en observerer noe, om kultur knyttet til å *dele kunnskap* og *erfaring,* samt kultur knyttet til *rapportering og læring*. Vi er enige i at det er viktig å ha etablert et *effektivt informasjonssystem,* og tenker at underkulturene som Reason beskriver er implementert, og at disse underkulturene er velfungerende for IT-ansatte. Dette støttes av fagekspert Gøran Tømte: «*at det handler om å gjøre smarte ting, som er relatert til beredskap, krisehåndtering, og rask gjenoppretting*» [Inf.1, sitat #113].

I et sikkerhetskultur-perspektiv tenker vi at det er forbedringspotensial knyttet til hvor ofte virksomheter skal overvåke og oppdatere sitt digitale risikobilde. I dag benytter myndighetene lover og forskrifter som virkemiddel for å styre samfunnssikkerheten, men vi stiller spørsmål ved om dette er tilstrekkelig med bakgrunn i de raske endringene i cyber og virksomhetene. Eksempel fra Njå og Vastveit sin kommune-undersøkelse, som tar utgangspunkt i lovpålagte plikter gjennom Forskrift om kommunal beredskapsplikt (2011), viser undersøkelsen at utarbeidelse av en helhetlig ROS-analyse fremstår som utfordrende og krevende for de som involveres. Deres forskning viser også at deres krav knyttet til å utarbeide helhetlig ROS-analyse er krevende for de involverte. Det gis tilbakemeldinger om at ROS-analysen blir «altomfattende» og at ROS-analysen gir ledelsen liten verdi.

På samme måte som offentlige virksomheter er underlagt kommunal beredskapsplikt, er det andre virksomheter som er underlagt andre lovverk med tilhørende krav om utarbeidelse av ROS, for eksempel er noen virksomheter som underlagt Sikkerhetsloven (2018). Felles for disse lovverkene er at det er krav knyttet til etablering av beredskap og gjennomføring av øvelser. Funn fra Njå og Vastveit sin undersøkelse i kommunene, viser at myndighetene ikke stiller

tydelige krav, eller beskriver *hvordan* virksomhetene skal dimensjonere en beredskap, som er tilpasset deres behov. NSM (2022) er likevel tydelig på at det er viktig å ha etablert en cyber-beredskap som er dimensjonert for det virkelige trusselbildet, men vi er ikke kjent med at NSM beskriver hvordan denne jobben skal utføres. Dette kommer derimot tydeligere frem i faglitteraturen, en 6-trinns systematisk metode (Beredskapsplanleggingshjulet) benyttes når virksomheter skal etablere beredskap som vist i Figur 24. I tillegg har vi i denne oppgaven blitt kjent med at det er mange forskjellige begreper som en skal forholde seg til når en skal etablere en cyber-beredskap. Dimensjonering er også et begrep en skal forstå, og hvordan dette gjøres påvirker både effektiviteten og robustheten knyttet til de tiltakene som skal håndtere cyber-hendelser når de inntreffer. NSM har ansvaret for den nasjonale cybersikkerheten i Norge, og det innebærer at de har et overordnet samordningsansvar for sivilsektor, og for å få tydeliggjort begreper som virksomhetene skal benytte når de skal etablere cyber-beredskap på en beredskapsfaglig og hensiktsmessig måte (NSM, 2017a).

I dag opplever mange virksomheter at det er mange krav knyttet til effektivisering og kostnadsreduksjoner. Samtidig preges virksomhetene hver dag av et høyt innovasjons-tempo, komplekse og sammensatte systemer som ikke alltid er i stand å håndtere overraskelser eller cyber-angrep som plutselig oppstår. Til tross for at en har dimensjonert en cyber-beredskap basert på en risikotenkning, viser det seg likevel at det utenkelige skjer. Virksomhetene som informantene var ansatt i, fikk erfare hva det betyr å bli rammet av et cyber-angrep. Dette viser at en ikke kan styre det utenkelige og at det er et behov for å utvikle dagens systematiske risikostyring. Resiliens er for mange et nytt fagfelt som det er forsket mye på i det siste ti-året, og det har en egenskap som skal bidra til at sosiotekniske systemer som utsettes for plutselige eller uventende påkjenninger, har en evne til å justere seg tilbake til utgangspunktet.

Risikobilde

Ifølge Aven et al. (2019) er det ulike måter å beskrive risiko på, og disse påvirkes av kontekst og betydning. Risiko er også *noens risiko*-beskrivelse. Begrepet cybersikkerhet har ikke noen entydig definisjon (NOU, 2018, s. 13). Upresise og uklare begrepsdefinisjoner en ifølge Aven et al. (2017) er en av årsakene til at risiko er vanskelig å forstå. Det er også mange eksperter og ledere innenfor risiko-analyse og styring som ikke helt forstår hva risiko er, eller ikke forstår grunnleggende analyser eller prinsipper ved beslutningstaking der risiko er et av elementene. Det er ifølge faglitteraturen ikke akseptabelt at de som er involvert i virksomhetenes arbeid med risikoanalyser har manglende kompetanse. Aven hevder at kunnskapsnivået hos de involverte

må heves, fordi de som utfører risikoanalysene må kunne forklare hva resultatet uttrykker og betyr, ref. Aven (2015).

Funn fra spørsmål 7 i vårt spørreskjema handler om hvordan informantene beskriver *begrepet risiko,* og resultatet viser at alle har ulik risikoforståelse, og at de har ulike måter å beskrive risiko på. Dette er i samsvar med ovennevnte teori om når en skal beskrive risiko. Eksempel på dette fremkommer også fra spørreundersøkelsen, hvor en av informantene beskriver at på hans eller hennes arbeidsplass er det en målsetting at hele deres organisasjon skal utføre helhetlige risikovurderinger. Informantene uttrykker videre at disse vurderingene blir begrenset dersom risikoarbeid kun utføres av spesialister eller enkelt-avdelinger. Kunnskap og læring for å øke bevisstgjøringen rundt cybersikkerhet er viktige sikkerhetstiltak. I spørsmål 19 undersøker vi om informantene har erfart eller har opplevd cyber-hendelser. Det fremkommer fra vår undersøkelse at 60 % er kjent med, eller har erfaring med cyber-hendelser i egen virksomhet, og av disse så viser undersøkelsen at 90 % av hendelsene skjedde i perioden 2020-2021 (spørsmål 20). Informanter har kunnskap om at deres virksomhet har blitt rammet av cyber-angrep en eller to ganger. 12 % av informantene ønsket ikke å gi ytterligere detaljer knyttet til cyber-hendelse pga. pågående politietterforskning og at informasjon er unntatt offentlighet. Vi ser også at det er 30 % av informantene som ikke kjenner til at deres virksomhet har vært rammet av cyber-hendelser, noe som indikerer at det er et forbedringspotensial knyttet til å øke sikkerhets-bevisstheten og læring for sine ansatte.

Når virksomhetene besvarer spørsmål 13- *Vi har risikobilde knyttet til cybersikkerhet i vår virksomhet* så svarer mer enn 92 % av informantene at dette finnes hos dem. Det er også lite uenighet når virksomhetene besvarer påstand i spørsmål 15 – *vi har et oppdatert risikobilde for cybersikkerhet*. Spørreundersøkelsen viser at 39 % svarer at de er *helt enige* og 35 % svarer at de er *enige* i dette, mens 23 % svarer at de er *litt enige*. Resultatet fra spørreundersøkelsen knyttet til spørsmål 14a viser at virksomhetene *oppdaterer risikobildet for cybersikkerhet* med ulike tidsintervall. Den største gruppen oppdaterer dette risikobildet en gang pr. år (25 %), mens den neste gruppen (21 %) gjør dette hvert kvartal. Videre svarer noen virksomheter at de oppdaterer risikobildet for cybersikkerhet en gang pr. mnd. (8 %), og 13 % av virksomhetene gjør dette flere ganger pr. mnd. I tillegg er det virksomheter som oppdaterer risikobildet først *etter* at det har oppstått alvorlige hendelser eller større endringer (21 %).

Ifølge fagekspertene (Vedlegg 7 og 8) har de fleste virksomhetene et risikobilde, men innenfor cyber og IKT-fagområdet er dette fortsatt noe umodent [Inf.2, sitat #12], og tilhørende risiko er i varierende grad kjent for virksomhetsledelsen [Inf.2, sitat #38], og dette handler om at

ledelsen ikke forstår det digitale trussel- og risikobildet [Inf.2, sitat #26]. Myndighetene har en viktig rolle i å formidle cyber-risiko på en effektiv måte, men vi stiller et stort spørsmål knyttet til hvor ofte det nasjonale risikobildet for digital sikkerhet blir publisert. I dag blir det digitale risikobildet publisert av NSM en gang i året (JD og FD, 2019, s. 4). Det fremkommer også fra spørreundersøkelsen at en av fire virksomheter oppdaterte sitt cyber-risikobilde en gang i året, samt at det kun er 12 % som gjør dette mer en to ganger pr. måned.

Ifølge Roar Thon er cyber-fagområdet ungt, umodent, og han hevder at mange benytter begreper som de selv ikke forstår [Inf. 1, sitater #12 og #15]. Når vi vurderer hvordan de opplever at *risikobildet for cybersikkerhet* er oppdatert, så gir virksomhetene en score som, etter vår oppfatning, ikke står i forhold til hvor ofte de oppdaterer sine risikobilder. Ifølge Boysen (2003) kan dette skyldes at enkeltpersonene er isolert i sin egen virkelighetsoppfatning, og hun forklarer at risikopersepsjon baserer seg på enkeltpersoners kognitive egenskaper, egne verdier, samt personlige erfaringer. NSM oppfordrer alle virksomheter til å regelmessig gjøre risikovurderinger, men de bidrar ikke med informasjon om hvor ofte dette bør gjøres. Derimot sier NSM at en også skal oppdatere risikoanalysene ved endringer, eller ved tilkobling av nye løsninger og funksjoner i virksomhetens digitale infrastruktur (NSM, 2021, s. 30).

Til tross for at virksomhetene ble rammet av cyber-hendelser i perioden 2017-2021, kan vi ikke, ut fra besvarelsene, finne at deres risikobilder blir oppdatert ofte nok til å håndtere dagens trusselbilde på en god måte. Funn fra fagekspertene beskriver at den åpenhetskulturen som er knyttet til cyber-hendelser er ekstremet varierende, og i prosent er åpenhetskulturen lav [Inf.1, sitat #137; Inf.2, sitater #28 og #29]. Ifølge fagekspertene skyldes dette at ledere ikke tror at de kan bli rammet flere ganger. Deling av kunnskap etter en cyber-hendelse er viktig for å oppnå læring, men funn fra fagekspertene viser at det er et stort forbedringspotensial knyttet til erfaringslæring, ref. oppsummert som følger (vedlegg 7)

> *«det er generelt dårlig med deling av informasjon, men jeg tror vi også kunne ha delt andre ting i tillegg» [Inf.1, sitat #138]:*

Resiliens og cyberberedskap

Det finnes mye litteratur om resiliens, og ifølge Aven (2017) kommer det mer og mer. Resiliens har som andre begreper mange definisjoner, og disse benyttes ifølge Stavland og Bruvoll (2019)

på forskjellig måte. Dette fordi begrepet er tilpasset ulike formål, samt at resiliens benyttes i et stort omfang. Dette stemmer godt med svarene vi fikk fra informantene i vår spørreundersøkelse når de ble spurt om å beskrive begrepet Resiliens (spørsmål 11) og Resilience Engineering (spørsmål 12). Alle beskrev dette ulikt. Resiliens omtales i faglitteraturen som et konsept som kan illustreres som en «paraply-betegnelse», en mekanisme som gjør noe, og som har en evne, og en kapasitet som bidrar til at systemer eller organisasjoner som har blitt utsatt for forstyrrelser, «spretter» tilbake til utgangspunktet (Nemeth og Hollnagel, 2014; Steen og Ferreira, 2021). En av fagekspertene beskrev resiliens som *motstandsdyktighet* [Inf.2, sitat #10]. Vi undersøke også om informantene kjente til både resiliens og Resilience Engineering (RE), og det viste seg at 54 % av informantene kjente til disse begrepene. Basert på antall besvarelser så kan dette indikere at det er de samme personene som har svart på spørsmål 11 og 12. Resiliens har for mange også et abstrakt preg, og ifølge Engen et al. (2020) skyldes dette manglende forståelse av organisasjoner som er, eller har vært resiliente, samt at det er vanskelig å kontekstualisere generelle teorier som knyttes til begrepet resiliens. Dette stemmer med vår forståelse som er basert på at forskere har endret sine definisjoner av resiliens og RE i takt med sin forskning, og at dette også må tas med i ovennevnte betraktning når informantene skulle beskrive begrepene. Erik Hollnagel omtales av Stavland og Bruvoll (2019) som en av pionerne innenfor RE, og han har sammen med Christopher Nemeth bidratt med mye forskning innenfor dette fagområdet. Deres siste resiliens definisjon er forenklet i forhold til tidligere definisjoner, og handler ikke lenger om å håndtere ukjente hendelser knyttet til å ivareta sikkerhet. Hollnagel og Nemeth (2022) beskriver at deres siste resiliens-definisjon handler mer om hvordan en organisasjon eller et system skal håndtere kompleksitet over tid, enn om hvordan de skal gjenskape normalsituasjonen. Slik vi forstår deres siste definisjon, åpner følgende resiliens tenkning for at resiliens kan benyttes innenfor mange fagområder i sosiotekniske systemer:

> *«Evne til å lykkes under varierende forhold, slik at antall tiltenkte og akseptable resultater er så høyt som mulig» (Nemeth og Hollnagel, 2022, s. 3, egen oversettelse)*

Nemeth og Hollnagel (2014) mener også at resiliens-tenkningen kan være nyttig for å utvikle sikkerhetskulturen i organisasjoner. De deler sikkerhetskulturen opp i fem nivåer, og beskriver at organisasjoner som er resiliente kjennetegnes ved at sikker adferd er integrert i alt

organisasjonen utfører. Dette mener vi stemmer godt med hvordan Roar Thon beskriver at en sikkerhetskultur skal være «vi skal ha en virksomhetskultur som inkluderer sikkerhet», og sikkerhet må være en del av normale aktiviteter [Inf. 2, sitater #13 og #14]. På sikkerhetskonferansen (2022) var NSM tydelige på at cybersikkerhet og cyber-beredskap må gjøres resilient, eller mer resilient, for å kunne håndtere morgendagens trusler. Dette fordi dagens systematiske og kunnskapsbaserte risikotenkning ikke bidrar til at vi etablerer cyber-beredskap for noe som er ukjent. Aven (2017) mener at resiliens-tenkning er spesielt relevant for komplekse sammensatte systemer når det er stor usikkerhet knyttet til håndtering av ukjente og usikre hendelser. Eksempel på dette kan forklares med ovennevnte resiliens-definisjon, og i en kontekst der en trusselaktører gjennomfører et cyber-angrep med ondsinnede hensikter i et komplekst sosioteknisk system. Organisasjoner i slike systemer som er resiliente, vil være i stand til å håndtere cyber-angrepet på en vellykket måte. Deres adferd knyttet til å håndtere kompleksiteten i et cyber-angrep vil være avhengig av deres kunnskap basert på normalsituasjon, cyber-sikkerhetskulturen og organisasjonens evner (resiliens-hjørnesteiner). Etablering og anvendelse av en resiliens-funksjonalitet i en slik betraktning vil bidra til å forbedre cyber-beredskapen. Samtidig vil organisasjoner i sosiotekniske systemer som er resiliente, også kunne anvende resiliens-egenskapen i det forebyggende arbeidet i IT-avdelinger. Dette skyldes at resiliens ikke knyttes til tid. En resilient organisasjon arbeider kontinuerlig, og er opptatt av å lære av det som til daglig er normalt, uavhengig av om det oppstår kjente eller ukjente endringer, eller forstyrrelser.

For å avgjøre om organisasjoner eller systemer er resiliente eller ikke, kan en benytte «Resilience Analysis Grid (RAG)» metoden som er omtalt i RE-teorien. RAG-metoden er, ifølge faglitteraturen, egnet til å utvikle og forbedre adferds karakteristikkene til f.eks. en organisasjon i et sosioteknisk system, og vår forståelse er at det er resultatet av dette som bidrar til at organisasjonen *evner* å håndtere hendelsen på en hensiktsmessig måte. En organisasjon eller et system er resilient når alle de fire hjørnesteinene (overvåke, forutse, respondere og læring) er til stede. Med utgangspunkt i at det finnes forskjellige sub-kulturer, og forskjellige sikkerhetskulturer, vil vi benytte en resilient IT-avdeling (i en liten organisasjon) som eksempel når vi diskuterer faktorer som kan påvirke evnen til hver enkelt hjørnestein. Ifølge RAG-metoden kan evnen til hver enkelt hjørnestein utvikles og forbedres, og dette påvirker IT-avdelingens adferd når de håndterer en cyber-hendelse. Med utgangspunkt i RE teori, har IT-avdelingen fokus på daglig drift og vedlikehold av IT-nettverkene med tilhørende IKT-utstyr og programvare. Med økt erfaring vil IT-avd. også få økt sin fagkompetanse, og vil da forstå

hva som er viktig for å opprettholde drift av alt som omfattes av deres ansvarsområde. Sett fra sluttbrukernes perspektiv, vil IT-systemene i virksomheten, gå fra å være reaktive til å bli proaktive.

Gøran Tømte er tydelig på at den tradisjonelle tilnærmingen innenfor cybersikkerhet ikke er tilstrekkelig. Han mener at Zero Trust konseptet må benyttes for å øke cybersikkerheten og beskriver Zero Trust begrepet på følgende måte «[Inf. 1, sitater #121, #123, #124 og #139]:

> *«Det meste innen cybersikkerhet handler om «principle of least privilege», altså tilgangskontroll, ved å begrense hva du skal ha tilgang til for å kunne gjøre jobben din. […]*
>
> *Kort oppsummert handler det om å gjøre smarte ting, som er relatert til beredskap, krisehåndtering, og rask gjenoppretting etter en hendelse, slik at virksomhetene blir proaktive og for å gjøre ting mer robuste. Proaktivt og forhindrer at hendelser skal oppstå og utvikle seg til å bli vellykket for de kriminelle (Vedlegg 7)*

Ifølge Rose et al. (2020) er Zero Trust bygger på prinsippet om sikkerhet i dybden. En Zero Trust-tilnærming tar til orde for at tilgangsstyring må være aktiv, og må kontrollere at alle tilganger til applikasjoner, tjenester og servere, ikke gis før det er 100% validert, f.eks. ved hjelp av multi-faktor autentisering uavhengig av fysisk eller logisk plassering. På den andre siden kan man si at dette ikke nødvendigvis er i konkurranse med KIT modellen, men at Zero Trust-tilnærming gir økt grad av cybersikkerhet. Gøran Tømte utdyper dette med noen eksempler på hvordan Zero Trust skal forstås (Vedlegg 7).

> *«Six serving men i Zero Trust tilnærmingen som går på at man må ha kontroll på:*
>
> - *Hvem skal ha tilgang?*
> - *Hva skal man ha tilgang til?*
> - *Hvor skal man ha tilgang fra?*
> - *Når trenger man tilgang?*
> - *Hvordan skal det kommuniseres?*

- *Hvorfor trengs denne tilgangen?*

Hvis man tar med disse seks kontrollene ifm. tilgangsstyring, vil man har god kontroll og sikkerhet.» [Inf. 1, sitat #139]

Evne til å overvåke

Ifølge faglitteraturen handler evnen til å overvåke om kunnskap for å forstå hva en skal overvåke, for eksempel ved endringer, trusler eller forstyrrelser. Slik vi forstår dette så handler det om å påvirke faktorer som enten er til stede, eller å etablere nye faktorer som sammen eller hver for seg bidrar til at IT-avdelingens overvåknings-evne blir bedre. I et beredskapsperspektiv kan en slik faktor være at IT-avdelingen får tilført kunnskap for å forstå hva de bør overvåke for å ivareta virksomhetens verdier dersom en cyber-hendelse skulle inntreffe. Når en IT-avd. skal overvåke sikringsrisiko innenfor sitt ansvarsområde, er det nødvendig med kunnskap om hva som er virksomhetens verdier. NSMs grunnprinsipper for IKT sikkerhet peker på viktigheten av å identifisere og kartlegge, se Figur 17 (NSM, 2020a, s. 6). Det er utfordrende for en IT-avdeling og drive med overvåkning knyttet til bindinger og eksisterende samspill mellom IT-infrastruktur, cyber-/IKT-systemer, datautstyr og programvare som kan skade virksomhetens informasjonssikkerhet, eller skade digitale verdier, over lang tid.

I Norge har NSM overordnet samordningsansvaret for cybersikkerheten i norske private og offentlige virksomheter (NSM, 2017a), og har som rådgivende organ også bidratt med å utvikle et rammeverk som skal bedre cybersikkerheten. Ved å etablere tiltakene som overvåknings-kategorien viser i kap. 3, vil virksomhetene få etablert en overvåkningsfunksjon som skal ivareta cybersikkerhet. Når det oppstår ulike typer av cyber-hendelser, skal beredskapsplaner benyttes, der cyber-beredskap, ifølge faglitteraturen, skal være etablert og dimensjonert iht. Beredskapsplanleggingshjulet (Figur 24) for å håndtere det beredskapsbehovet som oppstår. En av fagekspertene sier dette på følgende måte [Inf.2, sitat #74]: «*Det å ha oversikt over systemer, verdier, avhengigheter av andre er viktig for å lage god planer*»

Fagekspertene er også kjent med verdiforståelsen i virksomhetene, og beskriver dette på følgende måte (vedlegg 8)

«jeg tror ikke de fleste virksomhetene har god nok oversikt over sine verdier» [Inf.2, sitat #74]

En annen faktor kan være knyttet til kunnskap om egnet teknologi som ivaretar krav knyttet til at overvåknings-behov blir ivaretatt. Ved å dimensjonsjonere tiltakene som skal håndtere overvåkningsbehovet, vil IT-avdelingen også ivareta beredskapsbehovet når dette blir implementert i den daglige IT-driften. Når IT-avdelingens overvåkings-evne økes eller forbedres, vil dette bidra til å øke dens evne til å forutse hva dette betyr, eller til å forstå hvilke konsekvenser det kan få. I tillegg kan vi se for oss at den totale kunnskapen i IT-avdelingen bidrar til at overvåknings-evnen i avdelingen får en tilbakemelding fra responsfunksjonen, og at denne er tilpasset gjeldende cyber-situasjonsbilde. Dette pågår kontinuerlig, slik at IT-avdelingens evne til å overvåke blir mer effektiv og målrettet, samt til at de andre hjørnesteinene får tilført ny informasjon og kunnskap, noe som bidrar at deres evner forbedres.

Evne til å forutse

Ifølge faglitteraturen handler evnen til å forutse om kunnskap til å forstå hva en kan forvente, for eksempel ved endringer av trusler, muligheter eller forstyrrelser. Slik vi forstår det, så handler dette om å påvirke faktorer som enten er til stede, eller om å etablere nye faktorer som sammen eller hver for seg bidrar til at IT-avdelingens evne til å forutse blir bedre. I et beredskapsperspektiv kan en slik faktor være at IT-avdelingen får tilført tilstrekkelig kunnskap som skal bidra til å øke evnen til å forutse hvilke beredskapsbehov som er knyttet til å ivareta virksomhetens verdier, noe som vil redusere konsekvensene dersom en cyber-hendelse skulle inntreffe. Ved å sørge for at IT-avdelingen har drifts-kunnskap, vil de kunne forutse konsekvenser knyttet til det som overvåkes. En annen faktor som kan bidra til å øke IT-avdelingens evne til å forutse, er knyttet til å øke forståelsen for hva som skjer ved ulike responser (karakteristikk) som bidrar til at IT-avdelingen responderer på en hensiktsmessig måte. I tillegg kan vi se for oss at den totale kunnskapen i IT-avdelingen bidrar til at IT-avdelingens evne til å forutse får en tilbakemelding, og at denne er tilpasset gjeldende cyber-situasjonsbilde. Dette pågår kontinuerlig, slik at avdelingens evne til å forutse blir effektiv og målrettet, samt at de andre resiliens-hjørnesteinene får tilført ny informasjon og kunnskap, noe som bidrar til at deres evner forbedres. NSMs grunnprinsipper for IKT-sikkerhet peker på viktigheten av å *oppdage,* som betyr at IT-avdelingen bør etablere prosesser og rutiner for å ivareta forhold som bl.a. «*oppdage og fjerne kjente sårbarheter og trusler*» og «*etablere sikkerhetsovervåkning*», se Figur 17 (NSM, 2020a, s. 6)

Evne til å respondere

Ifølge faglitteraturen handler evnen til å respondere, om kunnskap knyttet til å forstå hvordan en skal respondere, for eksempel for å håndtere endringer, trusler eller forstyrrelser på en hensiktsmessig måte. Slik vi forstår det, handler dette om å påvirke faktorer som enten er til stede, eller om å etablere nye faktorer som sammen eller hver for seg bidrar til at IT-avdelingens respons-evne blir bedre. I et beredskapsperspektiv kan en slik faktor være at IT-avdelingen får tilført tilstrekkelig kunnskap til å forstå hvilken respons som er nødvendig for å ivareta virksomhetens verdier dersom en cyber-hendelse skulle inntreffe. Med kunnskap om hva som er virksomhetens verdier, vil IT-avdelingen benytte denne kunnskapen til å forstå viktigheten av å iverksette relevant beredskaps respons for IT-infrastruktur, IKT-systemer, datautstyr og programvare for å redusere konsekvenser knyttet til virksomhetens informasjonssikkerhet eller verdier ved et evt. cyber-angrep. Ved å dimensjonsjonere respons-tiltakene som skal ivareta beredskapsbehovet, vil respons-evnen i IT-avdelingen bli ivaretatt når tiltakene blir implementert i den daglige IT-driften. Når IT-avdelingens respons-evne økes eller forbedres, vil dette bidra til å øke IT-avdelingens evne til å respondere, samt til å forstå hva responsen medfører av endringer, eller hvilke konsekvenser responsen gir. I tillegg kan vi se for oss at total kunnskapen i IT-avdelingen bidrar til at respons evnen til IT-avdeling får en tilbakemelding, og at denne er tilpasset gjeldende cyber-situasjonsbilde. Dette pågår kontinuerlig, slik at IT-avdelingens evne til å respondere blir mer effektiv og målrettet, samt de andre resiliens-hjørnesteinene får tilført ny informasjon og kunnskap, og som bidrar at deres evner forbedres.

På den ene siden er det viktig å påse at IT-avdelingen har kunnskap, prosesser og resurser til å gjøre daglige arbeidsoppgaver, samt til å få øvd på beredskap innen sitt ansvarsområde. På den andre siden er det viktig å ha ressurser som kan håndtere en alvorlig cyber-hendelse over en lengre periode. Funn i spørreundersøkelsen (spørsmål 21), hvor vi spør informantene om «*hvor lang tid tok det før normalsituasjonen ble gjenopprettet?*». svarer en av informantene som følger:

> *«Produksjonstap kun 3 dager. Operasjonelt alle tjenester tilbake daterer vi til to måneder. Intern normaltilstand (rydding osv.) fire måneder» (spørsmål 21)*

Dette stemmer godt med Roar Thon sine erfaringer, da han forteller om at det vil ta mer enn 48 timer å gjenopprette en normal situasjon [Inf. 2, sitat #73].

Evne til læring

Ifølge faglitteraturen handler evnen å lære, om kunnskap til å forstå hva en skal lære, for eksempel ved endringer, trusler eller forstyrrelser på en hensiktsmessig måte. Slik vi forstår det så handler dette om å påvirke faktorer som enten er til stede, eller om å etablere nye faktorer som sammen eller hver for seg bidrar til at IT-avdelingens lærings-evne blir bedre. I et beredskapsperspektiv kan en slik faktor være at IT-avdelingen får tilført tilstrekkelig kunnskap til å forstå hvilken læring som er nødvendig for at avdelingen skal kunne ivareta virksomhetens verdier dersom en cyber-hendelse skulle inntreffe. Med kunnskap om hva som er virksomhetens verdier, vil IT-avd. forstå viktigheten av å lære hva som er avdelingens beredskapsverdier, og da innenfor deres IT-infrastruktur, IKT-systemer, datautstyr og programvare for å redusere konsekvenser knyttet til virksomhetens informasjonssikkerhet eller verdier. Læring knyttet til arbeidsprosesser for å dimensjonere IT-tiltakene for å ivareta beredskapsbehovet, er en faktor som vil bidra til økt læring i IT-avdelingen. Når lærings-evnen i IT-avdelingen økes eller forbedres, vil dette bidra til å øke IT-avdelingens evne til å lære, og hva læring medfører av endringer, eller hvilke konsekvenser læring gir. I tillegg kan vi se for oss at den totale kunnskapen i IT-avdelingen bidrar til at lærings-evnen i avdelingen får en tilbakemelding, og at denne er tilpasset gjeldende cyber-situasjonsbilde. Dette pågår kontinuerlig, slik at IT-avdelingens evne til å lære blir mer effektiv og målrettet, samt at de andre resiliens-hjørnesteinene får tilført ny informasjon og kunnskap som bidrar at deres evner forbedres.

Funn i spørreundersøkelsen (spørsmål 15) hvor vi spør informantene om *hvordan de oppmuntrer til å rapportere om negative positive hendelser*. Ca. 90 % er nokså enige om at de rapporterer negative hendelser», mens ca. 50 % av respondentene er nokså enige i at de rapporterer positive hendelser. Dette kan indikere at rapportering av positive hendelser ikke er like bra operasjonalisert hos informantenes virksomheter. I intervju med en av fagekspertene blir viktigheten med å få frem det som er positivt og vellykket knyttet til å håndtere en cyber-hendelse på følgende måter (vedlegg 7):

> *«Jeg tror det er viktig å dele erfaring og kunnskap om forsøkt på cyber-angrep som blir stoppet, og ikke bare dele etter at det har skjedd en katastrofe» [Inf. 1, sitat #130].*
>
> *«vi bør kunne dele mere informasjon og kunnskap om når et angrep blir stoppet suksessfullt» [Inf. 1, sitat #132]*

7 Konklusjon

Dersom man ser man cyber-, risiko- og beredskapsfagene under ett, har disse noen fellestrekk. Alle fagene er relativt unge, og har utviklet seg mye gjennom de siste 40-50 årene. Utviklingstakten er fortsatt økende.

Våre funn viser at det er en ubalanse knyttet til cyber-beredskapen i virksomheter, og ønsket tilstand. Endringer i den sikkerhetspolitiske situasjonen nasjonalt og internasjonalt, har medført økt fare for cyber-trusler, og derav økt behovet for å styrke cyber-beredskap og cyber-sikkerhet i virksomheter. I kombinasjon med grenseoverskridende kriminalitet, hvor kriminelle aktører med onde hensikter tar i bruk cyber-teknologi for egen vinning, er dette noe som må tas på alvor.

Funnene i vår masteroppgave viser at det er et behov for å styrke cyber-beredskap i virksomhetene ytterligere. Vi mener å ha funnet at anvendelse av resiliens-teori kan bidra til å styrke cyber-beredskap i virksomheter. Vi mener også å ha funnet at økt bevissthet og kompetanse om hva som kjennetegner mennesker i organisasjoner med god sikkerhetskultur, er en viktig faktor å hensynta for virksomheter som ønsker å utvikle en resilient sikkerhetskultur. Datagrunnlaget i denne masteroppgaven viser at noen av virksomhetene i ulik grad er resiliente, og at graden av resiliens er avhengig av hvor mye virksomheten benytter seg av egenskapene som de fire hjørnesteinene representerer (jfr. lære, respondere, overvåke og forutse). Vi mener å ha funnet at virksomheter ved å øke sin bevissthet og kompetanse om resiliens, på denne måten kan forbedre sin cyber-beredskap. Vi mener også at økt bevissthet og kompetanse om NSMs grunnprinsipper for IKT-sikkerhet er en viktig faktor for å bidra til større grad av resiliens i virksomheter.

Videre forskning

Gjennom våre funn har vi identifisert at det er utfordringer knyttet til informasjonsdeling av cyber-hendelser, hvor fokus på de positive cyber-hendelsene ikke må komme i skyggen av negative hendelser.

Gjennom våre funn har vi identifisert at det er behov for å få etablert et felles begrepsapparat med formål om å effektivisere kommunikasjon og eventuelt redusere misforståelser.

Gjennom våre funn har vi identifisert at Zero Trust konseptet bygger på flere av de samme prinsippene som resiliens. Vi mener det ligger et urealisert potensial i skjæringsfeltet mellom Zero Trust og resiliens, for å øke cybersikkerhet i virksomheter.

8 Referanser:

Eget arbeid (2021). Prosjektoppgave– *E-MRS100 risiko, sikkerhet og sårbarhet 2021*. Upublisert semesteroppgave. Universitet i Stavanger.

Andersen, S. S. (2006). Aktiv informantintervjuing. *Norsk statsvitenskapelig tidsskrift, 22(3), 278–298.* https://doi.org/10.18261/ISSN1504-2936-2006-03-03

Aven, T. (2015). *Risikostyring*, 2. utgave, Universitetsforlaget.

Aven, T. (2017). How some types of risk assessments can support resilience analysis and management. *Reliability Engineering and System Safety 167(2017),* 536-543.

Aven, T. (2021). A risk science perspective on the discussion concerning Safety I, Safety II and Safety III. *Reliability Engineering and System Safety 217*, 108077. (Lest 7. mai 2022)

Aven, T. og Renn, O. (2010). *Risk management and governance: Concepts, guidelines and applications* (Vol. 16). Springer Science & Business Media.

Aven, T., Boyesen, M., Njå, O., Olsen, K.H. og Sandve, K. (2019). *Samfunnssikkerhet, 9. opplag*, Universitetsforlaget.

Aven, T., Boysen, M., Heinzerling, G. og Njå, O, (2003). *Risikoakseptkriterier og akseptabel risiko i transportsektoren – en kunnskapsoversikt*. Rogaland forskning.

Aven, T., Røed, W. og Wiencke, H. S. (2017). *Risikoanalyse: prinsipper og metoder, med anvendelser*. Universitetsforlag.

Backman, S. (2021). Conceptualizing cyber crises. *Journal of contingencies and crisis management*, *29*(4), 429-438.

Bergsjø, H. og Windvik, R. (2018). Datasikkerhet for ledere: *hvordan beskytte din virksomhet.* Universitetsforlaget.

Boysen, M. (2003). Risikopersepsjon: *En innføring i fagfeltet*. Direktoratet for sivilt beredskap (DSB).

Busmundrud, O., Maal, M., Hagness, J. K. og Endregard, M. (2015). *Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger*. Forsvarets forskningsinstiutt.

Clarke, V., og Braun, V. (2017). Thematic analysis. *The Journal of Positive Psychology, 12(3),* 297–298. https://doi.org/10.1080/17439760.2016.1262613

Daler, T., Sjølstad, T., Høie, T. A. og Gulbrandsen, R. (2014). Håndbok i datasikkerhet: *informasjonsteknologi og risikostyring* (3. utgave, 2. opplag). Oslo: Fagbokforlaget.

DSB. (2022, 6. august). *Ansvarsområder og roller*. DSB. https://www.dsb.no/menyartikler/om-dsb/ansvarsomrader-og-roller/. (hentet 25. august 2022)

Engen, O. A. H., Kruke, B.I., Lindøe, P.H., Olsen, K.H., Olsen, O.E. og Pettersen, K.A. (2020). *Perspektiver på samfunnssikkerhet*. 4. opplag, Capplem Damm Akademisk

ENISA (2018, January). Reference Incident Classification Taxonomy. *Task Force Status and Way Forward. European Union Agency For Network and Information Security*. https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy/@@download/fullReport. (hentet 25. august 2022)

ENISA (2022, 29. July). *ENISA threat landscape for ransomware attacks*. European Union Agency for Cybersecurity. ISBN: 978-92-9204-509-8. DOI: 10.2824/168593.

https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks (hentet 5. august 2022)

Etterretningstjenesten (2020). Fokus 2020. *Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer*. Etterretningstjenesten. https://www.etterretningstjenesten.no/publikasjoner/fokus#:~:text=50%20MB-,Fokus%202020,-13%20MB (hentet 27. august 2022)

Etterretningstjenesten (2021). Fokus 2021. *Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer*. Etterretningstjenesten. https://www.etterretningstjenesten.no/publikasjoner/fokus#:~:text=52%20MB-,Fokus2021%2Dhighres,-50%20MB (hentet 27. august 2022)

Etterretningstjenesten (2022). Fokus 2022. *Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer*. Etterretningstjenesten. https://www.etterretningstjenesten.no/publikasjoner/fokus#:~:text=Filst%C3%B8rrelse-,Fokus%2D2022%2Dtil%2Dweb,-9%20MB (hentet 27. august 2022)

Forskrift om kommunal beredskapsplikt. (2011). *Forskrift om kommunal beredskapsplikt (FOR-2011-08-22-894)*. Lovdata. https://lovdata.no/dokument/LTI/forskrift/2011-08-22-894

Forsvarsbygg (2017). Sikringshåndboka. *Håndbok i sikring av eiendom, bygg og anlegg mot terror, abotasje, spionasje og annen kriminalitet*. Forsvarsbygg.

Forsvarsdepartementet og Justis- og beredskapsdepartementet. (2018). Støtte og samarbeid. *En beskrivelse av totalforsvaret i dag*. Forsvarsdepartementet og Justis- og beredskapsdepartementet

Hagen, J., Hermansen, O., Toftegård, Ø., Pettersen, J. M., Steen, R. og Paulen, S.L. (2017). Et helhetlig og fremtidsrettet sikkerhetsregime for forsyningssikkerhet i en digitalisert energisektor. *Regulering av IKT- sikkerhet*. Rapport nr. 26-2017. Norges vassdrags- og energidirektorat. Url: https://publikasjoner.nve.no/rapport/2017/rapport2017_26.pdf

Halvorsen, Knut. (2014). *Å forske på samfunnet: en innføring i samfunnsvitenskapelig metode*, 5.utg. Oslo: Cappelen akademisk forlag.

Hilbert, M. (2022). Digital technology and social change: *The digital transformation of society from a historical perspective*. Dialogues in Clinical Neuroscience., 189–194. https://doi.org/10.31887/DCNS.2020.22.2/mhilbert

Hollnagel, E. (Ed.). (2011). *Resilience engineering in practice: a guidebook*. Version date 26.02.2016. Ashgate Publishing, Ltd..

Hollnagel, E. (2014). Safety-I and Safety-II. *The Past and Future of Safety Management*. Ashgate, England.

ISO, I. (2009). Guide 73: 2009. *Risk management—vocabulary*. ISO 690

JD og FD (2019). *Hovedinstruks for Nasjonal sikkerhetsmyndighet*. Fastsatt av Justis- og beredskapsdepartementet og Forsvarsdepartementet med virkning fra 03.05.2019. Justis- og beredskapsdepartementet og Forsvarsdepartementet. https://nsm.no/getfile.php/134519-1606830131/NSM/Filer/Dokumenter/instruks-for-nsm.pdf

Lunde, I.K. (2019). *Praktisk krise- og beredskapsledelse* (2. utg.*). Oslo: Universitetsforlaget*, 2019.

Marsh, S. P. (1994). *Formalising Trust as a Computational Consept.* PhD thesis, University of Stirling, 1994. http://hdl.handle.net/1893/2010

Meld. St. 10 (2016-2017). *Risiko i et trygt samfunn - samfunnssikkerhet*. Justis- og beredskapsdepartementet. https://www.regjeringen.no/no/dokumenter/meld.-st.-10-20162017/id2523238/ (hentet 19 april 2022)

Meld. St. 12 (2005-2006). *Helse, miljø og sikkerhet i petroleumsvirksomheten.* Arbeids- og inkluderingsdepartementet. https://www.regjeringen.no/contentassets/da47b0ff07c14288821c68c9c7e19d82/no/pdfs/stm200520060012000dddpdfs.pdf (hentet 10 august 2022)

Meld. St. 12 (2017-2018). *Helse, miljø og sikkerhet i petroleumsvirksomheten*. Arbeids- og sosialdepartementet. https://www.regjeringen.no/contentassets/258cadcb3cca4e3c87c858fd787e0f75/no/pdfs/stm201720180012000dddpdfs.pdf (hentet 10 august 2022)

Meld. St. 17 (2001-2002). Samfunnssikkerhet. *Veien til et mindre sårbart samfunn*. Justis- og beredskapsdepartementet https://www.regjeringen.no/contentassets/ee63e1dd1a16409fa0bb737bfda9279a/no/pdfa/stm200120020017000dddpdfa.pdf (hentet 10. Juli 2022)

Meld. St. 38 (2016-2017). IKT-sikkerhet. *Et felles ansvar*. Justis- og beredskapsdepartementet. https://www.regjeringen.no/contentassets/39c6a2fe89974d0dae95cd5af0808052/no/pdfs/stm201620170038000dddpdfs.pdf (hentet 5. april 2022)

Mnemonic (2021). *Cyber Security Report 2021*. Mnemonic. https://www.mnemonic.no/globalassets/security-report/security_report_2021.pdf (hentet 27 mars 2022).

Nemeth, C. P. og Hollnagel, E. (2014). Resilience engineering in practice, Volume 2: Becoming resilient. Ashgate Publishing Limited.

Nemeth, C. P. og Hollnagel, E. (2021). Advancing Resilient Performance. Springer.

Njå, O. og Vastveit, K. R. (2016). Norske kommuners planlegging, gjennomføring og bruk av risiko-og sårbarhetsanalyse i forbindelse med samfunnssikkerhetsarbeidet. Stavanger: University of Stavanger.

Njå, O., Sommer, M., Rake, E.L. og Braut, G.S. (2020). Samfunnssikkerhet, analyse, styring og evaluering, Universitetsforlaget.

NOU 2015: 13. (2015). Digital sårbarhet – sikkert samfunn. *Beskytte enkeltmennesker og samfunn i en digitalisert verden*. Justis- og beredskapsdepartementet.

NOU 2016: 19.(2016). Samhandling for sikkerhet. *Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid.* Forsvarsdepartementet.

NOU 2017: 11. (2017). Bedre bistand. Bedre beredskap. Fr*emtidig organisering av politiets særorganer.* Justis- og beredskapsdepartementet.

NOU 2018: 14. (2018). Organisering og regulering av nasjonal IKT-sikkerhet. *IKT-sikkerhet i alle ledd.* Justis- og beredskapsdepartementet.

NOU 2021: 6. (2021). Myndighetenes håndtering av koronapandemien. *Rapport fra Koronakommisjonen*. Statsministeren.

Nowell, L. S., Norris, J. M., White, D. E., og Moules, N. J. (2017). Thematic Analysis: Striving to Meet the Trustworthiness Criteria. *International Journal of Qualitative Methods, 16(1)*, 1609406917733847. https://doi.org/10.1177/1609406917733847

NSM (2017a, 17. desember). *Rammeverk for handtering av IKT- sikkerhetshendelser*. Nasjonal sikkerhetsmyndighet. https://nsm.no/getfile.php/133853-1593022504/NSM/Filer/Dokumenter/rammeverk-for-handtering-av-ikt-sikkerhetshendelser.pdf (hentet 25. august 2022)

NSM (2017b, 17. desember). Vedlegg 5 – Rammeverk for håndtering av IKT-sikkerhetshetshendelser. *Klassifisering av IKT- sikkerhetshendelser*. Nasjonal sikkerhetsmyndighet. https://nsm.no/getfile.php/133866-1593022796/NSM/Filer/Dokumenter/vedlegg-5---klassifisering-av-ikt-sikkerhetshendelser.pdf (hentet 25. august 2022)

NSM (2020a, 16. april). *Grunnprinsipper for IKT-sikkerhet versjon 2*. Nasjonal sikkerhetsmyndighet. https://nsm.no/getfile.php/133735-1592917067/NSM/Filer/Dokumenter/Veiledere/nsms-grunnprinsipper-for-ikt-sikkerhet-v2.0.pdf (hentet 24. mars 2022)

NSM (2020b, 16. april). *Risiko 2020*. Nasjonal sikkerhetsmyndighet. https://nsm.no/getfile.php/131421-1587034764/NSM/Hermans%20undermappe%20med%20bilder/NSM_Risiko_2020_web_0104.pdf (hentet 12. april 2022)

NSM (2021, 11. mars). *Risiko 2021*. Nasjonal sikkerhetsmyndighet. https://nsm.no/getfile.php/136419-1616673370/NSM/Filer/Dokumenter/Rapporter/NSM_Risiko_2021_web_enkeltside_1203.pdf (hentet 12. april 2022)

NSM (2022a, 11. februar). *Risiko 2022*. Nasjonal sikkerhetsmyndighet. https://nsm.no/getfile.php/137798-1644424185/Filer/Dokumenter/Rapporter/NSM_rapport_final_online_enekeltsider.pdf (hentet 12. april 2022)

NSM (2022b). *Sikkerhetskonferanse 2022*. Nasjonal sikkerhetsmyndighet. https://ctnor.live/sikkerhetskonferansen-2022/

NSR (2022, 9. september). *Mørketallsundersøkelsen 2022*. Næringslivet sikkerhetsråd. https://www.nsr-org.no/uploads/documents/Publikasjoner/Morketalls-2022-web-sider.pdf (hentet 10. september 2022)

Ot.prp. Nr. 61 (2008-2009). *Om lov om endringer i lov 17. juli 1953 nr. 9 om sivilforsvaret mv. (innføring av kommunal beredskapsplikt)*. Justis- og beredskapsdepartementet. https://www.regjeringen.no/no/dokumenter/otprp-nr-61-2008-2009-/id553141/

Patriarca, R., Falegnami, A., Costantino, F., Di Gravio, G., De Nicola, A. og Villani, M. L. (2021). WAx: An integrated conceptual framework for the analysis of cyber-socio-technical systems. *Safety science*, *136*, 105142. (Lest 19 april 2022)

Patriarca, R., Di Gravio, G., Costantino, F., Falegnami, A. og Bilotta, F. (2018b). An analytic framework to assess organizational resilience. *Safety and health at work*, *9*(3), 265-276.

Personopplsyningsloven. (2018). Lov om behandling av personopplysninger (LOV-2018-06-15-38). Lovdata. https://lovdata.no/dokument/NL/lov/2018-06-15-38?q=personopplysningsloven

Prop. 78S (2021-2022). Endringer i statsbudsjettet 2022 (gjelder flere departemententer). Finansdepartementet. https://www.regjeringen.no/contentassets/8ec464ed072f4f459a3b0ad75e4637cd/no/pdfs/prp202120220078000dddpdfs.pdf (hentet 25. August 2022)

Politidirektoratet (2020). Politiets beredskapssystem Del I, *Retningslinjer for politiets beredskap*. https://www.politiet.no/globalassets/05-om-oss/03-strategier-og-planer/pbsi.pdf (lest 27 mars 2022)

PST (2020). *Nasjonal trusselvurdering. Hvitvasking og terrorfinansiering 2020*. Politiets sikkerhetstjeneste. https://www.pst.no/globalassets/artikler/utgivelser/2020/nasjonal-trusselvurdering-om-hvitvasking-og-terrorfinansiering-2020.pdf (25 august 2022)

PST (2021). *Nasjonal trusselvurdering 2021*. Politiets sikkerhetstjeneste. https://www.pst.no/globalassets/artikler/trusselvurderinger/nasjonal-trusselvurdering-2021/ntv_2021_final_web_1802-1.pdf (hentet 25. august 2022)

PST (2022). *Nasjonal trusselvurdering 2022*. Politiets sikkerhetstjeneste. https://www.pst.no/globalassets/ntv/2022/nasjonal-trusselvurdering-2022-pa-norsk.pdf (hentet 25. august 2022)

Rausand, M. og Utne, B.I. (2014). *Risikoanalyse – teorier og metoder*, 2. opplag. Fagbokforlaget Vigmodstad & Bjørke AS

Reason, J. (2016). *Managing the risks of organizational accidents*. Routledge.

Regjeringen Solberg (2020). *Regjeringens strakstiltak for å dempe de økonomiske virkningene av koronaviruset*. https://www.regjeringen.no/no/dokumentarkiv/regjeringen-solberg/aktuelt-regjeringen-solberg/smk/pressemeldinger/2020/regjeringens-strakstiltak-for-a-dempe-de-okonomiske-virkningene-av-koronaviruset/id2693442/ (hentet 27 mars 2022).

Roberts, V. L. 1984. Defensive design, *Mechanical Engineering*, 106(9), s. 88-93.

Rose, S., Borchert, O., Mitchell, S. og Connelly, S. (2019). Zero-Trust Architecture (No. NIST Special Publication (SP) 800-207 (Draft)). *National Institute of Standards and Technology*. https://doi.org/10.6028/NIST.SP.800-207

Seglsten, Per Helge (2022a). Lei årskavalkade: *38 kjente dataangrep rammet norske virksomheter i 2021*. Digi.no en del av Teknisk Ukeblad. https://www.digi.no/artikler/lei-arskavalkade-38-kjente-dataangrep-rammet-norske-virksomheter-i-2021/516067?key=6gQ99CFh (hentet 10 februar 2022)

Seglsten, Per Helge (2022b). Norske IT-angrep i 2021: *Året endte med en bølge av løsepengevirus*. Digi.no en del av Teknisk Ukeblad. https://www.digi.no/artikler/norske-it-angrep-i-2021-aret-endte-med-en-bolge-av-losepengevirus/516449?key=SAWSejCz (hentet 10 februar 2022)

Shariff, S. (2020, 12. november). *What is IT & OT Convergence*. Orignix. https://orignix.com/what-is-it-ot-convergence/ (Hentet 14. Mai)

Sikkerhetsloven. (2018). Lov om nasjonal sikkerhet. (LOV-2018-06-01-24). Lovdata. https://lovdata.no/dokument/LTI/lov/2018-06-01-24

Standard Norge (2012). Samfunnssikkerhet: Beskyttelse mot tilsiktede uønskede handlinger – *Terminologi (NS 5830)*. Lysaker: Standard Norge

Standard Norge (2014a). Samfunnssikkerhet: Beskyttelse mot tilsiktede uønskede handlinger - *Krav til sikringsrisikostyring (NS 5831)*. Lysaker: Standard Norge

Standard Norge (2014b). Samfunnssikkerhet: Beskyttelse mot tilsiktede uønskede handlinger - *Krav til sikringsrisikoanalyse (NS 5832)*. Lysaker: Standard Norge

Stavland, B. og Bruvoll, J.A (2019). Resiliense – hva er det og hvordan kan det integreres i risikostyring. *FFI-Rapport 19/00363*. Forsvarets forskningsinstitutt. https://publications.ffi.no/nb/item/asset/dspace:6458/19-00363.pdf

Steen, R. og Aven, T. (2011). Safety Science: *A risk perspective suitable for resilience engineering*. https://www.researchgate.net/publication/251615094

Steen, R. og Ferreira, P. (2020). Resilient flood-risk management at the municipal level through the lens of the Functional Resonance Analysis Model. *Reliability Engineering & System Safety*, *204*, 107150.

Steen, R., Patriarca, R. og Di Gravio, G. (2021). The chimera of time: Exploring the functional properties of an emergency response room in action. *Journal of Contingencies and Crisis Management*, *29*(4), 399-415.

Telenor (2020). Digital sikkerhet 2020. https://www.telenor.no/binaries/om/digital-sikkerhet/Telenor_Digital_Sikkerhet_2020_1.pdf (hentet 25. juni 2022)

Trend micro (2022). Lockbit, Conti, and Blackcat lead pack amid rise in active RaaS and extortion groups: Ransomware in Q1 2022. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/ransomware-by-the-numbers/lockbit-conti-and-blackcat-lead-pack-amid-rise-in-active-raas-and-extortion-groups-ransomware-in-q1-2022 (hentet 29. september 2022)

United Nations Department for Economic and Social Affairs (DESA). (2020). United Nations E-government Survey 2020: *Digital Government in the Decade of Action for Sustainable Development*. UN. https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020 (hentet 15. Februar 2022)

Veland, H. og Aven, T. (2013). Risk communication in the light of different risk perspectives. *Reliability Engineering & System Safety, 110, 34-40*. https://doi.org/10.1016/j.ress.2012.09.007

Vogt, L. F., Nordby, A. og Nordrum, I. A. (2022). Trente på dataangrep – *måneder senere ble de hacket*. NRK. https://www.nrk.no/innlandet/nortura-ovde-pa-dataangrep_-i-jula-ble-selskapet-hacket-1.15795956 (hentet 10. mars 2022)

Westrum, R., og Adamski, A. J. (1999). Organizational factors associated with safety and mission success in aviation environments. In D. J. Garland, J. A. Wise, & V. D. Hopkin (Eds.), *Handbook of aviation human factors (pp. 67–104)*. Lawrence Erlbaum Associates Publishers.

Wikipedia. (2022). Information Age. https://en.wikipedia.org/wiki/Information_Age (hentet 15. August 2022)

Woods, D. D. (2015). *Four concepts for resilience and the implications for the future of resilience engineering*. Reliability Engineering & System Safety, 141, 5-9.

Woods, D. D. (2019). *Essentials of resilience, revisited*. Handbook on resilience of socio-technical systems, 52-65.

Øien, K., Jovanovic, A. S., Grøtan, T. O., Choudhary, A., Øren, A., Tetlak, K., ... og Jelic, M. (2017). Assessing resilience of SCIs based on indicators. *Smart Resilience Project. European Virtual Institute for Integrated Risk Management, Stuttgart*.

Figur

Figur 1 - Trusselpyramiden (Telenor, 2020, s. 19) ..... - 3 -

Figur 2 – oversikt over cyberhendelser knyttet til trusselaktører (ENISA 2022, s. 26)..... - 4 -

Figur 3 – Cyber-hendelser. V. - tidspunkt på døgnet, H. - aktivitet i ukedagene (Mnemonic, 2021, s. 28-29)..... - 5 -

Figur 4 - Kjente cyber-hendelser offentlig og privat sektor..... - 6 -

Figur 5 - Type cyber-hendelser (Seglsten, 2022a, 2022b) ..... - 6 -

Figur 6 - Bilde av Kiwis ferskvarehylle med produkter fra Nortura (Haraldsen, 2021)..... - 6 -

Figur 7 - Bilde av Coops ferskvarehylle med produkter fra Nortura (NSM, 2022a)..... - 6 -

Figur 8 - Tre paradigmer med informasjonseraen (Wikipedia, 2022; Hilbert, 2022)..... - 9 -

Figur 9 - Basert på Informasjons-, IKT- og Cybersikkerhet (Hagen et al.,2017, s. 15)..... - 10 -

Figur 10 - basert på definisjon av informasjonssikkerhet (Daler et al., 2014, s. 35-36)..... - 11 -

Figur 11 - Cyber-perspektiver i virksomheter, informasjon, IKT og OT. (Shariff, 2020).. - 13 -

Figur 12 – Mørketalls undersøkelse 2022 (Næringslivets sikkerhetsråd, 2022, s.16) ..... - 15 -

Figur 13 – Oversikt over cyber-hendelser fordelt på land (ENISA, 2022, s. 22-23) ..... - 16 -

Figur 14 - Oversikt over nasjonalt beredskapssystem (Politidirektoratet, 2020, s. 18) ..... - 17 -

Figur 15 - Organisering av sentral krisehåndtering ved sivile nasjonale kriser (NOU 2021: 6, s.210)..... - 17 -

Figur 16 - Samhandling mellom NSM, SRM og virksomheter (NSM, 2017a, s. 12)..... - 19 -

Figur 17 - Oversikt over NSMs grunnprinsipper for IKT-sikkerhet (NSM, 2020a, s. 6) ... - 20 -

Figur 18 – Tre tidsaldere av sikkerhets perspektiver (Hollnagel, 2014) ..... - 22 -

Figur 19 – Skisse av teori kapittel..... - 23 -

Figur 20 – Risikotrekanten (Busmundrud et al., 2015, s. 34) ..... - 24 -

Figur 21 – Illustrasjon av sikringsmodell iht. NS5831 (Njå et al., 2020, s. 320)..... - 27 -

Figur 22 – Illustrasjon basert på Sveitserostmodellen (Reason, 1997, s.12)..... - 31 -
Figur 23 – Sløyfediagram (DSB, 2017) ..... - 33 -
Figur 24 - Beredskapsplanleggingshjul med 6 steg (Njå et al., 2020, s. 230)..... - 35 -
Figur 25 - Beredskapsområdet ..... - 38 -
Figur 26 – Resiliensparaplyen (Øien et al.2017)..... - 41 -
Figur 27 – Basert på de fire grunnleggende egenskapene for resiliens (Hollnagel, 2011, s. 279) ..... - 43 -
Figur 28 - Forskningsdesign..... - 49 -
Figur 29 - Tidslinje datainnsamling ..... - 51 -
Figur 30 - Utdrag fra LinkedIn innlegg..... - 56 -
Figur 31 - Steg en til seks ifm. etablering av tematisk analyse (Nowell et al., 2017, s. 4) . - 60 -

Tabell

Tabell 1 - Landene med høyest grad av digitalisering (United Nation, 2020, s.12) ..... - 2 -
Tabell 2 - Oversikt over masteroppgavens utforming..... - 8 -
Tabell 3 – NSMs kategorisering av cyber-hendelser (NSM, 2017b, s.1-2)..... - 14 -
Tabell 4 - Overordnet risikobilde fra sikkerhetsmyndighetene fra 2020 og 2021 ..... - 21 -
Tabell 5 – Fem nivåer av sikkerhetskultur (Nemeth og Hollnagel, 2014, s. 181, egen oversettelse)..... - 30 -
Tabell 6 – Overordnet plan og struktur på relevant teori og emperi ..... - 49 -
Tabell 7 – Utvalg av data (oppdatert 2. oktober 2022) ..... - 52 -
Tabell 8 - Gjennomføring av intervju med fageksperter (informanter) ..... - 57 -
Tabell 9 - Dokumentoversikt sekundærdata..... - 57 -
Tabell 10 - Utdrag fra tematisk analyse (vedlegg 10)..... - 69 -

Forkortelser

AOR Ansvarsområdet
BFF Beredskapssystemet for Forsvaret
CERT Computer Emergency Response Team
COVID-19 Navnet på virus SARS-Cov-2 som gir COVID-19 sykdom
DSB Direktoratet for samfunnssikkerhet og beredskap
DCS Distributed Control System
ENISA European Union Agency for Cybersecurity (tidligere. European Union Agency For Network and Information Security)
EU Europeiske Unionen
FD Forsvarsdepartementet
FCKS Felles cyberkoordineringssenter
FMEA Failure Mode and Effects Analyses
HAZOP Hazard and Operability Analysis
FN De forente nasjoner
IEC International Electrotechnical Commission
ICS Industrielle kontrollsystemer
IKT Informasjon- og kommunikasjonsteknologi
ISO Den internasjonale standardiseringsorganisasjonen
IT Informasjons teknologi
ITIL Information Technology Infrastructure Library
JD Justis- og beredskapsdepartementet
Meld. St. Stortingsmelding
NATO Den nordatlantiske traktats organisasjon
NBS Nasjonal beredskapssystem
NCSC Nasjonal cybersikkerhetssenter
NIST National Institute of Standards and Technology
NOU Nasjonal Offentlig Utredning
NS Norsk Standard
NSM Nasjonal sikkerhetsmyndighet
NSR Næringslivets sikkerhetsråd
OT Operasjonell teknologi (benyttes i prosess og industri systemer)
PBS Politiets beredskapssystem
PC Personlig datamaskiner
PLC / PLS Programable Logical Controler / Programmbare Logisk Systemer
PST Politiets sikkerhetstjeneste
RE Resilience Engineering
ROS Risiko og sårbarhets
ROS-analyse Risiko og sårbarhetsanalyse
SBS Sivil beredskapssystem
SCADA Supervisory Control and Data Acquisition
SRM Sektorvise responsmiljø

Vedlegg

Vedlegg 1 – NSDs vurdering av masteroppgaven - godkjent 103

Vedlegg 2 – Informasjonsskriv til informantene 105

Vedlegg 3 – Informasjonsskriv til informantene - purring 107

Vedlegg 4 – Spørreundersøkelsen 108

Vedlegg 5 – Informasjonsskriv til fagekspertene ifm. intervju 125

Vedlegg 6 – Intervjuguide 126

Vedlegg 7 – Intervju med Gøran Tømte 130

Vedlegg 8 – Intervju med Roar Thon 140

Vedlegg 9 – Dokumentanalyse 152

Vedlegg 10 – Tematisk analyse av intervju med fageksperter 157

Vedlegg 1 – NSDs vurdering av masteroppgaven - godkjent

Meldeskjema / Hvordan styrker resiliens i cyber-beredskap i virksomhetene / Vurdering

Vurdering

Dato
25.03.2022

Type
Standard

Referansenummer
833168

Prosjekttittel
Hvordan styrker resiliens i cyber-beredskap i virksomhetene

Behandlingsansvarlig institusjon
Universitetet i Stavanger / Det teknisk- naturvitenskapelige fakultet / Institutt for sikkerheit, økonomi og planlegging

Prosjektansvarlig
Riana Steen

Student
Anurag Shukla

Prosjektperiode
21.02.2022 - 31.03.2023

Meldeskjema

Kommentar
OM VURDERINGEN
Personverntjenester har en avtale med institusjonen du forsker eller studerer ved. Denne avtalen innebærer at vi skal gi deg råd slik at behandlingen av personopplysninger i prosjektet ditt er lovlig etter personvernregelverket.

Personverntjenester har nå vurdert den planlagte behandlingen av personopplysninger. Vår vurdering er at behandlingen er lovlig, hvis den gjennomføres slik den er beskrevet i meldeskjemaet med dialog og vedlegg.

TYPE OPPLYSNINGER OG VARIGHET
Prosjektet vil behandle alminnelige kategorier av personopplysninger frem til 31.03.2023.

LOVLIG GRUNNLAG
Prosjektet vil innhente samtykke fra de registrerte til behandlingen av personopplysninger. Vår vurdering er at prosjektet legger opp til et samtykke i samsvar med kravene i art. 4 og 7, ved at det er en frivillig, spesifikk, informert og utvetydig bekreftelse som kan dokumenteres, og som den registrerte kan trekke tilbake. Lovlig grunnlag for behandlingen vil dermed være den registrertes samtykke, jf. personvernforordningen art. 6 nr. 1 bokstav a.

PERSONVERNPRINSIPPER
Personverntjenester vurderer at den planlagte behandlingen av personopplysninger vil følge prinsippene i personvernforordningen om:

- lovlighet, rettferdighet og åpenhet (art. 5.1 a), ved at de registrerte får tilfredsstillende informasjon om og samtykker til behandlingen
- formålsbegrensning (art. 5.1 b), ved at personopplysninger samles inn for spesifikke, uttrykkelig angitte og berettigede formål, og ikke viderebehandles til nye uforenlige formål
- dataminimering (art. 5.1 c), ved at det kun behandles opplysninger som er adekvate, relevante og nødvendige for formålet med prosjektet
- lagringsbegrensning (art. 5.1 e), ved at personopplysningene ikke lagres lengre enn nødvendig for å oppfylle formålet

DE REGISTRERTES RETTIGHETER
Personverntjenester vurderer at informasjonen om behandlingen som de registrerte vil motta oppfyller lovens krav til form og innhold, jf. art. 12.1 og art. 13.

Så lenge de registrerte kan identifiseres i datamaterialet vil de ha følgende rettigheter: innsyn (art. 15), retting (art. 16), sletting (art. 17), begrensning (art. 18) og dataportabilitet (art. 20).

Vi minner om at hvis en registrert tar kontakt om sine rettigheter, har behandlingsansvarlig institusjon plikt til å svare innen en måned.

FØLG DIN INSTITUSJONS RETNINGSLINJER
Personverntjenester legger til grunn at behandlingen oppfyller kravene i personvernforordningen om riktighet (art. 5.1 d), integritet og konfidensialitet (art. 5.1. f) og sikkerhet (art. 32).

Nettskjema og Microsoft Office365 er databehandlere i prosjektet. Vi legger til grunn at behandlingen oppfyller kravene til bruk av databehandler, jf. art 28 og 29.

For å forsikre dere om at kravene oppfylles, må dere følge interne retningslinjer og eventuelt rådføre dere med behandlingsansvarlig institusjon.

MELD VESENTLIGE ENDRINGER
Dersom det skjer vesentlige endringer i behandlingen av personopplysninger, kan det være nødvendig å melde dette til oss ved å oppdatere meldeskjemaet. Før du melder inn en endring, oppfordrer vi deg til å lese om hvilke type endringer det er nødvendig å melde: https://www.nsd.no/personverntjenester/fylle-ut-meldeskjema-for-personopplysninger/melde-endringer-i-meldeskjema Du må vente på svar fra oss før endringen gjennomføres.

OPPFØLGING AV PROSJEKTET
Personverntjenester vil følge oppved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet.

Kontaktperson hos oss: Henning Levold
Lykke til med prosjektet!

Vedlegg 2 – Informasjonsskriv til informantene

Hei,

Vi er to studenter i sluttfasen av risikostyring og sikkerhetsledelsen masterstudier ved Universitet i Stavanger. Til daglig jobber vi ved Institutt for energiteknikk (IFE) innenfor beredskap og informasjonsteknologi, vi har erfaring fra ulike bransjer og forsøker nå på cyber-beredskap.

Vi har spørsmål til deg om du kunne tenke deg å delta i vårt forskningsprosjekt hvor formålet er å undersøke hvordan virksomheter arbeider med cyber-beredskap i Norge.

Formål og bakgrunn

Formålet med denne masteroppgaven og dens studie, er å se nærmere på hvordan virksomheter ivaretar og arbeider med cyber-beredskap. Bakgrunnen for undersøkelsen tar utgangspunkt i at det var 38 norske virksomheter som var berørt av ulike former for cyberhendelser i 2021. Vi ønsker å analysere nærmere på og se hvordan risiko, beredskap og resiliens kan styrke virksomhetenes cyber-beredskap (Seglsten, 2022, https://www.digi.no/artikler/lei-arskavalkade-38-kjente-dataangrep-rammet-norske-virksomheter-i-2021/516067?key=6gQ99CFh).

For å kunne besvare på overnevnte, har vi som mål å besvare oppgavens problemstilling:

- Hvordan styrker resiliens cyber-beredskap i virksomhetene?

Hvem er ansvarlig for masteroppgaven?

Universitet i Stavanger er ansvarlig for masteroppgave prosjektet.

Hvorfor får du spørsmål om å delta?

Vi kontakter deg fordi du besitter enten:

1) en aktuell og relevant rolle knyttet til cyber, risiko eller beredskap
2) kjernekunnskap om cyber, risiko eller beredskap
3) erfaring og kunnskap knyttet til involvering eller håndtering av cyber-hendelse
4) kunnskap om læring eller tiltak som ble utført etter at virksomheten ble normalisert igjen

Hva innebærer det for deg å delta?

- Som deltager i masteroppgaven vil du motta en spørreundersøkelse
- Spørreundersøkelse vil bli sendt ut fra Nettskjema (https://nettskjema.no) og vil ta ca. 20 - 30 minutter å besvare
- Bidra med dybdeintervju ved behov

Vi gjør oppmerksom på at resultatene fra spørreundersøkelsene vil bli anonymisert. Utfyllende informasjon hvordan dette blir gjennomført, viser vi til samtykkeskjema med ytterligere detaljer.

Hvor kan jeg finne ut mer informasjon om dette prosjektet?
Hvis du har spørsmål til studien, ta kontakt med en av følgende personer:

- Student, Anurag Shukla, a.shukla@stud.uis.no, 982 22 614
- Student, Even Solbakken, ea.solbakken@stud.uis.no, 454 11 287
- Veileder, Ass. Professor Riana Steen, riana.steen@uis.no

Dersom det er ønskelig, kan vi presentere våre funn knyttet til cyber-beredskap for deres virksomhet etter 1. november 2022. Alle selskapene som deltar i undersøkelsen, vil bli kontaktet av oss for å avklare om noen fra deres virksomhet ønsker dette.
Spørreundersøkelsen gjennomføres ved hjelp av Nettskjema.no (tjeneste levert av Universitet i Oslo) og er tilgjengelig gjennom denne lenken.
https://nettskjema.no/a/cyber-beredskap

Med vennlig hilsen

Even Solbakken
ea.solbakken@stud.uis.no

Anurag Shukla
a.shukla@stud.uis.no

Vedlegg 3 – Informasjonsskriv til informantene - purring

Hei,

Viser til hyggelig telefonsamtale og oversender som avtalt denne e-posten med mere informasjon knyttet til masteroppgaven.

Vi er to studenter i sluttfasen av risikostyring og sikkerhetsledelsen masterstudier ved Universitet i Stavanger. Til daglig jobber vi ved Institutt for energiteknikk (IFE) innenfor beredskap og informasjonsteknologi og har mere enn 64 års arbeidserfaring.

Frist for å svare på spørreundersøkelsen er 30. juni 2022.

Formålet med forskningsprosjekt er å se nærmere på hvordan virksomheter ivaretar og arbeider med cyber-beredskap. I 2021 var det 38 virksomheter som var berørt av ulike former for cyberhendelser som vi ønsker å analysere nærmere på og se hvordan risiko, beredskap og «Resiliense Engeeniering» kan styrke virksomhetenes cyber-beredskap (Seglsten, P. H./Digi.no, 2022, https://www.digi.no/artikler/lei-arskavalkade-38-kjente-dataangrep-rammet-norske-virksomheter-i-2021/516067?key=6gQ99CFh).

Problemstilling i masteroppgaven er:

Hvordan styrker resiliens cyber-beredskap i virksomhetene?

Hva innebærer det for deg å delta?

Spørreundersøkelse tar ca. 20 – 25 minutter og på siste siden har du muligheten for å få en kopi av din besvarelse.

Vi gjør oppmerksom på at resultatene fra spørreundersøkelsene vil bli anonymisert. Utfyllende informasjon hvordan dette blir gjennomført, viser vi til samtykkeskjema med ytterligere detaljer på neste side.

Hvis du har spørsmål til masteroppgaven, vennligst ta kontakt med en av oss personer:

- Student, Anurag Shukla, a.shukla@stud.uis.no, 982 22 614
- Student, Even Solbakken, ea.solbakken@stud.uis.no, 454 11 287

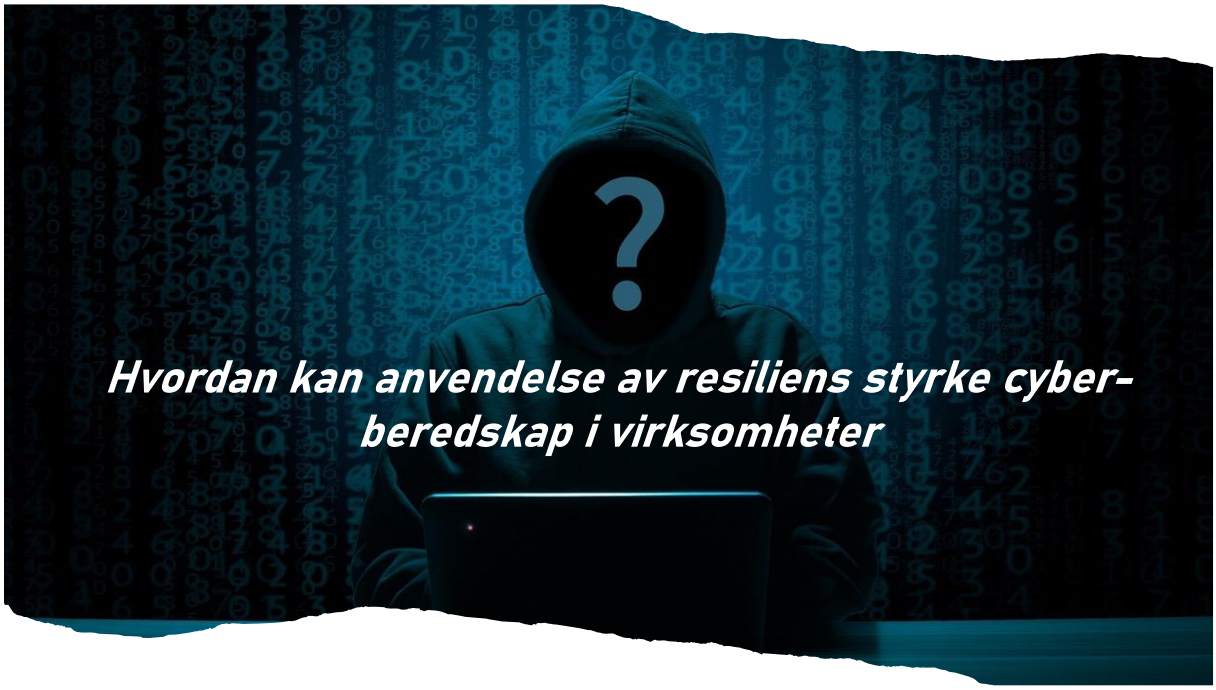
Spørreundersøkelsen gjennomføres ved hjelp av Nettskjema.no (tjeneste levert av Universitet i Oslo) og er tilgjengelig gjennom denne lenken.
https://nettskjema.no/a/cyber-beredskap

Med vennlig hilsen

Even Solbakken
ea.solbakken@stud.uis.no

Anurag Shukla
a.shukla@stud.uis.no

Vedlegg 4 – Spørreundersøkelsen



Vil du delta i et dagsaktuelt forskningsprosjekt innen cyber-beredskap i regi av Universitet i Stavanger?

Vi er to studenter i sluttfasen av risikostyring og sikkerhetsledelsen masterstudier ved Universitet i Stavanger. Til daglig jobber vi ved Institutt for energiteknikk (IFE) innenfor beredskap og informasjonsteknologi og har mere enn 64 års arbeidserfaring.

Frist for å svare på spørreundersøkelsen er 30. juni 2022.

Formålet med forskningsprosjekt er å se nærmere på hvordan virksomheter ivaretar og arbeider med cyber-beredskap. I 2021 var det 39 virksomheter som var berørt av ulike former for cyberhendelser som vi ønsker å analysere nærmere på og se hvordan risiko, beredskap og «Resiliense Engeeniering» kan styrke virksomhetenes cyber-beredskap (Seglsten, P. H./Digi.no, 2022, https://www.digi.no/artikler/lei-arskavalkade-38-kjente-dataangrep-rammet-norske-virksomheter-i-2021/516067?key=6gQ99CFh).

Problemstilling i forskningsprosjektet er:

Hvordan styrker resiliens cyber-beredskap i virksomhetene?

Hva innebærer det for deg å delta?

Spørreundersøkelse tar ca. 20 – 25 minutter og på siste siden har du muligheten for å få en kopi av din besvarelse.

Vi gjør oppmerksom på at resultatene fra spørreundersøkelsene vil bli anonymisert. Utfyllende informasjon hvordan dette blir gjennomført, viser vi til samtykkeskjema med ytterligere detaljer på neste side.

Hvis du har spørsmål til forskningsprosjektet, vennligst ta kontakt med en av oss personer:

- Student, Anurag Shukla, a.shukla@stud.uis.no, 982 22 614
- Student, Even Solbakken, ea.solbakken@stud.uis.no, 454 11 287

Sideskift

Det er frivillig å delta
Du kan når som helst trekke ditt samtykket tilbake uten å oppgi årsak og dine personopplysninger vil bli slettet.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

Vi behandler personopplysningene konfidensielt og i samsvar med personvernsforordningen (GDPR).

- Det er kun vi, Anurag Shukla og Even Solbakken, som vil ha tilgang og kjennskap til informasjon som kan identifisere deg (koblingsnøkkel).
- Koblingsnøkkel for anonymisert informasjon vil bli lagret kun på Universitetet i Stavanger sine systemer og vil ikke på noe tidspunkt bli lagret på andre enheter.
- Data og informasjon er kryptert og iht. til personvernsforordningen.
- For å kunne ivareta dine rettigheter for å kunne trekke samtykke på et senere tidspunkt, har vi behov for å spørre om din e-post adresse (evnt. kodeord). Gjerne bruk privat e-post adresse slik at vi kan identifisere din besvarelse.

Det vil ikke være mulig å identifisere deg eller din organisasjon i den ferdige publikasjonen av forskningsprosjektet.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?

Personopplysningene anonymiseres, samt at koblingsnøkkel slettes når forskningsprosjektet avsluttes 31. mars 2023.

Dine rettigheter

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

- å få innsyn i hvilke personopplysninger som er registrert om deg, og å få utlevert en kopi av opplysningene,
- å få rettet personopplysninger om deg,
- å få slettet personopplysninger om deg, og
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger.

Vi behandler personopplysninger om deg basert på ditt samtykke som er i samsvar med personvernregelverket til Universitet i Stavanger og Norsk senter for forskningsdata AS (*NSD referanse nr: 833168*)

Samtykker du til deltagelse i prosjektet? *

- ○ Ja
- ○ Nei

ⓘ Dette elementet vises kun dersom alternativet «Nei» er valgt i spørsmålet «Samtykker du til deltagelse i prosjektet?»

Dersom du ikke ønsker å bli med i prosjektet, kan du lukke din nettleser.

E-post adresse eller kodeord *

ⓘ Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Samtykker du til deltagelse i prosjektet?»

Som nevnt over, trenger vi din e-post adresse for å ivareta dine rettigheter om du ønsker å trekke ditt samtykke på et senere tidspunkt. Bruk gjerne privat e-post adresse. Om du ønsker å benytte et kodeord som kun du kjenner til er det muligheten for det også, men da er det viktig at du oppgir kodeord til oss på et senere tidspunkt.

Spørsmål 1a - Hva er din høyeste utdanning?

Svar	Antall	Prosent
Videregående skole / fagbrev	7	26,9 %
Fagskole	0	0 %
Høyskole / Bachelorgrad (3 år eller mere?)	11	42,3 %
Universitet / Mastergrad (5 år eller mere?)	8	30,8 %
Doktorgrad eller høyere	0	0 %
Annet (vennligst spesifiser under)	0	0 %

Spørsmål 1b Annet: Har du annen utdanning eller kurs som er relevant?

Vi ønsker å kartlegge om du har annen kompetanse som kan være relevant.
Det kan være kurs med tilhørende sertifisering, eller kurs uten studiepoeng eller tilsvarende. Eksempler på slik utdanning kan være. Digitalt kurs i NS5814:2021 - krav til risikovurdering, Norsk, olje og gas - grunnleggende sikkerhet og beredskap mfl.

- Diverse kurs ved NSM og DSB
- ROS analyse ved NUSB Sikkerhetsledelse ved NSM
- Diverse kurs DSB kurssenter; CIM Øvelsesplanlegging Helhetlig risiko- og sårbarhetsanalyse Beredskapsplanlegging
- Mange kurs, bl.a. SANS ICS410, div kurs i offensive ops, risikostyring, etterretning.
- ISO-27001 ISO-27032
- GIAC GPEN, PCSAE, PCNSE, PEN200 OSCP
- CISSP, CISM, CRISC, ISO 27001
- Min initielle utdannelse/bakgrunn er fra teknisk tegning Valgte å gå over til IT fra 1998 Har tatt flere kurs og sertifiseringer innen IT området: Microsoft, Cisco, Citrix ++ Andre relevante kurs/sertifiseringer er: Prince2, ITIL, Lean, Risk Management, Internal Audit, IEC62443.
- IPC sertifisert Quality Manager, Quality lead auditor, Risk Manager. Krise og beredskapsledelse
- En rekke kurs innen IT-faget, lederkurs.
- Sertifisert Risk Manager - Kurs i Information Security Management (ISO 27001)
- Kryptosertifisering, CEH, ISO 27000

- 12 år som brannkonstabel, 10 år som utrykningsleder, Beredskapsledelse Norges brannskole, Aksjonslederkurs oljevern Kystverket, diverse kurs ROS, stabsarbeid, beredskapsplaner og tiltakskort

Spørsmål 2 - Hvilken stilling eller rolle har du?

Svar	Antall	Prosent
Leder	6	23,1 %
Mellomleder	4	15,4 %
Fagleder	7	26,9 %
Fagarbeider / fagperson / fagspesialist	2	7,7 %
Rådgiver / konsulent	7	26,9 %
Annet (vennligst spesifiser under)	0	0 %

Spørsmål 3 - Hvor lenge har du jobbet hos dagens arbeidsgiver eller virksomhet

Svar	Antall	Prosent
Mindre enn et år (< 1)	7	26,9 %
Mellom et og fem år (1 - 5 år)	11	42,3 %
Mellom fem og ti år (5 - 10)	3	11,5 %
Mellom ti og femten år (10 - 15)	3	11,5 %
Mellom femten og tyve år (15 - 20)	0	0 %
Tyve år eller mere (> 20)	2	7,7 %

Spørsmål 4 – Hvor lang arbeidserfaring har du totalt?

Kartlegging av total arbeidserfaring (inkludert andre roller og funksjoner, virksomheter osv.)

Svar	Antall	Prosent
Mindre enn et år (< 1)	0	0 %
Mellom et og fem år (1 - 5 år)	0	0 %
Mellom fem og ti år (5 - 10)	0	0 %
Mellom ti og femten år (10 - 15)	1	3,8 %
Mellom femten og tyve år (15 - 20)	5	19,2 %
Tyve år eller mere (> 20)	20	76,9 %

*Spørsmål 5 - Hvor mange ansatte er det i din virksomhet? **

Her ønsker vi å kartlegge hvor stor din virksomhet er, basert på antall ansatte (SSBs kategorier er lagt til grunn for svaralternativer).

Svar	Antall	Prosent
Ingen ansatte	1	3,8 %
1-4 ansatte	1	3,8 %
5-9 ansatte	1	3,8 %
10-19 ansatte	0	0 %
20-49 ansatte	2	7,7 %
50-99 ansatte	4	15,4 %
100 - 249 ansatte	2	7,7 %
250 ansatte og over	15	57,7 %

Spørsmål 6a - Hvilken sektor tilhører din arbeidsgiver eller virksomhet?

Her ønsker vi å kartlegge hvilken sektor din arbeidsgiver eller virksomhet tilhører (SSBs oversikt over virksomheter url: https://www.ssb.no/virksomheter-foretak-og-regnskap/virksomheter-og-foretak/statistikk/virksomheter)

Svar	Antall	Prosent
Industri	2	7,7 %
Kraftforsyning	1	3,8 %
Vannforsyning, avløp og renovasjon	0	0 %
Bygge- og anleggsvirksomhet	1	3,8 %
Varehandel, reparasjon av motorvogner	1	3,8 %
Transport og lagring	1	3,8 %
Overnattings- og serveringsvirksomhet	0	0 %
Informasjon og kommunikasjon	6	23,1 %
Finansiering og forsikring	1	3,8 %
Omsetning og drift av fast eiendom	0	0 %
Faglig, vitenskapelig og teknisk tjenesteyting	2	7,7 %
Forretningsmessig tjenesteyting	0	0 %
Offentlig administrasjon og forsvar, trygdeordninger underlagt offentlig forvaltning	6	23,1 %
Undervisning	2	7,7 %
Helse- og sosialtjenester	0	0 %
Kultur, underholdning og fritid i alt	0	0 %
Personlig tjenesteyting	0	0 %
Lønnet arbeid i private husholdninger	0	0 %
Internasjonale organer	0	0 %
Jordbruk, skogbruk og fiske	0	0 %
Bergverksdrift og utvinning	0	0 %
Leverandør eller underleverandør til overnevnte sektorer	0	0 %
Annet (vennligst spesifiser under)	3	11,5 %

Spørsmål 6b – annet:

- Mediabransjen
- ekom
- Kraftsalg
- Entreprenør
- lokalradio
- Forskning
- Bygging, utleie og drift av spesialiserte bygg
- Har hele kommunen beredskap

Risiko

Spørsmål 7 - Hva legger du i begrepet risiko?

Vi ønsker å få kunnskap om hvordan du og din virksomhet beskriver risiko, hvis dere har ulik beskrivelse ønsker vi at du utdyper dette.

- Vi har inndelt risiko i flere områder: Med strategiske risiko menes markedsrisikoer knyttet til utviklingen i reklamemarkedet, forbrukermarkedet, samt omstilling knyttet til produkter og organisasjoner. En operasjonell risiko er en risiko for økonomisk tap som følge av at interne prosesser og sikkerhetssystemer ikke blir fulgt opp, menneskelige feil, systemfeil, uventede ytre hendelser, tap av kritisk kompetanse eller andre tap forårsaket av eksterne forhold som ikke er knyttet til strategiske risikoer eller markedsrisikoer. Mislighold er en operasjonell risiko knyttet til bevisste villedende handlinger for å oppnå personlig vinning eller ulovlig fordel. En finansiell risiko er en risiko for tap knyttet til endrede rente- og valutakurser, evnen til å betjene gjeld og forvaltning av midler. Risikoen for at konsernet ikke opptrer i samsvar med lover, retningslinjer og policyer, etisk adferd og forhold som kan påføre konsernet tap av omdømme, betegnes som en samsvarsrisiko.
- Trussel mot en verdi og verdiens sårbarhet mot trusselen
- Sannsynlighet for at en hendelse med en viss konsekvens skal inntreffe
- Kombinasjon av usikkerhet med konsekvensbilde. I rene sikringsrelaterte spørsmål er også triangelet som definerer risiko som kombinasjonen av sårbarhet, trusselaktører og verdi nyttig.
- Usikkerhet. 2. Et uttrykk for hvor sårbare virksomheten er for å bli utsatt for hendelser som påvirker i negativ retning
- For min del, så legges Aven mfl. sine observasjoner vedr. risiko og tilhørende usikkerhet til grunn.
- Momenter som påvirker ønsket resultatet/prosjekt
- Risiko har et bredt aspekt. I all hoved grad er risiko i mitt felt, når det oppstår hendelser man kan knytte mot MITRE, som vi ikke klarer å løse innenfor 60 sekunder.
- Sannsynligheten for at en gitt hendelse vil inntreffe
- Summen av verdi, trussel og sårbarhet. Avhenger dog av problemstillingen
- RISK: The likelihood and consequence of the business use of IT (or other business critical assets) are exposed to adverse events or interruptions
- Risiko er en kombinasjon av sannsynligheten for at en gitt hendelse vil inntreffe og følgende av at hendelsen inntreffer. F.eks. vil en hendelse med alvorlige følger, men liten sannsynlighet kunne innebære like stor risiko som en hendelse med høy sannsynlighet og mindre alvorlige følger.
- Risiko beskrives som sannsynlighet x konsekvens
- Risiko bestegnes som kombinasjon av mulige konsekvenser og også usikkerhet til dette.
- Risiko er noe vi tar på alvor. Prøver alltid å forebygge det.
- utsatt for strømbrudd alvorlig feil på utstyret og dataangrep
- Det er en målsetning at hele organisasjonen skal utføre risikovurderinger. (ref. helhetlig risiko tilnærming). Effekten blir etter min mening begrenset dersom bare «spesialister» og enkelte avdelinger jobber med risk. For å få med alle er det valgt å bruke enkle begrep og metoder (ref. opplæring og egeninteresse) Vi velger og å knytte det mot mål hvor ulike roller vil ut ifra nivå i organisasjon velge etter sitt «perspektiv», egne mål, avdelingsmål og selskapsmål. «uncertainty that matters» er derfor et begrep som brukes for å forenkle. Dette er det en forenklet versjon av effekten av usikkerhet på målsetninger.
- Vi definerer risiko som utfallet av en analyse om aktuell hendelse har stor sannsynlighet for å skje og påvirkningen av dette.
- Når vi vurderer risiko, tar hensyn til: a) hvilke verdier har vi b) hvilke trusler kan verdiene bli utsatt for c) sannsynligheten for at sikkerhetstruende virksomhet kan inntreffe d) hvilke sårbarheter er knyttet til verdiene e) konsekvensen av

sikkerhetstruende virksomhet for verdiene f) i hvilken grad vi er avhengig av andre virksomheter
- Virkningen av usikkerhet knyttet til mål. Det benyttes, flere beskrivelser avhengig av type risikovurdering.
- Risiko er muligheten for at en uønsket hendelse/sitasjon oppstår som kan skade mennesker eller bedriftens verdier. Verdier kan være både fysiske verdier og/eller ber abstrakte verdier som f.eks. forskningsresultater.
- Selskapet beskriver risiko slik: "Uncertain future events which might lead to the failure to meet one or more of the key business goals as measured in terms of stakeholder expectations".
- Risiko er alle faktorer, kjente og ukjente, som kan påvirke virksomheten negativt, også i direkte, dersom den ikke identifiseres, kvantifiseres og kontrolleres.
- Risiko er noe som kan og vil true kommunens innbyggere på liv, helse, manglende dekning av grunnleggende behov, forstyrrelser i dagliglivet, natur, kultur og økonomisk tap.
- Sjanse for at en uønsket hendelse skal inntreffe.

Spørsmål 8 – Hvilken/hvilke av følgende risikobeskrivelser/definisjoner benyttes eller passer til deres virksomhet?

Under har vi tatt utgangspunkt i noen av definisjon av risiko og ønsker å kartlegge hvilke av disse risiko definisjonene som passer med din eller deres virksomhets definisjon av risiko.

Svar	Antall	Prosent
Risiko uttrykkes gjennom - Sannsynlighet x Konsekvens = Risiko	22	**84,6 %**
Risiko uttrykkes gjennom - Frekvens x Konsekvens = Risiko	6	**23,1 %**
Risiko - opptreden av hendelser med påfølgende konsekvenser, og tilhørende usikkerhet (en vet ikke hvilke hendelser som vil skje og hva konsekvensene vil bli) [Aven, T., 2015. Risikostyring. 2. utgave]	5	**19,2 %**
Risiko – uttrykkes gjennom - usikkerhet knyttet til om en uønskede hendelse vil inntreffe og hvilke konsekvenser den kan få (usikkerhet kan uttrykkes gjennom sannsynlighet) [NS5814:2021]	4	**15,4 %**
Risiko – effekten av usikkerhet på målsetninger [ISO 31000, ISO 73 og ISO 27005]	4	**15,4 %**
Risiko er knyttet til verdi, trussel og sårbarheter (trefaktor modellen eller VTS trekanten)	12	**46,2 %**
Jeg eller vår virksomhet benytter en annen beskrivelse/definisjon på risiko (vennligst spesifiser under)	0	**0 %**

Spørsmål 9a – Hvilken av følgende risikometodikk, analyser eller rammeverk har du kjennskap til?

Om du kjenner til eller forstår noen av de følgende, ønsker vi at du velger en eller flere i listen under

Svar	Antall	Prosent
Trefaktor modellen - Verdi, trusel og sårbarhet (VTS)	16	61,5 %
Forventningsverdi (sannsynlighet x konsekvens = forventningsverdi)	11	42,3 %
Feiltreanalyse (FTA)	8	30,8 %
Hendelsestreanalyse (ETA)	9	34,6 %
Sikkerjobbanalyse (SJA)	10	38,5 %
Failure modes and effect analysis (FMEA)	5	19,2 %
Hazard and operability analysis (HAZOP)	8	30,8 %
ISO 27005 - Information security risk management	13	50 %
ISO 31000 – Risikostyring	12	46,2 %
Norsk Standard 5814 – Risikovurdering	12	46,2 %
Norsk Standard 5832 – Sikringsrisiko	7	26,9 %
NIST Risk Management Framework (RMF)	8	30,8 %
Committee of Sponsoring Organizations of the Treadway Commission (COSO)	3	11,5 %
Annet (vennligst spesifiser under)	2	7,7 %

Spørsmål 9b – annet:

- Ingen kjennskap
- Jeg kjenner til, som i «har hørt om», en rekke av disse, men vil ikke kunne beskrive noen av dem kun ut fra navn/forkortelse.
- Jeg vil da også trolig være kjent med, og bruke, flere av dem, uten å kunne si hva de heter.

Spørsmål 10 – Kjenner du til begrepet Resiliens eller Resiliense Engineering?

Svar	Antall	Prosent
Ja	14	53,8 %
Nei	12	46,2 %

Spørsmål 11: Kan du beskrive nærmere hva du legger i begrepet «Resiliens»?

- evnen til å håndtere stress og katastrofer
- Motstandsdyktighet
- Robusthet for å tåle påvirkning fra uønskede hendelser med definert nivå av midlertidig degradering av ytelse.
- I og med det ikke finnes noen forhold hvor «resiliens» kan oversettes direkte til Norsk – Så bruker jeg begrepet resiliens på flere måter. Men i all hovedsak, så anser jeg resiliens som «et systems evne til å motstå en uønsket hendelse eller uventet belastning».
- Motstandsdyktighet
- Robusthet i møte med påkjenning. Evne til å gjenoppta produksjon etter hendelse
- Resiliens er hvor stabil/sterkt et system er, og derav hvor mye unormale hendelser/feil systemet tåler før det

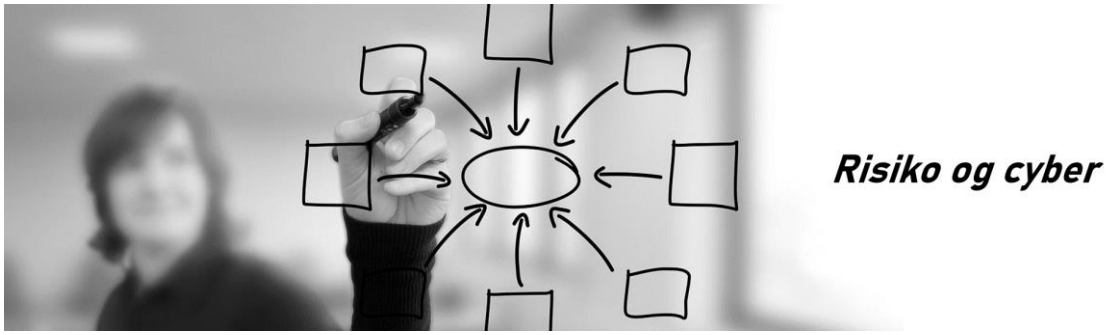
slutter å fungere, eller har vesentlig redusert funksjonalitet.
- Evne til å håndtere endringer som kan ha negativ effekt
- Hvor motstandsdyktige vi er på IT siden mot ulike hendelser.
- Motstandsdyktige systemer
- Motstandsdyktighet

- Evnen til å hurtig jobbe seg gjennom kriser /komme tilbake til normalen.
- Resiliens er evne til motstand mot uønskede negative hendelser.
- Motstand mot at uønskede hendelser kan oppstå og/eller få store konsekvenser (Fritt etter personlig erfaring, utdanning og oppfatning)

a) Hvilken stilling eller rolle har du?

Spørsmål 12 – Kan du beskrive nærmere hva du legger i begrepet «Resiliense Engineering»?

- evne til å forutse, forberede og respondere på en hendelse
- Aktiviteter som utføres for å oppnå robusthet, gjennom systematiske metoder (arkitekturdesign, risikoanalyse, driftsplanlegging, forbedringsarbeid, etc.)
- Med henvisning til forrige punkt, så anser jeg resiliens engineering til det arbeidet som legges til grunn for å gjøre ett stand til å være «motstandsdyktig» (ref. dårlig oversettelse). Fokus må flyttes fra reaktivt fokus, til proaktivt fokus hvor en må så på hva en gjør «rett» og videre hvordan en kan gjøre mer «rett»
- Utviklingsorientert / kontinuerlig motstandsdyktighet
- Lage robuste systemer og prosesser
- Resiliense engineering er design av systemer for å være så resiliente som mulig, mao at de skal tåle mest mulig før funksjonalitet er redusert. Dette kan f eks være bruk av redundans og/eller diversitet, slik at enkelthendelser ikke har negativ innvirkning på systemet som helhet.
- Strategier og metoder for å kunne påvirke utfallet av uønskede hendelser
- F.eks. pen. Test. Oppdage, måle og forbedre
- Hvordan skape motstandsdyktige systemer ved å identifisere mulige hendelser og forebygge dem – styre sikkerhetsarbeidet mot det som gir effekt
- Kjenner ikke til begrepet resiliense engineering, men oppfatter at det omhandler metodikk for å styrke motstandsdyktighet.
- Designe og bygge systemer og prosesser som absorberer eller forhindrer alvorlige feil eller skader.
- Resiliense Engineering er design av motstand mot uønskede negative hendelser for alle deler av verdikjeden, gjennom ett eller flere parallelle eller etterfølgende tiltak per risikoutsatte teknologi, prosess eller organisasjon Begrepet som sådan har jeg ikke vært mye borti, men det vil bety å designe/forme systemer for økt resiliens.



Spørsmål 13 – Vi har risikobilde knyttet til cybersikkerhet i vår virksomhet

Svar	Antall	Prosent
Ja	24	92,3 %
Nei	2	7,7 %
Vet ikke / usikker	1	3,8 %

Spørsmål 14a – Hvor ofte oppdateres cybersikkerhet risikoer?

Svar	Antall	Prosent
Mindre enn gang pr. år	1	4,2 %
En gang pr. år	6	25 %
To ganger pr. år	1	4,2 %
Hvert kvartal	5	20,8 %
En gang pr. måned	2	8,3 %
Flere ganger pr. måned	3	12,5 %
Kun ved alvorlig hendelse eller større endringer	0	0 %
Flere gang pr. år og ved alvorlig hendelse eller større endringer	5	20,8 %
Annet (vennligst spesifiser under)	1	4,2 %

Spørsmål 14b – annet:

- Revideres minimum hvert kvartal, men skal oppdateres ved relevante eksterne /interne hendelser.

Spørsmål 15 – Hvor enig er i følgende påstander?

Gradering «helt uenig» til «helt enig». Hvis du ikke føler at du kan svare på spørsmålet velger du «vet ikke»

Svar fordelt på prosent

	Helt uenig	Uenig	Litt uenig	Litt enig	Enig	Helt enig	Vet ikke
Vi har en felles risikoforståelse i vår virksomhet	0 %	0 %	23,1 %	26,9 %	30,8 %	15,4 %	3,8 %
Vi oppmuntrer til å rapportere negative hendelser	3,8 %	0 %	3,8 %	3,8 %	34,6 %	53,8 %	0 %
Vi oppmuntrer til å rapportere positive hendelser	3,8 %	3,8 %	26,9 %	23,1 %	15,4 %	23,1 %	3,8 %
Vi har et oppdatert risikobilde for cybersikkerhet	0 %	3,8 %	0 %	23,1 %	34,6 %	38,5 %	0 %
Vi har nødvendig kunnskap om risikostyring	3,8 %	7,7 %	3,8 %	15,4 %	42,3 %	23,1 %	3,8 %
Vi har kunnskap om risikofaget for å kunne utføre cyber risikovurderinger	3,8 %	3,8 %	7,7 %	15,4 %	34,6 %	30,8 %	3,8 %
I vår virksomhet har vi identifisert informasjons- og digitale verdier	3,8 %	0 %	15,4 %	19,2 %	34,6 %	26,9 %	0 %
Vi har kunnskap om hvilke trusler som kan ramme vår virksomhet?	3,8 %	0 %	3,8 %	23,1 %	34,6 %	34,6 %	0 %
Vi har oversikt over våre sårbarheter	3,8 %	3,8 %	3,8 %	23,1 %	50 %	15,4 %	0 %
Vår virksomhet overvåker sårbarheter knyttet til cybersikkerhet	3,8 %	0 %	7,7 %	30,8 %	23,1 %	34,6 %	0 %
Vi har en etablert prosesser og/eller rammeverk for oppfølging av våre leverandører (jf. informasjonssikkerhet, digital sikkerhet og/eller cybersikkerhet)	0 %	0 %	11,5 %	34,6 %	26,9 %	23,1 %	3,8 %

I denne delen av spørreundersøkelsen skal vi fokusere på beredskap tema.

Spørsmål 16 – Beredskap del 1

Gradering «helt uenig» til «helt enig». Hvis du ikke føler at du kan svare på spørsmålet velger du «vet ikke»

	Helt uenig	Uenig	Litt uenig	Litt enig	Enig	Helt enig	Vet ikke
Vi har beredskapsplaner for å kunne håndtere krise- og beredskapssituasjoner for vår virksomhet	0 %	3,8 %	0 %	23,1 %	30,8 %	42,3 %	0 %
Vi har cyber-beredskap som er dimensjonert i forhold til virksomhets risikoer	0 %	7,7 %	11,5 %	34,6 %	23,1 %	19,2 %	3,8 %
Vi har etablert en beredskapsorganisasjonen for å kunne normalisere cyber-hendelser	0 %	3,8 %	23,1 %	26,9 %	11,5 %	30,8 %	3,8 %
I vår virksomhet gjennomfører vi trening og/eller øving på uønskede hendelser	3,8 %	11,5 %	11,5 %	30,8 %	11,5 %	30,8 %	0 %
Vår cyberberedskap har tilgang på ekspertkompetanse	0 %	0 %	3,8 %	11,5 %	42,3 %	38,5 %	3,8 %

Spørsmål 17 - Vi blir revidert på beredskapsplanverket (effektivitet, kapasitet eller kompetanse)

Svar	Antall	Prosent
Ja	14	53,8 %
Nei	7	26,9 %
Vet ikke	5	19,2 %

Spørsmål 18 – Beredskap del 2

	Helt uenig	Uenig	Litt uenig	Litt enig	Enig	Helt enig	Vet ikke
Vi forbedrer vår beredskap basert på erfaringer fra cyberøvelser	0 %	7,7 %	11,5 %	26,9 %	26,9 %	11,5 %	15,4 %
Vi kan tilføre flere beredskapsressurser for å håndtere beredskapshendelser	0 %	0 %	7,7 %	19,2 %	53,8 %	15,4 %	3,8 %
Vi har etablert en beredskap som er basert på det reelle trusselbildet	3,8 %	3,8 %	11,5 %	23,1 %	34,6 %	19,2 %	3,8 %
Vi er kjent med hva som er vårt beredskapsbehov dersom det oppstår en alvorlig cyberhendelse	3,8 %	0 %	7,7 %	26,9 %	38,5 %	23,1 %	0 %
Vi er kjent med hva som er viktig å beskytte dersom det oppstår en alvorlig cyberhendelse	3,8 %	0 %	3,8 %	26,9 %	34,6 %	30,8 %	0 %
Våre sikkerhetstiltak inneholder krav knyttet til responstid, utstyr og kompetanse	3,8 %	7,7 %	7,7 %	30,8 %	26,9 %	19,2 %	3,8 %

Spørsmål 19 - Har du erfart eller opplevde cyber-hendelsene som fikk konsekvenser for deg eller din virksomhet?

Svar	Antall	Prosent
Ja, og det fikk alvorlig konsekvenser for meg eller virksomheten	6	23,1 %
Ja, og personopplysninger eller viktig informasjon var på avveie	1	3,8 %
Ja, men det fikk ingen alvorlig konsekvenser	8	30,8 %
Ja, men ønsker ikke å dele detaljer (vennligst spesifiser under)	3	11,5 %
Nei, jeg er ikke kjent med at jeg eller virksomheten jeg jobber for er utsatt for cyber-hendelse	5	19,2 %
Nei, jeg eller min virksomhet har ikke vært utsatt for cyber-hendelse	2	7,7 %
Vet ikke	1	3,8 %

Spørsmål 20 - Når skjedde cyber-hendelsen (årstall), hvis flere cyber-hendelser ønsker vi å få kunnskap om det?

Kun relevant hvis man svarer ja på spørsmålet 19. Vi ønsker å få kunnskap om årstall og evnt. frekvens / antall gang du eller din virksomhet har blitt utsatt for Cyber-hendelse.

Spørsmål 20 - når skjedde cyberhendelse i din virksomhet?

Svar	Antall	Prosent
2016	0	0 %
2017	1	6,7 %
2018	0	0 %
2019	1	6,7 %
2020	5	33,3 %
2021	10	66,7 %
2022	1	6,7 %

Spørsmål 21 Hvor lang tid tok det før normalsituasjonen ble gjenopprettet?

Her ønsker vi å kartlegge tiden det tok før normalsituasjon ble etablert etter cyber-hendelse. I noen tilfeller kan det være vanskelig å skille mellom tidligere normalsituasjonen og ny normalsituasjon.

- tre dager
- Produksjonstap kun 3 dager. Operasjonelt alle tjenester tilbake daterer vi til to måneder. Intern normaltilstand (rydding osv.) fire måneder.
- en uke
- Jeg har inntrykk av at situasjonen ganske raskt var tilbake til normalen
- tre dager
- to dager
- en uke
- en dag

- 1en til to dager. Kun avgrensede deler av IT-løsningene ble rammet.
- tre dager
- tre uker
- tre – fire måneder
- tre dager
- to til fire timer
- to til tolv timer er det mest normale ved opprydning av innbrudd eller kryptovirus.

Spørsmål 22a - Hvilken/hvilke metode/metoder benyttet trusselaktørene for å bryte seg inn i IT systemene

(hvis flere benytter gjerne tekstboks under for å utdype dette)?

Svar	Antall	Prosent
Innbrudd via e-post	7	26,9 %
Innbrudd via vannhull (lurer brukeren til å installere et program)	0	0 %
Innbrudd via skyleverandører	0	0 %
Innbrudd via gammelt utstyr	1	3,8 %
Innbrudd via Internet of Things (IoT)	0	0 %
Innbrudd via nettsider og databaser	2	7,7 %
Innbrudd via brukernavn og passord (innlogging detaljer på avveie eller lett passord å gjette)	5	19,2 %
Innbrudd via ved bruk av innsider	0	0 %
Direktørsvindel og klassisk svindel	2	7,7 %
Innbrudd gjennom avlytting og tilgang til trafikk	0	0 %
Vet ikke	3	11,5 %
Annet (vennligst spesifiser under)	3	11,5 %

Spørsmål 22b – annet:

- Feilen skjedde ved feil i korrelasjons mellom kunde ID og digital strømmåler
- Phishing (via e-post)
- Deles ikke på nåværende tidspunkt

Spørsmål 23 - Hvilken type cyberhendelser ble dere berørt av?

Svar	Antall	Prosent
Løsepengevirus	6	23,1 %
Datainnbrudd	4	15,4 %
Phising	6	23,1 %
Tjenestenekt angrep	1	3,8 %
Vet ikke eller ukjent	2	7,7 %

Spørsmål 24 - Ble det fremsatt økonomiske krav før, under eller etter cyberhendelsen?

Svar	Antall	Prosent
Ja, det ble fremsatt øknimiske krav/utpressing	6	40 %
Nei	7	46,7 %
Vet ikke	2	13,3 %

Spørsmål 25 - Vi valgte å betale trusselaktørene ifm. cyberhendelsen?

Svar	Antall	Prosent
Ja, vi betalte helt eller delvis av trusselaktørens øknomisk krav	0	0 %
Nei, vi betalte ikke	6	100 %

Kommentar eller tilbakemelding til oss:

Her ønsker vi dine tilbakemeldinger, innspill eller kommentar på denne spørreundersøkelsen:

Dette er bra

- Vi er en del av interkommunalt IKT. Dette innebærer at jeg ikke har god nok oversikt over hvor godt de jobber med dette temaet
- Vår kjernevirksomhet er risikostyring, og vi har betydelige ressurser for egensikring i tillegg til rådgivning til kunder. Derfor er modenheten også høy.
- Kommentar til spørsmålsett ovenfor. Besvarelse er gitt fra «vi» som en del av den enkelte del av virksomheten og ikke helheten som et konsern. «Vi» er også for virksomheten og ikke den kompetansen «jeg» besitter.
- Tips til spørsmål kan være noe målrettet, men her var spørsmål rettet mot egen virksomhet, men for bedrifter som leverer cybersikkerhet for sluttkunder, kan muligens svar være annerledes.
- Gjenstår prosesser mht oppfølging av alle leverandører.
- Tommel opp
- Alt kan bli bedre og det er en reise hvor målet flyttes. Fokuset er derfor å ha prosesser for kontinuerlig forbedring
- Revisjon er under arbeid
- Kommentar til spørsmålsett ovenfor. Besvarelse er gitt fra «vi» som en del av den enkelte del av virksomheten og ikke helheten som et konsern. «Vi» er også for virksomheten og ikke den kompetansen «jeg» besitter.
- Spørsmål er rettet direkte mot virksomhet, ikke mot eventuelle deltakelser for sluttkunder som er rammet av cyber-hendelser.
- vi tok aldri kontakt med de som krypterte filene våre
- Vi har hatt mindre hendelser, men ikke som har gitt negative konsekvenser for selskapet, kunder eller andre interessenter. Ressursbruk for å håndtere og følge opp selve hendelsen er ikke medregnet her selv om det er å anse som negativ konsekvens
- Gode rutiner knyttet til backup og tilgang styring

Vedlegg 5 – Informasjonsskriv til fagekspertene ifm. intervju

Hei .....,

Even Andre Solbakken og Anurag Shukla skriver masteroppgaven med følgende problemstilling

«Hvordan kan resiliens styrke cyber-beredskapen i virksomheter»? Og i den sammenheng har vi behov for å gjennomføre intervju med fagekspert og første navnet vi tenkte på i denne sammenhengen var ditt.

Vi har gjennomført spørreundersøkelse og har empiriskdata som vi vil legge til grunn for intervjuet med deg. Vi regner med at intervjuet tar inntil en time og lurer på du har tid og anledning til å gjennomføre dette.

Når det gjelder sted, ønsker vi å gjøre det fysisk og i den sammenheng er vi fleksible. Hvis det ikke er mulig å gjennomføre det fysisk kan evnt. gjøre det gjennom Teams tilsvarende løsninger. Vi ønsker å gjennomføre intervju i tidsrommet uke 34 og 35.

Mvh
Anurag og Even

Vedlegg 6 – Intervjuguide

Intervju av:

Stilling:

Dato: dd.mm.åååå
Tid: fra tt:mm til tt:mm
Sted: Teams møte eller fysiskmøte
Lydopptak: Ja / Nei
Samtykke: Ja / Nei

Spørsmål til intervjuet

Innledning og start av intervju:

Informant ønskes velkommen til intervjuet og intervjuer orienterer kort om hvordan masteroppgaven gjennomføres i regi av pågående studium på Universitetet i Stavanger, samt hensikten med intervjuet.

Del 1

- Hvem er informanten?
- Stilling eller rolle
- Erfaring?
    - Hvor mange års arbeid har du?
    - Hvor lenge har du arbeidet i dagens stilling
- Kunnskap?
- Utdanning?
- Andre relevante bakgrunn informasjon om informanten

Del 2

Informer om at intervjuet deles opp i følgende tema:

A: Risiko
B: Cyber-beredskap
C: Resiliens

Hovedspørsmål (A):

1. Kan du beskrive begrepet «risiko» med egne ord?
2. Hva er etter ditt syn det viktigste suksesskriterier for å

gjennomføre en god risikoanalyse knyttet til Cybersikkerhet?

5. Beskriv hvordan dere gjennomførte ROS-analysen(e)?
6. Beskriv hvordan dere velger ut hvem som skal delta i ROS-analysen(e)?
7. Hvilke utfordringer støter dere ofte på i den praktiske

   gjennomføringen av risiko- og sårbarhetsanalyser?

8. Hvordan videreformidles informasjon om de utførte

   Risiko- og sårbarhetsanalysene til de øvrige ansatte (faste fora etc.)?

9. Har du noen oppfatninger om det er behov for å endre måten denne informasjonen videreformidles på?
10. Hvordan mener du at din utdanning og arbeidserfaring påvirker gjennomføringen av risiko- sårbarhetsanalyser?

    2. Beskriv hvordan risiko blir presentert for beslutningstakere?

12. Har du noen oppfatninger om det er behov for å endre måten risiko presenteres?
13. Beskriv hvordan dere håndterer risiko i deres selskap?
14. Har du noen oppfatninger om det er behov for å endre måten deres virksomhet håndterer risiko på?
15. Noen tilleggs kommentarer?

    4. Inkluderer behandling av ROS-analysen
    beslutningsprosesser angående planlegging?

Hovedspørsmål (B: Cyber- / IKT-Beredskap):

1. Kan du beskrive begrepet «Cyber-/ IKT-beredskap» med egne ord?
2. Hvordan har du lært det du i dag vet om Cyber- / IKT-beredskap (egne erfaringer, kurs etc.)?
3. Kan du beskrive fremgangsmåte / metodikk for etablering av Cyber- /IKT-beredskap i deres virksomhet?
4. Kan du beskrive hvordan deres virksomhet vedlikeholder Cyber-/ IKT-beredskapen?
5. Kan du beskrive hvordan deres virksomhet hensyntar Cyber-/ IKT-relatert risiko i beredskapsplanlegging?
6. Kan du beskrive hvordan deres virksomhet får dimensjonert Cyber-/ IKT-beredskapen til det deres virksomhet har behov for?
7. Har du noen oppfatninger om det er behov for å endre måten deres virksomhet har etablert Cyber-/ IKT-beredskap på?
8. Noen tilleggs kommentarer?

Hovedspørsmål (C: Resilience):

1. Har du beskrive med dine egne ord hva deres virksomhet har utført for å få en Cyber-/ IKT beredskap» i deres virksomhet er resilient?
2. Kan du beskrive med egne ord hvordan deres virksomhet vil responderer etter at deres virksomhet har blitt utsatt for en Cyber / IKT-relatert hendelse?
3. Når deres virksomhet har blitt utsatt for en cyber / IKT-hendels -kan du beskrive hvordan
4. Når deres virksomhet har blitt utsatt for en cyber / IKT-hendels -kan du beskrive hvordan deres virksomhet vurderer potensialet av cyber-hendelsen?
5. Kan du beskrive med egne ord hvordan deres virksomhet hvordan organisasjonen / øvrige interessenter deltar i for å kunne håndtere cyber hendelsen etter at deres virksomhet har blitt rammet?
6. Kan du beskrive med egne ord hvordan deres virksomhet benytter erfaringer knyttet til cyber hendelser til læring i egen organisasjon?

Andre spørsmål

Vår erfaring med denne masteroppgaven har blandet, vi har innledende fått positivie tilbakemeldinger før spørreundersøkelsen ble sendt. Resultatet har vært noe lavt (26 besvarelser) som er i kontrakt med det som ble kommunisert på sikkerhetskonferansen 2022, hvor alle sa at det var viktig å dele informasjon.

- Hvilke erfaringer har du med åpenhet knyttet til cyber-hendelser?
- Hvilke erfaringer har du med deling av kunnskap om cyber-hendelser?
    - Kan du si noe om hvorfor det er «viktig»/«helt avgjørende» / osv?

Kan du beskrive kjennetegner at cyber-beredskap i virksomheter er resilient?

Kan du beskrive hvordan virksomheter kan styrke sin cyber-beredskap?

Kan du beskrive hvordan norske virksomheter deler erfaring knyttet til cyber-hendelse?

Kan du beskrive cyber kompetanse i norske virksomheter?

Kan du beskrive beredskap kompetanse i norske virksomheter?

Kan du beskrive hvordan resiliens kan styrke cyber-beredskap i norsk virksomheter?

- Hvorfor?
- Hva skal til?
- Hvordan mener du at vi bør gå frem?

Vedlegg 7 – Intervju med Gøran Tømte

Intervju med: Gøran Tømte

Stilling: «Field Security Responsible and Zero Trust soldier» i Rubrik (et av ledende selskapene i verden innen sikkerhetskopiering)

Erfaring: mer enn 26 års arbeidserfaring IT bransjen og mer enn 10 års erfaring med cybersikkerhet i ulike roller og funksjoner. Har deltatt i håndtering av en rekke cyberhendelser nasjonalt og internasjonal. Innført begrepet «VG testen» som enkelt og effektiv kan teste cybersikkerheten i virksomheter.

- Dato: 24.08.2022
- Tid: 1300 – 1500
- Sted: Lillestrøm, Kjeller
- Lydopptak: Ja

Spørsmål til intervjuet

Innledning og start av intervju:

Anurag og Even ønsker Gøran velkommen til intervjuet og orienterer kort om forsknings-prosjektet som gjennomføres i regi av pågående studium ved Universitetet i Stavanger, samt om hensikten med intervjuet.

Etter å ha informert om overnevnte, fortalte studentene kort om hvordan en hadde innhentet forskningsdata, samt om at en har lagt til grunn den systematiske og den systemiske risikostyringstenkning når en utarbeidet spørreskjemaene.

I tillegg informerer studentene intervjuobjektet om at han må føle seg fri, samt at han kan endre på spørsmålene dersom han har behov for dette, eller ikke ønsker å svare.

- Det blir avtalt at det tas lydopptak av intervjuet.

Utdrag fra intervjuet:

> *På sikkerhetskonferansen og ISF konferansen på Lillehammer står Østre Totens kommunedirektør på scenen og sier at «du må risikovurdere det uventede». Et*

annet eksempel er at politidirektør i Finnmark står på scenen ifm. flyktningstrømmen fra Syria som kommer fra Russland og inn til Norge. «Dette betyr at man er nødt til å tenke på det usannsynlige [...]» Begge har opplevd det utenkelige.

Lange og unike passord:

Fagekspert: «Lange passord er god anbefaling, det er vi alle enig i. Hvis man går ut på gata og spør 1000 personer om hvor lange passord de har, så er min hypotese er at vi kan telle på en eller to hender hvor mange som har lange passord.

En annen god anbefaling er å ha unike passord pr. tjeneste, alle er enig i at det også er god ting. Dersom man gjør samme øvelsen og spør 1000 personer, er jeg redd for at antall personer med unikt passord kan telles på en hånd. Vi kan også spørre om hvor mange som benytter passordgenerator og resultatet blir mest sannsynlig enda dårligere. Dette er et Paradox, - er gode råd gode, hvis ingen følger dem.»

Vi stiller oppfølgingsspørsmål; "hvorfor tror du at rådene ikke blir fulgt opp?»

Fagekspert: «Man kan følge et av rådene, ved å ha lange passord f.eks. et langt passord kan være «lisa gikk til skolen fra Biri». Om man skal ha unike lange passord pr. tjeneste blir dette veldig komplisert. Det blir umulig å holde oversikt. Dette krever at man begynner å notere ned passordene med penn og papir eller i et passord- system. Det er svært få som gjør dette, og det stopper opp. Og da er min utfordring at gode råd er ikke gode når ingen etterlever dem? I sum blir gode råd, ikke gode. I utgangspunktet er det et godt råd, men det blir så komplisert at ingen klarer å etterleve det!

Mitt råd at man skiller på privat - eller forbruker-sikkerhet og virksomhetssikkerhet. Når det gjelder private anliggender ligger ansvaret helt opplagt på deg som privatperson, mens i en virksomhet har man administratorer med sikkerhetsansvar som kan legge på krav om to faktor i forbindelse med tilgangskontroll til systemer og applikasjoner. Brukerne er fortsatt anbefalt å ha gode passordrutiner, men verifiseringen er sikret av administratoren.

Man må endre på tankesett fra å ha to-faktor autentisering på en bruker, til å tenke at man skal ha to-faktor kontroll på applikasjoner og tjenester. Og jeg vil oppsummere med at gode råd ikke er gode når det blir altfor vanskelig å følge dem».

Cyber-angrep

[...] et angrep er ikke en ting, det består av mange steg. Når det sies at phishing tok ned Østre Toten kommunens IT-systemer, er vel dette noe upresist. Ting som kan være bidragsytere til hendelsen er: manglende to-faktor autentisering, manglende sikkerhetsoppdatering, manglende segmentering av infrastruktur, manglende logging, manglende alarmering, manglende menneskelig interaksjon, manglende utgående kontroll på datatrafikken og mer. Dvs. den listen som de kriminelle måtte gjennom for å gjøre suksess, inneholder 10 – 15 momenter som Østre Toten ikke hadde forberedt seg godt nok på. Å skylde på at brukernavn og passord er en risiko når man mangler to-faktor. Da blir det forenklet å skylde på phishing. [...] Det er viktig å bygge god sikkerhetskultur ved å få de ansatte med på laget, men ikke gi dem ansvaret, om det skulle skje en hendelse. Dette er sammensatt!

Hva er Zero Trust?

Fagekspert: Zero Trust har vært viktig for meg de siste 10 årene, nå jobber jeg i en virksomhet som er kjent for sikkerhetskopiering og gjenopprettelse. Kort oppsummert handler det om å gjøre smarte ting, som er relatert til beredskap,

krisehåndtering, og rask gjenoppretting etter en hendelse~~,~~ slik at virksomhetene blir proaktive og for å gjøre ting mer robuste. Proaktivt og forhindrer at hendelser skal oppstå og utvikle seg til å bli vellykket for de kriminelle. Det er en lang rekke oppgaver som må til for at et cyber-angrep skal bli vellykket, og dette er komplisert og sammensatt. F.eks. er det fryktelig vanskelig å stoppe starten av en slik hendelse. det kan være fra sosiale medier og det kan være e-post. Men det å stoppe prosessen, slik at aktiviteten ikke blir vellykket er kanskje den viktigste del som tankesettet til Zero trust.

Vi stiller oppfølgingsspørsmålet; «hva kjennetegner Zero Trust?»

Fagekspert: La oss ta det fra av et datanettverks ståsted. Begrepet brannmur ble introdusert ca i 1989. Ser man på hvordan brannmur blir presentert i dag, kan vi se at brannmur har en utside hvor alle de slemme er representert, men på innsiden er alle viktige digitale verdier som server og tjenester. Om man spør fagpersonene om hva man bruker brannmuren til, vil de ofte svare at man sperrer og hindrer de kriminelle i å komme inn på servere og tjenester. Dette er feil, primæroppgaven til enhver brannmur er å tillate datatrafikk. Så kommer jeg til det tilfellet der vi mennesker tillater mer enn det som er nødvendig. Dette har en bakgrunn i at vi stoler på ting, vi tar det menneskelige aspektet inn i den digitale verdenen. Dette fordi vi kjenner til denne serveren, og den neste serveren er også kjent, osv. Dette fordi vi stoler på alt, fordi det er våre servere, det er våre nettverk, det er våre kabler, og det er vi som gjør oppgradering av servere og programvare m.m. Vi tror ikke at noen eksterne kan komme inn i disse systemene, og dette er «Trust».

Zero Trust perspektiv er at man <u>ikke</u> skal ha Trust. Trust er farlig, og Trust gjør deg utrolig sårbar. Man må ha et tankesett om å ha Zero Trust, det vil si at du man må anta at noen er inne i systemet ditt, og verden og trusselbildet har blitt veldig mye mere komplisert siden introduksjon av brannmur i 1989. Det er flere angrepsflåter, man får flere inngangsporter, og man får flere sårbarheter. I tillegg har programvare sårbarheter, manglende to-faktor autentisering, man

får dårlig to-faktor autentisering som betyr at kriminelle klarer å komme seg på innsiden. Og da er det viktig og tenkte Zero Trust fordi man ikke vet hvem som står bak denne datapakken som kommer der, det er binært, det er en datapakke som består av ENere og NULLere. Det står ikke «Anurag» på denne pakken, og om det står «Anurag» på denne datapakken er man ikke sikker på om det er «Anurag» som står bak denne datapakke likevel. Da må vi faktisk verifisere at det er «Anurag» som står bak denne datapakken, og ved å sende en verifikasjon eller verifisere det, ved å sende en forespørsel til «Anurag» for å spørre om denne datapakken tilhører deg. Da har vi verifisert at det er «Anurag» som har sendt datapakken. For å oppsummere dette, om det er PCen til «Anurag» som gjør en ting er det ikke sikkert det er «Anurag» som faktisk gjør det.

Vi stiller oppfølgingsspørsmål «hvilke type kontroller finnes det i Zero Trust og hva er vanlig brukt?»

Fageksperten: I 2010 publiserte John Kindervag sine analyser knyttet til en rekke cyberhendelser og hvordan disse kunne motvirkes. Begrepet Zero Trust ble videreutviklet til å bli brukt til å beskrive ulike cybersikkerhetsløsninger som flyttet sikkerhet bort fra underforstått tillit basert på nettverksplassering, og i stedet fokuserte på å evaluere tillit per transaksjon. Mange virksomheter har også gjennomgått denne utviklingen fra perimeterbasert sikkerhet til en sikkerhetsstrategi basert på Zero Trust prinsipper. [...] John Kindervag introduserte begrepet «Six serving men» i Zero Trust tilnærmingen som går på at man må ha kontroll på:

- *Hvem skal ha tilgang?*
- *Hva skal man ha tilgang til?*
- *Hvor skal man ha tilgang fra?*
- *Når trenger man tilgang?*
- *Hvordan skal det kommuniseres?*
- *Hvorfor trengs denne tilgangen?*

Hvis man tar med disse seks kontrollene ifm. tilgangsstyring, vil man har god kontroll og sikkerhet.

VG-testen

Det meste innen cybersikkerhet handler om «principle of least privilege», altså tilgangskontroll, ved å begrense hva du skal ha tilgang til for å kunne gjøre jobben din. Alt som du får utover dette vil øke angreps flaten og dermed øke risiko. Så er det en balansegang mellom hvor paranoid man skal være, og stramme det ned til 100 % kan nok være vanskelig og en utopi. Hvis man tar utgangspunkt i at IT-systemene er kompromittert eller at kriminelle er på innsiden av serveren din. Hva er det kriminelle ofte trenger teknisk? å ha muligheten for å kommunisere til «Command and Control», altså muligheten for å kommunisere tilbake til sine tjenester («call home» og «call back»). Derfor introduserte jeg et konsept med navnet VG-testen.

La meg vise til et eksempel, en tilfeldig virksomhet har ikke eget datasenter lenger, men tjenester er flyttet til skyen og alle servere til virksomhet er i Microsoft Azure datasenter (Microsoft skyen). Så, hva er forskjellen med eget datasenter og med datasenteret til Microsoft, egentlig ingenting. Bare at man ikke kjører servere på eget datasenter og infrastruktur, med switcher, rutere og brannmurer, men kjører det på Microsoft sitt datasenter istedenfor. Men serveren er fortsatt din, Windows installasjon og applikasjonen er fortsatt din, ditt ansvar med å passe på at sikkerhets-oppdatering blir gjennomført og kommunikasjonen går over internett er som tidligere.

Da kommer VG-testen som betyr at man skal gå på sine kritiske servere og se om man kan surfe på www.vg.no. Og hvis du får lov til å surfe på VG fra serveren din, så er det etterdønning og perimeter tankesett. Hvor formålet er å holde kriminelle på utsiden mens på innsiden av brannmuren er det kun bare snille folk og da trenger vi ikke tilgangskontroll på utgående trafikk. Hvis du får surfet

på VG betyr det mest sannsynlig at utgående tilgangskontroll er liberal og da antas det at alt er tillatt utgående trafikk. Når kriminelle kommer inn, vil de ha tilgang til kritiske servere og dermed kan de etablere utgående kommunikasjon til sin «Command and Control» systemene fordi det ikke er i tankesettet ditt. Så, med Zero Trust tilnærming skal du anta at du er blitt kompromittert, og så må en etablere tilgangskontroll på innsiden. Man må ta kontroll på hva servere og tjenester trenger av kommunikasjon mot internett, og bare tillate det som er strengt nødvendig for at systemer skal fungere [...]

Min påstand er at om du kan surfe på VG fra dine servere, så er det sannsynlig at cybersikkerheten er generelt veldig dårlig. Og hvis man kan gjøre dette, er det stor sannsynlighet for at kriminelle også kan gjøre uønskede handlinger.

Åpenhets kultur og dilemma med løsepenger

Vi spør: Hvilken erfaring har du til åpenhet knyttet til cyber-hendelser?

Fagekspert: Ekstremt varierende, prosentvis er det lavt. Politiet og NSM kan ikke si noe om cyber-hendelser som de jobber med, dette forstår jeg. Det er mange grunner til at man ikke snakker om cyber-hendelser. [...]

La oss se på et eksempel, Østre Toten kommune oppdaget 29. januar 2021 at de ble utsatt for ransomware. Det som er interessant er at det var to andre tilfeller som skjedde samtidig i Norge, og kanskje flere som ikke er kjent. Den ene var Aqua group på Nord-Vestlandet, en privat aktør, som er en leverandører til oppdrett sektoren. Østre Toten kommune er en offentlig aktør som av moralske og etiske grunner ikke ville betale løsepenger. Den største forskjellen mellom disse virksomhetene er at Østre Toten kommune ikke går konkurs, så kommunen kan si nei til ransomware og de kan bruke et år på å gjenopprette IT-systemene. Mens for Aqua group er dette annerledes. En artikkel om Aqua group hendelsen ble publisert og etter dette har vi ikke hørt noe om Aqua group. Regnskapstallene fra første kvartal 2021 viser at de har registrert et tap på 50 millioner kroner. Så kan en spekulere i hvor mye av disse pengene har gått til å betale løsepenger

og hvor mye av dette som gått til å gjenopprette IT- systemene. Hvis de har betalt løsepenger kan det være vanskelig å snakke om dette offentlig. Så åpenhet er veldig sammensatt av forskjellige grunner, noen avstår fra å være åpne fordi det er tidskrevende. Se hvor mange timer som er medgått for at Østre Toten kommune har stått på ulike scener og eventer, hvor både ordføreren og kommunedirektøren har vært delende, men de har samtidig høstet mye skryt for å dele sine erfaringer.

Se på et annet eksempel, Nordland fylkeskommune som ble forsøkt utsatt for et cyber-angrep i desember 2021, som også ble publisert artikkel i bransje tidsskriftene digi.no. Denne hendelsen kom ikke så langt at det ble vellykket cyber-hendelse med alvorlig konsekvenser, med bakgrunn i at hendelsen ble oppdaget i kjeden. [...] Jeg fikk fylkesordføreren i Nordland Fylkeskommune til å stille opp i vår konferanse tidligere i år for å snakke om denne hendelsen, og som ikke ble vellykket, og som ble stoppet. [...]

Jeg tror det er viktig å dele erfaring og kunnskap om forsøkt på cyber-angrep som blir stoppet, og ikke bare dele etter at det har skjedd en katastrofe. Vi bør ha diskusjon på hva som er et angrep, og når skal vi dele, her bør vi kunne dele mere informasjon og kunnskap om når et angrep blir stoppet suksessfullt. Hvilke tiltak ble implementert eller hva ble gjort for å stoppe et suksessfullt cyber-angrep. Uten erfaringsdeling blir det kun underholdning og liten grad kunnskapsdeling som videre utvikler oss. [...]

Så for å oppsummere dette, det er generelt dårlig med deling av informasjon, men jeg tror vi også kunne ha delt andre ting i tillegg.

Vi stiller oppfølgingsspørsmål «at det bør være fokus på den positive biten og knytte dette til læring om hvordan man har stoppet et cyber-angrep eller alvorlig cyber-hendelse»

Fagekspert: Nordland Fylkeskommune og Nordic Choice hotellene ble mest sannsynlig rammet av samme cyber-angrep, den ene av disse fikk stor oppmerksomhet i media, mens den andre ble lite omtalt i media fordi de hadde god kontroll på ende punkt sikkerhet i sine IT-systemer.

Taktskifte med høy grad av kompleksitet:

Kriminelle kan være inne i systemene til virksomhetene, og det kan skje via Software as a Service (SaaS), og som noen omtaler som skyen. [...] Jeg kaller SaaS for et kjempestort spøkelse og bare venter på apokalypse. Jeg venter bare på at SaaS skal eksploderer i negativ omtale. SaaS er «convenient», alle skal til «skyen» og er dert strategisk smart i kombinasjon med vi skal legge ned interne datasenter?

Dersom vi ser nærmere på datasenteret til en virksomhet:

- *Hvilke nettverksutstyr har man? Kanskje man har nettverksutstyr fra Cisco.*
- *Hvilke server har man? Kanskje man har servere fra Dell.*
- *Hvilken brannmur har man? Kanskje man brannmur fra Palo Alto Networks.*
- *Hvilke operativsystem benyttes på servere? Kanskje en blanding av Linux og Windows servere.*

Hvor mange variabler har man i dette eksemplet? Fem, og kanskje har man noen flere variabler, og dette er håndterbart. Alle disse variabler bør man ha kompetanse på, og sende personell på kurs, og man må gjøre revisjon av dette osv. Med andre ord, man har to håndfuller av variabler som man må håndtere. Når man går til SaaS så har man slike variabler for alle SaaS leverandørene, og det er stor sannsynlighet for at disse er forskjellige, da det ikke finnes noen standard som ivaretar kvalitet, sikkerhet og policyer. Om man spør virksomheter på hvor mange SaaS applikasjoner som de benyttes, får jeg ofte tilbakemelding på mellom 50 og 100 applikasjoner. Dermed får man økt risiko ved at man har multiple systemer uten kompetanse eller risikoforståelse for hver enkelt løsning.

Vedlegg 8 – Intervju med Roar Thon

Intervju av: Roar Thon

Stilling: Fagdirektør sikkerhetskultur i NSM

Erfaring: Vært ansatt i NSM siden 2003 og har tjenestebakgrunn fra Forsvaret og politiet. I dag arbeider med hvordan mennesker bruker teknologi og hvordan dette påvirker sikkerhet i samfunnet, hos virksomheter og for enkeltmennesker. Roar er en prisbelønnet foredragsholder med over 1400 foredrag om sikkerhet i NSMs tjeneste, og sannsynligvis en av landets mest etterspurte foredragsholdere. I sikkerhetsmåneden oktober 2022 skal Roar gjennomføre mere 40 foredrag. For sin innsats har Roar mottatt pris for sitt engasjement i 2012 (ITAKT 2012) og årets fremragende sikkerhetsrådgiver (OSPA 2018)

- Dato: 30.08.2022
- Tid: 1400 - 1530
- Sted: Lillestrøm, Kjeller og Microsoft Teams
- Lydopptak: Ja

Spørsmål til intervjuet

Innledning og start av intervju:

Anurag og Even ønsker Roar velkommen til intervjuet og orienterer kort om forsknings-prosjektet som gjennomføres i regi av pågående studium på Universitetet i Stavanger, samt hensikten med intervjuet.

Etter å ha informert om ovennevnte fortale studentene kort om hvordan en hadde innhentet forskningsdata, samt at en har lagt til grunn den systematiske og den systemiske risikostyrings tenkning når en utarbeidet spørreskjemaene.

I tillegg informerer studentene intervjuer om at han må føle seg fri, samt at han kan endre på spørsmålene dersom han har behov for dette, eller ikke ønsker å svare.

Under intervjuet leser studentene opp spørsmålene til Roar.

Begrepsbruk

Begrepet «Resiliens», hva legger vi i det? For meg betyr resiliens motstandsdyktighet og hva er da vi snakker om i beredskaps sammenheng? Er det vår evne over tid til å håndtere hendelser, eller er vi fortsatt før hendelsen, slik at vi kan forhindre at noe skjer. [...]

Jeg syns det er særpreg i denne bransjen som fortsatt er ganske ung, og det må vi erkjenne. Det er en fortsatt umoden bransje som strør om seg med rare begreper og ord som en selv ikke forstår, eller hva det innebærer. Jeg har en tittel som jeg tøyser litt med, fagdirektør sikkerhetskultur i NSM, men jeg går samtidig og sier at vi i realiteten ikke skal ha sikkerhetskultur. Vi skal ha en virksomhetskultur som inkluderer sikkerhet. For sikkerhet i seg selv skal ikke leve sidelinjen, eller utenfor alle andre prosesser. Ideelt sett, er dette en helt normal del av å drive en virksomhet. Den delen blir viktigere og viktigere for oss uansett hvilken bransje eller sektor vi er i. Og denne forståelsen har vi ikke på plass enda.

Jeg sier at bransjen vår er umoden, men det handler ikke bare om bransjen. Det handler selvsagt om alle som er involvert i dette. Det er til syvende og sist alle virksomhetsledere og alle ansatte som er del av dette, og som innbyggere er vi også den del av dette. Vi forstår ikke teknologien, selv om vi bruker den og implementerer den, og samtidig så mener jeg ikke at alle skal ha doktorgrad fra NTNU i å forstå teknologi. Men vi blir likevel overrasket over at det er teknologisk mulig. At noen andre har gjort noe med teknologien som du kan gjøre, men nå ble det brukt til å gjøre noe negativt. Dette blir vi fortsatt overrasket over i virksomhetsperspektiv og som individ.

Vi lever fortsatt i en analog tilnærming, jeg møter fortsatt virksomhetsledere som snakker om cybersikkerhet som om det er noe virksomheten deres er for liten til. Det er ikke av interesse fordi de holder til på Vestlandet og bare driver med laks. De virksomhetene har ikke tatt innover seg at de har digital tilstedeværelse og alle er digitale mål. For mange av virksomhetene rammes av tilfeldigheter, det er ikke nødvendigvis at noen bestemte seg for å angripe Nortura. Det var mulig

å angripe Nortura, ergo går man løs med alt man har for å nå målene som man har satt seg. De som står bak dette har ikke peil på om de har endt opp i Harstad, Tromsø, Trondheim eller Drammen. Om bedriften er med 500 eller 50 ansatte og de bryr seg heller ikke fordi det har dukket opp en teknologisk mulighet som gjør at de kommer inn og kan gjøre det de ønsker å gjøre.

Så er det selvsagt en annen side av det hvor det faktisk handler om hvem du er, hva du driver med og hvilken virksomhet du er og hvilke verdier du operer med. Hvor ting er målrettet. Men vi har en sterk tendens til å, kanskje litt basert på amerikanske filmer og tv-serier å tenke på alt er målrettet, så devaluerer vi egen betydning og blir like overrasket når det skjer ting likevel. Selvsagt er det forskjell om du heter Kongsberg Air Defence og holder til på Kongsberg innen forsvarsektoren eller om du heter Floriner blomster og selger blomster. Det er vesentlig forskjell mellom disse virksomheter, men begge har behov for digital sikkerhet. Erfaringen vår er at ikke alle har forstått dette enda, og da snakker vi ikke om så små virksomheter som Floriner blomster engang. Vi snakker forholdsvis om store virksomheter, i hvert fall i norsk perspektiv.

Sikkerhetstrussel

Jeg jobber med en kronikk som skal publiseres og bakgrunn for kronikken er at jeg blir ganske provosert av at sikkerhetskonsulent selskapene snakker om at de ansatte og ledelsen er virksomhetens aller største sikkerhetstrussel. Det de røper med dette er at de ikke vet forskjeller på hva en risiko og trussel er. Trussel er noe som er uttrykt konkret, det vil si at du har en ansatt som går på jobben den dagen, men en tanke om å faktisk formatere harddiskene på jobben. I min verden sørger man for at den ansatte ikke får komme på jobben, hvis man vet at denne personen er en trussel.

Det man mener med dette er jo selvsagt, som mennesker, som ledere og ansatte så utgjør vi en sikkerhetsrisiko fordi vi er mennesker med sårbarheter. Det at ledelsen ikke forstår det digitale trussel og risikobilde. Det er ikke en trussel, men det er en risiko som faktisk gjør det lettere å gjøre det trusselaktørene

ønsker. At man ikke greier å se forskjellen mellom risiko og trussel er frustrerende. Å gå i dialog med fagforeningene og si at samtidig her er en trussel vil ikke fungere. Dette er ikke overførbart til virkeligheten, da skjønner man ikke det man i realiteten må gjøre hvis det er definisjon og utgangspunkt. For trusler må man håndtere på en helt annen måte.

Cyberhendelser

Hvilken erfaring har du fra cyberhendelser i Norge og hvilken rolle har du hatt?

Jeg har erfaring fra flere cyberhendelser, hvor i noen av hendelsene har blitt håndtert fra et kommunikasjons perspektiv, hvor jeg har hatt ansvaret for å forklare på hva som har skjedd på en folkelig måte. Samt bidratt til beslutningsgrunnlaget på hva bør vi si nå, hva kan vi si og hva bør vi fokusere på nå.

Bakenfor noen av utfordringene dere har opplevd med spørreundersøkelsen, hvor åpne er man egentlig? Hvor mye er man villig til å dele. Mange av cyberhendelsene starter med at disse blir detektet av min organisasjon som da sender henvendelse videre og så ruller ballen derfra. Det som er viktig i norsk perspektiv, og som har gjort at dette og mye mer fungerer så bra som det gjør; Det er at prinsippene fra NSM vedrørende hendelseshåndtering og alt fra sensor nettverket (VDI – varsling av digital infrastruktur) er basert på at virksomheten som selv eier hendelsen. Det er virksomheten selv som får lov til å bestemme om de ønsker å gå ut offentlig med full pakke med riksdekkende media eller hvordan de ønsker å håndtere dette. Sånn at de ikke risikerer at myndighetene kaller inn til en pressekonferanse og henger ut virksomheten. Og det er ganske viktig prinsipp for oss i hendelseshåndtering at virksomheten selv får lov til å ta de beslutningene på hvor langt de vil gå. Samtidig kan dette føre til en del frustrasjon, plutselig står du ovenfor en virksomhet med utenlandsk eier som i prinsipp ikke ønsker å uttale seg om sikkerhetsmessige spørsmål.

Alle vet at hendelsene eksisterer, media har forstått at hendelsen eksisterer, men det kommer ingenting. NSM har heller ikke anledning til å dele informasjon, men blir enig med virksomheten om å dele teknisk informasjon om skadevare (altså teknisk skadevare analyse) om det er noe andre bør se etter og utover det så stopper det. På den andre siden har den virksomheter som er helt åpne, f.eks. Østre Toten kommune. Hvor jeg har berømt de ved flere anledninger på hvordan Østre Toten har stilt opp i enhver tenkelig anledning om ganske ubehagelig ting å snakkes om. Opplæringseffekten av det, bl.a. i kommune Norge har vært enorm og oppvåkning på hva som faktisk kan ramme en virksomhet og en kommune. Det er forståelig at på et eller annet tidspunkt begynner noen av disse personen å bli ganske lei også, f.eks. å besvare på spørreundersøkelse fra dere, eller alltid stå på senen å snakke om disse tingene. Østre Toten kommune har vært åpne om at de har tatt noen feil valg og prioriteringer før hendelsen inntraff og som flere av kommunene med stor sannsynlig også har gjort. Men det var de som ble rammet av cyberhendelsen. Østre Toten kommune har stått ved sitt budskap om at de ikke var godt nok forberedt og at det var konsekvensene. De fortjener kudos for at de har valgt å stå i det på denne måten. Og så tror jeg at de kommer betydelig bedre ut av dette, nettopp fordi de har valgt en åpen kommunikasjons strategi. For vi har virksomheter til tross av at de er rammet av hendelser som er synlig ovenfor kunder og det offentlige. Det blir litt flaut når man sier at man holder på planlagt vedlikehold på den sjette dagen og ingen ting av leveransene fungerer. Og på den syvende dagen kall inn til pressekonferanse og erkjenne det folk viste om to timer etter at hendelsen inntraff – at virksomheten er kryptert eller utsatt for et eller annet. NSM er i stadig dialog med kommunikasjonsavdelinger og ledere i veldig mange virksomheter for å snakke om den siden av beredskapsarbeidet. Og tenke over den omdømmemessig delen av dette som går på å bli utsatt for denne type cyberhendelse.

Vi stiller følgingsspørsmål «når man er på det nivå, hva møter du? Har virksomhetene vært forberedt? Har virksomhetene en beredskapsplan for å kunne svare ut informasjon kommunikasjon og har de planer?

Erfaringsmessige er at de aller færrest har planer for dette her, kanskje har virksomhetene en eller annen form for kommunikasjonsplan som omhandler driftsstans, men sjeldent en plan for en forsettlig handling som kompliserer driftsstans.

Vi stiller et nytt oppfølgingsspørsmål «du snakker om omdømmerisiko, er ditt inntrykk av at virksomhetene har omdømmerisiko som er basert på den faktisk risiko som en virksomhet til enhver tid har? Er det noen kobling mellom kommunikasjonsavdeling og den faktisk risikobilde til virksomheten?»

Jeg tror for veldig mange av virksomhetene er dette helt uavhengig og så er det noen som har profesjonalisert dette over tid. [...] La oss se på et eksempel fra 2013, hvor ledelsen i Telenor sto fram og fortalte og var utsatt for en kompromittering, hvor de hadde mistet som de selv kalte bedriftssensitivt informasjon på høyt nivå fra Telenors ledelse. Vi applauderte de da og dette skjedde rett før NSMs sikkerhetskonferansen og de slapp informasjon om hendelsen fra senen. Da satt jeg og observerte Oslobørs for å se om dette hadde noe konsekvens, at toppledelsen i Telenor forteller om at de har mistet sensitiv informasjon på et strategisknivå som de selv sier. Nei, overhodet ikke, Telenors kurs på børsen gikk opp. Det var ikke noe negativt respons fra finansmarkedet. [...]

Vi var i dialog med flere meglerhus og lurte på hvordan markedet reagerte på budskapet fra Telenor, har finansmarkedet forstått konsekvensene av budskapet? Vår forståelse av situasjonen var at finansmarkedet hadde ikke tenkt så veldig mye på det. Vi konkluderte med at, hvis Telenor hadde vært et telekomselskap i Amerikansk kontekst ville dette ha medført en særdeles kraftig reaksjon fra markedet på Telenors markedsverdi. Fordi dette er helt annen modenhet på dette området i Amerika.

På den andre siden, er det positiv greie er at man ikke har store omdømmemessige konsekvenser ved å stå fram og fortelle om at virksomheten er blitt rammet av en alvorlig cyber-hendelse. Men da er det faktisk viktig at man gjør det så raskt som mulig og ikke trekker det ut til den syvende dagen, altså så rask som mulig erkjenne at situasjonen er kjempealvorlig for oss og kommuniserer deretter. Norsk Hydro er et klassisk eksempel her, hvor de høstet mange priser for sin kommunikasjon og for måten de hadde stått i det ifm. håndtering av alvorlig hendelse. Det gir kredibilitet i det tekniske miljøet, det gir kredibilitet ovenfor kunder og hele pakka rett og slett. Enn det å forsøke å fornekte eller å tie. Dette er noe vi jobber med å formidle til virksomhetene og vi er bevist på hvordan vi tar dette ut til virksomhetene. Vi er to stykker som har invitert oss selv ut i utvalgte miljøer, hvor vi har hatt spesielt fokus på finansdirektører eller CFOer i virksomheter. Fordi de lever med en risikoforståelse som er mye breiere, de ser på helhetlig risiko for virksomheten med målsetning for at finansdirektører forstår konsekvensene og hva vi snakker om at virksomhetene ikke klarer å produsere noe ting. Og hva om dette varer i 14 dager og hva tenker dere om det? Min erfaring er at ikke alle har tenkt på dette senarioet til tross for at det ikke har vært mangel på historier i media om løsepengevirus. Men da er vi tilbake til at, at denne skjer ikke dem, fordi de holder til på Vestlandet og driver bare med oppdrett laks.

Vi stiller oppfølgingsspørsmål «om man snur på problemet, de gode historiene, at det ikke har vært en cyber-hendelse, at hendelsen ikke fikk muligheten for å utvikle seg til å få alvorlig konsekvenser. Hva tenker du om det?»

Det er underkommunisert til de grader, for det er tusenvis av dem og jeg gjør et poeng av dette i nesten hvert foredrag jeg holder. Det er masse som forbedres, vi sier at hver norske virksomhet har forbedringspotensiale når det gjelder digital sikkerhet, ref. NSM trusselvurdering – Risiko 2022. Men vi må ikke glemme de tusenvis forsøkene som stanses hver dag med potensielle katastrofale konsekvenser for samfunnet, hvor ingenting skjer fordi sikkerhetstiltakene som er implementert er der for å stanse disse forsøkene. Dessverre får ikke disse oppslag i VG eller Dagbladet. Men det som også er et problem med dette er at

dette får heller ikke oppmerksomhet i virksomhetene. Fordi jeg har en opplevelse av at, når jeg blir invitert inn til konsernleder gruppe og det kanskje etter jeg har snakket til en CFO forsamling. Hvor CFOen sier at du kommer til oss og snakker om dette her. Så jeg er ikke invitert fra teknisk side, altså CISO eller teknologiske del av virksomheten, men fra finans delen. Fordi jeg følger i disse situasjonene at nå kommer det noen fra sidelinja og ledere med tekniskansvar blir nervøse og syns det er ekkelt i seg selv. Det som er interessant er, da jeg snakker om risiko og det som kan ramme dem. Så snur konsernsjefen seg til den som er CISO eller teknisk ansvarlig og spør «skjer det oss også»? I det øyeblikket forstår man at det ikke er et tema på det nivå i virksomheten. De har ikke oversikt over hvor mange forsøk bedriften deres stanser daglig, ukentlig og månedlig. Når de stiller spørsmål på denne måten internt. Det er også uttrykt mål for oss å få toppledere til å stille noen av de riktige spørsmålene, vi opplever til tider at disse blir også avspist av fagmenneskene. Nei, vi krypterer ... Jeg hører hva du sier, men er det kryptologi fra «Donald» eller hva slags krypto er det vi snakker om her?

Oppfølgingsspørsmål: tror du det handler om at ledergruppene, CFOene eller andre ledere i disse virksomhetene har oversikt over andre risikoer for virksomheten, har de noe risikobilde?

Ja, det har de, tradisjonelt har de det. Dette er basert på min dialog og erfaring. Det er noe med cyber og IKT delen som foreløpig så umoden og bare noe IKT menneskene skal holde på med. Det er ikke løftet opp på strategisk nivå for å forstå betydningen fult ut av det. Videre mener at vi har kommet så langt at de aller fleste virksomheter, hvert fall av en viss størrelse uavhengig av en hva man holder på med har erkjent at IT er «core buiness», dvs. at virksomheten er helt avhengig av IT i sin daglig drift. Men man har ikke kommet til at sikring av IT er av samme «core buiness». Kostnad for sikkerhet er kostnad for «doing buiness», man er mere opptatt av hvordan teknologien kan effektivisere oss, mere effektive på flere ulike måter. Vi i Norge er veldig flinke til å se positiv sidene av teknologi, men vi er ganske dårlig til å samtidig se at vi introduserer en rekke sårbarheter og som andre kan misbruke.

Det er en evig diskusjon som alltid har vært der, det finnes teknologer som sier at du ikke kan være toppleder i dag om du ikke kan teknologi. Jeg er en av de som er helt uenig i det, det er fint om man har teknologisk bakgrunn, og være toppleder, men det å være toppleder i dag betyr i realiteten om at du omringer deg med en rekke fagmennesker innenfor forskjellige områder. Som toppleder kan du ha jurist bakgrunn eller markedsføring eller økonom, og sette deg inn i en rekke områder. Samtidig har du fagpersoner rundt deg for de sammensatte tingene og cyber er en del av disse tingene som blir viktigere og viktigere opp det nivået. Toppleder må forstå det fra et strategisk perspektiv og ikke «bits and bytes».

Oppfølgingsspørsmål: Når du snakker med toppledere, skjønner de hvilke verdier de har om de skulle bli rammet av cyberhendelse?

Ikke fult og helt, nei. Kanskje den alle største utfordringen forsøker å rette opp ved gjennom bl.a. gjennom den nye sikkerhetsloven som kom i 2019, det er verdikjedene. Det å kunne se sin egen verdi uten for sin virksomhet drift. Stille seg spørsmål på hvem vi er 100% avhengig av for å fungere og hvem er 100% avhengig av oss for å fungere. Slik at man må se undersøke og over seg, samt se dette i en sammenheng.

Informasjonssikkerhet, cybersikkerhet og backup

Jeg begynte å benytte datamaskiner i ca. 1991 og da var det disketter og diskettstasjoner og hele bransjen var opptatt av at man måtte ta backup av sine data og det var ekstremt viktig. Det var et mantra som levde det veldig lenge og så ble det borte. Det forsvant, men samtidig var det noe man gjorde. Men man testet aldri om man kom tilbake til normal drift igjen og dette har blitt veldig blitt aktualisert gjennom bl.a. digital utpressing med løsepenger-virus, jeg ser at dette har snudd ved at flere virksomheter nå tester og sjekker at backup fungerer. Før det var det noe man bare gjorde for det måtte man gjøre og hadde

ikke peiling på om backup fungerte eller ikke, det er mange som har fått erfart gjennom løsepengevirus, at backup ikke har fungert eller backupen har blitt kryptert og ubrukelig. I noen tilfeller hvor virksomheten har hatt backup men ikke klart å komme tilbake til drift.

Hvis vi ser nærmere på begrepet informasjonssikkerhet, så består det av tre ting, 1) konfidensialitet, 2) integritet og 3) tilgjengelig. I vår analoge tilnærming til denne verden på så har vi i Norge i dag fortsatt en ekstrem slagside på at den største bekymringen er konfidensialitets perspektivet. Tap av informasjon som ikke andre skal se, lese og høre. Jeg bruker veldig ofte et eksempel, hvor jeg bruker bilde av meg selv. Jeg er pasient på Ahus med diverse ting i hånda og det er livs kritisk. Og i den sammenheng stiller jeg spørsmål «i et informasjons- eller cybersikkerhets perspektiv, hva er det mest kritisk for meg da?» 1) er det at noen har hacket seg inn på datasystemer og lest min pasientjournal? Altså konfidensialitet perseptiv. 2) at de har hacket seg inn og endret på mine pasientdata? Altså integritet i data. 3) eller noen har tatt over alle sykehuset data systemer og gjort disse utilgjengelig, noe som ville bidratt til å gjøre informasjonen tilgjengelig for helsepersonell som skulle reddet livet mitt denne dagen. Altså tilgjengelighets perspektivet. Jeg vil ha alltid velge tilgjengelighet i denne situasjon 10 av 10 ganger. Jeg hadde gladelig latt flere tusen mennesker lese min pasientjournal i bytte mot at den dagen så funger datasystemene optimalt og bidro til at mitt liv ble reddet. Jeg sier ikke at konfidensialitet ikke er viktig, kunder, pasienter og innbyggere skal stole på at informasjon blir passet på en god måte, det vil gå utover tilliten og den er veldig avhengig av. Men det er ganske viktig å forstå at verden har gått videre fra den analoge tilnærmingen, til å ta det innover seg. Jeg møter fortsatt toppledere i helsesektoren som forstår at det ikke bare handler om pasientjournaler, men også tonnevis med teknologi som er med på å redde menneskeliv hver eneste dag som også er mulig å nå fra hele verden av krefter som ikke nødvendigvis ønsker oss noe vel. Og det har de ikke fult ut tatt innover seg. Tap av tilgjengelighet er den raskeste vei for tap av menneske liv i et modernesamfunn som vårt. La oss se på et eksempel, mediedekning av Helse sørøst og mange av de store sakene, så er det desidert første spørsmålet som blir stilt fra media er «er det informasjon på avveie?».

Det er ganske irrelevant når hele kommunen er mørk. Men det er det første spørsmålet som garantert kommer til å bli stilt. [...]

Det jeg pleier å avslutte mine foredrag med, vi har nå snakket om at vi har verdier, disse verdiene tiltrekker seg trusselaktører og så har vi sårbarheter som er av menneskelig, teknologisk og prosessuell art. Disse sårbarhetene eksponerer verdiene våre og de utnyttes av trusselaktørene. Hva er det vi har snakket om som dere kan få gjort noe med? 1) dere får ikke gjort noe med at verdi har verdi 2) dere får ikke gjort noe med at trusselaktørene eksisterer 3) men dere har gjøre noe med sårbarhetene deres. Det å faktisk sette søkelys på noe man kan gjøre noe med og påvirke selv er et viktig valg. Våre anbefalinger til ledere er 1) hva skal dere være stand til å gjøre selv og hvem andre kan hjelpe deg.

Oppfølgingsspørsmål hva tenker du er de tre viktigste tingene som en liten eller mellomstor virksomhet eller kommune bør fokusere på med tanke på cyberberedskap?

For å gjøre det lett og se det i kommune perspektiv, ville jeg ha anbefalt hyllevare og da snakker vi om teknologi. Bruk ting som andre er i stand til å kjenne igjen og kan. Litt flåsete sagt, gå i skyen, eller finn deg et sted hvor man kan forsvare og få hjelp. Og ikke sitt der med en gammel utdatert DOS system som passer på innbyggere i kommunen. Neste er å kartlegge hva en er i stand til å gjøre selv og hvem andre kan hjelp oss, altså kompetanse og ressurs kartlegging. Slik som Østre Toten har beskrevet det selv, en ting er kompetanse og annen ting er å ha ressursene til å stå i det over lang tid. For ved en alvorlig cyberhendelse er ikke normal tilstanden tilbake i løpet av 48 timer. Ha oversikt over verdiene, jeg tror ikke de fleste virksomhetene har god nok oversikt over sine verdier, hvis alt går ned hva som faktisk må gjøres og hva som er viktigst å gjør med tilhørende rekkefølge. Ta eksempel med Østre Toten kommune som har nevnt det ved flere anledninger, elbil lader foran kommunehuset som fortsatt ikke fungerer og det var kanskje ikke det viktigste prioriteringen for det var andre ting som var viktigere. Det er typisk veldig synlig når det ikke fungerer

lenger, og som man ikke nødvendigvis har på plass når i dokumentasjon eller planverk. [...] Det å ha oversikt over systemer, verdier, avhengigheter av andre er viktig for å lage god planer. Disse planene tåler aldri virkeligheten og man må øve på disse. Det vil alltid være en diskusjon på hvor mye tid man får til å øve og trene, samt hvor realistisk man disse øvelsene blir, men det å gjøre øvelser for å teste ut planverket.

Vedlegg 9 – Dokumentanalyse

Dokument	Fokusområder	Relevans til forskningsprosjektet
DSB (2003) Risikopersepsjon – en innføring i fagfeltet	Rapporten er på 19 sider og handler om risikopersepsjon. Fokus er rettet mot å forstå hva- og hvordan risikopersepsjon påvirker adferden til oss mennesker	DSB rapporten bidro til at vi fikk oppdatert kunnskap om faktorer som påvirker risikopersepsjon. Risikoforståelse, risikoperspektiv og kommunikasjon av risiko er viktig for å få innsikt i faktorer som påvirker adferden i sikkerhetsarbeid
DSB (2016) Befolkningsundersøkelse om risikopersepsjon og beredskap i Norge	Rapporten er på 55 sider og handler om en befolknings-undersøkelse i 2016, hvor risikopersepsjon og beredskap i Norge kartlagt av DSB.	DSB rapporten bidro til vi fikk innsikt i hva folk flest er bekymret for skal inntreffe i Norge i de kommende fem år. 9 % (s.35) av befolkningen var svært bekymret for at det skulle inntreffe et cyberangrep på styringssystemer
Etterretningstjenesten (2020), Fokus 2020	Trusselvurdering – Fokus 2020, 65 sider	Etterretningstjenestens rapport «Fokus» er én av fire offentlige trussel- og risikovurderinger som utgis årlig. De øvrige tre gis ut av Politiets sikkerhetstjeneste (PST), Nasjonal sikkerhets-myndighet (NSM) og Direktoratet for samfunnssikkerhet og beredskap (DSB).
Etterretningstjenesten (2021), Fokus 2021	Trusselvurdering – Fokus 2021, 104 sider	Etterretningstjenestens rapport «Fokus» er én av tre offentlige trussel- og risikovurderinger som utgis i første kvartal hvert år. De øvrige gis ut av Politiets sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet
Etterretningstjenesten (2022), Fokus 2022	Trusselvurdering – Fokus 2022, 38 sider	Etterretningstjenestens rapport «Fokus» er én av tre offentlige trussel- og risikovurderinger som utgis i første kvartal hvert år. De øvrige gis ut av Politiets sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet
Forsvarets forsknings-institutt (2019), Resiliens – hva er det og hvordan kan det integreres i risikostyring?	FFI-rapporten er på 44 sider og vi har fokusert på flere temaer knyttet til resiliens. Mange definisjoner på s.10-11. og s.33	Rapporten bidro til at vi fikk oppdatert kunnskap om resiliens- teori, mangfold av resiliens-definisjoner, samt kunnskap knyttet til bruk av resiliens uten bruk av risikobegrepet.
Forsvarsdepartementet, Justis- og beredskaps-departementet (2018), Støtte og samarbeid. En beskrivelse av totalforsvaret i dag	Rapporten er på 99 sider og vi har fokusert på deres utvikling av totalforsvaret på s. 9-10. Fokus på sivil-militært samarbeid i det norske totalforsvaret på s.15. Videre hvem andre som er en del av det nasjonale beredskaps-systemet s.26-27. Fokus på hvem som har ansvaret for beredskapen s.66-67	Utredningen bidro til å få kunnskap om hvordan det norske totalforsvaret er bygget opp, samt til å forstå hvem som har ansvaret for den norske beredskapen, noe som var viktig for oppgaven
Meld. St. 17 (2001-2002), Samfunnssikkerhet. Veien til et mindre sårbart samfunn.	Stortingsmeldingen er på 151 sider og vi har fokusert på side 100, hvor Justis-departementets samordnings-ansvar for planleggingen av den sivile beredskapen beskrives	Kunnskap om hvem som har samordningsansvaret for departementene for planleggingen av den sivile beredskapen var viktig for oppgaven
Meld. St. 12 (2005-2006)	(Definisjon av beredskap i petroleumssektoren)	Stortingsmelding, kunnskap om beredskap
Meld. St. 10 (2016-2017), Risiko i et trygt samfunn – samfunnssikkerhet	Stortingsmeldingen er på 192 sider og vi har fokusert på flere temaer. På s.7 fremkommer at enkeltmennesker har et ansvar for IKT-sikkerhet. Viktigheten av	Kunnskap om enkeltmenneskers ansvar knyttet til IKT-sikkerhet og forståelse av viktighet knyttet til ulike sentrale begreper og resiliens-definisjon innenfor samfunnsikkerhetsarbeidet er relevant for oppgaven

	felles begrepsforståelse på s.25, samt definisjoner av sentrale begreper på s.26, og definisjon av resiliens på s.31	
Meld. St. 38 (2016-2017), IKT-sikkerhet. Et felles ansvar	Stortingsmeldingen er på 85 sider og vi har satt søkelys på flere sider i denne rapporten. Meldingen er den første meldingen om IKT- sikkerhet (s.11), og beskriver IKT-ansvar på ulike nivåer (s.19)	Kunnskap om hvem som ansvar for IKT-sikkerhet på flere nivåer i samfunnet er relevant for forsknings-prosjektet
Meld. St. 12 (2017-2018)	(Definisjon av beredskap i petroleumssektoren)	Stortingsmelding, kunnskap om beredskap
Meld. St. 5 (2020-2021), Samfunnssikkerhet i en usikker verden	Stortingsmelding	Tema Korona kommisjonsrapport, hvordan beredskap er organisert i Norge
Mnemonic (2021). Cyber Security Report 2021	Rapporten er på 59 sider og vi har benyttet deres kunnskap, på side 28-29, knyttet til hvordan arbeidshverdagen til trusselaktører er gjennom døgnet og i ukedagene	Rapporten bidro til at vi fikk oppdatert kunnskap om hvordan trusselaktørene arbeider gjennom uken
NOU (2018:14), Organisering og regulering av nasjonal IKT-sikkerhet	Utredningen er på 147 sider og vårt fokus var på s 13-14, begrepet IKT-sikkerhet og grenseflater /synonymer knyttet til informasjonssikkerhet, cybersikkerhet og digital sikkerhet	Utredningen bidro til å få kunnskap om hvordan Norges offentlige utredninger har beskrevet IKT-begrepet, samt grenseflater knyttet til begrepet var viktig for oppgaven
NOU (2021:6), Myndighetenes håndtering av koronapandemien — Rapport fra Koronakommisjonen	Rapportener på 452 sider og vårt fokus var på s 210, knyttet til figur som viser hvordan regjeringen og myndighetsorgan er organisert ved nasjonale kriser for å sikre en helhetlig krisehåndtering	Rapporten bidro til at vi fikk oppdatert kunnskap om hvordan regjeringen og myndighetsorgan var organisert i 2021 for å håndtere koronapandemien som er relevant for deres håndtering av Cyber-beredskap
NSM (2020), Risiko 2020	Rapporten er på 30 sider og vi har benyttet kunnskap om hvordan en beskytter	Nasjonal risiko bilde 2020
NSM (2021) Risiko 2021	Rapporten er på 48 sider og vi har benyttet kunnskap om hvordan en beskytter	Nasjonal risiko bilde 2020
NSM (2022), Risiko 2022	Rapporten er på 38 sider og vi har benyttet kunnskap om hvordan en beskytter nasjonale verdier, nasjonalt risikobilde, taktskifte i cyberdomene. Økt lederforståelse knyttet til cyber-risiko, samt viktigheten av å gjennomføre helhetlig risikostyringsprosesser, prosjektet. NSM grunnprinsipper	Rapporten bidro til at vi fikk oppdatert kunnskap om det nasjonale risikobildet, etablering av helhetlig risiko-styringsprosesser i virksomhetene, NSM grunnprinsipper for styring av IKT-sikkerheten. Ledelsens ansvar og behov for økt ledelsesfokus knyttet til å arbeide med virksomhetenes sikkerhetsarbeid
NSM (2022), Den digitale	NSM sikkerhetskonferanse ble gjennomført over ca. 3,5 timer. Den innledende delen, krigen i	Konferansen bidro til økt forståelse av det globale og nasjonale digitale risikobildet. Fokusområde forebyggende sikkerhet, hvor utfordringer knyttet

sikkerhetskonferansen 2022	Ukraina, samt kjente sårbarheter. Endringer og betydning av norske verdier i virksomheter har i det globale risikobildet. Fokus knyttet til digitale sårbarheter, bygge motstand og resilient beredskap, knyttet til cyberangrep.	til trusler, sårbarheter, og resilient cyber-beredskap er viktige for vår oppgave. Tema som innsideproblematikk, fokus «*på den en ikke ser*», hva preger sikkerhetstilstanden globalt, nasjonalt og for våre virksomheter i et økende digitaliseringstempo var relevant for denne oppgaven
Næringslivets sikkerhetsråd (NSR), Mørketallsundersøkelsen 2022	NSR mørketalls-undersøkelse for 2022 er på 62 sider. I 2020 versjonen var verden preget av Covid-19, 2022 rapporten er preget av krigen i Ukraina som innledet en ny sikkerhetspolitisk epoke. Det digitale trusselbildet er nå påvirket av taktskifte og sammensatte trusler. Årets mørketallsundersøkelse skal bidra med å belyse den digitale sikkerhetstilstanden i Norge.	Rapporten bidro til at vi fikk oppdatert kunnskap og status om den digitale sikkerhetstilstanden i Norge gjennom det siste året. Videre fikk vi innsikt i hvordan offentlige og private virksomheter arbeider med å forbedre den digitale sikkerheten. I tillegg fikk vi innsikt i andre virksomheters erfaringer knyttet til cyberkriminalitet, metoder som trusselaktører benytter
Regjeringen (2021)	Regjeringens strakstiltak for å dempe de økonomiske virkningene av coronaviruset omfattet bruk av hjemmekontor, informasjon på Regjeringen.no med link til tilhørende konferanse	Kunnskap om krav knyttet til bruk av hjemmekontor var relevant i vår oppgave
Politidirektoratet (2020), Politiets beredskapssystem Del I, Retningslinjer for politiets beredskap	Rapporten er på 255 sider og vi har benyttet kunnskap knyttet til det nasjonale beredskapssystemet, samt om politiets beredskaps-system beskrevet på side 18-19.	Rapporten bidro til at vi fikk oppdatert kunnskap om hvordan det sivile (SBS) og nasjonale beredskapssystemet (NBS) i Norge er sammensatt, noe som er relevant for denne oppgaven
Seglsten, Per Helge (2022a), Lei årskavalkade: 39 kjente dataangrep rammet norske virksomheter i 2021	Digi reportasje 15. januar 2022 om de 39 Cyber-angrepene som rammet Norge i 2021. Reportasjen omfattet navn på selskapene som hadde blitt rammet av cyber-angrep, samt hvilke typer angrep de ble utsatt for	Kunnskap om hvilke virksomheter som var rammet var viktig for å få spisset utvalg av informanter, samt kategori knyttet til phishing, datainnbrudd, løsepenge etc. Relevant i vår oppgave
Seglsten, Per Helge (2022b), Norske IT-angrep i 2021: Året endte med en bølge av løsepengevirus	Digi reportasje 16. januar 2022 (årskavalkade), med fokus på data-angrep på Toten kommune og Stortinget og de 36 andre kjente Cyber-angrepene, samt hvordan cyber-kriminelle arbeider fikk fokus	Kunnskap om at cyber-kriminelle er profesjonelle og når og hvordan de de arbeider var relevant for dette forskningsprosjektet.
Telenor (2020), Digital sikkerhet	Rapporten er på 58 sider og vi har benyttet informasjon på s.18-19 knyttet til kunnskap om trusselforståelse, trussel-bilde og trusselaktører	Kunnskap om trusselforståelse, trusselbilde og trusselaktører er relevant for denne oppgaven
Telenor (2021), Telenor årsrapport	Rapporten er på 181 sider og vi har benyttet informasjon på s.17 knyttet til krigen i Ukraina hvor Telenor beskriver sannsynlighet knyttet til cyber-angrep på	Kunnskap om at trusselbildet er i endring, samt at det kommer nye trusselaktører som knyttes til krigen som Ukraina er rammet av, er relevant for denne oppgaven

	vestlige land og kritisk infrastruktur.	
PST (2020), Nasjonal trusselvurdering 2020	Nasjonal trusselvurdering 2020, side 74	Nasjonal risikovurdering hvitvasking og terrorfinansiering (National Risk Assessment - NRA) er en nasjonal, tverretatlig risikovurdering som beskriver de største truslene, sårbarhetene og risikoene innen hvitvasking og terrorfinansiering.
PST (2021), Nasjonal trusselvurdering 2021	Nasjonal trusselvurdering 2021, side 40	Nasjonal risikovurdering hvitvasking og terrorfinansiering (National Risk Assessment - NRA) er en nasjonal, tverretatlig risikovurdering som beskriver de største truslene, sårbarhetene og risikoene innen hvitvasking og terrorfinansiering.
PST (2022), Nasjonal trusselvurdering 2022	Nasjonal trusselvurdering 2022, side 17	Nasjonal risikovurdering hvitvasking og terrorfinansiering (National Risk Assessment - NRA) er en nasjonal, tverretatlig risikovurdering som beskriver de største truslene, sårbarhetene og risikoene innen hvitvasking og terrorfinansiering.
UN (2020), UN E-Government Survey 2020,	Rapporten er på 364 sider og vi har benyttet informasjon knyttet til hvordan Norge er rangert i forhold til andre land når det gjelder å ta i bruk teknologi og digitalisering	Norge er flinke til å ta i bruk ny teknologi og gode på digitalisering av det norske samfunnet. E-Government Development Index (EGDI) viser på s.12-14 og 270 at Norge er rangert på 13.plass i verden og på 8. plass i Europa

Vedlegg 10 – Tematisk analyse av intervju med fageksperter

Nr	Utdrag fra intervju med fageksperter (ref. Vedlegg 7 og 8)	Kode gruppering	Tema/kategori
Inf. 2	(1) Det å ha oversikt over systemer, verdier, avhengigheter av andre er viktig for å lage god planer.	**A. Læring**	**Cyberhendelse**
Inf. 2	(2) De har ikke oversikt over hvor mange forsøk bedriften deres stanser daglig, ukentlig og månedlig.	50, 52, 76, 77	J, K, L, M
Inf. 2	(3) Ha oversikt over verdiene, jeg tror ikke de fleste virksomhetene har god nok oversikt over sine verdier	**B. Respondere**	**Resiliens og Cyberberedskap**
Inf. 2	(4) Det å ha oversikt over systemer, verdier, avhengigheter av andre er viktig for å lage god planer	1, 4, 5, 17, 34, 41, 52, 59, 75, 110	A, B, C, D, E, O, P, N
Inf. 2	(5) Planene tåler aldri virkeligheten	**C. Overvåking**	**Risikopersepsjon**
Inf. 2	(6) Hvor CFOen sier at du kommer til oss og snakker om dette her	41, 48, 74, 75	F, G, M, P,
Inf. 2	(7) ikke invitert fra teknisk side, altså CISO eller teknologiske del av virksomheten, men fra finans delen	**D. Forutse**	**Sikkerhetskultur og beredskap**
Inf. 2	(8) Det som er interessant er, da jeg snakker om risiko og det som kan ramme dem	8, 17, 26, 41, 102	A, B, C, D, E, O, P
Inf. 2	(9) Så snur konsernsjefen seg til den som er CISO eller teknisk ansvarlig og spør «skjer det oss også»?	**E. Ansvar**	**Risikobilde**
Inf. 2	(10) For meg betyr resiliens motstandsdyktighet og hva er da vi snakker om i beredskaps sammenheng?	9, 20	J, G, M, P
Inf. 2	(11) Jeg syns det er særpreg i denne bransjen som fortsatt er ganske ung, og det må vi erkjenne	**F. Kunnskaps- / informasjonsdeling**	**Risikostyring**
Inf. 2	(12) Det er en fortsatt umoden bransje som strør om seg med rare begreper og ord som en selv ikke forstår, eller hva det innebærer	28, 29, 30, 31, 32, 36, 37, 39, 40, 59, 126, 127, 128, 129, 130, 131, 132, 133, 138	E, F, G, I, P, M,
Inf. 2	(13) Vi skal ha en virksomhetskultur som inkluderer sikkerhet.	**G. Risiko**	
Inf. 2	(14) For sikkerhet i seg selv skal ikke leve sidelinjen, eller utenfor alle andre prosesser.	8, 13, 24, 26, 27, 33, 35, 38, 47, 48, 55, 56, 57, 58, 100, 107, 125, 136	
Inf. 2	(15) Jeg sier at bransjen vår er umoden, men det handler ikke bare om bransjen	**I. Sikringsrisiko / VTS**	
Inf. 2	(16) Det er til syvende og sist alle virksomhetsledere og alle ansatte som er del av dette	26, 35	
Inf. 2	(17) Vi forstår ikke teknologien, selv om vi bruker den og implementerer den	**J. Verdier**	
Inf. 2	(18) andre har gjort noe med teknologien som du kan gjøre, men nå ble det brukt til å gjøre noe negativt	1, 3, 4, 19, 49, 59, 60, 61, 63, 64, 67, 73, 74, 75	
Inf. 2	(19) jeg møter fortsatt virksomhetsledere som snakker om cybersikkerhet som om det er noe virksomheten deres er for liten til	**K. Sårbarheter**	
Inf. 2	(20) mange av virksomhetene rammes av tilfeldigheter	18, 21, 22, 25, 65, 66, 67, 69, 106, 123	

Inf. 2	(21) har dukket opp en teknologisk mulighet som gjør at de kommer inn og kan gjøre det de ønsker	**L. Trussler**	
Inf. 2	(22) blir like overrasket når det skjer ting likevel	2, 21, 24, 25, 26, 27, 68, 118	
Inf. 2	(23) Erfaringen vår er at ikke alle har forstått dette enda	**M. Zero Trust**	
Inf. 2	(24) ikke vet forskjeller på hva en risiko og trussel	108, 110, 111, 113, 114, 115, 116, 117, 119, 120, 121, 122, 123, 124, 125, 134, 139	
Inf. 2	(25) ledere og ansatte så utgjør vi en sikkerhetsrisiko fordi vi er mennesker med sårbarheter	**N. Begrep**	
Inf. 2	(26) ledelsen ikke forstår det digitale trussel og risikobilde	10, 12, 53, 54	
Inf. 2	(27) ikke greier å se forskjellen mellom risiko og trussel er frustrerende	**O. Kunnskap**	
Inf. 2	(28) hvor åpne er man egentlig	1, 5, 6, 9, 11, 12, 15, 17, 18, 23, 36, 44, 45, 48, 56, 57, 58, 60, 61, 62, 103, 104, 107, 111, 130, 131, 132, 133, 135, 136, 138	
Inf. 2	(29) Hvor mye er man villig til å dele	**P. Ledelse**	
Inf. 2	(30) På den andre siden har den virksomheter som er helt åpne, f.eks. Østre Toten kommune	6, 7, 9, 13, 14, 16, 19, 20, 26, 38, 42, 43, 44, 46, 47, 48, 70, 71, 72, 77, 112, 135	
Inf. 2	(31) Østre Toten har stilt opp i enhver tenkelig anledning om ganske ubehagelig ting å snakkes om		
Inf. 2	(32) de kommer betydelig bedre ut av dette, nettopp fordi de har valgt en åpen kommunikasjons strategi		
Inf. 2	(33) over den omdømmemessig delen av dette som går på å bli utsatt for denne type cyberhendelse		
Inf. 2	(34) Erfaringsmessige er at de aller færrest har planer for dette her		
Inf. 2	(35) sjeldent en plan for en forsettlig handling som kompliserer driftsstans		
Inf. 2	(36) Fordi dette er helt annen modenhet på dette området i Amerika		
Inf. 2	(37) høstet mange priser for sin kommunikasjon og for måten de hadde stått i det ifm. håndtering av alvorlig hendelse.		
Inf. 2	(38) de lever med en risikoforståelse som er mye breiere, de ser på helhetlig risiko for virksomheten		
Inf. 2	(39) alle har tenkt på dette senarioet til tross for at det ikke har vært mangel på historier i media om løsepengevirus		
Inf. 2	(40) Det er underkommunisert til de grader, for det er tusenvis av dem		

Inf. 2	(41) må ikke glemme de tusenvis forsøkene som stanses hver dag med potensielle katastrofale konsekvenser for samfunnet		
Inf. 2	(42) nå kommer det noen fra sidelinja og ledere med tekniskansvar blir nervøse		
Inf. 2	(43) å få toppledere til å stille noen av de riktige spørsmålene		
Inf. 2	(44) vi krypterer [...] Jeg hører hva du sier, men er det kryptologi fra «Donald» eller hva slags krypto er det		
Inf. 2	(45) cyber og IKT delen som foreløpig så umoden og bare noe IKT menneskene skal holde på med		
Inf. 2	(46) Det er ikke løftet opp på strategisk nivå for å forstå betydningen fult ut av det		
Inf. 2	(47) Toppleder må forstå det fra et strategisk perspektiv og ikke «bits and bytes»		
Inf. 2	(48) hvem vi er 100% avhengig av for å fungere og hvem er 100% avhengig av oss for å fungere		
Inf. 2	(49) hele bransjen var opptatt av at man måtte ta backup av sine data og det var ekstremt viktig		
Inf. 2	(50) testet aldri om man kom tilbake til normal drift igjen og dette har blitt veldig blitt aktualisert		
Inf. 2	(51) jeg ser at dette har snudd ved at flere virksomheter nå tester og sjekker at backup fungerer		
Inf. 2	(52) I noen tilfeller hvor virksomheten har hatt backup men ikke klart å komme tilbake til drift.		
Inf. 2	(53) begrepet informasjonssikkerhet, så består det av tre ting, 1) konfidensialitet, 2) integritet og 3) tilgjengelig		
Inf. 2	(54) Norge i dag fortsatt en ekstrem slagside på at den største bekymringen er konfidensialitets perspektivet		
Inf. 2	(55) i et informasjons- eller cybersikkerhets perspektiv, hva er det mest kritisk for meg da?		
Inf. 2	(56) noen har hacket seg inn på datasystemer og lest min pasientjournal? Altså konfidensialitet perseptiv.		
Inf. 2	(57) hacket seg inn og endret på mine pasientdata? Altså integritet i data		
Inf. 2	(58) noen har tatt over alle sykehuset data systemer og gjort disse utilgjengelig		
Inf. 2	(59) ville bidratt til å gjøre informasjonen tilgjengelig for helsepersonell som skulle reddet livet mitt denne dagen		
Inf. 2	(60) Jeg vil ha alltid velge tilgjengelighet i denne situasjon 10 av 10 ganger.		
Inf. 2	(61) latt flere tusen mennesker lese min pasientjournal i bytte mot at den dagen så funger datasystemene optimalt		
Inf. 2	(62) ikke at konfidensialitet ikke er viktig, kunder, pasienter og innbyggere skal stole på at informasjon blir passet på en god måte		
Inf. 2	(63) det ikke bare handler om pasientjournaler, men også tonnevis med teknologi som er med på å redde menneskeliv		

Inf. 2	(64) Tap av tilgjengelighet er den raskeste vei for tap av menneske liv i et modernesamfunn som vårt		
Inf. 2	(65) sårbarheter som er av menneskelig, teknologisk og prosessuell art		
Inf. 2	(66) Disse sårbarhetene eksponerer verdiene vår og de utnyttes av trusselaktørene		
Inf. 2	(67) dere får ikke gjort noe med at verdi har verdi		
Inf. 2	(68) dere får ikke gjort noe med at trusselaktørene eksisterer		
Inf. 2	(69) har gjøre noe med sårbarhetene deres		
Inf. 2	(70) sette søkelys på noe man kan gjøre noe med og påvirke selv er et viktig valg		
Inf. 2	(71) hva skal dere være stand til å gjøre selv og hvem andre kan hjelpe deg.		
Inf. 2	(72) kartlegge hva en er i stand til å gjøre selv og hvem andre kan hjelp oss, altså kompetanse og ressurs kartlegging.		
Inf. 2	(73) For ved en alvorlig cyberhendelse er ikke normal tilstanden tilbake i løpet av 48 timer		
Inf. 2	(74) jeg tror ikke de fleste virksomhetene har god nok oversikt over sine verdier		
Inf. 2	(75) Det å ha oversikt over systemer, verdier, avhengigheter av andre er viktig for å lage god planer		
Inf. 2	(76) Disse planene tåler aldri virkeligheten og man må øve på disse		
Inf. 2	(77) hvor mye tid man får til å øve og trene, samt hvor realistisk man disse øvelsene blir, men det å gjøre øvelser for å teste ut planverket		
Inf. 1	(101) Totens kommunedirektør på scenen og sier at «du må risikovurdere det uventede».		
Inf. 1	(102) Dette betyr at man er nødt til å tenke på det usannsynlige		
Inf. 1	(103) har opplevd det utenkelige		
Inf. 1	(104) Lange passord er god anbefaling, det er vi alle enig i		
Inf. 1	(105) er gode råd gode, hvis ingen følger dem?		
Inf. 1	(106) Om man skal ha unike lange passord pr. tjeneste blir dette veldig komplisert		
Inf. 1	(107) Mitt råd at man skiller på privat - eller forbruker-sikkerhet og virksomhetssikkerhet		
Inf. 1	(108) Man må endre på tankesett fra å ha to-faktor autentisering		
Inf. 1	(109) et angrep er ikke en ting, det består av mange steg		
Inf. 1	(110) bidragsytere til hendelsen er: manglende to-faktor autentisering, manglende sikkerhetsoppdatering		
Inf. 1	(111) den listen som de kriminelle måtte gjennom for å gjøre suksess		
Inf. 1	(112) Det er viktig å bygge god sikkerhetskultur ved å få de ansatte med på laget		

Inf. 1	(113) Zero Trust handler det om å gjøre smarte ting, som er relatert til beredskap, krisehåndtering, og rask gjenoppretting		
Inf. 1	(114) Det er en lang rekke oppgaver som må til for at et cyber-angrep skal bli vellykket, og dette er komplisert og sammensatt		
Inf. 1	(115) det å stoppe prosessen, slik at aktiviteten ikke blir vellykket er kanskje den viktigste del som tankesettet til Zero trust		
Inf. 1	(116) vi mennesker tillater mer enn det som er nødvendig		
Inf. 1	(117) Zero Trust perspektiv er at man ikke skal ha Trust		
Inf. 1	(118) verden og trusselbildet har blitt veldig mye mere komplisert siden introduksjon av brannmur i 1989		
Inf. 1	(119) utviklingen fra perimeterbasert sikkerhet til en sikkerhetsstrategi basert på Zero Trust prinsipper		
Inf. 1	(120) begrepet «Six serving men» i Zero Trust tilnærmingen som går på at man må ha kontroll på		
Inf. 1	(121) Det meste innen cybersikkerhet handler om «principle of least privilege», altså tilgangskontroll		
Inf. 1	(122) Hvis du får surfet på VG betyr det mest sannsynlig at utgående tilgangskontroll er liberal og da antas det at alt er tillatt utgående trafikk		
Inf. 1	(123) Når kriminelle kommer inn, vil de ha tilgang til kritiske servere og dermed kan de etablere utgående kommunikasjon		
Inf. 1	(124) Så, med Zero Trust tilnærming skal du anta at du er blitt kompromittert, og så må en etablere tilgangskontroll på innsiden		
Inf. 1	(125) Min påstand er at om du kan surfe på VG fra dine servere, så er det sannsynlig at cybersikkerheten er generelt veldig dårlig		
Inf. 1	(126) Politiet og NSM kan ikke si noe om cyber-hendelser som de jobber med, dette forstår jeg. Det er mange grunner til at man ikke snakker om cyber-hendelser.		
Inf. 1	(127) åpenhet er veldig sammensatt av forskjellige grunner, noen avstår fra å være åpne fordi det er tidskrevende		
Inf. 1	(128) har samtidig høstet mye skryt for å dele sine erfaringer		
Inf. 1	(129) fikk fylkesordføreren i Nordland Fylkeskommune til å stille opp i vår konferanse tidligere i år for å snakke om denne hendelsen, og som ikke ble vellykket, og som ble stoppet		
Inf. 1	(130) Jeg tror det er viktig å dele erfaring og kunnskap om forsøkt på cyber-angrep som blir stoppet, og ikke bare dele etter at det har skjedd en katastrofe.		
Inf. 1	(131) bør ha diskusjon på hva som er et angrep, og når skal vi dele		
Inf. 1	(132) bør vi kunne dele mere informasjon og kunnskap om når et angrep blir stoppet suksessfullt		
Inf. 1	(133) for å oppsummere dette, det er generelt dårlig med deling av informasjon, men jeg tror vi også kunne ha delt andre ting i tillegg		

Inf. 1	(134) Kriminelle kan være inne i systemene til virksomhetene, og det kan skje via Software as a Service (SaaS), og som noen omtaler som skyen		
Inf. 1	(135) det ikke finnes noen standard som ivaretar kvalitet, sikkerhet og policyer		
Inf. 1	(136) økt risiko ved at man har multiple systemer uten kompetanse eller risikoforståelse for hver enkelt løsning		
Inf. 1	(137) Ekstremt varierende, prosentvis er det lavt		
Inf. 1	(138) det er generelt dårlig med deling av informasjon, men jeg tror vi også kunne ha delt andre ting i tillegg		
Inf. 1	(139) Six serving men» i Zero Trust tilnærmingen som går på at man må ha kontroll på: Hvem skal ha tilgang? Hva skal man ha tilgang til? Hvor skal man ha tilgang fra? Når trenger man tilgang? Hvordan skal det kommuniseres? Hvorfor trengs denne tilgangen? Hvis man tar med disse seks kontrollene ifm. tilgangsstyring, vil man har god kontroll og sikkerhet		