Petroleumstilsynet

Beskyttelse av data i ro og i transit

Forfattere:
Andreas Grefsrud, Kenneth Titlestad, Øystein Aspøy, Kristin Weiseth, Kari Anette Sand

Sopra Steria
2021-12-01

Innholdsfortegnelse

1 Sammendrag

Denne rapporten sammenfatter kunnskap og erfaring fra petroleumssektoren knyttet til sikring av data og informasjon. Videre drøftes ulike sentrale perspektiver med relevans til dette. Det tas utgangspunkt i at data må sikres i ro og i transit og at utvikling innenfor digital teknologi i og utenfor sektoren gir økt kompleksitet, nye sårbarheter og endringer i trusselbildet. Data og informasjonssikkerhet blir mer vesentlig, og som et resultat av dette utfordres sektoren på kunnskapsutvikling, prosesser for styring, kontroll og risikostyring. Teknologisk utvikling, slik som omtales som Industri 4.0, hvor OT integreres tett med IT og skytjenester, gir muligheter for bedre kontroll på et sammensatt bilde av leveranser, systemer og datastrømmer mellom leverandører og operatørselskaper, men gir samtidig høyere kompleksitet, lengre verdikjeder og flere usikre faktorer vedrørende informasjonssikkerhet, IT-sikkerhet og generelt sikkerhetsarbeid. I drøftingen i denne rapporten ses det på hvilke relaterte menneskelige, teknologiske og organisatoriske sårbarheter petroleumssektoren står overfor og hvilke sentrale prosesser som kan måtte styrkes for få et godt arbeid med informasjonssikkerhet og IT-sikkerhet.

2 Innledning

2.1 Bakgrunn for prosjektet

Oppgavens hensikt er å kunne svare på i hvilken grad data og informasjon blir sikret, i både ro og i transit.

Størst kjennskap om teknologiske løsninger for lagring og overføring av informasjon besittes ofte av en eller flere leverandører. Dette skaper avhengigheter mellom leverandører i flere ledd. Sky, datalake, SaaS og nyere mekanismer for datatransport, kablet og trådløst, presenterer muligheter for mer leverandørstyrte leveranser og driftskontrakter i den digitale verdikjeden. Denne sammenkoblingen mellom flere systemer og løsninger som involverer flere aktører bidrar til enda mer komplekse leverandørkjeder. Graden av kompleksitet og avhengigheter i slike leverandørkjeder gjør det vanskeligere å få god oversikt og kunnskap om informasjonsverdier og -eiere, sårbarheter, trusler, sannsynlighet for hendelser og angrep, samt konsekvenspotensial. Gjennom slike avhengigheter kan det oppstå kjedereaksjoner med konsekvenser for hele verdikjeden.

For å gi et svar på hvordan data og informasjon blir sikret, har denne oppgaven et særskilt fokus på samspillet mellom operatørene og andre aktører i petroleumssektoren. Oppgaven tar for seg hvorvidt risikoeierskap blir ivaretatt tilfredsstillende, om styringen og kontrollen ligger hos operatørene, eller om dette overlates til leverandører og hvordan dette påvirker risiko og muligheter for kontroll.

2.2 Begreper, definisjoner og forkortelser

2.2.1 Begreper

Begrep	Definisjon / Beskrivelse
A-Standard Handlingsmønster	Equinors handlingsmønster som beskriver hvordan en planlegger, utfører og evaluerer en konkret jobb eller aktivitet på sitt beste, slik at den utføres korrekt første gang [1]
Datadiode	En nettverkskommunikasjonsenhet som gjennom optikk og/eller elektronikk muliggjør transport av data kun i en retning
Digital tvilling	En digital representasjon av fysiske objekter, systemer og prosesser
DIKW	Data – Information – Knowledge - Wisdom er en modell som viser måten vi beveger oss fra data

	til informasjon, kunnskap og visdom gjennom beslutninger og aksjoner
Edge	Begrep for beregning og databehandling i nærhet av datakildene. I denne sammenhengen er dette oftest en server eller datamaskin offshore
Ekstraktor	Løsning som har som funksjon å hente ut data fra ett eller flere system og transportere til annet system
GDPR	General Data Protection Regulation (Personvernforordningen) er en forordning for beskyttelse av data og personvern ved behandlinger av personopplysninger i Den europeisk union (EU)
Integritet	Pålitelighet og korrekthet av data/informasjon
Internkontroll	Helhetlig virksomhetsprosess forankret hos ledelsen, som bidrar til målrettet og effektiv drift, pålitelig rapportering og etterlevelse av regelverk
Konfidensialitet	Sensitivitetsgrad av data/informasjon som betyr at det ikke skal gjøres kjent eller tilgjengelig for uvedkommende
Model Based System Engineering	En modell for formalisert bruk av modellering for å understøtte kravsetting, design, analyse, verifikasjon og validering
Personvern	Personvern handler om retten til et privatliv og retten til å bestemme over egne personopplysninger
Risikoeier	Rolle som har fått delegert resultatansvar. Rollen er ansvarlig for både gode og dårlige resultater innen sitt ansvarsområde, og følgelig eier av risikoen innenfor dette området.
Syslog	En standard for logging av meldinger innen databehandling
Tilgjengelighet	Et mål på hvorvidt data/informasjon er tilgjengelig for de som har behov for den
Virksomhet	Fellesbetegnelse på offentlig forvaltningsorgan eller privat bedrift med eller uten et styre
Virksomhetsledelse	Ledelsen i virksomheten, enten administrerende direktør/daglig leder alene, eller toppledergruppen.

2.2.2 Forkortelser

Forkortelse	Beskrivelse
AMQP	Advanced Message Queuing Protocol
INL CCE	Idaho National Lab's Model for Consequence-Driven Cyberinformed Engineering
CIA	Confidentiality, Integrity, Availability
COBIT	Control Objectives for Information and related Technologies
DDoS	Distributed Denial of Service
EPC	Engineering, Procurement and Construction
FTP	File Transfer Protocol
HAZOP	Hazard and Operability
HMI	Human Machine Interface
HMS	Helse, miljø og sikkerhet
ICS	Industrial Control Systems, industrielle kontrollsystem
IMS	Information Management System
IoT	Internet of Things
ISMS	Information Security Management System
IT	Informasjonsteknologi
KIT	Konfidensialitet, Integritet, Tilgjengelighet
LOPA	Levels of Protection Analysis
MQTT	Message Queuing Telemetry Transport
NOA	Namur Open Architecture
OPC UA	OPC Unified Architecture
OSINT	Open Source Intelligence
OT	Operasjonell Teknologi
PHA	Process Hazards Analysis
PIMS	Production Information Management System
PLC / PLS	Programmable Logic Controller / Programmerbar Logisk Styreenhet
SaaS	Software as a Service
SFTP	SSH File Transfer Protocol
SIS	Safety Instrumented System – Instrumentert sikkerhetssystem
SSH	Secure Socket Shell

2.3 Metode og gjennomføring

Prosjektet har benyttet kvalitativ metode ved gjennomføring av arbeidet. Det er gjennomført dybdeintervjuer med sentrale leverandører og selskaper i petroleumssektoren, litteraturstudie, og innhentet informasjon har blitt systematisert og analysert. Dybdeintervjuer og

litteraturgjennomgang har sikret innsamling av viktig informasjon fra ulike kilder og samtidig dannet grunnlaget for analyse, drøftinger i rapporten og anbefalinger. Sopra Steria har benyttet eget tverrfaglig team bestående av fagspesialister innen OT/IT, informasjonssikkerhet og risikostyring gjennom alle faser i prosjektet for å sørge for faglig kvalitet i innsamling og bearbeiding av informasjon.

2.3.1 Dybdeintervjuer

Det ble gjennomført dybdeintervjuer med sentrale selskaper og personell i petroleumssektoren som besitter relevant kunnskap om dagens initiativer, tilstand, utfordringer og muligheter. Intervjuene ble gjennomført som semistrukturerte intervjuer hvor det i forkant ble utarbeidet et sett med spørsmål og en intervjuguide. Alle informantene mottok samme spørreskjema der spørsmålene i all vesentlighet ble besvart skriftlig forut for intervjuene. Svarene informantene har gitt skriftlig ble deretter gjennomgått muntlig i fellesskap med dem, hvilket ga rom for ytterligere dialog rundt de opprinnelige spørsmålene. Utgangspunktet for intervjuene var intervjuguiden, samt spørsmål utenfor guiden som ble formulert og tilpasset hver enkelt informant avhengig av svar som ble gitt på spørsmålene og hvor i verdikjeden aktøren var lokalisert.

Gjennomtenkt utvelgelse av selskaper ble gjort for å sørge for å få et representativt og bredt bilde av petroleumsvirksomheten og verdikjeden. Det ble derfor gjennomført intervjuer med ulike operatørselskaper og leverandører. Flere selskaper har i sum dekket rollene:

- Operatørselskap
- Kontraktørselskap (EPC)
- Leverandør av industrielle kontrollsystem og instrumenterte sikkerhetssystem
- Leverandør av løsninger for industriell digitalisering (Industri 4.0)

2.3.2 Litteraturgjennomgang

Litteraturgjennomgang omfatter gjennomgang av relevant og oppdatert informasjon fra retningslinjer og tidligere kunnskapsrapporter. Dette inkluderer de siste års relevante rapporter fra IRIS, Sintef, DNV og DSB, samt nyere utgaver av internasjonale standarder, herunder blant annet IEC 62443, ISO 27001, ISO 27002, ISO 27005 og ISO 31000.

2.3.3 Analyse

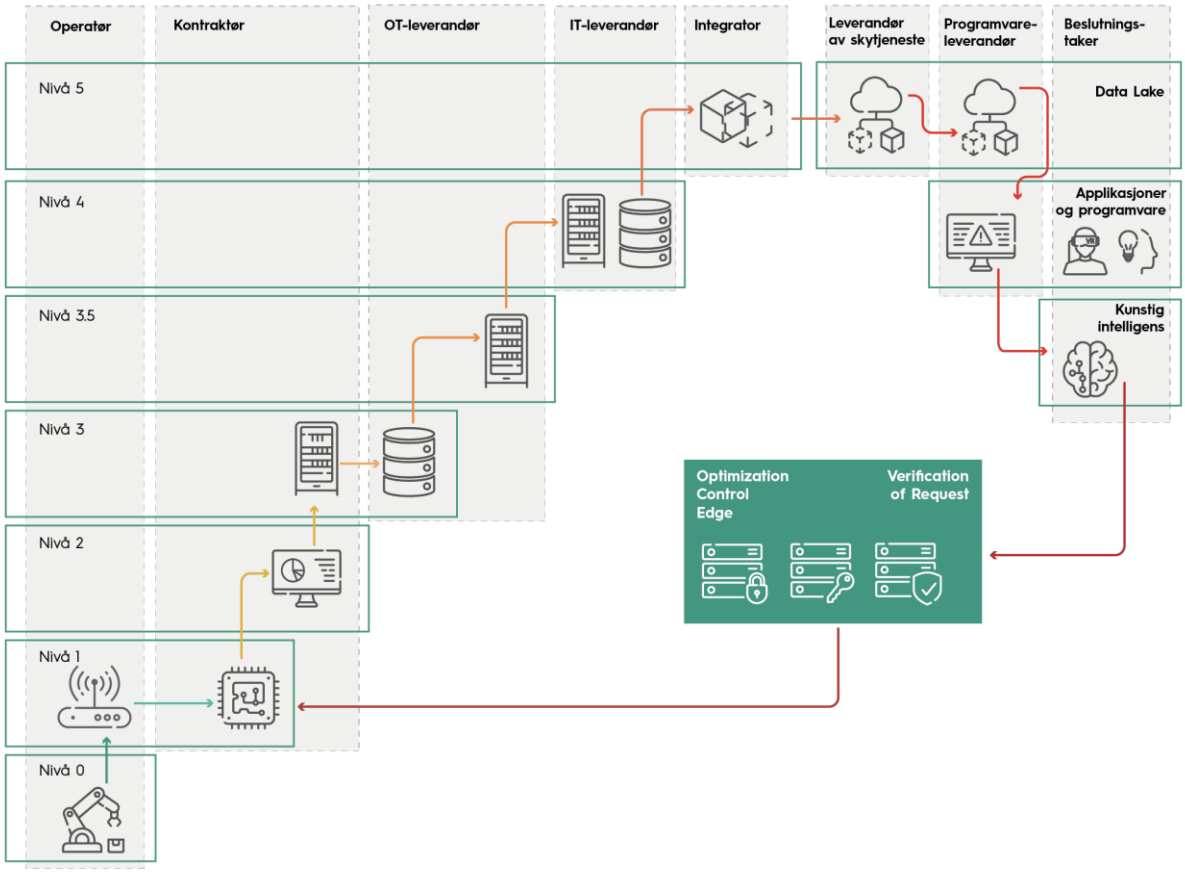
For analyse har det blitt gjort en sammenstilling av informasjon fra dybdeintervjuer, litteraturgjennomgang og erfaringen til fagspesialistene i prosjektet. Dette danner grunnlaget for drøftingen som er gjort i rapporten og anbefalingene som er gitt.

3 Historikk og bakgrunn

Gjennom den teknologiske utviklingen som har skjedd de siste årene, spesifikt utvikling innenfor industriell digitalisering og Industri 4.0, ser petroleumssektoren økte muligheter for å anvende digital teknologi på tvers av OT og IT, på tvers av operatører/leverandører og gjennom større deler av anlegg og utstyrs levetid. Nye systemer utvikles og tas i bruk for å øke evnen til å designe, bygge, overvåke og vedlikeholde anlegg og utstyr fra desentrale lokasjoner hos en eller flere leverandører i en digital verdikjede. Tegninger, modeller, konfigurasjon og tidsseriedata smeltes sammen, kontekstualiseres og berikes til ny informasjon. Dette er informasjon som søkes tilgjengeliggjort i en voksende og digital verdikjede som strekker seg fra sensorer, via industrielle kontrollsystemer og Edge- og/eller kontorsystemer, frem til skybaserte dataplattformer hos operatører og leverandører. Gjennom berikelse av data fra flere kilder kan modeller og beslutninger gis et sterkere datagrunnlag og være bedre egnet for direkte eller indirekte overvåking og styring.

På denne teknologiske reisen er det imidlertid uklart i hvilken grad aktørene i de digitale verdikjedene er bevisst iboende risikoer og hvorvidt de sørger for tilstrekkelig sikring av data og informasjon, både ved overføring (transit) og ved lagring (i ro). Det er videre uklart hvorvidt de ulike aktørene er bevisst sin rolle i verdikjeden, og om det ansvarlige operatørselskap tilstrekkelig følger opp og sikrer egen og leverandørers styring og risikohåndtering av data og informasjon.

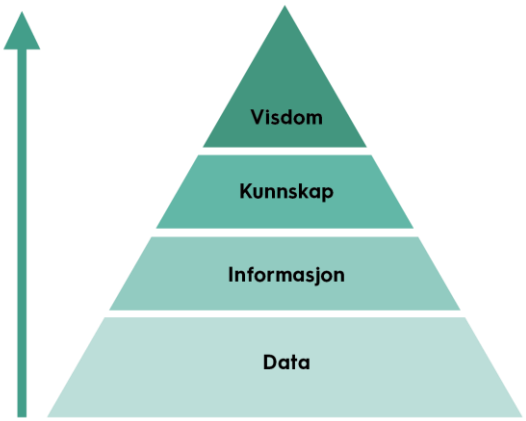
Historisk sett har petroleumsvirksomheten benyttet industrielle kontroll- og sikkerhets-systemer som er adskilt fra øvrige IT-systemer. Risikobildet for disse systemene har i stor grad vært håndterbart. Imidlertid har fremveksten av cloud, IoT/IIoT og andre teknologifremskritt skapt muligheter for effektivisering og optimalisering innen engineering, overvåking, kontroll og vedlikehold. Det er dermed duket for en utvikling hvor tidligere isolerte systemer (Purdue-nivåene 1 til 3 i Figur 1) nå kobles sammen og berikes med funksjoner i skytjenester fra en eller flere leverandører. Dette bidrar til at det oppstår et mer sammensatt og komplekst bilde av eierskap til tjenester og informasjon. Det er utfordrende å vurdere hvilke risikoer dette kan introdusere, og hvilke kontroll- og sikkerhetsmekanismer som vil kunne bidra til å redusere slike risikoer.



Figur 1: Sensordata sendes ut av kontrollsystemet og til sky for avansert databehandling. Leverandør-landskapet blir mer sammensatt, kompleksiteten øker og datakvalitet blir mer usikker. Generell risiko knyttet til informasjons-sikkerhet kan øke i takt med kompleksiteten.

4 Informasjon om anlegg og systemer

For drift og vedlikehold av olje- og gassanlegg er det mye data som brukes og som er nødvendig. Ved å se data på riktig måte, i riktig kontekst, vil det kunne gi informasjon - som på sin side danner grunnlaget for kunnskap, beslutning og aksjon, som vist i Figur 2.



Figur 2: DIKW modellen viser hvordan vi beriker dataene gjennom mer informasjon om dataen, kunnskap og visdom. Dette gjør det enklere å ta bedre, informerte og databaserte beslutninger.

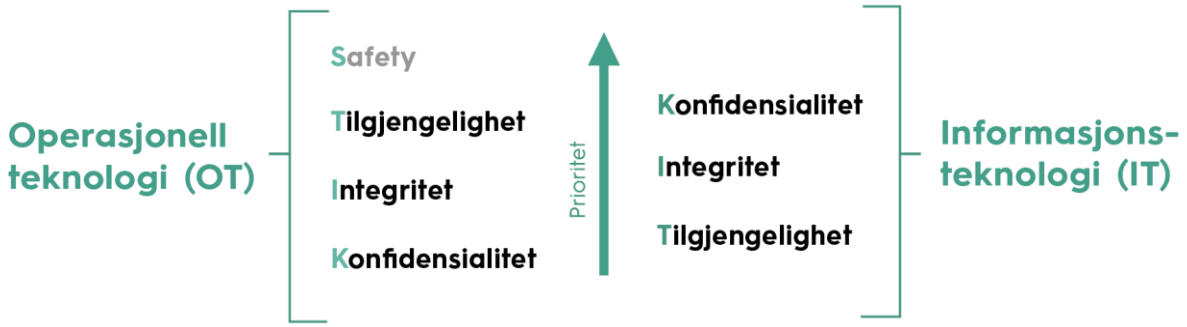
Både mennesker og IKT-systemer benytter data og den informasjonen som kan utledes av data, som grunnlag for å treffe beslutninger og ta de riktige eller optimale avgjørelsene.

Det er dermed en forutsetning at dataene er korrekte, komplette, oppdaterte, leses på riktig tidspunkt og forstås riktig. Det samme gjelder metadata - data som beskriver data - for å gi nødvendig, tilstrekkelig og riktig kontekst. Feil eller manglende kontekst for data kan gi mangelfull eller helt feil informasjon, som igjen kan lede til feil beslutninger og aksjoner.

I intervjuer og samtaler blir begrepene data og informasjon i stor grad brukt med likelydende betydning. Med fremveksten av modeller, eksempelvis brukt i Model Based System Engineering, og aggregering/kontekstualisering av data, ser vi også at det er blitt vanskeligere å skille entydig mellom hva som er data og hva som er informasjon utledet av data.

Med forutsetningene som gjelder for informasjon og beslutningstaking er det muligheter for at data eller metadata kan være mangelfull, feil, ha blitt forfalsket eller ikke er tilgjengelig når det er behov for dem. For data som kan avsløre sensitiv informasjon er det også en risiko for at de kan bli tilgjengelige for uønskede parter. Sikkerhetsmål for data og informasjon kategoriseres derfor gjerne i Konfidensialitet, Integritet, Tilgjengelighet, og forkortes til K-I-T. Innen petroleumssektoren omtales dette vanligvis med de engelske begrepene Confidentiality, Integrity, Availability, og forkortes til C-I-A.

For typiske IT-systemer har konfidensialitet og integritet i en del tilfeller prioritet over tilgjengelighet, se Figur 3. Dette kommer gjerne som et resultat av at IT-systemer lagrer og behandler personopplysninger eller annen informasjon som krever konfidensialitets-beskyttelse. Derfor er også personvern svært sentralt i sikkerhetsarbeid knyttet til IT-systemer.



Figur 3: Prioriteringer for sikkerhetsmålene generelt for typiske OT- vs. IT-systemer.

Med fremveksten av internett, og den økende avhengigheten som bygges til digitale tjenester og digitale verdikjeder, ser vi derimot økende krav til tilgjengelighet for IT-systemer [2].

For Operasjonell Teknologi (OT) er ikke behandling av personopplysninger sentralt. OT-systemers primærfunksjon er å overvåke, kontrollere og styre fysiske prosesser. I OT-domenet er prosessverdier, konfigurasjonsdata, logikk, tegninger over maskiner og systemer i fokus og behandles derfor omhyggelig. Disse dataene benyttes for å kunne sørge for sikker, stabil og effektiv drift av anlegg og industrielle prosesser. På grunn av dette formålet er derfor tilgjengelighet og integritet langt viktigere enn konfidensialitet i OT. I enkelte tilfeller trekkes også «Safety» frem som et sikkerhetsmål - for å illustrere at dette i konfliktilfeller er et overordnet mål.

Når data overføres ut av de industrielle kontrollsystemene, der formålet med overføringen er å kunne gjøre analyser, rapportering og optimalisering, medfører endringen i formålet at kravene til tilgjengelighet gjerne reduseres. Samtidig øker antallet transportetapper og transaksjoner, noe som bidrar til at data og informasjon eksponeres i større grad. Dermed blir sikring av konfidensialitet og integritet stadig viktigere. Slik sett ser man at data må sikres med hensyn til K-I-T både i ro og i overføring, og at vektingen av sikkerhetsmålene kan være forskjellig ut fra formålet i det domenet de blir anvendt i. Det må derfor gjøres vurderinger av risiko utfra aktuelt formål og domene. Perspektiver på risikovurdering tas videre opp i kapittel 8 – «Risiko og risikostyring».

4.1 Ulike typer data og informasjon

Innenfor petroleumsvirksomheten finnes det en rekke ulike typer data som lagres og overføres. I denne rapporten, og i intervjuer, har vi valgt å gruppere data inn i statisk og dynamisk data. Dette er ikke ment som et presist skille, men er brukt som en benevnelse for å kunne omtale to til dels forskjellige grupper av data, informasjon og systemer.

Statiske data og informasjon: Data som primært ligger i ro, dvs. lagret. Dette er ofte større mengder data, som lagres og overføres i bulk, inneholder mye informasjon og har gjerne en

del informasjon om kontekst. Eksempler på dette er tekniske tegninger/skjemaer, konfigurasjonsfiler, programfiler, sikkerhetsoppdateringer og logikk- og prosjektfiler.

Dynamiske data og informasjon: Data som primært er i bevegelse, dvs. under overføring. Dette er ofte små fragmenter, verdier eller beskjeder og inngår gjerne i en strøm av data slik som tidsserier, men kan også være kommandoer, beskjeder, signaler eller API-kall. Dynamiske data inneholder ofte lite eller ingen informasjon om kontekst. Eksempler på slike data kan være måleverdier fra transmittere, signaler til eller fra PLSer, kommunikasjon over Modbus TCP, OPC DA eller gjennom message-queue-baserte protokoller slik som AMQP eller MQTT.

Ved kommunikasjon over OPC UA stilles det høyere krav til å kommunisere kontekst/metadata parallelt med signaler/beskjeder. Data og informasjon i denne kommunikasjonsprotokollen anser vi derfor for å være en kombinasjon av statisk og dynamisk informasjon.

4.2 Systemer og deling av informasjon

For både statisk og dynamisk informasjon benyttes det i petroleumssektoren en rekke forskjellige systemer, både for internt bruk i bedriften og for deling av data og informasjon mellom bedrifter. For statiske data og informasjon, som primært ligger i ro, benyttes det for eksempel interne fildelingsområder, dokumenthåndteringssystemer, engineering-verktøy, generiske databaser og dedikerte database-baserte løsninger for krav, design/engineering, arbeidsprosesser, etc.

For deling av statisk informasjon forteller informantene at det er foretrukket å bruke dedikerte dokumenthåndteringssystemer. Flere ulike systemer benyttes for å kunne gjøre deling på tvers av selskaper på en kontrollert måte. Tilgangskontroll blir da i hovedsak styrt av informasjonseier eller premissgiver, oftest operatørselskap. Eksempler på slike løsninger som blir brukt i sektoren i dag er ProArc, ProcoSys, Documentum, D2, STID, Meridian, Intergraph, PIMS, Aveva-suite og SharePoint (On-Premises). Løsningene har varierende grad av funksjonalitet for tilgangskontroll, informasjonsklassifisering og deling.

Gjennom intervjuer tegner det seg et komplekst bilde av systemer, samt utfordringer med mangelfull funksjonalitet. Dette bildet bekreftes ytterligere av at de fleste informantene også sier at det blir brukt andre systemer og kanaler for deling, slik som epost og FTP/SFTP. De siste års utvikling innen Office 365 har videre gjort at det foretas mer lagring og deling av informasjon gjennom Sharepoint Online, Teams og OneDrive. Covid-19-pandemien og hjemmekontor har forsterket dette ytterligere. Informanter forteller også om at rigid eller tungvint tilgangskontroll gjør at brukere i enkelte tilfeller benytter Dropbox, Google Drive og liknende, gjerne på private kontoer. Sektoren ser ikke ut til å ha tilstrekkelig oversikt eller kontroll over andre delingskanaler som blir brukt utover dokumenthåndteringssystemer.

Det nevnes som en utfordring at informasjonsklassifisering og tilgangskontroll ikke automatisk følger med informasjonsobjekter om de blir kopiert til et annet system eller til en annen kanal. Når tilgangsstyrt, sensitiv informasjon i et dokumenthåndteringssystem blir kopiert ut og delt

via Teams eller OneDrive, fragmenteres den opprinnelige informasjonsklassifiseringen og tilgangskontrollen. En løsning på denne utfordringen kan være å beskytte informasjonen fra å kunne bli kopiert ut, eksempelvis gjennom begrensinger i tilgang og gjennom å benytte funksjonalitet for Digital Rights Management/ Information Protection. Med en slik løsning, eksempelvis Microsoft/Azure Information Protection, finnes det muligheter for å kryptere informasjonsobjekter slik at de fortsatt kan kopieres og deles, ved at de kun kan dekrypteres og leses om man besitter riktig tilgang og dekrypteringsnøkler. Imidlertid fordrer dette at systemene som blir brukt for deling støtter de relevante mekanismene for kryptering og dekryptering. Vi ser at det er et omfattende arbeid som må til for å få et stort utvalg av selskaper til å enes om hvilke mekanismer som skal benyttes for kryptering/dekryptering, samt gjøre implementasjon og adopsjon av dette. Microsofts løsninger i Azure og Office 365 (Azure/Microsoft Information Protection) ser ut til å være mest utbredt i petroleumssektoren på tvers av verdikjeden. Dette er tilsvarende det vi også erfarer fra andre sektorer.

En sikkerhetsmessig mekanisme som benyttes av flere er å la informasjon ligge på kildesystemet og gi de relevante brukerne tilgang gjennom fjerntilgang. Eksempler på dette er portal-løsninger, eksempelvis Citrix, både for IT og for OT. Brukerne logger på en portal og går derfra til spesifikke systemer for å få tilgang til informasjon. Tilgang til tyngre fagsystemer, IMS, og HMI/operatørstasjoner blir oftest gitt på denne måten. På grunn av økt interesse for å bringe sensordata ut av anlegg og til sky ser vi både gjennom intervjuene og i ulike prosjekter en antydning til økt bruk av fjerntilgang. Dette for å implementere ulike løsninger for datatransport, samt gjøre kvalitetskontroll eller ytterligere undersøkelser der hvor data i sky virker å være mangelfull, feil eller uforståelig. På lengre sikt, forutsatt at sektoren får styrket datakvaliteten og informasjonen i skyløsninger og digitale tvillinger, vil det kunne være muligheter for redusert bruk av fjerntilgang.

Fjerntilgangsløsningene i sektoren er i de fleste tilfeller svært eksponert på internett. Ettersom de også har en funksjon i å sikre skjermingsverdig informasjon/systemer utgjør disse løsningene derfor også en betydelig risikofaktor for informasjonssikkerhet, IT-sikkerhet og potensielt storulykke. Slike løsninger må som minimum være motstandsdyktige mot trusselaktører med moderate kapasiteter. Dersom andre sentrale sikkerhetsmekanismer og barrierer ikke er tilstrekkelig kvalitetssikret og vedlikeholdt, eksempelvis segregeringen mellom IT/OT og prosesskontroll/instrumenterte sikkerhetssystemer, må fjerntilgangsløsningene etter vår oppfatning også være motstandsdyktige mot målrettede trusselaktører med betydelige kapasiteter. Ved å bringe nødvendig data og informasjon ut av anleggene på en sikker måte, og tilrettelegge for bruk av sikre skyløsninger og digitale tvillinger, vil man kunne oppnå gevinster også på sikkerhet og sikring.

Dynamisk informasjon og data, slik som tidsserier og signaler, er i sin natur i hovedsak i bevegelse («transit»). Data utveksles mellom endepunkter og systemer i stor grad, dog foreløpig i mindre grad på tvers av selskaper. Gjennom intervjuer ser vi at det fortsatt er slik at denne utvekslingen primært skjer innenfor gitte lag eller spesifikke kanaler i henhold til en tradisjonell Purdue-modell, eksempelvis internt i et leverandørspesifikt kontrollsystem eller fra

og til et begrenset og kontrollert antall systemer/endepunkter. Eksempler på systemer med slik datautveksling er innen industrielle kontrollsystemer, kontrollrom på land, instrumenterte sikkerhetssystemer, IMS, Osisoft PI, samt mellom en eller flere slike systemer. Det finnes også datautveksling på PLS-nivå mellom operatørselskap, eksempelvis for kontroll og styring av elkraft, og for prosessanlegg som er avhengige av hverandre på tvers av anlegg og operatørselskap.

Med satsningen som skjer på Industri 4.0 er det en vekst av pågående arbeid for å få datastrømmer ut av anleggene. Det foretrekkes å gjøre dette i form av protokollene OPC UA, AMQP eller MQTT, men andre mekanismer benyttes også, slik som filkopiering over FTP/SFTP, database-replikering, syslog eller ved andre mer proprietære mekanismer. Datatransport gjøres gjennom dedikerte data-gateways og ekstraktorer. Datadioder benyttes i svært liten grad, imidlertid er det flere aktører som forteller at de vurderer å ta dette i bruk. Namur Open Architecture (NOA), inkludert NOA Diode blir også nevnt som interessant av flere aktører. Data transporteres til industrielle datalakes i sky, som Omnia, Cognite Data Fusion, Kognifai, Veracity m.fl. Det investeres i, og piloteres på, å få data til ulike SaaS-løsninger, og kunne etablere digitale tvillinger og Asset Administration Shells.

Informantene synes å være klar over noen risikofaktorer ved satsningen på Industri 4.0, eksempelvis hvor viktig og vanskelig det er å påse dataintegritet og datakvalitet. Enkelte informanter utrykker også noe bekymring om hvordan datatransport-kanaler bygges og implementeres, og at ved å åpne for datatransport ut fra sikre soner økes risikoen for at trusselaktører kan utnytte kjente eller ukjente sårbarheter for å hacke seg inn. Med hendelser som SolarWinds/Sunburst, Triton og Ekans-viruset i bakhodet får derimot den sistnevnte tematikken etter vår mening for lite oppmerksomhet i petroleumssektoren. Det er fra tid til annen enkelte diskusjoner i sektoren om sikkerhetsmekanismer for OPC UA, sårbare protokoller, datadioder og NOA Diode, men dette blir likevel viet lite oppmerksomhet sammenliknet med fokuset på informasjonsmodeller, interopabilitet og digitale tvillinger. Grundige sikkerhetsvurderinger bør gjøres for data-gateways og for hvordan OPC UA, AMQP og MQTT blir sikret. NOA Diode på sin side, når det kommer løsninger for dette, må også gjennomgås med hensyn til sikkerhetsdesign, forutsetninger, byggekvalitet og svakheter.

Enkelte informanter formidler at det på denne teknologiske reisen er svært komplekst å få god oversikt og kunnskap om informasjonsverdier og eiere, sårbarheter, trusler, sannsynlighet for hendelser/angrep og konsekvenspotensial.

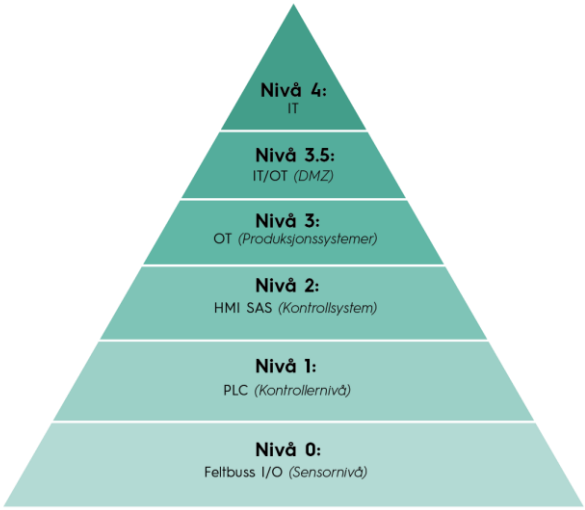
5 Industri 4.0

Industri 4.0 blir brukt som et begrep for den fjerde industrielle revolusjon der en skal bruke avansert teknologi, digitalisering og interoperabilitet for å full-automatisere og robotisere produksjon og industri på tvers av verdi og forsyningskjeder.

Petroleumssektoren har en lang tradisjon for å automatisere og kontrollere prosesser og operasjoner med bruk av automasjon og teknologi. Det er også god historikk på å flytte data til land for analyse, både innen boring, leting og produksjon av olje og gass. Neste evolusjon kan være autonome systemer som kommuniserer og tar avgjørelser utover den funksjonaliteten som ligger i den enkelte PLS i dag. Dette vil være en tilnærming til styring uten kontrollrom og operatører, men som er basert på dataanalyse og autonom styring.

For å oppnå dette trenger beslutningssystemene en rikere datastrøm enn det som har vært vanlig til nå - gjerne uten komprimering eller behandling av data, og med mer metadata, informasjon om datakvalitet og annen informasjon fra flere kilder. Slike datastrømmer sendes gjerne til en eller flere skytjenester for analyse, og/eller til systemer på kontornivå der det også eksisterer simuleringsprogrammer og annet som ikke nødvendigvis kjører i et isolert system som tidligere.

I petroleumssektoren har Purdue-modellen, se forenklet versjon i Figur 4, vært innarbeidet som et tankesett for å sikre integriteten til industrielle kontroll-systemer. Modellen er i hovedsak laget for å kunne beskrive ulike funksjoner i det industrielle systemet, og den var ikke ment som en modell for sikkerhet. Den har likevel vist seg å være svært anvendelig til sikkerhetsformål for OT. Den blir brukt som veileder til fysisk arkitekturdesign og blir hyppig referert til som oppskrift på hvordan kritisk infrastruktur kan sikres.



Figur 4: Forenklet versjon av Purdue-modellen.

5.1 Observasjoner og drøfting

Industri 4.0 utfordrer nå bruken av Purdue-modellen som oppskrift på sikkerhet for OT-systemer. Nivå 2 kommer til å være mer spredt, noe vi ser allerede, eksempelvis innenfor boring og brønnvedlikehold der det nå settes utstyr ute på installasjonene for overvåking, logging og berikelse av informasjonen direkte fra brønner og utstyr i brønn. I visse tilfeller kobles dette også direkte til kontrollsystem for brønnene, som på sin side gjerne er direkte koblet opp til plattformers hovedkontrollsystem.

Vi ser eksempler på at det settes «Edge-utstyr» ute på industrielt utstyr for logging av data og som gjerne kommuniserer med en tjeneste utenfor det industrielle miljøet for å berike data og gi brukere en bedre analyse av dataene i realtime. Fragmentering av Purdue-sonene ser vi også innen de større kontrollsystemene, selv om de fleste eksemplene foreløpig sender en rikere strøm av data fra nivå 2 til skyen og deretter presenteres i en applikasjon eller tjeneste som operatørene i kontrollrom bruker til analyse/støtte, eller som veiledning i operasjon av de industrielle prosessene.

For løsninger bygget etter Purdue-modellen er det viktig at en i fremtiden beveger seg i retning «Zero Trust» for å kunne sikre datastrømmer og samtidig styre hva enheter, personer og systemer har mulighet til å gjøre - i form av kontroll på identiteter/tilganger, rettigheter til kjøring av kode, rettigheter på operasjoner i HMI, osv. I dag er det lite system i begrensninger for hva en kan gjøre så lenge en har nettverksmessig kontakt med kontrollere og industrielle systemer. Når datastrømmer til sky ikke sikres tilstrekkelig gir det økt mulighet for at uvedkommende, eksempelvis hackere, kan klare å operere og omprogrammere både prosesskontroll og instrumenterte sikkerhetssystemer fra fjerntliggende lokasjoner, med potensiale for skade på maskiner, anlegg, mennesker og miljø. Gjennom rekognosering og stegvis tilnærming fra en målrettet trusselaktør kan skadepotensialet være katastrofalt, og med dagens utbredelse av programmerbar, digital teknologi, er det ikke gitt at det finnes tilstrekkelig uprogrammerbare eller uavhengige barrierer for å hindre eller begrense en slik ulykke.

Alt kommer til å stadig endres i fremtiden, og med dagens endringshåndtering i tung industri er det et gap mellom det som er installert og i drift og hva som er dokumentert. Det bør vurderes å ta i bruk mer moderne, dedikerte verktøy - som er i bruk innen programvareutvikling - for endring- og versjonshåndtering slik at en ikke ender opp med utdatert og ukorrekt dokumentasjon.

Videre bør det implementeres funksjoner i endepunkt som begrenser hvilke verdier som kan endres og hva en generelt skal få tilgang til. Det bør også søkes å gå bort fra privilegerte tilganger med rettigheter utover det som er nødvendig. Det er fullt mulig å sikre tilganger, både for lesetilgang og for skrivetilgang. Men hvordan sikre tillit mellom avsender og mottaker?

Fremover vil det sannsynligvis være færre statiske systemer som bare konfigureres og settes i drift. Et eksempel på dette er utstyr som i dag står isolert med en lokal kontroller/PLS. Dette er utstyr som tidligere ikke har vært koblet på nett eller har blitt sikkerhetsoppdatert - disse vil i fremtiden kobles på nett og kommunisere med løsninger andre steder for optimalisering. For å sikre integritet og tilgjengelighet på moderne industrielle systemer vil det være avgjørende at det er velfungerende mekanismer rundt tilgangskontroll, autentisering og andre tekniske sikkerhetsmekanismer. For å vurdere hva som er tilstrekkelig nivå av disse, og sørge for at de til enhver tid er på dette nivået, er det helt sentralt å påse at prosesser og etterlevelse er

forankret i god risikoforståelse og håndteres gjennom god risikostyring. Dette er tema for de neste kapitelene i rapporten.

6 Informasjonssikkerhet

Det er tydelig at de aller fleste selskapene i sektoren er avhengig av informasjon og data for å kunne utføre sine operasjoner. Informasjon forekommer muntlig og skriftlig og den både lagres og transporteres av analoge og digitale systemer og løsninger.

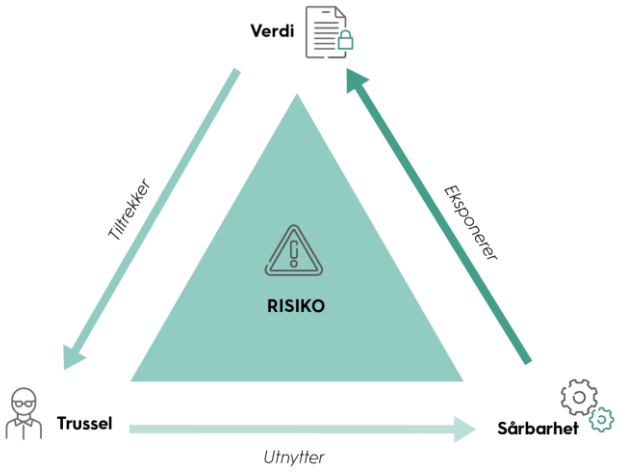
Informasjon og data som inngår i og påvirker alle prosesser, aktiviteter og beslutninger bør sikres på en måte som bidrar til at selskapene oppnår resultatene som eierne og samfunnet forventer. Herunder forventningene om at ulykker ikke skal skje, eller at samfunnet blir påført andre negative eksternaliteter som en konsekvens av sektorens operasjoner.

Data og informasjon har dermed en direkte betydning for selskapenes resultater og regelverksetterlevelse. Det vil si at jo viktigere informasjonen er, jo større kan konsekvensene være på både kort og lang sikt dersom den er feil, ikke er tilgjengelig eller kommer uvedkommende i hende. Som det fremgår av kapittel 4 handler informasjonssikkerhet om å sikre informasjonens

- integritet,
- tilgjengelighet og
- konfidensialitet

Hvilke av disse tre dimensjonene som er viktigst, må balanseres med utgangspunkt i bedriftens og samfunnets behov.

Det er i hovedsak to faktorer som påvirker informasjonssikkerheten; trusler og sårbarheter, se Figur 5. Hvilke tiltak som er hensiktsmessige å implementere for å redusere sårbarhetsnivået, og derigjennom forhindre en trusselaktør i å nå målet, har sammenheng med hvor verdifull informasjonen eller dataene er med hensyn til gevinst- og/eller skade-potensiale, både for informasjonseier, samt for trusselaktører.



Figur 5: Figuren viser faktorene som påvirker informasjonssikkerheten.

Det kan dermed hevdes at uten god oversikt over trusler, sårbarheter og verdier, vil det være svært utfordrende å identifisere hensiktsmessige tiltak og barrierer. Samtidig vil en økende grad av sammenkobling av systemer og løsninger, tettere knytninger mellom IT og OT, mer automatisering og økt grad av digitalisering generelt, bidra til mer komplekse verdikjeder som involverer flere aktører. Det er god grunn til å anta at mer komplekse og sammenkoblede verdikjeder øker sårbarhetsnivået, slik det også fremgår av Lysne-rapporten «Risikostyring i digitale verdikjeder» [2].

Samlet sett kreves det av alle aktørene i verdikjeden å etablere god styring og kontroll på informasjonssikkerhetsområdet. I de påfølgende kapitlene redegjør vi for hva dette innebærer, samt våre observasjoner om status hos aktørene omkring disse temaene.

7 Styring og kontroll

En forutsetning for god informasjonssikkerhet er *styring og kontroll*, som i korte trekk handler om å:

- fastsette mål for selskapet i tråd med eiernes og samfunnets forventninger
- prioritere, planlegge og budsjettere ressursbruk
- følge opp og rapportere resultater og ressursbruk

Det er ledelsen som prioriterer både kortsiktige og langsiktige mål for selskapet med utgangspunkt i styrets og eventuelt samfunnets forventninger. For å kunne følge opp at målene nås, er det nødvendig å etablere mekanismer som gir ledelsen anledning til å vite om dette skjer eller ikke. Det er disse mekanismene som utgjør det man ofte omtaler som styring og kontroll, eller *internkontroll*. For operatørselskapene vil spesielt styringsforskriftens [3] krav til internkontroll og ansvaret knyttet til oppfølging av kontraktører og leverandører være særlig relevant.

Formålet med internkontroll er at ledere på alle nivåer skal ha rimelig trygghet for at målene som er satt blir nådd. Det vil si at alle deler av selskapet gjøres i stand til å [4]:

- nå mål og resultatkrav
- etterleve lover og regler
- ha pålitelig rapportering

Effektiv internkontroll legger til rette for at selskapenes operasjoner blir gjort riktig første gang, og bidrar på denne måten til å forebygge feil, negative hendelser og ulykker. Selskapene oppnår dermed den ønskede kvaliteten og effektiviteten i produkt- og tjenesteleveransene sine. Når arbeidsprosesser og oppgaver gjennomføres på en måte som sikrer ønsket kvalitet, kan ledelsen frigjøres fra brannslukking, feilretting og korrigering.

Internkontrollen bør integreres i så stor grad som mulig i driften, dvs. bygges inn i eksisterende prosesser og aktiviteter på en måte som sørger for systematikk og kvalitet også når systemer, infrastruktur, prosesser og rutiner utsettes for negativ påvirkning. Dette gir en økt trygghet for at selskapets aktiviteter og oppgaver blir utført med forventet kvalitet og i tråd med lover og regler og samfunnets forventninger. Equinors «A-standard Handlingsmønster» er et eksempel på hvor slike prinsipper benyttes i drift.

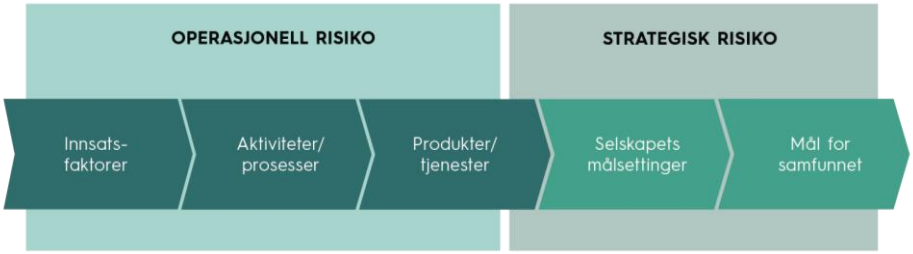
Det er viktig at internkontrollen er tilpasset selskapets størrelse og risikoen det er eksponert for, slik at kontroll og tiltak i størst mulig grad rettes dit behovet er. Dette forutsetter at internkontrollarbeidet er risikobasert, noe som legger til rette for en kostnads- og formålseffektiv balanse mellom ressurser som blir brukt på kontroll og ressurser som blir brukt til andre oppgaver.

Risikobasert internkontroll betinger at ledere på ulike nivåer har tilstrekkelig oversikt over risiko som faller inn under deres ansvarsområder. Med andre ord er det risikoene selskapet bør være opptatt av å identifisere, vurdere og håndtere. På den måten opprettholdes en tilstrekkelig

trygghet for at målene som er satt blir nådd. Dette krever systematikk på operativt nivå. Det er der virksomhetens arbeid utføres, og det er der mulige avvik og konsekvenser kan oppstå.

8 Risiko og risikostyring

Det underliggende premisset for risikostyring er at de fleste bedrifter eksisterer for å gi verdi for sine eiere, og i mange sammenhenger også for samfunnet. I dette ligger det mye usikkerhet, og utfordringen for ledelsen er å avgjøre hvor mye usikkerhet som er akseptabelt på veien mot å møte eiernes og samfunnets forventninger. Usikkerheter innebærer både risiko og muligheter, noe som kan bety tap eller gevinst for selskapet. Risikostyring handler derfor om å håndtere disse usikkerhetene, blant annet gjennom å styre mot strategiske mål og håndtere de operasjonelle risikoene som kan true måloppnåelsen på en kostnadseffektiv måte. Figur 6 illustrerer hvordan risikoer som ligger langt fra ledelsens direkte påvirkning kan true virksomhetens evne til å nå målene. Risikostyring handler derfor om å håndtere disse usikkerhetene, blant annet gjennom å etablere mekanismer og prosesser som bidrar til at potensielt alvorlige operasjonelle risikoer, blir håndtert på en kostnadseffektiv måte.



Figur 6: Risikoer på operativt nivå truer virksomhetens evne til å nå målene sine.

Det må påses tilstrekkelig nivå av kunnskap og kvalitet i risikohåndteringen. Jevnlige, kvalitative vurderinger av risiko bidrar til å gi oversikt over mulige hendelser og konsekvenser, en oppdatert risikoforståelse, og økt kunnskap om risikobildet. Uten denne kunnskapen er det svært utfordrende å ta stilling til hvilke tiltak som skal eller kan iverksettes for å bringe risikoen til et tilfredsstillende nivå.

Godt sikkerhetsarbeid er avhengig av at den forventede sikkerhetstilstanden uttrykkes tydelig og forståelig. Dette er nødvendig for at de ansatte skal kunne forstå hva som forventes av dem og hva som søkes oppnådd. Denne forventningen er det ingen andre enn selskapets eiere og ledelse som kan fastsette. En slik tilnærming understøttes dessuten av både regelverk og standardisering; kravbasert sikkerhetsarbeid viker for en risikobasert tilnærming. Et eksempel på dette er IEC 62443-3-2. Et annet eksempel er sikkerhetsloven og endringene fra gammel sikkerhetslov til ny, som i ny drakt er mer deskriptiv. Det vil si at den stiller større krav til bedriftens egen evne til å identifisere risiko og derigjennom implementere tilstrekkelige tiltak for å håndtere disse. Dette i motsetning til normativt regelverk som går mye lenger i å pålegge spesifikke tiltak som kan oppleves som lite hensiktsmessige for selskapene og virksomhetene det gjelder. For at informasjonssikkerheten skal bli forholdsmessig ivaretatt på denne måten, må selskapene ha interne prosesser som understøtter det. Det vil si at det bør eksistere et system som sikrer at det blir gjennomført sikkerhetsvurderinger på operativt og taktisk nivå, med tilstrekkelig kunnskap i disse prosessene, og at vurderingene blir uttrykt, kommunisert og

forstått godt nok. IEC 62443, inkludert til nå upubliserte deler av denne serien, og ISO 27001 gir en hel del god veiledning til prosesser og systematikk for informasjonssikkerhet.

Som det vises til i kapittel 6 handler informasjonssikkerhet om å beskytte verdier knyttet til informasjon og data mot ulike typer trusler som kan nå disse verdiene gjennom å utnytte sårbarheter i selskapet. Innen petroleumsvirksomheten er det helt nødvendig å se verdiene i relasjon til skade/konsekvenspotensiale og kritikalitet. Dermed forutsetter gode risiko-vurderinger på informasjonssikkerhetsområdet at selskapene har oversikt og kontroll på hvilken og hva slags data/informasjon de behandler og håndterer og hvilken betydning disse har i ulike verdikjeder og systemer. Videre må det foreligge en bevissthet om hvilke menneskelige, teknologiske og organisatoriske sårbarheter som eksisterer eller kan komme til å eksistere, og til slutt bør det kunne gjennomføres vurderinger av trusselbildet. Disse faktorene bør deretter sammenstilles i en helhetlig risikovurdering.

Det finnes ulike metoder for å gjøre dette, men uavhengig av hvilken metode som benyttes, er det avgjørende at roller og ansvar i dette arbeidet er avklart, og at det er integrert med den helhetlige risikostyringen i selskapet. Dette bidrar til at toppledelsen holdes informert om forhold som potensielt kan true de ulike strategiske målsettingene.

8.1 Informasjonsverdier

Som nevnt tidligere er alle bedrifter i alle bransjer avhengig av informasjon i ulike former i sin oppgaveløsning. Med andre ord har informasjon en verdi, ofte målt ved det skadepotensialet det har dersom informasjonen eller data blir utilgjengelig, ikke er korrekt, eller kommer uvedkommende i hende. Informasjon er aktiva for bedriften og bør beskyttes deretter. Kartlegging av dette har dermed stor betydning for hvilke sikringstiltak som bør implementeres, både logiske og fysiske. God oversikt over disse verdiene og hvilket skadepotensial det har for bedriften og samhandlende aktører dersom de går tapt eller på annen måte blir kompromittert, bidrar til bedre utnyttelse av knappe ressurser. Det betyr i denne sammenhengen at sikringstiltak etableres der de trengs, og at disse er dimensjonert riktig. For å kunne avgjøre dette skadepotensialet er det viktig å først identifisere informasjonen og deretter sette den i sammenheng med andre verdier. Det bør også tildeles eierskap og en klassifisering på bakgrunn av verdivurderingen, noe som er hensiktsmessig for å kunne si noe om hvilke krav den enkelte verdi skal være underlagt. Innenfor OT kan det dreie seg om å sette spesifikke sikkerhetskrav for de mest kritiske funksjoner, systemer, soner, kanaler eller signaler. Det kan eksempelvis defineres høyere kritikalitet, som omtalt i NOG123, og/eller settes høyere Security Level Target, som referert i IEC 62443-3-2 / -3-3 og NORSOK I-002:2021.

Det pågår arbeid med IEC 62443-2-2 (konseptet Security Protection Rating, tidligere navngitt som Protection Level) for å kunne definere risikobaserte krav for systemer i drift. Samtidig arbeides det med å harmonisere dette konseptet for operatørselskap («Asset Owners») i IEC 62243-2-1 ED2 og generelt sett for hele denne standardserien gjennom en ny utgave av 62443-1-1. Flere aktører i sektoren ser med stor interesse på disse nye delstandardene. De prøver å

basere en del av arbeidet sitt på prinsipper som finnes tilgjengelig i draft-utgaver av disse dokumentene, og som drøftes i ulike nasjonale fora (som Sintef CDS-forum og NEK NK65). Forventet publiseringsdato i IEC for disse delstandardene er:

- IEC 62443-1-1 ED2: uvisst, er under utvikling i ISA 99.
- IEC 62443-2-1 ED2: mai 2022
- IEC 62443-2-2 ED1: desember 2022

8.1.1 Kartlegging av verdikjeder og gjensidige avhengigheter

Det er altså en viktig forutsetning å ha oversikt over verdiene som inngår i de digitale verdikjedene som på ulike måter understøtter formålet med virksomheten. Dette er også i tråd med Nasjonal sikkerhetsmyndighet (NSM) sine grunnprinsipper for IKT-sikkerhet [5]. Operatør-selskap har som nevnt tidligere også et særskilt ansvar i henhold til styringsforskriften.

Graden av kompleksitet og innbyrdes avhengigheter i slike verdikjeder har en direkte påvirkning på sårbarhetene selskapet er utsatt for. Jo flere avhengigheter, jo større konsekvenser kan en enkeltstående hendelse utløse ved at det oppstår kjedereaksjoner. Jo mer komplekse verdikjedene er, jo mindre oversikt vil en kunne anta at man har over hvor mange aktører som er involvert og hvem som besitter systemansvaret. Hendelser i komplekse verdikjeder kan derfor komme ut av kontroll og føre til at kritiske prosesser stopper opp. Eksempelvis, dersom det innføres funksjoner for prosess-overvåking eller -kontroll som er avhengige av data eller funksjoner i sky, vil det kunne bli store driftsforstyrrelser for operatørselskap og anlegg dersom noen av funksjonens leverandører (eksempelvis leverandører av linjer, datalakes eller SaaS/IaaS-løsninger) utsettes for DDOS-angrep, løsepengevirus eller andre hendelser. Systemer og funksjoners avhengigheter kan være forstått i for liten grad og nødvendig redundans kan være uoversiktlig og usikker (falsk redundans).

8.1.2 Observasjoner og drøfting

For å i det hele tatt kunne gi informasjon en verdi/klassifikasjon, forutsetter det at selskapet har gode prosesser for å identifisere informasjonselementer og deres anvendelse.

Hos de fleste informantene synes dette å være utfordrende, men vi ser at enkelte har bedre kontroll på disse prosessene enn andre. Utfordringen er dermed at det er noe ulik praksis for hvordan selskapene utfører og dokumenterer verdivurderinger av informasjonen disse forvalter og benytter. I forlengelsen av dette er det derfor sannsynlig at menneskelige, teknologiske og organisatoriske sikringstiltak ikke er godt nok tilpasset behovet. I en del tilfeller vil disse antakelig være for inngripende og kostbare, mens i andre er de for svake.

Det er relativt stor variasjon i hvorvidt informasjon blir klassifisert eller ikke hos informantene. Dette henger sammen med utfordringer knyttet til selve verdivurderingen og hvem som skal gjennomføre disse, som igjen har sin årsak i at det er krevende å knytte eierskap til en stadig voksende og kompleks mengde av data og informasjon, og at det kan være utfordrende å forstå ny teknologi og nye systemer. De fleste informantene har etablert en god forståelse for at informasjonseierskap bør tildeles, men det er ingen av dem som har en entydig formening

om hvordan dette gjøres godt i praksis. Svarene vi får er at dette i mange tilfeller er for komplekst og for tidkrevende.

At det er komplekst og tidkrevende, er vi enige i. På et aggregert nivå bør det ikke være utfordrende å knytte eierskap til informasjon, men straks modeller, tabeller, tegninger osv. blir beriket med ny informasjon, blir det mer komplekst. Hvem eier databasen og hvem eier ulike tabeller, views, relasjoner og informasjonsobjekter som inngår i den? Dette er utfordringer ikke bare petroleumssektoren står overfor; dette er en klassisk problemstilling på tvers av sektorer og noe som blir forsøkt adressert i flere ulike regelverk.

Som eksempel kan personopplysningsloven nevnes, som klart skiller mellom «behandlingsansvarlig» og «databehandler», der førstnevnte på mange måter kan sidestilles med begrepet *informasjonseier*. *Databehandleren* gjør som navnet tilsier: behandler data og informasjon på vegne av den ansvarlige. Følgelig må det eksistere et sett krav og kriterier som må være oppfylt for at slik behandling kan finne sted. Disse kravene og kriteriene følger mer eller mindre direkte av regelverket, og det skal foreligge avtale mellom behandlingsansvarlig og databehandler, en databehandleravtale, der dette kommer frem.

Prinsippene som følger av dette, bør også kunne benyttes på informasjon som ikke nødvendigvis er å regne som personopplysninger. Altså at informasjonseier er den som bærer risikoen dersom informasjon eller data blir kompromittert, blir borte eller ikke lenger kan stoles på. I en verdikjede vil dette trolig være den samme rollen, dvs. den som er ansvarlig for resultatene innenfor det området der informasjonsverdiene og dataene har størst betydning, eller kan medføre størst konsekvens ved kompromittering. Altså er det prosesseier som eier informasjonen ettersom verdikjeden understøtter prosessen. Dette er i tråd med Styringsforskriften med hensyn til ansvaret som påligger operatørselskap. Dette resonnementet løser imidlertid ikke det faktum at det kan være mange prosesseiere (aktører, operatører) som blir påvirket av at ett informasjonselement blir kompromittert. Dette er en kompleks utfordring som vi vet er tilstedeværende, men denne rapporten svarer ikke på den direkte. Vi anbefaler derfor petroleumssektoren å utrede dette nærmere i samarbeid med akademia, andre sektorer, tilsynsorganer (eksempelvis NSM), og myndigheter. I disse utredningene bør det etter vår oppfatning trekkes inn kunnskap og erfaringer som er gjort fra andre sektorer, også internasjonalt, som også behandler data som kan få store konsekvenser ved kompromittering.

Det bør trekkes kunnskap, prinsipper og erfaringer fra IEC 62443-3-2. Den gir interessante vurderinger og argumentasjon for konsekvensdrevet risikovurdering, samt fokus på vurderinger av worst-case og risiko for essensielle funksjoner. Idaho National Lab sin modell for Consequence-Driven Cyberinformed Engineering (CCE) ble også omtalt av noen av informantene og blir ofte trukket frem i ulike internasjonale fora. TR.84.00.09 omtaler også konsekvensdrevet risikovurdering. Andre rammeverk vi ser som interessante og relevante å hente kunnskap og prinsipper fra i forbindelse med risikostyring og verdier:

- STPA-Sec

- MITRE Mission Assurance Engineering
- Cyber Terrain Mission Mapping

8.2 Sårbarheter

Sårbarheter er i sikkerhetssammenheng de svakheter som gjør det mulig for en trussel eller trusselaktør å kompromittere integriteten, konfidensialiteten og/eller tilgjengeligheten på verdiene i en virksomhet. Det er derfor viktig å ha kunnskap om sårbarheter for å avdekke hvilke svakheter som muliggjør at skader kan inntreffe. Kunnskap om sårbarheter er helt vesentlig for å kunne se hele risikobildet for både selskapet, og for sektoren.

Det finnes mange ulike sårbarheter i digital teknologi. Noen av de mest typiske for OT og industrielle kontrollsystemer, er sårbarheter knyttet til fjerntilganger, feil installert/ konfigurert programvare, bruk av standard passord, åpne protokoller, feil installert utstyr som brannmurer, porter og tjenester som er åpne for utsiden, operativsystem som ikke er oppdatert med nyeste oppdateringer, mv.

De ulike sårbarhetene deles normalt inn i ulike kategorier ut ifra dens årsak:

- **Menneskelige sårbarheter:** Svakheter direkte knyttet til mennesket og dets handling. Eksempelvis manglende kunnskap, menneskelige feil i behandling/analyse av data, hastverk og uvaner, begrenset rasjonalitet og kognitive tilbøyeligheter/bias.

- **Tekniske og fysiske sårbarheter:** Svakheter knyttet til teknologi og fysiske objekter. Eksempler på tekniske og fysiske sårbarheter kan være utilstrekkelig konfigurasjon av tilganger, dårlig nettverkskonfigurasjon, programvarefeil, åpne protokoller, feilinstallert utstyr, svakheter i utstyr, utdatert programvare og operativsystem som ikke er oppdatert.

- **Organisatoriske sårbarheter:** Svakheter knyttet til organisasjonen og virksomheten. Eksempelvis dårlig sikkerhetskultur som muliggjør menneskelige feil, mangelfull kunnskapsutvikling og bevisstgjøring, manglende oppfølging på ledernivå, mangel på retningslinjer og definerte prosesser for utbedringer av tekniske sårbarheter, svakheter i tilgangsstyringsprosesser, mangelfull organisatorisk innsikt i verdier/sårbarheter/trusler, mangelfull bakgrunnssjekk av ansatte fra andre land vi ikke har et sikkerhetspolitisk samarbeid med, fragmentert kommunikasjon og mangelfull internkontroll.

Flere av disse sårbarhetene, eksempelvis manglende kunnskap, mangel på retningslinjer, mangelfull organisatorisk innsikt i verdier/sårbarheter/trusler og mangelfull internkontroll, kan føre til Open Source Intelligence-hendelser (OSINT). Dette dreier seg om informasjon som trusselaktører kan finne i åpne kilder, typisk på internett, og hvor deling av informasjon i en sammenheng kan avsløre sårbarheter som en trusselaktør kan utnytte.

8.2.1 Observasjoner og drøfting

En rekke leverandører har valgt å publisere identifiserte sårbarheter i egne løsninger overfor sine kunder, i tillegg til at denne informasjonen gjøres offentlig tilgjengelig. Dette er imidlertid ikke tilfelle for alle aktører. Noen publiserer ikke informasjon om sårbarheter, men velger å være mer lukket rundt dette og håndtering av det i egne løsninger. For dem det gjelder, kan det tyde på at evnene til å identifisere og kommunisere sårbarheter er svake. Dette har sannsynligvis sammenheng med blant annet mangelen på kunnskap om sårbarheter og manglende evne til å se viktigheten av kunnskapsdeling.

En annen problemstilling relatert til sårbarheter er at det heller ikke er uvanlig at nokså enkle tekniske sårbarheter blir identifisert og kommunisert, men at rotårsakene til disse ikke adresseres tilstrekkelig. Derfor er det grunn til å anta at mer alvorlige sårbarheter ikke blir identifisert og adressert. Igjen handler dette om manglende kunnskap, samt ressursknapphet på fagfolk.

Flere av informantene viser at de har forståelse for ulike sårbarheter som er aktuelle for sektoren. Det er imidlertid stor forskjell på hva de ulike aktørene vurderer som sentrale sårbarheter. Informantene nevner blant annet følgende:

Menneskelige svakheter:

- Manglende forståelse av anlegg og for prosesser
- Manglende forståelse av trusselbilde, sårbarheter og for angrepsvektorer
- Manglende kompetanse tilknyttet informasjonssikkerhet/cybersikkerhet
- Manglende kjennskap til krav og retningslinjer
- Manglende kunnskap om hvordan man utfører arbeidsoppgaver på en sikker måte.

Teknologiske svakheter:

- Tilgangskontroll og problemer med å ha full oversikt over alle enheter i infrastrukturen, verdikjedeproblematikk
- IoT-enheter som er eksponert mot internett
- Manglende oversikt og/eller kontroll over grensesnitt/kommunikasjonskanaler på tvers av nettverk
- OT-komponenter er ikke designet for å ivareta krav til cyber- og informasjonssikkerhet
- Utdaterte operativsystemer i OT-komponenter
- Avhengigheter til andre komponenter
- Manglende eller ikke aktivert tofaktor-autentisering
- Feil i tilgangsstyring og manglende opprydding av tilganger
- Manglende herding av systemer
- Manglende oppdateringer av systemer, End-of-Life, og liknende

Organisatoriske svakheter:

- Forskjellige ansvarsområder innenfor landskapet, ikke klart definert ansvarsområder innen cyber- og informasjonssikkerhet
- Mangelfulle krav til informasjonssikkerhet

I flere av intervjuene ble OSINT nevnt. Noen av kildene som ble omtalt i intervjuene var LinkedIn, Facebook, Shodan, nyhetsartikler og pressemeldinger, VirusTotal (og programvare lastet opp til dette nettstedet), presentasjoner fra konferanser og seminarer o.l., samt lister med brukernavn, passord mv. fra digitale innbrudd.

De fleste informantene har kjennskap til sensitiv informasjon om deres virksomhet som utilsiktet har vært tilgjengelig i åpne kilder. Selskapene gjør reaktive tiltak for å fjerne slik informasjon, og brorparten av dem virket også å ha proaktive prosesser for å hindre utilsiktet deling av sensitiv informasjon til åpne kilder. Det gjennomføres bevisstgjøringskampanjer og kartlegging av informasjon på åpne kilder, og enkelte selskap foretar også kartlegginger på det mørke nettet. Derimot forteller informantene at det kan være utfordrende å vurdere hvilken grad av informasjon om sårbarheter som kan utledes av den voksende mengden med selskaps-spesifikk informasjon som er tilgjengelig i åpne kilder. Brukernavn, passord og IP-adresser ansees i de fleste tilfeller som informasjon som skal håndteres konfidensielt. Det diskuteres hvorvidt topologi-tegninger, SCD og P&ID etc. bør håndteres konfidensielt, men det er ikke konsensus om dette. I denne diskusjonen ligger det eksempelvis utfordringer med at ikke-sensitiv informasjon i dag kan bli vurdert som sensitiv informasjon i fremtiden, samt at for streng håndtering av informasjonsdeling skaper utfordringer rundt samarbeid, kunnskapsutvikling og resultatoppnåelse for selskapene og for sektoren som helhet.

Fra intervjuene fremkommer det også ulike måter aktørene avdekker sårbarheter på; fra reaktivt/ad-hoc til mer proaktivt og systematisk. For de menneskelige sårbarhetene benyttes det gjerne intern trening og testing på phishingangrep, oppfølging og kartlegginger/ granskninger etter uønskede hendelser. Et selskap forteller at det gjennomføres årlige øvelser på store hendelser der hele beredskapsapparatet involveres, samt øvelser på enkeltanlegg. For de organisatoriske sårbarhetene oppgis det at det benyttes eksterne og interne vurderinger, risikovurderinger og at det etableres styringssystem for informasjonssikkerhet (ISMS). For de som allerede har et styringssystem, oppdateres og følges dette opp. For de tekniske sårbarhetene utføres det blant annet kartlegging (scanning) for identifisering av sårbarheter på endepunkter, ulike former for testing, slik som kodetesting og gjennomgang, og penetrasjonstesting. Det benyttes også ulike sensorer for å fange opp tekniske sårbarheter i digital infrastruktur. Det innhentes videre informasjon om tekniske sårbarheter fra blant annet NCSC og KraftCERT.

For de menneskelige sårbarhetene fremkommer det at det er ulike parter som er involverte i å avdekke og få innsikt i disse. Opplæringsmateriell lages av spesialistmiljøene og ledelsen har ansvar for å sikre at de ansatte har tilstrekkelig med kompetanse og kunnskap. For de tekniske sårbarhetene involveres både sikkerhetsteam, driftsleverandører, spesialistmiljøer innen cyber- og informasjonssikkerhet og risikoeiere for å avdekke disse sårbarhetene. Det opplyses om at

de som involveres i de organisatoriske tiltakene ofte er spesialister innenfor området eller eiere av prosesser og krav.

Samlet oppgir informantene mange relevante og sentrale sårbarheter innenfor cyber- og informasjonssikkerhet. Vi sitter likevel med et inntrykk av at sårbarhetene gjerne blir en oppramsing fra lærebøkene og at det kan være mangel på god kompetanse på dette området, og spesielt innenfor noen av sårbarhetskategoriene. Det kommer også tydelig frem fra alle informantene at det største fokuset er på de tekniske sårbarhetene i digitale systemer. Det virker å være denne kategorien av sårbarheter de fleste har mest kunnskap om, både i form av hvilke sårbarheter de mener er sentrale sårbarheter og metoder som benyttes for å avdekke slike sårbarheter. Det er generelt lite fokus på menneskelige og organisatoriske sårbarheter. Vi opplever også at det er for lite fokus på ikke-digitale, tekniske sårbarheter som bør ses i sammenheng med digitale sårbarheter. Med dette mener vi eksempelvis svakheter eller begrensninger i anleggsdimensjonering, design/filosofi i prosesskontroll og safety-systemer og eventuelle feil i Cause & Effect-logikk. Dette er en indikasjon på at det kan være manglende kompetanse og bevissthet i sektoren. Lange verdikjeder, komplekse systemer og usikkerhet knyttet til uavhengighet mellom barrierer gir også et mer uoversiktlig bilde av relevante sårbarheter.

En er avhengig av å ha et oversiktlig bilde av systemene og arkitekturen for å kunne kartlegge verdiene og sårbarhetene som trusselaktører kan utnytte. Uten god nok oversikt over, og kompetanse om, sentrale sårbarheter og kjeder av sårbarheter, samt et etablert ansvar for oppfølging og håndtering av sårbarhetene, er det vanskelig å se hele risikobildet.

Det ville hjulpet flere av aktørene i å avdekke, kommunisere og håndtere sårbarheter dersom de hadde hatt tilgang til en mer omforent bransjestandard. Forskriftene, NoG-dokumenter, NORSOK-standarder og NSMs Grunnprinsipper for IKT-sikkerhet dekker ikke dette tilstrekkelig i dag. IEC 62443 og DNV-GL-RP-G108 er etter vår mening gode underlag for å kunne skape en mer omforent bransjestandard fremover.

Det ville også vært en styrke om olje- og gassektoren hadde hatt en tydeligere felles plattform eller kanal for å kunne dele informasjon og kunnskap om sårbarheter, som for eksempel KraftCERT. Det er spesielt viktig at man deler informasjon om sårbarheter med hverandre i verdikjeden. En sårbarhet langt oppe eller langt nede i verdikjeden kan få like store, om ikke større, konsekvenser i den andre enden av kjeden dersom sårbarheten forblir uoppdaget og ikke håndtert eller kommunisert over lengre tid. Angrepet mot SolarWinds er et godt eksempel på dette. For en mer utfyllende beskrivelse av SolarWinds-hendelsen, se Vedlegg 1.

8.3 Trusler

Å definere trusselbildet innenfor informasjons- og cybersikkerhet er ikke en enkel matematisk øvelse. Mange forsøker å kvantifisere risiko gjennom å tallfeste konsekvens og sannsynlighet forbundet med en uønsket hendelse. Slik kvantifisering kan være nyttig i forbindelse med sammenlikning mot akseptkriterier og prioritering av risikoer som det må gjøres tiltak på. Et

kvantifisert bilde av risiko gir imidlertid en betydelig forenklet representasjon av risikobildet. Det kan også gi inntrykk av at trusselbildet er forstått tilstrekkelig, gjennom en presisjon i tall, mens risikoen i realiteten kan spenne over et stort spekter, være knyttet til høy grad av usikkerhet og/eller basert på svært mangelfull data, lite historiske data eller svak kunnskap/ekspertise. Petroleumssektoren har store utfordringer med å få overblikk over svakheter, avhengigheter og skadepotensiale, og det er derfor mange kvalitative aspekter som ikke lar seg omsette til tall med et tilstrekkelig presisjonsnivå eller som egner seg for å kommunisere forståelig om risiko. For å forstå trusselbildet kan det derfor være hensiktsmessig å se på relevante hendelser og angrep, både tilsiktede og utilsiktede, og utfra dette få et bilde på hva som har vært mulig tidligere, hva som er mulig nå, og hva som kan bli mulig i fremtiden.

Det er et sammensatt trusselbilde som næringen står overfor. Aktuelle trusler for petroleumssektoren kan være teknologisk avanserte, og trusselaktørene kan besitte store ressurser ved at de i en del tilfeller har hele nasjonalstater i ryggen. Deres motivasjon kan være svært ulik, fra grupper som ønsker å påføre sektoren økonomiske og omdømmemessige tap, til avanserte aktører som jobber med å profittere på militær- og/eller industrispionasje, og kanskje kun vil posisjonere seg for en fremtidig situasjon med større geopolitisk uro. Dette trusselbildet er også gjeldende på tvers av sektorer og bransjer. Trusselaktører for industrielle kontrollsystemer kan for øvrig være alt fra individuelle angripere og aktivister til organiserte kriminelle grupper eller terror-relaterte grupper.

8.3.1 Tilsiktede og utilsiktede hendelser

Villede og tilsiktede hendelser, med ondsinnede aktører bak, er noe som gjør trusselbildet ytterligere komplisert å vurdere. En villet, ondsinnet aktør vil kunne utnytte det som måtte finnes av svakheter på tvers av menneske, teknologi og organisasjon, på tvers av systemer, og vil også kunne skape nye svakheter gjennom sine systematiske, målrettede handlinger. Hvilke handlinger en trusselaktør kan utføre, kan være umulig å forutse. Historiske hendelser og frekvens kan vise til trender og utvikling, men vil ikke eksakt kunne brukes til å beregne hvem som blir angrepet, hvordan det gjøres, hvor det gjøres, hvor ofte eller hva trusselaktøren er på jakt etter. Eksempler på tilsiktede hendelser vi ser har en økende trend og forekommer hyppigere, er løsepengevirus, leverandørkjedeangrep og Ransom-DDoS-angrep («rDDoS»). I tillegg har vi utilsiktede hendelser som kan oppstå både gjennom menneskelige feil og naturlige hendelser. Noen eksempler på relevante hendelser og angrep er listet opp under. For en mer utfyllende beskrivelse av hendelsene, se Vedlegg 1.

- **Triton/TRISIS** var et avansert, komplekst og tilsiktet angrep i 2017 som gjorde endringer/sabotasje i instrumenterte sikkerhetssystemer (SIS).
- **Ekans** var et løsepengevirus som ble detektert i 2019 og som hadde ICS-spesifikke mål og egenskaper for å stoppe ICS-prosesser.
- **Colonial pipeline,** et av USAs største rørledningssystem for transport av raffinerte oljeprodukt, ble i 2021 utsatt for et løsepengevirus som resulterte i massive utfordringer i deres distribusjon.

- **Telenor** ble i 2020 rammet av et Ransom-DDoS-angrep som krevde løsepenger for å ikke utsette de for ytterligere angrep.
- **SolarWinds** ble i 2020 utsatt for et leverandørkjedeangrep. Flere store aktører benytter seg av tjenesten deres, Orion, herunder det amerikanske finansdepartementet, Microsoft, samt flere kunder i Norge, også innen petroleumssektoren. Hundrevis av selskaper over store deler av verden ble utsatt for dette indirekte angrepet.
- **Kaseya** ble i 2021 utsatt for et leverandørkjedeangrep som påvirket blant annet Coop i Sverige og medførte at de måtte stenge flere av sine butikker i en periode.
- **Raffineriet på Mongstad** ble i 2014 utsatt for en utilsiktet hendelse som resulterte i at de måtte gå over til manuell lasting og et tap på 200 000-300 000 kr for Equinor (tidligere Statoil).

8.3.2 Åpne trusselvurderinger for 2021

Norges etterretnings- og sikkerhetstjenester publiserer hvert år sine åpne trusselvurderinger. Nedenfor har vi sammenstilt de viktigste elementene fra hver av disse for 2021.

Politiets Sikkerhetstjeneste (PST) legger hovedvekt på tre trusler i sin trusselvurdering for 2021; statlig etterretningsvirksomhet, politisk motivert vold, og trusselen mot myndighetspersoner. For petroleumssektoren utpeker statlig etterretning seg. Motivasjonen er informasjonsinnhenting og beslutningspåvirkning. Det forventes at fremmede staters etterretningstjenester vil gjennomføre kartlegging av norsk infrastruktur, i tillegg til å rekruttere kilder. Det vises spesifikt til at virksomheter innen petroleumssektoren bør være forberedt på forsøk på stjeling av informasjon. I tillegg er det interesse for fysiske og digitale smartby-løsninger som kan gi en detaljert oversikt over Norges kritiske infrastruktur. Oppkjøp og investeringer i næringslivet, utnyttelse av akademia til ulovlig kunnskapsoverføringer, og overvåkning av dissidenter og flyktninger som er i Norge blir oppgitt. [6]

I Nasjonal Sikkerhetsmyndighet (NSM) sin rapport «Nasjonalt digitalt risikobilde 2021» beskriver NSM hvilke typer digitale hendelser som rammer de norske virksomhetene og konsekvensen av disse for den felles digitale sikkerheten. I rapporten belyses problemet med lange verdi- og leverandørkjeder som bidrar til at det blir vanskeligere å ha oversikt over sårbarhetene som kan utnyttes av trusselaktører gjennom blant annet et leverandørkjede-angrep. NSM peker på at for å motstå uønskede digitale hendelser er ikke implementering av tekniske tiltak alene tilstrekkelig, men vil sammen med menneskelige og prosessuelle tiltak bidra til å redusere risikoen. Digital sikkerhet er et lederansvar der virksomheten og ledelsen alltid har ansvaret for sikring av egne verdier, hvor risikovurderinger og risikohåndtering er helt nødvendig for å oppnå et forsvarlig sikkerhetsnivå i virksomheten. NSM trekker også frem viktigheten av åpenhet rundt hendelser og informasjonsdeling fordi det fører til en økt bevisstgjøring generelt i samfunnet. [7]

Etterretningstjenesten (E-tjenesten) legger vekt på stormaktrivalisering, terrorisme og digitale trusler i sin rapport «Fokus 2021». Tjenesten skriver at «utenlandsk etterretnings- og påvirkningsaktivitet forblir en betydelig trussel mot Norge og norske interesser.»

Primærtrusselen i det digitale rom er spionasje fra statlige aktører. I forbindelse med digitale trusler som nevnes i rapporten, skriver tjenesten at nettverksoperasjoner benyttes både til etterretning og destruktive operasjoner som sabotasje. I tillegg til dette ser man påvirkningsoperasjoner som har som formål å påvirke valg, politiske prosesser og spredning av desinformasjon. Etterretningsoperasjoner for å hente ut informasjon foregår innenfor forsvarssektoren, i sikkerhets- og utenrikspolitikken, samt innen helse- og energisektorene. Aktører i norsk industri som forvalter informasjon innenfor blant annet norsk energi-, olje-, og gassektor er nevnt som mål for russiske aktører. [8]

8.3.3 Observasjoner og drøfting

Sektoren er til dels bevisst og klar over de beskrevne truslene og hendelsene. Likevel kan vi ikke trekke slutningen at strategiske og operasjonelle valg er basert på denne bevisstheten og at kunnskapen anvendes tilstrekkelig ved sikring av industrielle kontrollsystemer og tilhørende data i ro og i transit. Fra et bedriftsøkonomisk ståsted er det åpenbart at industrispionasje vil kunne få alvorlige økonomiske skadefølger. Tilsvarende vil statlig etterretningsvirksomhet i sektoren kunne påføre samfunnet store tap som ikke nødvendigvis vil være synlige i selskapenes balanse- og resultatoppstillinger på kort sikt. Likevel ser det ikke ut til at aktørene har tilstrekkelig gode mekanismer for styring, internkontroll og internkommunikasjon for å avdekke og forhindre slike trusler i stor nok grad. Potensiale for sabotasje og terror-rettede angrep gjennom digital teknologi har enda mindre fokus. Dette gjelder blant annet i leverandørforhold, tilgangsstyring og -rettigheter, klassifisering av informasjon og verdier, manglende kontroll på verdikjedene og mangelfull endringskontroll på digitale verdikjeder og løsninger. Det gis inntrykk av at et trusselbilde med utenlandske og statlige trusselaktører blir for stort og komplekst for virksomhetene. Samtidig argumenteres det med at det er lav sannsynlighet for slike trusler. Vi stiller spørsmålstegn ved denne argumentasjonen basert på trenden vi ser knyttet til hendelser internasjonalt, hva vi ser av hendelser selv, hva vi uformelt får innblikk i, samt faktumet at sannsynlighetsvurderinger innenfor cyberangrep er en svært vanskelig og kompleks oppgave som selv de beste etterretningsorganer ser ut til å ha utfordringer med.

Samlet er dette en indikasjon på kunnskapsmangel og ressursknapphet på fagfolk innenfor dette feltet. Både PST og E-tjenesten trekker i sine åpne trusselvurderinger for 2021 frem at vi vil se stadig mer av utenlandske og statlige aktører i årene fremover. Det er derfor viktig at virksomhetene er bevisste på disse og innehar nok kunnskap og kompetanse til å kunne håndtere og beskytte seg mot disse sentrale trusselaktørene. Dermed er det utilstrekkelig å kun implementere flere tekniske tiltak slik det også påpekes i NSM sin rapport for «Nasjonalt digitalt risikobilde 2021». Virksomhetene må også ha på plass de menneskelige og organisatoriske tiltakene for å redusere risikoene som trusselaktørene representerer. For at digitaliseringen og økt grad av automatisering skal kunne gi de forventede gevinstene som ligger til grunn for de strategiske valgene som aktørene har tatt, krever det kunnskap og bevissthet om disse temaene, og god styring og god kontroll på informasjonssikkerhets-arbeidet.

Både tilsiktede og utilsiktede hendelser kan i større grad unngås ved tilstrekkelig kunnskap om trusler og det helhetlige trusselbildet. I tillegg er kontinuerlig arbeid med å kartlegge trusler sentralt for å redusere risikoene knyttet til hendelser. En viktig faktor for å lykkes med dette arbeidet er å kommunisere på en god måte og å være mer åpne om trusler og sårbarheter på tvers i sektoren, på tvers av flere sektorer og mellom selskaper og myndigheter.

Dette synes imidlertid å være en relativt stor utfordring p.t. Det påpekes av flere informanter at det er vanskelig å finne god informasjon om sårbarheter og trusler for OT, generelt for energi-, olje- og gassektoren og for industrielle kontrollsystemer. Selv om flere av intervju-objektene har partnerskap, abonnement eller tilegner seg informasjon om trusselbildet og hendelser gjennom blant annet NSM, KraftCERT og NCSC, gir ikke dette nok informasjon, da mye av informasjonen rundt hendelser og sårbarheter kun deles i begrenset grad eller er konfidensiell eller gradert. Informasjon rundt hendelser er dessuten gjerne kompleks og innehar en del usikkerhet. Derfor er det utfordrende å kommunisere dette klart, tydelig, omforent og forståelig. Selv om budskapet virker tydelig fra avsenderens side, trenger det ikke å bli forstått riktig av mottaker. Således oppstår store utfordringer i kommunikasjonen internt i selskapene, mellom selskapene, på tvers av sektorer, og overfor myndigheter. Med henblikk på DIKW-modellen omtalt i kapittel 4 blir data således ikke til god informasjon, og det skapes verken kunnskap eller visdom.

Vi ser samme kommunikasjonsutfordring både når det gjelder trusselbilde, sårbarheter, verdier og når det gjelder konsekvenspotensiale. Selskapene har ulike fagmiljøer, ulike perspektiver og meninger, og kommunikasjon mellom dem foregår i en del tilfeller formelt og gjennom linjevei. Gjennom disse kanalene og transportetappene er det sannsynlig at informasjonen blir uklar, usikker, fraværende, ufullstendig og misforstått. Dette kan skyldes at informasjon ikke blir formidlet mellom aktører, at det oppstår feil i informasjonen som blir utvekslet, at ikke all informasjon blir overført eller at informasjonen som gis blir misforstått av mottakeren [9]. En står dermed igjen med informasjon som isolert sett ikke gir økt forståelse og dermed blir beslutningsgrunnlaget utilstrekkelig. Dette kommunikasjonsgapet ses tydelig mellom fagfolk på IT på den ene siden og fagfolk på OT/automasjon på den andre. De er gjerne i forskjellige forretningsområder, og dermed mange organisatoriske ledd fra hverandre. IT kan mye om sårbarheter i digitale systemer og trusselbilde, mens OT kan mye om det fysiske konsekvenspotensialet. For kunnskap om sårbarheter, trusselbilde og konsekvenser står de på hver sin side i bedriften, med hvert sitt stammespråk, med mangelfull, fragmentert informasjon, og har store utfordringer med å forene deres felles data/informasjon til kunnskap og visdom for virksomheten.

9 Ledelsessystem for informasjonssikkerhet (ISMS)

Informasjonssikkerhet er bare ett av mange områder som krever styring og kontroll. Som tidligere nevnt i denne rapporten, handler det om å etablere strukturer og prosesser som gjør selskapene i stand til å identifisere informasjon og data, kartlegge sårbarheter, samt kunne få oversikt over hvilke trusler som til enhver tid kan være aktuelle. De bedriftene og organisasjonene som jobber systematisk med informasjonssikkerhet, herunder jobber risikobasert, klarer i større grad å iverksette kostnadseffektive tiltak der de trengs for å forhindre uønskede hendelser, eller for å redusere omfang og konsekvens av slike. Gevinstene er bedre håndtering av hendelser og raskere gjenoppretting til normaltilstand hvis det først går galt. Godt sikkerhetsarbeid må derfor være kostnadseffektivt. Dette krever styring, og god styring innebærer at:

- roller og ansvar i organisasjonen er definert, tydeliggjort og entydig forstått
- prosesser for risikostyring er etablert og at de riktige rollene vurderer og håndterer identifisert risiko i tråd med vedtatte kriterier
- det eksisterer mekanismer som sikrer oppfølging og kontroll av at sikkerhetskrav etterleves

En systematisk og risikobasert tilnærming til informasjonssikkerhet forutsetter normalt et ledelsessystem for informasjonssikkerhet (ISMS). Et ISMS er for informasjonssikkerhet det et kvalitetssystem er for selskapets øvrige produkter og tjenester; et rammeverk som beskriver minimumskrav til selskapets arbeid med informasjonssikkerhet. Dette rammeverket bør være forankret i toppledelsen og forvaltes av en informasjonssikkerhetsleder eller tilsvarende rolle. For operatørselskaper må deres rammeverk og krav også være i tråd med det ekstra ansvaret som er gitt dem gjennom Styringsforskriften. Gjennom å stille overordnede krav innenfor en rekke områder som påvirker både horisontale og vertikale arbeidsprosesser og -aktiviteter, vil bedriften kunne være i stand til å avdekke og forhindre informasjonssikkerhetshendelser, samt å raskere gjenopprette til normaltilstand dersom hendelser først inntreffer. Det overordnede formålet er hele tiden å kunne sikre informasjonsverdiene slik at kravene til integritet, konfidensialitet og tilgjengelighet blir identifisert, balansert og ivaretatt.

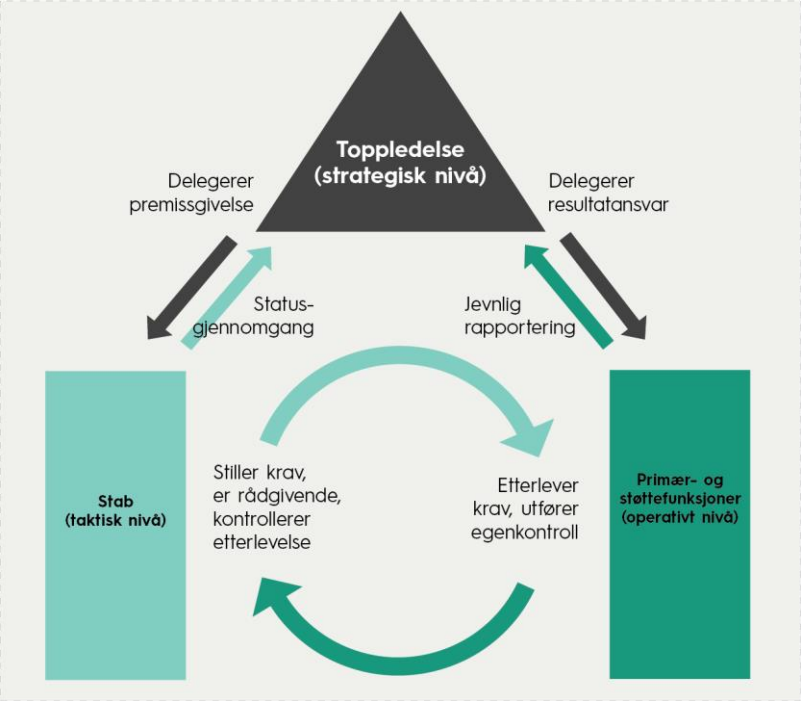
Uten struktur og internkontroll, vil de færreste virksomheter være i stand til å få oversikt over alle verdikjeder og prosesser som ulik informasjon passerer gjennom og påvirker. Enda mindre oversikt vil en ha over organisatoriske, menneskelige og teknologiske sårbarheter. Mangelfull struktur, risikostyring og kontroll innebærer at utviklingsprosjekter og andre digitaliserings-initiativer heller ikke støtter opp om og ivaretar de reelle virksomhetsbehovene. Altså er det stor fare for at gevinstene ikke realiseres.

Et styringssystem for informasjonssikkerhet, basert på anerkjente standarder som eksempelvis NS-ISO/IEC 27001, er et viktig virkemiddel for å kunne oppnå slik styring og kontroll.

9.1 Organisering av sikkerhetsarbeidet

En annen vesentlig komponent i alt internkontrollarbeid, herunder på informasjonssikkerhets-området, er organisering. Det kan argumenteres for at uten tilfredsstillende organisering, er det heller ikke mulig å etablere tilstrekkelig internkontroll. Det vil si at det er tydelige rammer for hvilke roller som har beslutningsmyndighet for hva, og at dette særlig sees i sammenheng med hvem som eier risiko.

Det er alltid styret ved styreleder som er overordnet ansvarlig for selskapets resultater. Dette ansvaret delegeres normalt til en daglig leder som på vegne av styret sørger for at bedriften oppnår de resultatene som eierne forutsetter. Dermed er det daglig leder som i all hovedsak har fått delegert selskapets risikoer, men det er lite hensiktsmessig at alle beslutninger går via topp-leder. Stort sett løses dette gjennom at ulike deler av selskapets samlede risiko-portefølje delegeres nedover i linjen til de rollene som er utpekt som resultatansvarlige innenfor sine områder. Disse eier informasjonen som understøtter forretnings-prosessene som de er ansvar-lige for. Samtidig er det ikke nødvendigvis slik at hver enkelt resultatansvarlig har nok kompetanse eller innsikt til å stille adekvate informasjons-sikkerhetskrav, ei heller at disse er i tråd med toppledelsens krav og forventninger. Dermed bør denne kravstillelsen ha sitt utgangspunkt i en stabsfunksjon eller tilsvarende, ikke ulikt måten de fleste aktører i oljebransjen organiserer HMS-arbeidet.



Figur 7: Separasjon av roller, rollenes ansvar og forholdet mellom dem.

Denne kravstillelsen bør delegeres til noen med god sikkerhets-, forretnings- og internkontrollkompetanse som formulerer premissgivelsen gjennom å støtte og følge opp sikkerhetsarbeidet, og ha tett dialog med toppledelsen om risikonivå. En slik rolle er normalt en informasjonssikkerhetsleder, eller CISO. Toppledelsen bør være tydelig i sin kommunikasjon på at CISOs rolle er å fastsette og uttrykke sikkerhetsbehov på deres vegne, og at CISOs viktigste oppgaver er dette, samt å følge opp at sikkerhetstilstanden er i tråd med ledelsens forventninger.

Det springende elementet er uansett å sørge for rolleseparasjon, det vil si at det eksisterer et skille mellom kravstiller og de som utfører de daglige operasjonene slik figur 7 viser. Disse prinsippene er like gyldige innen informasjonssikkerhet som det er innen andre internkontroll-områder, og denne typen rolleseparasjon bidrar til at ledelsen oppnår to ting:

- jevnlig status fra linjen gjennom regelmessig risikorapportering, som kan sammen-holdes med
- periodevis og uhildet status fra premissgiver

En slik organisering reduserer sannsynligheten for at kravstiller havner i uheldige dobbeltroller. Rollen rendyrkes dermed som premissgivende, kontrollerende og rådgivende. De resultatansvarlige, dvs. de som eier risiko og informasjon, vil på sin side kunne konsentrere seg om å tilpasse og justere prosesser og aktiviteter slik at identifiserte sårbarheter blir redusert på beste mulige måte i tråd med forretningsbehovene og de kravene som måtte fremgå av styringssystemet ellers.

IT kjenner IT best, og IT blir målt på IT. Ved å organisere premissgivelsen for informasjons-sikkerhet i IT-organisasjonen *kan* det foreligge incentiver til å underspille eventuelle bekymringer knyttet til eksempelvis kulturutfordringer og etterlevelse i organisasjonen, og isteden fremsnakke betydningen av enda flere tekniske sikkerhetstiltak. Dette kan utarte i ulike former, slik som nedjusteringer av risikovurderinger og skjønnmaling i rapporteringen til toppledelsen. En slik virkelighetsbeskrivelse fører i tilfelle til at toppledelsen styrer i blinde ved at den ikke blir gjort kjent med det reelle risikonivået og ikke får satt informasjonssikkerhet på agendaen før en ekstern myndighet oppdager avvik og regelverksbrudd, eller at virksomheten viser seg å være kompromittert. Da er det imidlertid for sent.

De samme mekanismene og utfordringene kan gjøre seg gjeldende om premissgivelsen er organisert i OT.

9.2 Observasjoner og drøfting

I utvalget vårt fremkommer det at de fleste informantene jobber strukturert med informasjonssikkerhet, dvs. at de som minimum har etablert styrende dokumenter forankret hos toppledelsen. Når det gjelder i hvilken grad disse er implementert, altså hvorvidt informasjonssikkerhet er integrert i prosesser og aktiviteter for øvrig, slik som innen overordnet HMS-arbeid og internkontroll, ser vi større variasjon.

Noen er sertifisert i henhold til ISO 27001, noen er i ferd med å implementere standarden i deres helhetlige internkontrollsystem og daglige arbeidsprosesser, flere jobber etter standarden mens andre hverken er sertifisert eller jobber etter ISO 27001. Et positivt funn fra intervjuene er at en større andel har etablert strukturer som sikrer internkontroll på informasjonssikkerhetsområdet, enn andelen som ikke har det. Det er også positivt at flere forstår betydningen og viktigheten av at styring og kontroll på informasjonssikkerhetsområdet bør integreres i så stor grad som mulig med det øvrige internkontrollarbeidet. Dette er etter vår mening isolert sett et tegn på at bevisstheten er høy hos både ledere og medarbeidere. Et

av selskapene i utvalget, en leverandørbedrift, overrasket oss svært positiv med deres tankesett og modenhet på styring av informasjonssikkerhet. Vi er av den oppfatning at dette på sikt vil bære frukter i prosjekter og løsninger som denne bedriften er involvert i. Slik kontinuerlig, prosessbasert forbedring, som i COBIT defineres som «leading indicators», utkonkurrer ad-hoc sprintløp. På samme måte kan Equinor sitt «A-standard Handlingsmønster», med læringssløyfe, øke kvaliteten i leveranser over tid.

På spørsmål om hvem i selskapene som fastsetter risikoaksepten, svarer de fleste aktørene at det enten direkte eller indirekte er toppledelsen som gjør dette. De selskapene vi oppfatter som mest modne har dette formalisert gjennom policyer eller andre overordnet styrende dokumenter. Disse er godkjent og signert av toppledelsen. Våre funn tyder ellers på at de fleste aktørene har etablert mekanismer som skal sikre at ledelsen i de respektive selskapene holdes orientert om risikobildet. De aller fleste svarer at de gjennomfører risikovurderinger når dette er nødvendig og at det er etablert prosesser som sikrer at sikkerhetskravene også gjenspeiles i kontrakter og avtaler.

Vi stiller imidlertid spørsmål til i hvilken grad svarene gjenspeiler realitetene. Som det allerede er drøftet i kapitlene 4 og 8.1, er det nokså ulike svar når det blant annet gjelder kartlegging av informasjonsverdier, og hvem i de ulike selskapene som er ansvarlige for dette. Vi mener det er utfordrende å få til adekvat risikostyring dersom bedriften ikke har oversikt over hvilke informasjonsverdier de sitter på. Det vil også være en utfordring hvis det ikke er mulig å knytte eierskap til disse. Betydningen av begrepet «risikoeier», altså hva det innebærer, synes dessuten å være heftet med en del usikkerhet hos flere av informantene.

Når det gjelder kommunikasjon og eventuell håndtering av risiko mellom aktørene i verdikjedene, er svarene også utydelige. Det er forståelig; det er mer utfordrende og komplisert å etablere god risikostyring som involverer flere aktører med ulike interesser. Dette kan løses gjennom at oppdragsgiver oversetter sin vilje til å ta risiko gjennom presise og tydelige krav til blant annet informasjonssikkerhet i avtaler og kontrakter og at det er etablert gode prosesser for oppfølging av leverandørene. Dette forutsetter god bestillerkompetanse. IEC 62443-2-1 ED2 og IEC 62443-2-2 ED1 er svært interessante i denne sammenheng.

Slik vi forstår særlig leverandørene, er det imidlertid ikke alltid tilfelle at det finnes god bestillerkompetanse. Det er flere informanter som sier at operatørene ofte aksepterer «dårligere» leveranser enn det som fremgår av kontrakt, og at dette bare i noen tilfeller håndteres tilstrekkelig i etterkant. Dette har blitt grunngitt med at operatørene ikke er like profesjonelle i IT-aspekter i anskaffelser som i andre sammenhenger, altså kan det tyde på at det handler om manglende innkjøpskompetanse på IT eller kompleks digital teknologi. Det er i så fall en interessant observasjon, da dette isolert sett er en indikasjon på at informasjonssikkerhet både anses som et IT-anliggende og/eller at det ikke oppleves som spesielt forretningskritisk. Dette understøttes ellers av hvem som har deltatt i intervjuene. Med noen unntak har informantene i stor grad representert IT i de ulike selskapene, og det har på

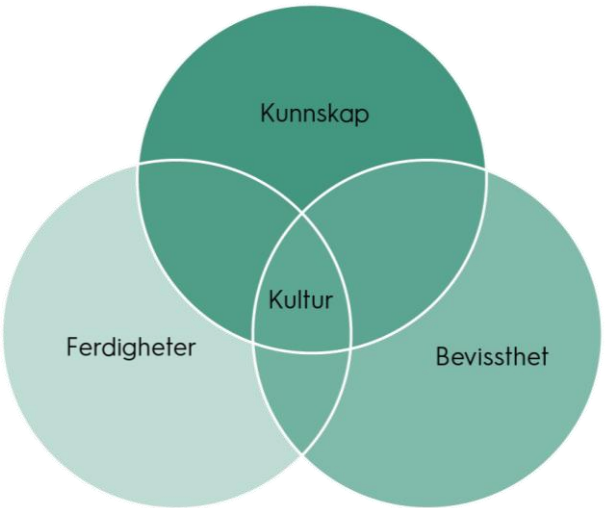
mange måter vært utfordrende å få innsikt i hvordan internkontroll og risikostyring foregår på et virksomhetsovergripende nivå, inkludert hvordan dette er organisert.

Samlet sett er vår vurdering at de fleste aktørene vi har snakket med, både operatører og leverandører, har en grunnleggende forståelse for informasjonssikkerhet. Imidlertid blir dette i veldig stor grad knyttet til IT, og dermed blir informasjonssikkerhet for fjernt fra kjerneoppgavene ved at det oppfattes som et ansvar som IT skal håndtere. I en del sammenhenger vil en slik tilnærming kunne fungere, men IT bør ikke ta risiko på vegne av prosess-/risikoeier slik det er stor sannsynlighet for at det blir. Vi vurderer at det nettopp er dette som er tilfellet hos flertallet av informantene vi har snakket med. Resultatet kan være at risikoeier og selskapene utsettes for større risiko enn det som er akseptabelt, og dette dras videre med i kontrakter og avtaler – noe som kan eksponere oppdragsgiver i enda større grad.

10 Kunnskap

For å ivareta et tilfredsstillende sikkerhetsnivå er det vesentlig at alle ansatte har tilstrekkelig kunnskap om informasjonssikkerhet og IT-sikkerhet. Spesielt når den digitale utviklingen skjer i rekordfart. Som det vises til i denne rapporten, kan mange hendelser, både tilsiktede og utilsiktede, tilskrives mangelfull eller fravær av sikkerhetskompetanse hos medarbeidere; Trusselaktører manipulerer medarbeidere for å få uautorisert tilgang til systemer og infrastruktur, eller medarbeidere utfører handlinger de ikke skal som et resultat av manglende kunnskap. Begge deler bidrar til kompromittering av data og informasjon.

Kompetanse og kunnskap hos den enkelte ansatte er viktig, men sett i det større bildet er det en god sikkerhetskultur i virksomheten som er sentral for at tiltak som er besluttet innført, blir fulgt og etterlevd. Organisasjonskultur påvirkes både av kunnskap, bevissthet og ferdigheter som vist i Figur 8. Kunnskap bidrar til at arbeidsoppgaver utføres på en tilfredsstillende måte, mens bevissthet bidrar til å forsterke eller endre oppførsel og holdninger, samt oppmuntre til å følge virksomhetens verdier. Ferdigheter er også nødvendig for å kunne handle riktig og påvirke virksomheten positivt.



Figur 8: Kunnskap, bevissthet og ferdigheter er viktige faktorer for en god sikkerhetskultur i virksomheten.

Det finnes ulike måter å bygge kunnskap, bevissthet og ferdigheter på. I henhold til ledende praksis [10] [11] bør alle ansatte i organisasjonen, og kontraktører der det er relevant, få hensiktsmessig bevisstgjøring, utdanning og opplæring. Disse aktivitetene bør blant annet bygge på erfaringer fra tidligere sikkerhetsbrudd.

For å bygge kunnskap, bevissthet og ferdigheter er det viktig å fokusere på «hvorfor» i tillegg til «hva» og «hvordan». Et godt kunnskapsgrunnlag bidrar til økt bevissthet rundt følgende:

- **Hva betyr det for meg?** Det er viktig at alle medarbeidere har kjennskap og kunnskap om hva sikkerhet er og hva det betyr for en selv og egen virksomhet. Medarbeideren må forstå formålet med informasjonssikkerhet og de potensielle konsekvensene for virksomheten, både positive og negative, av deres egen adferd.
- **Hvorfor er det viktig?** Medarbeideren må ha forståelse for hvorfor den enkelte skal ivareta informasjonssikkerheten, samt viktigheten av dette.
- **Hvordan kan jeg etterleve våre interne krav best mulig?** Den enkelte må også ha forståelse for det ansvaret en har som ansatt for at virksomheten etterlever vedtatte instrukser og styrende dokumenter.

10.1 Observasjoner og drøfting

Det er varierende hvor stort fokus det er på opplæring og kunnskapsutvikling hos informantene. Noen har mer formaliserte opplegg enn andre. Det synes som om alle tilbyr opplæring av sine ansatte i ulik grad, spesielt for nyansatte, og flere gjennomfører ulike kurs. Det varierer imidlertid i hvilken grad opplæringen har fokus på sikkerhet.

Noen fokuserer mer på fysisk sikkerhet i opplæringen, mens andre vektlegger informasjonssikkerhet og IT-sikkerhet. Noen aktører benytter seg av opplæringsverktøy som NanoLearning og PluralSight, mens andre kurser sine ansatte både gjennom interne og eksterne kurs. Noe av opplæringen er innrettet mot ISO 27001 der denne benyttes, samtidig er lite av opplæringen rettet mot IEC 62443-standarden eller industriell cybersikkerhet. En anbefaling vil være å få inn mer sikkerhet og flere områder innen sikkerhet i opplæringen innad hos de ulike aktørene og spesielt rettet mot IEC 62443/industriell cybersikkerhet. Det finnes flere alternativer for å gjennomføre opplæring av de ansatte på, dette kan gjennomføres som klasseromsbasert undervisning, foredrag, e-læring, øvelser, dilemmatrening, «train the trainer», mm. Det er vesentlig at opplæringsmaterialet og tiltakene oppleves som relevante for dem det angår i henhold til deres roller, ansvar og ferdighetsnivå. Det anbefales derfor å identifisere og prioritere målgrupper for at de kunnskapshevende aktivitetene skal ha positiv effekt for den enkelte ansatte. Materialet bør også være sektorrelevant, noe som kan oppnås gjennom å benytte eksempler på aktuelle sårbarheter, verdier, trusler og hendelser fra industri- og petroleumssektoren.

Erfaringer fra holdningsskapende arbeid i en rekke organisasjoner tyder på at e-læringskurs er en effektiv måte å nå ut til alle ansatte på. E-læring er et tiltak som kan benyttes for bevisstgjøring om områder det er viktig at alle ansatte har et forhold til, slik som å rapportere avvik, sikker behandling av informasjon, passord og sosial manipulering. Komplekst materiale, som krever mer bearbeiding for å forstås og internaliseres, egner seg ikke til E-læring. Dette betyr at E-læring om informasjonssikkerhet ikke vil være tilstrekkelig alene for å nå ut til alt personell og alle roller.

Det opplyses om at bevisstgjøringsaktiviteter helst skjer gjennom brosjyrer, holdnings-kampanjer, phishing-tester, øvelser og deling av informasjon på interne kanaler slik som Yammer, WorkPlace og Teams. Flere benytter også den årlige sikkerhetsmåneden i oktober som arena for å øke sikkerhetskulturen gjennom bevisstgjøring.

En av leverandørene opplyser at de har et løpende Security Awareness Program som inkluderer ukentlig intern kommunikasjon, innlegg på allmøter, trusselmodellering og kursing av ansatte både digitalt og fysisk. I tillegg ser denne leverandøren på erfaringer de har gjort i forbindelse med hendelseshåndtering, og denne informasjonen deles på tvers av virksomheten. Det opplyses om at en av operatørene har gjennomført holdningsskapende aktiviteter i form av phishing-tester som ble sendt ut til både internt ansatte og leverandører.

Samtlige av aktørene tilegner seg også kunnskap om blant annet hendelser og forebyggende sikkerhetsarbeid gjennom partnerskap med blant annet NSM og KraftCERT, samt deltakelse i sikkerhetsfora som eksempelvis i Norsk Olje og Gass og CDS-forum. Dette gir kunnskapsdeling på tvers av fag, tjenesteveier, bedrifter og roller. Flere informanter forteller om hvordan initiativer fra KraftCERT begynner å bli gode fora som bidrar til kommunikasjon og kunnskapsutvikling. I denne sammenhengen nevnes det også Sintef PDS/CDS-forum, NCSC's IRC-kanal, OT-forum, komiteer, konferanser/seminarer/kurs og at ansatte får bruke av arbeidstid til kunnskapsutvikling og være med i slike fora. Deltakelse i aktuelle fora, samt partnerskap med blant annet NSM og KraftCERT, bidrar til økt kunnskap og bevissthet omkring relevante hendelser og mulige sårbarheter. Som nevnt tidligere er denne informasjonen imidlertid fragmentert i og med at informasjon rundt sårbarheter og hendelser ofte er gradert eller behandles konfidensielt, og således er mye av den viktige informasjonen utilgjengelig for de fleste aktører innen petroleumsnæringen. Det gis ellers inntrykk av at det *ikke* pågår *tilstrekkelig* kunnskapsdeling om hendelser, sårbarheter, trusler og annen relevant og god sikkerhetsrelatert informasjon på tvers av selskapene. Det skrapes bare litt på overflaten. Dette er også et inntrykk vi sitter med etter mye arbeid på tvers av selskaper. Mangel på deling ser vi også i flere andre sektorer, samt mellom sektorer. Flere informanter opplyser om at det er vanskelig å få god oversikt over blant annet sårbarheter, trusler og sannsynlighet for hendelser og angrep, og at økt kunnskapsdeling på tvers av selskaper og sektorer er nødvendig.

Hos ett av selskapene, som vi oppfatter at har noe fokus på opplæring og kursing av ansatte og ledere, opplyses det om at det p.t ikke benyttes måleindikatorer for å se om denne opplæringen har effekt. Ett av leverandørselskapene som anvender Pluralsight som opplæringsplattform, benytter seg av Pluralsights innebygde verktøy for å måle de ansattes ferdigheter. Vi har blitt opplyst om at disse sammenligner resultatene før og etter gjennomført opplæring. Denne metoden har hos den aktuelle leverandøren blitt benyttet til blant annet opplæring i sikkerhet i sammenheng med Azure.

Overordnet gis det inntrykk av at kun et fåtall av aktørene har en etablert målingsprosess som ser på situasjonsbildet før og etter at kompetansehevende tiltak har blitt implementert. Det er dermed vanskelig å si om opplæringen, bevisstgjøringsaktivitetene og treningen har en positiv innvirkning på de ansatte. Uten målinger vil det være svært utfordrende, for ikke å si umulig, å kunne gi et konkret svar på om opplæringen fungerer som forutsatt, og om aktørene dermed oppnår de ønskede resultatene. Vi anbefaler derfor å evaluere effekten av aktivitetene som utføres i forbindelse med bygging av kunnskap, bevissthet og ferdigheter. Dette krever at selskapene definerer virksomhetstilpassede læringsmål og evaluerer opp mot disse.

11 Konklusjoner og anbefalinger

Petroleumssektoren er kontinuerlig utsatt for ulike typer risiko. Om vi forutsetter at informantene er representative for sektoren, stiller vi oss tvilende til at den er i stand til å identifisere og håndtere risiko forbundet med informasjonssikkerhet på en god nok måte. Sett i sammenheng med at informasjonssikkerhet i for liten grad blir hensyntatt i leverandørstyringen, er vår konklusjon at informasjon og data ikke blir sikret godt nok, hverken i transit eller i ro.

Det er mye som tyder på at operatørene ikke kjenner til risikoene de er eksponert for, blant annet ved at trusselbildet både er uklart og til en viss grad ignoreres når det blir tydeligere, samt at det ikke eksisterer gode prosesser for å kunne identifisere og kartlegge interne sårbarheter, især de som er av organisatorisk og menneskelig karakter. Og med bakgrunn i at de organisatoriske sårbarhetene er tilstedeværende i den grad vi har sett, herunder svakheter i organiseringen av sikkerhetsarbeidet, risikostyring og opplæring, blir arbeidet med å avdekke og håndtere risiko reaktivt og i mindre grad planlagt. Etter vår mening er det derfor overveiende sannsynlig at trusselaktører med tilstrekkelig kapasitet og motivasjon allerede har kompromittert infrastruktur og systemer.

Våre observasjoner og funn indikerer at det er svært mye informasjon og data som svært få i verdikjedene har god oversikt over, og følgelig finnes det ikke konkrete vurderinger av hvilke konsekvenser det kan ha dersom disse blir kompromittert. De fleste har en formening om at det kan få konsekvenser, men ettersom eierskap ikke er tydeliggjort, eksisterer det et vakuum som tillater at nye løsninger og IT-systemer blir knyttet opp til eksisterende infrastruktur uten at operatørene nødvendigvis har tilstrekkelig kunnskap om det og kontroll på det. Dermed flyter informasjon og data mellom systemer og løsninger uten at nødvendige tiltak blir implementert. Leverandørene gjør sine vurderinger, men dette skjer stykkevis og delt uten at det er en større helhet i det eller at riktige roller hos operatørene er tilstrekkelig involvert. Konsekvensene kan som diskutert tidligere i rapporten være mange, og følgene av dette kan spenne over mange flere dimensjoner enn rene økonomiske kostnader. Også samfunnet kan bli skadelidende.

Vi tilskriver disse forholdene flere ting slik vi har redegjort for i denne rapporten:

- Manglende styring og kontroll på informasjonssikkerhet hos både operatører og leverandører, og spesielt i komplekse verdikjeder
- Manglende fokus på informasjonssikkerhet i leverandørstyring og -oppfølging
- Manglende kunnskap, kompetanse og bevissthet om trusler, verdier og sårbarheter
- For lite utveksling av både trusselinformasjon og informasjon om sårbarheter mellom myndigheter og næringen, samt internt i næringen
- Sårbarheter blir ofte adressert ved å implementere nye tekniske løsninger, som i mange tilfeller kan komplisere verdikjedene ytterligere, fremfor å jobbe systematisk med bevisstgjøring og kunnskapsbygging, eller ta ordentlig tak i større organisatoriske utfordringer.

For styrking av kunnskapsutvikling bør det utvises varsomhet med varslingsplikt. Vi ser at krav og reguleringer til varsling kan virke mot sin hensikt fordi det ofte er usikkerheter rundt hendelser og risiko, at det skaper internt og eksternt støy, og at det kan komme i konflikt med produksjonsmål og resultatkrav. Vår erfaring er at det oppstår underrapportering, mangelfull kommunikasjon og manglende vilje til å gjøre analyser eller granskninger når det knyttes formelle krav til varsling innenfor områder som gjerne er konfidensielt. Derimot ser vi at kunnskapsutveksling og informasjonsdeling skjer mer effektivt i uformelle fora.

Slik vi forstår det, baserer Petroleumstilsynet seg på ISO 19011 som grunnlag for tilsyns-metodikken. Vi registrerer at noen aktører opplever seg som mer utpekt enn andre for slike tilsyn, hvilket i seg selv ikke trenger å være feil. Imidlertid kan dette være et tegn på at den opplevde vesentligheten blir vektlagt mer enn den objektive iboende risikoen når tilsyn planlegges. Samtidig er vi gjort kjent med at tilsynet i for liten grad fanger opp de tilfellene der styringssystemer og internkontroll ikke fungerer slik det gjerne blir presentert fra selskapenes side. Dette kan det være ulike årsaker til, men normalt kreves det en tradisjonell revisjonstilnærming for å avdekke dette, blant annet gjennom såkalt systemtesting (sjekk/test av selskapenes kontroller/internkontroll) og substanskontroller basert på statistisk utvalg. Dette bidrar også til at tilsynene blir mer effektive og at antallet tilsyn kan økes uten at ressursbruken øker tilsvarende.

11.1 Anbefalinger

- Selskapene bør øke innsatsen for å integrere eksisterende internkontroll på sikkerhetsområdet i selskapenes helhetlige internkontroll, herunder at prosesser for risikostyring og leverandøroppfølging blir omfattet av krav til sikkerhet.
- Selskapene bør sørge for at ulike rollers betydning og ansvar blir oppfattet likt innad i selskapet og gjennom hele verdikjeden.
- Selskapene bør i større utstrekning enn i dag gjennomføre vurderinger av hvilken betydning tap av konfidensialitet, integritet og tilgjengelighet har, sett opp mot hvilke prosesser og hvilke verdikjeder ulik data og informasjon understøtter. Konsekvenspotensiale må vurderes grundig og tverrfaglig.
- Alle aktører bør i større grad knytte eierskap til informasjon og data. Det påligger særlig operatørselskapene et ansvar sett opp mot blant annet styringsforskriften å stille krav til dette overfor kontraktørene og underleverandører.
- Det bør søkes å oppnå enighet om hvilke mekanismer som skal benyttes for å sikre data og informasjon som er i ro.
- Det bør stilles større og tydeligere krav til at det implementeres tilgangsstyrings-funksjoner i endepunkter som begrenser hvilke verdier som kan endres og hva det generelt skal gis tilgang til. Herunder gå bort fra privilegerte tilganger med rettigheter utover det som er nødvendig.
- Det bør vurderes å ta i bruk mer moderne, dedikerte verktøy for endring- og versjons-håndtering i OT
- Selskapene bør gjennomgå organiseringen av informasjonssikkerhetsarbeidet, her-under sikre større grad av rolleseparasjon

- Det bør søkes å få inn mer sikkerhet, særlig IEC 62443/ industriell cybersikkerhet, i opplæringen hos de ulike aktørene. Det er i den forbindelse vesentlig at opplærings-materialet og tiltakene oppleves som relevante.
- Effekten av opplæringsaktiviteter bør i større grad kunne måles og være gjenstand for evaluering.
- Det bør etableres mer uformelle fora og møteplasser for å få kunnskapsutvikling om hendelser, sårbarheter, trusler og verdier, på tvers av fagmiljøer, bedrifter, sektorer og myndigheter.
- Petroleumstilsynet kan ta en tydeligere rolle i kommunikasjonen med aktørene. Prosjektet opplever at enkelte informanter uttrykker et ønske om tydeligere styrings-signaler, spesielt når det gjelder fastsettelse av relevante standarder og regelverk
- Petroleumstilsynet kan søke å oppnå en mer risikobasert tilnærming i gjennomføringen av tilsyn, gjennom adopsjon av tradisjonell revisjonsmetodikk så langt dette er hensiktsmessig. Våre vurderinger og anbefaling samsvarer i denne sammenheng med DNV GL-rapport «IKT-sikkerhet – Robusthet i petroleumssektoren, Regelverk og tilsynsmetodikk»

12 Referanser

[1] S. Pedersen, «Vær et A-standard menneske!,» *BIS Magasinet,* pp. 22-23, 2012.

[2] O. Lysne, «Risikostyring i digitale verdikjeder,» Direktoratet for samfunnssikkerhet og beredskao (DSB), 2020.

[3] Lovdata, Forskrift om styring og opplysningsplikt i petroleumsvirksomheten og på enkelte landanlegg (styringsforskriften), Helse- og omsorgsdepartementet, Klima- og miljødepatementet, Arbeids- og sosialdepartementet, 2011.

[4] M. E. Everson, S. E. Soske, F. J. Martens, C. M. Beston, C. E. Harris, J. A. Garcia, C. I. Jourdan, J. A. Posklensky og S. J. Perraglia, «Internal Control- Integrated Framework,» COSO, 2013.

[5] «NSMs Grunnprinsipper for IKT-sikkerhet versjon 2.0,» Nasjonal sikkerhetsmyndighet, 2020.

[6] «Nasjonal trusselvurdering 2021,» *Politiets Sikkerhetstjeneste (PST),* 2021.

[7] «Nasjonalt digitalt risikobilde 2021,» Nasjonal Sikkerhetsmyndighet (NSM), 2021.

[8] «Fokus 2021,» Etterretningstjenesten, 2021.

[9] P. M. Salmon, G. J. M. Read, G. H. Walker, M. G. Lenné og N. A. Stanton, «Distributed Situation Awareness in Road Transport,» 2018.

[10] «ISO/IEC 27001:2017». 2017.

[11] «ISO/IEC 27002:2017». 2017.

[12] «EKANS Ransomware and ICS Operations,» *Dragos,* 2020.

12.1 Informative referanser

«Datakvalitet ved digitalisering i petroleumssektoren», SINTEF, 2020.

«Premisser for digitalisering og integrasjon IT-OT», SINTEF, 2020.

«Aktørenes tilstandsvurdering, vedlikehold og oppfølging av sikkerhetskritiske funksjoner og utstyr», SINTEF, 2018

«Datakvalitet ved digitalisering i petroleumssektoren», SINTEF, 2020

«Digitalisering i petroleumsnæringen», IRIS, 2018

«Cyber security in the oil and gas industry based on IEC 62443», DNVGL, 2018

«IKT-sikkerhet – Robusthet I petroleumssektoren – Regelverk og tilsynsmetodikk», DNVGL, 2020

ISO/IEC 27005:2018

ISO/IEC 31000:2018

IEC 62443

13 Vedlegg 1 - Relevante hendelser

13.1 Triton/TRISIS 2017

Triton/TRISIS var et tilsiktet angrep i 2017, der selve skadevaren hadde kapabilitet til å gjøre endringer i instrumenterte sikkerhetssystemer (SIS). Triton skadevaren gjorde det mulig for trusselaktøren å endre definerte kontrollnivåer i SIS, slik at dersom det eksempelvis oppstod et for høyt trykk i en gassturbin, ville det ikke genereres alarm eller trippsignal. Konsekvensen ved å slå ut siste sikkerhetsmekanisme kan være enorm, og innebære fare for langvarig produksjonsstans, miljøutslipp og menneskeliv. Grepene som ble gjort i Triton-angrepet viser at trusselaktøren i realiteten måtte hatt som mål å forårsake en eller flere av disse konsekvensene.

13.2 Løsepengevirus

I 2019 ble det detektert et nytt løsepengevirus «Ekans» som i tillegg til å kryptere datasystemer hadde spesifikke ICS funksjonaliteter med formål om å blant annet stoppe ICS-prosesser. Dette løsepengeviruset er ifølge Dragos unikt og en av de første kjente løsepengevirusene som har ICS-spesifikke operasjoner [1].

I mai 2021 ble også Colonial Pipeline som er et av USAs største rørledningssystem for transport av raffinerte oljeprodukter utsatt for et løsepengevirus. Løsepengeviruset infiserte datautstyr som administrerte rørledningen, som medførte at operatører så seg tvungne til å utføre full nedstengning.

13.3 Ransom-DDoS-angrep på Telenor i 2020

I oktober 2020 meldte Telenor om at de var rammet av et rDDoS-angrep der utpressere angrep Telenor med et DDoS-angrep, og deretter krevde løsepenger utbetalt for ikke å utsette Telenor for ytterligere angrep [2]. Ransom-DDoS-angrep («rDDoS») er en form for tjenestenektangrep der en trusselaktør truer med å gjennomføre et DDoS-angrep mot offeret hvis ikke løsepenger blir betalt til trusselaktøren.

13.4 Leverandørkjedeangrepet på SolarWinds i 2020

SolarWinds ble i 2020 utsatt for et leverandørkjedeangrep. SolarWinds tilbyr Orion som er et network management system (NMS) som brukes som system for cybersecurity. Angrepet skjedde ved at en trusselaktør lastet opp filer med skadevare på oppdateringsserveren til SolarWinds og inkluderte dette i programvareoppdateringer. Alle kunder som var flinke med sine prosesser for programvareoppdateringer og oppdaterte til nyeste versjon av Orion, ble infisert med skadevaren som inkluderte installasjon av en bakdør (kalt «Sunburst») til systemet. Trusselaktøren hadde dermed tilgang til alle systemer med denne installasjonen hvis den var eksponert mot internett.

13.5 Leverandørkjedeangrepet på Kaseya i 2021

I juli 2021 ble også programvareselskapet Kaseya utsatt for leverandørkjedeangrep. Dette medførte at deres kunder fikk en programvareoppdatering som skjulte et løsepengevirus. Kassasystemene til Coop i Sverige var blant de som mottok denne oppdateringen, og som følge av dette måtte 800 butikker holde stengt i en uke til systemene var oppe igjen.

13.6 Hendelsen på raffineriet på Mongstad i 2014

21. mai 2014 ble raffineriet på Mongstad utsatt for en utilsiktet hendelse. Det resulterte i at de måtte gå over til manuell lasting ettersom en IT-ansatt hos driftsleverandøren HCL i India utførte en restart av en feil server, en server som driftsleverandøren ikke skulle hatt tilgang til. Serveren som ble restartet var en av Equinors (daværende Statoil) produksjonsservere som styrte den automatiske prosessen for blanding og overføring av bensin til tankskip [3]. Equinors ansatte som var fysisk på lokasjonen hadde kompetanse til å ta over prosessen, og fikk fullført prosessen manuelt med minimal skade. I dette tilfellet var konsekvensen et økonomisk tap for Equinor på 200 000-300 000 kr. Store mengder av prosesser i olje- og gassproduksjonen er drevet av datasystemer, og konsekvensen kunne derfor vært mye større avhengig av hva som hadde var berørt. I 2017 ble det kjent at Equinor hentet hjem drift av sikkerhetskritiske oppgaver fra India tilbake til Norge [4].

13.7 Referanser for Vedlegg 1

[1] «EKANS Ransomware and ICS Operations,» *Dragos,* 2020.

[2] «Telenor ble truset med pengekrav: Cyberkriminelle angriper og presser norske selskaper,» *Telenor,* 2020.

[3] «Tastefeilen som stoppet Statoil,» *NRK,* 2016.

[4] «Statoil henter hjem sikkerhetskritiske IT-oppgaver fra India,» *NRK,* 2017.