DNV·GL

PROSJEKTRAPPORT

Håndtering av innsiderisiko

Utført på oppdrag for Petroleumstilsynet

Rapportør.: 2019-0280, Rev. 1
Dato: 2019-10-18

	Prosjektrapport	DNV GL AS Oil & Gas
Rapporttittel:	Håndtering av innsiderisiko	Asset Risk Management
Oppdragsgiver:	Utført på oppdrag for Petroleumstilsynet	Veritasveien 1
Kontaktperson:	Ingvild Klaveness og Tommy Bugge Hansen	1363 Høvik
Dato:	2019-10-18	Norway
Prosjektnr.:	10142953	Tel: 67 57 99 00
Org. enhet:	Asset Risk Management	
Rapportnr.:	2019-0280, Rev. 1	

Levering av denne rapporten er underlagt bestemmelsene i relevant(e) kontrakt(er):

Oppdragsbeskrivelse:

Bakgrunnen for prosjektet var Ptil sine erfaringer fra tilsyn og at innsiderisiko ved flere anledninger hadde blitt trukket frem som en trussel av bl.a. Politiets sikkerhetstjeneste (PST), Nasjonal sikkerhetsmyndighet (NSM) og Næringslivets sikkerhetsråd (NSR), samtidig som tilsynene viste at petroleumsnæringen opplever innsidetrusselen som utfordrende å håndtere. Målsettingen med prosjektet har vært å øke Ptils og petroleumsnæringens kunnskapsgrunnlag om innsiderisiko, herunder fenomenforståelse og beste praksis mht. en systematisk tilnærming til risikohåndtering. Økt kunnskap er tenkt å skulle føre til bedre og mer systematisk styring av risiko knyttet til innsiderisiko (herunder barrierestyring, ref. Styringsforskriften §5).

Utført av:	Verifisert av:	Godkjent av:
Jon Jerre Senior Principal Consultant	Sture Angelsen Head of Section	Sture Agnelsen Head of Section
Espen Funnemark Principal Specialist		

DNV GL distribusjon:

☒ ÅPEN. Fri distribusjon, internt og eksternt.

☐ INTERN. Fri distribusjon internt i DNV GL.

☐ KONFIDENSIELL. Distribusjon som angitt i distribusjonsliste *

☐ HEMMELIG. Kun autorisert tilgang.

*Distribusjonsliste:

Nøkkelord:

Innsider, trussel, sikring, risiko, personellsikkerhet, tiltak, sikringsledelse, modenhetsundersøkelse

Rev.nr.	Dato	Årsak for utgivelser	Utført av	Verifisert av	Godkjent av
0	2019-09-13	Første utgivelse	Jon Jerre og Espen Funnemark	Sture Angelsen	Sture Angelsen
1	2019-10-18	Enkelte mindre justeringer	Jon Jerre og Espen Funnemark	Sture Angelsen	Sture Angelsen

Innholdsfortegnelse

1 SAMMENDRAG

Bakgrunnen for Petroleumstilsynets (Ptils) initiering av prosjektet var at innsiderisiko ved flere anledninger har blitt trukket frem som en trussel av bl.a. Politiets sikkerhetstjeneste (PST), Nasjonal sikkerhetsmyndighet (NSM) og Næringslivets sikkerhetsråd (NSR), samtidig som tilsyn viste at petroleumsnæringen opplever innsidetrusselen som utfordrende å håndtere. Målsettingen med prosjektet har vært å øke Ptils og petroleumsnæringens kunnskapsgrunnlag om innsiderisiko, herunder fenomenforståelse og beste praksis mht. en systematisk tilnærming til risikohåndtering.

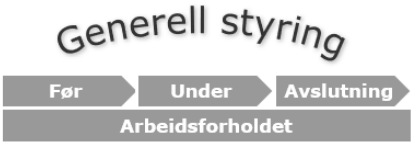
Arbeidet ble gjennomført i perioden mars – august 2019, under ledelse av DNV GL. En workshop med 36 deltakere fra næringen, Ptil, NSM og PST ble arrangert i mars. Workshopen ble etterfulgt av dybdeintervjuer med utvalgte selskaper. I tillegg ble det gjennomført en litteraturstudie som omfattet rundt 75 dokumenter, både norske og utenlandske.

Denne rapporten sammenfatter resultatene fra prosjektet, og består av fire hoveddeler:

- Dybdebeskrivelse av fenomenet innsidetrussel – hvem, hva, hvordan
- God praksis for å håndtere innsidetrusselen (totalt 45 forslag), inkl. lovmessige begrensinger
- Oppsummering av hvor petroleumsnæringen står i dag – utfordringer og erfaringer
- Modenhetsundersøkelse – et enkelt verktøy for å vurdere hvor godt rustet man er

Det finnes ingen enhetlig og internasjonal definisjon av en innsider. Det er mest vanlig å definere en innsider som en person med autorisert tilgang til virksomhetens systemer, objekter, informasjon o.l., og som bevisst utfører handlinger som påfører virksomheten skade eller tap. Noen organisasjoner, spesielt innen IT-verdenen, inkluderer også ubevisste, og ikke-villede handlinger i definisjonen. Innsideren kan være enten en *infiltratør* (f.eks. plassert av en fremmed stat), en som er *rekruttert* (f.eks. gjennom trusler/press eller mot betaling), en som er *selvmotivert* (utfører på eget initiativ), eller en som *uforvarende* utfører en handling.

I tillegg til tiltak som er generelle for styring av sikring, er det spesiell fokus på tiltak knyttet til arbeidsforholdet (fast ansatte, innleide konsulenter og andre kontraktører). Tiltakene er gruppert i før ansettelse eller kontraktsinngåelse, under selve arbeidsholdet, og perioden der arbeidsforholdet avsluttes (oppsigelsestiden).



Tiltak for å håndtere innsiderisiko går i korthet ut på følgende fire elementer.

- *Forhindre* at en potensiell trusselaktør (innsider) får tilgang til virksomheten, enten gjennom å bli ansatt, eller å utføre oppdrag innen virksomhetens «fire vegger».
- *Forhindre* at en arbeidstaker som allerede har lovlig tilgang til virksomheten og dens systemer, utvikler seg til å utgjøre en innsidetrussel. I motsetning til eksterne trusler, er interne trusler noe virksomheten i større grad selv kan påvirke.
- *Detektere, forsinke* og *stoppe* en allerede igangsatt handling fra en innsider. Skulle en innsider likevel igangsette uønskede handlinger må dette oppdages og mottiltak iverksettes for å forhindre at innsideren får gjennomført sin handlingen.
- *Håndtere* en oppstått situasjon for å begrense skadene i størst mulig grad

Mye fokus legges i dag på tiltak under rekrutteringsprosessen ved fast ansettelse, og bakgrunnssjekk er et viktig element. Bakgrunnssjekker har imidlertid en rekke svakheter, eksempelvis i forhold til å avdekke en godt forberedt infiltratør. Personers sårbarheter, som gjør at de kan utnyttes (presses eller

kjøpes) på et senere tidspunkt, kan være mulig å oppdage, men lovverket setter visse begrensninger mht. hva man har lov å etterspørre.

Mens en person er i arbeid er det et sett med tiltak som bør iverksettes. Dette er av typen teknologiske tiltak (fysiske barrierer, elektroniske systemer og logiske tiltak), organisatoriske tiltak og menneskelige tiltak som typisk påvirker menneskers bevisstgjøring, persepsjon, vurderingsevne, forståelse osv.

Å skape et godt arbeidsmiljø, god trivsel og fornøyde medarbeidere er kanskje det viktigste en virksomhet kan gjøre for å forebygge at en person utvikler seg til å utgjøre en innsidetrussel. Ledelsens rolle er helt avgjørende – ledelsen må avsette tilstrekkelige ressurser, kommunisere viktigheten av sikring og være en god rollemodell. Ledere må legge til rette for en god dialog med sine medarbeidere – dette vil gjøre det lettere for en ansatt å ta opp forhold dersom vedkommende skulle ha blitt lurt eller presset inn i en vanskelig situasjon, eller har observert unormal adferd hos kollegaer. Sikring berører flere enheter i en organisasjon – spesielt HR, juridisk, IT, sikringsenheten og linjeledelsen – en god dialog disse imellom er viktig.

Klare og forståtte regler som etterleves av alle er helt nødvendig. Tilgangs- og adgangskontroll er en viktig faktor i å begrense personers tilgang til systemer og adgang til områder. Fysiske sikringstiltak, prosedyrer og regler har en viss effekt for å begrense en innsiders muligheter til å utføre en uønsket handling.

Imidlertid er den menneskelige faktor svært viktig – som vår bevisstgjøring og forståelse, vår observasjonsevne og vår adferd. Tiltak som øker arbeidstakeres bevisstgjøring og forståelsen rundt innsiderisikoen kan være med på å forhindre at en innsider lett får tilgang til de verdiene vedkommende er på utkikk etter. Det må skapes en kultur i virksomheten om at man tar opp ting dersom man observerer noe man stusser over – det å skape en generell forståelse for at «*Det handler ikke om å sladre, men om å bry seg….*».

Overvåking er en naturlig del av arbeidet med å detektere en planlagt eller pågående handling. Samtidig må virksomheten være klar over de muligheter og begrensinger som ligger i lovverket, både mht. spesielle kontrolltiltak og personvern. Det er begrensninger i hva man har lov til å spørre en arbeidstaker om og hva man har lov til å undersøke vedrørende arbeidstakeren. I visse tilfeller er det lov å iverksette spesielle kontrolltiltak, dersom dette ansees som høyst nødvendig. I så fall må dette være avklart med de som blir berørt av kontrolltiltakene og med de ansattes tillitsvalgte.

Avslutningsfasen i et arbeidsforhold kan være kritisk. Det bør legges vekt på å vurdere hvorvidt det skal legges begrensinger i en persons tilganger i den perioden vedkommende er i avslutningsfasen.

I tilfelle en sikringshendelse inntreffer er det viktig å være godt forberedt. Virksomheten bør ha utarbeidet en plan for hvordan man skal håndtere sikringshendelser og regelmessig trene på dette.

Som et ledd i prosjektet er det utarbeidet et enkelt modenhetsverktøy som enhver virksomhet kan benytte for å vurdere seg selv. Man gir seg selv score for hvert av de totalt 45 foreslåtte tiltakene. Resultatet (beregnet i prosent av maksimalt mulig oppnåelig) angir hvor moden organisasjonen er – det vil si hvor langt man har kommet i arbeidet med å håndtere innsidetrusselen.

2 INTRODUKSJON

2.1 Bakgrunn og formål

Denne rapporten er et utarbeidet på bakgrunn av et prosjekt for Petroleumstilsynet (Ptil) gjennomført av DNV GL våren 2019. Rapporten er utarbeidet av Jon Jerre (DNV GLs prosjektleder) og Espen Funnemark.

Bakgrunnen for Ptils initiering av prosjektet var at Ptil gjennom tilsyn observerte at petroleumsnæringen opplever at innsidetrusselen er utfordrende å håndtere, samt at dette var et område som man i liten grad hadde satt fokus. I tillegg har innsiderisiko ved flere anledninger blitt trukket frem som en trussel av bl.a. Politiets sikkerhetstjeneste (PST), Nasjonal sikkerhetsmyndighet (NSM) og Næringslivets sikkerhetsråd (NSR).

Ptils målsetting med prosjektet har vært å øke Ptils og petroleumsnæringens kunnskapsgrunnlag om innsiderisiko, herunder fenomenforståelse og beste praksis mht. en systematisk tilnærming til risikohåndtering. Økt kunnskap er tenkt å skulle føre til bedre og mer systematisk styring av risiko knyttet til innsiderisiko (herunder barrierestyring, ref. Styringsforskriften §5).

I tillegg vil denne økte forståelsen også bidra til å styrke effekten av Ptils tilsyn og derigjennom bidra til at arbeidet med håndtering av innsiderisiko i petroleumsnæringen kan styrkes.

Prosjektet har sett på tiltak for å håndtere innsiderisiko. Tiltakene omfatter en kombinasjon av teknologiske, organisatoriske og menneskelige tiltak. Dette prosjektet har imidlertid ikke adressert system- og nettverksløsninger innen informasjonsteknologi (cyber security).

2.2 Rapportens intensjon og oppbygning

Denne rapporten er ment å være et verktøy for aktører innen petroleumssektoren der man finner god praksis for hvordan håndtere innsiderisikoen i eget selskap. Samtidig er denne rapporten anvendelig også for andre næringer. Videre inneholder den en sjekkliste som kan benyttes som en enkel modenhetsundersøkelse for å finne ut av hvor godt eget selskap er rustet for å håndtere en mulig innsidetrussel.

Rapporten er basert på den informasjon og innspill som fremkom gjennom en workshop med selskapene, gjennom dybdeintervjuer og litteraturstudiet som ble gjennomført som en del av prosjektet. Se kapittel 3 for mer informasjon om disse tre aktivitetene.

Rapporten beskriver følgende:

- Generelt om sikring (kapittel 4.1) og spesielt om innsiderisiko (kapittel 4.2) – hvem er innsideren, hvordan operer en innsider og generelt om barrierer/tiltak
- God praksis for å håndtere innsiderisiko
    - Beskrivelse av konkrete tiltaksforslag (kapittel 5)
    - Enkelt verktøy for å måle egen modenhet ved håndtering av innsiderisiko (Appendix C)
- Sammenfatning av status i næringen i dag – hvilke utfordringer står selskapene overfor (kort oppsummering i kapittel 6.1, og mer utdypende i Appendix B)
- Lovkrav som det er viktig å ha kjennskap til i arbeidet med innsiderisiko (Appendix E)
- Litteraturstudien – en sammenfatning av litteraturens omtale av innsiderisiko (Appendix F)

Tabell 2-1: Forkortelser som benyttes i denne rapporten

ASIS	American Society for Industrial Security
FBI	Federal Bureau of Investigation (US Department of Justice)
CPNI	Centre for the Protection of National Infrastructure (UK)
CRISP	Connecting Research in Security to Practice (US department of Justice)
GDPR	General Data Protection Regulation – Personvernforordningen i EU, av 2018
IAEA	International Atomic Energy Agency
NGO	Non-Governmental Organisation
NSM	Nasjonal sikkerhetsmyndighet
NSR	Næringslivets Sikkerhetsråd
PST	Politiets sikkerhetstjeneste
Ptil	Petroleumstilsynet

3 GJENNOMFØRING

Prosjektet ble gjennomført i perioden mars – august 2019, og bestod av tre hovedelementer som illustrert i figuren under.

Figur 3-1: Prosjektets gjennomføring, rapporten er basert på informasjon innhentet gjennom disse tre aktivitetene

Workshop: En heldags workshop ble planlagt i felleskap mellom Ptil og DNV GL. Workshopen ble avholdt 5. mars i Ptils lokaler. I alt 36 personer deltok, fra i alt 15 selskap innen petroleumsnæringen deltok samt NSM, PST og Ptil. Det var en bred deltakelse på workshopen, personer fra sikringsmiljøet i virksomhetene, fra HR, fra IT og fra juridisk. Deltakende selskap og organisasjoner er vist i Appendix A. DNV GL fasiliterte workshopen.

Hensikten med workshopen var å utveksle erfaring med forebygging og håndtering av innsiderisiko – hvilke utfordringer selskapene hadde erfart og få innspill til hva som kan være god praksis. Workshopen ble gjennomført med en blanding av enkelte forberedte innlegg, gruppearbeid med gruppediskusjoner og presentasjon av gruppearbeidet i plenum med tilhørende plenumsdiskusjoner. Workshopen ble gjennomført iht. Chatham House Rules[1].

Dybdeintervjuer: I samarbeid mellom Ptil og DNV GL ble det identifisert organisasjoner som ble invitert til å delta i dybdeintervjuer. DNV GL gjennomførte i alt 6 intervjuer. Oversikt over selskap som deltok i dybdeintervjuene finnes i Appendix A. Hensikten med dybdeintervjuene var å gå nærmere inn på de utfordringer selskapene hadde erfart mht. innsiderisiko, hva man gjør for å håndtere denne risikoen (konkrete tiltak – god praksis), samt få innspill til gode veiledere, rapporter og andre dokumenter som kunne være nyttige for DNV GL i den videre arbeidet med å utarbeide denne rapporten.

Litteraturstudier: Rundt 75 dokumenter ble identifisert, både norske og utenlandske – lover, forskrifter, veiledere, standarder, spesielle studier, studentavhandlinger osv. De utenlandske dokumentene kom i all hovedsak fra Australian Government, CPNI, FBI, IAEA, NATO, samt diverse universiteter og andre organisasjoner. En sammenfatning av hva som skrives om innsiderisiko i disse dokumentene finnes i Appendix F, mens kapittel 8 inneholder alle referanser benyttet i rapporten.

I tillegg er noe informasjon hentet fra presentasjonene gitt på Ptils Fagdag om Sikring som ble holdt 15. mai 2019 i Ptils lokaler.

[1] *Chatham House Rules*: Informasjonen som utveksles i et lukket møte og som gjennomføres iht. *Chatham House Rules* kan benyttes av deltakerne seg imellom, men det skal ikke avsløres hvem som har sagt hva.

4 SIKRING OG INNSIDERISIKO – NOEN AVKLARINGER

Dette kapittelet omtaler først sikring generelt (kapittel 4.1), og gir en kortfattet oversikt over de viktigste etterfulgt av et kapittel som er spesielt rettet mot innsiderisiko (kapittel 4.2). Kapittelet beskriver karakteristika knyttet til trusselaktøren, og generelt om barrierer for å håndtere innsidetrusselen.

4.1 Generelt om sikring

4.1.1 Terminologi

Sikkerhet og sikring: Terminologien knyttet til *sikkerhet* og *sikring* er på norsk ikke like entydig som de tilsvarende termene på engelsk – som *safety* og *security.* Litt avhengig av hvilket miljø man er i brukes noen ganger ordet *sikkerhet* når man omtaler det som på engelske kalles *security*, mens andre ganger brukes ordet *sikring*. Tilsvarende brukes også ordet sikring der man gjerne omtaler forhold knyttet til det man på engelske ville kategorisere under begrepet safety – som f.eks. brannsikring, stillassikring o.l. I dette dokumentet brukes gjennomgående begrepet sikring for det som på engelske er security.

Oversikten nedenfor gir noen korte karakteristika for hva som skiller de to begrepene.

Karakteristika for *Sikkerhet* («Safety»)

- Uønsket handling eller tilstand
- Ubevisst, ikke ondsinnet
- Ikke planlagt

Karakteristika for *Sikring* («Security»)

- Bevisst handling
- Ondsinnet handling
- Planlagt handling

Sannsynlighet – begrepet sannsynlighet oppfattes og brukes noe forskjellig, avhengig hvilket dokument man leser og hvem man snakker med. På engelsk er det to forskjellige begreper – *probability* og *likelihood*. Standarden ISO 22300:2018 *Security and rescilience – Vocabolary* definerer probability som «*measure of the chance of occurrence expressed as a number between 0 and 1 where 0 is impossibility and 1 is absolute certainty*» og likelihood som «*chance of something happening*».

På den annen side, i ISO 31000:2018 er begrepet «likelihood» benyttet i den engelske utgaven av standarden, mens i den norske oversettelsen benyttes begrepet *sannsynlighet* og dette er i den norske utgaven av standarden definert som «*potensialet for at noe kan skje*».

I denne rapporten er begrepet sannsynlighet gjennomgående benyttet, iht. definisjonen i den norske utgaven av ISO 31000:2018.

4.1.2 Tre faktorer viktig i sikring

Generelt innen sikringsarbeid er det tre enkle spørsmål som må stilles og besvares:

1. Hva skal beskyttes – hvilke verdier er viktige og som derfor må beskyttes?
2. Hvem skal man beskytte seg mot – hvem kan ønske å skade verdier eller tilegne seg disse?
3. Hvordan kan man beskytte seg – hvilke barrierer må være på plass for å ta vare på verdiene?

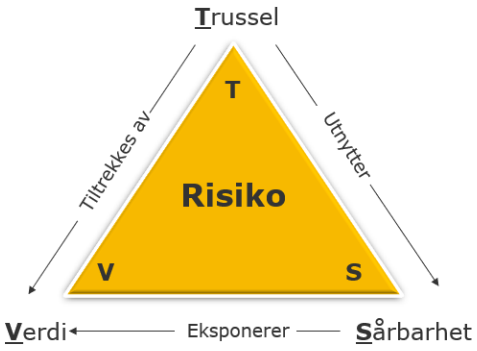
Figur 4-1: De tre viktige spørsmålene. Spørsmålene leses i rekkefølgen «Hva», «Hvem» og «Hvordan».

Verdier er alt som har betydning for virksomheten, og som dersom de blir skadet, stjålet, misbrukt eller kompromittert, kan skade virksomheten. Verdier kan være sensitiv informasjon, omdømme, nettverksinfrastruktur, spesielle installasjoner, utstyr eller deler som er kritisk for produksjonen, personer generelt eller spesielle grupper (ledelse, personer med spesiell kompetanse eller som besitter spesiell informasjon) m.m.

Trusler som f.eks. industrispionasje, terroranslag, sabotasje, hærverk, skade av omdømme o.l., og utføres av en eller flere *trusselaktører*. En trusselaktør kan være ekstern – enkeltperson eller gruppe – eller en innsider, dvs. en som arbeider i virksomheten og som har lovlig adgang til områder og tilgang til systemer. Når man vurderer trusselaktøren vurderer man gjerne vedkommendes *kapasitet* og *intensjon*.

Barrierer er tiltak som tidlig skal detektere trusler, forsinke en trusselaktørs angrep slik at man kan iverksette nødvendige mottiltak og på den måten hindre et vellykket angrep eller annen bevisst og ondsinnet handling. Tiltakene kan være teknologisk tiltak, organisatoriske eller menneskelige tiltak. Se mer om tiltak i neste kapittel, kapittel 4.1.3.

Ofte vurderes disse tre faktorene når sikringsrisiko skal vurderes. Virksomheten besitter en elle flere verdier og disse kan bli utsatt for en trussel – trusselaktøren tiltrekkes av verdien. Sårbarheter i virksomheten gjør verdien lettere tilgjengelig, og trusselaktøren forsøker å utnytte disse svake punktene for å få tilgang til verdien. Dette kan illustreres av figuren nedenfor.



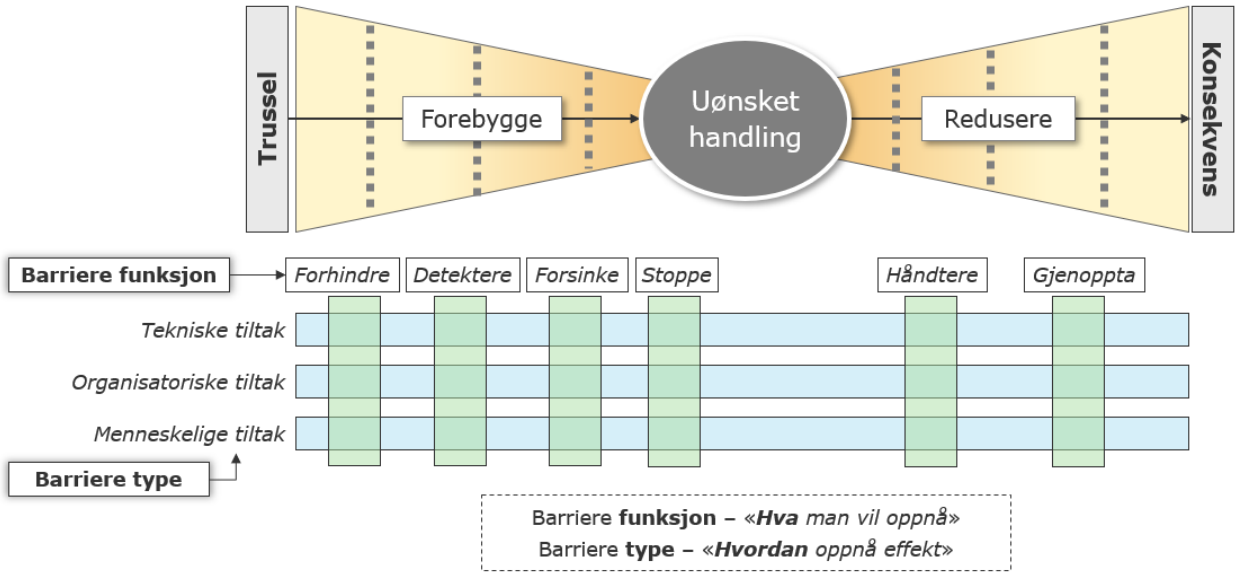
Figur 4-2: Trefaktormodellen benyttes ofte for å beskrive sikringsrisiko – sammenhengen mellom en verdi, trussel og sårbarhet

Siden det normalt er lite en virksomhet kan gjøre for å redusere en *ekstern* trussel, vil de fleste tiltak for å redusere sikringsrisikoen normalt være knyttet til å redusere sårbarhetene. Derimot, overfor en *intern* trusselaktør har virksomheten en større mulighet til å påvirke denne gjennom f.eks. å sikre at arbeidstakere blir godt ivaretatt og føler seg fornøyde med egen arbeidsgiver.

4.1.3 Generelt om barrierer

Barrierer skal, ifølge Styringsforskriften § 5, oppdage tilløp til hendelser, hindre utviklingen av et hendelsesforløp og begrense skader. Det samme gjelder også i forbindelse med sikring mot planlagte, bevisste handlinger. Barrierer er tiltak som skal ha som funksjon å beskytte dersom virksomheten blir utsatt for bevisst uønsket handling, utført av en person eller en gruppe – enten av noen fra utsiden eller noen fra innsiden.

Som illustrert i figuren under skal tiltakene ha en *funksjon* – man ønsker å oppnå noe med de tiltakene man iverksetter. Videre er det slik at tiltakene er av en viss *type* – det kan være tekniske tiltak, organisatoriske tiltak eller menneskelige tiltak, som sammen sikrer at man oppnår den effekten man ønsker.



Figur 4-3: Barrierer – deres funksjon og type – for å forhindre en uønsket handling, og for å redusere konsekvensene av denne

Barrierenes *funksjon* angir *hva man ønsker å oppnå* med tiltaket:

- *Forhindre* – tiltaket skal primært sørge for at en uønsket handling ikke blir planlagt eller igangsatt. Dette skjer enten ved å gi inntrykk av at det ikke er mulig å gjennomføre en planlagt handling eller at denne ikke vil bli vellykket (avskrekke fra å igangsette), eller ved å skape forhold/oppfatninger som ikke utløser ønske om å planlegge eller igangsette en uønsket handling.
- *Detektere* – oppdage adferd, forsøk på inntrengning eller annen handling, så tidlig som mulig, slik at eventuelle mottiltak kan iverksettes før trusselaktøren når målet sitt.

- *Forsinke* – tiltak som forsinker utførelsen av handlingen, slik at man sparer tid og rekker å iverksette eventuelle umiddelbare mottiltak.
- *Stoppe* – er tiltak som skal vanskeliggjøre adkomst til kritiske områder, være seg fysiske eller elektroniske områder, dette er ofte tiltak av teknologisk karakter.

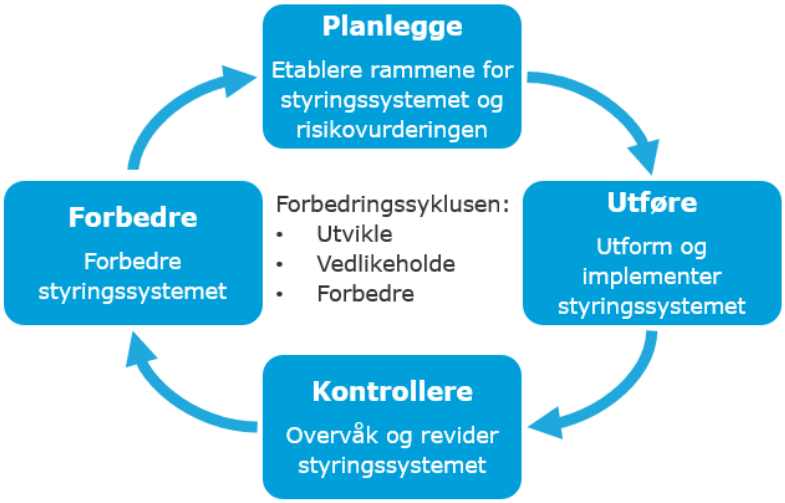
Barrierene kan være av *typen*[2]:

- *Teknologiske tiltak* - Utstyr og systemer som inngår i realiseringen av en barrierefunksjon, som fysiske tiltak (f.eks. dører, låser, sperrer), elektroniske tiltak (f.eks. sensorer, alarmer, kameraovervåking) eller logiske tiltak (f.eks. passord, PIN koder)
- *Organisatoriske tiltak* – Tiltak i form av skriftlige eller muntlige beskrivelser, vurderinger og beslutninger som regulerer ledelse, organisering, prosesser, analyser, rutiner, adferd og/eller anvendelse av andre sikringstiltak.
- *Menneskelige tiltak* – Tiltak som påvirker persepsjon, vurderingsevne, kunnskap, adferd og reell evne til å bruke teknologiske sikringstiltak og følge organisatoriske sikringstiltak.

4.1.4 Generelt om styring av sikring

Sikringsledelse er i utgangspunktet det samme som annen ledelse – det følger de samme prinsipper. Det finnes flere standarder og veiledninger som adresserer det samme, og som beskriver dette rundt forbedringssirkelen ofte kjent som PDCA (Plan-Do-Check-Act). På norsk er denne gjerne omtalt som PUKK (Planlegge-Utføre-Kontrollere-Korrigere), eller som PUKF (Planlegge-Utføre-Kontrollere-Forbedre). Forskjellige varianter er presentert i bl.a. internasjonale standarder som ISO 31000:2018 og ISO 9001:2015, og i nasjonale standarder og veiledninger som NS 5832:2015 og NSMs to veiledninger om sikkerhetsstyring fra hhv. 2015 (ref. /15/) og 2019 (ref. /20/).

Figuren nedenfor er hentet fra NSMs veileder i sikkerhetsstyring fra 2019.



Figur 4-4: Styring og kontinuerlig forbedring

[2] Inndelingen og definisjonen er hentet fra hhv. NS 5830:2012 «*Samfunnssikkerhet. Beskyttelse mot tilsiktede uønskede handlinger. Terminologi*», og NSMs veileder «*Sikkerhetsstyring*». Til orientering, Ptil benytter inndelingen Teknologiske, Organisatoriske og Operasjonelle tiltak (se ref. /17/).

Styringssystemet for sikring bør i samordnes med virksomhetens øvrige styringssystem. Dette vil gi grunnlag for felles tilnærming i håndteringen av de risikoer virksomheten står overfor. Med utgangspunkt i prinsippene for styring av sikring vil det være mulig å identifisere de deler av eksisterende virksomhetsstyring som kan utvides og tilpasses til også å dekke forebyggende sikringsarbeid. Eksempler kan være virksomhetens opplegg for opplæring og kompetanseheving, rutiner for hendelsesrapportering, interne revisjoner m.m.

4.2 Spesielt om innsiderisiko

4.2.1 Innsideren – de forskjellige kategoriene

Begrepene innsiderisiko, innsidetrussel og personellsikkerhet brukes litt om hverandre, litt avhengig av sammenhengen. Det finnes ingen entydig definisjon av verken innsider eller av personellsikkerhet. Standarden *ISO 22300 Security and resilience – Vocabulary* (ref. /12/) omtaler verken *insider* eller *personnel security*. Derimot har de forskjellige organisasjonene og selskapene benyttet sine egne forklaringer på begrepene. Det gjennomgående er at disse stort sett adresserer bare de bevisste handlingene.

Definisjonen nedenfor er hentet fra fellesdokumentet utgitt av NSM, Politiet, PST og NSR (*Sikkerhet ved ansettelsesforhold*, ref. /19/). Denne definisjonen er igjen hentet fra en håndbok utgitt av de australske myndighetene (*Managing the insider threat to your business*, ref. /47/).

> «*Innsider er en nåværende eller tidligere ansatt, konsulent eller kontraktør som har eller har hatt autorisert tilgang til virksomhetens systemer, prosedyrer, objekter og informasjon, og som misbruker denne kunnskapen og tilgangen for å utføre handlinger som påfører virksomheten skade eller tap*».

En innsider kan normalt deles tre kategorier – knyttet til personer som bevisst utfører en handling i den hensikt å påføre skade eller tap, eller for å oppnå egen vinning. Denne inndelingen og beskrivelsen nedenfor er hentet fra veilederen *Sikkerhet ved ansettelsesforhold*, ref. /19/:

- *Infiltratøren* – vedkommende er plassert i virksomheten av en tredjepart som ønsker å utnytte tilgangen vedkommende gis.
- *Rekrutterte* – en person som enten er utsatt for press av en tredjepart til å utføre en handling, eller en som utfører handlingen frivillig, f.eks. mot betaling, eller pga. politisk eller ideologisk overbevisning.
- *Selvmotiverte* – en person som gjennomfører den bevisste handlingen på eget initiativ og i utgangspunktet ikke har kontakt med eller styres av en tredjepart.

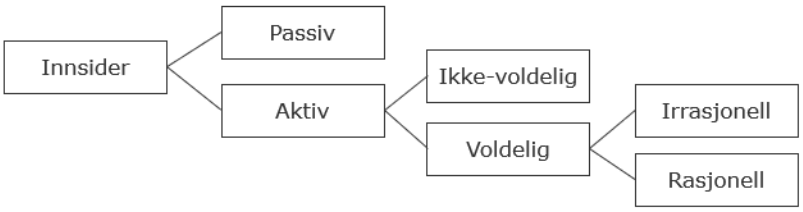
Det er verdt å merke seg at noen av referansene, spesielt de som fokuserer på IT-sikkerhet, også inkluderer uforvarende/ikke-villede handlinger utført av ansatte, eller andre med lovlig tilgang til systemer, dvs. handlinger som ikke er bevisste. Vedkommende kan ha gjort en feilhandling på grunn av manglende kompetanse eller forståelse, eller vedkommende kan ha vært sliten og ukonsentrert. Dette gjelder f.eks. referansene /49/, /61/ og /75/.

I den ovennevnte veilederen *Sikkerhet ved ansettelsesforhold* (ref. /19/) omtales også en kategori knyttet til uvitenhet eller unøyaktighet, dog uten at denne inkluderes i definisjonen av en innsider.

- *Uforvarende* – en som uten å forstå eller ville det, gjennomfører en handling som resulterer i økt sårbarhet, skade eller tap for virksomheten. Vedkommende kan ha blitt manipulert eller forledet

eller vedkommende har ikke kompetanse til å forstå konsekvensene av handlingen sin. Eventuelt kan vedkommende være i en sinnstilstand der uoppmerksomhet eller sløvhet medfører at handlingen blir utført uten at dette er tilsiktet.

En annen måte å kategorisere innsideren på kan være gjennom figuren og beskrivelsen nedenfor (hentet fra IAEA Nuclear Security Series, *Preventive and Protective Measures against Insider Threats,* ref. /57/)



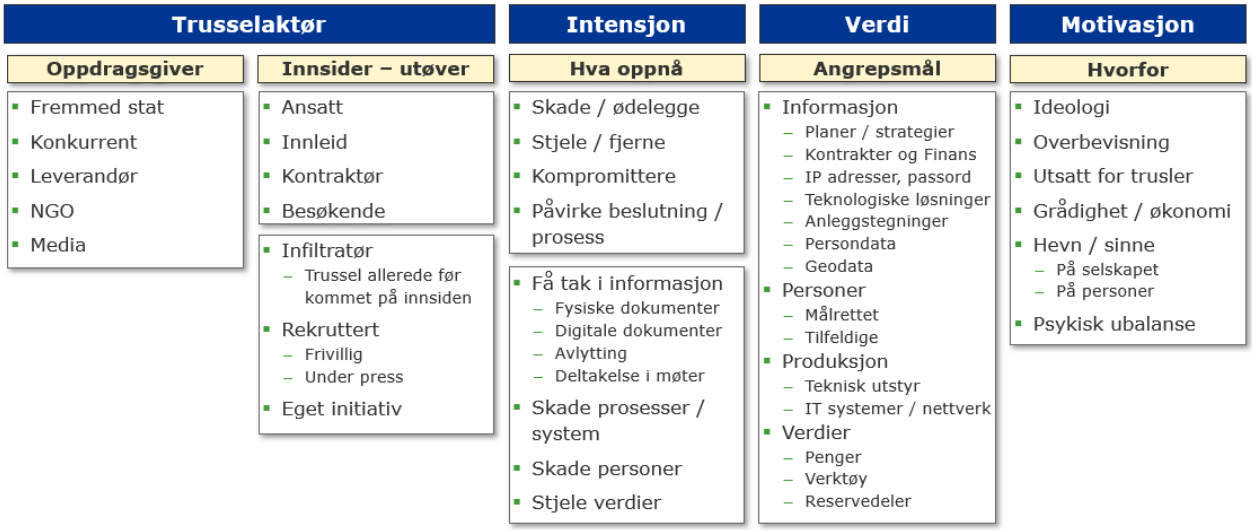
Figur 4-5: Kategorier av innsidere, bevisste handlinger (ref. IAEA)

Figuren ovenfor illustrerer at de forskjellige kategoriene av innsidere kan ha forskjellige motivasjoner for sitt engasjement – de kan være passive eller aktive, voldelige eller ikke-voldelige. Den «passive» innsideren er ikke-voldelig og begrenser sin handling til å fremskaffe lett tilgjengelig informasjon som utnyttes av en tredjepart. Den «aktive» innsideren er villig til å fremskaffe informasjon, utføre visse handlinger og kan være voldelig eller ikke-voldelig. En aktiv innsider kan være villig til å åpne dører eller låser, bistå direkte i et anslag mot virksomheten, f.eks. gjennom å hindre innsatspersonell i å utføre sine oppgaver. Ikke-voldelige aktive innsidere er ikke villige til å bli identifisert, eller er ikke villige til å ta risikoen med å bli konfrontert med innsatspersonell – de kan begrense sin deltakelse med f.eks. å tukle med adgangssystemer eller andre sikringssystemer. Den voldelige aktive innsideren kan bruke vold eller annen tvang, og de kan handle rasjonelt eller irrasjonelt (hentet fra ref. /57/).

Videre i denne rapporten er innsidetrusselen og tilhørende tiltaksforslag knyttet til de bevisste handlingene (ref. definisjonen over). Likevel vil mange av de foreslåtte tiltakene ha effekt også overfor de ubevisste handlingene.

4.2.2 Karakteristika på en innsider – hvem, hvorfor og hva

For å håndtere innsidetrusselen på en god måte er det nødvendig å forstå hvem innsideren kan være, og hvordan og hvorfor vedkommende har blitt en trussel, og hvordan vedkommende opererer. Figuren under sammenfatter de viktigste forholdene rundt en innsider.



Figur 4-6: Innsideren, hva vil vedkommende oppnå, hvordan og hvorfor

Hvem er innsideren

Innsideren kan være en ansatt, en innleid konsulent, en person fra et innleid selskap som er på arbeidsplassen i kortere eller lengre perioder (f.eks. rengjøringspersonale), eller en besøkende (f.eks. kunde eller konkurrent). I noen situasjoner handler en innsider på eget initiativ da vedkommende ser en egen vinning i f.eks. å stjele verdisaker eller tilegne seg informasjon helt på egen hånd, mens i andre sammenhenger kan en innsider handle på vegne av en tredjepart – oppdragsgiver – som står bak bestillingen. Handlingen kan være nøye planlagt og gjennomtenkt, eller den kan komme som en ren impulshandling, f.eks. ved å utnytte muligheten som tilfeldigvis var der – en opportunistisk handling.

I en studie CPNI fra (2013) der man undersøkte mer enn 120 innsidehendelser fra både offentlig og privat sektor (ref. /44/), fant man at i 88 % av hendelsene var disse uført av fast ansatte, 7 % involverte kontraktører og bare 5 % gjaldt innleide. De fleste hendelsene var utført av menn (82 %). I 60 % av tilfellene var det utført personer som hadde arbeidet mindre enn fem år i virksomheten. I mer enn halvparten av tilfellene ble det oppdaget ila. det første året. Disse tallene er også gjengitt i en rapport fra de australske myndigheter (ref. /47/)

Selskapet Crown Research Partners publiserte i 2018 en rapport om innsidertrusselen knyttet til IT-sikring (ref. /72/, og kapittel F.2 i Appendix F). Rapporten påpeker at innen IT-sikring assosieres ofte begrepet innsidertrussel med ansatte som har med ondsinnete intensjoner om å skade selskapet gjennom tyveri eller sabotasje, men at sannheten imidlertid er at uaktsomme ansatte eller kontraktører utgjør en like stor trussel – dvs. ikke-villede handlinger. Videre fremhever rapporten at de spurte anser først og fremst egne ansatte og de med lovlig tilgang til systemer som de største truslene (ca. 55 % av de intervjuete svarte dette), mens bare 42 % mente at kontraktører og innleide utgjør den største trusselen.

Hvorfor utfører innsideren en handling

Intensjonen bak handlingen kan være en av flere. Innsideren selv, eller tredjeparten innsideren utfører handlingen på oppdrag for, kan ønske å skade virksomhetens omdømme, eller skape problemer eller forsinkelser i produksjonen. Motivasjonen for dette kan være så mangt, som f.eks. ideologi eller politisk

overbevisning, skape egne konkurransefordeler eller ønsket om hevn på grunn av opplevd dårlig behandling, f.eks. i en oppsigelsesprosess, dårlig ledelse eller andre arbeidsforhold.

Alternativt kan det være et ønske om å skade eller true personer i virksomheten, enten fysisk eller psykisk. Motivasjonen for dette kan være hevn på grunn av opplevd dårlig behandling eller dårlige kollegiale forhold, eller vedkommende kan være i psykisk ubalanse. I verste fall kan det dreie seg om å utnytte en innsider for å planlegge eller gjennomføre en terroraksjon.

Mht. hva som motiverer en innsider, viste tall fra CPNI-studien (ref. /44/) at økonomisk gevinst er den mest vanlige motivasjon (oppgitt i 47 % av hendelsene) etterfulgt av ideologi (20 %), anerkjennelse (14 %), lojalitet (14 %), og hevn (6 %).

Innsideren selv, eller vedkommendes oppdragsgiver, kan ønske å tilegne seg informasjon eller fysiske verdier som innsideren selv enten kan ha direkte nytte av eller selge videre til andre. Informasjon om økonomiske forhold, tekniske løsninger eller nyvinninger (Intellectual Property – IP), kontrakter, timepriser osv. kan også være av interesse for virksomhetens konkurrenter.

En innsider kan også ha som mål å påvirke prosesser eller beslutninger som vil være til egen eller oppdragsgivers fordel. Dette kan være knyttet til kontrakter, innkjøp eller oppkjøp m.m.

Underslag eller tyveri av verdier av forskjellige kategorier er gjerne knyttet til ønsket om egen vinning. Underslag er en kriminell handling som går ut på å tilegne seg en løsøregjenstand eller en annen verdi som helt eller delvis tilhører en annen, men som man er i besittelse av. Underslag skiller seg altså fra tyveri ved at man allerede er i besittelse av eller har tilgang til gjenstanden eller verdien, og noen besittelsesforrykkelse finner dermed ikke sted.

Hva angriper en innsider

CPNI har identifisert fem hovedtyper av innsideaktivitet (ref. /44/):

- Uautoriserte avsløringer av sensitiv informasjon
- Prosesskorrupsjon[3]
- Hjelpe en tredjepart til å få tilgang til en organisasjons verdier
- Fysisk sabotasje
- Sabotasje på IT eller annet elektronisk utstyr.

CPNI-studien viste at blant disse hendelsene var de hyppigst forekomne uautorisert avsløring av sensitiv informasjon (47 %) og prosesskorrupsjon (42 %).

I en annen studie utført av Crown Research Partners (ref. /72/) har man sett på hvilken type informasjon som er mest sårbar overfor innsiderangrep. Øverst på listen kommer konfidensiell forretningsinformasjon (finansiell, kundedata o.l.), dernest informasjon om bruker- og påloggingsdata (brukernavn, passord osv.), så sensitiv personinformasjon etterfulgt av åndsverk/immateriell eiendom (Intellectual Property) og informasjon om drift og infrastruktur.

[3] Prosesskorrupsjon er definert som en ikke-lovlig endring/tukling med en intern prosess eller system. Som eksempel, en som manipulerer økonomisystemet for å påvirke utbetalinger eller skjule forhold i regnskapet.

4.2.3 Innsideren – Modus Operandi kort oppsummert

Infiltratøren

Infiltratøren er gjerne engasjert av en organisasjon, eller arbeider på vegne av myndighetene i et fremmed land. Infiltratørens oppgave er å komme på innsiden av en organisasjon – som regel ved at vedkommende blir ansatt eller innleid i virksomheten – for så senere å kunne hente ut sentral informasjon på vegne av oppdragsgiveren eller utføre konkrete oppdrag som f.eks. å observere og dokumentere uetiske handlinger utført av virksomheten eller andre ansatte i virksomheten, påvirke beslutningsprosesser, skade nettverk eller infrastruktur m.m.

Planleggingshorisonten kan være lang – oppdragsgiveren kan ha plantet infiltratøren med det for øye at vedkommende skal bruke lang tid på å bli kjent i organisasjonen, og kanskje klatre i hierarkiet. Dermed kan det eventuelt ta flere år før innsideren begynner å utføre sine handlinger med f.eks. å hente ut informasjon eller påvirke prosesser.

Infiltratøren kan være godt utdannet og kanskje være en spesialist innen sitt fagområde. Samtidig kan vedkommende også være godt trenet i hvordan arbeide skjult som en innsider, for ikke å bli oppdaget. Innsideren er sannsynligvis godt skolert og forberedt, og har et godt apparat i ryggen.

I forbindelse med ansettelsesprosessen er det naturlig å anta at det meste er planlagt og lagt godt til rette slik at en vanlig bakgrunnssjekk vanskelig vil kunne avdekke noe mistenkelig ved vedkommende. Utdannelsen og økonomien er i orden, det er sannsynligvis ingen hull i vedkommendes CV og all informasjon kan sannsynligvis verifiseres.

Etter at infiltratøren er ansatt, vil vedkommende sannsynligvis legge vekt på å oppføre seg normalt og unngå å pådra seg uønsket oppmerksomhet.

Det er imidlertid indikasjoner på at totalt sett utgjør infiltratøren en liten andel. Både CPNI (ref. /44/) og australske myndigheter (ref. /47/) anslår at infiltrasjon står for bare 6 % av tilfellene. Dog er det rimelig å anta at trusselen gjennom infiltrasjon vil kunne variere mellom type virksomheter – noen vil være mer utsatt enn andre.

Rekruttert innsider

Den rekrutterte innsideren er en som utfører en ulovlig handling på vegne av en tredjepart (oppdragsgiveren) – enten frivillig eller fordi vedkommende er under press. Rekrutteringen skjer gjerne etter at personen har fått tilgang til virksomheten – vedkommende er allerede ansatt eller er engasjert i et prosjekt/arbeid som gir vedkommende lovlig tilgang til deler av virksomheten, f.eks. gjelder dette innleide konsulenter, personer som utfører vedlikehold, renholdspersonale osv.

Den rekrutterte kan få i oppgave enten å fremskaffe informasjon fra innsiden av organisasjonen, å påvirke beslutningsprosesser, fjerne/stjele utstyr som er kritisk for virksomheten, utføre sabotasje mot prosesser, systemer og utstyr, eller til og med skade eller true personer.

Den rekrutterte innsideren kan være uerfaren i oppgaven og kanskje til og med ukomfortabel i situasjonen, spesielt dersom vedkommende er satt under press. Resultatet kan være at den ukomfortable situasjonen medfører endring i adferd, endringer som muligens nære kollegaer kan legge merke til. Eksempler på slik adferdsendring er at vedkommende blir mer nervøs, er mindre sosial og holder seg mer for seg selv, arbeider til unormale tider, får dyre vaner og bruker mer penger osv.

Rekruttert innsider – Frivillig: En arbeidstaker kan bli kontaktet av en tredjepart og bedt om å utføre noen ulovlige handlinger som f.eks. å fremskaffe sensitiv informasjon fra eller om virksomheten eller om

utvalgte personer, eller å utføre sabotasje mot anlegg, prosesser eller nettverkssystemer, eller forsøke å påvirke en beslutningsprosess. Kontakten kan tilby penger eller andre goder, alternativt kan den rekrutterte ønske å utføre oppgaven uten motytelser, motivert i f.eks. ideologi, ønske om å skade virksomhetens omdømme m.m.

Rekruttert innsider – Utsatt for press: En arbeidstaker i en virksomhet kan bli blir utsatt for trusler av en tredjepart, og på den måten blir vedkommende presset til å utføre en handling. Dette er kan være å fremskaffe informasjon som krever at innsideren utnytter sin tilgang eller kjennskap til virksomheten. En annen mulighet er at innsideren blir presset til å utføre en sabotasjehandling eller tukle med systemer slik at tredjeparten selv kan utføre et eget angrep mot virksomheten i kjølvannet av innsiderens handling. Det er flere måter en person kan utsettes for press på. Vedkommende kan f.eks. ha blitt lurt inn i en pinlig situasjon som er blitt dokumentert (bilder, video) og deretter trues det med å offentliggjøre materialet. Eller, tredjeparten kan fremsette trusler om å skade vedkommende eller dennes familie dersom ikke vedkommende gjør som han/hun blir bedt om.

Honningfelle (Honey trap) er situasjoner der en person blir forført og lurt inn i et kortvarig seksuelt forhold eller langvarig romantisk/følelsesmessig forhold, og på den måten blir presset eller lurt til å fremskaffe sensitiv informasjon. Kanskje benyttes det fotografiske bevis fra et seksuelt forhold som så benyttes til å presse vedkommende for informasjon eller andre tjenester.

Rekruttert innsider – lurt: En tredjepart med uærlige hensikter kan benytte sosial manipulering eller andre metoder for å etablere en god relasjon til en arbeidstaker i en virksomhet (om sosial manipulering, se også nedenfor under «Uforvarende innsider»). Tredjeparten kan så, når relasjonen er etablert, be arbeidstakeren om å fremskaffe informasjon som i utgangspunktet kan synes ufarlig, f.eks. informasjon om selskapet som uansett ligger åpent tilgjengelig på nettet. Etter hvert etterspørres mer informasjon som gradvis er mindre offentlig tilgjengelig og som krever noe mer aktiv innsats fra den fortsatt uvitende og kanskje godtroende arbeidstakeren. Til slutt kan man være «fanget i nettet», og tredjeparten utnytter det at vedkommende har fremskaffet informasjon som er i gråsonen mellom offentlig tilgjengelig og kanskje er klassifisert som «bare» intern. Etterfølgende argumentasjon om at «*….du har jo allerede fremskaffet interne prosedyrer…..*» kan så bli til trusler om å fremskaffe ytterligere informasjon.

Selvmotiverte innsider

Den selvmotiverte kan iverksette en ulovlig handling basert på egen interesse, f.eks. tyveri av verdisaker som penger, elektronisk utstyr, verktøy, kritiske deler, foreta underslag, tilegne seg sensitiv informasjon m.m.

Tyveri av visse kritiske reservedeler og spesialverktøy kan i verste fall gi store forsinkelser i produksjonen med tilhørende økonomiske tap. I tillegg kan dette også gå ut over selskapets renommé.

Slike stjålne verdisaker kan enten benyttes av innsideren selv, eller vedkommende kan selge dette videre til en tredjepart. Videre kan også sensitiv informasjon om selskapet, eller om enkeltindivider, samles og selges til en tredjepart. Basert på innsiderens egenmotivasjon eller politiske holdning, kan slik informasjon også formidles videre, uten vederlag, til andre i den hensikt å skade

Case: Selskapet oppdaget underslag ved et kontor i USA, av en person som hadde tilgang og mulighet til å utstede fakturaer og utføre overføringer. I forbindelse med granskingen av saken kom vedkommende med trusler mot både selskapet og mot enkeltpersoner.

selskapets eller en kollegas renommé. Mottakere kan være media som ønsker å samle informasjon for å lage en nyhetssak med negativ vinkling om virksomheten, eller NGO-er som ønsker å benytte dette i forbindelse med planlegging eller gjennomføring av en aksjon mot virksomheten.

En person som har autorisert tilgang til virksomhetens bankkonto vil kunne på ulovlig vis overføre penger til egen konto og på den måten begå underslag. Se også mer om *misligheter* omtalt under.

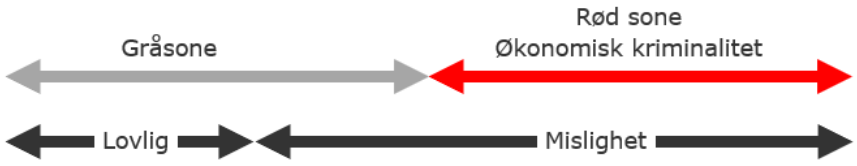
Det er viktig å være klar over at en person som stjeler en fysisk gjenstand, eller tilegner seg lett tilgjengelig informasjon, ikke nødvendigvis trenger å ha planlagt dette i forkant. Vedkommende kan tilfeldigvis komme i en situasjon der verdigjenstander eller dokumenter er lett tilgjengelig, eller en PC-skjerm står åpen og viser interessant og sensitiv informasjon som er lett å avfotografere. Dette kan være et lett og fristende bytte for en som utnytter muligheten der og da.

Den selvmotiverte innsideren kan være uerfaren i oppgaven og kanskje endre i adferd, endringer som muligens nære kollegaer kan legge merke til. Eksempler på slik adferdsendring er at vedkommende blir mer nervøs, er mindre sosial og holder seg mer for seg selv, arbeider til unormale tider, får dyre vaner og bruker mer penger osv.

Besøkende: I tillegg til kategorien omtalt over – som gjelder ansatte, innleide eller andre kontraktører – vil besøkende som er på møte i bygget, også kunne utgjøre en trussel. Dette kan gjelde konkurrenter, partnere, leverandører, media, NGO-er m.m. som er på besøk en kort tid, f.eks. deltar på et møte. I den sammenhengen vil de kunne tilfeldig komme over informasjon som de vil kunne dra nytte av eller misbruke. Dette være seg at de overhører en samtale mellom to arbeidstakere i et fellesområde, ser og avfotografere informasjon på en ulåst PC-skjerm og ingen andre er tilstede, stjele eller avfotografere fysiske dokumenter som ligger på et bord der gjesten har tilgang.

Spesielt om mislighet (teksten nedenfor er hentet fra ref. /41/):

Begrepet *mislighet* benyttes og er definert i en revisjonsstandard som «*en bevisst handling begått av en eller flere personer innen ledelsen, av personer som har overordnet ansvar for styring og kontroll, av ansatte eller andre, som innebærer uredelighet for å oppnå en urettmessig eller ulovlig fordel*». Ordet *uredelighet* omfatter handlinger som tilslører, fordreier eller skjuler de virkelige forhold. Riksrevisjonen mener at det er et bredt spekter av handlinger som kan oppfattes å grense mot eller være misligheter.



Figur 4-7: Misligheter, gråsone og økonomisk kriminalitet

Mislighet er et videre begrep enn økonomisk kriminalitet. Den røde sonen inneholder økonomisk kriminalitet med straffbare handlingene som omfatter blant annet korrupsjon, bedrageri, underslag og regnskapslovbrudd. Gråsonen i figuren over inneholder både (a) handlinger som kan være ubevisste feil og som ikke er misligheter, og (b) handlinger som oppfattes som uetiske og/eller er brudd på regler, normer og standarder.

Misligheter i forbindelse med regnskapene omtales ofte som *regnskapsmanipulasjon* og handler om brudd på bestemmelsene i bokføringsloven eller regnskapsloven. I det norske språket finner man flere

begreper som er nære synonymer til regnskapsmanipulering, som regnskapssvindel, regnskapsjuks, resultatstyring, kreativ regnskapsføring og rapporteringsstrategi.

For at en person skal begå en mislighet må det foreligge tre forhold som ofte er definert i den såkalte mislighetstrekanten. En mislighet kan skje når: a) en person opplever en mulighet for mislighet, b) personen opplever et press eller behov, og c) personen mener å kunne forsvare og rettferdiggjøre sine handlinger.

Uforvarende innsider

I tillegg har man den som uforvarende som uten å forstå det, gjennomfører en handling som resulterer i økt sårbarhet, skade eller tap for virksomheten. Vedkommende kan ha blitt manipulert eller forledet eller har ikke kompetanse til å forstå konsekvensene av handlingen sin.

Den uforvarende innsideren er en person som selv ikke har intensjon om å gjøre noe ulovlig, men vedkommende gjør en uautorisert handling uten at vedkommende er klar over dette og heller ikke har ønske om å gjøre noe ulovlig. Vedkommende kan ha blitt manipulert eller forledet av en tredjepart til å utføre handlingen, uten å være klar over dette, som å fortelle noe om virksomheten eller kollegaer som f.eks. et prosjekt, oppkjøpsplaner, en persons spesielle legning eller interesse og liknende, noe som en tredjepart kan planlegge å utnytte. I denne sammenhengen kan sosial manipulering være en metode for å skape en god relasjon som danner grunnlaget for å tappe den ansatte for informasjon.

Sosial manipulering (Social engineering) referer til manipulering der man prøver å lure den ansatte til å oppgi sensitiv informasjon gjennom f.eks. å skape en sosial relasjon. Tredjeparten kan ha benyttet informasjon fra Facebook eller andre sosiale medier til å gjøre seg kjent med den ansattes fritidsinteresser eller andre interesseområder, og utnytter dette til å skape en god relasjon med vedkommende.

Også handlinger utført av den interne, handlinger som ikke er bevisste eller ondsinnete, kan få konsekvenser. Manglende kompetanse, forståelse eller innsikt kan medføre at informasjon kommer på avveie eller at systemer blir utsatt. Studien til Crowd Research Partners (ref. /72/, og kapittel F.2 i Appendix F) antyder at uaktsomme ansatte og kontraktører utgjør en tilnærmet like stor risiko som beviste handlinger fra en innsider med ondsinnete intensjoner.

Uaktsomme personer kan også, uten å mene det, føre til at sensitiv informasjon kommer «i hendene» på en tredjepart som så kan misbruke eller utnytte den. Eksempler kan være en samtale med kollega om sensitiv prosjekt- eller personinformasjon på et offentlig sted som tilfeldigvis blir overhørt av noen som sitter ved siden av, bruk av PC på åpne og usikrete nett på hotellrom eller flyplasser, bruk av PC på flytoget eller flyet slik at andre lett kan lese skjermbildet, ta med seg ikke-vaskete PC-er eller mobiltelefoner på reise til enkelte utsatte land, koble til andres USB-minnepinner på egen PC, ikke låse skjermen når man forlater PC-en på kontoret eller i møter med andre, ikke følge interne rutiner om håndtering av sensitiv informasjon ved f.eks. å ta denne med seg ut av kontoret og hjem – eksemplene er mange.

4.2.4 Barrierer knyttet til innsiderisiko

I forbindelse med innsiderisiko er det spesielt barrierer / tiltak knyttet til den ansatte, innleide konsulenter og andre kontraktører som gis spesiell fokus. Dette gjelder hele prosessen fra før vedkommende blir engasjert i virksomheten, mens vedkommende er engasjert og gjennom hele

avslutningsprosessen (oppsigelse eller avslutning av kontraktsforhold). Dette kan illustreres i figuren nedenfor.

Figur 4-8: Fasene i et arbeidsforhold kan deles inn i tre – før, under og avslutning

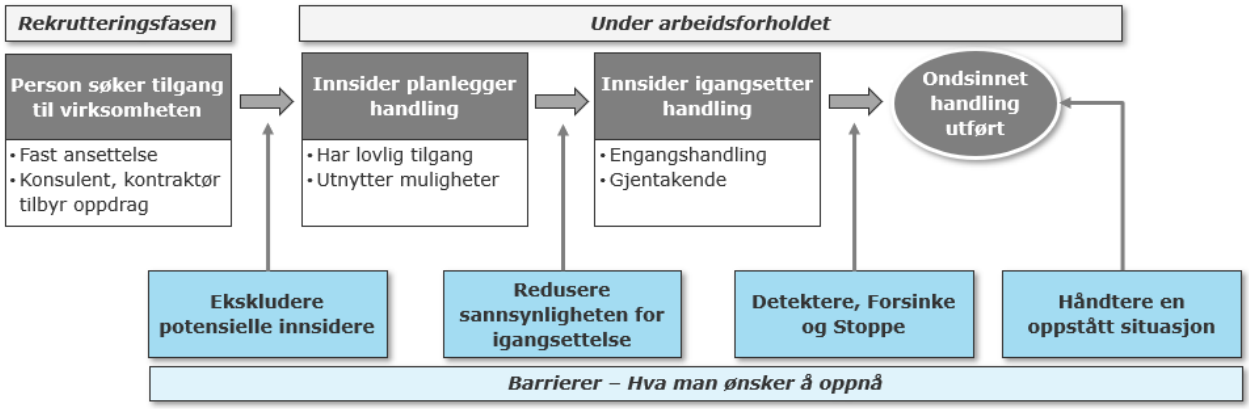
De barrierer og andre tiltak som iverksettes for å håndtere innsiderisikoen er naturlig knyttet til disse tre fasene. I tillegg er det en del generelle virksomhetsgenerelle tiltak som også bør være på plass, som en del av virksomhetens generelle styringssystem for sikring (ref. kapittel 4.1.4). Håndtering av innsiderisiko går i korthet ut på følgende fire elementer.

Først og fremst gjelder det å forhindre at en potensiell trusselaktør (innsider) får tilgang til virksomheten, enten gjennom å bli ansatt, eller å utføre oppdrag innen virksomhetens «fire vegger».

For det andre handler det om å unngå at en som allerede har lovlig tilgang til virksomheten og dens systemer utvikler seg til å utgjøre en innsidetrussel. Det å skape fornøyde arbeidstakere vil redusere sannsynligheten for at de utvikler seg til å bli misfornøyde og dermed ville ønske å gjøre noe ulovlig eller annet som kan skade virksomheten. Det er viktig å ha forståelse for at i motsetning til eksterne trusler – der det normalt er lite virksomheten selv kan gjøre for å påvirke trusselaktøren – er interne trusler noe virksomheten i større grad selv kan påvirke, gjennom å legge til rette for at arbeidstakere føler at de blir godt ivaretatt av egen arbeidsgiver.

For det tredje, skulle en innsider likevel igangsette uønskede handlinger må man prosesser, teknikker og en kultur på plass for å oppdage dette så tidlig som mulig og iverksette mottiltak for å forhindre at innsideren får gjennomført sin ondsinnete handlingen.

For det fjerde, skulle en uønsket handling bli gjennomført må man være forberedt og kunne håndtere situasjonen slik at konsekvensene begrenses. Disse fire stegene er illustrert i figuren under.



Figur 4-9: Tilnærming for å forebygge en ondsinnet handling; de enkelte fasene og tilhørende barrierer

5 GOD PRAKSIS FOR HÅNDTERING AV INNSIDETRUSSELEN

Dette kapittelet sammenfatter god praksis mht. å håndtere innsidetrusselen. De foreslåtte tiltakene er basert på innspill gitt gjennom workshopen 5. mars, dybdeintervjuene og beskrivelser funnet i den gjennomgåtte litteraturen. Tiltakene er forløpende nummerert, slik at nummereringen gjenkjennes i tiltaksopplisting i modenhetsverkøyet i Appendix C.

5.1 Introduksjon

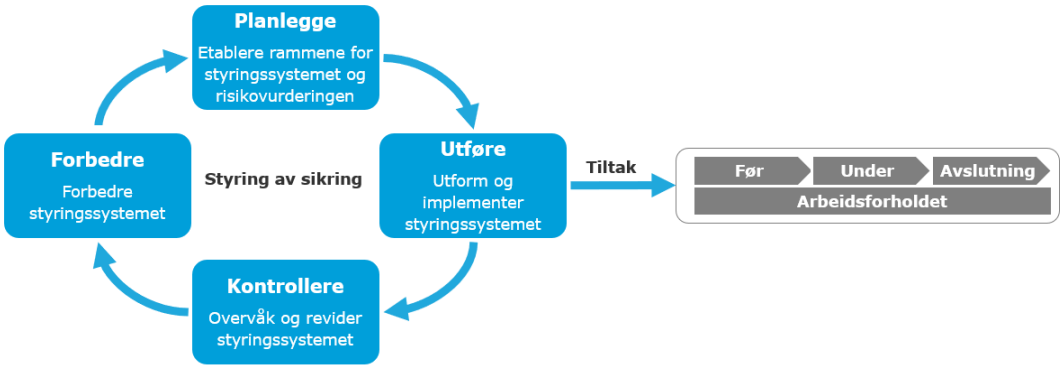
I forbindelse med god praksis er det enkelte lærepunkter som kan være nyttige å kjennskap til. Dette er lærepunkter over hva man ikke skal anta – lærepunkter som NATO har beskrevet i sitt dokument (Insider Threat Detection Study, ref. /75/). I utgangspunktet er dette dokumentet knyttet til IT-sikkerhet, men lærepunktene er likevel relativt generelle.

1. Ikke anta at alvorlige innsideproblemer ikke finnes i min organisasjon
2. Ikke anta at bakgrunnssjekker løser innsideproblemet
3. Ikke anta at annonserte «red flags» blir lest skikkelig
4. Ikke stol på enkeltstående beskyttelsestiltak
5. Ikke anta at organisasjonskultur og ansattes misnøye ikke betyr noe
6. Ikke glem at innsidere kan kjenne til sikringstiltak og dermed vet hvordan man kan omgå disse
7. Ikke anta at sikringsregler følges
8. Ikke anta at bare bevisste, ondsinnede handlinger fra en innsider betyr noe – de ubevisste handlingene mer vanlige enn bevisste, ondsinnete handlinger
9. Ikke fokuser bare på forebyggende tiltak, og dermed overse konsekvensreduserende tiltak

Videre har CPNI i sin undersøkelse påpekt at det er en klar kobling mellom innsiderisikohendelser og svakheter i forebyggende sikring og ledelsesprosesser (ref. /44/). Hvert av punktene er ytterligere utdypet og forklart i omtalen i Appendix F, kapittel F.2.A.

- *Mangelfull ledelse* – tar ikke tak i problemer
- *Mangelfull bruk av revisjonsfunksjonen* – fanger ikke opp irregulariteter
- *Mangelfulle beskyttelsestiltak* – etter at vedkommende har sluttet
- *Dårlig sikkerhetskultur* – manglende etterlevelse, ledelsen følger ikke opp
- *Manglende funksjonsbasert risikovurdering av personer* – ikke utført stillingsspesifikk vurdering
- *Dårlig bakgrunnssjekk* – ikke gjort godt nok
- *Svak kommunikasjon mellom enheter* – utveksling av informasjon risikoer
- *Mangelfull bevisstgjøring om personellsikring hos øverste ledelse* – manglende fokus og forståelse medfører mangelfulle ressurser

Håndtering av innsiderisiko krever at man først og fremst har det generelle ved et styringssystem for sikring på plass. I tillegg må de spesifikke tiltak relevante for innsideproblematikken implementeres – tiltak som er spesielt rettet mot arbeidsforholdet (ref. kapittel 4.2.4). Dette gjelder både *før* arbeidsforholdet iverksettes (rekrutteringsfasen eller kontraktsinngåelse), *under* selve arbeidsforholdet, og i den perioden arbeidsforholdet *avsluttes* – som illustrert i figuren under.



Figur 5-1: Håndtering av innsiderisiko – et generelt styringssystem for sikring må være på plass, supplert med spesifikke tiltak knyttet til arbeidsforholdet

De etterfølgende delkapitlene er derfor delt inn i de naturlige fasene:

Kapittel 5.2: Styringssystem for sikring

Kapittel 5.3: Tiltak i rekrutteringsfasen – Utlysning og ansettelse

Kapittel 5.4: Tiltak under arbeidsforholdet

Kapittel 5.5: Tiltak for å håndtere en oppstått situasjon

Kapittel 5.6: Avslutning av arbeidsforholdet

Kapittel 5.7: Implementering

Merk at rekkefølgen på tiltakene innenfor hver av de definerte fasene i de etterfølgende del kapitlene (kapitlene 5.3 til 5.6) er ikke et forsøk på å rangere tiltakene i henhold til effektivitet eller viktighet. Rekkefølgen forsøker heller å reflektere tid og temaer som logisk hører sammen. Selvsagt vil flere av tiltakene kunne gjøres i parallell innenfor hver fase.

I løpet av workshopen og dybdeintervjuene ble det nevnt enkelte eksempler fra reelle hendelser. Noen av disse eksemplene er anonymisert og gjengitt i små faktabokser, merket «Case».

5.2 Styringssystem for sikring

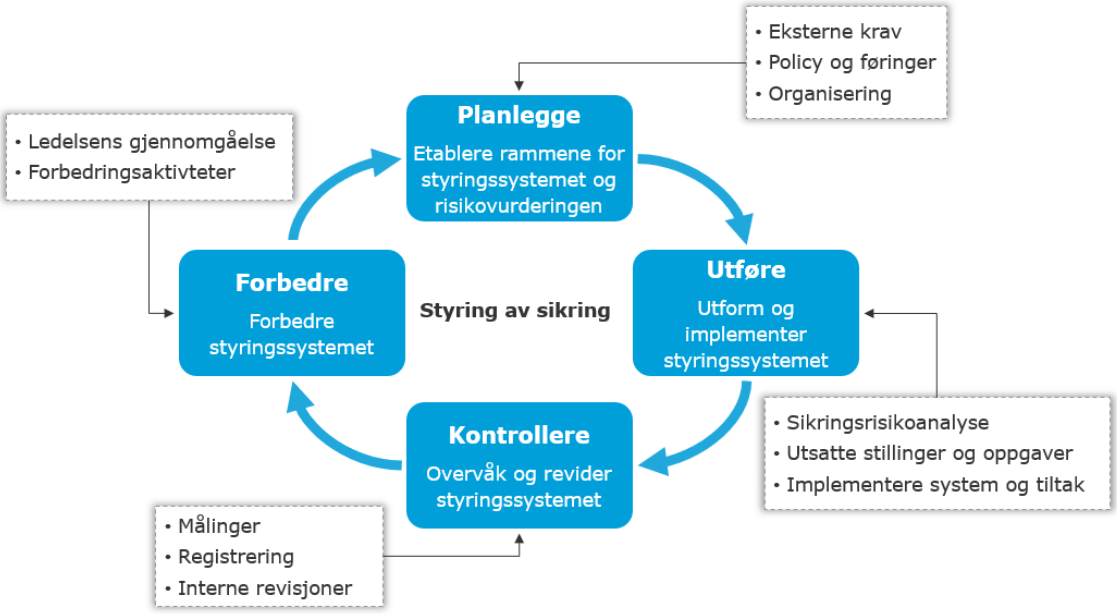
Utformingen av styringssystemet for sikring avhenger av de verdier som skal beskyttes og bør, som for all annen risikostyring, tilpasses den enkelte virksomhet.

I standarden ISO 31000:2018 beskrives visse prinsipper som bør legges til grunn for å sikre et godt og levende styringssystem. Videre omtaler ISO 9001:2015 visse punkter knyttet til lederskap. Punktene nedenfor sammenfatter de viktigste fra disse to standardene, og kan ansees som *suksessfaktorer* – forhold som er viktige for å sikre et godt og levende styringssystem.

- Forankring hos og forpliktelse fra ledelsen – promotere sikring og gå foran som et godt eksempel

- Tilstrekkelige ressurser må være tilgjengelig – både mht. riktig kompetanse, antall personer, teknologiske hjelpemidler og systemer, så vel som finansielt grunnlag
- Integrert – Styringssystemet for sikring bør være en integrert del av virksomhetens styringssystem
- Inkluderende – Det bør være en hensiktsmessig deltakelse av interessenter (dvs. arbeidstakere, og enheter på tvers i virksomheten), som gjør det mulig å ta hensyn til deres kunnskap, synspunkter, oppfatning og forståelse.
- Menneskelige og kulturelle faktorer – menneskelig adferd, forståelse og kultur påvirker i vesentlig grad alle aspekter ved risikostyring, bl.a. viktig å sikre forståelse og bevisstgjøring.
- Klare kjøreregler etablert, kommunisert og forstått.
- Kontinuerlig forbedring – gjennom å lære av andre og av egen erfaring, krever evne til å omsette dette i kontinuerlig forbedring

Figuren nedenfor illustrer de viktigste generelle elementene som bør være på plass i styringssystemet for sikring.



Figur 5-2: De viktigste elementene som må være på plass i et styringssystem for sikring

***Planlegge* – Etablere rammene for styringssystemet og risikovurderingen:** Først og fremst må arbeidet med sikring må være forankret hos ledelsen, og ledelsen må gå foran og kommunisere viktigheten av god sikring utover i organisasjonen. Man må kjenne til hvilke eksterne krav som gjelder for virksomheten – som lovkrav (lov og forskriftskrav er omtalt i Appendix E) og eventuelle krav fra kunder og mellom partnere. Virksomheten må etablere overordnet(e) policy(er) og andre føringer.

I sammenheng med innsiderisiko bør det utarbeides policy for bl.a. informasjonssikring og -håndtering, og etikk (knyttet til problematikk rundt bedrageri/underslag). Roller og ansvar knyttet til sikring må klart defineres og formidles. Utfordringen kan ligge i at innsiderisiko og håndtering av denne vil berøre forskjellige organisatoriske enheter – som f.eks. sikringsenheten, HR, juridisk, IT, facility management og kommunikasjon.

***Utføre* – Utform og implementer styringssystemet:** Virksomheten må kjenne til tilstanden knyttet til sikring slik den er i dag, og til sårbarhetene i virksomheten. Sikringsrisikoanalysen som gjennomføres må også dekke innsideproblematikken. Man må ha kjennskap til virksomhetens verdier, og hvilke funksjoner eller arbeidsoppgaver som vil kunne komme i kontakt med sensitiv informasjon eller kritiske systemer eller områder. Informasjonen fra denne sikringsrisikovurderingen er viktig input til den stillingsspesifikke risikovurderingen omtalt under tiltak 1. NSM har utgitt en håndbok i gjennomføring av sikringsrisikovurdering (ref. /16/).

Basert på disse vurderingene må det etableres tilstrekkelige tiltak i en fornuftig kombinasjon av teknologiske tiltak, organisatoriske tiltak og tiltak som går på den menneskelige faktor. Krav som innføres må tydelig kommuniseres og være forstått.

Det må settes klare, fornuftige og hensiktsmessige kjøreregler som alle ansatte kjenner til og forstår, og organisasjonen må sikre at de ansatte er bevisste og vet hvilke farer som lurer. Videre må det etableres en kultur som sikrer at de ansatte etterlever de regler som er satt og sier ifra dersom man observer forhold som kan være mistenkelige.

Gode ledere – som er med på å skape et godt arbeidsmiljø, god trivsel og fornøyde medarbeidere på arbeidsplassen er blant de aller viktigste tiltak for å forebygge at en person utvikler seg til å bli en innsidetrussel.

Erfaringsmessig er ofte implementeringen av et styringssystem, og å holde dette levende og vedlike, en krevende oppgave. Implementering er ytterligere omtalt i kapittel 5.7.

Spesifikke tiltak for å håndtere innsidetrusselen er omtalt i kapitlene 5.3 til 5.6.

***Kontrollere* – Overvåk og revider styringssystemet:** Ingen prosedyrer, regler og andre interne krav fungerer om ikke disse blir etterlevd. I tillegg til de spesifikke overvåkingssystemene (logg) omtalt i kapittel 5.4, bør virksomheten har gode målesystemer – gjennom registreringer, logger, rapportering av hendelser, interne revisjon o.l. er med å følge med på hva som skjer i virksomheten. I denne sammenhengen er årsaksforståelse og implementeringen av fungerende korrigerende tiltak helt essensielt.

***Forbedre* styringssystemet**: Basert på resultatene fra «Kontrollere» aktivitetene nevnt ovenfor, bør ledelsen regelmessig gjøre en vurdering av hvordan styringssystemet og arbeidet er i forhold til planen og ønsket nivå. I alle standarder (kvalitetsstandarden ISO 9001, og til svarende) er «Ledelsens gjennomgåelse» en viktig forutsetning for å sikre kontinuerlig forbedring – der man avklarer hva man bør endre og hva som kan forbedres i kommende periode.

5.3 Tiltak i rekrutteringsfasen – Utlysning og ansettelse

Dette kapittelet beskriver tiltak som skal redusere sannsynligheten for at virksomheten ansetter eller engasjerer personer som enten utgjør en potensiell trussel allerede før ansettelse eller engasjement (infiltratør), eller en som ansees å ha potensiale til å kunne utvikle seg til å bli en innsider på et senere tidspunkt – rekruttert eller selvmotivert innsider. Se kapittel 4.2.2 for nærmere karakteristika på en innsider.

Som angitt over, er rekkefølgen på etterfølgende tiltakene i rekrutteringsfasen ikke i henhold til en rangering mht. på effektivitet/viktighet, men mht. gjennomføring i tid (f.o.m. utlysning til ansettelse).

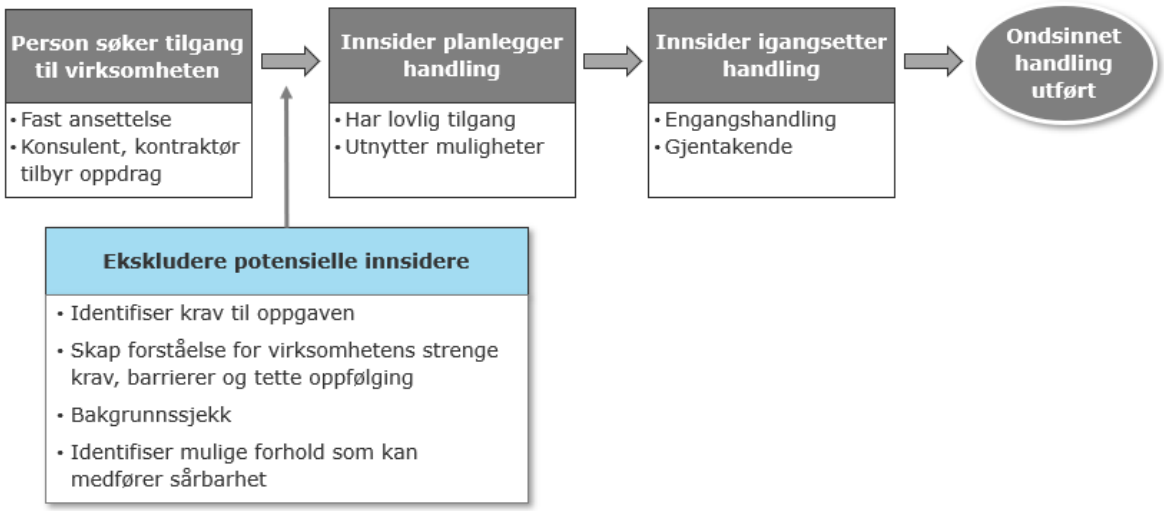
5.3.1 Tiltak oppsummert

Først og fremst må selve stillingen, eller arbeidsoppgavene, vurderes – vil vedkommende som skal utføre arbeidsoppgavene få tilgang til sensitiv informasjon, til kritiske systemer eller områder, og bør det derfor settes spesielle krav til vedkommende. Det bør i så fall signaliseres i utlysningen at det stilles krav og at det vil bli utført en grundig bakgrunnssjekk. Utfordringen med bakgrunnssjekk er imidlertid at det kan være meget vanskelig å avdekke hvorvidt en person enten har uærlige hensikter, eller har svakheter som kan utnyttes senere av en tredjepart. For en infiltratør som arbeider for en fremmed stat vil sannsynligvis alt være lagt godt til rette og forberedt, og en bakgrunnssjekk vil vanskelig kunne avdekke noe mistenkelig. Videre setter lovverket visse begrensninger mht. hva man kan spørre om vedrørende alkoholbruk, pengebruk, seksuell legning, osv.

Den viktigste effekten av dette settet med tiltak er at personen på vei inn i virksomheten får forståelse av at sikring tas på alvor og at dette vil kunne virke avskrekkende for enkelte personer som har uærlige hensikter.

Rekrutteringsfasen kan igjen deles i to:

- *Utlysning* – man gjør vurderinger av stillingen, dens innhold og profil, og hvilke krav som skal stilles til søkerne, og man ennå ikke har bestemt hvem som skal tilbys ansettelse eller kontrakt
- *Ansettelse* – man har bestemt hvem som skal tilbys ansettelse, og frem til vedkommende starter sin første dag på jobb



Figur 5-3: Kategorier av tiltak for å forhindre uønsket ansettelse eller engasjement

5.3.2 Spesifikke tiltak

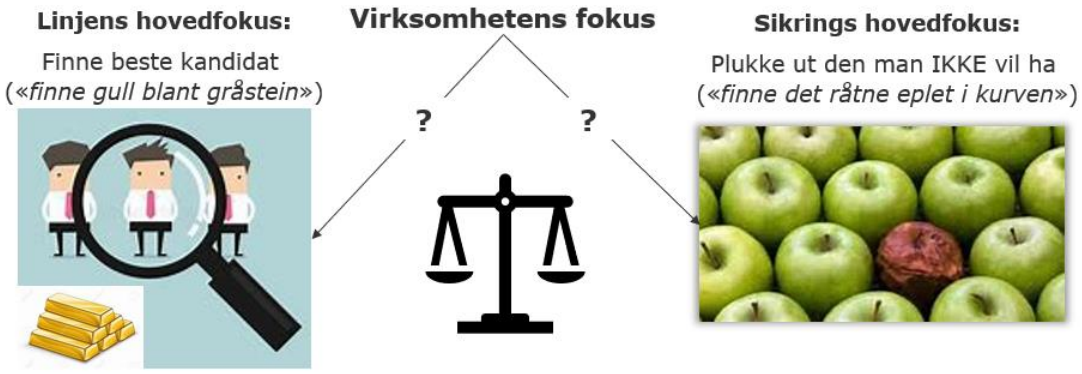
Dette delkapittelet sammenfatter anbefalte tiltak i rekrutteringsfasen.

Tiltak 1: Gjennomfør en stillingsspesifikk risikovurdering

I forkant av arbeidet med å lyse ut en stilling eller innhente et tilbud fra en kontraktør, bør det gjennomføres en vurdering av den aktuelle stillingen eller arbeidsoppgaven. Vurderingen bør adressere hvilken type informasjon, kritiske systemer eller områder/soner som vedkommende skal få tilgang til. Dette bør danne grunnlaget for hvilke krav man bør sette til vedkommende i form av en eventuell bakgrunnssjekk, hvordan eventuelle slike krav og informasjon om bakgrunnssjekk skal fremkomme i den aktuelle utlysningen (se også neste tiltak, tiltak 2), oppfølgingen mens vedkommende er i stillingen eller utfører oppgavene (se tiltakene i neste fase «5.4 – Tiltak under arbeidsforholdet»).

Denne vurderingen bør gjennomføres som et ledd i arbeidet med å lage stillings- eller funksjons-beskrivelse. Denne prosessen bør gjennomføres som et samarbeid mellom HR, sikringsenheten, juridisk og den aktuelle fagenheten der vedkommende skal arbeide.

I studien til Crowd Research Partners (ref. /72/) var mangel på samarbeid mellom de forskjellige avdelingene den tredje største hindringen for å få til bedre håndtering av innsiderisiko, se Appendix F.



Figur 5-4: Å finne den rette kandidat er en balanse mellom «å finne gull blant gråstein» og «unngå det råtne eplet i kurven»

Tiltak 2: Tydeliggjør i utlysningsteksten at bakgrunnssjekk vil bli gjort

La det fremkomme i stillingsannonsen at det vil bli gjennomført en bakgrunnssjekk av vedkommende som blir innstilt, dersom det er aktuelt.

Hensikten med en slik forhåndsvarsling er å formidle at virksomheten er opptatt av å sikre seg mot å engasjere personer med uærlige hensikter eller som ikke egner seg i stillingen. Videre vil en slik annonsering kunne ha en viss avskrekkende effekt overfor enkelte personer med uærlige hensikter eller en fortid som ikke er forenelig med den aktuelle arbeidsoppgaven, slik at disse muligens avstår fra å søke.

Personer som infiltreres på vegne av en fremmed stat vil neppe skremmes av et slikt varsel da slike forsøk gjerne er nøye planlagt og forberedt. Derimot, personer som selv har jukset med, eller pyntet på, sin CV i den hensikt å skaffe seg en bedre jobb – som de kanskje ikke er kvalifisert for – vil kunne forventes å bli påvirket av et slikt forhåndsvarsel.

Tiltak 3: Søk i åpne kilder på nettet

Som en første screening på kandidater som har søkt på den aktuelle stillingen bør det søkes på vedkommende i åpne kilder på nettet, som f.eks. Facebook, Twitter og Instagram. Hensikten er å skaffe seg et første overordnet inntrykk av vedkommende og se om det er forhold som klart antyder at vedkommende ikke er aktuell for stillingen. Eventuelle interessante observasjoner fra disse søkene kan så forfølges videre gjennom intervjuene og/eller den etterfølgende bakgrunnssjekken. Det er imidlertid viktig å være klar over hvilke begrensninger som ligger lovverket mht. hva en virksomhet har lov til å innhente (se også Appendix E, Lovmessige og andre krav).

En person som bevisst søker seg inn i en virksomhet og som har uærlige hensikter (f.eks. en infiltratør) vil sannsynligvis være bevisst på hva vedkommende legger ut på sosiale medier. Derimot, en person som tydelig synliggjør interesser/levesett/aktiviteter på sosiale media som kan utnyttes av en tredjepart (eks. festing og rusbruk, dyre innkjøps- eller forbruksvaner, svak for det motsatte eller samme kjønn osv.), kan potensielt utgjøre en sårbarhet på et senere tidspunkt (som en rekruttert innsider).

Tiltak 4: Gjennomfør bakgrunnssjekk

Avhengig av konklusjonen på den innledende stillingsspesifikke risikovurderingen, bør det gjennomføres en bakgrunnssjekk før ansettelse. Hensikten med bakgrunnssjekken er å bekrefte eller avkrefte den informasjonen søkeren selv oppgir, samt å avdekke om det er forhold ved vedkommende som gjør at personen kan utgjøre en sikringsrisiko.

I tillegg til at bakgrunnssjekken skal gi virksomheten muligheten til å forsikre seg om at opplysningene som søkeren gir er korrekte, så vil bakgrunnssjekken kunne virke forebyggende. Gjennomført på en god måte kan den redusere sannsynligheten for å ansette personer som har sårbarheter, og som vil kunne utgjøre en trussel møt selskapet.

Hvorvidt virksomheten velger å utføre bakgrunnssjekken selv eller engasjere et eksternt profesjonelt byrå er avhengig av kompetanse og tilgjengelighet av egne ressurser.

NSRs Kriminalitets- og sikkerhetsundersøkelsen i Norge (KRISINO) for 2017 (ref. /28/) adresserer bl.a. spørsmål knyttet til ansettelsesprosessen og gjennomføring av visse sjekker. Generelt synes offentlig sektor å være flinkere til å gjennomføre slike sjekker enn private virksomheter. Studien viser f.eks. at referansesjekk gjennomføres i 95 % av tilfelle for offentlig sektor, mot bare 76 % i privat sektor. Tilsvarende, ekthetssjekk av vitnemål ble gjennomført for 55 % i offentlig sektor og bare 25 % i privat sektor. For sjekk av jobbsøker på internett var tallene hhv. 72 % (offentlig) og 53 % (privat).

Videre er det en kjent problemstilling at det jukses med CV-er i forbindelse med jobbsøknader. I en artikkel fra 2013 på nettstedet til NSR (ref. /29/) omtales at 1 av 5 jukser med CV-en. Der henvises også til en undersøkelse fra 2012 gjort av et konsulentselskap (Semac) at det var kritikkverdige forhold hos hele 40 % av 1120 kontrollerte jobbsøkere. Et annet selskap (Meditor Search) utfører også bakgrunnssjekk av jobbsøkere på vegne av kunder, og de opplyser at de finner feil i én av fire CV-er, og dette tallet har holdt seg stabilt over flere år.

Jobbsøkere som jukser seg inn ved forfalskning av CV har ikke nødvendigvis kriminelle hensikter – status, karrieremuligheter og høyere lønn kan være nok til at noen ønsker å benytte juks som virkemiddel for å nå sine mål. Man må likevel kunne anta at en person som har til hensikt å infiltrere et selskap på vegne av en større organisasjon eller fremmed stat, har et tilstrekkelig ressurssterkt apparat i ryggen som vil kunne etablere en historikk og CV som gjør det vanskelig å oppdage at dette ikke er ekte.

Ved hjelp av nettstedet *Vitnemålsportalen* (www.vitnemalsportalen.no/) kan en person selv hente ut egne resultater fra høyere utdanning (gjelder kun utdanning i Norge) og dele disse med potensielle arbeidsgivere. Tjenesten er utviklet på oppdrag fra Kunnskapsdepartementet og er gratis å benytte. Det er ikke mulig å hente ut denne informasjonen på vegne av andre, men i en søknadsprosess kan virksomheten vurdere å be søker om å få en utskrift fra Vitnemålsportalen. Dette vil da kunne bekrefte at vedkommende har tatt den utdanningen som vedkommende har oppgitt i sin søknad, dog begrenset til utdanning tatt i Norge.

Spesielt for innleie av personer: Hvis en person har to arbeidsgivere på samme sted skal man bestemme hvilken av disse som er hovedarbeidsgiver. En konsulent ansatt i og utleid fra et utleieselskap, skal oppdragsgiver sørge for arbeidsvilkår på lik linje som for egne ansatte. Overfor selskaper som leier ut personer kan oppdragsgiver og utleieselskapet avtale at det skal gjøres en bakgrunnssjekk av den innleide personen. Oppdragsgiver kan ikke selv gjøre dette, men er avhengig av at utleieselskapet (som vedkommende er ansatt i) utfører bakgrunnssjekken. Imidlertid kan det oppdragsgivende selskap ta inn ekskluderingsbestemmelser i kontrakten. I så tilfelle, skulle utleieselskapet ikke utføre bakgrunnssjekken som avtalt, kan oppdragsgiver ta den innleide personer av oppgaven vedkommende er satt til.

Tiltak 5: Utfør ID-sjekk ved intervju og ved ansettelsesstart

Bruk av falske identiteter ansees generelt sett å kunne være et problem også i Norge. Det anbefales derfor at man ber kandidatene om å ta med seg id-bevis (primært pass) til intervjuet og til første arbeidsdag, slik at man kan sjekke og sikre seg at kandidaten er den vedkommende utgir seg for, og at den som starter arbeidet er den samme som var på intervjuet.

NSRs Kriminalitets- og sikkerhetsundersøkelsen i Norge (KRISINO) for 2017 (ref. /28/) adresserer bl.a. spørsmål knyttet til ansettelsesprosessen og gjennomføring av identitetssjekk. Offentlig sektor synes å være flinkere til å gjennomføre slike sjekker – totalt 56 % av de offentlige virksomhetene gjennomført identitetssjekk, mens bare 38 % av de private oppga at de gjorde det.

I tilfelle av utenlandske statsborgere kan man benytte åpne referansedatabaser på nettet der man kan finne informasjon om hvordan pass, førerkort etc. i de forskjellige landene ser ut. Én av disse er PRADO (EUs Public Register of Authentical travel and identify Documents Online, https://www.consilium.europa.eu/prado).

5.4 Tiltak under arbeidsforholdet

Dette kapittelet adresserer tiltak gjeldende for hele arbeidsforholdet – for både ansettelse av fast eller midlertidig arbeidskraft, og for innleie av konsulenter og andre engasjementer av kontraktører, f.eks. til vedlikehold og rengjøring. Når vedkommende er i organisasjonen, kan det være at personen enten allerede er en innsider (infiltratør), eller utvikler seg til å bli en innsider (f.eks. presset, kjøpt, utvikler selvmotivasjon).

Tiltakene i dette delkapittelet er gruppert etter de tre kategoriene menneskelige, organisatoriske og teknologiske sikringstiltak, og innenfor hver gruppe, etter temaer som logisk hører sammen.

5.4.1 Tiltak oppsummert

Tiltak omfatter forebyggende elementer som skal forsøke å unngå at en arbeidstaker i det hele tatt tenker på eller blir fristet til å utføre en uønsket handling, eller initierer handlingen. Videre, dersom handlingen likevel utføres må det være tiltak på plass som sikrer at dette oppdages så tidlig som mulig, og at man gjøre det vanskeligst mulig, eller umulig, for innsideren å gjennomføre den uønskede handlingen.

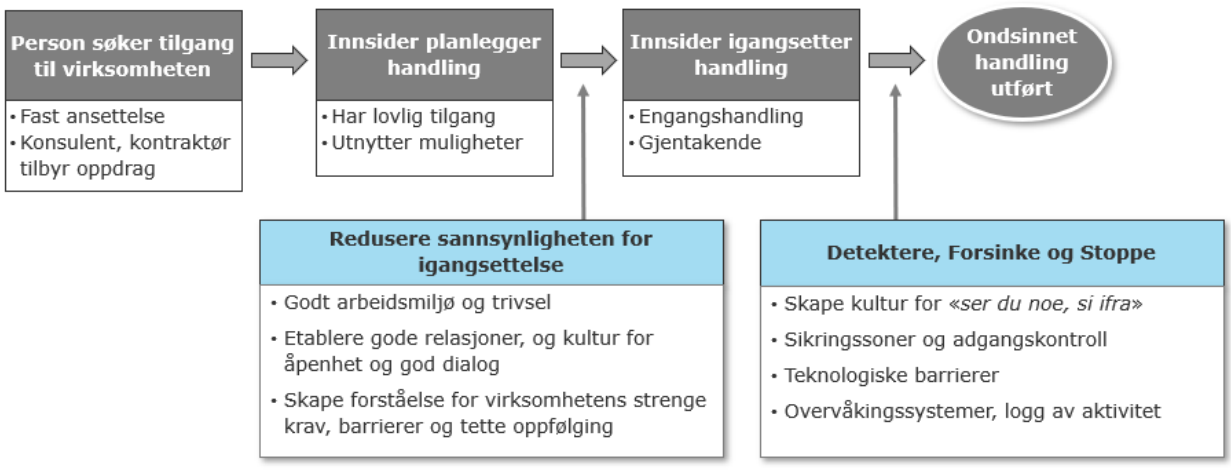
Å skape et godt arbeidsmiljø, god trivsel og fornøyde medarbeidere på arbeidsplassen er et av de aller viktigste tiltakene for å forebygge at en person utvikler seg til å bli en innsidetrussel. En fornøyd arbeidstaker, som opplever gjensidig tillitt i sitt arbeidsforhold, vil i mindre grad være utsatt for å bli fristet til å gjøre noe ulovlig som kan skade virksomheten. Og, dersom en situasjon skulle oppstå, f.eks. der arbeidstaker er blitt forsøkt vervet eller lurt opp i en vanskelig situasjon, er det viktig å ha etablert en kultur for åpenpenhet og god dialog mellom kollegaer, og mellom ansatt og linjeleder.

Videre er det viktig at øvrige ansatte blir bevisst på innsidetrusselen – bevisste på at de kanskje omgås informasjon som noen kunne ha interesse av å få tak i, hva de skal gjøre for å beskytte denne informasjonen, og at det skapes en kultur for å si ifra dersom man observerer noe mistenkelig eller fatter mistanke, som for eksempel en adferdsendring hos en kollega. Det må også være kultur for at dersom en ansatt skulle bli utsatt for press eller trusler fra en tredjepart, så er det naturlig og ikke skremmende å ta dette opp med egen leder eller gjennom en etablert varslerkanal. Godt arbeidsmiljø, trivsel, åpen og god kommunikasjon er i stor grad et lederansvar.

Uansett er det viktig at virksomheten har definert hvilke områder som ansees som kritiske og at det er gode teknologiske barrierer som både hindrer uautorisert adgang/tilgang og som overvåker og detekterer dersom mistenkelig adferd/aktivitet observeres.

Videre bør alle arbeidstakere få et inntrykk av at i denne virksomheten er det vanskelig å komme til de verdiene man ønsker å få tilgang til for å tilegne seg eller skade, og hvis man likevel skulle prøve, er sannsynligheten for å bli oppdaget stor.

Det er nødvendig at virksomheten er kjent med hvilke lovkrav som gjelder slik at det ikke iverksettes kontrolltiltak som bryter med lovverket. I flere tilfeller er det også både nødvendig, og lurt, å involvere ansatterepresentanter før spesielle kontrolltiltak innføres.



Figur 5-5: Kategorier av tiltak for å forhindre igangsettelse av handling, og for å detekter og forsinke et mulig angrep, og hindre adkomst til kritiske verdier

5.4.2 Spesifikke tiltak

Dette delkapittelet omfatter anbefalte tiltak som gjelder i den perioden vedkommende er ansatt, eller kontraktøren utfører sitt oppdrag. Arbeidstaker benyttes som fellesbetegnelse på både fast og midlertidig ansatte, og på innleide kontraktører. Kapittelet er inndelt i hhv. Menneskelige sikringstiltak, organisatoriske sikringstiltak og teknologiske sikringstiltak.

A: MENNESKELIGE SIKRINGSTILAK

Tiltak 6: Obligatorisk introduksjonskurs fokuserer på sikring

De aller fleste virksomheter har en eller annen form for introduksjonspakke for nyansatte. Denne bør også ha et element som adresserer innsiderisiko og sikring. Temaene som tas opp bør dekke blant annet beskrivelse av hvilken type verdier som er i virksomheten (sensitiv informasjon, kritiske systemer og områder, osv.), eksterne og interne trusler, eksempler på sårbarheter (ref. rekrutterte innsidere), relevante krav og tiltak i virksomheten, som f.eks. policyer (f.eks. om informasjonshåndtering, etikk, korrupsjon), prosedyrer, regler, rapporterings-/meldingssystemer o.l. Kurset bør dekke både etikk, korrupsjon, sensitiv informasjon, dilemmaer o.l.

Introduksjonskurset bør gis så tidlig som mulig etter ansettelse, og senest i løpet av de 3 første månedene. Det bør også være et system som sikrer at kurset blir gjennomført, med påminnelse til vedkommendes linjeleder dersom kurset ikke er tatt innen fristen. Et slikt kurs er med på å heve bevisstgjøringen rundt sikring og vise at virksomheten tar temaet sikring på alvor. I tillegg til alle nyansatte, bør introduksjonskurset – i hvert fall den delen som omhandler sikring – også gis til innleide konsulenter som skal være i virksomheten over lengre tid. For korttidsengasjementer kan det eventuelt utarbeides et kurs av kortere varighet, f.eks. som et e-læringskurs.

Tiltak 7: Etabler et opplæringsprogram for ledere

Uten nødvendig forståelse hos, og støtte fra, ledelsen vil mye av sikringsarbeidet i resten av organisasjonen være vanskelig å få til. Det bør etableres et program for å styrke forståelsen og kompetansen hos ledere om temaet innsiderisiko, hvordan dette håndteres i egen virksomhet og hvilken rolle lederne har i dette arbeidet med bl.a. å gå foran som et godt eksempel og promotere sikringsarbeidet. Opplæringen kan gjennomføres f.eks. som e-læring eller at en med tilstrekkelig tyngde, kompetanse og kommunikasjonsevne holder en kort presentasjon for den øverste ledergruppen, typisk varighet ca. 30 minutter. Tilsvarende bør det etableres opplæringsprogram for ledere på alle nivåer i organisasjonen.

Hensikten er å styrke forståelsen og kompetansen hos alle ledere mht. innsiderisiko og trekke frem hvilken rolle ledere har innenfor dette området. Det bør legges vekt på viktigheten av å følge opp egne arbeidstakere og sikre en god dialog slik at om en arbeidstaker observerer mistenkelige forhold, eller skulle bli utsatt for press eller annen form for vervingsforsøk, så skal det være naturlig å ta dette opp med egen leder. Det må være en klar policy i virksomheten som er til hjelp for ledere i hvordan de skal håndtere gitte situasjoner, f.eks. en ansatt forteller at vedkommende har vært utsatt for press eller en vanskelig situasjon, en bekymringsmelding om en ansatt osv.

Tiltak 8: Etabler et bevisstgjøringsprogram

Bevisstgjøring av innsiderrisiko ansees som en av de viktigste barrierene for å avdekke innsideren og forhindre en uønsket handling – være seg en bevisst og ondsinnet handling eller en ubevisst og utilsiktet handling. Virksomheten bør etablere et bevisstgjøringsprogram som adresserer innsidetrusselen. Programmet bør inneholde forskjellige temaer og kan kjøres gjennom forskjellige kommunikasjonskanaler og fora. Programmet skal øke den generelle forståelsen om innsidetrusselen hos ansatte generelt. Gjennom programmet bør de ansatte få forståelse for temaer som f.eks.:

- Hva en innsider er og hvordan innsideren opererer
- Hvilken type verdier (informasjon, systemer osv.) finnes i egen organisasjon, og som en innsider kan ha interesse av
- Hvilke systemer og regler/krav finnes i egen organisasjon som har til hensikt å beskytte mot en innsider
- Hva kan en ansatt selv bli utsatt for – forsøk på verving gjennom trusler, bestikkelser eller lurt – både på jobben, på reiser, ved på deltakelse på konferanser osv.
- Hvordan bør man forholde seg og melde fra om, dersom man observerer mistenkelig adferd hos kollegaer eller selv blir forsøkt vervet.

Et slikt program vil berøre forskjellige fagdisipliner som f.eks. fysisk sikring, organisatoriske forhold, mellommenneskelige forhold og IT-systemer. I utarbeidelse av bevisstgjøringsprogrammet bør man derfor involvere de fagdisipliner som har ansvaret for de forskjellige fagdisipliner, f.eks. HR, facility management, sikring, IT, kommunikasjonsavdelingen osv.

I følge NSMs rapport *Risiko 2018* (ref. /25/) viser internasjonale studier at innsidesaker ofte oppstår tre til fem år inn i et arbeidsforhold. NSM har imidlertid observert at i mange virksomheter avtar sikkerhetsbevisstheten og sikkerhetsoppfølgingen av den ansatte samtidig med at ansettelsesforholdet modnes. Det bør derfor legges opp til at bevisstgjøringsprogrammet også omfatter en oppfølging eller repetisjon som gjentas med jevne mellomrom.

Hensikten er å øke den generelle forståelsen rundt innsiderisikoen i virksomheten, og hvordan man håndterer den. Slike programmer eller kampanjer kan være generelle og rettet mot alle i virksomheten, eller spesialtilpasset og rettet mot enkeltpersoner eller grupper, avhengig av funksjon og tilgang på f.eks. sensitiv informasjon. Gjennomføringen kan være som e-læringsprogrammer, klasseromsundervisning, nanolearning[4], allmøter, avdelingsmøter, medarbeidersamtaler osv.

Effekten av tiltaket ansees å være meget god. Fysiske sikringstiltak, prosedyrer og regler har en viss effekt for å hindre en innsider i å utføre en uønsket handling. Men til syvende og sist er den menneskelige faktor som vår forståelse, vår observasjonsevne og vår adferd som muligens er de viktigste type tiltak for å avdekke en innsider og derigjennom forhindre en uønsket handling.

Tiltak 9: Skap en kultur «*Det er lov å bry seg*»

For de fleste vil det oppleves vanskelig å ta opp med sin leder eller kollega direkte dersom man observerer adferd kan oppfattes som unormal eller mistenkelig. Det kan være at kollegaen har begynt å være på jobb til uvanlige tider (f.eks. kommer spesielt tidlig, jobber sent om kveldene eller i helgene), at vedkommende endrer adferd (f.eks. holder seg mer for seg selv, ikke lenger så sosial som

[4] Nanolearning er små korte læringsmoduler (2-5 minutter) som sendes til alle eller noen utvalgte i virksomheten via e-post, sendt med jevne mellomrom, f.eks. månedlig gjennom hele året.

vedkommende var, omgås andre mennesker), eller har fått et større personlig pengeforbruk (f.eks. kjøpt ny bil, reiser mer enn vanlig) – for å nevne noen eksempler.

Slike forhold kan ha sin naturlige forklaring, som øket arbeidsmengde, utfordrende situasjoner i familielivet med mer. Men, de kan også være en indikasjon på at vedkommende har kommet i en situasjon der han/hun har blitt vervet, eller forsøkt vervet, gjennom å bli truet, bestukket eller lurt til å utføre ulovlige handlinger. I slike situasjoner er det viktig at det allerede er etablert en kultur der det er akseptert å stille spørsmål og ta opp ting med vedkommende – for å hjelpe vedkommende (om vedkommende har et problem), eller å avdekke eller forhindre en videre ulovlig aktivitet, dersom dette er den bakenforliggende årsaken.

En slik kultur tar tid å bygge opp, og linjeledelsen har en vesentlig rolle i dette. Viktige elementer i å bygge en slik kultur er bl.a. ledelsens engasjement, medarbeidersamtalene, sikring på møter og bevisstgjøringsprogrammet (se tiltakene 7, 8, 13 og 15).

Hensikten er at det skapes en generell aksept i virksomheten for å ta opp forhold man stusser over, der det er en generell forståelse for at «*Det handler ikke om å sladre, men om å bry seg….*». Effekten av tiltaket ansees å være meget god. Den menneskelig faktor, gjennom vår observasjonsevne og dertil hørende evne til å kunne si ifra dersom vi observerer mistenkelige forhold, er en meget viktig barriere.

Tiltak 10: Etabler en varslingskanal

Det bør etableres en varslingskanal («Whistleblower»-kanal) som er gjort godt kjent blant alle arbeidstakere. I arbeidsmiljølovens kapittel 2A settes det krav om varsling knyttet til arbeidsforhold. På lik linje anbefales det å sette opp en varslingskanal knyttet til sikring. Det må være en klar policy i virksomheten som er til hjelp for de som skal håndtere et varsel, se også Tiltak 7: Etabler et opplæringsprogram for ledere.

Tiltaket over, om å skape en kultur «*Det er lov å bry seg*» (Tiltak 9), er tenkt at man tar opp saken direkte med den det gjelder, mens dette tiltaket (varslingskanal) er knyttet til å varsle om en annen person, eller situasjon, til en tredjepart. Gjennom denne kanalen skal alle kunne melde ifra dersom man observerer eller har mistanke om noe som er knyttet til innsiderisiko – å formidle en «bekymringsmelding». Rutinen for varsling (til hvem, hvordan, hva og når) må gjøres kjent i hele organisasjonen. Mottaker av varselet kan være enten en angitt person/funksjon internt i virksomheten, eller den kan være til en uavhengig tredjepart – utenfor virksomheten.

Tiltak 11: Etabler god dialog internt mellom HR og sikringsenheten

Det bør etterstrebes en god dialog mellom relevante enheter i selskapet, spesielt mellom HR-funksjonen og sikringsenheten. Dialogen behøver ikke nødvendigvis være formalisert. Uformelle kanaler synes også å virke dersom man har en omforent forståelse for hverandres problemstillinger og gjensidig tillit. Med en god relasjon er det lettere å snakke åpent og ta tak i vanskelige situasjoner, og at man da evner å se sakene fra flere sider. Dette gjelder gjennom hele arbeidsforholdet – både i rekrutteringsfasen, under arbeidsforholdet, i avslutningsfasen og ikke minst dersom det skulle inntreffe en sikringshendelse der en ansatt eller innleid er involvert.

Det er viktig at HR-funksjonen har forståelse for sikringsfunksjonens prioriteringer ut fra et sikringsbehov, og vice versa. Slike prioriteringer bør være basert på resultater fra sikringsrisikoanalysen.

Videre er en god kommunikasjon nødvendig dersom en sikringshendelse som involverer en ansatt skulle inntreffe, og det er nødvendig at man raskt avklarer hvordan saken skal håndteres videre. Dette gjelder

både for å ivareta det rent sikringsmessige, den ansattes rettigheter og at man sikrer for at virksomheten ikke bryter lovkrav, f.eks. krav i personopplysningsloven.

Tiltak 12: Gjennomfør sikringssamtale regelmessig

Når en nyansatt, eller innleid konsulent, tiltrer bør det så tidlig som mulig gjennomføres en samtale om temaet sikring med vedkommende. En slik samtale bør gjentas med jevne mellomrom, f.eks. årlig. Virksomheten bør ha satt en standard for samtalen – hvem som utfører den og hvor ofte, det bør være en opplæring av vedkommende som skal utføre den og det bør finnes en veiledning eller sjekkliste over temaer som samtalen bør adressere.

I utgangspunktet bør en slik samtale gjennomføres med alle, men samtalens dybde og omfang bør tilpasses den ansattes tilgang til og omgang med sensitiv informasjon og kritiske systemer. Samtalen bør i utgangspunktet gjennomføres med en representant fra sikringsenheten i virksomheten. For personer som har tilgang til spesiell sensitiv informasjon eller kritiske systemer eller områder, bør samtalen kjøres av en representant fra sikringsenheten for å gi samtalen mer tyngde.

Gjennom samtalen skal det fremheves verdier i virksomheten og potensielle trusler som er relevante i forhold til vedkommendes funksjon og plass i virksomheten, og hvilke regler og forventinger som gjelder for arbeidstaker. Vedkommende bør oppfordres til å snakke åpent om forhold som kan påvirke sårbarheter, for eksempel om vedkommende har opplevd at noen har prøvd å presse, bestikke eller på annen måte etterspørre informasjon. Det bør utarbeides en sjekkliste eller mal for hvilke temaer samtalen skal adressere.

Virksomheten, og den som gjennomfører samtalen, må være kjent med lovverket slik at man ikke etterspør informasjon ut over det lovlige, se også Appendix E om krav i lovverket.

Hensikten med samtalen om sikring er å bidra til å styrke sikringskulturen gjennom å øke den generelle bevisstgjøringen, å vise at selskapet tar sikring på alvor, samt skape en arena for en god dialog slik at dersom en situasjon skulle inntreffe, vil terskelen være lavere for den ansatte til å ta opp dette med egen leder. En slik regelmessig og strukturert sikringssamtale ansees å ha en god effekt overfor personer som vil kunne bli forsøkt rekruttert, men i forhold til infiltratører og andre som utfører ulovlige handlinger for egen vinning, vil tiltaket antakelig bare ha en begrenset effekt.

Terminologi: Tiltaket er bevisst kalt «sikringssamtale» og ikke «sikkerhetssamtale» eller «autorisasjonssamtale» da disse to sistnevnte er formelle og definerte begreper som benyttes i Sikkerhetsloven, kapittel 8 Personellsikkerhet. Se rapportens Appendix E for mer informasjon om Sikkerhetsloven og begrepene.

Sikkerhetslovens definisjoner:

Sikkerhetssamtale er en formell samtale som klareringsmyndigheten kan gjennomføre med den som er forespurt sikkerhetsklarert dersom det er tvil om en person er sikkerhetsmessig skikket til å bli sikkerhetsklarert.

Autorisasjonssamtale er en godkjennelse som enkeltpersoner må ha av sin leder for å få tilgang til sikkerhetsgradert informasjon

Tiltak 13: Adresser innsiderisiko i medarbeidersamtaler

Mange virksomheter kjører regelmessige (ofte årlige) medarbeidersamtaler. I samtalene bør linjeleder ta opp temaer om tilfredshet, misnøye og andre problemer som den ansatte opplever. Like viktig er det at gjennom en god dialog og åpenhet mellom leder og ansatt, så vil det være lettere for den ansatte senere å ta opp situasjoner dersom vedkommende har opplevd f.eks. trusler, pinlige situasjoner eller andre ubehagelige tilnærminger som kan være et forsøk på rekruttering. Dette tiltaket (medarbeidersamtale)

skiller seg fra foregående tiltak (sikringssamtale) ved at sistnevnte kjøres av en representant for sikringsenheten og adresserer de sikringsmessige krav, forventinger og relaterte prosesser (varslingsrutiner) osv., mens medarbeidersamtalen, som holdes av linjeleder, adresserer tilfredshet i det daglige arbeidet og er et ledd i arbeidet med å etablere en kultur for en god og åpen kommunikasjon internt i organisasjonen.

Tiltak 14: Regelmessig bekreftelse på forståelse av virksomhetens krav

Virksomheten bør vurdere å innføre et formelt system der ansatte og innleide med jevne mellomrom (f.eks. årlig eller hvert 3. år) må signere på at man har lest og forstått de sentrale interne krav – f.eks. knyttet til informasjonshåndtering, retningslinjer i forhold til korrupsjon o.l. Systemet kan innføres enten for alle, eller i det minste for de ansatte som kan være spesielt eksponert – f.eks. de som håndterer forretningsmessig sensitiv informasjon som f.eks. anbudsdokumenter, kontrakter, regnskap o.l. Systemet kan eventuelt innføres som et ledd i den årlige oppfølgingen gjennom sikringssamtale (se foregående tiltak). Signert dokumentasjon bør oppbevares i vedkommendes personalmappe.

Hensikten er i utgangspunktet å sikre at ansatte og innleide kjenner til de mest sentrale og til enhver tid gjeldende krav. Det er kan imidlertid være en svakhet ved slike «signeringer» at vedkommende bare signerer uten egentlig å ha satt seg inn i de nyeste kravene. Derfor er det å foretrekke at en slik signering gjøres i forbindelse med den regelmessige samtalen om sikring (se tiltaket over), der hovedpunktene i gjeldende krav gjennomgås.

Tiltak 15: Sikring settes på agendaen for møter på lik linje med HMS

I tillegg til opplæringsprogrammet for ledere (se tiltak Tiltak 7) temaet sikring regelmessig adresseres på ledermøter – nettopp siden ledere har en sentral rolle for at arbeidet med sikring blir vellykket. Videre bør sikring også tas opp på alle regelmessige møter nedover i organisasjonen, også blant ikke-ledere – på lik linje med HMS som i dag er vanlig hos de aller fleste. Det bør innføres et opplegg for «security moment», på lik linje med dagens «safety moment» som mange organisasjoner har innført.

Tiltak 16: Bevisstgjør om trusler ved utenlandsreiser og deltakelse på konferanser

Personer i petroleumsnæringen som reiser mye utenlands og som deltar på internasjonale konferanser kan være målobjekt for andre organisasjoners eller staters agenter – de kan bli forsøkt rekruttert eller lurt opp i en situasjon der det senere kan bli utøvd press for å tappe vedkommende for informasjon. Virksomheten bør ha et program for å informere disse personene om trusselen, hvilke feller man kan gå i, hvordan man skal opptre og hva man kan gjøre hvis man har kommet i en situasjon der man er lurt eller forsøkt vervet. Det må være en klar policy i virksomheten som er til hjelp for ledere som skal bistå arbeidstaker som har blitt utsatt for en slik situasjon, se også Tiltak 7: Etabler et opplæringsprogram for ledere.

Tiltak 17: Bevisstgjør utenlandske statsborgere om muligheten for verving

Enkelte personer med utenlandsk statsborgerskap kan bli utsatt for press og forsøk på rekruttering fra egne myndigheter. Gjennom noen år har PST i sine årlige åpne trusselvurderinger navngitt enkelte land som vil kunne være interessert i visse typer informasjon, og som kan utøve press på landets borgere og som arbeider i petroleumsnæringen. I tillegg kan også virksomhetene selv ha gjennomført egne trusselvurderinger som kan danne grunnlag for å vurdere hvorvidt et land bør ansees som risiko-land.

Virksomheten bør derfor ha opplegg for å forberede arbeidstaker på at de kan bli utsatt for slikt press, og informasjon om hvordan de bør handle dersom de blir utsatt for dette. At arbeidsgiver har pekt på denne muligheten vil også være med på å senke terskelen for å melde fra dersom en ubehagelig eller mistenkelig situasjon skulle oppstå. Det må være en klar policy i virksomheten som er til hjelp for de som skal bistå arbeidstaker som har blitt utsatt for slikt press, se også Tiltak 7: Etabler et opplæringsprogram for ledere.

Slik bevisstgjøring kan gjøres gjennom samtalene om sikring (se tidligere tiltak) eller som en del av linjeleders medarbeidersamtale. Det gjøres oppmerksom på at den ansatte det gjelder kan oppleve fokuset som mistenkeliggjørende og stigmatiserende. Av samme grunn kan ledere oppleve oppfølgning av de det gjelder som utfordrende. Det er derfor nødvendig at ledere gis nødvendig opplæring og informasjon om oppfølgning av utenlandske ansatte fra risiko-land.

Tiltak 18: Etabler praksis for ikke å omtale/lese sensitiv informasjon i åpne områder

Virksomheten bør ha en policy, eller regler med etablert praksis, om hvordan man skal omgås sensitiv informasjon på åpne steder – både muntlig omtale så vel som bruk av PC og håndtering av fysiske dokumenter. Når to kollegaer snakker sammen, eller man snakker i telefon, på en flyplass, på flytoget, i en taxi osv., er det mulig at den eller de som står i umiddelbar nærhet kan overhøre samtalen. Er man uheldig er dette en person som er en konkurrent, en leverandør, en fra media som kan fange opp og bruke denne informasjonen videre. Det er flere eksempler på at slikt har skjedd. Også i eget kontorlandskap, i kantinen, i kaffepauseområder osv. kan det være potensielle innsidere (kollegaer, gjester osv.) som kan fange opp samtalen og bruke eller misbruke informasjonen videre.

Ved lesing av dokumenter, eller bruk av PC, på offentlig sted (f.eks. flyet, flytoget, hotellobby) kan en som sitter ved siden av eller bak den som leser, fange opp informasjonen.

Det bør være en regel og etablert praksis om at sensitiv informasjon ikke skal diskuteres muntlig i slike åpne eller offentlige områder. Tilsvarende, at sensitive dokumenter (fysiske eller elektroniske) ikke skal åpnes i åpne eller offentlige områder.

Case: «Jeg satt på flyet og ved siden av meg satt en som arbeidet med anbudsdokumentasjon – et anbud knyttet til et prosjekt for vårt selskap. Hvem som helst kunne ha sittet ved siden av vedkommende og fanget opp viktig informasjon.»

Tiltak 19: Etabler løpende dialog med stedlig politi

Etabler og hold vedlike løpende og god kontakt med stedlig politi, eventuelt PST. Gjennom en god og løpende kontakt vil virksomheten lettere kunne få bistand til å tolke eller forstå innholdet i de åpne trusselvurderingene fra PST, og hva dette kan betyr for virksomheten. Videre, skulle en hendelse inntreffe, er god dialog med politiet en nødvendighet.

B: ORGANISATORISKE SIKRINGSTILTAK

Tiltak 20: Informasjonspolicy inneholder klassifisering av sensitiv informasjon

Etabler en informasjonspolicy der det tydelig fremgår de forskjellige klassifiseringsnivåene som benyttes i virksomheten. I tillegg til å definere klassifikasjonskriterier, må man sikre at arbeidstakere kjenner til og forstår hvordan sensitiv dokumentasjon skal klassifiseres slik at det blir brukt enhetlig i virksomheten. Erfaringen tilsier at dette ofte kan være et problem. Det bør etableres en veiledning som skisserer hvilken type informasjon som normalt vil høre til i hvilken klasse.

Eksempler på informasjon som kan ansees som sensitiv kan være: Strategidokumenter, oppkjøps- eller salgsplaner, kontrakter, tilbudsdokumenter med priser, finansielle data, kvartals eller årsregnskapstall før de er offentliggjort, persondata (helseopplysninger, lønnstall) anleggstegninger med oversikt over kritiske funksjoner/utstyr, geodata, teknologiske løsninger (Intellectual Property) m.m.

Det varierer hvordan virksomheter klassifiserer informasjon – alt fra en todeling (bare inndelt i intern informasjon og sensitiv informasjon), til en fire- eller femdeling av klassifiseringen (f.eks. åpen, intern, begrenset, konfidensiell, hemmelig).

Terminologi i Sikkerhetsloven: Det er imidlertid viktig å notere seg terminologien i Sikkerhetsloven (ref. /1/) – der defineres fire nivåer for sikkerhetsgradert informasjon – *Begrenset, Konfidensiell, Hemmelig* og *Strengt Hemmelig*. Videre er det i Sikkerhetsloven satt strenge krav til personer som skal håndtere sikkerhetsgradert informasjon, f.eks. krav om at personer som skal ha tilgang til denne type informasjon gradert «Konfidensiell» eller høyere, skal inneha gyldig sikkerhetsklarering, og det er videre krav om at personer som skal få tilgang til sikkerhetsgradert informasjon, skal autoriseres i tillegg til å inneha en sikkerhetsklarering (les mer i Appendix E om Sikkerhetsloven).

Per august 2019 er ikke Sikkerhetsloven gjeldende for petroleumsnæringen. Men, for å unngå eventuelle misforståelser i fremtiden, anbefales det at man ikke benytter de samme betegnelsene som i Sikkerhetsloven da kravet til behandling av informasjon klassifisert «Konfidensiell» vil ha forskjellig betydning og at det er forskjellig krav til håndtering avhengig av om organisasjonen er underlagt Sikkerhetsloven eller ikke. Denne forskjellen vil kunne medføre misforståelser mellom forskjellige virksomheter.

Tiltak 21: Etabler retningslinjer for håndtering av sensitiv informasjon

Virksomheten bør etablere entydige retningslinjer for hvordan informasjon i hver av de forskjellige klassifiseringsnivåene skal håndteres. Informasjonen må formidles til alle arbeidstakere, og sikre at den er forstått og etterlevd.

Retningslinjene bør være entydige og forstått av alle i virksomheten. Retningslinjene bør klart beskrive hvordan sensitiv informasjon skal håndteres. Dette gjelder både papirversjoner og elektroniske dokumenter som Word, Excel, Power Point, PDF og eventuelt andre formater. Kravene bør adressere bl.a. hvem som kan få tilgang til informasjonen, merking av dokumenter, forsendelse via både e-post, fax og vanlig post, kryptering av elektronisk informasjon, kopiering og utskrifter, lagring og sletting/destruksjon/makulering av dokumenter. I tillegg bør krav til muntlig omtale av sensitiv informasjon beskrives, se også Tiltak 18: Etabler praksis for ikke å omtale/lese sensitiv informasjon i åpne områder.

Videre bør retningslinjene beskrive krav vedrørende håndtering av informasjon som f.eks. hvem har tilgang til hvilken type informasjon, hvem setter eller endrer klassifisering av dokumenter, krav vedrørende hvilke typer dokumenter som ikke lov til å fjerne fra kontoret, krav vedrørende overføring av elektronisk informasjon til privat utstyr som f.eks. PC, nettbrett, mobiltelefon m.m.

Klare entydige retningslinjer, som er godt kjent blant alle arbeidstakere, vil redusere sannsynligheten for at sensitive dokumenter kommer på avveie eller kan kopieres av en innsider.

Tiltak 22: Krav om Clean Desk og låst PC-skjerm

Virksomheten bør etablere et krav om at sensitiv informasjon ikke skal være tilgjengelig eller synlig for uvedkommende. Det betyr f.eks. at sensitive papirdokumenter ikke skal ligge igjen på kontoret/bordet når vedkommende ikke er tilstede (Clean Desk Policy), PC-skjermer skal være låst når man ikke er tilstede, sensitiv dokumentasjon skal ikke kunne tas ut av kontorområdet og liknende. Det finnes eksempler der PC-skjermer har vært avfotografert med mobiltelfonen.

Case: Det ble oppdaget at vaske-hjelpen ved et innleid rengjøringsbyrå hadde tatt bilder med mobiltelefonen av dokumenter og åpne PC-skjermer mens vedkommende gjorde rent. I den videre etterforskningen ble det oppdaget at vaskehjelpen hadde fått betalt av en person som vedkommende leiet rom hos for å utføre handlingen.

Tiltak 23: Gjennomfør ny screening av ansatte ved skifte av arbeidsoppgaver

I tilfeller der en ansatt, eller innleid konsulent, skifter funksjon eller arbeidsoppgaver, kan det være behov for å gjennomføre en ny screening av vedkommende. Virksomheten bør etablere en formell prosess som sikrer at det gjennomføres en ny vurdering av personer som skifter funksjon eller arbeidsoppgaver, og der dette vil endre vedkommendes tilgang til sensitiv informasjon eller kritiske systemer.

C: TEKNOLOGISKE SIKRINGSTILTAK

Tiltak 24: Definer fysiske sikringssoner

Bestem hvilke fysiske områder eller rom etter kritikalitet. Dette kan gjelde både områder som inneholder sensitiv informasjon (f.eks. persondata, geodata, finansiell informasjon, informasjon om tekniske anlegg eller informasjon om spesielle sikringstiltak osv.) så vel som områder som kan bli utsatt for sabotasje og dermed påvirke driften eller sikkerheten til anlegget (f.eks. kontrollrom, serverrom, rom til koblingspanel/patcherom osv.). Ofte benyttes fargekoder eller tallkoder for å angi kritikaliteten av en sone.

For virksomheter som ikke faller inn under Sikkerhetsloven, anbefales det å bruke andre betegnelser enn de som benyttes i Sikkerhetslovens § 7-2 for klassifiseringen av skjermingsverdige objekter (Viktig, Kritisk og Meget kritisk), eller Virksomhetsikkerhetsforskriftens (kapittel 6) betegnelse for soner (Kontrollert, Beskyttet og Sperret), se Appendix E for mer informasjon om lovens og forskriftens terminologi.

Effekten av å ha klart definerte sikringssoner ansees å være god, under forutsetning av at den tilhørende adgangskontroll (se neste tiltak) er på plass.

Tiltak 25: Tilpass adgangskontroll basert på definerte sikringssoner

Definer hvilke grupper av personer / funksjoner som skal ha tilgang til de forskjellige sikringssonene – for hvilket tidsrom (tid på døgnet), og hvor lenge (f.eks. inntil videre eller bare for en kortere avgrenset periode), samt hvem som er autorisert til å gi tilgang til de forskjellige sonene. Videre er det nødvendig å ha systemer for regelmessig oppdatering av hvem som har aktiv tilgang til hvilke soner. Når en person slutter i virksomheten, eller skifter funksjon/stilling, bør dette reflekteres umiddelbart i vedkommendes tilgang til sonene – man bør ikke vente til neste oppdatering av listene, noe som kanskje skjer årlig eller kvartalsvis. Det samme gjelder for innleide konsulenter – deres tilgang til systemer og områder bør deaktiveres straks vedkommende ikke lenger har behov for denne tilgangen, selv om vedkommende skal tilbake til samme funksjon, system eller område etter en viss tid. Effekten av å ha en slik

adgangskontroll, med kontinuerlig oppdatering av aktive tilganger ansees å være god – under forutsetning av at oppdateringen skjer løpende.

Tiltak 26: Etabler spesielle kontrolltiltak for særs kritiske soner

For soner som ansees som spesielt kritiske, bør det etableres spesielle kontrolltiltak, som f.eks. kameraovervåking, adgangskontroll med to-faktorløsning (f.eks. kombinere PIN-kode, adgangskort, irisgjenkjenning, fingeravtrykkgjenkjenning eller ansiktsgjenkjenning), logg over hvem som entrer sonen og når, regelmessig sjekk av adgangslogger, oppfølging overfor personer dersom logger viser unormal adferd, egne samtaler om sikring for personer med autorisert adgang (se også Tiltak 12: Gjennomfør sikringssamtale regelmessig).

I henhold til Arbeidsmiljølovens kapittel 9 må det gis informasjon om spesielle kontrolltiltak til de personene som dette omfatter og kontrolltiltakene skal avklares med de arbeidstakers tillitsvalgte. Videre er det en egen forskrift om kameraovervåking i virksomheter. Se Appendix E for mer informasjon om slike kontrolltiltak.

Tiltak 27: Krav om adgangskontroll også offshore for særs kritiske soner

Tiltak rettet mot adgangskontroll for spesielt kritiske områder som er innført på land, blir ikke nødvendigvis innført i samme grad offshore. Ofte skyldes dette krav ut fra et sikkerhetsmessig aspekt (safety). Imidlertid er det indikasjoner på at visse spesielt kritiske områder ikke har fysiske eller andre barrierer for å hindre uautorisert adgang, selv om området ikke nødvendigvis må være åpent av sikkerhetsmessige grunner. Virksomheten bør derfor sikre at det gjennomføres en egen vurdering offshore med det for å øye å kunne vurdere å innføre egne adgangs- og andre kontrolltiltak offshore.

Tiltak 28: Spesielt gode låsordninger for særs kritiske soner/objekter

Mange virksomheter benytter kombinasjonen adgangskort og vedkommendes vanlige firesifrete PIN-kode som to-faktorløsning ved adgang til også særs kritiske soner. Dersom kortet er av den typen som lett kan kopieres, vil det med litt planlegging kunne være en enkel sak for en med uærlige hensikter, og litt teknisk innsikt, å observere PIN-koden og deretter kopiere eller stjele adgangskortet. Andre virksomheter benytter fysiske nøkler til dører og skap. Nøkler som oppbevares f.eks. i resepsjonen eller hos vekter må ofte signeres ut og inn. Andre steder ligger kanskje nøklene til et skap med sensitiv informasjon i en ulåst skuff. Dersom etterlevelsen av nøkkeladministrasjonen ikke fungerer helt etter hensikten, vil dette lett kunne medføre nøkler på avveie.

For særs kritiske områder bør virksomheten velge en låsløsning og administrasjon av denne fult ut sikrer at ingen uvedkommende kan utnytte sårbarheten og misbruke kort, PIN-koder eller fysiske nøkler.

Tiltak 29: Møterom egnet for utveksling av sensitiv informasjon

Møterom beregnet for besøkende bør, om mulig, lokaliseres slik at gjestene ikke trenger å passere første fysiske barriere mellom resepsjonen og inn i bygget. Flere virksomheter har lokalisert slike møterom i resepsjonsområdet.

Videre bør det legges til rette for at noen møterom har fasiliteter som gjør disse egnet for møter der sensitiv informasjon diskuteres og utveksles. Dette gjelder både møterom beregnet for besøkende så vel som møterom inne i bygget for virksomhetens arbeidstakere. Slike møterom bør ha fasiliteter (f.eks. låsbare skap) for å kunne legge igjen mobiltelefoner, nettbrett og annet elektronisk utstyr utenfor

møterommet. Videre bør det være en rutine for å sikre at elektronisk utstyr ikke tas med inn i møterommet, og for å sjekke at avlyttingsutstyr ikke er gjemt i rommet. Slikt utstyr kan være plantet i forkant av personer med lovlig tilgang til området.

Tiltak 30: Etabler regler for tilgangsstyring til intranett og applikasjoner

En virksomhet har normalt svært mange applikasjoner som benyttes av mange arbeidstakere, og noen av disse inneholder sensitiv informasjon. Dette gjelder gjerne sider på intranett og applikasjoner som f.eks. SharePoint, Teamsite, samt andre områder på serveren (foldere) som kun er beregnet for en lukket gruppe osv. Når nye personer trenger tilgang, gis dette ofte av vedkommende som «eier» applikasjonen. Erfaringen er også at den som skal administrere tilgang kan få en forespørsel om tilgang for en person som vedkommende ikke kjenner – og dermed ikke nødvendigvis har muligheten å vurdere om vedkommende er autorisert for tilgang eller ikke.

Ifølge Crowd Research Partners (ref. /72/) viser deres undersøkelse at for mange brukere med unødvendig tilgang til systemer ansees å være den problemet knyttet til dataangrep utført av innsidere. Dette etterfølges av økende antall enheter med tilgang til sensitive data, og en mer kompleks teknologi. Se også Appendix F, kapittel F.2.

Virksomheten bør ha klare og entydige regler for hvem som skal ha tilgang til hva (se også Tiltak 31: Restriksjon i tilgang for utvalgte grupper), hvem som kan innvilge/godkjenne tilgang, hvem som kan gi tilgang. For arbeidsoppgaver og stillinger identifisert som kritiske (ref. Tiltak 1: Gjennomfør en stillingsspesifikk risikovurdering) bør man vurdere å trekke inn representanter fra sikringsenheten i denne vurderingen.

Tiltak 31: Restriksjon i tilgang for utvalgte grupper

For enkelte grupper av personer er det aktuelt å gi eller begrense tiltak til nettet – permanent eller for en periode. Innleide konsulenter og andre kontraktører har gjerne behov for tilgang til store deler av intranettet og tilhørende applikasjoner. Det bør gjøres en konkret vurdering i hvert enkelt tilfelle mht. hva vedkommende skal ha tilgang til – basert på «need-to-have»-prinsippet, ikke på «nice-to-have»-prinsippet. Dette kan gjelde utvalgte sider på intranettet, så vel som applikasjoner som inneholder sensitiv informasjon. For arbeidsoppgaver og stillinger identifisert som kritiske (ref. Tiltak 1: Gjennomfør en stillingsspesifikk risikovurdering) bør man vurdere å trekke inn representanter fra sikringsenheten i denne vurderingen.

Videre er det nødvendig at ved endringer i arbeidsoppgaver, så må det umiddelbart (samme dag) gjøres tilsvarende endringer i vedkommendes tilganger. Det samme kan gjelde for arbeidstakere som er over i en oppsigelsesfase dersom det er vurdert at vedkommende skal ha begrenset til tilgang (se også Tiltak 39: Vurder behov for å begrense tilgang til systemer eller områder, i kapittel 5.6.2).

Tiltak 32: Jevnlig opprydding av tilgangsrettigheter

Like viktig som å gi riktig tilgang til rett person, er det å justere tilgang når en person skifter arbeidsoppgaver, ansvarsområder eller slutter. Når en person skifter arbeidsoppgaver får vedkommende gjerne umiddelbart ny tilgang basert på behovet i de nye arbeidsoppgavene, mens derimot eldre tilganger vedkommende ikke lenger har behov for, blir ikke nødvendigvis umiddelbart deaktivert.

Virksomheten bør ha en prosess som sikrer regelmessig opprydding i tilgangsrettighetene. Ideelt sett bør en slik endring implementeres umiddelbart (samme dag) som vedkommende endrer

arbeidsoppgaver. For en stor organisasjon kan det imidlertid vise seg å være krevende å gjøre dette umiddelbart. I det minste bør virksomheten etterstrebe en umiddelbar oppdatering av tilgang for de personer som gjennom risikokartleggingen (se Tiltak 1: Gjennomfør en stillingsspesifikk risikovurdering) er identifisert å ha spesielle arbeidsoppgaver med tilgang til særs kritiske områder eller systemer.

For områder der det er etablert en «eier» (f.eks. en TeamSite, en folder på spesielt område på serveren osv.) bør det være «eieren» som har ansvaret for løpende eller regelmessig oppdatering. Videre er det ofte arbeidstakers linjeleder som er ansvarlig for å melde inn eventuelle endringer til «eieren» i arbeidssituasjon som tilsier en endring i tilgang.

Tiltak 33: IT-adminpersonell har personlig adminkonto

For personer med aksess til høyprioriterte systemer (vedlikehold, administrasjon osv.) bør hver enkelt ha sin personlige adminkonto – det bør ikke være felleskontoer som flere kan benytte. Dersom flere personer benytter en felles adminkonto vil en logg ikke kunne avdekke hvem som har vært inne på systemet og gjort hva og når. Med bruk av en personlig adminkonto vil imidlertid dette være mulig.

Tiltak 34: Arbeidsoperasjoner på høyprioriterte systemer utføres under fire øyne

For arbeidsoperasjoner på høyprioriterte systemer bør virksomheten ha et krav om at slike arbeidsoperasjoner skal utføres av minst to personer. Dette vil redusere sannsynligheten for at én person med uærlige hensikter vil kunne benytte muligheten og utføre en uautorisert og bevisst handling siden det da hele tiden vil være en annen person tilstede som observerer arbeidsoperasjonen. Dette vil også kunne oppleves som positivt for en utførende arbeidstaker med kun ærlige hensikter, siden man i ettertid ikke vil kunne beskyldes for å ha gjort noe ulovlig.

Tiltak 35: Elektronisk logg av aktiviteter

Virksomheten bør sikre at man har en hendelseslogg – logg over aktiviteter som f.eks. entring av forskjellige sikringssoner (hvem og når), aktivitet på nettet, gjentakende forsøk på å komme inn på sider man ikke har autorisert tilgang til, gjentakende forsøk på innlogging på systemer uten autorisert tilgang/adgang, nedlasting av store mengder data, hyppig forespørsel etter adminrettigheter[5] m.m.

Slik informasjon kan dog ikke brukes i vanlig kontrollvirksomhet iht. Arbeidsmiljølovens kapittel 9, og Forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale (for mer informasjon se Appendix E) med mindre det er saklig grunn for det, som f.eks. berettiget mistanke om sikkerhetsbrudd (se også Tiltak 26: Etabler spesielle kontrolltiltak for særs kritiske soner). Derimot er slik informasjon nødvendig i forbindelse med gransking av eventuelle hendelser. I slike tilfeller er det lovlig å hente ut informasjon og informasjonen dersom den brukes i granskningsøyemed.

Ifølge Insider Threat report 2018 fra Crowd Research Partners gjort blant 472 IT-sikringseksperter (ref. /72/), endrer virksomhetene sitt fokus til å detektere innsidertrusler (64 % svarte dette), etterfulgt av å implementere metoder for å avskrekke (58 %) og analyse og granskning av aktuelle hendelser (49 %). Metoder for å overvåke adferd øker, og 88 % av organisasjonene benytter seg av en eller annen form for overvåking av brukere.

[5] Adminrettigheter: Flere organisasjoner har lagt på en sperre slik at arbeidstaker ikke kan installere programmer på egen PC, men må be om å få adminrettigheter for en begrenset periode (f.eks. 24 timer) for å kunne foreta slik nedlasting og installasjon. I denne perioden er PC-en mer sårbar for angrep, og virksomheten har ikke kontroll på hva vedkommende installerer.

Ny teknologi åpner opp for flere muligheter for å kartlegge hva som er normal data-aktivitet for å avsløre unormal/uautorisert tilgang til systemer og data og gi varsel. Eksempler kan f.eks. være kunstig intelligens, maskinlæring, osv. Det er imidlertid viktig at innføring av slike tiltak heller ikke kommer i konflikt med gjeldende lovverk og forskrifter (se Appendix E).

Tiltak 36: Manuelle observasjoner og andre måleaktivteter

Manuelle observasjoner er observasjoner gjort av personer som f.eks. vektere, streifvakt, resepsjonen, sikringspersonell eller andre. Dette kan typisk være observasjoner om at en arbeidstaker har unormale og/eller endrede arbeidstider, oppholder seg i områder der vedkommende normalt ikke hører hjemme eller annen merkelig adferd. Selskapet bør ha en kultur for, og et system for, at slike observasjoner blir rapportert – til sikringsenheten og/eller til vedkommendes leder. Disse bør så ta dette opp med vedkommende og avklare bakgrunnen for dette. Slik adferd kan gjerne ha forklarlige årsaker – som spesielt arbeidspress i en begrenset periode eller en privat familiesituasjon som gjør at unormale arbeidstider er nødvendig. Skulle derimot adferd være knyttet til at personen planlegger eller utfører uærlige hensikter, kan en tett oppfølging virke avvergende på eventuell videre handling.

Virksomheten bør også utnytte resultatene fra andre og forskjellige typer måleaktivteter som allerede benyttes i organisasjonen. Dette kan være f.eks. test-phishing mail som sendes til alle ansatte, registrering og rapportering av forskjellige typer sikringshendelser, resultater fra arbeidsmiljøundersøkelser som adresserer tilfredshet, medarbeidersamtaler, varslingssaker.

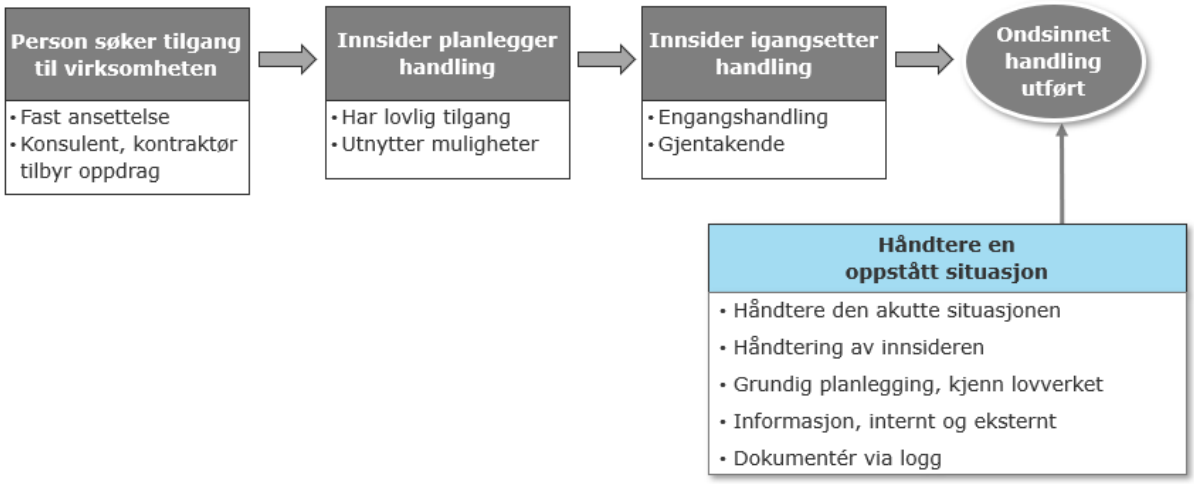
NATO-dokumentet Insider Threat Detection Study (ref. /75/) påpeker at det ikke finnes noen standard indikatorer for å oppdage innsidere, men at disse bør utvikles av hver enkelt organisasjon. Imidlertid har rapporten noen oversiktstabeller som kan være nyttige som underlag i denne sammenhengen. En samletabell er vist i Appendix D.

5.5 Tiltak for å håndtere en oppstått situasjon

Dette kapittelet omhandler tiltak for å håndtere en innsidesituasjon som har oppstått. Enten har virksomheten oppdaget at en person er i ferd med å planlegge eller utføre en handling, eller det er oppdaget at en ondsinnet handling er utført – og man kjenner ikke nødvendigvis til hvem gjerningspersonen er.

5.5.1 Tiltak oppsummert

I første omgang er det vesentlig å sikre at konsekvensene av den utførte handlingen begrenses så mye som mulig, og gjerne så raskt som mulig. Videre må man vurdere hvem som kan bli berørt (f.eks. eget personell, kunder, partnere, eiere, omgivelser), og det må legges et løp for hvordan situasjonen skal kommuniseres – hva som skal kommuniseres til hvem, på hvilken måte, når og i hvilken rekkefølge. Avhengig av om gjerningspersonen(e) er kjent eller ikke må det legges et løp for hvordan vedkommende skal håndteres eller eventuelt hvordan hendelsen skal granskes for å identifisere gjerningspersonen(e). I visse situasjoner kan det være naturlig at politiet kobles inn. Alt som gjøres bør grundig loggføres slik at det på et senere tidspunkt kan dokumenteres, dersom det skulle bli en oppsigelsessak eller politisak ut av dette. Uansett må virksomheten kjenne til lovverket slik at man holder seg innenfor dette i granskingen og oppfølgingen av hendelsen.



Figur 5-6: Kategorier av tiltak for å håndtere en situasjon som har oppstått, enten oppdaget en person som er i prosess med å utføre en handling, eller at en handling er utført

5.5.2 Spesifikke tiltak

Tiltak 37: Plan for å håndtere en potensiell hendelse

Virksomheten bør lage en plan for hvordan en potensiell hendelse skal håndteres. Hendelsen kan være at det er fattet mistanke overfor en person om at vedkommende er i ferd med å planlegge eller utføre en uønsket handling, eventuelt at det er oppdaget at noen har utført en handling, men at det ikke er identifisert hvem dette er. Planen bør adressere bl.a.

- Etablere team som håndterer saken og hvem som bør involveres i teamet, de mest sentrale antas å være ressurser fra HR, juridisk, IT, sikring og kommunikasjon
- Avklare med ledelsen mht. behov for å fristille ressurser til eventuell gransking og oppfølging av saken, samt løpende kontakt med ledelsen – omfang er avhengig av alvorlighetsgrad
- Behov og mulighet for å gjennomføre elektroniske søk i logger over aktivitet på nettet, applikasjoner, entring av soner osv.
- Lovmessige muligheter og begrensinger som foreligger vedr. elektroniske søk og reaksjon overfor vedkommende
- Kommunikasjon med vedkommende dersom denne er kjent (hvem kommuniserer hva og når), eventuelt aksjoner for å identifisere aktøren (i tilfelle vedkommende ikke er kjent)
- Informasjon innad og utad – hva kan sies, til hvem og når (innad i egen organisasjon, og utad mot f.eks. partnere i prosjekter/lisenser, mediene, familie, myndigheter og andre)
- Ta kontakt med politiet f.eks. i tilfelle at det utført en kriminell handling
- Etabler en virksomhetskontinuitetsplan (engelsk: Business Continuity Plan) for å sikre videre drift dersom en kritisk hendelse skulle inntreffe

I tillegg til selve planen, bør det legges opp til at det gjennomføres nødvendig opplæring og trening i hele eller deler av planen.

Se også erfaringene fra hendelsen hos Aker Solutions som inneholder mer aksjonspunkter knyttet til en helt konkret hendelse, omtalt i kapittel 6.2.

5.6 Avslutning av arbeidsforholdet

Det kan være flere grunnet til at et ansettelses- eller kontraktsforhold avsluttes. Vedkommende kan selv ha sagt opp for å gå over i annen jobb, vedkommende kan ha blitt sagt opp av arbeidsgiver, kontrakten går ut og det er ikke innvilget fornyelse (typisk ved innleie eller midlertidig ansettelse), eller vedkommende kan være en del av en nedbemanningsprosess som rammer flere. Det er med andre ord flere forhold som kan føre til at vedkommende på vei ut av virksomheten har blitt frustrert, irritert, føler seg urettmessig behandlet o.l.

Resultatet kan være at vedkommende utfører handlinger i oppsigelsestiden som kan få negative konsekvenser for virksomheten eller enkeltindivider. I ytterste konsekvens kan vedkommende urettmessig ta med seg verdisaker (f.eks. elektronisk utstyr) eller informasjon (sensitive opplysninger, programvare, modeller eller annen Intellectual Property), alternativt at vedkommende ønsker å skade selskapet (f.eks. plante virus, offentliggjøre forhold som kan skade omdømmet) eller til og med utøve trusler eller vold mot enkeltpersoner.

Hvordan virksomheten håndterer prosessen frem til oppsigelsestiden starter, vil kunne være avgjørende for om vedkommende blir motivert til å utføre slike uønskede handlinger eller ikke.

Avslutningsfasen kan være kritisk siden en uheldig avslutning på et arbeidsforhold kan medføre at en person som ikke tidligere har vært betraktet som en innsidetrussel, kan utvikle seg til å bli det hvis vedkommende opplever å bli urettferdig behandlet, eller om vedkommende er i psykisk ubalanse. Denne opplevelsen og sinnstilstanden vil kunne være påvirket av årsaken til hvorfor vedkommende slutter / må slutte. Et arbeidsforhold som avsluttes ved at vedkommende selv sier opp og skal over i en ny jobb, kan være mindre kritisk enn et arbeidsforhold der vedkommende har blitt sagt opp eller er en del av en nedbemanningsprosess der også andre kollegaer må forlate virksomheten.

Vedkommende kjenner i stor grad til virksomhetens systemer og rutiner og til eventuelle svakheter, har muligens tilgang til kritisk informasjon eller systemer, og har potensiale til å kunne gjøre stor skade i siste fase av arbeidsforholdet. Videre kan en person, dersom virksomheten ikke har gjort jobben sin med å deaktivere tilganger, utrette stor skade etter avsluttet arbeidsforhold. Også materiale (metoder, løsninger osv.) som virksomheten har opphavsrett til, kan være fristende for en med uærlige hensikter å ta med seg før vedkommende forlater organisasjonen.

5.6.1 Tiltak oppsummert

Tiltak for å redusere sannsynligheten for at en potensiell innsider utfører uønskede handlinger mens vedkommende er i oppsigelsesfasen, eller etter av vedkommende har avsluttet forholdet, begynner allerede mens vedkommende er i normalt arbeid, altså før selve avslutningsfasen. Dersom vedkommende har opplevd et positivt ansettelsesforhold, reduseres sannsynligheten for at vedkommende er misfornøyd og skulle ønske å utføre uønskede handlinger i oppsigelsestiden eller i etterkant.

Tilsvarende, en god prosess knyttet til selve oppsigelsen, vil også kunne virke forbyggende. I oppsigelsesfasen må man vurdere hvorvidt det skal gjøres endring i vedkommendes tilganger eller arbeidsoppgaver for å redusere muligheten for at vedkommende tilegner seg informasjon eller kommer inn på systemer og kan utføre sabotasjeliknende handlinger. Det er også viktig å minne arbeidstaker om krav i ansettelseskontrakten – eventuelle konfidensialitetskrav, Intellectual Property og hva arbeidstaker ikke har lov å ta med seg o.l. Innlevering av utstyr og deaktivering av tilganger må også skje senest siste arbeidsdag. Skulle en hendelse inntreffe i etterkant, etter at vedkommende har forlatt virksomheten, er dette erfaringsmessig ofte ressurskrevende og vanskelig å håndtere.

.

Figur 5-7: Tiltak for å hindre uønskede handlinger i oppsigelsestiden og etter at forholdet er avsluttet

5.6.2 Spesifikke tiltak

Tiltak 38: Ha en god oppsigelsesprosess

En god prosess vil kunne virke forebyggende og sannsynligheten muligheten for at arbeidstaker blir ytterligere misfornøyd eller forbitret[6], og blir fristet til å utføre uønskede handlinger. Dette gjelder både dersom vedkommende selv sier opp (oftest er det da ikke knyttet spesielle «sure miner» til avslutningen), blir sagt opp eller er en del av en større nedbemanning der også andre som personer må forlate virksomheten. En god prosess omfatter bl.a. en åpen, løpende og god dialog der vedkommende også har følelsen av å bli hørt, blir gitt en god begrunnelse for avslutning av forholdet, akseptable økonomiske kompensasjoner (spesielt gjelder dette ved nedbemanning) m.m. I tillegg bør linjeleder i dialogen med vedkommende, så tidlig som mulig, minne om ansettelseskontrakten og eventuelle forhold som har med sensitiv informasjon å gjøre, slik at vedkommende i oppsigelsesperioden er klar over hva han/hun har lov til, eller ikke, å ta med seg fra arbeidsplassen. Oppsigelsesprosessen bør være tydelig beskrevet i virksomhetens styringssystem.

Tiltak 39: Vurder behov for å begrense tilgang til systemer eller områder

I det øyeblikket en person er under oppsigelse, være seg at vedkommende har sagt opp selv eller har blitt sagt opp, bør man vurdere om det er tilrådelig at vedkommende fortsatt skal ha uendret tilgang til soner og/eller datasystemer, eller om disse skal helt eller delvis begrenses i oppsigelsesperioden. En slik

[6] Forbitret: På engelsk brukes ofte begrepet «disgruntled employee». Med forbitret («disgruntled») menes at man er mer enn bare misfornøyd, man er sint på organisasjonen eller personen.

beslutning bør gjøres basert på en risikovurdering der vedkommendes funksjon og tilganger i den ansattes siste arbeidsperiode, og om det kan være muligheter for at vedkommende vil kunne utgjøre en innsidetrussel, vurderes opp mot hvilke konsekvenser det kan få om vedkommende kopierer informasjon eller har mulighet for å sabotere enkelte systemer eller prosesser. Eventuelt kan utfallet av vurderingen være at vedkommende umiddelbart fritas for sine oppgaver og blir bedt om å forlate arbeidsstedet med umiddelbar virkning.

Det er argumenter både for og imot en beslutning om å begrense tilgang under avslutningsperioden. *Fordelen* er at det begrenser muligheten for en person å tilegne seg sensitive informasjonen i oppsigelsestiden, eller å gjøre noen ondsinnede grep knyttet til virksomhetens prosesser eller systemer. *Ulempen* er at vedkommende vurderer dette som at virksomheten ikke har tillit til ham/henne og at det kan forsterke eventuelle negative oppfatninger hos vedkommende og være spiren til å begå uønskede handlinger. Videre kan det sies at en person som har sagt opp selv kan ha planlagt dette i forkant og allerede har kopiert over sensitiv informasjon før oppsigelsen ble innlevert.

Tiltak 40: Sikre retur av dokumenter som eies av virksomheten

Når arbeidstaker avslutter et forhold, bør man sikre at alle dokumenter som ansees som virksomhetens eie, og som arbeidstaker ikke har lov til være i besittelse av etter avsluttet arbeidsforhold, er returnert. Dette bør skje senest siste arbeidsdag.

Tiltak 41: Sikre innlevering av utstyr

Når arbeidstaker avslutter et forhold, bør man sikre at alt elektronisk utstyr (PC, mobiltelefon, nettbrett, harddisker, PIN-kodebrikker, adgangskort o.l.) returneres senest samme dag som vedkommende slutter. I noen virksomheter er det mulig for den som slutter å overta mobiltelefonen vederlagsfritt. I så fall bør det være en prosess for at utstyret «vaskes» av IT-avdelingen for å sikre at det ikke inneholder informasjon eller systemer som vedkommende i ettertid kan benytte. Eventuelle fysiske nøkler innleveres.

Tiltak 42: Deaktiver tilganger og adganger senest siste arbeidsdag

Når en arbeidstaker avslutter et forhold, bør man sikre at alle påloggingsmuligheter deaktiveres umiddelbart, og senest siste arbeidsdag. I tillegg, at adganger gjennom bruk av f.eks. adgangskort og PIN-koder deaktiveres. Dette gjelder både egne ansatte og kontraktør (f.eks. innleid konsulent eller personer som driver vedlikehold på systemer).

Tiltak 43: Gjennomfør sluttintervju

Mange virksomheter avholder sluttintervju. Sluttintervjuet bør benyttes til å minne arbeidstaker om kontrakten og forhold som har med sensitiv informasjon å gjøre, eventuell taushetsplikt – som også gjelder etter avsluttet arbeidsforhold. Videre er det viktig å sørge for en god form på sluttintervjuet, slik at intervjuobjektet sitter igjen med en god følelse – følelse av å bli hørt. Dette vil kunne være med på å etterlate et godt inntrykk, og eventuelt redusere muligheten for at vedkommende utvikler ideer om å gjøre noe som i ettertid kan skade virksomheten.

Tiltak 44: Deaktiver tilgang for kontraktører ved midlertidig opphold i engasjement

Mange virksomheter avholder sluttintervju. Sluttintervjuet bør benyttes til å minne arbeidstaker om Når en kontraktør (f.eks. innleid konsulent eller vedlikeholdsperson) skal ha et opphold i sitt engasjement for virksomheten, må det sørges for at alle tilganger deaktiveres/slettes umiddelbart, selv om det er forventet at vedkommende er tilbake i sin funksjon som innleid etter kort tid. En ikke uvanlig svakhet knyttet til slike situasjoner er man ikke deaktiverer tilgangen dersom man vet at vedkommende skal tilbake i samme oppgave en tid senere. Ofte skyldes dette virksomhetenes interne prosesser – da slipper vedkommendes linjeleder eller kontaktperson å søke tilgang.

Case: Det gikk rykter ved et av utenlandskontorene til selskapet at det var nedbemanning og oppsigelser på gang. IT avdelingen i selskapet oppdaget etter hvert at 3 av de oppsagte personene hadde lastet ned store mengder (1,4 TB) kommersiell og teknisk informasjon om et prosjekt. Dette ble oppdaget først etter at personene hadde sluttet. Selskapet brukte store ressurser på å finne ut av omfanget og av mulige konsekvenser ved at informasjonen var kommet på avveie.

Tiltak 45: Innfør tiltak som hindrer tilgang for personer som har sluttet

Virksomheten bør innføre systemer som kan fange opp og eventuelt hindre ikke-autorisert aktivitet etter at personer har sluttet. CPNI har i sin studie (ref. /44/) påpekt at selv enkle systemer for å kontrollere hvordan ansatte kunne introdusere eller fjerne elektroniske data, og manipulere organisasjonsinformasjon selv etter at de hadde sluttet i virksomheten, var ikke implementert, se også Appendix F, kap. F.2.A.

5.7 Implementering

En vellykket implementering av et styringssystem, og av spesifikke tiltak, er helt nødvendig for at styringssystem og tilhørende spesifikke tiltak skal ha den effekten som er tiltenkt. Det er viktig å være klar over at implementering er noe langt mer enn bare å sende ut en e-post med informasjon om at en ny regel eller prosedyre er innført.

Nedenfor følger noen generelle råd for å sikre en god implementering.

Status – hvor står virksomheten i dag: Gjennomfør en enkel gapanalyse for å finne ut av hvor godt rustet virksomheten er. Modenhetsundersøkelsen omtalt i kapittel 7 og Appendix C kan være et godt verktøy. Undersøkelsen danner grunnlag for å finne ut av hvilke ytterligere tiltak organisasjonen bør vurdere å innføre.

Forankring og forpliktelse fra ledelsen: Det er helt nødvendig å sikre god forankring og forpliktelse hos, uten dette vil det være vanskelig, kanskje umulig, å få til en vellykket implementering, og levedyktig system.

- Ledelsen må avsette tilstrekkelige ressurser til implementeringen – dette kan være en kombinasjon av ressurser i kraft av tilgjengelig tid, kompetanseoppbygging, økonomiske midler, teknologiske løsninger.
- Ledelsen må synliggjøre at sikringsarbeidet er viktig for virksomheten, at ledelsen står bak og støtter de som driver dette frem. Eksempler på måter å promotere sikring på kan være å ha temaet på allmøter, i de regelmessige møter i ledergruppen, sette krav om at dette også skal

gjøres videre nedover i organisasjonen, og omtale sikring i regelmessige rundskriv, nyhetsbrev eller på intranettet.

- Ledelsen må være en rollemodell. Enhver leder, uansett nivå, må gå foran med et godt eksempel. Det tar normalt lang tid å bygge opp en god sikringskultur, men det kan brytes meget for ned igjen. Skulle en leder selv ikke følge interne regler, f.eks. om å bære adgangskort synlig eller å låse PC-en når den forlates, kan man ikke forvente at ansatte skal gjøre det heller. En slik feilaktig adferd vil lett gi et feil signal.

Involver og kommuniser ved implementering av tiltak: Ideelt sett bør de som berøres av et tiltak involveres i utarbeidelsen av tiltaket. Dette er med på å skape forståelse for hvorfor det er behov for tiltaket, og det kan skape et større eierskap som også gjør at de involverte sannsynligvis i større grad vil etterleve tiltaket. I tillegg vil de kunne fungere som «ambassadører» overfor kollegaer. Tilsvarende er det nyttig at de arbeidstakers tillitsvalgte er involvert i utarbeidelse av tiltak. Vær også spesielt oppmerksom på at det også er lovkrav om involvering av de tillitsvalgte ved innføring av kontrolltiltak i virksomheten (se også Appendix E, om lovkrav).

I tillegg må det tydelig kommunisere til alle ansatte som berøres av tiltaket – både at tiltaket er innført, hvorfor det innføres, hva tiltaket skal bidra til å løse, og hva dette i praksis betyr for den enkelte.

Vurder behov for kompetanseheving: I visse sammenhenger kan det også være behov for opplæring eller trening knyttet til innføring av spesifikke tiltaket. Det er viktig at dette tas høyde for, og at nødvendig opplæring gjennomføres – gjerne i rimelig tid før tiltaket implementeres. Undersøkelsen fra Crowd Research Partners (ref. /72/) viste at mangelfull opplæring og tilgang på ekspertise var den største hindringen for å få til et godt opplegg for å håndtere innsidetrusselen på, se også Appendix F.

Øk bevisstgjøringen gjennom et promoteringsprogram: Et promoteringsprogram har til hensikt å øke bevisstheten og forståelsen både om de verdier virksomheten besitter og som kan være av interesse for en innsider, og om hvem innsideren kan være og hvordan vedkommende kan opptre, og ikke minst om de sikringstiltak som er innført. Det bør lages en plan for hvordan promoteringsprogrammet skal gjennomføres. Gjennomføringen kan være som e-læringsprogrammer, klasseromsundervisning, nanolearning, allmøter, avdelingsmøter, medarbeidersamtaler osv.

Etabler en egen side på intranett som omhandler sikring: Sørg for at all praktisk informasjon rundt sikring ligger på en lett tilgjengelig og forståelig side på intranettet. Samle nødvendig og nyttig informasjon på en enkel måte slik at siden oppleves som fornuftig og brukervennlig. Jo mer brukervennlig, desto større er sannsynligheten for at informasjonen når ut til de ansatte og at den benyttes. På denne siden kan man også ha informasjon f.eks. om sikringsorganisasjonen i virksomheten (hvem er hva), om rapportering av sikringshendelser og varslingskanal, praktiske råd og tips for reiser, bruk av krypteringsløsninger og mye mer.

6 ANDRE FUNN FREMKOMMET GJENNOM PROSJEKTET

Dette kapittelet sammenfatter de viktigste funnene som er fremkommet gjennom prosjektet. Først omtales kort status i petroleumsnæringen – deres utfordringer og tiltak for å håndtere innsiderisikoen. En mer utfyllende beskrivelse finnes i Appendix B. Dernest er hovedtrekkene fra litteraturstudien sammenfattet.

6.1 Situasjonen i petroleumsnæringen

Som nevnt i kapittel 3 ble det gjennomført en workshop med deltakelse fra 15 selskaper innen petroleumsnæringen samt NSM, PST og Ptil. Selskapene stille med representanter fra sikringsmiljøet i virksomhetene, HR, IT og fra juridisk. Hensikten med workshopen var å utveksle erfaring med forebygging og håndtering av innsiderisiko, hvilke utfordringer selskapene hadde erfart og få innspill til hva som kan være god praksis:

- Hvilke utfordringer vedr. innsiderisiko kan eget selskap stå overfor
- Hvilke aksjoner som er, eller kunne ha vært, innført for å håndtere innsiderisikoen, i den hensikt å kunne:
    - forebygge at en person som ansees å kunne utgjøre en innsiderisiko ansettes/engasjeres eller at ansatt/innleid utvikler seg til å bli en innsider
    - detektere (identifisere/oppdage) en typisk innsider (f.eks. gjennom vedkommendes adferd)
    - hindre en innsider i å utføre en vellykket ondsinnet handling
- Diskutere utfordringer ved å implementere de foreslåtte aksjonene/tiltakene (f.eks. personellmessige, organisatoriske, lovmessige, tekniske, kostnadsmessige eller andre utfordringer)

Videre, ble det i etterkant av workshop, gjennomført dybdeintervjuer av representanter fra utvalgte selskaper (se liste i Appendix A) for å kunne gå nærmere inn på de utfordringer selskapene hadde erfart mht. innsiderisiko, hva man gjør for å håndtere denne risikoen (konkrete tiltak – god praksis), samt få innspill til identifisering av gode veiledere, rapporter og andre dokumenter som kunne være nyttige for i det videre arbeidet med utarbeidelse av denne rapporten.

En oppsummering av resultatene fra tilbakemeldingene fra petroleumsnæringen, gjennom workshopen 5. mars 2019 og etterfølgende dybdeintervjuer, er å finne i Appendix B.

6.2 Case – Håndtering av en reell situasjon – Aker Solutions

Sikringshendelser blir ofte holdt hemmelig og ofte ikke delt med andre. En hendelse som derimot fikk mye oppmerksomhet i media var knyttet til en situasjon der en ansatt i Aker Solutions ble pågrepet i 2015, og senere dømt. Denne hendelsen hadde en del læringspunkter, og Aker Solutions har delt en del av disse punktene.

Oppsummering av hendelsen og de faktiske forhold:

Gjennom interne kontrollrutiner ble det avdekket bilder og tekster på internett som bl.a. uttrykte støtte til den Islamske Stat (IS). Det var mistanke om at disse innleggende var koblet til en ingeniør ansatt i Aker Solutions.

Aker Solutions gjennomførte diverse videre søk for å finne ut av om kilden til innleggene på nettet stammet fra den mistenkte ingeniøren. Det var viktig at så få personer som mulig kjente til mistanken og til arbeidet med å undersøke mulige koblinger. I Aker Solutions var det derfor i denne fasen bare en meget liten gruppe med utvalgte personer som ble gjort kjent med situasjonen, mistanken og undersøkelsene. Samtidig var det vesentlig at man internt i Aker Solutions gjorde formelle avklaringer relatert til lovverket siden man, som en del av granskningen, måtte inn og granske datatrafikk og e-post til den mistenkte.

En av flere praktiske utfordringer lå bl.a. i å få oversatt de arabiske tekstene som lå på nettet – å finne en tolk man kunne stole på og involvere i oversettelsesarbeidet, uten at man risikerte at informasjonen ble gitt videre til uvedkommende. Det var vesentlig at verken ingeniøren eller media skulle få nyss om saken og arbeidet, da man stod overfor en potensiell straffesak. Need-to-know-prinsippet var gjeldende og tolken fikk ikke vite mer enn absolutt nødvendig.

Etter funn av en manual for ukonvensjonell bruk av håndholdt bakke til bakke-våpen ble politiet varslet. Det var enighet om at selskapet kun fokuserte på det arbeidsrettslige, mens politiet fokuserte på det strafferettslige.

Vedkommende ble suspendert av selskapet, og samtidig med dette pågrepet av PST, som siktet vedkommende for terrorrelatert aktivitet.

Det ble avdekket at vedkommende, som hadde norsk statsborgerskap, tidligere hadde vært offiser i Irak og at det var et hull i hans CV på 6 år. Ingeniøren ble stilt for retten, og i september 2018 ble vedkommende dømt til fengsel i 2,5 år for oppfordring til terror og for opplæring i terrormetoder på internett. Tingretten mente vedkommende opererte på egenhånd i perioden januar 2014 og frem til pågripelsen i mai 2015. (Tiltalte har anket domsbeslutningen, og dommen er således ikke rettskraftig.)

Hva er læringspunktene i denne saken:

Etter hendelsen gikk Aker Solutions igjennom den og identifiserte flere læringspunkter – både hva som var gjort riktig og hva man kunne ha gjort annerledes. De viktigste læringspunktene er følgende:

- Etabler et godt samarbeid og gode relasjoner internt mellom HR-funksjonen og security-funksjonen
- Systematiser arbeidet med personellsikkerhet, og sørg for å ha etablerte rutiner for både rekruttering, under ansettelsesforholdet og ved avvikling av arbeidsforhold.
- Gransk søkeres CV-er nøye og sørg for å sjekke opp eventuelle hull i vedkommendes CV-en
- Etterrettelighet er viktig i granskningen – lag en detaljert logg som tydelig angir hvem, hva og når
- Granskning av denne typen er ressurskrevende – tar tid og kan være langvarig, sørg for å stille til disposisjon tilstrekkelig ressurser og de riktige ressursene
- Sørg for et tett samarbeid med politiet/PST – sett av tilstrekkelig tid
- Sørg for jevnlig statusoppdatering med sentrale beslutningstakere i egen organisasjon
- Involver personer bare etter need-to-know-prinsippet – jo færre som kjenner til saken, desto mindre sannsynlighet for at informasjon lekker ut

Hendelsen fikk stor oppmerksomhet i media, spesielt i Norge, men også utenlandske media omtalte saken. Utvalgte linker til media som beskriver saken:

- E24, 11.5.2015: https://e24.no/boers-og-finans/aker-solutions/aker-solutions-ansatt-i-40-aarene-paagrepet-av-pst-og-terrorsiktet/23450588
- News in English, 11.5.2015: https://www.newsinenglish.no/2015/05/11/terror-suspect-detained-at-aker/
- DN, 12.5.2015: https://www.dn.no/terror/aker-solutions/terrorsiktet-aker-solutions-ansatt-fremstilles-for-varetekt/1-1-5376093
- TU, 13.5.2015: https://www.tu.no/artikler/terrorsiktet-ingenior-tilhorte-cia-stottet-gruppe/223521
- VG, 24.8.2016: https://www.vg.no/nyheter/innenriks/i/WrpwG/pst-om-terrorsiktet-aker-solutions-ingenioer-lagde-manual-for-bruk-av-rakettvaapen
- NRK 31.8.2018: https://www.nrk.no/norge/terrortiltalt-ingenior-erkjenner-ikke-straffskyld-1.14186746
- VG, 24.9.2018: https://www.vg.no/nyheter/innenriks/i/3jbwv9/tidligere-aker-solutions-ingenioer-51-doemt-for-terror
- MarketScreener, 24.9.2018: https://www.marketscreener.com/AKER-SOLUTIONS-18088137/news/Aker-Norway-convicts-man-of-providing-terror-attack-instructions-27307158/

7 MODENHETSUNDERSØKELSE

Det er i prosjektet utarbeidet et enkelt verktøy for å vurdere egen modenhet mht. å håndtere innsiderisiko. Verktøyet består i at virksomheten selv gir seg score på en skala fra 1 (dårligst) til 4 (best) for hvert av de foreslåtte tiltakene angitt i kapitlene 5.3 til 5.6. Resultatet (beregnet i prosent av maksimalt mulig oppnåelig) angir hvor moden organisasjonen er – hvor langt man har kommet i arbeidet med å håndtere innsidetrusselen.

Verktøyet er presentert mer i detalj i Appendix C. I tillegg finnes verktøyet i Excel som kan benyttes til å legge inn score direkte. Excel-dokumentet kan fås ved henvendelse til Petroleumstilsynet, eller lastes ned fra tilsynets nettsted.

Egenvurdering score gis etter følgende skala:

- *Score 4:* Tiltaket er fullt ut implementert og fungerer iht. intensjonen
- *Score 3:* Tiltaket er implementert, det fungerer relativt tilfredsstillende, men det er fortsatt enkelte forbedringsbehov for å oppnå optimal effekt
- *Score 2:* Tiltaket er nylig eller delvis implementert, det fungerer ikke tilfredsstillende
- *Score 1:* Tiltaket er ikke implementert

Score på egenvurderingen summeres og %-andel oppnåelse regnes ut. Maksimalt oppnåelig score er 180. Samlet modenhetsresultat er som følger:

0 – 30 %	31 – 50 %	51 – 80 %	81 – 100 %
Meget utsatt: Organisasjonen er i startfasen. Svært få tiltak er implementert, og organisasjonen er svært sårbar overfor innsidetrusler.	**I læringsfasen**: Organisasjonen har «kommet ut av startgropen» og har implementert en del tiltak. Det er imidlertid langt igjen og organisasjonen er fortsatt ikke spesielt godt rustet for å møte innsidetrusselen.	**I god flyt**: Organisasjonen er godt i gang med å implementere tiltak, selv om noe gjenstår. Organisasjonen begynner å bli godt rustet for å håndtere innsidetrusselen, men det er fortsatt en god vei å gå.	**Meget moden**: Organisasjonen er meget moden og godt rustet for å møte innsidetrusselen. Majoriteten av anbefalte tiltak er implementert og fungerer iht. hensikten.

8 REFERANSER

Lover, forskrifter, standarder og avtaler:

/1/ *Lov om nasjonal sikkerhet (sikkerhetsloven)*. LOV 2018-06-01-24. Ikrafttredelse 01.01.2019

/2/ *Forskrift om virksomheters arbeid med forebyggende sikkerhet (virksomhetsikkerhetsforskriften)*. FOR 2018-12-20-2053. Ikrafttredelse 01.01.2019

/3/ *Lov om behandling av personopplysninger (personopplysningsloven)* LOV-2018-06-15-38. Sist endret 11.2.2019

/4/ *Lov om arbeidsmiljø, arbeidstid og stillingsvern mv. (arbeidsmiljøloven)* LOV-2005-06-17-62. Ikrafttredelse 1.1.2006

/5/ *Lov om likestilling og forbud mot diskriminering (likestillings- og diskrimineringsloven)*. LOV-2017-06-16-51. Ikrafttredelse 01.01.2018

/6/ *Forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale*. FOR-2018-07-02-1108. Ikrafttredelse 20.07.2018

/7/ *Forskrift om kameraovervåking i virksomheter*. FOR-2018-07-02-1107. Ikrafttredelse 20.07.2018.

/8/ *NS 5831:2014 Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Krav til sikringsrisikostyring*

/9/ *NS 5832:2014 Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Krav til sikringsrisikoanalyse*

/10/ *Hovedavtalen LO-NHO 2018-2021.* Utgitt av LO 2018

/11/ *NS-ISO 31000:2018 Risikostyring – Retningslinjer*. Utgitt 01.04.2018

/12/ *ISO 22300:2018 Security and resilience – Vocabulary* (2018)

/13/ *NS-EN ISO/IEC 27001:2017: Informasjonsteknologi - Sikringsteknikker - Ledelsessystemer for informasjonssikkerhet - Krav (ISO/IEC 27001:2013 innbefattet Cor 1:2014 og Cor 2:2015).* Publisert 01.05.2017

Veiledere, retningslinjer andre rapporter – Norske forfattere:

/14/ *Barrierenotat 2017 – Prinsipper for barrierestyring i petroleumsvirksomheten*. Utgitt av Petroleumstilsynet 15.03.2017.

/15/ *Sikkerhetsstyring – Veileder*. Utgitt av NSM mars 2015 https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/veileder-i-sikkerhetsstyring--endelig.pdf

/16/ *Risikovurdering for sikring – Håndbok*. Utgitt av NSM mars 2016 https://www.nsm.stat.no/publikasjoner/rad-og-anbefalinger/risikovurdering-handbok/

/17/ *Sikkerhetsfaglig råd*. Nasjonal sikkerhetsmyndighet (NSM). Publisert 11.05.2016 https://www.nsm.stat.no/globalassets/rapporter/nsm-sikkerhetsfaglig_raad_2015_web.pdf

/18/ *Håndbok i autorisasjon og autorisasjonssamtaler*. Nasjonal sikkerhetsmyndighet (NSM). Publisert april 2011 https://www.nsm.stat.no/globalassets/dokumenter/handboker/2011---handbok-i-autorisasjon-og-autorisasjonssamtale.pdf

/19/ *Sikkerhet ved ansettelsesforhold – før, under og ved avvikling.* Politiets sikkerhetstjeneste, Nasjonal sikkerhetsmyndighet (NSM), Politiet og Næringslivets Sikkerhetsråd (NSR). Mai 2017 https://www.nsm.stat.no/aktuelt/ny-veileder-om-innsideproblematikk/

/20/ *Veileder i sikkerhetsstyring.* Veileder til ny Sikkerhetslov. NSM, utgitt august 2019 *https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/2019/veileder-i-sikkerhetsstyring.pdf*

/21/ *Veileder i personellsikkerhet.* Veileder til ny Sikkerhetslov. NSM, utgitt august 2019 *https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/2019/veileder-i-personellsikkerhet.pdf*

/22/ *Veileder i fysisk sikkerhet.* Veileder til ny Sikkerhetslov. NSM, utgitt august 2019 *https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/2019/veileder-i-fysisk-sikkerhet.pdf*

/23/ *Veileder i håndtering og beskyttelse av sikkerhetsgradert informasjon.* Veileder til ny Sikkerhetslov. NSM, utgitt august 2019 https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/2019/veileder-i-handtering-og-beskyttelse-av-sikkerhetsgradert-informasjon.pdf

/24/ *Veileder for virksomheters håndtering av uønskede hendelser.* Veileder til ny Sikkerhetslov. NSM, utgitt august 2019 https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/2019/veileder-for-virksomheters-handtering-av-uonskede-hendelser.pdf

/25/ *Risiko 2018 – Verdifulle individer, verdifulle virksomheter, verdifull infrastruktur*. Nasjonal sikkerhetsmyndighet (NSM) 2018 https://www.nsm.stat.no/publikasjoner/rapporter/rapport-om-sikkerhetstilstanden/

/26/ *Risiko 2019 – Krafttak for et sikrere Norge*. Nasjonal sikkerhetsmyndighet (NSM) 2019 https://www.nsm.stat.no/publikasjoner/rapporter/rapport-om-sikkerhetstilstanden/

/27/ *Mørketallsundersøkelsen 2018*. Næringslivets Sikkerhetsråd (NSR) 2019 https://www.nsr-org.no/moerketall/

/28/ *Kriminalitets- og sikkerhetsundersøkelsen i Norge (KRISINO) 2017*. Næringslivets Sikkerhetsråd (NSR) https://www.nsr-org.no/krisino/

/29/ *Juks med CV.* Næringslivets Sikkerhetsråd (NSR). https://www.nsr-org.no/aktuelle-saker/1-av-5-jobbsokere-article316-110.html.

/30/ *Kameraovervåking – hva er lov?* Veileder fra Datatilsynet. Utgitt juli 2018. https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/kameraovervaking/

/31/ *Kameraovervåking – Spørsmål og svar.* Datatilsynet. https://www.datatilsynet.no/regelverk-og-verktoy/verktoy/sporsmal-svar/kameraovervaaking/

/32/ *Personvern på arbeidsplassen.* Veileder fra Datatilsynet. Utgitt juli 2018. *https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/personvern-pa-arbeidsplassen/*

/33/ *Innsyn i ansattes e-post og private filer*. Informasjonsside. Datatilsynet. https://www.datatilsynet.no/personvern-pa-ulike-omrader/personvern-pa-arbeidsplassen/innsyn-epost-filer/

/34/ *Trusselvurdering 2019*. Politiets sikkerhetstjeneste (PST) 2019 https://www.pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2019/

/35/ *Fokus 2019. Etterretningstjenestens vurdering av aktuelle sikkerhetsutforinger*. E-tjenesten 2019. https://forsvaret.no/fakta_/ForsvaretDocuments/fokus2019_web.pdf

/36/ *104 – Norwegian Oil and Gas recommended guidelines on information security baseline requirements for process control, safety and support ICT systems*. Norsk olje & gass. Rev. 06, 05.12.2016 https://norog.no/contentassets/15263fd7f781409286f319bbeb427d93/104-recommended-guidelines-on-security-baseline-requirements2.pdf

/37/ *091 – Anbefalte retningslinjer for Sikring av forsyninger og materiell i olje- og gassindustrien*. Norsk olje og gass, Rev. 03, 1.9.2015 https://www.norskoljeoggass.no/arbeidsliv/retningslinjer/helse-arbeidsmiljo-og-sikkerhet/sikring/091-anbefalte-retningslinjer-for-sikring-av-forsyninger-og-materiell-i-olje--og-gassindustrien/

/38/ *Personnel security – a Guideline*. DNV GL report no. 2009-1032, rev. 0. 03.06.2009

/39/ *Bruk av sikkerhetssamtalen som metode ved et utvalg klareringsmyndigheter.* Rune Melby, Politihøgskolen, Master i politivitenskap 2016 https://phs.brage.unit.no/phs-xmlui/bitstream/handle/11250/2428109/Master_Melby_2016.pdf?sequence=1&isAllowed=y

/40/ *The Norwegian Downsizing Approach in Terms of the Insider Threat – An interpretive study*. Terje Benjaminsen. Master Thesis in Information Security. NTNU, juni 2017 https://www.nsr-org.no/getfile.php/139955-1511872396/Dokumenter/Eksterne%20publikasjoner/master_terje_benjaminsen.pdf

/41/ *Forebygging, avdekking og håndtering av misligheter.* Masteroppgave i økonomi og administrasjon, av Stein-Ove Jørgensen, august 2015 https://munin.uit.no/bitstream/handle/10037/8234/thesis.pdf?sequence=2

/42/ *The Conceptual and Scientific Demarcation of Security in Contrast to Safety.* S.H. Jore, 2017.

/43/ *Operatørselskapene i petroleumssektoren sitt syn på sikringskultur.* Masteroppgave i Samfunnssikkerhet. Institutt for medie-, kultur- og samfunnsfag. Universitetet i Stavanger. Caroline Østensjø & Caroline Irwin Larsen. Våren 2015 https://core.ac.uk/download/pdf/52118063.pdf

Veiledere, retningslinjer og andre rapporter – Utenlandske:

/44/ *Insider Data Collection Study – Report of main Findings*. Centre for the Protection of National Infrastructure (CNPI). April 2013 https://www.cpni.gov.uk/system/files/documents/63/29/insider-data-collection-study-report-of-main-findings.pdf

/45/ *Personnel Security Risk Assessment – A Guide*. Centre for the Protection of National Infrastructure (CNPI). 4th Edition, June 2013 https://www.cpni.gov.uk/system/files/documents/46/06/Personnel-security-risk-assessment-a-guide-4th-edition.pdf

/46/ *Personnel security and contractors – A good practice guide for employers*. Centre for the Protection of National Infrastructure (CNPI). July 2014 https://www.cpni.gov.uk/system/files/documents/51/4a/personnel-security-and-contractors.pdf

/47/ *Managing the Insider Threat to Your Business – A personnel security handbook*. Australian Government. 2014 https://www.tisn.gov.au/Documents/InsiderThreatBooklet-ManagingTheInsiderThreatToYourBusiness.pdf

/48/ *Protective Security Policy Framework – Personnel Security. PERSEC 12 Eligibility and suitability of personnel.* v2018.0. Australian Government https://www.protectivesecurity.gov.au/personnel/

/49/ *Protective Security Policy Framework – Personnel Security PERSEC 13 Ongoing assessment of personnel.* v2018.1. Australian Government https://www.protectivesecurity.gov.au/personnel/

/50/ *Protective Security Policy Framework – Personnel Security PERSEC 14 Separating personnel.* v2018.0. Australian Government https://www.protectivesecurity.gov.au/personnel/

/51/ *The Insider Threat to Business – A personnel security handbook*. Australian Government. 2010

/52/ *Introduction to Personnel Security – Student Guide*. Center for Development of Security Excellence, Maryland – USA, August 2017 https://www.cdse.edu/documents/student-guides/introduction-to-personnel-security.pdf

/53/ *Tackling the Insider Threat*. CRISP (Connecting Research in Security to Practice) Report. ASIS Foundation. Nick Catrantzos, CPP. 2010. https://popcenter.asu.edu/sites/default/files/library/crisp/insider-threat.pdf

/54/ *Best Practices: Mitigating Insider Threats. The Security Architecture And Operations Playbook.* Joseph Blankenship and Claire O'Malley. Forrester, November 2, 2017. https://pages.observeit.com/rs/248-SYG-803/images/Forrester_Report_Best_Practices_Mitigating_Insider_Threats.pdf

/55/ *Pre-employment-screening-A-good-practice-guide.* Centre for the Protection of National Infrastructure (CNPI). 5th edition, January 2015
https://www.cpni.gov.uk/pre-employment-screening
https://www.cpni.gov.uk/system/files/documents/61/e9/pre-employment-screening-A-good-practice-guide-edition-5.pdf

/56/ *Reducing Insider Risk*. Centre for the Protection of National Infrastructure (CNPI).
https://www.cpni.gov.uk/reducing-insider-risk

/57/ *Preventive and Protective Measures against Insider Threats – Implementing Guide*. IAEA Nuclear Security Series No. 8, 2008
https://www-pub.iaea.org/MTCD/publications/PDF/Pub1359_web.pdf

/58/ *The Insider Threat – an introduction to detecting and deterring an insider spy.* US Department of Justice, FBI. Udatert https://www.fbi.gov/file-repository/insider_threat_brochure.pdf

/59/ *Insider Threat Guide – A Compendium of Best Practices to Accompany the National Insider Threat Minimum Standards.* National Insider Threat Task Force, 2017.
https://www.dni.gov/files/NCSC/documents/nittf/NITTF-Insider-Threat-Guide-2017.pdf

/60/ *Common Sense Guide to mitigating Insider Threats - 5th Edition.* Carnegie Mellon University – Software Engineering Institute. Report CMU/SEI-2015-TR-010. December 2016
https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484758.pdf

/61/ *Common Sense Guide to mitigating Insider Threats - 6th Edition.* Carnegie Mellon University – Software Engineering Institute. Report CMU/SEI-2018-TR-010. December 2018
https://resources.sei.cmu.edu/asset_files/TechnicalReport/2019_005_001_540647.pdf

/62/ *The insider threat to information systems and the effectiveness of ISO17799.* Theoharidou, Kokolakis, Karyda, Kiountouzis. Computers & Security 2005, 24(6), 472 – 484
https://www.sciencedirect.com/science/article/pii/S0167404805000684

/63/ *An Insider Threat Indicator Ontology*. Costa, Albrethsen, Collins, Perl, Silowash, Spooner. May 2016. Report CMU/SEI-2016-TR-007.
https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_454627.pdf

/64/ *Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes*. Posey et al. Computers & Security, 30(6–7), 486 – 497 (2011). https://www.sciencedirect.com/science/article/pii/S0167404811000630

/65/ *Guidelines 3/2019 on processing of personal data through video devices*. Veileder utgitt av European Data Protection Board, vedtatt 10.07.2019
https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf

/66/ *The Insider Threat – Safeguarding UPSI.* Utgitt av KPMG og ASSOCHAM 2019
https://assets.kpmg/content/dam/kpmg/in/pdf/2018/03/Safeguarding-UPSI.PDF

/67/ *Insider threat study: Computer system sabotage in critical infrastructure sectors.* Keeney, Kowalski, Cappelli, Moore, Shimeall & Rogers. U.S. Secret Service and CERT/SEI, 2005*:*
https://resources.sei.cmu.edu/asset_files/SpecialReport/2005_003_001_51946

/68/ *The insider problem revisited*. Bishop (2005). Proceedings of the 2005 Workshop on New Security Paradigms, NSPW '05, 75–76. http://doi.acm.org/10.1145/1146269.1146287,doi:10.1145/1146269.1146287

/69/ *Defining the insider threat*. Bishop & Gates (2008). Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research: Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead, CSIIRW '08, 15:1–15:3. https://pdfs.semanticscholar.org/cff4/586ee9d6651f2d5a6136c1334ad24940aa5a.pdf

/70/ *Towards a theory of insider threat assessment*. Chinchani, Iyer, Ngo, & Upadhyaya (June 2005).2005 International Conference on Dependable Systems and Networks https://cse.buffalo.edu/~hungngo/papers/dsn05.pdf

/71/ *Identifying at-risk employees: Modeling psychosocial precursors of potential insider threats.* Greitzer et al (Jan 2012). In 2012 45th Hawaii International Conference on System Sciences, 2392–2401 https://www.researchgate.net/profile/Frank_Greitzer/publication/261527163_Identifying_At-Risk_Employees_Modeling_Psychosocial_Precursors_of_Potential_Insider_Threats/links/5aafd1afa6fdcc1bc0bd08b1/Identifying-At-Risk-Employees-Modeling-Psychosocial-Precursors-of-Potential-Insider-Threats.pdf?origin=publication_detail

/72/ *Insider threat – 2018 Report.* Crowd Research Partners, 2018. *https://crowdresearchpartners.com/portfolio/insider-threat-report/*

/73/ *Insider Threat – Oil & Gas*. Presentasjon, Ernst & Young LLP, 28.02.2017

/74/ *Managing Insider Threat.* Ernst & Young LLP. 2016 https://www.ey.com/Publication/vwLUAssets/EY-managing-inside-threat/$FILE/EY-managing-inside-threat.pdf

/75/ *Insider Threat Detection Study*. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). 2015 https://ccdcoe.org/uploads/2018/10/Insider_Threat_Study_CCDCOE.pdf

/76/ *Detecting Insider Behavior on Corporate Systems – D3.1 Short Report on Findings from Case Studies*. Whittey & Wright, University of Leicester. 01.08.2013

APPENDIX A
Bidragsytere

Virksomhetene som deltok på workshopen 5. mars, og som bidro gjennom dybdeintervjuer:

Deltakere på workshopen 5. mars (totalt 36 personer):

AkerBP	2 personer
Conoco Philips	2 personer
Equinor	4 personer
Faroe Petroleum	1 person
Gassco	2 personer
Lundin	2 personer
Maersk Drilling	1 person
Neptune Energy	1 person
Norske Shell	1 person
Oceaneering	1 person
Repsol	1 person
Spirit Energy	1 person
Total E&P Norge	1 person
Vår Energi	2 person
Wintershall	1 person
NSM	2 personer
PST	1 person
Ptil	8 personer
DNV GL (fasilitator)	2 personer

Selskap som bidro gjennom dybdeintervjuer:

Conoco Philips

Lundin

Maersk Drilling

Norske Shell

Aker ASA

Statkraft

APPENDIX B
Tilbakemelding fra petroleumsnæringen

Dette vedlegget oppsummerer funnene og informasjonen som fremkom gjennom workshopen som ble holdt 5. mars 2019, og de etterfølgende dybdeintervjuene.

B.1: Generelt

Truslene: Majoriteten av selskapene oppgir at den største trusselen knyttet til innsiderisiko er knyttet til tap av sensitiv informasjon. I tillegg nevnes forhold som korrupsjon, bedrageri og svindel, og konkurranseforhold/kartellvirksomhet (anti trust). Bare i mindre grad nevnes andre fysiske trusseltyper som terror, angrep på personer, skade på anlegg, tyveri, osv. Bekymring rundt dataangrep ble naturlig nok nevnt av flere, men primært knyttet til eksterne aktører, dvs. ikke typisk som innsideproblematikk.

Case: Et selskap oppgir at informasjon om ansattes lønn er klassifisert som en av de mest sensitive informasjonene. I enkelte utsatte land ansees selskapets ansatte å tjene meget bra i forhold til lokalt ansatte, og dersom denne informasjon blir kjent blant kriminelle grupper vil familiemedlemmer til den ansatte kunne bli utsatt for kidnapping med tilhørende krav om løsepenger.

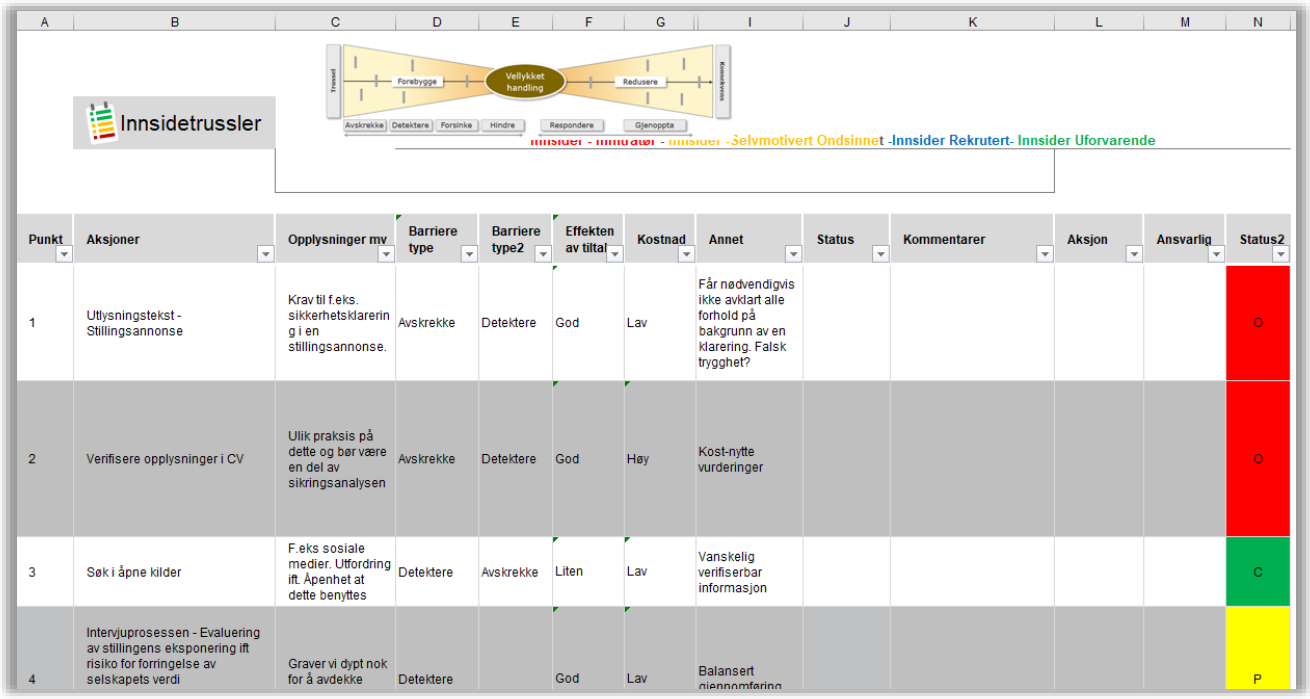
Eksempler på sensitiv informasjon er kontraktsopplysninger, anbudsdokumenter i forbindelse med større prosjekter, finansiell informasjon før offentliggjøring av kvartals- eller årsrapporter (lekkasjer kan påvirke selskapets aksjekurs), oppkjøpsplaner, seismikk og geologidata m.m.

I forbindelse med anbudsrunder ble spesielt fare for lekkasje av sensitiv informasjon i forkant av f.eks. andre runde. Lekkasjer kan være knyttet til bevisst lekkasje (f.eks. på grunn av personlig vennskap) eller ubevisst lekkasje som omtale av informasjon med en kollega der en tredjepart fanger opp informasjonen.

Ansvar er plassert i flere organisatoriske enheter: Det er flere organisatoriske enheter som på en eller annen måte har betydning i innsideproblematikken – linjen, HR, juridisk og security. I tillegg er det en kontinuerlig avveining i forhold til åpenhet for å sikre erfaringsoverføring og effektiv bruk av ressurser på den ene siden, og det å sikre at sensitiv informasjon ikke kommer på avveie eller blir brukt på en ikke tilsiktet måte. Disse problemstillingene er illustrert i Figur 5-4, i kap. 5.3.2. Hovedfokus mht. å vurdere kandidater for stillinger i selskapet kan variere avhengig av hvor i selskapets organisasjon man er. Det vil hele tiden være en balanse mellom det å finne beste kandidat, men samtidig unngå å ansette en som kan utgjøre en innsidetrussel.

Risikovurdering: Gjennomføring av sikringsrisikovurderinger er vanlig praksis, og da med utgangspunkt i trefaktormodellen (trussel, verdi, sårbarhet) slik den er beskrevet i bl.a. NS 5832 (ref. /9/). For å vurdere trussel, legges normalt de offentlig tilgjengelige vurderingene fra PST, NSM og E-tjenesten til grunn. Omfanget av trusselbeskrivelsen internt i virksomhetene kan variere – det er også eksempler på temmelig omfattende og grundige beskrivelser av truslene.

I figuren nedenfor vises for øvrige et eksempel på hvordan et av selskapene hadde laget et enkelt og praktisk verktøy for å sammenfatte hvilke aksjoner man hadde identifisert for å forebygge en innsidetrussel – med kortbeskrivelse av barrieretype, kostnader, og status på implementering av de identifiserte aksjoner.



Punkt	Aksjoner	Opplysninger mv	Barriere type	Barriere type2	Effekten av tiltak	Kostnad	Annet	Status	Kommentarer	Aksjon	Ansvarlig	Status2
1	Utlysningstekst - Stillingsannonse	Krav til f.eks. sikkerhetsklarering i en stillingsannonse.	Avskrekke	Detektere	God	Lav	Får nødvendigvis ikke avklart alle forhold på bakgrunn av en klarering. Falsk trygghet?					O
2	Verifisere opplysninger i CV	Ulik praksis på dette og bør være en del av sikringsanalysen	Avskrekke	Detektere	God	Høy	Kost-nytte vurderinger					O
3	Søk i åpne kilder	F.eks sosiale medier. Utfordring ift. Åpenhet at dette benyttes	Detektere	Avskrekke	Liten	Lav	Vanskelig verifiserbar informasjon					C
4	Intervjuprosessen - Evaluering av stillingens eksponering ift risiko for forringelse av selskapets verdi	Graver vi dypt nok for å avdekke	Detektere		God	Lav	Balansert gjennomføring					P

Figur 8-1: Enkelt og praktisk verktøy å følge opp status på identifiserte tiltak/aksjoner knyttet til ansettelse (eksempel fra et selskap)

Ansettelser: I utgangspunktet har selskapene stort sett tatt inn over seg sikkerhetsmyndighetenes myndighetenes veileder *Sikkerhet ved ansettelsesforhold* (ref. /19/) i sitt arbeid ifm. ansettelser. Det generelle inntrykket er at selskapene har størst fokus på, og gjør mest, i forhold til fasen før ansettelse, og ved avslutning av arbeidsforholdet. Den største utfordringen ligger i mellomfasen – under selve ansettelsesforholdet. Dette skyldes i stor grad at det er vanskelig å avdekke en innsider når vedkommende allerede har kommer inn i organisasjonen. Det ble også uttalt at muligens er selskapene mer reaktive enn proaktive – det er lettere å ta tak i aktuelle hendelser. Det er noe varierende mht. i hvilken grad det gjøres systematisk bakgrunnssjekk av kandidater til stillinger i selskapet. For noen selskap gjøres det en vurdering av hvilken stillingskategori eller funksjons vedkommende skal ha og dette avgjør hvorvidt det gjennomføres en bakgrunnssjekk eller ikke.

Bevisstheten bedret seg: Det er en gjennomgående oppfatning at bevisstheten rundt innsiderisiko og tilhørende sikringstiltak har bedret seg de senere årene, mye takket være åpenhet og omtale i mediene og myndighetenes fokus på tematikken.

Klassifisering av dokumentasjon – begrepsbruk. Det er ingen enhetlig begrepsbruk mht. klassifiseringen. Ofte brukes begreper / inndeling som Open eller Public, Internal, Restricted, Confidential, Secret eller liknende. Et selskap har nevnt at de har bevisst valgt å bare ha to nivåer – *Intern* og *Sensitiv*, dvs. sløyfet *Åpen*, *Konfidensiell* og *Hemmelig*. «Åpen» brukes ikke da man ikke anser dette får å være en klassifiseringsgrad. Videre unngås begrepet *Konfidensiell* for å ikke forveksle med

begrepene og tilhørende krav som ligger i Sikkerhetsloven (se lovens §5-3). Bl.a. sier Sikkerhetsloven at personer som skal ha tilgang til informasjon gradert Konfidensielt skal være sikkerhetsklarert.

Status på barrierer/tiltak: Den generelle oppfatning er selskapene er best på *tekniske* tiltak, og noe mindre god på *organisatoriske* og *menneskelige* tiltak, for å håndtere innsidetrusselen. Dette vil også omfatte bevissthet rundt det å håndtere informasjon på offentlig sted – lese dokumenter på reiser, snakke i telefon om sensitiv informasjon der flere er tilstede, legge igjen telefon på utsiden av møterom osv.

Konsernkrav i strid med norsk lovkrav: For noen selskaper hvor konsernet er lokalisert i utlandet har det det dukket opp et spørsmål om det kan det finnes konsernkrav som strider mot norsk lov. Et tenkt eksempel kan være at konsernet har visse interne regler og krav om at dersom man bryter en eller flere av disse kan dette medføre oppsigelse. Et slikt krav kan føre til et problem da norsk lov krever at det skal være en saklig grunn for å bli sagt opp. På den annen side, blant de involverte selskapene var dette pr. dags dato ikke et problem knyttet til innsiderisiko.

Målinger: Det gjennomføres forskjellige typer målinger som kan ha relevans for innsiderisikoen, som f.eks. IT avdelingen sender ut test-phishing mail til ansatte, registrering og rapportering av forskjellige typer sikringshendelser, gjennom arbeidsmiljøundersøkelser, medarbeidersamtaler, varslingssaker, IT-deteksjonssystemer (eks. kontinuerlig sjekk om nedlasting av store mengder filer), adgangskontroll (gis beskjed hvis uregelmessigheter, eks. unormal arbeidstid). Det er imidlertid indikasjoner på at disse målingene ikke blir gjennomført og i tilstrekkelig grad brukt på en systematisk måte mht. å fange opp innsiderisikoen.

B.2: Før ansettelse eller kontraktsinngåelse

Falske CV-er: Det er en kjent problemstilling at det jukses med CV-er. I en artikkel fra 2013 på nettstedet til NSR (ref. /29/) omtales at 1 av 5 jukser med CV-en. Der henvises også til en undersøkelse fra 2012 gjort av et konsulentselskap (Semac) at det var kritikkverdige forhold hos hele 40 % av 1120 kontrollerte jobbsøkere. Et annet selskap (Meditor Search) utfører også bakgrunnssjekk av jobbsøkere på vegne av kunder, og de opplyser at de finner feil i én av fire CV-er, og dette tallet har holdt seg stabilt over flere år. I følge NSR er det kun 26 % av norske selskap som sjekker bakgrunnen og identiteten til dem de ansetter. Jobbsøkere som jukser seg inn ved forfalskning av CV har ikke nødvendigvis kriminelle hensikter – status, karrieremuligheter og høyere lønn kan være nok til at noen ønsker å benytte juks som virkemiddel for å nå sine mål, dette finnes det dessverre flere eksempler på i Norge. Man må likevel kunne anta at en person som har til hensikt å infiltrere et selskap på vegne av en større organisasjon eller fremmed stat, har et tilstrekkelig ressurssterkt apparat i ryggen som vil kunne etablere en historikk og CV som gjør det vanskelig å oppdage at dette ikke er ekte.

Selskapene erkjenner at gjennomføring av CV-sjekk i stor grad vil kunne avdekke «amatørene», men ikke profesjonelle aktører.

Bakgrunnssjekk og ID-sjekk av nyansatte: I følge NSR- KRISINO 2017 (ref. /28/) utfører 3 av 4 bedrifter i privat sektor en bakgrunnssjekk av kandidater, men bare 1 av 4 gjennomfører en

ekthetskontroll av vitnemålet. Dog gjøres det søk etter opplysninger på internett i drøyt halvparten av ansettelsene. Videre er det under 4 av 10 som gjennomfører en ID-sjekk ved ansettelse. Alle disse fire kontrolltiltakene gjøres i større grad i offentlig enn i privat sektor. Dog er det viktig å påpeke at dette er tall fra et bredt spekter av næringer, og er ikke nødvendigvis ment å gjenspeile petroleumsindustrien.

Et selskap forklarte at man utfører analyser av søkerens personlighet, men opplyste at dette ikke er lov i f.eks. USA slik at der gjøres det ikke. Videre ble det også nevnt at ikke nødvendigvis alle kandidater blir id-sjekket i forkant av en eventuell ansettelse.

Ekstra sjekk av personer fra utvalgte land: I PSTs åpne trusselvurdering fra 2019 har det vært nevnt at trusselen mht. spionasje er størst fra enkelte navngitte land.

Et av selskapene oppga, med PSTs trusselvurdering som bakgrunn, at man setter krav til at for søkere fra disse navngitte landene, så skal det gjennomføres ekstra sjekker og egen sikkerhetssamtale basert på en egenutviklet samtalemal. I tillegg ble det oppgitt at for søkere fra enkelte land der omfanget av og kulturen for korrupsjon er stor, skal det også iverksettes ekstra vurderinger.

System for sjekk av ansatte: Et av selskapene har laget et strukturert system for krav til vurdering av nyansatte. For alle nyansatte skal det gjennomføres id-sjekk supplert med sjekk opp mot enkelte spørsmål som selskapet selv har utviklet. For alle som skal inn i spesielle lederstillinger skal det i tillegg gjøres en mer omfattende bakgrunnssjekk utført av et eksternt firma som gjør dette profesjonelt. For alle som skal ha tilgang til kritiske systemer skal det i tillegg utføres en utvidet sjekk og intern godkjenning. Dersom det er ansettelse i Sverige eller Tyskland kreves det formell sikkerhetsklarering med hjemmel i nasjonal lovgivning i disse landene. En utfordring er ved outsourcing av enkelte tjenester, f.eks. IT-tjenester til India dersom vedkommende har tilgang til kritiske funksjoner – det kan være vanskelig å kreve og/eller få gjennomført ønsket utvidet sjekk og godkjenning.

B.3: Under ansettelses- eller kontraktsforholdet

Etablering av sikringssoner brukes for å avgrense adgangsmuligheter til forskjellige kritiske områder/soner/rom. F.eks. stilles det strenge krav for å kunne entre serverrom, evalueringsrom, områder der kommersielle og tekniske data o.l. lagres.

Tilgang til datasystemer: Det er normalt styring av tilgang til områder/foldere og/eller på enkeltfiler som ligger på fellesområder (eks. Sharepoint). Det oppleves imidlertid som noe krevende å skulle hele tiden oppdatere tilganger etter hvert som personer enten slutter eller skifter funksjoner i selskapet. Spesielt gjelder dette større organisasjoner. Det opplyses at det ligger mange muligheter til i Office365, flere muligheter mht. å logge/spore, men dette er ikke godt nok kjent og brukt ennå. Tilsvarende er det også slik at for enkelte selskaper er det ikke aktuelt å benytte skytjenester (f.eks. OneDrive i Office 365) for lagring av sensitiv informasjon da dette ikke anses som sikkert nok. Videre kan visse nettsider stenges slik at ansatte ikke kan benytte disse. Det er også forskjell mht. om det er lov å benytte USB port på PC-er. Motargumentet fra IT-ansvarlig kan være at dokumenter uansett kan lastes opp via f.eks. OneDrive.

Disiplin på håndtering av informasjon: Selskapene selv opplever at man har god disiplin på håndtering av sensitiv informasjon (kategorisering av informasjon, etterlevelse av krav, krypteringssystemer etc.), som f.eks. helse/personal opplysninger, kjøp og salg av lisenser, seismiske data etc.

Bevisstgjøring er et tema de fleste selskapene påpeker er viktig og som man kan gjøre mer med for å styrke (se også punktet nedenfor). Clean Desk policy og oppfordring om at skjermen skal låses når man ikke er på plassen sin har de fleste, men implementeringen av dette er et område som kan forbedres hos mange. Enkelte kan lett ha den oppfatningen at «*Vi har ikke informasjon som noen er interessert i*».

Det var gjennomgående at selskapene stort sett legger opp til å håndtere innleide på samme måte som ansatte mht. krav til opplæring, involvering i det daglige arbeid, jobbe for at de opplever at de er en del av selskapets kultur og fellesskap.

Interne bevisstgjøringskampanjer: Flere av selskapene gjennomfører forskjellig former for bevisstgjøringskampanjer, som f.eks. laget videoer (korte «snutter» på 2-4 minutter), nanolearning som distribueres til alle, e-læringskurs (10-20 minutter som alle nyansatte og innleide skal gjennomgå), introduksjonskurs som dekker bl.a. etikk, korrupsjon osv., samt oppfølgingskurs om de samme temaene. Videokampanjene har vært rundt temaer som «Ikke legg fra deg kortet», «Ikke slipp inn folk bak deg uten at de har kort», «Ikke gi bort passordet ditt til noen» osv. I tillegg er sikring temaer på noen medarbeidersamtaler, ukentlige møter mellom leder og ansatt, månedlige en-til-en samtaler osv.

Kritiske temaer diskuteres i sikre områder: Håndtering av informasjon knyttet til anbud på større prosjekter ansees å være kritisk informasjon. Det kan være en stor økonomisk gevinst dersom en leverandør får tak i informasjon om konkurrentenes løsnings- og pristilbud i slike prosjekter. Derfor er det meget viktig at slik informasjon ikke lekker ut til omverdenen f.eks. mellom første og annen runde av prosessen. Også finansiell informasjon før offentliggjøring av kvartals- eller årsrapporter ansees å være kritisk og kan skade selskapet om dette lekker ut, f.eks. ved å påvirke selskapets aksjekurs. Dette er eksempler på informasjon som gjerne behandles i sikre områder der ekstra sikringstiltak kan være innført.

Slike ekstra sikringstiltak kan f.eks. være at området er avsperret for alle andre som ikke har noe direkte med saken å gjøre, området voktes 24/7 i den aktuelle perioden, rengjøringspersonale har ikke adgang eller bare under bevoktning, rommet er sjekket for skjulte mikrofoner, mobiltelefoner legges igjen utenfor rommet, bare godkjente/kontrollerte PC-er kan benyttes, og ingen dokumenter skal tas ut av rommet. I tillegg kan de aktuelle personene som er med i prosessen bli avkrevd at de signerer en erklæring om at informasjon ikke skal formidles til andre.

Lite på papir, mest elektronisk: I de fleste selskapene legger man opp til å skrive ut minst mulig på papir. Dette reduserer muligheten for at sensitive dokumenter/kopier kommer på avveie, enten ved at de gjenglemmes et sted, dokumentmappen stjeles, dokumentene leses på offentlig sted der noen tyvtitter og får med seg essensiell informasjon, osv.

Dokumenter legges gjerne på spesielle området på Sharepoint – enten på selskapets egen Sharepointløsning, eller i skyen som en del av Office 365 pakken. Ved visse tilfeller er noen dokumenter

satt opp slik at de ikke kan åpnes utenfor Sharepoint, som umuliggjør kopiering på en ekstern disk og leses et annet sted.

Avdekke adferd: Generell oppfatning er at det er vanskelig å avdekke endret/unormal adferd og varsle om mistanke hos en kollega, og derfor er terskelen for å si ifra til personen selv eller ledelse. Dette bunner bl.a. i at det er vanskelig å etablere en «baseline» for normal adferd. Dette gjelder både fysisk adferd (person) og datatrafikk/brukeraktivitet (f.eks. nedlasting av store mengder data).

Varsling (Whistleblower): Når unormal/mistenkelig adferd oppdages må det være rom og mulighet («kanaler») for varsling samt aksept hos ledelsen for å gjøre det. Noen selskaper har etablert interne varslingskanaler, andre bruker eksterne kanaler. Det er viktig at denne informasjonen blir håndtert på en slik måte at den ikke misbrukes.

Case: Det ble oppdaget at vaske-hjelpen ved et innleid rengjøringsbyrå hadde tatt bilder med mobiltelefonen av dokumenter og åpne PC-skjermer mens vedkommende gjorde rent. I den videre etterforskningen ble det oppdaget at vaskehjelpen hadde fått betalt av en person som vedkommende leiet rom hos for å utføre handlingen.

Penetrasjonstesting er vanlig å gjennomføre. I et konkret tilfelle kom testeren helt inn til et sentralt/høykritisk område i selskapets datasystemer.

B.4: Ved avslutning av ansettelses- eller kontraktsforholdet

Tilganger: Når en ansatt er under oppsigelse, være seg at vedkommende har sagt opp selv eller har blitt sagt opp (pga. nedskjæringer eller personlige årsaker), bør man vurdere om det er tilrådelig at vedkommende fortsatt skal ha uendret tilgang til soner og eller datasystemer, eller om disse skal helt eller delvis begrenses i oppsigelsesperioden.

Selskapene oppgir at stort sett beholdes tilganger/brukerrettigheter/adgang for ansatte gjennom hele avslutningsfasen (oppsigelsestiden). Bare i enkelte tilfeller ble det oppgitt at vedkommende fikk begrenset tilgangene sine i denne perioden.

Sluttintervju: De aller fleste selskapene har en prosess for å gjennomføre sluttintervju. Derimot blir ikke alltid slike intervjuer avholdt, og det er varierende i hvilken grad informasjon fra sluttintervjuene flyter tilbake til relevant mottaker og behandlet videre. Videre har sluttintervjuene primært til hensikt å avklare andre forhold enn det som er spesifikt relevant for reduksjon av innsiderisiko.

APPENDIX C
Verktøy for modenhetsvurdering

Tabellen under er et enkelt verktøy for å vurdere egen modenhet mht. å håndtere innsiderisiko. Alle tiltakene er løpende nummerert og samsvarer med nummereringen angitt i kapitlene 5.3 til 5.6. For mer utfyllende forklaring til de enkelte punktene, se tilhørende tiltaksnummer i de nevnte delkapitlene i kapittel 5.

Egenvurdering score gis etter følgende skala:

- *Score 4:* Tiltaket er fullt ut implementert og fungerer iht. intensjonen
- *Score 3:* Tiltaket er implementert, det fungerer relativt tilfredsstillende, men det er fortsatt enkelte forbedringsbehov for å oppnå optimal effekt
- *Score 2:* Tiltaket er nylig eller delvis implementert, det fungerer ikke tilfredsstillende
- *Score 1:* Tiltaket er ikke implementert

Score på egenvurderingen summeres og %-andel oppnåelse regnes ut. Maksimalt oppnåelig score er 180. Samlet modenhetsresultat er som følger:

0 – 30 %	31 – 50 %	51 – 80 %	81 – 100 %
Meget utsatt: Organisasjonen er i startfasen. Svært få tiltak er implementert, og organisasjonen er svært sårbar overfor innsidetrusler.	**I læringsfasen**: Organisasjonen har «kommet ut av startgropen» og har implementert en del tiltak. Det er imidlertid langt igjen og organisasjonen er fortsatt ikke spesielt godt rustet for å møte innsidetrusselen.	**I god flyt**: Organisasjonen er godt i gang med å implementere tiltak, selv om noe gjenstår. Organisasjonen begynner å bli godt rustet for å håndtere innsidetrusselen, men det er fortsatt en god vei å gå	**Meget moden**: Organisasjonen er meget moden og godt rustet for å møte innsidetrusselen. Majoriteten av anbefalte tiltak er implementert og fungerer iht. hensikten.

Modenhetsundersøkelse

#	Tiltaksbeskrivelse	Score	Egne kommentarer
Nr. 1: Tiltak i rekrutteringsfasen – Utlysning og ansettelse (kapittel 5.3)			
1	Gjennomfør en stillingsspesifikk risikovurdering		
2	Tydeliggjør i utlysningsteksten at bakgrunnssjekk vil bli gjort		
3	Søk i åpne kilder på nettet		
4	Gjennomfør bakgrunnssjekk		
5	Utfør ID-sjekk ved intervju og ved ansettelsesstart		
Nr. 2: Tiltak under arbeidsforholdet (kapittel 5.4)			
	2.1 Menneskelige tiltak		
6	Obligatorisk introduksjonskurs fokuserer på sikring		
7	Etabler et opplæringsprogram for ledere		
8	Etabler et bevisstgjøringsprogram		
9	Skap en kultur «*Det er lov å bry seg*»		
10	Etabler en varslingskanal		
11	Etabler god dialog internt mellom HR og sikringsenheten		
12	Gjennomfør sikringssamtale regelmessig		
13	Adresser innsiderisiko i medarbeidersamtaler		
14	Regelmessig bekreftelse på forståelse av virksomhetens krav		
15	Sikring settes på agendaen for møter på lik linje med HMS		
16	Bevisstgjør om trusler ved utenlandsreiser og deltakelse på konferanser		
17	Bevisstgjør utenlandske statsborgere om muligheten for verving		
18	Etabler praksis for ikke å omtale/lese sensitiv informasjon i åpne områder		
19	Etabler løpende dialog med stedlig politi		
	2.2 Organisatoriske tiltak		
20	Informasjonspolicy inneholder klassifisering av sensitiv informasjon		
21	Etabler retningslinjer for håndtering av sensitiv informasjon		
22	Krav om Clean Desk og låst PC-skjerm		
23	Gjennomfør ny screening av ansatte ved skifte av arbeidsoppgaver		
	2.3 Teknologiske tiltak		
24	Definer fysiske sikringssoner		
25	Tilpass adgangskontroll basert på definerte sikringssoner		
26	Etabler spesielle kontrolltiltak for særs kritiske soner		
27	Krav om adgangskontroll også offshore for særs kritiske soner		
28	Spesielt gode låsordninger for særs kritiske soner/objekter		
29	Møterom egnet for utveksling av sensitiv informasjon		
30	Etabler regler for tilgangsstyring til intranett og applikasjoner		
31	Restriksjon i tilgang for utvalgte grupper		

#	Tiltaksbeskrivelse	Score	Egne kommentarer
32	Jevnlig opprydding av tilgangsrettigheter		
33	IT-adminpersonell har personlig adminkonto		
34	Arbeidsoperasjoner på høyprioriterte systemer utføres under fire øyne		
35	Elektronisk logg av aktiviteter		
36	Manuelle observasjoner og andre måleaktivteter		
Nr. 3: Tiltak for å håndtere en oppstått situasjon (kapittel 5.5)			
37	Plan for å håndtere en potensiell hendelse		
Nr. 4: Avslutning av arbeidsforholdet (kapittel 5.6)			
38	Ha en god oppsigelsesprosess		
39	Vurder behov for å begrense tilgang til systemer eller områder		
40	Sikre retur av dokumenter som eies av virksomheten		
41	Sikre innlevering av utstyr		
42	Deaktiver tilganger og adganger senest siste arbeidsdag		
43	Gjennomfør sluttintervju		
44	Deaktiver tilgang for kontraktører ved midlertidig opphold i engasjement		
45	Innfør tiltak som hindrer tilgang for personer som har sluttet		
	Samlet score		

Resultat for hele undersøkelsen

Oppnådd score for egen virksomhet	
Maksimalt oppnåelig	180
Oppnådd score i % av maksimalt oppnåelig	_____ %

Delresultat

	1: Rekruttering-fasen	2: Under arbeidsforholdet	3: Håndtere en situasjon	4: Avslutnings-fasen
Oppnådd score				
Maksimalt oppnåelig	20	124	4	32
Oppnådd score i % av maksimalt oppnåelig	_____ %	_____ %	_____ %	_____ %

0 – 30 %	31 – 50 %	51 – 80 %	81 – 100 %
Meget utsatt	I læringsfasen	I god flyt	Meget moden

APPENDIX D
Indikatorer

Dette vedlegget gir en oversikt over deteksjonsindikatorer mht. innsideprofiler sammenfattet i NATOs dokument *Insider Threat Detection Study*, ref. /75/).

- Personal indicators (table 2)
- Behavioral indicators (table 3)
- Background indicators (table 4)
- Network indicators (table 5)

Indicator	Sabotage	Theft	Fraud	Espionage	Unintentional
Depression	High	Low	Low	Medium	High
Financial obligations	Low	High	High	Medium	Low
Address change (moving)	Low	High	High	Medium	Medium
Death among family or friends	Medium	Medium	Low	Medium	High
Feelings of inadequacy	High	Medium	Low	High	Medium
Break-up or divorce	Medium	Low	Low	Medium	High
Impending termination of contract	High	High	Low	Medium	Medium

Table 2: Personal indicators

Indicator	Sabotage	Theft	Fraud	Espionage	Unintentional
Unwillingness to comply with established rules and procedures	High	Medium	Low	Medium	High
Repeated breach of procedures	Medium	High	High	High	High
Excessive or unexplained use of data copy equipment (fax, copy, camera)	Low	High	Low	High	High
Excessive volunteering which would elevate access to sensitive data	Low	High	High	High	Medium
Excessive overtime work	Low	High	High	High	Low
Bringing personal equipment to high-security areas	Low	High	Medium	High	High
Carelessness	Low	Low	Low	Low	High
Concerning statements, jokes, or bragging	Medium	Low	Low	Medium	High
Impulsiveness	Medium	Medium	Low	Low	High
Poor social interaction	High	Medium	Low	Low	Medium
Aggression	High	Medium	Low	Low	Medium

Table 3: Behavioural indicators

Indicator	Sabotage	Theft	Fraud	Espionage	Unintentional
Involvement with individuals or groups who oppose core beliefs of organisation	High	Medium	Medium	High	Medium
Criminal record	Medium	High	High	Medium	Low
Addiction (alcohol, drugs, gambling)	Medium	High	High	Medium	Medium
History of mental or emotional disorder	High	Medium	Low	Medium	Medium
Indebtedness	Low	High	High	Medium	Low
Sexual behaviour which indicates lack of judgement	Low	Medium	Medium	Medium	High
Engagement in activities which can cause a conflict of	Medium	High	High	High	Medium
Business dealings	Low	High	Medium	Medium	Low
Active presence in social media	Low	Low	Low	Low	High
Number of previous employers and average time of employment	High	High	Low	Low	High
Spending exceeds income	Low	High	High	High	Low

Table 4: Background indicators

Indicator	Sabotage	Theft	Fraud	Espionage	Unintentional
Correspondence with competitors	Low	High	High	Medium	Low
E-mail messages with abnormally large amount of data	Low	High	High	High	Low
DNS queries which indicate involvement with internet underground	Medium	High	Low	Medium	Low
Use of suspicious protocols (e.g. IRC)	Low	High	Low	Low	High
Use of suspicious services (e.g. VPN, Tor)	Low	High	Low	Low	Low
Execution of offensive tools	Medium	High	Low	Medium	Low
Execution of malware	Medium	Low	Low	Low	High
Anomalous peaks in outgoing connection count	Medium	High	Low	High	Low
An unauthorised device is connected to the network	Medium	High	Low	High	Medium
Download of blacklisted software	High	Medium	Low	Medium	Medium
Connections initiated from a workstation outside working hours	Medium	High	Low	Medium	High

Table 5: Network Indicators

APPENDIX E
Lovmessige og andre krav

Dette vedlegget oppsummerer de viktigste lovkravene og avtalekrav som regulerer hva en arbeidsgiver har lov til å gjøre, og hva som ikke er lov. Det er imidlertid nødvendig at enhver arbeidsgiver selv gjør en vurdering av hva som gjelder for egen virksomhet.

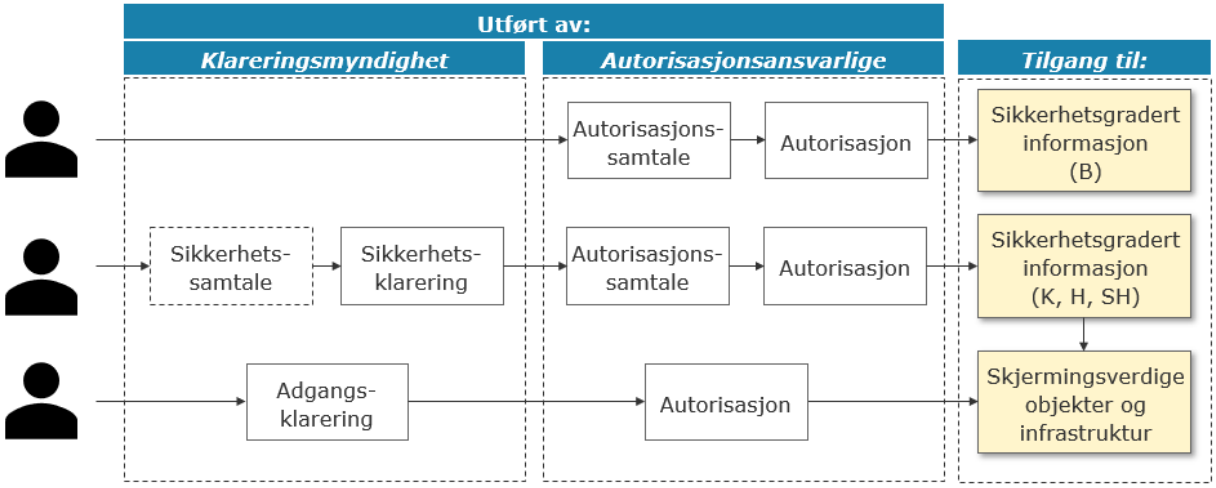
E.1: Sikkerhetsloven

Ny Sikkerhetslov ble utgitt 1.1.2019 (ref. /1/). I utgangspunktet gjelder Sikkerhetsloven for statlige, fylkeskommunale og kommunale organer, samt for leverandører av varer eller tjenester i forbindelse med sikkerhetsgraderte anskaffelser. I tillegg gir lovens § 1-3 departementene anledning til å fatte vedtak om at loven helt eller delvis skal gjelde innen sitt ansvarsområde. Per august 2019 gjelder ikke Sikkerhetsloven for petroleumsnæringen.

Sikkerhetsloven definerer enkelte begreper og setter krav til personer som skal ha tilgang til sikkerhetsgradert informasjon eller til skjermingsverdige objekter og infrastruktur.

I tillegg beskriver *Forskrift om virksomheters arbeid med forebyggende sikkerhet (virksomhetsikkerhets-forskriften)* (ref. /2/) soner og soneinndeling.

Begrepene brukt i Sikkerhetsloven er nyttige å kjenne til for å sikre riktig terminologi i egen virksomhet.



Figur E-1: Illustrasjon av godkjenningsprosessen for en som skal håndtere sikkerhetsgradert informasjon eller få adgang til skjermingsverdige objekter eller infrastruktur. Sikkerhetssamtale (stiplet linje) gjennomføres ved behov

Nedenfor er noen av de mest sentrale begrepene i Sikkerhetsloven forklart.

- *Sikkerhetsgradert informasjon*: Skjermingsverdig informasjon som er gitt beskyttelse i form av en sikkerhetsgrad: *Begrenset (B), Konfidensiell (K), Hemmelig (H) og Strengt hemmelig (SH).* Sikkerhetsgradert informasjon skal bare overlates til personer som har tjenstlig behov og er autorisert. Alle som får tilgang til sikkerhetsgradert informasjon har taushetsplikt om innholdet. Taushetsplikten gjelder også etter at arbeidet eller tjenesten er avsluttet. (Ref. § 5-3 og § 5-4)

- *Skjermingsverdige objekter og infrastruktur*: Objekter og infrastruktur er skjermingsverdige dersom det kan skade grunnleggende nasjonale funksjoner om de får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse. Skjermingsverdige objekter og infrastruktur klassifiseres i: *Meget kritisk*, *Kritisk* eller *Viktig* (ref. § 7-1 og § 7-2). Adgang til skjermingsverdige objekter og infrastruktur krever enten egen adgangsklarering, eller at spesielle sikringstiltak er iverksatt, eller at vedkommende er sikkerhetsklarert for minst *Konfidensiell* informasjon (ref. § 8-1 og § 8-3). I tillegg må vedkommende være autorisert.
- *Soneinndeling*: Virksomheter som har informasjon som er gradert Konfidensiell eller høyere, skal etablere en kontrollert og beskyttet sone for å beskytte den sikkerhetsgraderte informasjonen. Det benyttes tre nivåer på sonene: *Kontrollert sone, Beskyttet sone* og *Sperret sone* (ref. virksomhetsikkerhetsforskriften, §§ 38 – 41).
- *Adgangsklarering*: Personer som skal ha adgang til skjermingsverdige objekter og infrastruktur skal normalt på forhånd være adgangsklarert. En person som er sikkerhetsklarert trenger kun autorisasjon for adgang til skjermingsverdig objekt eller infrastruktur (ref. § 8-3).
- *Sikkerhetsklarering* er en avgjørelse fra klareringsmyndigheten om at en person er sikkerhetsmessig skikket til å kunne håndtere sikkerhetsgradert informasjon gradert til Konfidensiell eller høyere (ref. § 8-2).
- *Sikkerhetssamtale*: Dersom det er tvil om en person er sikkerhetsmessig skikket til å bli sikkerhetsklarert, holder klareringsmyndigheten en sikkerhetssamtale med personen. Dette er en formell samtale som klareringsmyndigheten kan gjennomføre med den som er forespurt sikkerhetsklarert, for eventuelt å fjerne usikkerhet i vurderingen av sikkerhetsmessig skikkethet og om sikkerhetsklarering kan gis (ref. § 8-4).
- *Autorisasjon*: En godkjennelse som enkeltpersoner må ha av sin leder (autorisasjonsansvarlig) for å få tilgang til sikkerhetsgradert informasjon. Personer som skal få tilgang til sikkerhetsgradert informasjon, skal autoriseres. Autorisasjon kommer i tillegg til sikkerhetsklarering (ref. § 8-9).
- *Autorisasjonssamtale*: En formell samtale som avholdes mellom autorisasjonsansvarlig og den som skal autoriseres. Hensikten er å avklare at det ikke foreligger opplysninger som gir rimelig grunn til å tvile på om en person er sikkerhetsmessig skikket, og at leder har nødvendig tillit til den som skal ha tilgang på sikkerhetsgradert informasjon (ref. § 8-9).
- *Klareringsmyndighet* er den myndighet som avgjør om en person kan sikkerhetsklareres eller ikke. Det finnes i hovedsak to klareringsmyndigheter – én for sivile sektorer (Sivil klareringsmyndighet, SKM) og én for forsvarssektoren (Forsvarets sikkerhetsavdeling, FSA). (ref. § 8-16).

For mer info, se også:

- NSMs side med veiledninger knyttet til den nye Sikkerhetsloven av 2019: https://www.nsm.stat.no/aktuelt/veiledere-ny-sikkerhetslov-publisert/
- NSMs side med ord og uttrykk knyttet til Sikkerhetsloven: https://www.nsm.stat.no/om-nsm/tjenester/personellsikkerhet/slik-blir-du-sikkerhetsklarert/ord-og-uttrykk/

E.2: Personvern og arbeidsmiljø

Personvern og hva virksomheten har lov til å gjøre eller ikke gjøre er regulert gjennom forskjellige lover og forskrifter. De viktigste i denne sammenhengen er:

- Lov om behandling av personopplysninger (personopplysningsloven)
- Lov om arbeidsmiljø, arbeidstid og stillingsvern mv. (arbeidsmiljøloven)
- Forskrifter hjemlet i Arbeidsmiljøloven, Datatilsynet er tilsynsmyndighet:
    - Forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale
    - Forskrift om kameraovervåking i virksomhet
- Lov om likestilling og forbud mot diskriminering (likestillings- og diskrimineringsloven)
- Hovedavtalen mellom LO og NHO 2018-2021

Personopplysninger og vern om disse er regulert gjennom *personopplysningsloven*. Loven kom i 2018 og består av nasjonale regler og EUs personvernforordning (GDPR - General Data Protection Regulation). Forordningen er et sett regler som gjelder for alle EU/EØS-land. Loven handler om behandling – altså innsamling og bruk – av personopplysninger. Reglene gir virksomhetene en rekke plikter samtidig som den gir enkeltpersoner en rekke rettigheter. Loven gjelder stort sett alle virksomheter, men det finnes situasjoner der loven ikke gjelder.

Datatilsynet er tilsynsorgan for personopplysningsloven, og ytterligere informasjon finnes på tilsynets nettsted. Blant annet finnes en side som omhandler personvern på arbeidsplassen, der også en veileder med samme tittel finnes i www.datatilsynet.no/personvern-pa-ulike-omrader/personvern-pa-arbeidsplassen/

Kontrolltiltak i virksomheter er primært regulert gjennom *arbeidsmiljøloven,* kapittel 9 – Kontrolltiltak i virksomheten. Ifølge loven kan arbeidsgiver bare iverksette kontrolltiltak overfor arbeidstaker når tiltaket har saklig grunn i virksomhetens forhold og det ikke innebærer en uforholdsmessig belastning for arbeidstakeren. Videre sier lovens § 9-2 at før tiltaket iverksettes skal arbeidsgiver gi de berørte arbeidstakerne informasjon om formålet med kontrolltiltaket, varighet av dette samt informasjon om mulige praktiske konsekvenser av tiltaket. Kontrolltiltaket skal også drøftes med arbeidstakers tillitsvalgte. Arbeidsmiljøloven presiserer at personopplysningsloven gjelder for arbeidsgivers behandling av opplysninger om arbeidstakere i forbindelse med iverksatte kontrolltiltak.

Loven har egne paragrafer knyttet til innføring av kontrolltiltak og drøfting med tillitsvalgte, om helseopplysninger og medisinske undersøkelser, om innsyn i arbeidstakers e-postkasser og annet elektronisk lagret materiale og om kameraovervåking. Det er strenge krav knyttet til innhenting av helseopplysninger ved ansettelse (f.eks. rusmisbruk) og til medisinske undersøkelser (§§ 9-3 og 9-4).

På Arbeidstilsynets nettsted finnes en egen side med praktisk informasjonsside med tittelen «Kontroll og overvåking» www.arbeidstilsynet.no/arbeidsforhold/kontroll-og-overvakning/. På denne siden er det også en veileder «*Veileder om kontroll og overvåking i arbeidslivet*» utgitt i felleskap av Arbeidstilsynet, Datatilsynet, Ptil og partene i arbeidslivet.

Innsyn i e-postkasse og annet elektronisk lagret materiale er nevnt i arbeidsmiljølovens § 9-5, og spesielt regulert gjennom en egen forskrift (*Forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale*).

Temaet er også nærmere omtalt på Datatilsynets nettsted. Kortversjonen av kravene er at en arbeidsgiver kan bare gjøre innsyn i ansattes e-post eller private filer i to tilfeller; det første er når det er nødvendig for å ivareta driften av virksomheten, det andre er ved mistanke om grove brudd på arbeidstakerens plikter. Når innsyn er tillat og hvordan arbeidsgiver i så fall skal gå frem, er regulert i forskriften nevnt over om arbeidsgivers innsyn i e-postkasse. Forskriften gjelder også sletting når arbeidsforholdet tar slutt. Disse reglene gjelder både nåværende og tidligere arbeidstagere.

Disse reglene gjelder både nåværende og tidligere arbeidstakere. Forskriften gjelder også for arbeidsgiverens adgang til gjennomsøkning av og innsyn i arbeidstakerens personlige område i virksomhetens datanettverk, samt for andre elektroniske kommunikasjonsmedier eller elektronisk utstyr som er stilt til arbeidstakers disposisjon, slik som chat-tjeneste, PC, mobiltelefon og nettbrett. Bestemmelsene gjelder også for arbeidsgiverens innsyn i opplysninger som finnes lagret på sikkerhetskopier eller lignende som arbeidsgiveren har tilgang til.

Opplysninger som er lagret på fellesområder eller i e-postkasser som er felles for hele virksomheten, slik som postkasse@virksomhet.no, vil arbeidsgiveren ha rett til innsyn i uten at de særlige vilkårene i forskriften gjelder.

Forskriftens § 2 sier bl.a. at arbeidsgiver har bare rett til innsyn i når det er nødvendig for å ivareta den daglige driften eller andre berettigede interesser ved virksomheten, eller ved begrunnet mistanke om at arbeidstakers bruk av e-postkasse eller annet elektronisk utstyr medfører grovt brudd på de plikter som følger av arbeidsforholdet eller kan gi grunnlag for oppsigelse eller avskjed. Videre sier forskriften at arbeidsgiver har ikke rett til å overvåke arbeidstakers bruk av elektronisk utstyr, herunder bruk av Internett, med mindre formålet med overvåkingen er å administrere virksomhetens datanettverk eller å avdekke eller oppklare sikkerhetsbrudd i nettverket.

Forskriftens § 3 omhandler prosedyre ved innsyn, der det bl.a. nevnes at arbeidstaker skal så langt som mulig varsles og få anledning til å uttale seg før arbeidsgiver gjennomfører innsyn.

Kameraovervåking er nevnt i arbeidsmiljølovens § 9-6, i personopplysningslovens kapittel 8 og spesielt regulert gjennom en egen forskrift (*Forskrift om kameraovervåking i virksomhet*). Ifølge forskriften § 1 defineres kameraovervåking som vedvarende eller regelmessig gjentatt personovervåking ved hjelp av fjernbetjent eller automatisk virkende overvåkingskamera eller annet lignende utstyr som er fastmontert. Som kameraovervåking anses både overvåking med og uten mulighet for opptak av lyd- og bildemateriale. Det samme gjelder uekte kameraovervåkingsutstyr eller skilting, oppslag eller lignende som gir inntrykk av at kameraovervåking finner sted, jf. personopplysningsloven § 31.

Forskriftens § 3 sier at kameraovervåking av område i virksomheten hvor en begrenset krets av personer ferdes jevnlig, er bare tillatt dersom det ut fra virksomheten er behov for å forebygge at farlige situasjoner oppstår og ivareta hensynet til ansattes eller andres sikkerhet eller det for øvrig er et særskilt behov for overvåkingen.

Forskriften § 6 omtaler sletting av opptak, og sier bl.a. at opptaket skal slettes senest én uke etter at opptakene er gjort. Hvis det er sannsynlig at opptaket vil bli utlevert til politiet i forbindelse med etterforskning av straffbare handlinger eller ulykker, kan opptakene oppbevares inntil 30 dager.

Datatilsynet har utgitt en veileder «*Kameraovervåking – hva er lov?*» som gir praktiske råd og tips. Veilederen finnes på Datatilsynets nettsted: www.datatilsynet.no/regelverk-og-verktoy/veiledere/kameraovervaking/

Sommeren 2019 vedtok det europeiske personvernrådet (European Data Protection Board – EDPB) retningslinjer for kameraovervåkning. «Guidelines 3/2019 on processing of personal data through video devices» (ref. /65/). Retningslinjene skal sørge for større klarhet rundt kravene til kameraovervåkning og sikre lik praksis i hele EU og EØS. De gir praktiske og mer detaljerte retningslinjer for kameraovervåkning enn det som kommer frem av personvernforordningen. I retningslinjene er det presiseringer om blant annet lagringstid, sletteplikt, ansiktsgjenkjenning og varsling/skilting. Der er også praktiske eksempler for hvor og når overvåking er tillatt. Mer kan leses på Datatilsynets sider, under tittelen «*Retningslinjer for kameraovervåking fra Personvernrådet*»

Likestilling og forbud mot diskriminering er regulert gjennom arbeidsmiljølovens kapittel 13 og likestillings og diskrimineringsloven. I kapittel 2 i likestillings- og diskrimineringsloven omtaler forbud mot å diskriminere på grunn av bl.a. etnisitet (eks. nasjonal opprinnelse, avstamning, hudfarge), religion, livssyn, seksuell orientering. Det er et generelt forbud mot innhenting av opplysninger i ansettelsesprosessen (lovens kapittel 5), som f.eks. religion, livssyn, etnisitet og seksuell orientering, dog er visse muligheter dersom det har avgjørende betydning for utøvelse av arbeid.

Arbeidsmiljølovens § 13-4, første ledd, sier at «*Arbeidsgiver må ikke i utlysing etter nye arbeidstakere eller på annen måte be om at søkerne skal gi opplysninger om hvordan de stiller seg til politiske spørsmål eller om de er medlemmer av arbeidstakerorganisasjoner. Arbeidsgiver må heller ikke iverksette tiltak for å innhente slike opplysninger på annen måte.*»

Imidlertid er det en åpning gjennom paragrafens annet ledd som sier at «*Forbudet i første ledd gjelder ikke dersom innhenting av opplysninger om hvordan søkerne stiller seg til politiske spørsmål eller om de er medlemmer av arbeidstakerorganisasjon er begrunnet i stillingens karakter eller det inngår i formålet for vedkommende virksomhet å fremme bestemte politiske syn og arbeidstakerens stilling vil være av betydning for gjennomføringen av formålet. Dersom slike opplysninger vil bli krevet, må dette angis i utlysingen av stillingen.*»

Kredittvurderinger: I *Forskrift til personopplysningsloven (personopplysningsforskriften),* § 4-3 *Utlevering av kredittopplysninger,* står at «*Kredittopplysning kan bare gis til den som har saklig behov for den.*» Ifølge opplysninger gitt av Datatilsynet på telefon via tilsynets veiledningstjeneste (august 2019) er slik saklig behov primært knyttet til personer med overordnet lederansvar og personer med stort økonomisk ansvar. Personer som har tilgang til sensitiv informasjon og kritiske systemer vil således normalt ikke falle inn under dette kravet.

Det gjøres oppmerksom på at selv om personopplysningsforskriften fra 2001 (FOR-2000-12-15-1265) er opphevet, så gjelder likevel kapittel §4 *Kredittopplysningsvirksomhet* i denne forskriften. Dette fremkommer av forskrift «*Overgangsregler om behandling av personopplysninger* FOR-2018-06-15-887» der det i § 4 *Overgangsregler for kredittopplysningsvirksomhet* presiseres at kapittel 4 Kredittopplysningsvirksomhet i personopplysningsforskriften fortsatt gjelder selv om resten av forskriften er opphevet.

Hovedavtalen mellom LO og NHO 2018-2021: Avtalen er omfattende (62 sider). Av spesielle deler med relevans kan nevnes:

- Kapittel IX Informasjon, samarbeid og medbestemmelse, § 9-11 Personellregistre og kontrolltiltak, fjernsynsovervåking
- Kapittel IV Rammeavtale om teknologis utvikling og datamaskinbaserte systemer, punkt VI Behandling av personopplysninger
- Kapittel V Avtale om kontrolltiltak i bedriften

APPENDIX F
Litteraturstudier

F.1: Generelle trekk fra litteraturstudien

Som en del av prosjektet ble det gjennomført en litteraturstudie med formål om å få en oversikt over mulige problemstillinger og tilhørende utfordringer, forskning, lover, forskrifter og standarder, statistiske undersøkelser, veiledere, samt relevante tiltak relatert til innsiderisiko, både nasjonalt og internasjonalt. Rundt 75 dokumenter er gjennomgått, hvorav ca. halvparten er utenlandske utarbeidet f.eks. av australske myndigheter, CPNI, FBI, IAEA, CRISP/ASIS, NATO samt diverse universiteter og organisasjoner.

Et fellestrekk for de aller fleste av kildene er at de gir eksempler på hvem innsideren er («profil»), hva er det som motiverer/inspirerer en innsider til å utføre sine handlinger og hva er de typiske konsekvensene for en virksomhet. Videre fokuserer de fleste kildene på ondsinnede handlinger, men også noen, spesielt de som omtaler IT-sikkerhet, adresserer at ansatte i virksomheter uforvarende utfører handlinger som kan skade virksomheten.

Et gjennomgående trekk ved alle kildene er at de fremhever viktigheten av å ha et klart og entydig program for håndtering av innside-trusler (eng. Insider Threat Programe; InTP), at dette må være forankret i selskapets ledelse og blir kontinuerlig vedlikeholdt.

Videre presenterer de aller fleste kildene eksempler på tiltak for å forhindre at en virksomhet blir utsatt for ondsinnede handlinger utført av innsidere. Tiltakene favner bredt og omfatter bl.a. bakgrunnssjekk (ifm. rekruttering), fysisk sikring, IT-sikkerhetsløsninger (f.eks. monitorer ING for å avsløre unormal datatrafikk), osv.

De fleste kildene adresserer at det er viktig å erkjenne at innsider-problematikken er relevant for hele ansettelses-prosessen, dvs. helt fra rekruttering, via ansettelse/kontrakt og til avslutning av engasjement.

I de aller fleste kildene er det primært fokusert på at en innsider utnytter sin stilling til å få tilgang til, og utnytte, (sensitiv) informasjon for å dele denne med andre utenfor selskapet samt å påføre selskapet skade (sabotasje). I bare mindre grad er tyveri av fysiske produkter/verdier omtalt – det er primært IAEA som har fokuser på dette i sin rapport da de omtaler tyveri av kjernefysisk materiale til bruk i terrorvirksomhet.

Sju av kildene inneholder statistikk/tallmateriale/case studies spørreundersøkelser og analyser. Spesielt gir rapporten fra CPNI (ref. /44/) statistikk på hvem er den typiske innsider (alder, kjønn, ansettelsesforhold, osv.), ubevisste vs. bevisste handlinger, motivasjon etc. Se kapittel F.2 nedenfor for detaljer.

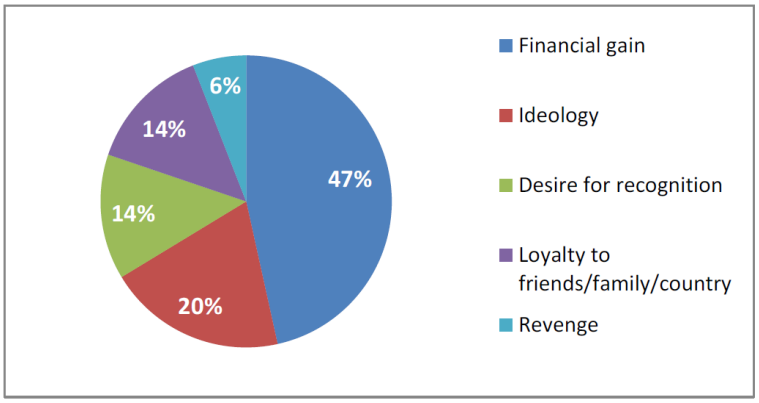
F.2: Erfaringsdata – hva litteraturen forteller

Noen av dokumentene i litteraturstudien har omtalt resultater fra undersøkelser og annet statistisk materiale. De fleste av disse var dog knyttet til cyber security problemstillinger. I dette kapittelet er de utvalgte og mest relevante resultater sammenfattet.

A) CPNI gjennomførte i 2013 en studie der man undersøkte mer enn 120 tilfeller av innsidehendelser fra både offentlig og privat sektor (ref. /44/). Studien ble gjennomført i perioden 2007 – 2012. CPNI identifiserte fem hovedtyper av innsideraktivitet: uautorisert avsløringer av sensitiv informasjon; prosesskorrupsjon[7], hjelpe en tredjepart til å få tilgang til en organisasjons verdier; fysisk sabotasje; og sabotasje på IT eller annet elektronisk utstyr.

De hyppigst forekomne type hendelser var uautorisert avsløring av sensitiv informasjon (47 %) og prosesskorrupsjon (42 %). Videre viste undersøkelsen følgende:

- *Kjønn*: Flest menn (82 %), færre kvinner (18 %).
- *Alder*: I 49 % av hendelsene var innsideren i alderen 31-45 år. Antall hendelser økte med alderen til den toppet seg i denne aldersgruppen, for så å avta etter ca. 45-års alderen
- *Ansatte*: De fleste hendelser var blant fast ansatte (88 %); bare 7 % involverte kontraktører og bare 5 % gjaldt midlertidig ansatte.
- *Varighet*: Varierte fra mindre enn seks måneder (41 %) til mer enn 5 år (11 %). 60 % av tilfellene hadde arbeidet for organisasjonen mindre enn 5 år.
- *Oppdagelse*: Mer enn halvparten av tilfellene ble oppdaget ila. det første året.
- *Kategori*: Flest selvinitiert (76 %), heller enn bevisst infiltrasjon (6 %)
- *Motivasjon*: Økonomisk gevinst mest vanlige motivasjon (47 %), ideologi (20 %), Anerkjennelse (14 %), Lojalitet (14 %), Hevn (6 %) (se figur til høyre).



Figur F-1: Motivasjon for innsideaktivtet

Det var en klar kobling mellom innsiderhendelser og svakheter i forebyggende sikring og ledelsesprosesser:

- *Mangelfull ledelse* – adferd, problemer og diverse aktiviteter hadde vært observert av lederne, men ikke fulgt opp eller tatt tak i
- *Mangelfull bruk av revisjonsfunksjonen* – organisasjoner hadde ikke systematisk tatt i bruk mulighetene som finnes gjennom IT eller finansiell revisjon til å kontrollere og raskt oppdage irregulariteter eller annen uvanlig adferd.
- *Mangelfulle beskyttelsestiltak* – selv enkle systemer for å kontrollere hvordan ansatte kunne introdusere eller fjerne elektroniske data, og manipulere organisasjonsinformasjon selv etter at de hadde sluttet i virksomheten, var ikke implementert.
- *Dårlig sikringskultur* – ofte var det dårlig sikringskultur der innsiderhendelser hadde skjedd, med en generell mangelfull etterlevelse av prosedyrer og andre regler, og med en ledelse som enten ikke kjente til denne mangel fulle etterlevelsen eller som ikke i tilstrekkelig grad tok tak i dette.

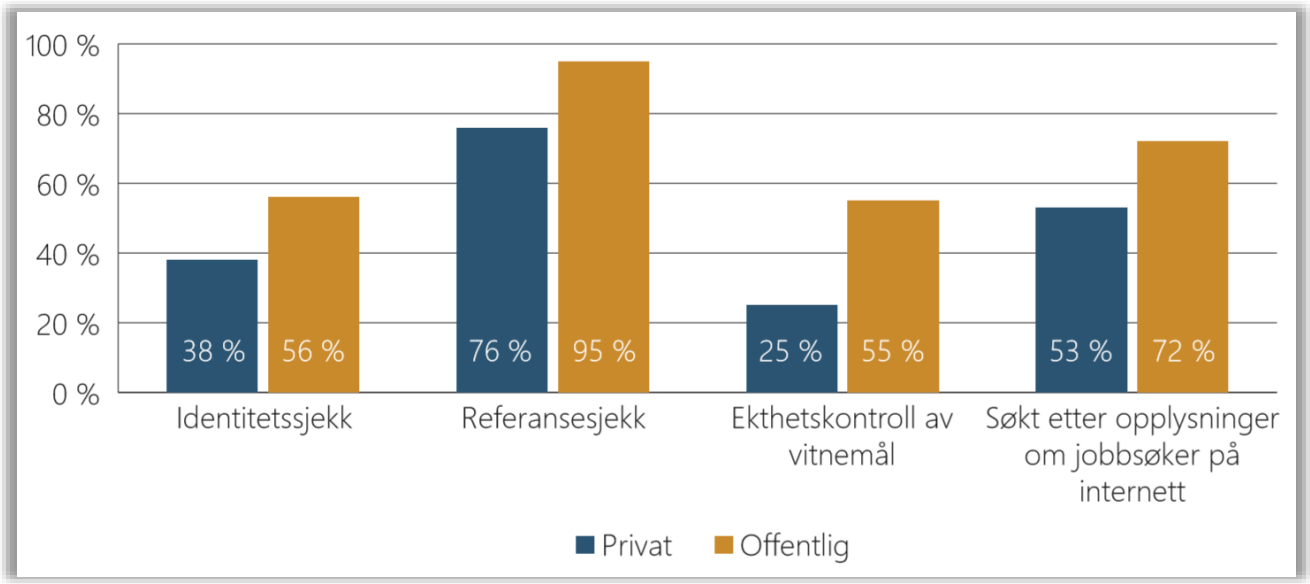
[7] Prosesskorrupsjon er definert som en ikke-lovlig endring/tukling med en intern prosess eller system

Det vanligste syntes å være at passord ble delt mellom arbeidstakere, PC-skjermen ble ikke låst da man forlot PC-en, man tillot andre å bruke terminaler som var pålogget, sensitivt materiale ble liggende på pulten, containere beregnet for kast av sensitivt materiale var ikke låst og adgangskontrollen til sikre områder ble ikke godt nok fulgt.

- *Manglende funksjonsbasert risikovurdering av personer før ansettelse* – I noen tilfeller hadde vedkommende fått arbeidsoppgaver uten at man hadde vurdert personens egnethet for oppgaven, og mulige komplikasjoner dette kunne medføre. Som eksempler ble nevnt tilfeller der ansatte hadde blitt plassert i funksjoner som gjorde at de kunne utgjøre en sårbarhet pga. deres nasjonalitet, familieforhold eller ideologiske sympatier. Det var også tilfeller der arbeidstaker manglet kunnskaper, erfaring og evner. Kombinert med mangelfull ledelse, kunne vedkommende lette bli manipulert av en tredjepart, eller vedkommende kunne uforvarende utføre en uønsket handling.
- *Dårlig bakgrunnssjekk* – i noen få tilfeller av prosesskorrupsjon var det klart at tilstrekkelig grad av bakgrunnssjekk av vedkommende ikke hadde blitt utført. Det viste seg da at vedkommende hadde en uredelig fortid, f.eks. misbruk av kredittkort.
- *Svak kommunikasjon mellom enheter* – undersøkelsen viste at dersom virksomheten ikke kommuniserte internt og ikke delte informasjon om risikoer (trusler, verdier og sårbarheter), ble muligheten for å beskytte og håndtere innsiderrisikoen betraktelig redusert.
- *Mangelfull bevisstgjøring om personellsikring hos øverste ledelse* – en slik mangel kan lett føre til at ledelsesfokus på innsidetrusselen ikke er tilstrekkelig, og at det derfor ikke avsettes tilstrekkelige ressurser.

B) NSMs rapport Risiko 2018 (ref. /25/) viser til at i internasjonale studier påpekes at innsidesaker ofte oppstår tre til fem år inn i et arbeidsforhold. På tross av dette har NSM imidlertid observert at i mange virksomheter avtar sikkerhetsbevisstheten og sikkerhetsoppfølgingen av den ansatte samtidig med at ansettelsesforholdet modnes.

C) NSRs Kriminalitets- og sikkerhetsundersøkelsen i Norge (KRISINO) for 2017 (ref. /28/) adresserer bl.a. spørsmål knyttet til ansettelsesprosessen og gjennomføring av visse sjekker. Tallene viser at generelt synes offentlig sektor å være flinkere til å gjennomføre slike sjekker – som vist i figuren under.



Figur F-2: Oppsummering av svar på spørsmål om virksomhetene har gjennomført følgende i en sin ansettelsesprosess. Fra KRISINO 2017

Falske CV-er: Det er en kjent problemstilling at det jukses med CV-er. I en artikkel fra 2013 på nettstedet til NSR (ref. /29/) omtales at 1 av 5 jukser med CV-en. Der henvises også til en undersøkelse fra 2012 gjort av et konsulentselskap (Semac) at det var kritikkverdige forhold hos hele 40 % av 1120 kontrollerte jobbsøkere. Et annet selskap (Meditor Search) utfører også bakgrunnssjekk av jobbsøkere på vegne av kunder, og de opplyser at de finner feil i én av fire CV-er, og dette tallet har holdt seg stabilt over flere år. Jobbsøkere som jukser seg inn ved forfalskning av CV har ikke nødvendigvis kriminelle hensikter – status, karrieremuligheter og høyere lønn kan være nok til at noen ønsker å benytte juks som virkemiddel for å nå sine mål, dette finnes det dessverre flere eksempler på i Norge. Man må likevel kunne anta at en person som har til hensikt å infiltrere et selskap på vegne av en større organisasjon eller fremmed stat, har et tilstrekkelig ressurssterkt apparat i ryggen som vil kunne etablere en historikk og CV som gjør det vanskelig å oppdage at dette ikke er ekte.

D) EY: I en presentasjon fra EY holdt februar 2017 kalt «Insider Threat – Oil & Gas» ble det nevnt at ca. 50 % av alle ansatte delte bruken av utstyr med andre utenfor organisasjonen, at 18 % av ansatte delte sine passord med kollegaer og 25 % av ansatte delte sensitiv informasjon med venner, familie og fremmede EY oppgir at kilde for disse tallene var «*CISCO, 2014*» og er tatt fra en undersøkelse som involverte 2.000 svar fra mange forskjellige industrier, og omfattet svar fra både sluttbrukere og IT-eksperter.

E) Crowd Research Partners (www.crowdresearchpartners.com): Selskapet utgir, sammen med andre organisasjoner som bla. Dashlane (www.dashlane.com), diverse rapporter spesielt knyttet til IT-sikring (cyber security) basert på undersøkelser og intervjuer blant et stort antall selskaper. En av rapportene adresserer innsidetrusselen (Insider Threat – 2018 Report, ref. /72/), basert på en undersøkelse blant 472 IT-eksperter. Det presiseres at resultatene omtalt under er spesielt fokusert på IT-sikring.

Rapporten påpeker at innen IT-sikring assosieres ofte begrepet innsidertrussel med ansatte som har med ondsinnete intensjoner om å skade selskapet gjennom tyveri eller sabotasje, em at sannheten er imidlertid at uaktsomme ansatte eller kontraktører utgjør en like stor trussel, målt i antall sikringsbrudd eller hendelser der informasjon kommer på avveie pga. uaktsomhet.

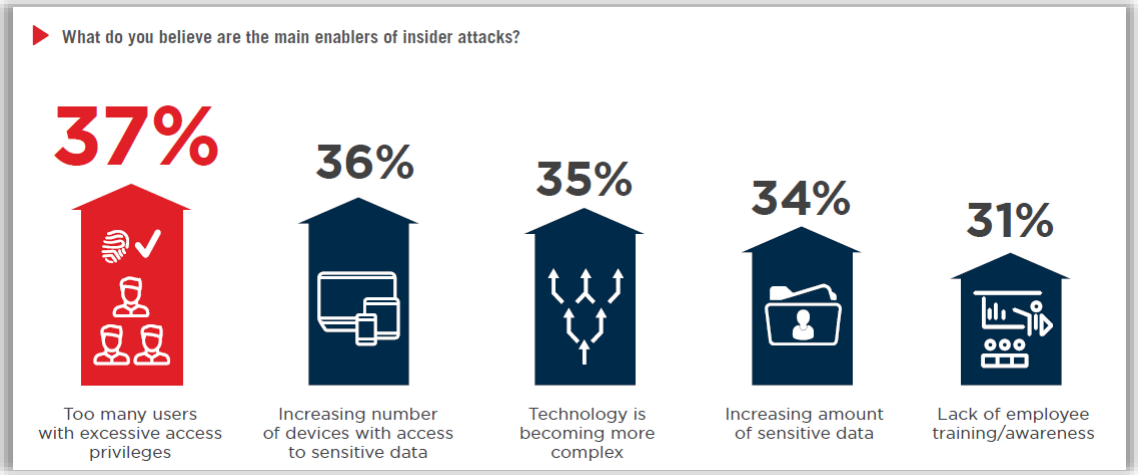
Undersøkelsen viste også at de fleste av de spurte anser at den største trusselen er vanlig ansatte og personer med adminrettigheter eller lovlig tilgang, og at denne trusselen er noe større enn kontraktører og innleide. Se figuren under.

Figur F-3: Hvilken type innsider som ansees å utgjøre den største trusselen?

Videre – på spørsmålet om hvilke type data som ansees som mest sårbar overfor innsidere, kommer forretningsmessig informasjon (finans, kundedata o.l.) høyest, dernest av informasjon som brukernavn og passord, så sensitiv personinformasjon etterfulgt av åndsverk/immateriell eiendom (Intellectual Property) og informasjon om drift og infrastruktur.

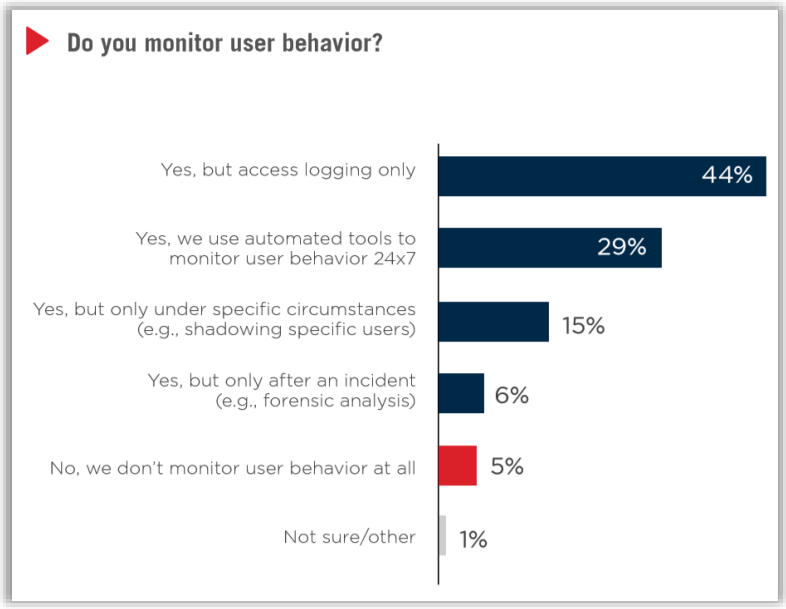
Figur F-4: Hvilken type data som ansees å være mest sårbar overfor innsiderangrep?

På spørsmålet om hva som muliggjør at insidere kan gjennomføre et angrep kom det at for mange brukere har tilgang til systemer, tett etterfulgt av økende antall enheter som inneholder sensitiv data. Også det at teknologien etter hvert blir mer kompleks er på listen. Manglende opplæring og bevisstgjøring er også med på listen.



Figur F-5: Hva muliggjør at en innsider kan gjennomføre et angrep?

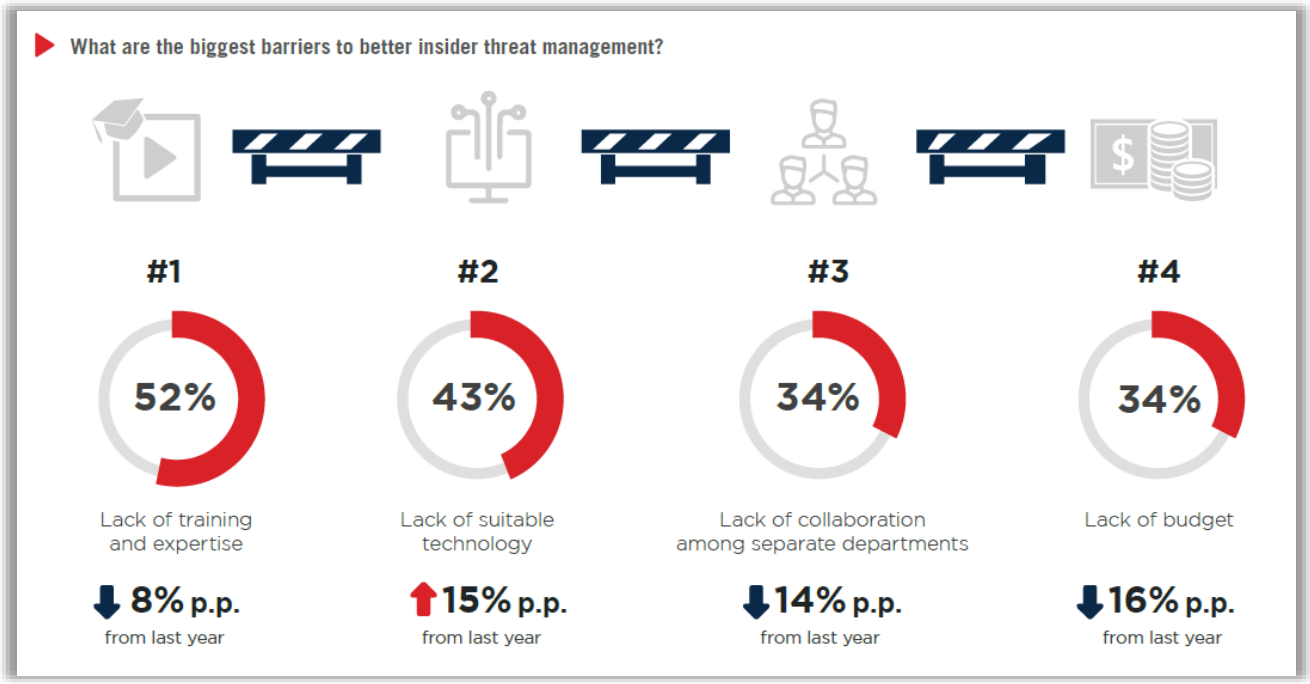
Undersøkelsen viste at antall virksomheter som gjennomfører overvåking av brukeradferd har økt betraktelig. Undersøkelsen fra 2018 viste at 94 % av virksomhetene gjør dette, mens tallet året før var bare 42 %. En viss form for kontinuerlig måling av brukeradferd skjedde blant 73 % av de spurte.



Figur F-6: Måles brukeradferd?

På spørsmålet om hvilken type tiltak de forskjellige virksomhetene fokuserer mest på, var det flest som primært fokuserer på deteksjon (64 %), dernest på å forhindre (adgangskontroll, kryptering osv.), dernest analyser og granskning etter en hendelse (49 %)

Videre, de største hindringene for å få til et godt program for å håndtere innsidetrusselen oppgis å være mangel på opplæring og ekspertise, dernest mangel på passende teknologi, og mangel på samarbeid avdelingene seg imellom, og på fjerdeplass lå mangelfullt budsjett.



Figur F-7: De største hindringene for å håndtere innsidetrusselen

Om DNV GL

DNV GL er et internasjonalt selskap innen kvalitetssikring og risikohåndtering. Siden 1864 har vårt formål vært å sikre liv, verdier og miljøet. Vi bistår våre kunder med å forbedre deres virksomhet på en sikker og bærekraftig måte.

Vi leverer klassifisering, sertifisering, teknisk risiko- og pålitelighetsanalyse sammen med programvare, datahåndtering og uavhengig ekspertrådgivning til maritim sektor, til olje- og gass-sektoren, og til energibedrifter. Med 80,000 bedriftskunder på tvers av alle industrisektorer er vi også verdensledende innen sertifisering av ledelsessystemer.

Med høyt utdannede ansatte i 100 land, jobber vi sammen med våre kunder om å gjøre verden sikrere, smartere og grønnere.