KPMG

Innsiderisiko

Dybdeundersøkelse om økonomisk kriminalitet og innsidetrusselen

25. november 2025

Sammendrag

Samfunnsøkonomisk Analyse (SØA) og KPMG har på oppdrag fra Justis- og beredskapsdepartementet kartlagt omfanget av økonomisk kriminalitet som norske virksomheter og kommuner utsettes for. Som del av oppdraget har KPMG i år gjennomført en dybdeanalyse av innsiderisiko. Formålet er å styrke kunnskapen om hvordan virksomheter og kommuner rammes av innsidetrusler, samt gi veiledning i hvordan slike trusler kan forebygges og håndteres.

Innsiderisiko innebærer at ansatte eller andre med tilgang til virksomhetens informasjon, systemer eller verdier misbruker sin posisjon på en måte som påfører virksomheten skade. Slike hendelser kan være økonomisk motivert, men innsiderisiko omfatter også datalekkasjer, svekket sikkerhet og tap av tillit. Innsiderisiko er relevant for både økonomisk, digital og operasjonell sikkerhet, og må forstås og håndteres som en del av virksomhetens samlede risikobilde.

Det finnes i dag begrenset statistikk og få systematiske kartlegginger av innsidehendelser i Norge. Eksempler fra intervju, politi, Økokrim og medieomtale viser likevel at dette er en reell utfordring, både i privat og offentlig sektor. Flere trusselvurderinger peker på økt risiko for at kriminelle aktører forsøker å få tilgang til informasjon, systemer og tjenester gjennom personer på innsiden.

Det er grunn til å tro at mørketallene er store. Mange hendelser blir ikke avdekket, ikke anmeldt, eller ikke kategorisert som innsidehendelser. Flere virksomheter rapporterer ikke innsidehendelser av frykt for tap av omdømme.

Samtidig vet vi at mange virksomheter ikke har et bevisst forhold til egne sårbarheter. Innsiderisiko er vanskelig å forebygge uten en systematisk tilnærming til sikkerhetsarbeidet. Det første og viktigste steget for mange virksomheter vil være å kartlegge hvilke verdier de skal beskytte, hvilke trusler de står overfor, og hvor de mest sårbare punktene i organisasjonen er. Uten slik innsikt er det vanskelig å vite hvilke tiltak som faktisk virker.

På bakgrunn av dybdeanalysen anbefaler vi at:

- Virksomheter bør etablere en helhetlig tilnærming til innsiderisiko, som kombinerer forebyggende, detekterende og håndterende tiltak, tilpasset virksomhetens størrelse og risikobilde.
- Virksomheter bør betrakte innsiderisikoen fra flere perspektiver, herunder også sammenhengen mellom økonomisk kriminalitet og innsidere som tilretteleggere.
- Myndighetene bør vurdere en nasjonal kartlegging av faktisk og opplevd innsiderisiko, for å bygge et bedre kunnskapsgrunnlag og målrettet forebyggende arbeid.

Innhold

1.Innledning

Samfunnsøkonomisk Analyse (SØA) og KPMG har på oppdrag fra Justis- og beredskapsdepartementet kartlagt omfanget av økonomisk kriminalitet som norske virksomheter og kommuner utsettes for. Undersøkelsen dekker seks lovbruddstyper: bedrageri, digital utpressing, underslag og økonomisk utroskap, korrupsjon, konkurskriminalitet og ulovlig samarbeid. Kartleggingen er basert på spørreundersøkelser rettet mot et representativt utvalg virksomheter og alle landets kommuner.

Som del av oppdraget har KPMG i år gjennomført en dybdeanalyse av innsiderisiko, det vil si risikoen for at ansatte eller andre med lovlig tilgang misbruker sin posisjon på en måte som påfører virksomheten skade. Formålet med analysen er å styrke kunnskapen om hvordan virksomheter og kommuner rammes av innsidetrusler, og gi veiledning i hvordan slike trusler kan forebygges og håndteres.

1.1 Metode og datakilder

Analysen bygger på en kombinasjon av kvantitative og kvalitative datakilder, samt KPMGs erfaring fra bistand til offentlige og private aktører i forebygging og håndtering av innsiderisiko.

En sentral datakilde i arbeidet har vært kvalitative intervjuer med aktører med særskilt innsikt i problemstillingen. Det er gjennomført fire intervjuer med ledere i Økokrim, Equinor, BN Bank og Finans Norge. Selv om antallet er begrenset, gir intervjuene verdifulle innspill om hvordan innsidetrusler oppdages og håndteres i praksis. Innsiktene har vært viktige både for å underbygge analysen av forebyggingstiltak og for å belyse hvor og hvordan slike hendelser kan oppstå. Intervjuene er brukt som interne arbeidsdokumenter og er ikke vedlagt rapporten.

I tillegg er det gjennomført dokumentgjennomgang av relevant faglitteratur, veiledere og analyser, særlig fra Nasjonal sikkerhetsmyndighet (NSM), National Protective Security Authority (NPSA) og DNV. Vi har videre sett til nasjonale trusselvurderinger og medieomtaler for å identifisere og beskrive ulike former for innsidehendelser.

Rapporten bygger også på offentlig tilgjengelig kriminalitetsstatistikk, samt funn fra ovennevnte omfangsundersøkelse vi gjennomfører for Justis- og beredskapsdepartementet og en undersøkelse av omfanget av uetisk atferd, korrupsjon og velferdskriminalitet vi har gjennomført på oppdrag fra KS.

1.2 Avgrensninger

Kapittelet om omfang er primært avgrenset til innsidehendelser med økonomisk motiv. Dette innebærer at hendelser relatert til etterretning, sabotasje eller andre nasjonale sikkerhetstrusler faller utenfor. Avgrensningen er gjort for å sikre et tydelig tematisk fokus.

2. Innsiderisiko og økonomisk kriminalitet

Innsiderisiko har fått økt oppmerksomhet de siste årene, i takt med en skjerpet sikkerhetspolitisk situasjon, økende digitalisering og økende aktivitet fra organiserte kriminelle. Nasjonale trusselvurderinger fra sikkerhetsmyndigheter og politiet peker alle på innsiderisiko som en sentral utfordring for både private og offentlige virksomheter.

I dette kapitlet gjennomgår vi hva innsiderisiko er, hvilke motiver og drivkrefter som ligger bak, samt eksempler på innsidehendelser.

2.1 Definisjon

Nasjonal sikkerhetsmyndighet (NSM) definerer en innsider som en nåværende eller tidligere ansatt, konsulent eller kontraktør som har eller har hatt legitim 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 (Nasjonal Sikkerhetsmyndighet, 2020).

Et kjennetegn ved en innsider er kjennskap til virksomhetens interne rutiner, prosesser og sårbarheter. Denne kunnskapen kan utnyttes til å skade virksomheten, enten på egenhånd eller i samarbeid med andre.

Begrepet *innsider* kan ha varierende betydning avhengig av kontekst. Innen økonomisk kriminalitet og selskapsrettslige problemstillinger benyttes ofte betegnelser som *utro tjener*, *spion*, *tillitsbrudd*, *interessekonflikter* eller *illojal adferd*. Disse eksemplene illustrerer hvordan ett og samme fenomen kan omtales på ulike måter, og hvordan en presis begrepsbruk er viktig for å kunne identifisere og håndtere slike forhold.

Det er mange ulike typer innsidere. Det er hele spekteret fra enkeltpersonen som av ulike årsaker stjeler verdier fra virksomheten, typisk underslag, til alvorlig og organisert kriminalitet hvor det er sammenblanding mellom statlig aktivitet og økonomisk kriminalitet, organiserte kriminelle og legale strukturer.

Alene

En person som jobber i virksomheten og bruker sin tilgang til systemer og informasjon for egen vinning. Vedkommende handler alene, uten hjelp fra andre, og utnytter tilliten en har fått i jobben. Aktivitetene kan som eksempel være å hente ut kundedata, endre interne prosesser eller misbruke tilgang før de slutter i jobben.

En ansatt ved kundeservice i Posten manipulerte datasystemet slik at hen fikk overført penger fra fiktive erstatningskrav til seg selv. Dette utgjorde ca. 340 000 kroner og foregikk over en fireårsperiode. Vedkommende betalte tilbake beløpet, men ble anmeldt og dømt til samfunnsstraff (FriFagbevegelse, 2024).

En til en

En ansatt i virksomheten har kontakt med en person utenfor organisasjonen, for eksempel en kriminell aktør. Innsideren bruker som eksempel sin tilgang til systemer og informasjon for å hjelpe den eksterne parten, mot betaling, andre fordeler eller fordi de er under press.

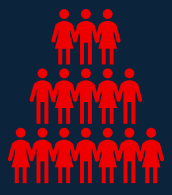
En tidligere DNB-ansatt ble dømt til to år og fire måneders fengsel for å ha underslått 12 millioner kroner fra bankens kontoer mellom 2019 og 2024. Vedkommende skulle kontrollere at andre ikke begikk bedrageri mot banken, men overførte selv penger til blant annet samboeren og andre «andre dårligere stilte personer» (E24, 2025).

Organisert

En eller flere ansatte i virksomheten har kontakt med flere personer utenfor organisasjonen, for eksempel kriminelle aktører eller mellommenn.

Låneagenter fungerer som mellomledd mellom banker og privatkunder. I noen tilfeller krever de store beløp fra kunder som ikke får lån på ordinær måte. For å få gjennom lånesøknaden, benytter de blant annet innsidere i bank til å sikre finansiering (VG, 2022).

Nettverk



En ansatt i virksomheten er enten rekruttert av et kriminelt nettverk eller har infiltrert virksomheten for å kunne fungere som en innsider i legale strukturer.

En hemmeligstemplet rapport fra svensk politi avdekket at kriminelle nettverk systematisk hadde plassert egne medlemmer i politiet, fengselsvesenet og andre offentlige etater. Dette ga dem tilgang til sensitiv informasjon som kunne brukes til å hindre etterforskning og beskytte kriminelle aktiviteter (Nettavisen, 2024)

2.2 Risikofaktorer

Innsiderisikoen kan forklares med hjelp av følgende begreper: *intensjon, kapasitet* og *mulighet* (Nasjonal Sikkerhetsmyndighet, 2020, s. 10).

Intensjon handler om motivasjonen til å utføre en skadelig handling. En person med intensjon har en vilje til å utnytte sin posisjon for å skade virksomheten, enten det gjelder økonomisk vinning, ideologiske årsaker, press fra eksterne aktører eller konflikter.

Motivasjonen bak innsidevirksomhet er sjelden entydig. I de fleste tilfeller skyldes handlingene et samspill mellom personlige forhold, arbeidsmiljø og eventuelt press fra eksterne aktører. Motivasjonen kan endres over tid, og innsideren har ofte utfordringer med å gi en entydig forklaring på egne handlinger.

Selv om motivasjonen kan være kompleks, peker tidligere studier og erfaringer på noen typiske drivere, som økonomiske problemer, ideologisk overbevisning, hevn eller ønsket om status. Disse omfatter blant annet:

- **Ideologisk overbevisning:** Innsidere som begår innsidevirksomhet basert på ideologi har en overbevisning om at deres meninger, oppfatninger eller opplevelser av situasjonen rettferdiggjør deres handlinger.

- **Forhold på arbeidsplassen**: Dersom ansatte opplever negative forhold på arbeidsplassen kan det i noen tilfeller føre til at ansatte ønsker å hevne seg eller skade virksomheten. Eksempelvis dårlige ledelse kan redusere en ansatts lojalitet og engasjement ovenfor arbeidsplassen. Mangel på sikkerhetskultur kan også føre til redusert etterlevelse av sikkerhetsprosedyrer.

- **Økonomiske motiver**: Økonomiske utfordringer kan gjøre personer sårbare for å bedrive innsidevirksomhet. Enten det handler om å bli gjeldfri, oppnå økonomisk trygghet, eller realisere personlige mål. I tillegg kan personer bli rekruttert av eksterne aktører gjennom tilbud om store økonomiske fordeler.

- **Endringer i livssituasjon**: Ved større endringer som kan oppleves plutselig og traumatiserende, som dødsfall, samlivsbrudd, psykisk sykdom som depresjon eller følelsesmessig ustabilitet, kan gjøre personer sårbare for å ubevisst eller bevisst begå innsidevirksomhet.

- **Avhengigheter**: Personer med avhengigheter til eksempelvis pengespill, alkohol eller narkotika kan være mer sårbare for å kunne begå innsidevirksomhet (NPSA, 2014).

- **Relasjonelle faktorer**: Familieforhold kan motivere illojale ansatte til å begå innsidehandlinger, dette kan skje gjennom at den ansatte gir urettmessig tilgang til lån eller informasjon til andre familiemedlemmer.

- **Press**: I noen tilfeller kan ansatte bli utsatt for trusler, utpressing eller sosialt press som tvinger dem til å dele informasjon eller utføre handlinger de normalt ikke ville gjort. Slike situasjoner kan for eksempel oppstå når personer har sårbare livssituasjoner, økonomiske problemer eller personlige relasjoner til kriminelle eller statlige aktører. Presset kan være direkte, som trusler mot familie, eller mer subtilt, som forventninger om lojalitet eller gjengjeldelse.

Kapasitet refererer til evnen til å gjennomføre handlingen. Dette kan forstås som summen av kunnskap, tilganger, erfaringer og personlig egnethet en person innehar for å kunne utføre innsidevirksomhet. En person med høy kapasitet kan utnytte tekniske systemer, forstå interne prosesser og skjule spor.

Kapasitet til å begå innsidevirksomhet vil variere alt etter hvilken aktivitet personen kan utøve uten å vekke mistanke i virksomheten. Disse omfatter blant annet:

- **Kunnskap om rutiner og svakheter**: Personer som kjenner interne prosesser, kontrollmekanismer og hvor det finnes sårbarheter kan utnytte det til å omgå sikkerhet eller skjule spor.

- **Autorisasjon og beslutningsmyndighet**: Ansatte med administrasjonsrettigheter i informasjonssystemer eller personer som i kraft av sin stilling har tilgang til en stor andel av virksomhetens verdier, kan sies å ha stor kapasitet.

- **Nettverk og relasjoner**: Ledere kan benytte sin naturlige autoritet eller sine nettverk og relasjoner til å omgå regler eller til å gjøre unntak fra rutiner og prosesser uten at det blir reagert.

Posisjon, plassering og faktisk tilgang er dermed viktig for vurderingen av en persons kapasitet til å begå innsidevirksomhet. Innsidevirksomhet kan være svært krevende for en person, da det kan ha store personlige konsekvenser og omfatte betydelig hemmelighold. Hvordan enkelt personer håndterer slike situasjoner vil påvirke individets kapasitet.

Mulighet beskriver den praktiske tilgangen til systemer, informasjon eller fysiske områder som gjør det mulig å utføre handlingen. Selv med intensjon og kapasitet, vil mangel på mulighet begrense risikoen.

Hvilke muligheter som eksisterer vil variere fra virksomhet til virksomhet, men noen eksempler er:

- **Fysiske tilganger:** Ansatte som har adgang til lokaler, arkiver eller utstyr som gjør det mulig å hente ut dokumenter, manipulere varer eller installere teknisk utstyr.

- **Systemtilgang**: Innsidere kan ha tilgang til interne IT-systemer, databaser eller saksbehandlingsverktøy, som gir mulighet til å hente, endre eller slette sensitiv informasjon, samt hindre tilgang til informasjonen.

- **Manglende kontrollrutiner:** Svake eller fraværende kontrollmekanismer gir rom til å handle uten å bli oppdaget.

De fleste virksomheter har til enhver tid personer med intern tilgang, som i teorien kan skade verdier gjennom kompromittering, sabotasje eller manipulering av informasjon og prosesser. Samtidig er trusselen dynamisk fordi den påvirkes av faktorer som holdninger hos ansatte, påvirkning fra eksterne aktører og interne forhold som sikkerhetstiltak, kultur og arbeidsprosesser. Disse elementene er i kontinuerlig endring, både på individnivå og i virksomheten som helhet.

Risikoen for en innsidehandling øker når ovennevnte faktorer virker sammen og forsterker hverandre. En person med både motivasjon, evne og mulighet til å misbruke sin posisjon representerer en reell trussel. Fjernes én av faktorene, for eksempel ved å begrense tilganger eller følge opp ansatte tettere, reduseres risikoen tilsvarende. Likevel må man være oppmerksom på at kombinasjonen av kapasitet og mulighet kan utgjøre en latent trussel, selv uten intensjon. En person som i utgangspunktet ikke har motivasjon til å skade virksomheten, kan påvirkes over tid gjennom eksterne faktorer, press eller endrede personlige forhold, slik at intensjon oppstår.

Ubevisste innsidere

Ved denne type innsideaktivitet har personen kapasitet og mulighet, men variabelen intensjon uteblir. Den ansatte har gjerne tilgang til en virksomhets verdier og informasjon, men ønsker ikke å påføre virksomheten skade eller tap. En årsak til at noen blir ubevisste insidere kan være lav sikkerhetsmessig bevissthet hos den aktuelle personen, mangelfull sikkerhetsstyring og daglig sikkerhetsmessig ledelse i virksomheten.

Finansielle institusjoner med ansatte som jobber med sammenslåinger (merger and acquisition) får ofte tilgang til informasjon som kan være børssensitivt. Ansatte som jobber med sammenslåinger, har ikke nødvendigvis forståelse for at det kan være utenforstående som kan være interessert i informasjon om slike prosesser. For disse er det særlig viktig å være oppmerksom på hva som deles i sosiale sammenkomster, offentlige steder og med familie og venner.

En ansatt i en virksomhet ble ilagt en bot på 250 000 kroner for lekkasje av innsideinformasjon. Vedkommende hadde mottatt informasjon om en mulig emisjon og videresendte denne informasjonen til tross for at hen hadde status som innsider i prosessen. Den ansatte beskrev det som «en helt ubetenksom glipp av meg en sen kveldstime». Politiet opplyste at de ikke kjente til motivet for å videresende e-posten, men at det heller ikke var nødvendig å vite motivasjon for å konstatere en overtredelse av loven (Dagens Næringsliv, 2014).

Bevisste innsidere

En bevisst innsider er en innsider med intensjon. Personen er klar over at vedkommende begår en handling som strider mot virksomhetens interesser. Det er derimot ikke nødvendigvis slik at innsideren i alle sammenhenger er kjent med konsekvensene av handlingene. En handling som for en innsider fremstår som et ufarlig brudd på sikkerhetsrutiner kan i noen tilfeller få store konsekvenser for virksomheten.

I rapporten «Energy Cyber Priority 2025» kommer det frem at konsulenter og ansatte i et av Norges største kraftselskaper solgte digital tilgang til det norske kraftselskapet på det mørke nettet. Ifølge tidligere NSM-direktør Sofie Nystrøm har de sett en enorm økning i innsidere, konsulenter og ansatte på det mørke nettet som selger tilgang til selskapene sine (Dagens Næringsliv, 2025).

I februar 2025 anmeldte et skolekorps i Bærum et tidligere styremedlem til politiet, etter at det i forbindelse med forberedelsene til årsmøtet ble avdekket uregelmessige transaksjoner fra korpsets kontoer. Ifølge tiltalen skal vedkommende i perioden fra juni 2024 til februar 2025 ha gjennomført 140 uttak fra korpsets drifts- og sparekontoer, og overført totalt 721 096 kroner til sin egen konto. Tiltalte har tilbakebetalt cirka 100 000 kroner til korpset, og har erkjent det objektive (Advokatbladet, 2025).

2.3 Rekruttering av innsidere

Rekruttering av innsidere innebærer noen ganger målrettet påvirkning eller manipulering av personer med tilgang til sensitiv informasjon eller systemer. Når en person blir forsøkt rekruttert vil ikke nødvendigvis vedkommende være klar over dette selv. Den første kontakten kan for eksempel være i en arbeidssituasjon, tilsynelatende tilfeldige møter, via sosiale medier eller ved en introduksjon fra en felles bekjent.

Personen som blir tilnærmet, vil ofte oppleve å ha kontroll og være del av en trygg situasjon. Den som ønsker å rekruttere vil ofte ønske å skape et vennskapelig forhold for å kunne rekruttere eller verve personen til å handle eller operere som en innsider uten at det foreligger noen form for press. Hensikten med relasjonsbyggingen er å etablere kontakt og samarbeid som over tid leder til at personen kan fungere som en innsider.

Dersom vedkommende lar seg overtale og rekrutteres så vil forholdet kunne endres over tid til å innebære både trusler og press. Dette er særlig aktuelt dersom den rekrutterte personen begår lovbrudd som for eksempel å lekke informasjon eller på annen måte skade virksomhetens verdier. Dette vil kunne sette personen i en vanskelig situasjon hvor den som rekrutterte får mulighet til å yte press mot personen for å opprettholde samarbeidet. I ytterste konsekvens kan det være snakk om manipulasjon, trusler om vold eller andre sanksjoner for å opprettholde samarbeid.

I enkelte tilfeller kan rekrutteringen av innsidere være mer direkte slik som tilbud om økonomisk kompensasjon, eller i form av trusler. Vi er kjent med en situasjon der en ansatt hadde begått en mindre alvorlig kriminell handling på fritiden. Kort tid etter ble vedkommende kontaktet av personer med tilknytning til kriminelle miljøer, som truet med å avsløre forholdet dersom den ansatte ikke gikk med på å bistå som innsider.

Den organiserte kriminaliteten er særlig skadelig der den omfatter infiltrering av offentlige instanser og påvirker beslutningsprosesser. Kriminelle aktører kan bruke ulike metoder for å infiltrere myndigheter, som å utnytte sosiale nettverk, trusler og vold, samt korrupsjon (ibid.).

I enkelte tilfeller blir ansatte rekruttert til innsidevirksomhet etter ansettelse. I andre tilfeller søker personer seg til stillinger med formål om å få tilgang til virksomhetens verdier. Slike personer omtales som infiltratører og kan fremstå som en ordinær søker eller ansatt, men har til hensikt å utnytte sin posisjon til å tilegne seg informasjon, påvirke beslutninger eller begå økonomisk kriminalitet.

Det finnes flere eksempler fra Sverige på alvorlige tilfeller av korrupsjon og infiltrasjon. Den svenske avisen Dagens Nyheter har avslørt hvordan kriminelle gjenger har rekruttert politiansatte, som så lekket informasjon til de kriminelle. Aftenposten har bl.a. i en serie artikler vist hvordan gjengkriminaliteten truer det svenske samfunnet, med Södertälje som eksempel (Aftenposten, 2024).

3. Omfang av innsidehendelser

Innsidehendelser skjer ofte i det skjulte, og det reelle omfanget er vanskelig å tallfeste. Mange hendelser blir aldri oppdaget, og blant dem som avdekkes, er det ikke gitt at de rapporteres videre. Noen saker håndteres internt for å unngå omdømmetap, mens andre kategoriseres under andre former for kriminalitet. Dette gjør at statistikk og registrerte hendelser kun gir et delvis bilde av problemet. I tillegg varierer begrepsbruken (se kapittel 2.1), noe som kan skape metodiske utfordringer ved både rapportering og analyse. Til tross for ovennevnte utfordringer finnes det flere indikasjoner på at innsidetrusler er et økende problem.

I dette kapittelet sammenstiller vi ulike kilder som kan si noe om omfanget, med særlig fokus på koblingen mellom innsiderisiko og økonomisk kriminalitet.[1]

3.1 Trusselvurderinger

Nordic Financial CERT (NFCERT)[2] vurderer at organiserte kriminelle utgjør den primære og mest alvorlige digitale trusselen mot den nordiske finanssektoren. Deres evne til å utvikle nye metoder for å skaffe seg tilgang til systemer, og utpresse penger fra virksomheter, gjør at trusselen vil vedvare i tiden framover. NCERT peker også på at den nordiske finanssektoren har opplevd en økning i innsidehendelser, særlig knyttet til tap av data eller økonomiske verdier. Det er imidlertid ikke dokumentert at organiserte kriminelle har lykkes i å rekruttere innsidere. Det er likevel registrert forsøk på å innhente sensitiv informasjon gjennom profesjonelle nettverksplattformer (Nordic Financial CERT, 2025).

Politiets trusselvurdering for 2025 har et eget kapittel om kriminalitet på innsiden av næringsliv og forvaltning. Her pekes det på at flere bankansatte i Norge etterforskes for å ha gitt lån på uriktig grunnlag, lekket sensitiv kundeinformasjon eller misbrukt tilganger til bankenes systemer. Politiet vurderer at ansatte i bank og finans også i årene fremover vil være særlig utsatt for bestikkelser, press eller trusler fra kriminelle aktører. Begrunnelsen er at bankenes investeringer i cybersikkerhet og transaksjonsovervåking gjør det vanskeligere å gjennomføre hvitvasking uten hjelp fra innsiden (Politiet, 2025).

Europol fremhever i sin trusselvurdering at kriminelle nettverk systematisk infiltrerer eller misbruker legitime virksomheter i nesten alle bransjer og kriminalitetsområder. Noen sektorer trekkes særlig frem som utsatte: bygg og anlegg, eiendomsvirksomhet, logistikk (særlig transport og lagring), samt kontantintensive (særlig overnatting og servering). Europol peker også på at korrupsjon er det som muliggjør slik infiltrasjon (Europol, 2025).

Økokrim har de senere årene viet innsiderisiko økt oppmerksomhet i sine trusselvurderinger. I 2024 vektla Økokrim særlig hvordan kriminelle nettverk forsøker å få tilgang til ansatte i banker, som også gjenspeiles i politiets siste trusselvurdering. Det ble også pekt på betydningen av tilgang til ansatte i logistikkvirksomheter,

[1] Tallene vi rapporterer fra kartleggingen av virksomheters og kommuners utsatthet for økonomisk kriminalitet (omfangsundersøkelsen) er nærmere omtalt i en egen rapport.

[2] Nordic Financial CERT (Computer Emergency Response Team) er en ideell organisasjon som styres og finansieres av medlemmene i den nordiske finansnæringen.

særlig i havner, for kriminelle nettverks mulighet for å få utført ulike tjenester som bl.a. smugling. Disse rekrutteres gjerne gjennom bestikkelser (Økokrim, 2024).

3.2 Tilgjengelig statistikk

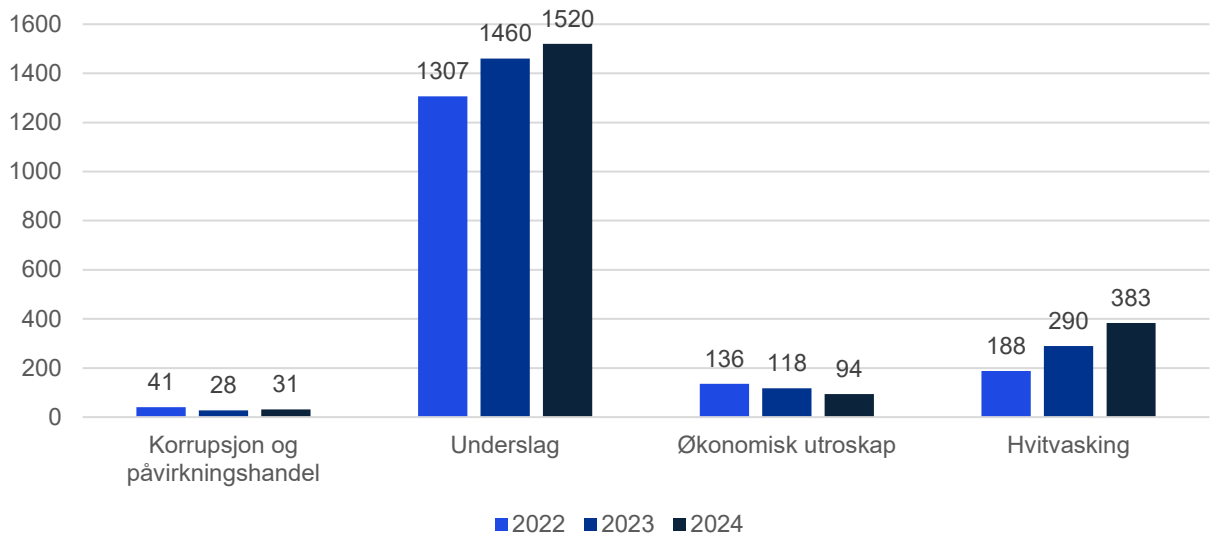
Næringslivets sikkerhetsråd har til og med 2021 gjennomført Kriminalitets- og sikkerhetsundersøkelsen i Norge (KRISINO) annethvert år. Undersøkelsen bygger på svar fra ledere og sikkerhetsansvarlige i 2 000 private og 500 offentlige virksomheter. I 2021 oppga 8 prosent av virksomhetene at de hadde avdekket *utro tjenere* blant egne ansatte de siste to årene. På oppfølgingsspørsmål om hva disse sakene dreide seg om, svarte virksomhetene at det i 64 prosent av tilfellene handlet om underslag, i 9 prosent om lekkasje av sensitiv informasjon og i 0,2 prosent om bestikkelser. Det var små forskjeller mellom bransjer og mellom offentlig og privat sektor. Funnene var i stor grad sammenlignbare med tilsvarende undersøkelse to år tidligere (Næringslivets sikkerhetsråd, 2021).

Resultatene fra KRISINO indikerer at underslag utgjør en betydelig andel av innsidehendelsene virksomheter selv har avdekket. Trusselvurderingene peker samtidig på at korrupsjon er en annen form for økonomisk kriminalitet som ofte er tett forbundet med innsiderisiko. Videre fremhever Politiets og Økokrims trusselvurderinger at behovet for innsidere i banksektoren særlig knytter seg til hvitvasking.

På bakgrunn av dette legger vi til grunn at utviklingen i lovbruddstyper som underslag, økonomisk utroskap, korrupsjon og i noen grad hvitvasking, kan gi en indikasjon på utviklingen i innsidehendelser, og særlig de med økonomisk motivasjon. Felles for disse lovbruddene er at de ofte forutsetter at gjerningspersonen har tilgang til virksomhetens systemer, midler eller beslutningsprosesser.

Statistisk sentralbyrås kriminalstatistikk gir blant annet tall for anmeldte og etterforskede lovbrudd. Statistikken over anmeldte lovbrudd viser en økning i antall tilfeller av underslag de siste tre årene, mens anmeldelser av økonomisk utroskap har falt. Antall hvitvaskingsanmeldelser har nesten doblet seg i samme periode. Anmeldelser av korrupsjon varierer noe fra år til år, men nivået er relativt lavt (jf. figur 3.1).

Figur 3.1 Antall anmeldelser, etter type lovbrudd. 2022-2024



Kilde: Statistisk sentralbyrå

Økningen i hvitvaskingsanmeldelser samsvarer med utviklingen i meldinger om mistenkelige transaksjoner (MT-rapporter). I 2024 mottok Økokrim 30 659 slike meldinger fra rapporteringspliktige virksomheter, opp fra

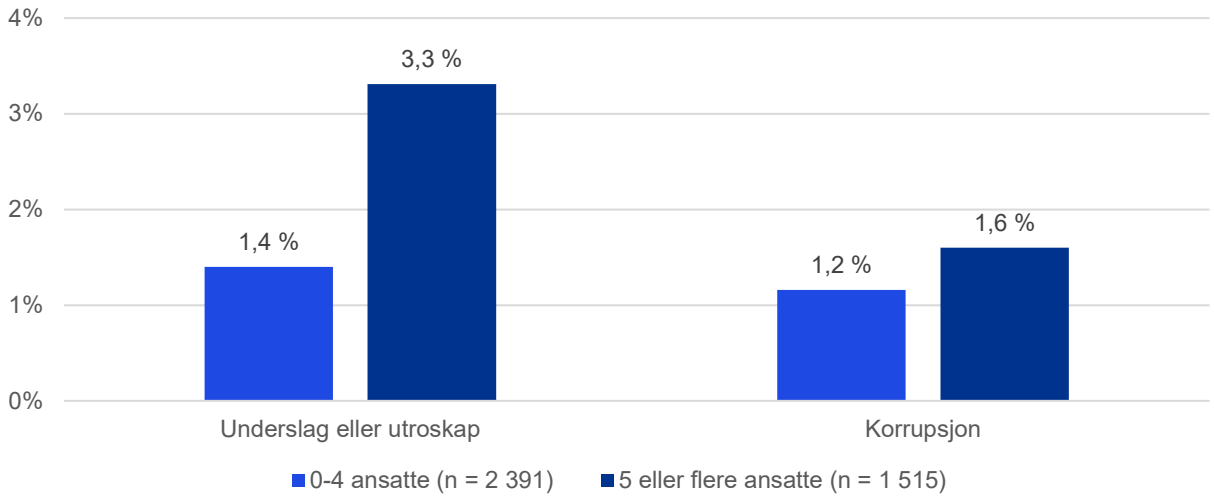
12 703 i 2020. De fleste rapportene kom fra banker, eiendomsmeglere og virksomheter innen betalingsformidling (SØA og KPMG, 2025b).

I årets omfangsundersøkelse oppgir 2,3 prosent av virksomhetene med fem eller flere ansatte at de har vært utsatt for underslag eller økonomisk utroskap, en svak økning fra året før. Blant virksomheter med 0-4 ansatte er andelen 0,8 prosent, om lag uendret. Denne typen lovbrudd ser særlig ut til å ramme de største virksomhetene: Blant virksomheter med 100 eller flere ansatte rapporterer 7,3 prosent å ha hatt økonomisk tap som følge av slike hendelser, mot 1,2 prosent blant de minste virksomhetene (SØA og KPMG, 2025b).

Når vi inkluderer dem som har vært utsatt for forsøk på underslag eller økonomisk utroskap, øker andelen til 3,3 prosent blant virksomheter med fem eller flere ansatte, og til 1,4 prosent blant virksomheter med 0-4 ansatte (jf. figur 3.2).

I 2024 oppgir 1,6 prosent av virksomhetene med fem eller flere ansatte å ha opplevd korrupsjon, en økning fra året før. Andelen er forholdsvis lik på tvers av størrelsesgrupper (jf. figur 3.2).

Figur 3.2 Andel virksomheter (vektet) som oppgir å være utsatt for minst ett forsøk på økonomisk kriminalitet (inkl. tilfeller med økonomisk tap) i 2024, etter type lovbrudd og virksomhetsstørrelse

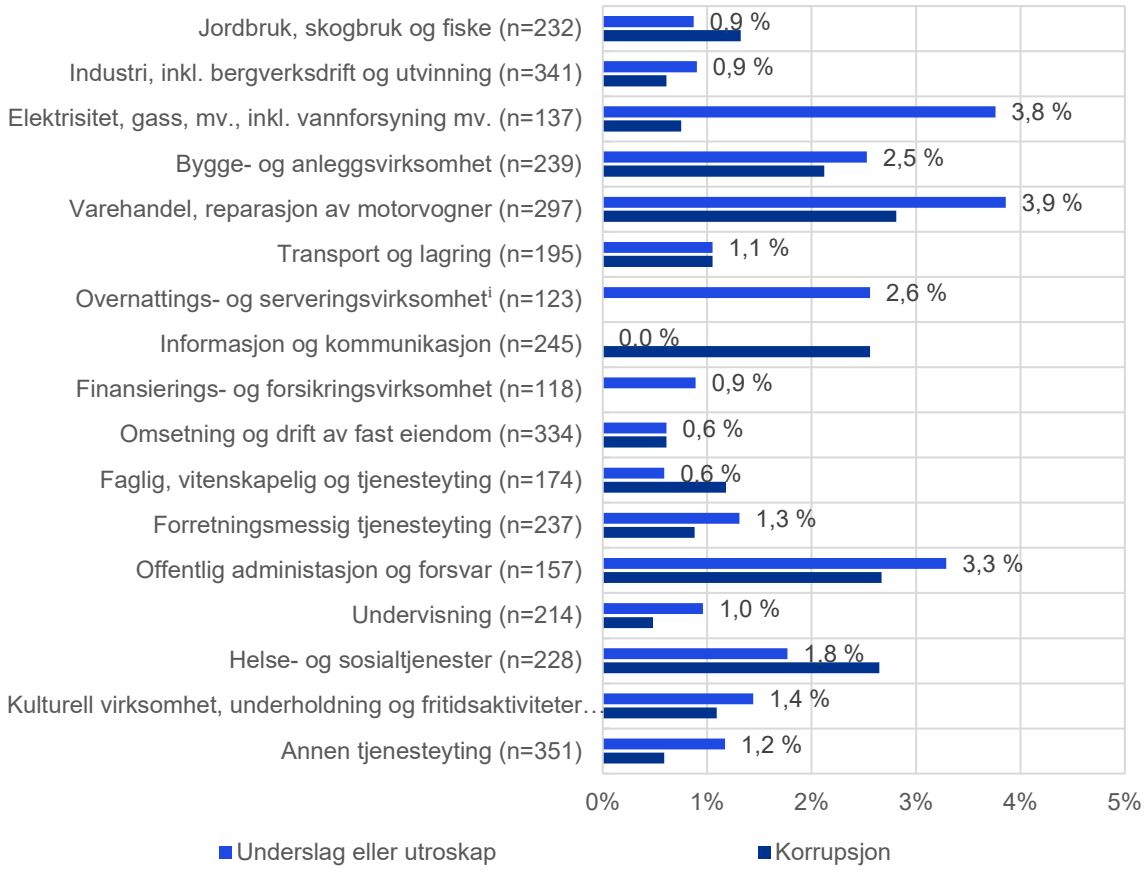


Note: Svarene er vektet for både virksomhetenes størrelse (antall ansatte) og næring. For korrupsjon er ikke økonomisk tap en forutsetning for at virksomheten regnes som utsatt, og det er ikke noe forskjell fra tallene som viser andelen utsatt for økonomisk tap.
Kilde: Spørreundersøkelse gjennomført av Samfunnsøkonomisk Analyse og KPMG

Omfangsundersøkelsen indikerer at underslag og økonomisk utroskap forekommer i så godt som alle næringer. I 2024 var andelen virksomheter som rapporterte å ha vært utsatt for slike lovbrudd høyest i varehandelen, etterfulgt av kraft- og vannforsyning (jf. figur 3.3). Korrupsjon ser også ut til å forekomme på tvers av de fleste næringer. Unntakene i årets undersøkelse er finansierings- og forsikringsvirksomhet samt overnattings- og serveringsvirksomhet. Dette er noe overraskende, sett i lys av ovennevnte trusselvurderinger.

Andelen som rapporterer å ha vært utsatt for korrupsjon er høyest innen varehandel, offentlig administrasjon og forsvar, samt helse- og sosialtjenester (jf. figur 3.3). Blant virksomheter som rapporterer om korrupsjon, er det mest vanlige at ansatte har fått tilbud om bestikkelser i forbindelse med utøvelse av sin stilling (SØA og KPMG, 2025b).

Figur 3.3 Andel virksomheter (uvektet) som oppgir å være utsatt for økonomisk tap som følge av økonomisk kriminalitet i 2024, etter type lovbrudd og næring



Note: Noen næringsgrupper er slått sammen på grunn av få observasjoner; bergverksdrift og utvinning er inkludert i industri og elektrisitets-, gass-, damp- og varmtvannsforsyning er slått sammen med vannforsyning, avløps- og renovasjonsvirksomhet. For overnattings- og serveringsvirksomhet har vi ikke et representativt antall svar (merket med [i]). Det er noe frafall underveis i undersøkelsen og antall respondenter varierer derfor noe for de ulike lovbruddene. Oppgitt n er for første lovbruddstype (bedrageri).
Kilde: Spørreundersøkelse gjennomført av Samfunnsøkonomisk Analyse og KPMG

Også kommunene rapporterer om noe økt utsatthet for korrupsjon, mens andelen som har vært utsatt for underslag eller økonomisk utroskap er halvert sammenlignet med forrige omfangsundersøkelse. I 2024 oppga 2,6 prosent av kommunene at de hadde vært utsatt for korrupsjon, mens 2,2 prosent rapporterte om underslag eller økonomisk utroskap (jf. figur 3.4).

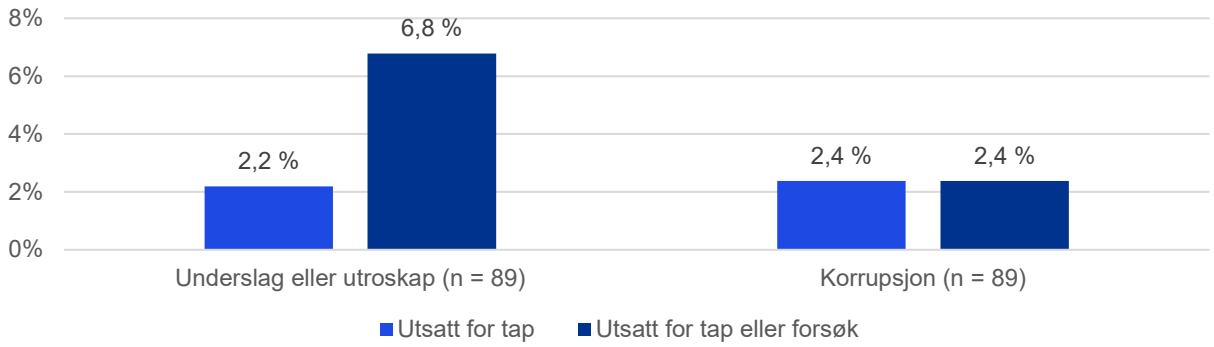
Ifølge politiet gjaldt et titall av anmeldelsene av økonomisk kriminalitet i 2023 korrupsjon, i hovedsak begått av kommunalt ansatte som har misbrukt sin stilling i forbindelse med kjøp eller salg av varer og tjenester mot betaling (Politiet, 2025).

I kartleggingen av uetisk atferd, korrupsjon og velferdskriminalitet i kommuner og fylkeskommuner utført for KS, fant vi at forventninger om uetisk atferd er langt mer utbredt enn faktisk rapportert korrupsjon (SØA og KPMG, 2025a).

En sammenstilling av svensk forskning på hvordan organisert kriminalitet påvirker stat og kommune peker på at svenske kommuner er særlig utsatt for korrupsjon, blant annet fordi de forvalter store velferdsressurser og har svak revisjon. Rapporten fremhever at økt bruk av private aktører som leverer offentlig finansierte velferdstjenester innebærer økt risiko. I tillegg gjør sosial og geografisk nærhet mellom politikere, tjenestepersoner og innbyggere det lettere å påvirke beslutninger (Gunnarson, 2023).

Svenske erfaringer er ikke nødvendigvis direkte overførbare til norske forhold. Organisert velferdskriminalitet vurderes fortsatt som et relativt begrenset problem i norske kommuner (SØA og KPMG, 2025a).

Figur 3.4 Andel kommuner (vektet) som oppgir å være utsatt for økonomisk tap som følge av økonomisk kriminalitet og andel kommuner (vektet) utsatt for minst ett forsøk på økonomisk kriminalitet i 2024, etter type lovbrudd



Note: Svarene er vektet for kommunestørrelse (antall innbyggere). For korrupsjon er ikke forsøk et alternativ, og andelen utsatt for tap og utsatt for tap eller forsøk er derfor den samme. Kilde: Spørreundersøkelse gjennomført av Samfunnsøkonomisk Analyse og KPMG

I omfangsundersøkelsen har vi også spurt virksomhetene og kommunene hvordan de vurderer risikoen for å bli utsatt for blant annet infiltrasjon og innsidere i nærmeste framtid. Om lag 9 av 10 virksomheter vurderer risikoen for dette som liten eller svært liten, mens nær 8 av 10 kommuner gjør det samme.

Årets omfangsundersøkelse indikerer at virksomhetene har anmeldt omtrent ett av fire tilfeller av henholdsvis underslag/økonomisk utroskap og korrupsjon, når vi justerer for virksomhetenes størrelse og næringstilhørighet. I 2023 var anmeldelsesandelen betydelig lavere. Selv om det er usikkerhet knyttet til virksomhetenes anmeldelsestilbøyelighet, viser tallene at langt fra alle lovbrudd blir anmeldt til politiet. Dette tilsier at det eksisterer betydelige mørketall. Den offisielle kriminalstatistikken fanger dermed bare opp en begrenset andel av de faktiske lovbruddene virksomheter utsettes for. Når vi samtidig vet at innsidehendelser ikke nødvendigvis fanges opp under de lovbruddskategoriene vi har omtalt her, understreker dette at mørketallene knyttet til innsiderisiko trolig er omfattende.

3.3 Innsikt fra intervju

Ingen av de vi har intervjuet hadde tilgang til data som viser det samlede omfanget av innsidehendelser. Samtidig ga flere uttrykk for at problemet er mer omfattende enn det som fremgår av offentlig statistikk og rapportering. En av informantene mente at innsidere i økende grad benyttes aktivt, og at kriminelle nettverk i større grad infiltrerer legale strukturer gjennom personer med tilgang. Det ble også reist spørsmål ved hvor mye virksomheter og myndigheter faktisk evner å avdekke. Når anmeldelsestilbøyeligheten er lav og virksomhetene ikke setter ord på eller registrerer slike hendelser, er det rimelig å anta at mange tilfeller aldri blir offentlig kjent.

Alle vi intervjuet kjente til konkrete innsidehendelser, og flere hadde selv håndtert slike saker, enten internt i egen virksomhet eller som rådgivere for andre. Enkelte fortalte også om forsøk på infiltrasjon, der det har vært forsøk på å plassere innsidere i virksomheten, men at dette ble avdekket under ansettelsesprosessen.

Flere informanter trakk frem erfaringer fra rekrutteringssituasjoner, der søkere til stillinger med tilgang til sensitiv informasjon fremsto som klart overkvalifiserte. Noen søkere var fra land Norge ikke har sikkerhetssamarbeid med, og motivasjonen for å søke seg til lavere stillinger enn tidligere fremsto som uklar. Intervjuene indikerer også geografiske forskjeller i hvor utbredt innsiderisiko oppleves som en utfordring.

4. Forebygging og håndtering

Økonomisk kriminalitet kan føre til betydelige økonomiske tap, svekket tillit og varig omdømmeskade for virksomheter som rammes. Samtidig er innsiderisiko ikke begrenset til økonomiske lovbrudd, men omfatter også andre former for skadelig atferd, som sikkerhetsbrudd eller spredning av sensitiv informasjon. Et systematisk arbeid med forebygging og håndtering av innsiderisiko bør derfor være en integrert del av virksomhetsstyringen.

Personellsikkerhet handler om å redusere risikoen for at personer med legitim tilgang til virksomhetens verdier, enten det er informasjon, systemer eller økonomiske midler, kan påføre skade eller tap. Innsiderisikoen omfatter ikke bare egne ansatte, men også leverandører og andre med tilgang til virksomheten. En god tilnærming til håndtering av denne risikoen må derfor inkludere både interne og eksterne aktører.

Hvordan personellsikkerheten organiseres vil variere med virksomhetens størrelse, kompleksitet og risikobilde. Det finnes ikke én riktig modell. Små virksomheter har gjerne enkle strukturer og få ressurser, mens større konsern har etablerte styringssystemer og tydelig definerte roller. Tiltak må tilpasses kontekst og modenhet.

Likevel finnes det noen felles prinsipper. For å styrke arbeidet med innsiderisiko anbefaler vi at virksomheter etablerer et helhetlig styringssystem som dekker menneskelige, tekniske og organisatoriske barrierer i tråd med anbefalinger fra blant andre Nasjonal sikkerhetsmyndighet (NSM).

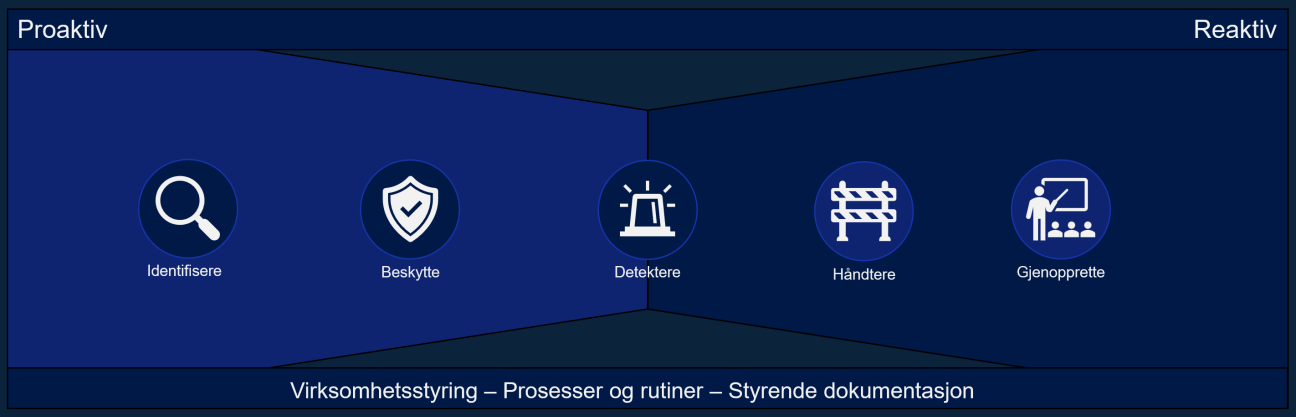
Dette omfatter blant annet at:

- **Styrende dokumenter** for personellsikkerhet bør være godkjent av ledelsen og gjelde for hele organisasjonen. Det er viktig at disse dokumentene oppdateres jevnlig og vedlikeholdes i tråd med endringer i trusselbildet, regelverk og organisatoriske forhold. Dokumentene må være lett tilgjengelige relevante ansatte og kommuniseres på en måte som sikrer forståelse og etterlevelse.

- **Roller og ansvar** knyttet til personellsikkerhet må være klart definert, dokumentert og forstått av alle relevante parter. Det bør være utpekt en funksjon eller person med overordnet ansvar for personellsikkerhet i virksomheten, med mandat til å følge opp innsiderisiko og rapportere til øverste ledelse. Vi opplever at det overordnede personellsikkerhetsansvaret (2. linje) stadig oftere legges til HR.

- **Ledelsen** i virksomheten bør gi personellsikkerhet en tydelig prioritet og integrere det i virksomhetens styringsdialog for å styrke både den strategiske forankringen og den operative evnen til å forebygge og håndtere innsidehendelser. Sørg for tilstrekkelig kompetanse og ressurser innen fagområdet.

I det videre har vi valgt å strukturere arbeidet med innsiderisiko etter den såkalte *bow-tie-modellen*. Denne modellen er et verktøy som brukes for å identifisere, forebygge og håndtere uønskede hendelser. Modellen gir en oversiktlig og helhetlig tilnærming til sikkerhetsarbeidet.



Bow-tie-modellen er en anerkjent metode for risikostyring som gir en visuell fremstilling av sammenhengen mellom årsaker, hendelser og konsekvenser. Modellen har form som en sløyfe, der den kritiske hendelsen, ofte kalt topphendelsen, plasseres i midten. På venstre side identifiseres trusler og årsaker som kan utløse hendelsen, sammen med forebyggende barrierer som skal hindre at den oppstår. På høyre side beskrives mulige konsekvenser dersom hendelsen skjer, samt konsekvensreduserende barrierer som skal begrense skadeomfanget.

I vår modell har vi definert fem underkategorier som representerer fem ulike faser innen forebygging og håndtering av innsiderisiko/-hendelser.

Identifisere

Identifiseringsfasen innebærer å kartlegge virksomhetens risikobilde, inkludert kritiske funksjoner og roller. Den omfatter også en analyse av potensielle trusler og vurdering av nødvendige tiltak for å redusere risikoen.

Beskytte

Når verdier, trusler og sårbarheter er kartlagt, må virksomheten etablere målrettede tiltak for å redusere risikoen for innsidetrusler og uønskede hendelser. Tiltakene skal være relevante, tilpasset virksomheten og gjennomføres i samsvar med gjeldende lover og forskrifter, inkludert personvern og arbeidsmiljøregler.

Deteksjon

Dette kapitlet gir eksempler på hvordan virksomheten kan styrke sin evne til å oppdage tidlige tegn på uønsket atferd eller sikkerhetsbrudd gjennom ulike tiltak som monitorering av brukeratferd, analyse av tilgangsmønstre og bruk av avanserte varslingssystemer.

Hendelse

Når en innsidehendelse oppstår, må virksomheten ha en plan som beskriver hvordan skade skal begrenses, bevis sikres og berørte parter ivaretas. Planen bør inneholde rutiner for håndtering, kommunikasjon, dokumentasjon og oppfølging, tilpasset virksomhetens behov.

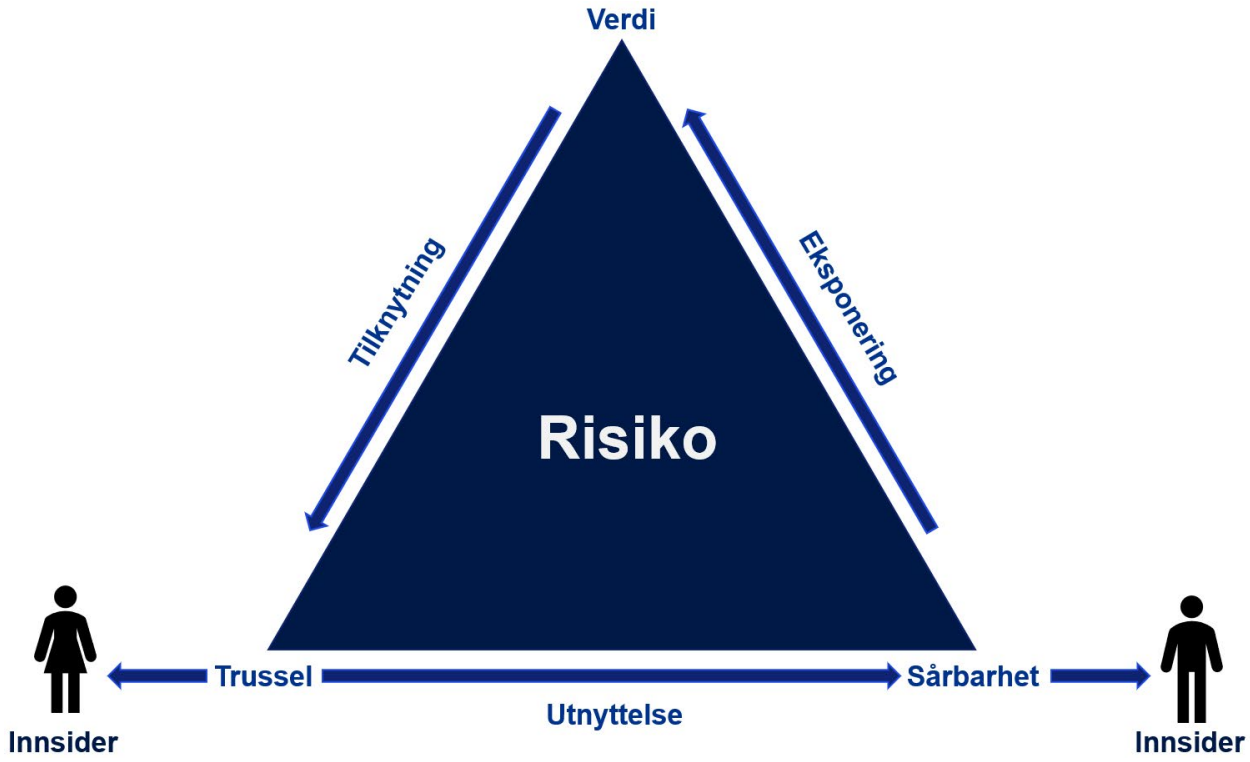
Gjenopprette

Etter en hendelse må virksomheten gjenopprette normal drift og samtidig evaluere hendelsen for å identifisere læringspunkter. Kontinuerlig læring og forbedring er avgjørende for å styrke fremtidige prosesser og opprettholde en robust innsiderisikostrategi.

4.1 Indentifisere

Identifiseringsfasen handler om å identifisere hvilken risiko virksomheten står ovenfor, og hvilke tiltak den bør iverksette for å redusere risikoen. Dette kan innebære å forstå organisasjonens risikobilde, identifisere kritiske funksjoner og roller, og en analyse av hvilke trusler som kan oppstå.

En klassisk modell for å forstå risiko er **risikotrekanten**, som består av tre elementer:



- **Verdier**: Det som skal beskyttes. Dette kan være konfidensiell informasjon, finansiell informasjon, persondata, kundedata, produksjonsutstyr, penger eller samfunnskritiske tjenester.
- **Trusler**: Aktører eller hendelser som har kapasitet og intensjon til å utnytte sårbarheter. Dette kan være illojale ansatte, infiltratører, kriminelle nettverk eller utilsiktede feil og svakheter.
- **Sårbarheter**: Forhold i virksomheten som gjør det mulig for trusler å få tilgang til og skade verdier. Det kan handle om manglende tilgangskontroll, svakheter i sikkerhetsrutiner, lav bevissthet eller interne konflikter.

Ved å forstå hvordan disse tre elementene samspiller, kan virksomheter vurdere sin egen eksponering for innsiderisiko.

Ansatte kan utgjøre både en *trussel*, for eksempel en person som bevisst ønsker å skade virksomheten, og en *sårbarhet*, dersom vedkommende blir manipulert eller utnyttet. Trusselbildet kan være komplekst og vanskelig å forutse, mens menneskelige sårbarheter er mer konkrete og håndterbare. Det er ofte mer hensiktsmessig for virksomheten å fokusere på sårbarheter hos mennesker fremfor hvilken trussel de utgjør.

Graden av innsiderisiko varierer mellom virksomheter, avhengig av faktorer som størrelse, sektor, oppdrag og eksisterende sikkerhetstiltak. Det er uansett viktig at virksomheten vurderer hvordan rekruttering gjennomføres, og identifiserer tiltak som kan redusere sannsynligheten for å ansette personer som enten ikke er egnet for stillingen, eller som bevisst søker seg til virksomheten med skadelige hensikter.

Virksomheten bør etablere en prosess som ivaretar sikkerhet ved ansettelse:

- **Stillingsanalyse**: Før en stilling lyses ut, bør virksomheten gjøre en vurdering av om rollen gir tilgang til sensitiv informasjon, systemer, lokaler eller gir fullmakter som kan øke risikoen.

- **Risikovurdering**: Stillingen bør risikovurderes basert på informasjonen fra stillingsanalysen. Vurderingen vil gi en forståelse av risikonivå for stillingen og hvilke tiltak som bør iverksettes for å redusere risiko. For stillinger som er vurdert som høyrisikostillinger (såkalt High Risk Positions – HRP) vil det være særlig viktig med risikoreduserende tiltak.

Hvilke tiltak som skal iverksettes vil variere ut ifra resultatet av risikovurderingen. Her lister vi opp noen eksempler på tiltak som kan iverksettes:

- **Bakgrunnssjekk**: Hvor omfattende bakgrunnssjekken skal være vil avhenge av risikovurderingen og hvilke tiltak virksomheten har lovlig tilgang til. Dette kan spenne fra enkle søk i åpne kilder til sikkerhetsklarering, men som et minimum bør virksomheten verifisere identitet, tidligere arbeidsforhold og vitnemål til aktuelle kandidater (sjekke referanser).

- **Sikkerhetssamtaler**: Virksomheten kan gjøre sikkerhetssamtaler som en del av rekrutteringsprosessen. Disse samtalene kan inneholde tema som tilknytning til land uten sikkerhetssamarbeid, økonomi eller andre personlige forhold som utgjør en risiko.
- **Sikkerhetskompetanse**: Basert på risikovurderingen bør virksomheten vurdere å ha med en person som har kompetanse på sikkerhet under intervjuet.

Virksomheter kan ha utfordringer med å definere hvilke roller som er «HRP», og det er ikke uvanlig at svært mange roller kan få denne betegnelsen i starten. Det er viktig at virksomheter som gjennomfører slike kartlegginger, kun definerte de mest kritiske rollene som HRP og at dette baseres på en vurdering av konsekvensene hvis noen med denne rollen utførte en innsidehandling.

4.2 Beskytte

Når virksomheten har identifisert og vurdert verdier, trusler og sårbarheter, må det etableres tiltak som reduserer risikoen for innsidetrusler og uønskede hendelser. Fordi medarbeidere har tilgang til virksomhetens verdier og informasjon, representerer de alltid en potensiell risiko sett fra et personellsikkerhetsperspektiv. Tiltakene bør være relevante, tilpassede og gjennomføres i samsvar med gjeldende lover og forskrifter, inkludert personvern (GDPR), arbeidsmiljø, likestilling, antidiskriminering, HMS og regler om offentlighet og privatlivets fred.

- **Sikkerhetskultur**: Etabler en kultur der sikkerhet er en naturlig del av arbeidshverdagen. Dette innebærer som eksempel tydelige verdier, omtale av ledelsen, visuelle uttrykk og avsatt tid til sikkerhetsfokus. Kommunikasjon om innsiderisiko er krevende, og dersom budskapet ikke formidles riktig kan ansatte oppfatte at arbeidsgiver mistenkeliggjør personellet. Det er derfor viktig med en balansert tilnærming, der forebygging og bevisstgjøring vektlegges.

- **Opplæring og bevisstgjøring**: Gi ansatte opplæring i personellsikkerhet, altså det å forstå innsiderisikoen i form av trusler, verdier og sårbarheter. Bevisstgjøring reduserer risikoen for menneskelige feil og sosial manipulering.

- **Sårbarhetssamtaler**: Gjennomføre samtaler med personer i roller med høy risiko (f.eks. tilgang til kritiske systemer) for å identifisere endringer i livssituasjon som kan øke sårbarheten.

- **Identitet og tilgangskontroll**: Iverksett sterke autentiseringsmekanismer, som flerfaktorautentisering, og sikre at tilganger revideres jevnlig.

- **Tilgangsstyring basert på behov**: Begrense tilganger til «need-to-know» og «least privilege». Dette minimerer konsekvensene dersom en konto kompromitteres eller en ansatt handler uaktsomt eller misbruker sine tilganger.

- **Logging og overvåking**: Aktiv digital overvåking av systemer for å oppdage uvanlig aktivitet tidlig. Dette gir mulighet til rask respons ved mistenkelige hendelser.

4.3 Detektere

Metodene for å detektere innsidehendelser varierer mellom virksomheter. I noen tilfeller avdekkes slike hendelser tilfeldig, for eksempel gjennom tips fra kolleger eller ved gjennomgang av avvik. I andre tilfeller benyttes mer systematiske og teknologibaserte tilnærminger, som monitorering av brukeratferd, analyse av tilgangsmønstre eller bruk av avanserte varslingssystemer.

Virksomhetens evne til å oppdage tidlige tegn på uønsket atferd eller sikkerhetsbrudd er viktig i det forebyggende arbeidet. Tidlig deteksjon gir mulighet til å gripe inn før skade oppstår og her gir vi noen eksempler på tiltak som bør vurderes:

- **Rutiner og systemer**: Virksomheten bør etablere rutiner og systemer som fanger opp avvik og uvanlig adferd, for eksempel avviksrapporter eller rutiner for revisjon.

- **Varsling**: Alle virksomheter med mer enn 5 ansatte må ha rutiner for varsling, og større virksomheter bør vurdere elektroniske varslingskanaler.

- **Teknologi**: Virksomheten bør vurdere implementering av teknologiske løsninger for deteksjon. Slike løsninger benytter ofte signaler fra ulike kilder, som brukeratferd, filtilgang og kommunikasjon, for å oppdage mønstre som kan indikere brudd på retningslinjer, datalekkasjer eller andre uønskede handlinger. Teknologiske løsninger for deteksjon gir ofte mulighet for å definere policyer, overvåke hendelser og iverksette tiltak på en strukturert og personvernvennlig måte.

Hvilke deteksjonstiltak en virksomhet bør iverksette, avhenger i stor grad av virksomhetens størrelse, risikobilde, tilgjengelige ressurser og kriterier for risikoaksept.

4.4 Håndtere

Når en innsidehendelse oppstår må organisasjonen ha en plan for håndtering som blant annet inneholder konkrete tiltak for å begrense skade, sikre bevis og ivareta berørte parter. Utforming av slike planer avhenger av virksomhetens behov, men vi anbefaler at de inneholder en beskrivelse rutiner for:

- **Beslutningsgrunnlag**: Virksomheten bør ha rutiner for når og hvordan hendelser skal undersøkes, slik at alle involverte er klar over når planverket skal benyttes.

- **Rollefordeling**: Det bør være en tydelig rollefordeling som fastslår hvem som bistår med hva i håndteringsprosessen, for eksempel IT, leder, juridisk eller HR. Dette fordeler ansvar på de ulike aktørene.

- **Medarbeidere**: En innsidehendelse kan ha konsekvenser for flere ansatte, både direkte og indirekte, og det er derfor viktig at virksomheten har etablerte rutiner for oppfølging av berørte medarbeidere. Dette omfatter blant annet vurderinger av hvem som skal informeres, hva slags informasjon som skal deles, og hvordan informasjonen skal tilpasses ulike målgrupper internt.

- **Kommunikasjon**: Særlig større eller alvorlige innsidehendelser kan utløse henvendelser fra media, samarbeidspartnere eller andre deler av virksomheten. En forhåndsdefinert plan for intern og ekstern kommunikasjon bidrar til at korrekt informasjon formidles til rett tid, og at kommunikasjonen ivaretar både sikkerhetshensyn, personvern og omdømme.

- **Ekstern bistand**: I enkelte tilfeller kan innsidehendelser kreve bistand fra eksterne aktører som Nasjonal sikkerhetsmyndighet (NSM), politiet eller andre relevante sikkerhetsmiljøer. Virksomheten bør ha etablerte rutiner som tydelig beskriver når ekstern bistand skal vurderes, hvilke aktører som skal involveres, og hvordan kontakten skal etableres. I tillegg bør det også være klart definert hvem i virksomheten som har myndighet og ansvar for å ta kontakt med eksterne instanser.

- **Bevissikring**: Virksomheten bør ha rutiner for å sikre at alle sikkerhetsrelaterte hendelser loggføres og dokumenteres.

Hvilke planverk som skal iverksettes vil avhenge av hendelsens alvorlighet og omfang. Det er imidlertid viktig at virksomheten håndterer hendelsen på en måte som står i rimelig forhold til alvorlighetsgraden. En uproporsjonal reaksjon, for eksempel å sanksjonere ansatte hardt for mindre feil eller uaktsomhet, kan bidra til å svekke tilliten til arbeidsgiver og skape misnøye i organisasjonen. I verste fall kan dette føre til en nedkjølende effekt, der ansatte vegrer seg for å melde fra om feil eller bekymringer i frykt for konsekvenser.

4.5 Gjenopprette

Etter en hendelse må virksomheten gjenopprette normal drift. Det kan være fristende å anse hendelsen som avsluttet når normalsituasjon er opprettet, men det er viktig at hendelsen evalueres for å identifisere læringspunkter og forbedre fremtidige prosesser. Kontinuerlig læring og forbedring er en sentral del av en robust innsiderisikostrategi.

Det anbefales at virksomheten som minimum har rutiner for å gjennomføre debrief med involverte parter og å utarbeide en skriftlig evalueringsrapport etter større hendelser.

5. Referanser

Advokatbladet. (2025, Juli 21). *www.advokatbladet.no*. Hentet fra https://www.advokatbladet.no/barnekorps-underslag-okonomisk-kriminalitet/tidligere-styremedlem-tiltalt-for-grovt-underslag-skal-ha-overfort-over-700000-kroner-fra-skolekorpsets-kontoer-til-sin-egen/232580

Aftenposten. (2024, Februar 01). *www.aftenposten.no*. Hentet fra https://www.aftenposten.no/verden/i/xgLnPn/organisert-kriminalitet-truer-sverige-sodertalje-er-verst

Dagens Næringsliv. (2014, November 17). *www.dn.no*. Hentet fra https://www.dn.no/jus/finanstilsynet/finans/-en-helt-urimelig-overreaksjon/1-1-5235510

Dagens Næringsliv. (2025, Mars 30). *www.dn.no*. Hentet fra https://www.dn.no/energi/ansatte-solgte-tilgang-til-norsk-energigigant/2-1-1798807

E24. (2025, November 10). *www.e24.no*. Hentet fra https://e24.no/boers-og-finans/i/Av80Mq/dnb-ansatt-doemt-for-grovt-underslag

Europol. (2025). *The changing DNA of serious and organised crime.* European Union, Serious and Organised Crime Threat Assessment.

FriFagbevegelse. (2024, Mai 13). *www.frifagbevegelse.no*. Hentet fra https://frifagbevegelse.no/posthornet/18-utro-tjenere-fikk-sparken-i-posten-i-2023-6.158.1048692.d4b4f1ae9b

Gunnarson, C. (2023). *Den sårbara staten. En forskningsöversikt om hur organiserad brottslighet påverkar stat och kommun.* Studieförbundet Näringsliv och Samhälle (SNS).

Nasjonal Sikkerhetsmyndighet. (2020). *Temarapport Innsiderisiko.* NSM.

Nasjonal Sikkerhetsmyndighet. (2021). *Grunnprinsipper for personellsikkerhet.* Oslo: NSM.

Nettavisen. (2024, August 29). *www.nettavisen.no*. Hentet fra https://www.nettavisen.no/nyheter/hemmeligstemplet-rapport-svenske-gjenger-infiltrerer-politiet/s/5-95-1987432

Nordic Financial CERT. (2025). *Cyber Threat Landscape for the Nordic Financial Sector.*

NPSA. (2014). *Ongoing Personell Security.* National Protective Security Authority.

Næringslivets sikkerhetsråd. (2021). *KRISINO 2021.*

Politiet. (2025). *Politiets trusselvurdering 2025.*

SØA og KPMG. (2025a). *Uetisk atferd, korrupsjon og velferdskriminalitet i kommuner og fylkeskommuner.* Samfunnsøkonomisk Analyse, Rapport nr. 20-2025.

SØA og KPMG. (2025b). *Kartlegging av virksomheters og kommuners utsatthet for økonomisk kriminalitet.* Samfunnsøkonomisk Analyse, Rapport nr. 35-2025.

VG. (2022, Mai 31). *www.vg.no*. Hentet fra https://www.vg.no/spesial/2022/laaneagentene/

Økokrim. (2024). *Trusselvurdering 2024.*

Kontakt oss:

Erik Arvnes
Partner
Tlf: +47 406 39 341
erik.arvnes@kpmg.no

Trygve Kringlebotn Aandstad
Executive Director
Tlf: +47 480 91 168
trygve.aandstad@kpmg.no

Sigve Røger
Senior Manager
Tlf: +47 909 20 184
sigve.roger@kpmg.no