

A person wearing a dark hoodie is seen from behind, sitting at a desk in a dimly lit room. Several computer monitors are visible on the desk, displaying various images. The room is illuminated by blue light, creating a high-tech or cyber-themed atmosphere. The person's face is not visible, emphasizing their anonymity.

# Kriminalitets- og sikkerhetsundersøkelsen i Norge 2019

# Forord

Kriminalitets og sikkerhetsundersøkelsen i Norge (KRISINO) har siden 2006 vært et viktig bidrag til kunnskapsbygging om kriminalitet og sikkerhet for næringsliv og myndigheter.

Å basere beskyttelsestiltak på kunnskap er klokt av flere grunner.



Kunnskap om sikkerhetsutfordringer gir oss de beste forutsetninger for godt forebyggende arbeid. Dernest gir kunnskap om utfordringene grunnlag for hurtig endring i forhold til nye trusler. Slik kan vi bedre beskytte våre verdier, næringer og virksomheter i en verden preget uforutsigbarhet, konnektivet og hurtige endringer. Vi er derfor svært takknemlige for at både våre medlemmer og myndighetene støtter undersøkelsen.

Kriminalitets- og sikkerhetsundersøkelsen i Norge gir oss, sammen med andre undersøkelser, for eksempel Mørketallsundersøkelsen og Hybridundersøkelsen, et godt bilde av hvilke kriminalitet som rammer næringslivet. Samtidig vet vi også mer om hvilke tiltak næringslivet gjennomfører, og hvordan disse virker. At undersøkelsen har gått over mange år, gjør den mer valid, samtidig som det er mulig å identifisere både positive og negative trender i kriminalitets og sikkerhetsutfordringene.

Mye av den tradisjonelle vinningskriminaliteten har funnet nye digitale former. Samtidig ser vi også nye ikke-digitale sikkerhetsutfordringer. Et helhetlig sikkerhetsarbeid må derfor omfatte mennesker, teknologi og organisasjon.

Reisesikkerhet har fått et sterkt fokus siden forrige undersøkelse. Vi har blant annet spurt om virksomheten har retningslinjer for digital reisesikkerhet.

Resultatet var ikke oppløftende, og er et område NSR vil fortsette å ha fokus på.

Henleggelse av anmeldelser utgjør fortsatt den klareste årsaken til å unnlate å anmelde straffbare forhold. Dette er uheldig for både de som rammes, og for samfunnet som helhet. Prinsippet om at kriminalitet ikke skal lønne seg, og at alle skal stå til rette for sine handlinger er et fundament for tillit og trygghet i samfunnet.

Forebygging og gode sårbarhetsreducerende tiltak er viktig for å redusere risikoen for næringsliv og virksomheter. Både undersøkelsen og analysen viser at vi fortsatt har en vei å gå på disse områdene. Samtidig ser vi en stigende tillit til politiets kompetanse. Gjennom nye former for samarbeid mellom privat og offentlig sektor kan dagens og morgendagens sikkerhetsutfordringer løses med bedre presisjon og effekt.

Vi håper at undersøkelsen og analysen vil være nyttig, både for næringsliv og myndigheter. NSR ønsker å takke alle som har støttet oss i arbeidet med undersøkelsen.

Odin Johannessen  
Direktør NSR



:RUD PEDERSEN GROUP





# Innhold

|                                     |           |
|-------------------------------------|-----------|
| <b>Sammendrag</b>                   | <b>6</b>  |
| Sikkerhet                           | 6         |
| Økonomisk kriminalitet              | 6         |
| Anmeldelser                         | 7         |
| Sikringskamera                      | 7         |
| Vold mot ansatte                    | 7         |
| <b>Innledning</b>                   | <b>8</b>  |
| Bakgrunn                            | 8         |
| Populasjon                          | 8         |
| Datainnsamling                      | 8         |
| Feilmarginer                        | 8         |
| Karakteristika                      | 9         |
| Geografi                            | 9         |
| <hr/>                               |           |
| <b>1 Sikkerhet</b>                  | <b>10</b> |
| 1.1 Risikovurdering                 | 12        |
| 1.2 Trusselvurdering                | 16        |
| 1.3 Kontrolltiltak ved ansettelse   | 18        |
| 1.4 Digital reisesikkerhet          | 20        |
| <hr/>                               |           |
| <b>2 Økonomisk kriminalitet</b>     | <b>22</b> |
| 2.1 Svindel                         | 24        |
| 2.2 Oppdagelsesrisiko og holdninger | 25        |
| <hr/>                               |           |
| <b>3 Anmeldelser</b>                | <b>28</b> |
| 3.1 Lovbrudd som ikke anmeldes      | 30        |
| 3.2 Utro tjenere                    | 32        |
| <hr/>                               |           |
| <b>4 Kameraovervåking og vold</b>   | <b>34</b> |
| 4.1 Kameraovervåking                | 36        |
| 4.2 Vold mot ansatte                | 38        |
| <hr/>                               |           |
| <b>Perspektiver</b>                 | <b>40</b> |

# Sammendrag

Dette er den niende utgaven av Kriminalitets- og sikkerhetsundersøkelsen i Norge – KRISINO. Undersøkelsen ble gjennomført første gang i 2006, og gjentatt årlig fram til 2009. Etter 2009 er KRISINO gjennomført annen hvert år. Undersøkelsen bygger på et utvalg ledere og sikkerhetsansvarlige i 2000 private og 500 offentlige virksomheter.

## Sikkerhet

Andelen virksomheter som har en skriftlig risikovurdering av kriminalitet i eller mot virksomheten holder seg stabilt sammenlignet med 2017 etter at det har vært en økning fra 2009 og fram til 2017. Mens det i 2009 var 20 prosent av virksomhetene som hadde en slik risikovurdering, falt det til 16 prosent i 2013 før det økte til 23 prosent i 2015. I 2017 og 2019 er tilsvarende tall 28 prosent. Som i 2017 er det også i 2019 klar forskjell på privat og offentlig sektor. 53 prosent av offentlige virksomheter har risikovurdering, mot 22 prosent av de private.

I 17 prosent av virksomhetene er det en eller flere som har lest PSTs trusselvurdering, mens tilsvarende tall for NSMs risikovurdering er 10 prosent. Begge leses i noe større grad i offentlige virksomheter enn i private og i store virksomheter i større grad enn i små. Blant de som har lest trusselvurderinger er det 58 prosent som har vurdert aktuelle trusler relatert til egen virksomhet og av disse er det igjen 70 prosent som har iverksatt tiltak som følge av aktuelle trusler.

## Økonomisk kriminalitet

43 prosent av virksomhetene har i løpet av de siste 12 månedene fått faktura for varer som ikke er bestilt, 15 prosent har blitt utsatt for løsepengevirus og 13 prosent direktørsvindel. Svindel i form av misbruk av merkevare/logo er mindre omfattende og er noe 5 prosent av virksomhetene har opplevd.

39 prosent mener det er liten sjans for at virksomheter som bryter regler, eller gir feilaktige opplysninger om inntekter og utgifter blir oppdaget av myndighetene. Det er spesielt i bygg/anlegg, industri og varehandel at man mener risikoen for å bli oppdaget er liten.

85 prosent ville valgt bort billigste leverandør dersom det var mistanke om at den billigste benytter ulovlige lønns og arbeidsforhold, mens 7 prosent ville ikke valgt bort den billigste. 82 prosent ville valgt bort billigste leverandør hvis det var mistanke om unndragelse av skatter og avgifter, mens 9 prosent ikke ville gjort det.



### Anmeldelser

10 prosent av virksomhetene har i løpet av det siste året opplevd lovbrudd som de ikke har anmeldt. Det er identisk med 2017. Det er spesielt vinningskriminalitet som ikke anmeldes (58 prosent), mens 19 prosent av de som ikke anmeldte er utsatt for kriminalitet i digitale rom og 14 prosent for økonomisk kriminalitet. Viktigste årsak til at disse virksomhetene ikke anmeldte forholdene er at de mener politiet som regel henlegger saken.

### Sikringskamera

31 prosent av virksomhetene har sikringskamera. En av ti av de som har kamera har i løpet av de siste 12 månedene opplevd at uønskede hendelser ikke kan dokumenteres fordi opptaket er slettet når hendelsen oppdages. Av disse igjen, mener nær halvparten at det at opptaket var slettet hadde betydning for om forholdet ble anmeldt eller ikke.

### Vold mot ansatte

I 13 prosent av virksomhetene har man opplevd at en eller flere ansatte er utsatt for vold eller trusler om vold. Mens det er 4 prosent av private som har opplevd dette, er det hele 49 prosent av offentlige virksomheter som har opplevd vold eller trusler om vold. Det skjer i størst grad i helse og sosial, der 63 prosent av virksomhetene opplever at ansatte er blitt utsatt for vold eller trusler om vold.



# Innledning

## Bakgrunn

I samarbeid med Næringslivets Sikkerhetsråd har Opinion gjennomført Kriminalitets- og sikkerhetsundersøkelsen i Norge - KRISINO™ for niende gang. Undersøkelsen bygger på en spørreundersøkelse blant 2500 virksomheter i privat og offentlig sektor.

## Populasjon

Populasjonen for denne undersøkelsen er norske bedrifter i privat sektor og virksomheter i offentlig sektor. Utvalget bedrifter i privat sektor inkluderer enheter (bedrifter) med minst 1 ansatt i NACE-koder 01-82. Det offentlige utvalget er trukket på NACE-koder 84-93 og vasket for å fjerne private bedrifter som faller inn under disse NACE-kodene. Private bedrifter som hører inn under NACE-kode høyere enn 82 er ikke representert i undersøkelsen. Undersøkelsens utvalg er trukket fra Bisnodes database. Disse er hentet fra Enhetsregisteret.

Det er gjort to utvalg i undersøkelsen, ett for private bedrifter (2000) og ett for offentlige virksomheter (500). Det offentlige utvalget er et rent tilfeldighetsutvalg, men barnehager og grunnskoler er holdt utenfor. I den private delen er det gjort et stratifisert utvalg, med fire gjensidig utelukkende strata:

- Virksomheter med 1 til 4 ansatte
- Virksomheter med 5 til 19 ansatte
- Virksomheter med 20 til 99 ansatte
- Virksomheter med 100 ansatte eller flere

I hvert stratum er det gjort et enkelt tilfeldig utvalg.

Resultatene blant de private virksomhetene er vektet på geografi, bransje og størrelse med utgangspunkt i de riktige populasjonsstørrelsene (basert på Bedrifts- og Foretaksregisteret (BoF) i Statistisk Sentralbyrå).

## Datainnsamling

Datainnsamling er gjennomført ved hjelp av telefonintervjuer (CATI), i perioden 29. april til 3. juni 2019.

## Feilmarginer

Opinion gjør oppmerksom på at enhver undersøkelse vil være beheftet med feilmarginer. Feilmarginene knytter seg i hovedsak til statistisk usikkerhet. Dette er utvalgsskjevheter, som medfører at utvalget ikke er identisk med universet eller målgruppen. Ulikheter kan knytte seg til bestemte kjennetegn eller atferd.

Ved 2500 respondenter eller intervjuer ( $n=2500$ ) kan vi med 95 % sannsynlighet si at det riktige resultatet ligger innenfor  $\pm 0,9$  og  $\pm 2,0$  prosentpoeng, avhengig av prosentresultatets størrelse. Usikkerheten er størst ved et prosentresultat på 50 % og minst ved prosentresultater på 5%/95%.





## Karakteristika

Respondentene i undersøkelsen har følgende fordeling mellom privat og offentlig sektor:

| Sektor    | Antall (n) | Andel Intervju |
|-----------|------------|----------------|
| Privat    | 1996       | 80,0 %         |
| Offentlig | 504        | 20,0 %         |
| Totalt    | 2500       | 100,0 %        |

## Geografi

Under er en oversikt over respondentenes fylkesvise tilhørighet:

| Fylke            | Privat sektor | Offentlig sektor | Antall Intervju (n) | Andel Intervju |
|------------------|---------------|------------------|---------------------|----------------|
| Østfold          | 117           | 19               | 136                 | 5,4 %          |
| Akershus         | 249           | 34               | 283                 | 11,3 %         |
| Oslo             | 301           | 52               | 353                 | 14,1 %         |
| Hedmark          | 55            | 21               | 76                  | 3,0 %          |
| Oppland          | 72            | 22               | 94                  | 3,8 %          |
| Buskerud         | 123           | 24               | 147                 | 5,9 %          |
| Vestfold         | 108           | 20               | 128                 | 5,1 %          |
| Telemark         | 76            | 31               | 107                 | 4,3 %          |
| Aust-Agder       | 27            | 11               | 38                  | 1,5 %          |
| Vest-Agder       | 56            | 16               | 72                  | 2,9 %          |
| Rogaland         | 144           | 44               | 188                 | 7,5 %          |
| Hordaland        | 189           | 56               | 245                 | 9,8 %          |
| Sogn og Fjordane | 38            | 16               | 54                  | 2,2 %          |
| Møre og Romsdal  | 104           | 26               | 130                 | 5,2 %          |
| Trøndelag        | 161           | 41               | 202                 | 8,1 %          |
| Nordland         | 84            | 34               | 118                 | 4,7 %          |
| Troms            | 62            | 24               | 86                  | 3,4 %          |
| Finnmark         | 30            | 13               | 43                  | 1,7 %          |
| Totalt           | 1996          | 504              | 2500                | 100 %          |

## Virksomhetsstørrelse

Undersøkelsen omfatter virksomheter i alle størrelsesgrupper.

| Virksomhetsstørrelse    | Privat sektor | Offentlig sektor | Antall Intervju (n) | Andel Intervju |
|-------------------------|---------------|------------------|---------------------|----------------|
| 1 til 4 ansatte         | 664           | 32               | 676                 | 27,0 %         |
| 5 til 19 ansatte        | 860           | 99               | 959                 | 38,4 %         |
| 20 til 99 ansatte       | 378           | 205              | 583                 | 23,3 %         |
| 100 ansatte eller flere | 114           | 168              | 282                 | 11,3 %         |
| Totalt                  | 1996          | 504              | 2500                | 100 %          |

## Bransje

Undersøkelsen omfatter virksomheter i følgende bransjer:

| Bransje             | Privat sektor | Offentlig sektor | Antall Intervju (n) | Andel Intervju |
|---------------------|---------------|------------------|---------------------|----------------|
| Industri etc.       | 338           |                  | 338                 | 13,5 %         |
| Bygg og anlegg      | 216           |                  | 216                 | 8,6 %          |
| Varehandel          | 720           |                  | 720                 | 28,8 %         |
| Transport/lagring   | 77            |                  | 77                  | 3,1 %          |
| Hotell/restaurant   | 111           |                  | 111                 | 4,4 %          |
| Tjenesteytende      | 534           |                  | 534                 | 21,4 %         |
| Off. administrasjon |               | 163              | 163                 | 6,5 %          |
| Undervisning        |               | 103              | 103                 | 4,1 %          |
| Helse og sosial     |               | 238              | 238                 | 9,5 %          |
| Totalt              | 1996          | 504              | 2500                | 100 %          |

# 1. Sikkerhet

Temaet sikkerhet dekker blant annet risikovurdering i virksomheten, bakgrunnsjekk av potensielle samarbeidspartnere og kontrolltiltak i forbindelse med ansettelser.





# 1. Sikkerhet

## 1.1 Risikovurdering

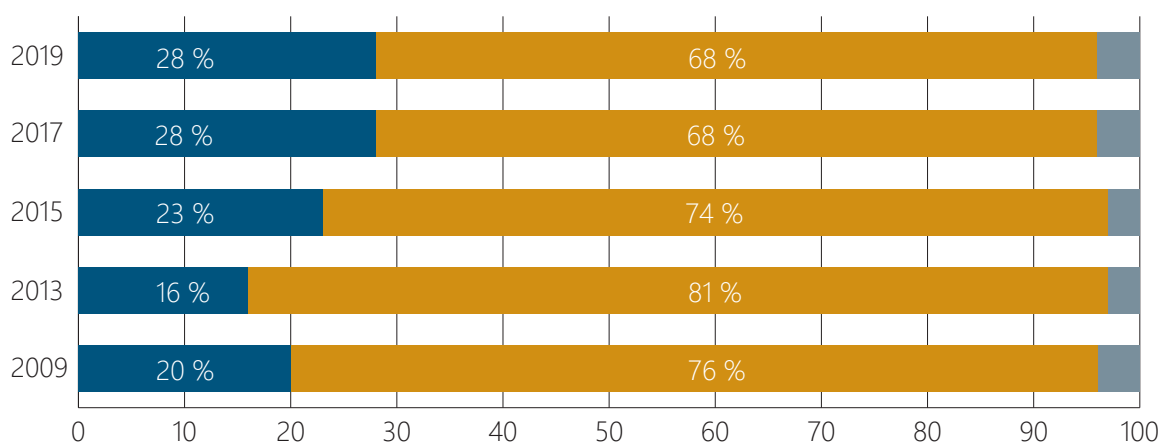
Andelen virksomheter som har en skriftlig risikovurdering holder seg stabil fra 2017. Nær 3 av 10 virksomheter har en skriftlig risikovurdering. Fra 2015 til 2017 økte denne andelen med 5 prosentpoeng og med 12 prosentpoeng fra 2013.

### **Spørsmål: Har virksomheten en skriftlig risikovurdering av kriminalitet i eller mot virksomheten?**

Det er langt større andel av offentlige virksomheter som har en skriftlig risikovurdering enn tilfellet er blant de private virksomhetene. 53 prosent av de offentlige virksomhetene har skriftlig risikovurdering, mens tilsvarende blant de private er 22 prosent. I 2017 var det henholdsvis 46 og 24 prosent som svarte det samme.

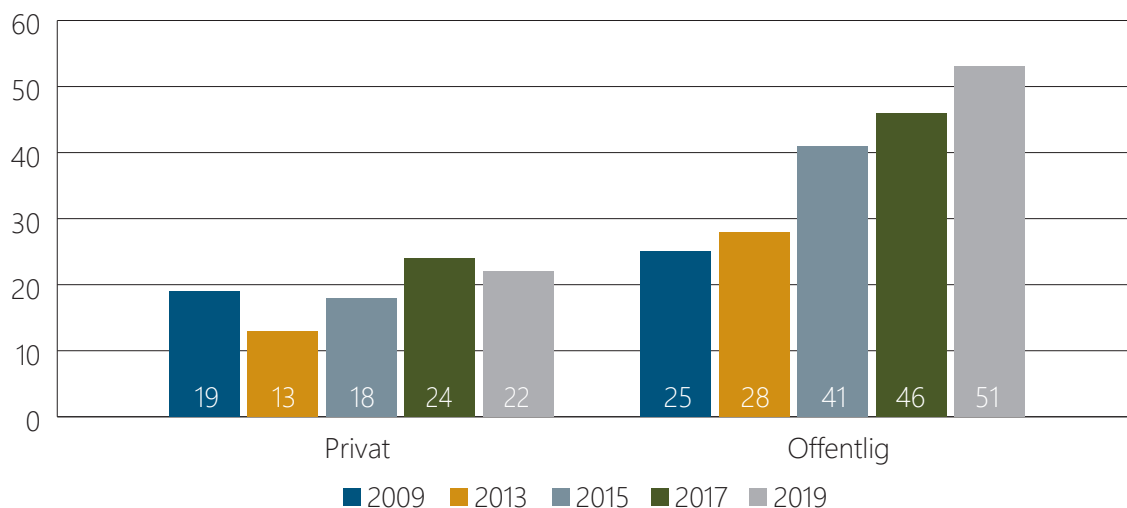
Sammenlignet med 2017, er det en signifikant økning blant virksomheter i offentlig sektor som har skriftlig risikovurdering, mens utviklingen i privat sektor er flat sammenlignet med 2017 (forskjellen er ikke statistisk signifikant).

Figur 1 Skriftlig risikovurdering (n=2500)



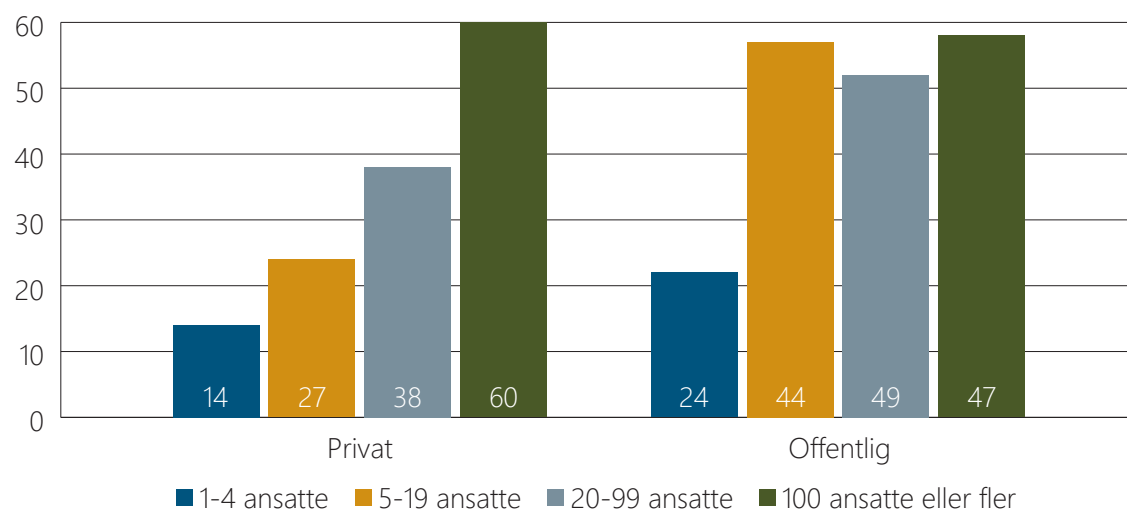


Figur 2 Andeler som har skriftlig risikovurdering



Størrelse på virksomheten spiller en stor rolle, og den gruppen som i størst grad har skriftlig risikovurdering er store private virksomheter med 100 ansatte eller flere. Resultatene i privat sektor er nær identisk med 2017, mens det er en økning i de tre største størrelsesgruppene i offentlig sektor.

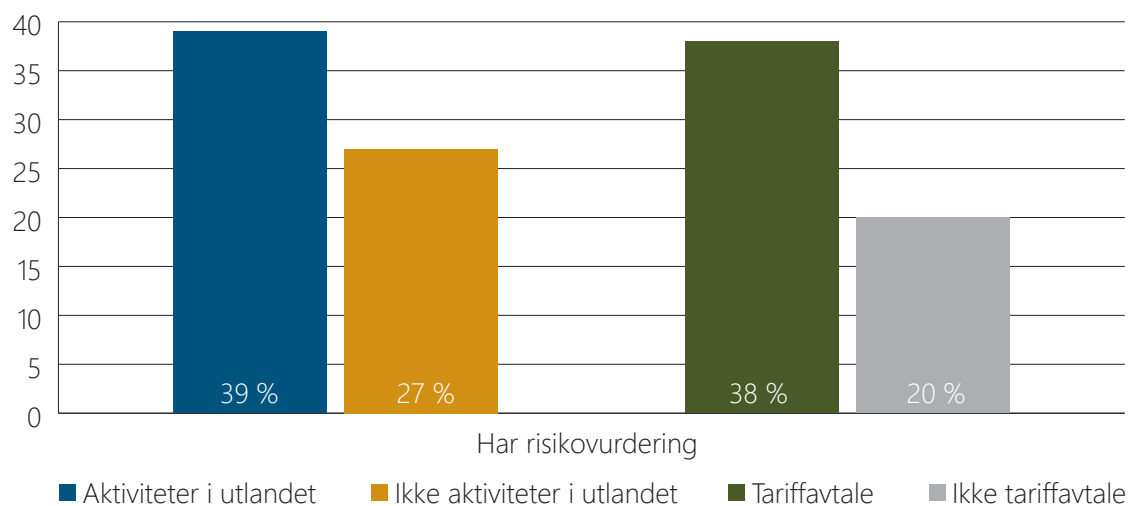
Figur 3 Risikovurdering og størrelse på virksomheten



Virksomheter som er omfattet av tariffavtale har i større grad enn andre en skriftlig risikovurdering, det samme er tilfelle med virksomheter som har aktiviteter i utlandet. Dette er i tråd med funn fra 2013, 2015 og 2017.

# 1. Sikkerhet

Figur 4 Andel bedrifter med risikovurdering - aktiviteter i utlandet og tariffavtale



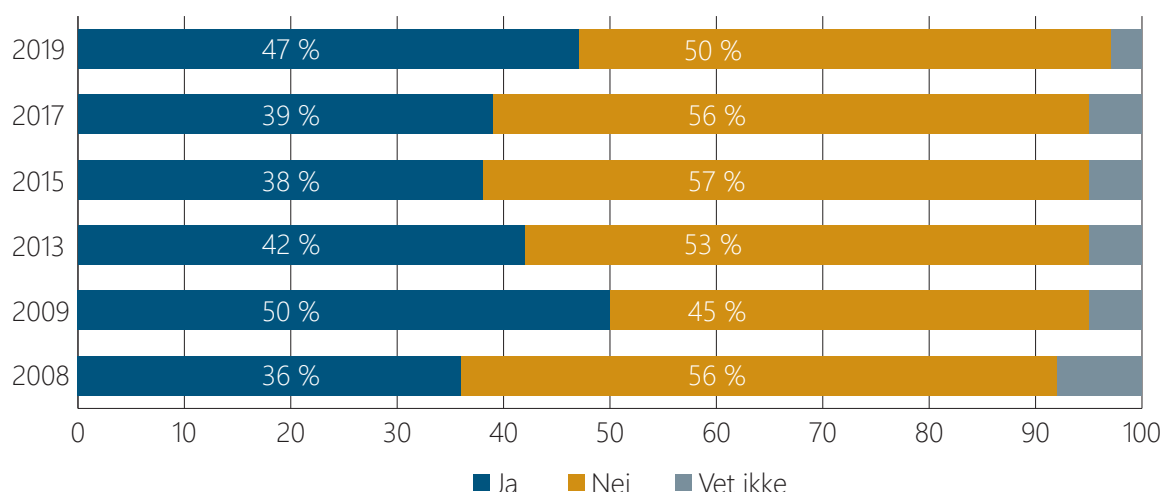
Det er i bransjene bygg og anlegg, industri og varehandel at virksomhetene i minst grad har en skriftlig risikovurdering, mens det i størst grad forekommer i offentlig administrasjon, undervisning og helse og sosial. Blant de «private» bransjene er det tjenesteytende, transport og overnatting/servering som i størst grad har skriftlig risikovurdering. Dette er samme bilde som i 2017.

De som har svart at de har en skriftlig risikovurdering har fått oppfølgingsspørsmål om når denne er utarbeidet og revidert. 17 prosent av virksomhetene opplyser at risikovurderingen er utarbeidet for første gang siste 12 måneder, mens 64 prosent har revidert den siste 12 måneder.

De som har en skriftlig risikovurdering har fått et ytterligere oppfølgingsspørsmål om risikovurderingen har medført at det ble iverksatt tiltak mot kriminalitet. I 47 prosent av virksomheter som har en skriftlig risikovurdering, har vurderingen resultert i at det har blitt iverksatt tiltak mot kriminalitet. Dette er en oppgang fra 2017 og på nivå med 2009.

**Spørsmål: Medførte denne risikovurderingen at det ble iverksatt konkrete tiltak mot kriminalitet i din virksomhet?**

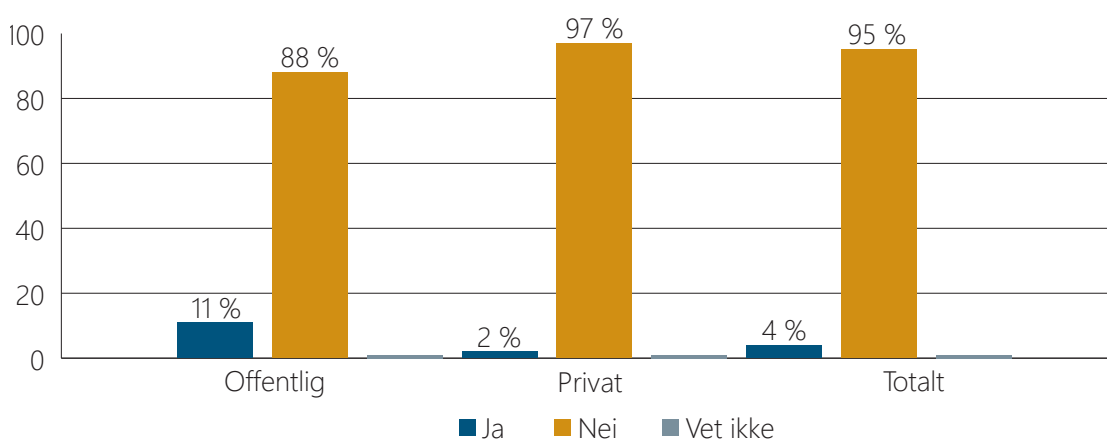
Figur 5 Tiltak mot kriminalitet som følge av risikovurdering (n=710)



Et spørsmål som ble stilt første gang i 2013 er hvorvidt virksomheten har én eller flere ansatte som arbeider fulltid med kriminalitetsforebygging og sikkerhet. I løpet av de siste to årene har andelen med slike ansatte holdt seg stabil.

**Spørsmål: Har din virksomhet én eller flere ansatte som arbeider fulltid med kriminalitetsforebygging og/eller sikkerhet? (Vi tenker her ikke på sikkerhet i forbindelse med HMS-arbeid, men sikkerhet i et kriminalitetsperspektiv.)**

Figur 6 Ansatt som arbeider med kriminalitetsforebygging og/eller sikkerhet

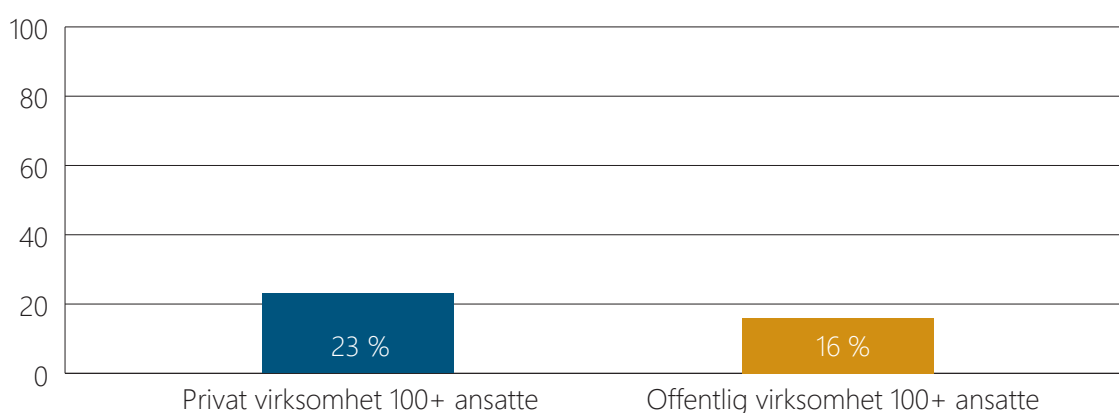




# 1. Sikkerhet

I offentlig sektor er det virksomheter innen offentlig administrasjon som i størst grad har ansatte som arbeider med kriminalitetsforebygging og sikkerhet (11 prosent). Blant store private virksomheter er det imidlertid større andel som har sikkerhetsansatte enn tilfellet er i store offentlige virksomheter. 23 prosent av private virksomheter med 100 ansatte eller flere har heltidsansatte i slike stillinger, mens tilsvarende for offentlige virksomheter med 100 ansatte eller flere er 16 prosent.

Figur 7 Ansatt som arbeider med kriminalitetsforebygging og/eller sikkerhet – 100 ansatte eller flere



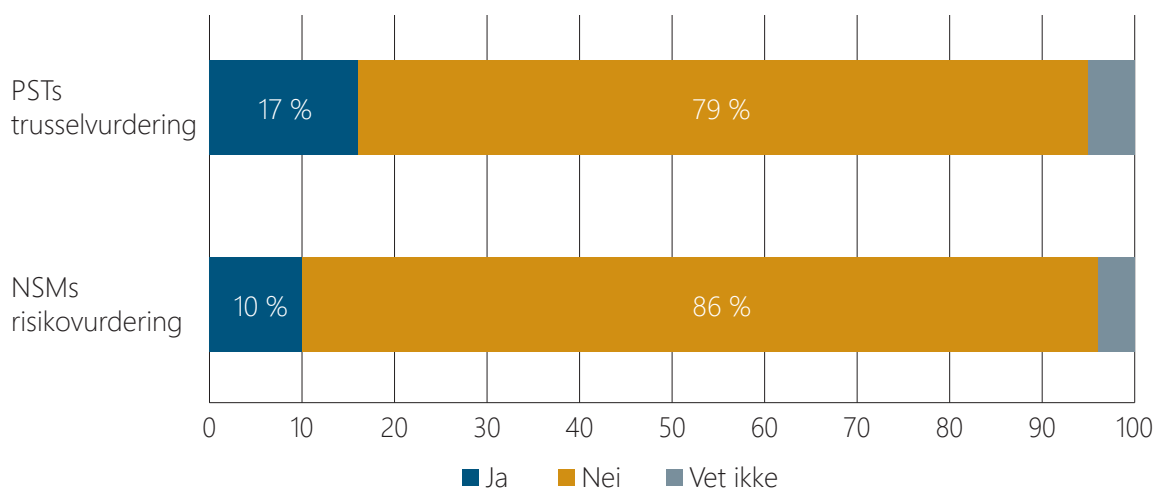
Den gruppen som i størst grad har heltidsansatte i slike stillinger er store private virksomheter.

## 1.2 Trusselvurdering

17 prosent har lest PSTs åpne sikkerhetsvurdering og 10 prosent har lest NSMs risikovurdering. Det er på nivå med 2017 da det var henholdsvis 16 og 11 prosent som svarte det samme.

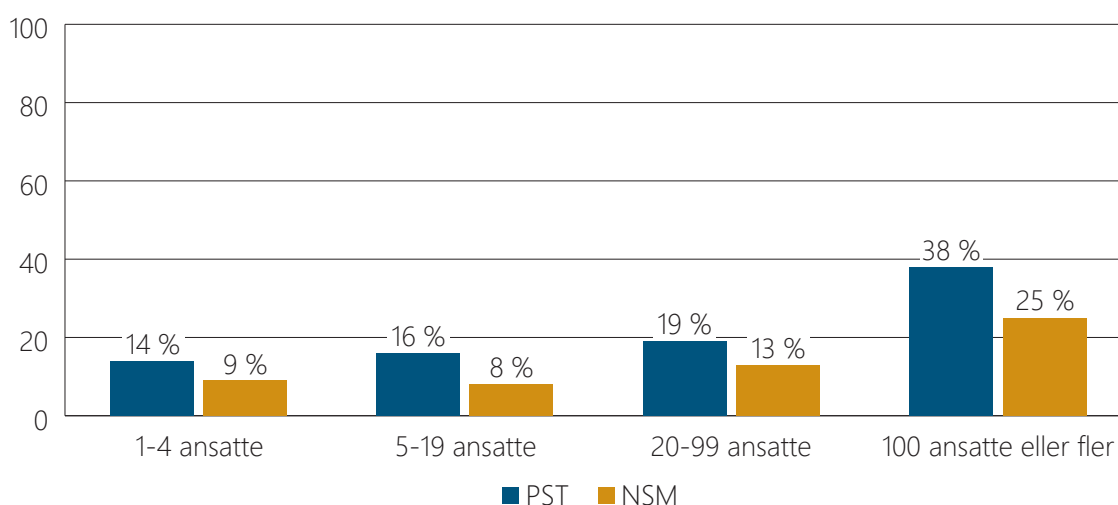
**Spørsmål: Har du eller andre i din virksomhet lest noen av følgende:**

Figur 8 Lest PSTs trusselvurdering/NSMs risikovurdering (n=2500)



I privat sektor er det 15 prosent som har lest PSTs trusselvurdering, mot 26 prosent i offentlig sektor. Tilsvarende for NSMs risikovurdering er 8 og 19 prosent. Det er nær identisk med 2017. Det er forskjell på små og store virksomheter på dette spørsmålet og mønsteret er det samme i privat som i offentlig sektor.

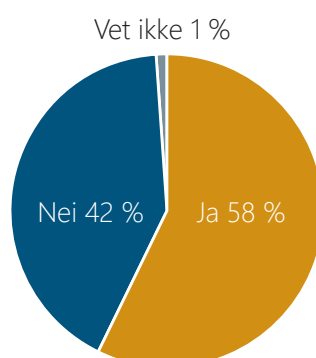
Figur 9 Andel som har lest PSTs åpne trusselvurdering/NSMs risikovurdering



De som har lest enten PSTs åpne trusselvurdering eller NSMs risikovurdering har fått spørsmål om de har vurdert aktuelle trusler på bakgrunn av trusselvurderingen. 58 prosent har vurdert aktuelle trusler relatert til egen virksomhet basert på trusselvurderingene. Virksomheter med 20 ansatte eller flere gjør dette i større grad enn mindre virksomheter og virksomheter i offentlig sektor i større grad enn de i privat sektor (72 vs. 51 prosent). Virksomheter med aktiviteter i utlandet gjør det mer enn de uten utenlandsaktiviteter (69 vs. 51 prosent).

**Spørsmål: Basert på trusselvurderingen(e), har din virksomhet vurdert aktuelle trusler relatert til egen virksomhet?**

Figur 10 Vurdert aktuelle trusler (n=2500)

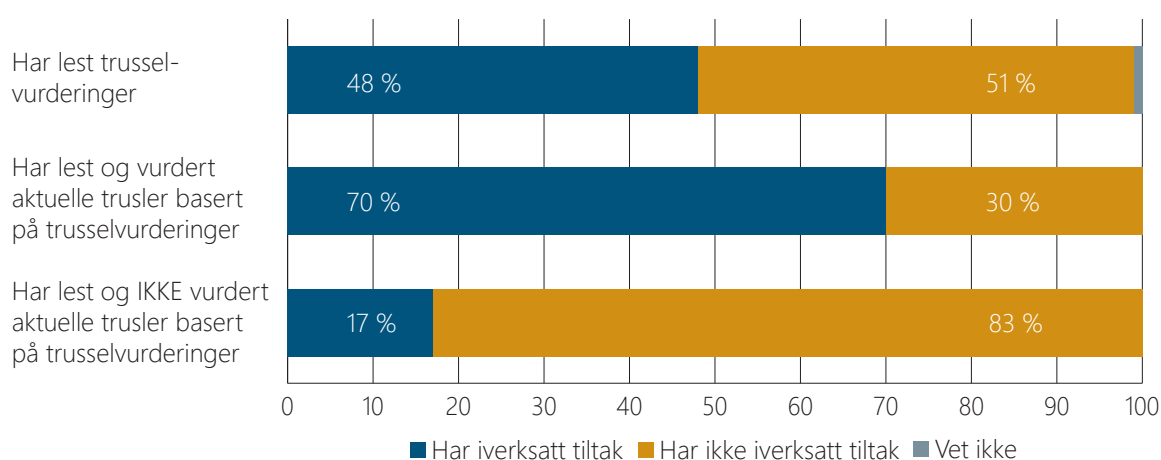


# 1. Sikkerhet

Blant de som har lest PSTs åpne trusselvurdering eller NSMs risikovurdering er det 48 prosent som har iverksatt tiltak som følge av aktuelle trusler. Blant de som har vurdert aktuelle trusler relatert til egen virksomhet, er det 70 prosent som har iverksatt tiltak som følge av aktuelle trusler.

## Spørsmål: Har din virksomhet iverksatt tiltak som følge av aktuelle trusler?

Figur 11 Iverksatt tiltak som følge av aktuelle trusler (n=535)

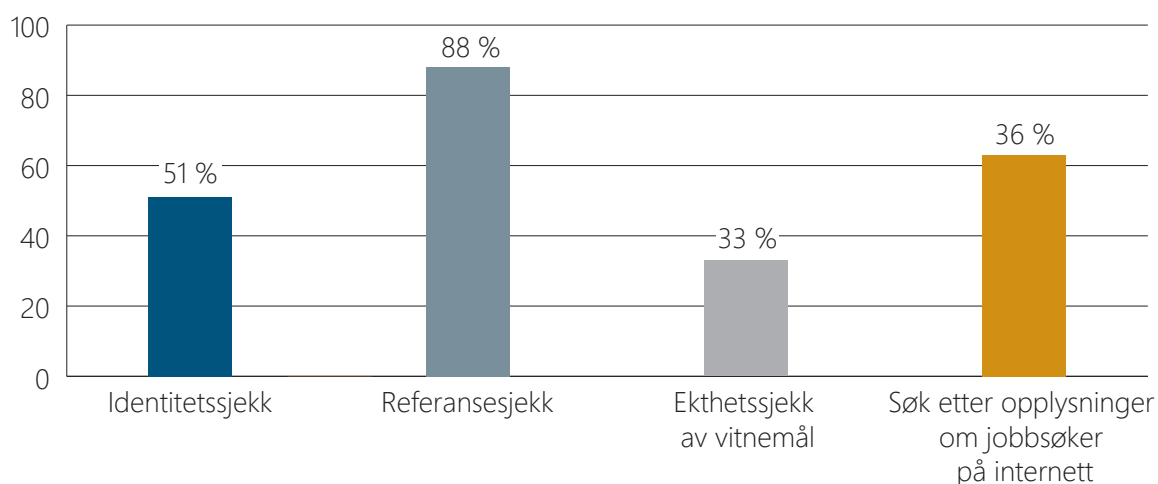


## 1.3 Kontrolltiltak ved ansettelser

Når det gjelder kontrolltiltak ved ansettelser er spørsmålet stilt på en litt annen måte i 2019 enn ved tidligere undersøkelser. Vi skal derfor være forsiktig med direkte sammenligninger. Et trekk vi kan si er på linje med tidligere er at referansesjekk er det vanligste kontrolltiltaket.

## Spørsmål: Gjør din virksomhet rutinemessig følgende i ansettelsesprosesser?

Figur 12 Kontroll ved ansettelser (andel som svarer ja) (n=2500)

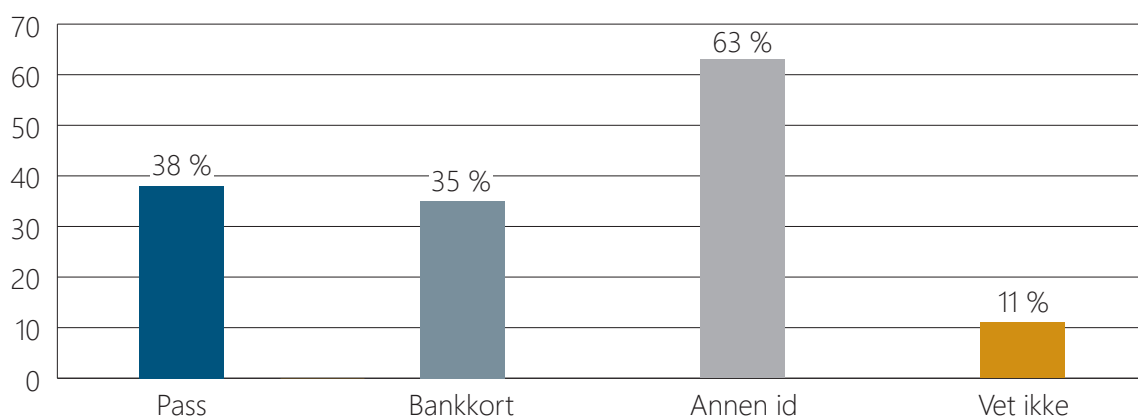


Identitetssjekk, referansesjekk og ekthetskontroll gjøres i større grad i offentlige virksomheter enn i private, mens det ikke er noen forskjell når det gjelder å søke etter opplysninger på internett.

Identitetssjekk gjøres i størst grad innen transport/lagring, offentlig administrasjon og helse/sosial. Referansesjekk gjøres i størst grad i offentlig administrasjon og helse/sosial. Ekthetskontroll av vitnemål er mest vanlig i transport/lagring, offentlig administrasjon, undervisning og helse/sosial, mens det ikke er klare mønstre når det gjelder søk på internett utover at bygg og anlegg gjør det i noe mindre grad enn andre.

De som rutinemessig utfører identitetssjekk er spurt om hvilken dokumentasjon som benyttes som identitetssjekk. Pass og bankkort er brukt i like stor grad, men det er en annen dokumentasjon enn disse to som i størst grad benyttes.

Figur 13 Identitetssjekk (n=1284) Flere svar mulig





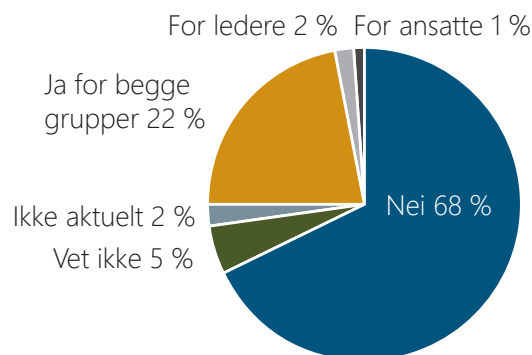
# 1. Sikkerhet

## 1.4 Digital reisesikkerhet

For første gang er det i 2019-undersøkelsen spurt om digital reisesikkerhet.

**Spørsmål: Har din virksomhet retningslinjer for digital reisesikkerhet for ansatte og/eller ledere?**

Figur 14 Digital reisesikkerhet (n=2500)



25 prosent har retningslinjer for digital reisesikkerhet enten for ansatte, ledere eller for begge grupper, mens det er 68 prosent av virksomhetene som ikke har det. Blant virksomheter i privat sektor er det 22 prosent som har retningslinjer, mens 36 prosent av de offentlige virksomhetene svarer det samme. 49 prosent av virksomheter med aktiviteter i utlandet har retningslinjer, men også i denne gruppen er det nesten halvparten som ikke har retningslinjer (47 prosent).

Blant virksomheter med 1 til 4 ansatte er det 80 prosent som ikke har retningslinjer, mens 45 prosent av virksomheter med 100 ansatte eller flere svarer det samme. Når det gjelder bransje er det 83 prosent av virksomhetene i bygg og anlegg som ikke har retningslinjer, og kun 10 prosent som har det. I motsatt ende er offentlig administrasjon er det 47 prosent som ikke har retningslinjer, mens 41 prosent har det.





## 2. Økonomisk kriminalitet

Under dette tema er virksomhetene spurt om forhold som blant annet svindel, prissamarbeid, korrupsjon og sannsynligheten for å bli oppdaget hvis man unnlater å rapportere alle skatter og avgifter.







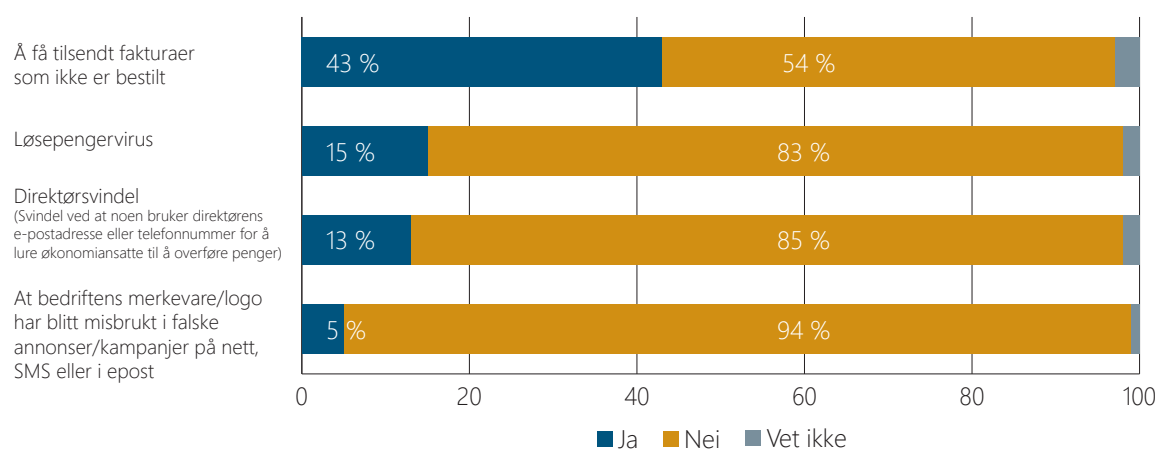
## 2. Økonomisk kriminalitet

### 2.1 Svindel

Spørsmål relatert til svindel er endret i 2019 og omfatter også enkelte forhold som ikke er spurt om tidligere.

**Spørsmål: Har din virksomhet i løpet av de siste 12 månedene blitt utsatt for følgende?**

Figur 15 Svindelforsøk (n=2500)



43 prosent har i løpet av de siste 12 månedene opplevd å få tilsendt faktura for varer som ikke er bestilt. Det klare skillet går mellom private og offentlige virksomheter, der 47 prosent av de private og 28 prosent av de offentlige har opplevd dette. Virksomheter med 1-4 ansatte er noe mindre utsatt enn større virksomheter, men også blant de minste virksomhetene er det 34 prosent som er blitt utsatt for dette.

15 prosent er utsatt for løsepengervirus i løpet av de siste 12 månedene. Private er mer utsatt enn offentlige. Industri/tjenesteytende mer enn bygg/anlegg, undervisning, helse/sosial. Industri og tjenesteytende skiller seg ikke signifikant fra alle andre bransjer.

13 prosent er utsatt for direktørsvindel. Også på dette forholdet er det mer vanlig blant private enn blant offentlige. Den klareste forskjellen er det imidlertid på størrelse. Mens kun 6 prosent av de minste virksomhetene er utsatt for dette, er det 27 prosent av de med 100 ansatte eller flere som utsettes for direktørsvindel. Ser vi på private bedrifter med 100 ansatte eller flere er det 50 prosent som er utsatt for det mens tilsvarende i store offentlige virksomheter er 20 prosent (merk base på 48 virksomheter i privat sektor).

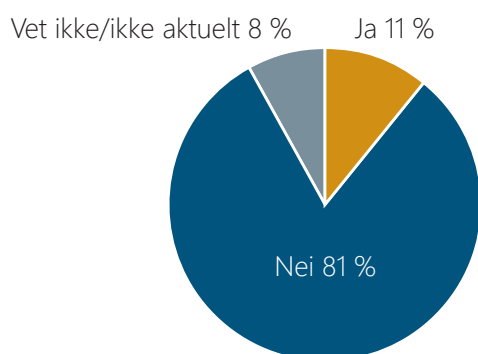


Av de fire forholdene som det er spurt om, er misbruk av merkevare/logo minst utbredt. 5 prosent har opplevd dette siste 12 måneder. Dette er like utbredt blant offentlig som blant private virksomheter. Dette rammer alle bransjer, men i mindre grad i tjenesteytende, undervisning og helse/sosial enn i andre bransjer.

Av de virksomhetene som har opplevd en eller flere av de fire svindelmethodene spurt om, er det 11 prosent som anmeldte ett eller flere forhold.

**Spørsmål: Ble svindelen eller forsøket på svindel politianmeldt?**  
**Dersom virksomheten er utsatt for dette flere ganger, svar ut fra siste hendelse.**

Figur 16 Anmeldt svindelforsøk (n=1325)



Store virksomheter anmelder svindelforsøkene i større grad enn små virksomheter. Mens det er 8 prosent av virksomheter med 1 til 4 ansatte som gjør det, er det 19 prosent av de med 100 ansatte eller flere som anmelder. Samtidig er det slik at offentlige virksomheter i større grad enn private anmelder (i alle størrelsesgrupper).

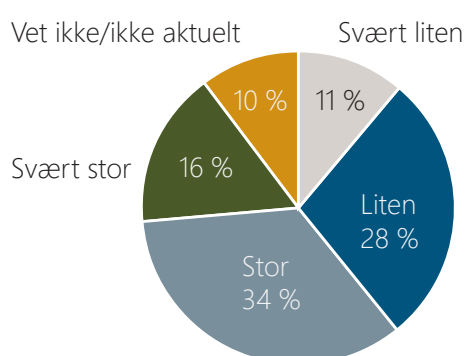
## 2.2 Oppdagelsesrisiko og holdninger

I hvilken grad man oppfatter sjansen for å bli oppdaget hvis man unnlater å rapportere inn alle skatter og avgifter er et forhold som er målt i samtlige KRISINO-undersøkelser. I årets undersøkelse er spørsmålet endret noe fra tidligere år. Mens vi tidligere har spurt om faren for å bli oppdaget hvis man unnlater å rapportere inn alle skatter og avgifter, er det i år spurt om hva oppdagelsesfaren er hvis man bryter regelverket i egen bransje eller gir feilaktige opplysninger om virksomhetens inntekter og utgifter. Mens tidligere spørsmål er spisset mot skattebetaling og oppdagelse av skattemyndighetene, peker årets spørsmål mer på en generell oppdagelsesrisiko.

## 2. Økonomisk kriminalitet

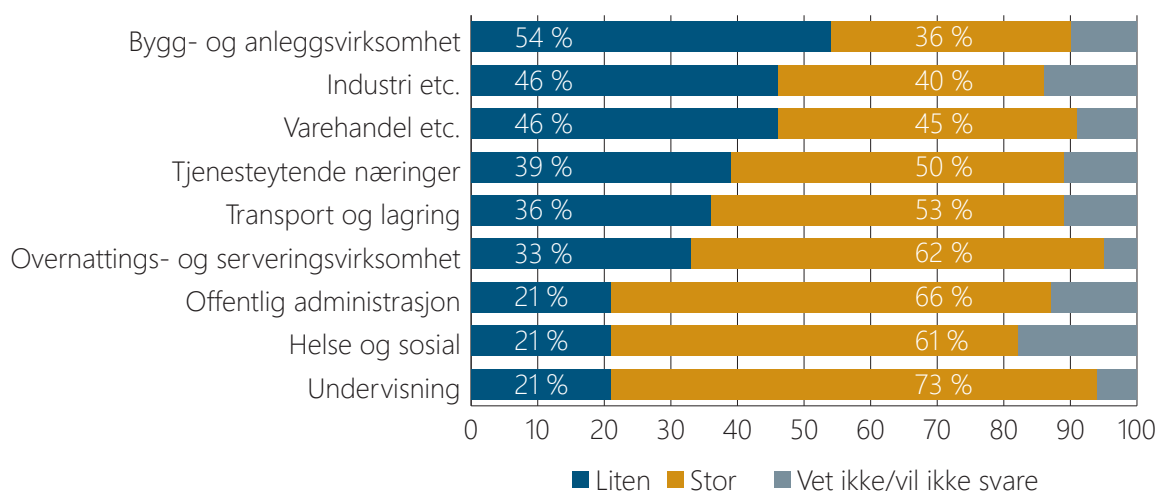
**Spørsmål: Dersom en virksomhet bryter regelverket i din bransje, eller gir feilaktige opplysninger om virksomhetens inntekter og utgifter, hvor stor sjanse tror du det er for at myndighetene vil oppdage det. Er den svært liten, liten, stor eller svært stor?**

Figur 17 Risiko for å bli oppdaget av myndighetene (n=2500)



Halvparten mener at det er stor eller svært stor sjanse for å bli oppdaget av myndighetene ved regelbrudd eller feilaktige opplysninger om inntekter og utgifter. Private virksomheter svarer i større grad at det er liten sjanse for å bli oppdaget enn tilfellet er blant offentlige, og det er spesielt i bygg/anlegg, industri og varehandel av man mener risikoen for å bli oppdaget er liten.

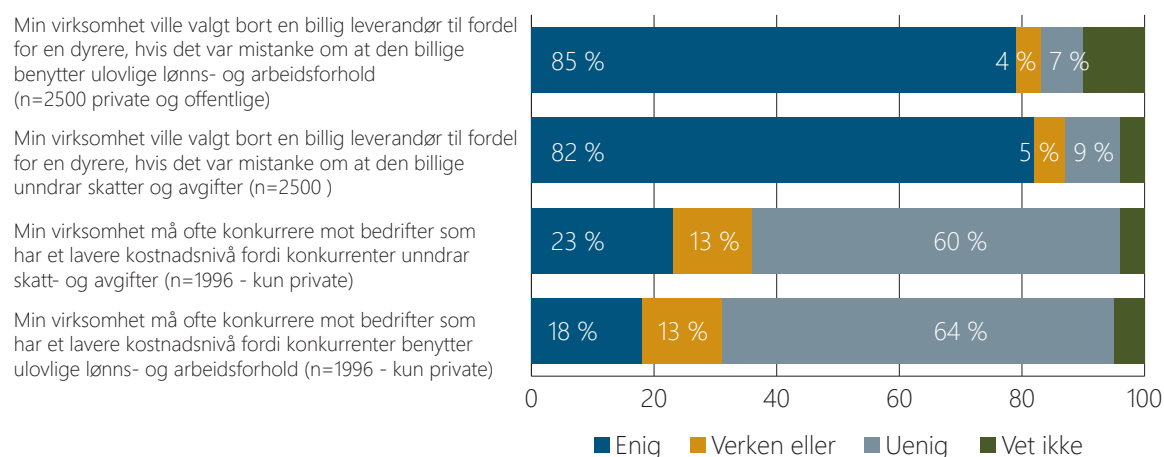
Figur 18 Oppfattelsen av oppdagelsesrisiko i ulike bransjer (svært liten og liten er slått sammen til liten, svært stor og stor er slått sammen til stor)



På spørsmål om hva man ville gjort dersom man har mistanke om at billigste leverandør unndrar skatter og avgifter eller har ulovlige lønns- og arbeidsforhold, er det henholdsvis 82 og 85 prosent som ville valgt bort slike leverandører.

**Spørsmål: Jeg vil nå lese opp noen påstander, og ønsker at du på vegne av din virksomhet oppgir hvor enig eller uenig du er i de enkelte påstandene. Jeg ber deg bruke en skal fra 1 til 5, der 1 er helt uenig og 5 er helt enig.**

Figur 19 Unndragelse av skatter og avgifter



Både når det gjelder å velge bort billigste leverandør på grunn av ulovlige lønns- og arbeidsforhold og unndragelse av skatter og avgifter, skiller industri, bygg/anlegg og varehandel seg fra overnatting/servering. I de tre førstnevnte bransjen er det høyere andel som vil velge bort billigste leverandør enn tilfellet er i overnatting/servering.

Å måtte konkurrere mot konkurrenter med lavere kostnadsnivå på grunn av unndragelse av skatter og avgifter er det 23 prosent som opplever, og i størst grad bedrifter innen bygg og anlegg og transport. Den samme bransjeforskjellen finner vi når det gjelder å konkurrere mot andre som har lavere kostnadsnivå på grunn av ulovlige lønns- og arbeidsforhold.

# 3. Anmeldelser

Dette temaet dekker anmeldelsevilje, type kriminalitet, herunder utro tjenere og grunner til ikke å anmelde straffbare forhold.





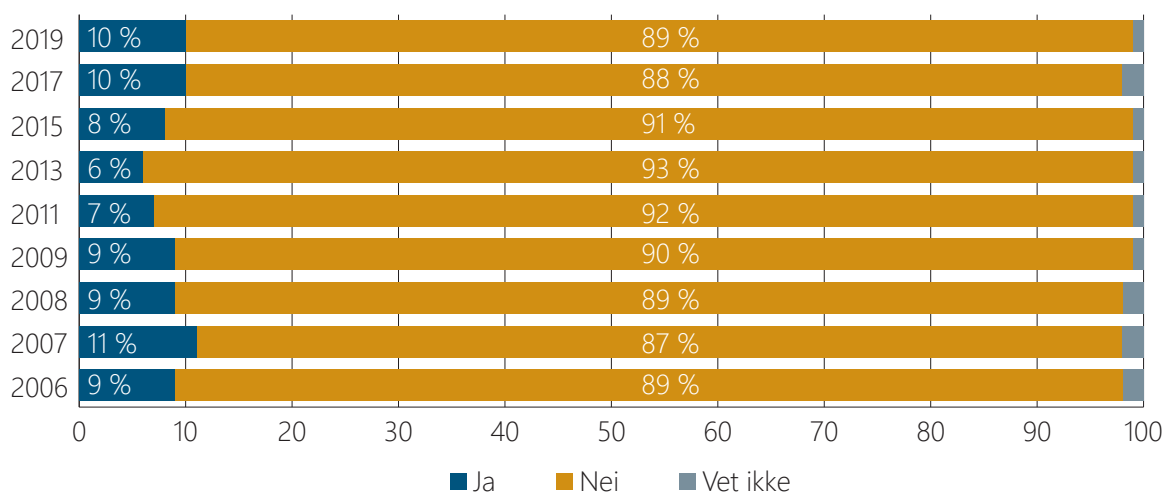
## 3. Anmeldelser

### 3.1 Lovbrudd som ikke anmeldes

Spørsmål om virksomheten har blitt utsatt for lovbrudd som ikke anmeldes har blitt stilt i samtlige KRISINO-undersøkelser.

**Spørsmål: Har din virksomhet de siste 12 månedene vært utsatt for lovbrudd som dere ikke anmeldte?**

Figur 20 Lovbrudd som ikke anmeldes (n=2502)

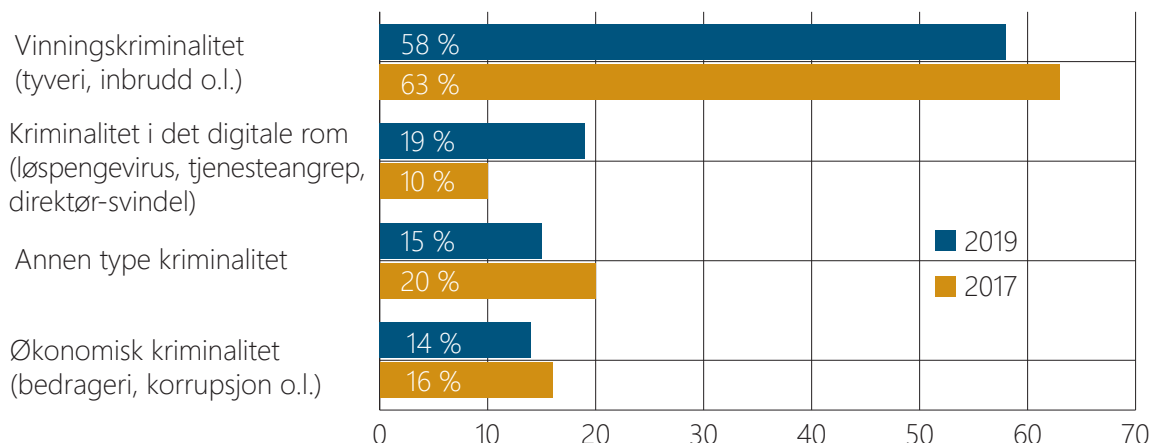


10 prosent av virksomhetene har i løpet av det siste året opplevd lovbrudd som de ikke har anmeldt. Denne andelen har holdt seg stabil de siste målingene, men det er svak økende trend fra 2013. Det er noe større andel i privat enn i offentlig sektor på dette som svarer ja, og når det gjelder bransje er det i størst grad varehandel og overnatting/servering som har vært utsatt for lovbrudd de ikke anmeldte (henholdsvis 13 og 15 prosent).

De virksomhetene som har opplevd lovbrudd som ikke anmeldes, er blitt spurt om både hvilken type kriminalitet de ikke anmeldte og hvorfor de ikke anmeldte forholdet.

**Spørsmål: Hvilken type kriminalitet var det dere ikke anmeldte?**

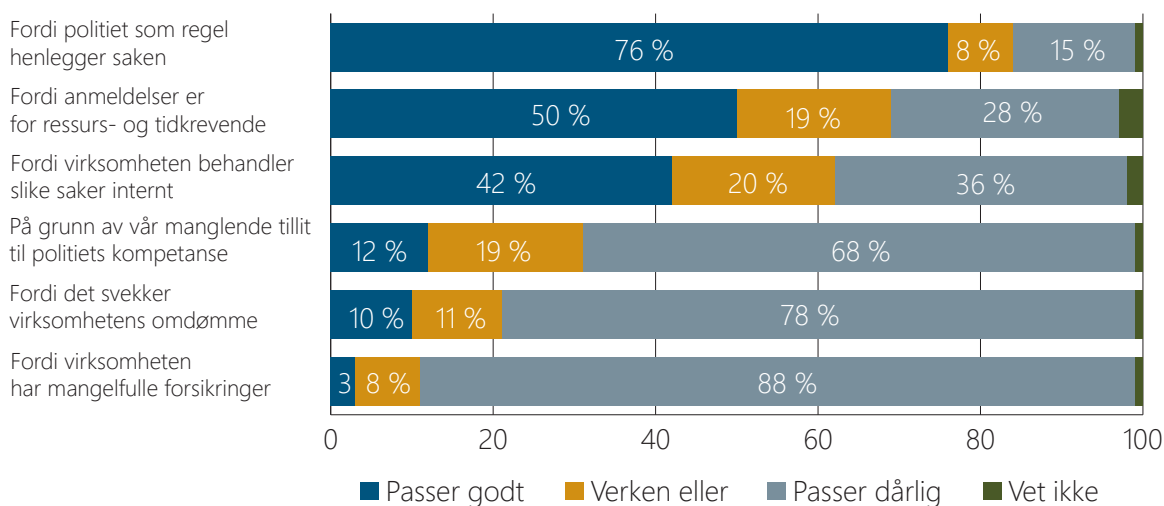
Figur 21 Type kriminalitet (n=238/245)



Blant virksomheter som er utsatt for lovbrudd som ikke ble anmeldt, er det 58 prosent av disse virksomhetene som ble utsatt for vinningskriminalitet, mens 19 prosent har blitt utsatt for kriminalitet i det digitale rom. Merk at vi ikke har spurt om antall for hver enkelt kriminalitetstype, så vi vet ikke fordelingen av antall lovbrudd.

**Spørsmål: I hvilken grad passer følgende beskrivelser som forklaring på hvorfor din virksomhet ikke anmeldte lovbrudd. Passer de godt, dårlig eller verken godt eller dårlig? Dersom virksomheten har hatt flere lovbrudd som ikke ble anmeldt, ber jeg deg svare ut fra siste tilfelle.**

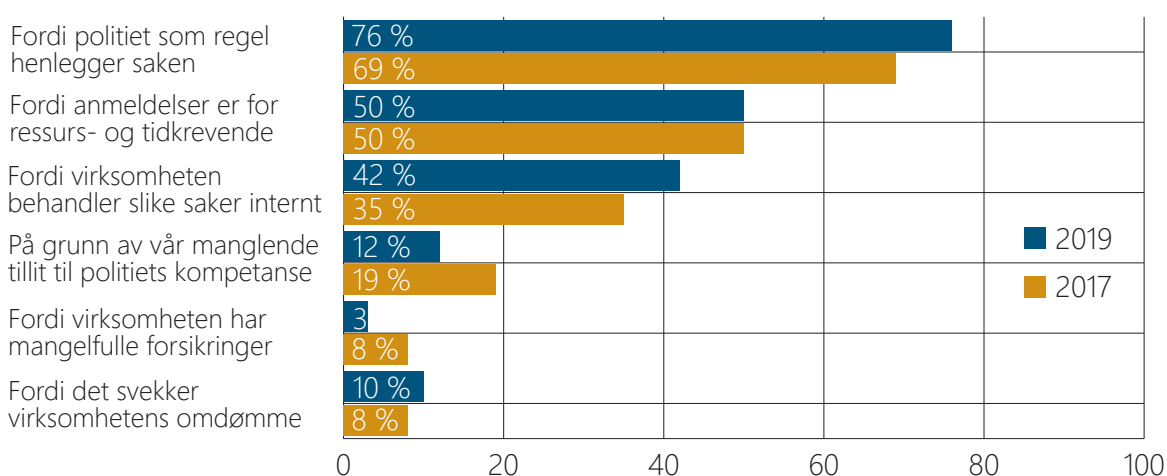
Figur 22 Årsaker til at lovbrudd ikke anmeldes (n=238)



### 3. Anmeldelser

Blant de som har opplevd lovbrudd som ikke er anmeldt, er man i størst grad enig i at politiet henlegger saken som er årsak til at de ikke anmelder. Sammenlignet med 2017 er det høyere andel som ikke anmelder fordi man mener politiet som regel henlegger saken, mens det er en lavere andel som ikke anmelder på grunn av manglende tillit til politiets kompetanse.

Figur 23 Årsaker til at lovbrudd ikke anmeldes (n=238/245)



Årsakene til å ikke anmelde følger samme mønster uavhengig av kriminalitetstype. Å ikke anmelde fordi man ikke har tillit til politiets kompetanse oppgis av 21 prosent av de som har blitt utsatt for kriminalitet i det digitale rom. Det er imidlertid få respondenter som er utsatt for denne type kriminalitet, så vi skal være forsiktig med å konkludere om denne forskjellen er reell eller skyldes tilfeldigheter.

#### 3.2 Utro tjenere

8 prosent av virksomhetene har avdekket utro tjenere blant egne ansatte i løpet av de siste 2 årene. Det er i overnatting/servering at dette er mest utbredt (18 prosent).

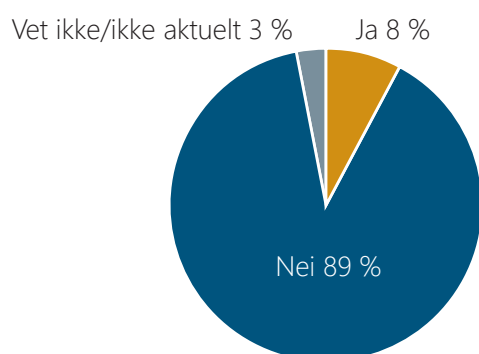
Spørsmålet om utro tjenere er i tidligere undersøkelser stilt uten noen tidsavgrensning (Har din virksomhet noen gang avdekket utro tjenere blant egne ansatte?). I 2017 ble det imidlertid stilt med en tidsavgrensning der vi spør om de siste 2 årene. Sammenlignet med 2017 er resultatet på samme nivå (10 prosent svarte ja i 2017).

Blant de som har oppdaget utro tjenere, er det 25 prosent som anmeldte forholdet. Det er en nedgang sammenlignet med 2017, da det var 37 prosent som anmeldte.



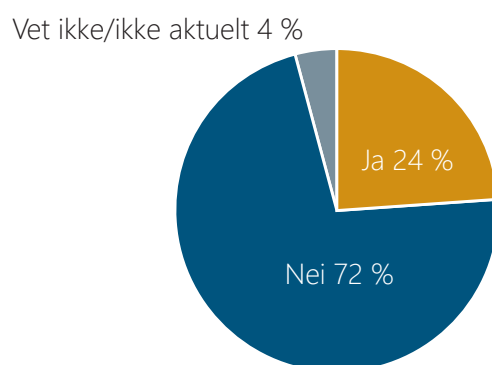
**Spørsmål: Har din virksomhet i løpet av de siste 2 årene avdekket utro tjenere blant egne ansatte?**

Figur 24 Utro tjenere (n=2502)



**Spørsmål: Ble forholdet anmeldt?**

Figur 25 Anmeldelse utro tjenere (n=200)



Det er stor forskjell på privat og offentlig sektor når det gjelder anmeldelser, der kun 16 prosent av de private virksomhetene har anmeldt utro tjenere mot 53 prosent i offentlig sektor. Tilsvarende forskjell fant vi også i 2017.

# 4. Kameraovervåking og vold

Under dette tema inkluderes bruk av sikringskamera, lagring av opptak, samt trusler om vold mot ansatte.





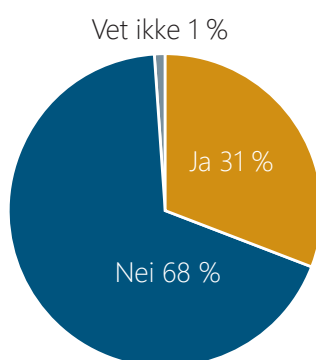
## 4. Kameraovervåking og vold

### 4.1 Kameraovervåking

3 av 10 virksomheter har installert sikringskamera (31 prosent i 2019, 28 prosent i 2017). Det er ikke forskjell på private og offentlige virksomheter. Bygg/anlegg, tjenesteytende og helse/sosial skiller seg fra andre ved å i mindre grad ha sikringskamera.

#### *Spørsmål: Har din virksomhet installert sikringskamera?*

Figur 26 Sikringskamera (n=2500)

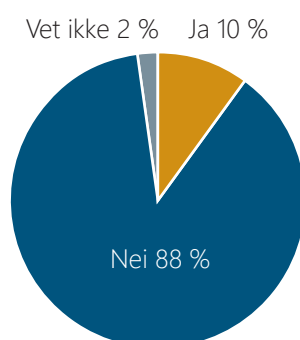


Blant de som har sikringskamera er det 1 av 10 som i løpet av de siste 12 månedene har opplevd at uønskede hendelser ikke kan dokumenteres fordi opptaket er slettet når hendelsen oppdages. Det er en klar nedgang fra 2017 da det var 27 prosent som svarte det samme.



**Spørsmål: Har virksomheten i løpet av de siste 12 måneder erfart at uønskede hendelser ikke kan dokumenteres fordi opptaket er slettet når hendelsen oppdages?**

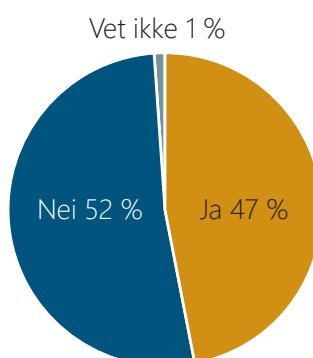
Figur 27 Dokumentasjon slettet (n=769)



Blant de som har erfart at uønskede hendelser ikke kan dokumenteres fordi opptaket er slettet når hendelsen oppdages, er det nær halvparten som mener dette hadde betydning for om forholdet ble anmeldt eller ikke. I 2017 var det 58 prosent i tilsvarende gruppe som svarte det samme.

**Spørsmål: Har dette hatt betydning for om forholdet er blitt anmeldt eller ikke?**

Figur 28 Slettet opptak og anmeldelser (n=74)



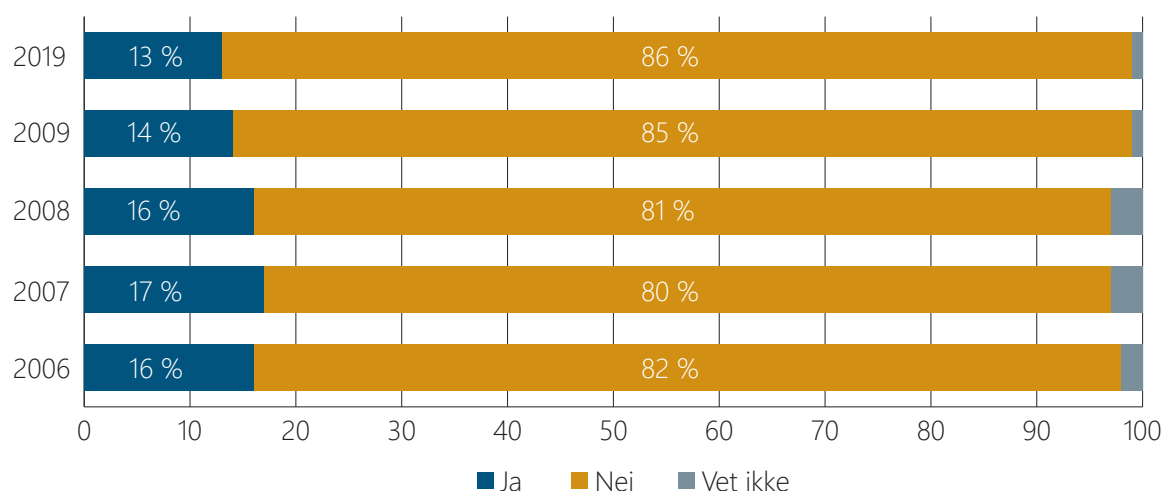
## 4. Kameraovervåking og vold

### 4.2 Vold mot ansatte

13 prosent av virksomhetene har opplevd at ansatte har blitt utsatt for vold eller trusler om vold. Det er på nivå med forrige gang spørsmålet ble stilt i 2009.

**Spørsmål: Har ansatte i din virksomhet vært utsatt for vold eller trusler om vold i jobbsammenheng i løpet av de siste 12 månedene?**

Figur 29 Vold i jobbsammenheng (n=2500)



Det er stor forskjell på private og offentlige virksomheter. Hele 49 prosent av de offentlige virksomhetene har opplevd at ansatte er utsatt for vold eller trusler om vold, men det er 4 prosent i private virksomheter som sier det samme. Tilsvarende forskjell fant vi også i 2009.

Blant de «private» bransjene er det overnatting/servering som er mest utsatt. 16 prosent har opplevd vold eller trusler om det, mens de andre private bransjene er mellom 3 og 7 prosent som svarer det samme. I offentlig sektor er det spesielt helse og sosial som er utsatt, der 63 prosent av virksomhetene opplever vold eller trusler om vold mot ansatte. I offentlig administrasjon er det 44 prosent som er utsatt og i undervisning er det 27 prosent.

Blant de som er utsatt for vold eller trusler om vold er i størst grad eksterne som utgjør trusselen. I 7 prosent av virksomheter som har opplevd vold eller trusler om vold, er det egne ansatte som står bak, mens det i 92 prosent er eksterne. Andre ansatte er i større grad en trussel i private bedrifter og i virksomheter med aktiviteter i utlandet. I bransjene industri, bygg/anlegg og overnatting/servering tenderer egne ansatte til å stå bak i større grad enn andre bransjer (skiller seg signifikant fra offentlig administrasjon og helse/sosial). Eksterne er mer vanlig som trussel i helse/sosial, offentlig administrasjon, undervisning og varehandel enn i bygg/anlegg (signifikant forskjellig).



# Krisino 2019: Perspektiver



Krisino 2019 byr på tall som vekker både interesse og nysgjerrighet – kanskje også uro og frustrasjon. I det følgende skal vi løfte frem noen av resultatene og diskutere bakgrunn så vel som konsekvenser. Vi skal også søke å sette noen av resultatene inn i et bredere perspektiv i lys av annet tilgjengelig materiale.

*Av Kjetil Skogrand, partner og Eirik Torsvoll, analytiker i Rud Pedersen Public Affairs.*

**Først et lite forbehold:** Vi vet strengt tatt ikke mer enn det de nakne tallene kan fortelle oss. En samfunnsforsker ville kanskje pekt på ønskeligheten av flere undersøkelser – nye studier med flere og mer detaljerte spørsmål og dybdeintervjuer – for å kunne forklare hvorfor respondentene har svart som de har. Når vi i det følgende skal reflektere over resultatene, er det altså delvis hypoteser som

ikke kan dokumenteres; kall det gjerne informert spekulasjon. Det kan likevel være nyttig å fremsette noen teorier om hva som ligger bak tallene. Delvis for å provosere til debatt, og delvis for å spore til aktiv handling. Og skulle vi inspirere noen til å etterprøve vurderingene våre, så desto bedre.



# Forebygging: undervurdert?

**De som jobber aktivt** med sikkerhet og kriminalitetsbekjempelse vet at forebygging er langt mer kostnadseffektivt enn å håndtere konsekvenser i etterkant. Riktignok er det viktig å sikre effektiv bevissikring og etterforskning etter at en forbrytelse har funnet sted, slik at man kan identifisere og straffeforfølge gjerningspersonene. Men aller best er det å motvirke at kriminaliteten finner sted. Ikke minst gjelder det for datakriminalitet, der de ansvarlige ofte befinner seg lang utenfor landets grenser og vanskelig lar seg etterspore.

Flere funn i undersøkelsen peker i retning av at det er mye å hente ved å styrke forebyggingsarbeidet i Norge. Særlig gjelder dette små og mellomstore private virksomheter. Tallene indikerer at få har gjennomført en risikoanalyse og at få har lest PSTs eller NSMs åpne trusselvurderinger. Samtidig viser undersøkelsen at de som har tatt seg tid til å lese trusselvurderingene, åpenbart har hatt nytte av det: Et flertall av disse har nemlig gjennomført forebyggende tiltak som en følge av dem.

Risikoanalyser er mye mer utbredt i offentlige virksomheter. Det kan skyldes at flere offentlige etater er pålagt å gjennomføre slike analyser<sup>1)</sup>. Kanskje ser private virksomheter slike undersøkelser som formaløvelser som ikke er verdt ressursbruken. Det er i tilfelle en feilvurdering. All forebygging må baseres på en analyse av hva man vil beskytte og hva som utgjør mulige trusler. Det trenger ikke være en omfattende prosess. Blant de sentrale spørsmålene er hva som utgjør virksomhetens sentrale **verdier** – det som skal beskyttes mot uønskede handlinger. Trusselvurderingen retter søkelyset på hvem som kan tenkes å true disse verdiene og hvor sårbar man vil være i ulike scenarier. En risiko-vurdering munner ut i konkrete tiltak for å håndtere risikoen.

Den innledende verdivurderingen vil for svært mange virksomheter peke i retning av det som sammenfattes under merkelappen sensitiv informasjon. Design, produktutvikling, kostnadsberegninger, kundelister, tilbud og kontraktutkast – hvis noe av dette kommer utedkommende i hende,



<sup>1)</sup> <https://dfo.no/fagomrader/risikostyring/risikostyring-i-staten>  
<https://vtsanalyse.no/vts-analyse/hvordan-gjennomfore-vts-analyser>



kan det skade virksomheten og svekke konkurranseevnen alvorlig. I mange tilfeller kan også bedriftens omdømme få et grunnskudd hvis noe av dette kommer på avveie.

Like alvorlig kan det være dersom virksomheten skulle miste eller bli blokkert fra tilgang til egen vital informasjon, eksempelvis hvis noen kommer inn på informasjonssystemene, krypterer informasjonen og krever løsepenger for å åpne dem igjen.<sup>2)</sup> Slike hendelser kan lamme bedriftens virksomhet i ett slag.

Fysisk infrastruktur som kontorer, inventar og maskiner er selvsagt også viktige, men disse lar seg ofte lettere erstatte. De kan dessuten forsikres. Informasjon er til sammenlikning krevende å rekonstruere hvis man ikke har en trygg sikkerhetskopi. Informasjon kan dessuten utnyttes og selges til konkurrenter på et svart marked.

Like fullt – alle virksomheter er forskjellige. Det er derfor alle bør ta seg tid til å gjennomføre sin egen risikoanalyse, og på bakgrunn av denne vurdere tiltak for å redusere sårbarhetene.

Det er urovekkende at små og mellomstore virksomheter er de som vier minst tid til risikovurderinger. Oftest er det nemlig de små som har aller mest å tape. Store konsern har gjerne styrke til å omfordele ressurser og dempe konsekvensene av kriminelle anslag. Mindre bedrifter kan oppleve at et enkelt kriminelt anslag lammer virksomheten – særlig hvis tilgangen til digital informasjon blokkeres over tid. De små har heller ikke robustheten til å la tiden reparere et svekket omdømme. Raskt kan kassen være tom og veien til skifteretten kort.

Strengt tatt skulle det altså forholdt seg motsatt – det er de små og mellomstore bedriftene som burde toppet statistikken over virksomheter med risikoanalyser.

Så må det samtidig understrekes at den høyere utbredelsen av risikoanalyser i offentlig sektor ikke nødvendigvis innebærer at analysene faktisk benyttes til å styrke sikkerheten. Kanskje betraktes slike analyser også i offentlige virksomheter mer som et formalkrav mer enn som et reelt verktøy? Hvis risikoanalyser skal ha noen effekt, må de være del av en bevisst prosess for å identifisere risikoreduserende tiltak og iverksette dem.

<sup>2)</sup> <https://norsis.no/jhfkjsdhfkjhsdkfjhskhfk/>

# Integrert sikkerhetskultur

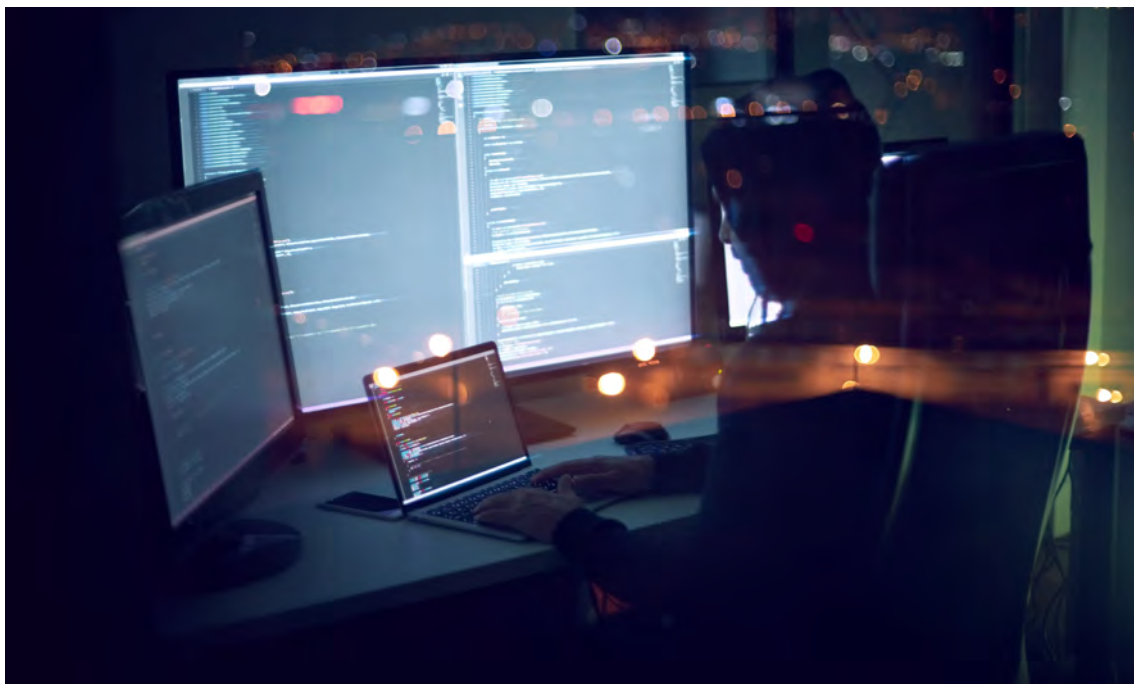
**Ikke overaskende** viser undersøkelsen at det kun er store virksomheter som har egne ansatte som jobber med sikkerhet. Å vie egne stillinger til slikt arbeid er sjelden aktuelt for små virksomheter, med mindre sikkerhetsutfordringene vurderes som særlig store.

Likevel må det advares mot å anta at det å ha eget sikkerhetspersonell nødvendigvis borger for et sterkere søkelys på sikkerhet i hele organisasjonen. Erfaringer viser at egne sikkerhetsansvarlige ofte står litt på sidelinjen av resten av virksomheten. Typisk er de rekruttert utenfra, med faglig bakgrunn fra politi eller forsvar. De er ofte plassert mange ledd under toppledelsen – sjelden ser vi en ledergruppe som omfatter en egen sikkerhetsdirektør. Den som har snakket med en sikkerhetsansvarlig vet dessuten at mange av dem opplever det som krevende å få gehør for sine synspunkter. Ikke sjelden oppleves de som brysomme hår i suppa; folk som konstant pukker på skjerpede

rutiner og tidkrevende prosedyrer og høster lite annet enn utålmodig avvisning.

Som i mange andre sammenhenger, spiller topplederen en nøkkelrolle gjennom sitt eksempel. De virksomhetene som har lyktes med sikkerhetsarbeid, er de som har en topplerer som i ord og handling viser interesse for sikkerhet. Der sikkerhetsrutinene observeres til punkt og prikke også i ledergruppen, på tross av en travel hverdag og en fullpakket agenda. Der alle ansatte gis god opplæring ikke bare i sikkerhetstiltakene, men også i årsakene til at de må følges. Der sikkerhetsbrudd følges opp, ikke for å straffe den enkelte, men for at alle skal kunne lære av dem.

I slike organisasjoner er det en positiv sikkerhetskultur, som er integrert i hele virksomheten. En topplerer som selv slurver med sikkerhetsrutiner og stadig tar snarveier, kan ikke regne med at resten av organisasjonen er annerledes.



# Styrket digital sikkerhet – en lavthengende frukt

**Vi lever i et stadig mer** digitalisert samfunn. Nær sagt all informasjon lagres digitalt – de tradisjonelle ringpermene har stort sett havnet på skraphaugen. Korrespondanse foregår på e-post og andre digitale kommunikasjonsmedier. Økonomiske transaksjoner utføres via nettet – selv detaljhandel er fullstendig dominert av elektronisk betaling, riktignok fortsatt mye med betalingskort, men i økende grad via mobile betalings-systemer. Dette er trender som kommer til å fortsette, og akselerere. Vi har sannsynligvis knapt sett begynnelsen.

Det er derfor ikke overraskende at kriminalitetsbildet beveger seg samme vei. Stadig mer av kriminell virksomhet foregår via nettet. I næringslivssammenheng vil det snart ikke gi mening å snakke om cyberkriminalitet som en egen kategori – nær sagt all kriminalitet vil ha en digital dimensjon. Selv fysiske innbrudd forberedes ofte ved å stjele digitale adgangskoder, og det er gjerne datautstyr som stjeles. Ja til og med trusler, mobbing og trakassering foregår nå gjerne på digitale plattformer.

Omfanget av digital kriminalitet stiger ikke bare på grunn av vår økende bruk av nettbaserte tjenester. Urovekkende trender gjør det stadig lettere å drive kriminell virksomhet i det digitale rom. Digitale løsninger gjør det mulig å opptre i skjul og med lav risiko for å bli avslørt – som det såkalte «mørke nettet». Her er ulike verktøy for digitale innbrudd og virusprogrammer lett tilgjengelige for kjøp og salg. Kryptovalutaer gjør det lettere å utveksle betaling uten ettersporing, inkludert løsepengekrav. Siden det digitale rommet er globalt, kan man angripe mål langt vekk fra eget fysisk oppholdssted – med lav risiko for å bli tatt. Nasjonale politietater sliter med å holde

følge. Verdensvevens mørke kjellerrom er blitt et fristed for kriminelle.

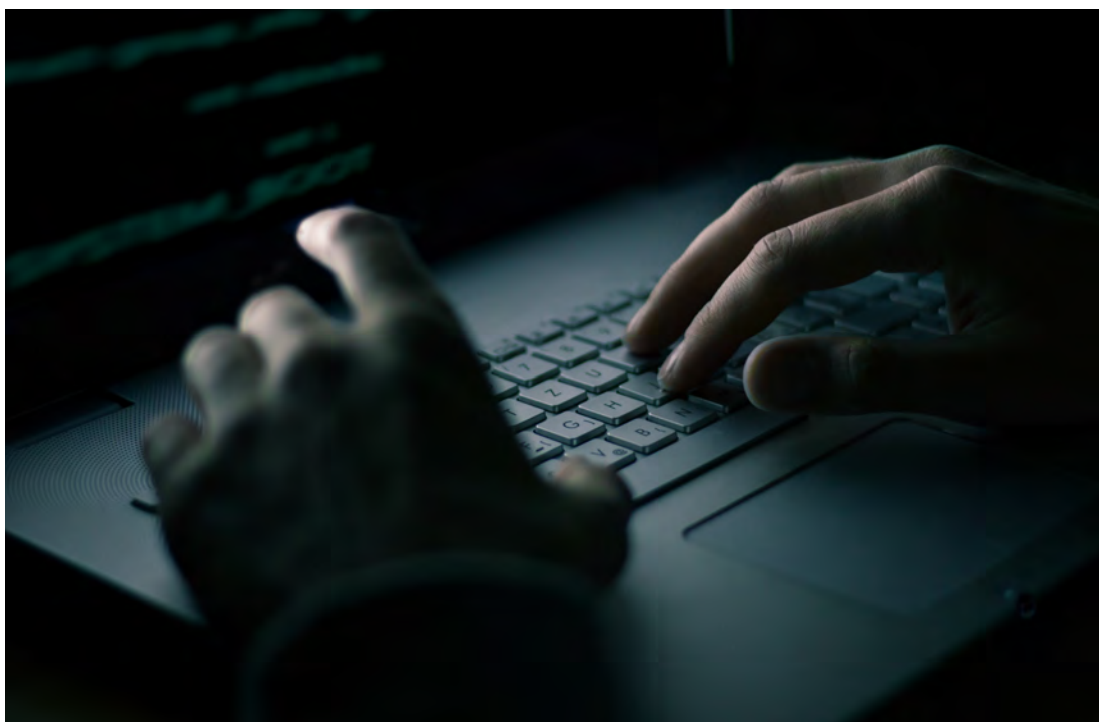
Det er ingen dristig spådom at NSRs skille mellom en alternerende digital mørketallsundersøkelse og en kriminalitetsundersøkelse om få år vil erstattes av én samlet undersøkelse, der ulike former for det vi i dag kaller datakriminalitet vil dominere totalt.

Samtidig ser vi at både privat og offentlig sektor henger etter i arbeidet med å beskytte seg mot digitale anslag. Dette er bemerkelsesverdig, siden ganske enkle mottiltak kan gi effektiv beskyttelse mot de fleste former for digital kriminalitet. Enda enklere er det å beskytte seg mot mange av effektene av dataforbrytelser – eksempelvis er bruk av enkle sikkerhetskopier til stor nytte for å gjenvinne data som er stjålet, ødelagt eller blokkert.

Som et eksempel kan det nevnes at 15 prosent av de spurte bedriftene og virksomhetene i Krisino sier at de har blitt utsatt for løsepengevirus. Tallet er kanskje verken overraskende eller høyt, men det er likevel alvorlig. I inneværende år var vi vitne til det største og mest alvorlige løsepengevirusangrepet mot en norsk virksomhet til nå: Dataangrepet mot Hydro i mars antas ha kostet selskapet mellom 300 og 350 millioner kroner i første kvartal.<sup>3)</sup>

Dette angrepet hadde selvsagt store konsekvenser, men Hydro har overkommet utfordringene. For små- og mellomstore bedrifter vil et vellykket løsepengevirusangrep kunne være enda mer alvorlig – det vil kunne bety kroken på døra. Små- og mellomstore bedrifter er nemlig dobbelt utsatt ved at prislappen koblet med omdømmemessige kostnader vil være spesielt tungt for dem å bære.





Dette ser vi i ulike studier som for eksempel peker på at rett over halvparten av alle digitale angrep regnes å skape økonomisk skade for minst 4,3 millioner kroner.<sup>4)</sup> Samtidig sier 58 prosent av respondene i en undersøkelse gjennomført av KPMG at de ville vært mindre villige til å anvende tjenestene til et selskap som har vært utsatt for et cyberangrep.<sup>5)</sup> Konsekvensen av dette er at så mange som halvparten av små- og mellomstore bedrifter slås konkurs seks måneder etter at de er blitt usatte for digitale angrep.<sup>6)</sup>

Ved datakriminalitet er forebygging i mange tilfeller det eneste effektive mottiltaket. Gjerningspersonene lar seg oftest vanskelig finne – enn si

straffeforfølge. En liten norsk virksomhet fulgte for eksempel sporene fra et digitalt angrep til en internettkafé i Cape Town. Der stoppet sporene.

Hva kan gjøres? Et sted å starte er tiltaksoversikten i regjeringens nye nasjonale strategi for digital sikkerhet, som ble presentert tidligere i år.<sup>7)</sup> Her fremstilles det i del 2 en plan på ti anbefalte tiltak for å øke virksomheters egenevne til digital sikkerhet presentert som en del av strategien. Dokumentet understreker viktigheten av tiltak som allerede er blitt nevnt ovenfor, slik som involvering fra ledelsen, utarbeidelse av risikoanalyser, og kartlegging av verdier. Andre tiltak inkluderer leverandørkontroll, sikker konfigurasjon og tilgangskontroll.

<sup>3)</sup> <https://www.tu.no/artikler/svekket-hydro-resultat-dataangrepet-kostet-300-350-millioner/466923>

<sup>4)</sup> [https://www.cisco.com/c/dam/m/hu\\_hu/campaigns/security-hub/pdf/acr-2018.pdf](https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf)

<sup>5)</sup> <https://home.kpmg/content/dam/kpmg/pdf/2016/02/small-business-reputation-new.pdf>

<sup>6)</sup> <https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html>

<sup>7)</sup> <https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/tiltaksoversikt---nasjonal-strategi-for-digital-sikkerhet.pdf>

# Sikkerhet på reise



**For første gang** er det i årets Krisino stilt spørsmål om digital reisesikkerhet. Dette er et viktig tema, i 2018 dro for eksempel nordmenn på over 600 000 utenlandsreiser i jobbsammenheng.<sup>8)</sup> Samtidig er bevisstheten rundt reisesikkerhet overraskende dårlig. Ovenfor var vi inne på at de viktigste verdiene for mange virksomheter finnes i form av digital informasjon – produktdesign, kostnadsberegninger, kundelister, tilbud og kontraktutkast. Mye av denne informasjonen ligger typisk i bærbar datamaskiner til personer i toppledelsen og andre som driver utadrettet virksomhet.

Ingen ville finne på å forlate jobben uten å se til at utgangsdøra er låst. Men mange kan finne på å reise til utlandet, kanskje også til land med en helt annen sikkerhetssituasjon enn Norge, og medbringe digitale plattformer som bærbar data-

maskiner, mobil og nettbrett, fullstappet med forretningshemmeligheter. Flere lar de tyngste av disse plattformene ligge ubevoktet igjen på hotellrommet når de spiser middag om kvelden. Mange kopler seg uten ettertanke på trådløse nettverk på flyplasser, restauranter og hoteller. De har sensitiv informasjon liggende ubeskyttet og ukryptert på det digitale skrivebordet, og sender ukritisk e-poster og digitale meldinger over nett som kan avlyttes.

Det finnes enkle sikkerhetsforanstaltninger som kan forebygge digitale tyverier og industrispioasje på reiser.<sup>9)</sup> Men det krever oppmerksomhet. Det er bekymringsfullt at to tredeler av norske virksomheter ikke har noe eget regelverk for beskyttelse av digital informasjon på reiser.

<sup>8)</sup> <https://www.ssb.no/reise>

<sup>9)</sup> <https://www.nsm.stat.no/aktuelt/reiserad-fra-nsm/>

# Manglende anmeldelser – et samfunnsproblem?

**Et gjennomgående funn** i Krisino over flere år har vært den lave andelen av avdekket kriminalitet som faktisk anmeldes til politiet. Tendensen er stigende. Fordelingen av lovbrudd som ikke anmeldes «fordi politiet som regel henlegger saken» er på 76 prosent i 2019, en økning fra 69 prosent i 2017. Dette er urovekkende tall.

Et nærliggende spørsmål er om den manglende tilliten til politiets etterforskningskapasitet har reelt grunnlag. Og det har den – særlig for hovedstadens del.

For et drøyt år siden meldte Østlandssendingen at Oslo-politiet hadde henlagt 55.448 saker på et drøyt år.<sup>10)</sup> Fungerende påtaleleder i Oslo politidistrikt innrømmet da at politiet henlegger for mange saker. Han understreket likevel at kriminalitet bør anmeldes selv om mange av sakene blir henlagt – slik at politiet kunne vite hva som skjer ute i samfunnet, og kanalisere ressursene på best mulig måte. Thor Martin Bjerke, sikkerhetsrådgiver i hovedorganisasjonen Virke, uttrykte imidlertid i samme oppslag at mange av butikkene de representerer har mistet troen på å anmelde saker til politiet.

Det fremgikk av oppslaget at en tidel av sakene var henlagt på grunn av manglende kapasitet. Over 3.300 av de henlagte sakene hadde kjent gjerningsperson. Men de ble altså likevel lagt til side.

Politidirektoratets rapport for første tertial 2019 tyder på at tendensen er den samme. I direktoratets risikobilde er målsetningen «effektiv straffebehandling med høy kvalitet» plassert i ruten for høy sannsynlighet for mangelfull måloppnåelse – og med alvorlige konsekvenser.<sup>11)</sup>

Oppklaringsprosenten for vinningskriminalitet for hele landet er på fattige 26 prosent, og i Oslo er den nede på 21 prosent. Oppklaringsprosenten innen økonomisk kriminalitet er marginalt høyere som landsgjennomsnitt (32 prosent), men i Oslo er også denne nede i 21 prosent.

I disse tallene skjuler det seg sikkert en del anmeldelser som er ufullstendige eller grunnløse, slik at de reelle tallene sannsynligvis ser litt bedre ut. Likevel kan det nøkternt fastslås at det er basert på realiteter når næringslivet har sviktende tro på politiets evne til å etterforske og påtale anmeldt kriminalitet.

Det neste naturlige spørsmålet er hvorfor vi er kommet i denne situasjonen. Det er rimelig å rette oppmerksomheten på to forhold: Andelen alvorlige saker som stjeler ressurser fra annen og mer prosaisk kriminalitet, samt gjennomføringen av politireformen.



<sup>10)</sup> <https://www.nrk.no/ostlandssendingen/oslo-politiet-har-henlagt-55.448-saker-pa-et-droyt-ar-1.14129595>

<sup>11)</sup> <https://www.politiet.no/globalassets/dokumenter/pod/rapporter/politidirektoratets-1.-tertrialrapport-2019.pdf>

Det meldes at politiets kapasitet i stor grad går med til å etterforske et fåtall alvorlige saker, som alvorlige voldshendelser og seksuelle overgrep. En tredel av politiets ressurser brukes på tre prosent av sakene; de aller mest graverende.<sup>12)</sup> Da blir det beskjedent rom for å etterforske andre typer kriminalitet. Ingen vil bestride at alvorlig vold og seksualforbrytelser må ha høyeste prioritet. Samtidig er det et samfunnsproblem dersom andre typer kriminalitet – som også kan ha alvorlige konsekvenser for de berørte – stadig taper i kampen om begrensede etterforskningsressurser. Det er åpenbart at det senker terskelen for å utføre ulike vinningsforbrytelser når risikoen for straffefølgelse har falt til et så lavt nivå. Innen data-kriminalitet er oppklaringsgraden så lav at vi nærmer oss et lovløst rom.

Så er det grunn til å spørre om den høye henleggesprosenten også kan forklares med måten politiet er organisert på, og av anvendelsen av de totale resursene. Her er det naturlig å rette søke-lyset mot omleggingene i politietaten de senere årene.

Nærpolitireformen ble vedtatt i 2015, som en konsekvens av svakheter som ble påpekt i etterkant av terroranslaget 22. juli 2011. I januar 2018 ble 27 politidistrikter redusert til 12 større og mer slagkraftige enheter. Det sier seg selv at arbeidet med denne omfattende omleggingen har krevd store ressurser og senket politiets kapasitet i en overgangsfase. Politidirektoratet har i sin fremdriftsplan lagt til grunn at det først er i årene 2018–2020 at effektene virkelig vil slå inn, slik at politiets kvalitet og effektivitet økes «vesentlig».<sup>13)</sup>

I følge Politidirektoratet, er det altså litt tidlig å vurdere resultatene i tidenes største reform av politiets organisering i Norge. Riktignok flommer media over av kritiske oppslag. Opposisjonspolitikere krever tiltak. Tillitsvalgte varsler om kriselignende tilstander. Lederen for politijuristene i Oslo politidistrikt, Asmund Riegels, forteller eksempelvis om høyt arbeidspress, store saksmengder og økt behandlingstid. Ifølge ham blir de enkle sakene raskt behandlet med den nye organiseringen. Alvorlige prioriterte saker blir også behandlet, om enn saktere enn de burde. Det er sakene som ligger i mellomstadiet, men som like fullt er alvorlige, som blir liggende, hevder han.<sup>14)</sup> Det er i tilfelle urovekkende, siden anmeldt kriminalitet fra næringslivet sannsynligvis faller nettopp i denne kategorien.

Politireformen er et enkelt angrepsmål når politiets henleggesprosent er bekymringsfullt høy. Det er likevel grunn til å mane til forsiktighet med å plassere hele årsakssammenhengen der. Utfordringene som kommer tydelig frem i Krisino har eksistert lenge før reformen ble vedtatt. Ja, reformen ble i stor grad igangsatt nettopp for å bøte på treg saksbehandling i politiet. Mange av grepene i reformen var dessuten basert på godt dokumenterte svakheter. Kritiske utspill fra politiets tillitsvalgte har forekommet ikke bare underveis, men også svært lenge før reformprosessen. Med andre ord er det liten grunn til å tro at totalbildet ville vært mer positivt uten en politireform.

Når dette er sagt, er det all grunn til å være bekymret over den tilsynelatende mangelen på positive effekter, som snart burde begynne å melde seg. Politidirektoratets forsikringer kan ikke kamuflere at reformen sliter med å levere.

<sup>12)</sup> [https://www.nrk.no/norge/store-saker-skaper-trobbel-for-politiet\\_-mangler-kompetanse-og-kapasitet-1.14622575](https://www.nrk.no/norge/store-saker-skaper-trobbel-for-politiet_-mangler-kompetanse-og-kapasitet-1.14622575)

<sup>13)</sup> <https://www.nrk.no/norge/krise-i-politiet-1.14121109>

<sup>14)</sup> <https://www.nrk.no/norge/krise-i-politiet-1.14121109>





Kanskje ligger utfordringene i norsk politi dypere enn det politireformen har maktet å adressere. Kanskje må årsakene søkes i en kombinasjon av mange faktorer: et kriminalitetsbilde i rivende utvikling, vansker med å legge om tradisjonsbundne og ineffektive arbeidsmetoder og systemer, mangel-full kompetanse på nye kriminalitetsområder, liten smidighet i intern ressursfordeling og et generelt for tynt ressursgrunnlag. Det er i tilfelle et komplekst årsaksbilde som det faller utenfor rammene av denne analysen å gå inn i.

Det som uansett er klart, er at et samfunn over tid vanskelig kan leve med en situasjon der verken næringsliv eller privatpersoner finner det bryet verdt å anmelde mange lovbrudd. Politi og på-talemakt må derfor moderniseres videre og til-

passes vår tids kriminalitet. En slik modernisering må pågå løpende for å fange opp endringer og behov. Det er en utfordring som kaller på grundig og kritisk refleksjon, snarere enn de kjappe, slag-ordspregende løsningene som preger dagens offentlige ordskifte.

I mellomtiden må det påpekes at anmeldelser faktisk har betydning, selv om sakene henlegges.<sup>14)</sup> Ved å anmelde, skapes et mer realistisk totalbilde av kriminaliteten. Usikre mørketall avløses av statistikk som kan benyttes for å kreve handling og drøfte løsninger. Vi gjør derfor oss selv og samfunnet som helhet en tjeneste ved å anmelde kriminalitet. Selv om det i et kortsiktig perspektiv kan fremstå som fåfengt.

<sup>15)</sup> <https://www.nrk.no/ostlandssendingen/ni-av-ti-bedrifter-i-byggebransjen-har-blitt-frastjalet-verktoy-1.14438818>

# Avslutning

*For den som har fulgt NSRs undersøkelser over tid, kommer ikke resultatene i Krisino 2019 som noen overraskelse. Mange av tallene i årets undersøkelse samsvarer med trendene fra tidligere år, enten ved at bildet ligger fast, eller ved at utviklingen har fortsatt i samme retning. Eksempelvis er andelen virksomheter som produserer skriftlige risikovurderinger identisk med 2017. Det samme gjelder andelen som har opplevd lovbrudd som de ikke har anmeldt. Særlig er det nedslående at de sistnevnte tallene har vist samme hovedbilde helt siden første Krisino-undersøkelse for 13 år siden. Underliggende trender i kriminalitetsutviklingen krever øket evne til å håndtere flere og mer komplekse trusler.*

*Dette maner til nøkternhet når det gjelder å finne løsninger som kan frembringe raske resultater. Det viser også at samfunnet vårt står overfor utfordringer som krever omfattende innsats og bredt samarbeid mellom privat og offentlig sektor, dersom vi skal lykkes i å snu trendene over tid.*

*Samtidig bekreftes verdien av uavhengige undersøkelser, gjennomført over tid. Krisino har vært, og fortsetter å være, en meget verdifull kilde til kunnskap om hvordan det faktisk står til hos offentlige og private virksomheter i Norge. Håpet er at denne undersøkelsen, sammen med annen tilgjengelig statistikk, kan benyttes til en opplyst, faktabasert debatt om hvordan vi sammen kan styrke samfunnets evne til å forebygge og håndtere trusselen fra ulike former for kriminell virksomhet mest mulig effektivt. Vi har mye å beskytte fordi vi har mye å tape.*







[www.nsr-org.no](http://www.nsr-org.no)

Rikur Kommunikasjon

