FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Risiko- og sårbarhetsanalyse (ROS) 2020

Finanssektorens bruk av informasjons- og kommunikasjonsteknologi (IKT)

Olav Johannessen, Pressebrief, 14.mai 2020

Finanstilsynets vurderinger - ROS 2020

- Den norske finansielle infrastrukturen er robust
- Ingen IKT-hendelser i 2019 med konsekvenser for finansiell stabilitet
- Noen flere IKT-hendelser i 2019 enn i 2018
- Tilgjengeligheten til betalings- og øvrige kunderettede tjenester var bedre i 2019 enn i 2018
- Tilgjengeligheten til tjenestene samlet sett tilfredsstillende


Foto: Einar Aslaksen

Koronakrisen

- Finanstilsynet og BFI rettet særlig oppmerksomhet mot virksomheter som støtter viktige funksjoner, herunder de kritiske samfunnsfunksjonene definert av DSB
  - Sikker formidling av kapital nasjonalt og til og fra utlandet
  - Gjennomføre betalinger og andre finansielle transaksjoner
  - Opprettholde befolkningens tilgang til nødvendige betalingsmidler
- De sentrale foretakene i den norske finansielle infrastrukturen har gode beredskapsplaner
- Aktørene har så langt hatt god kontroll på driftssituasjonen og har raskt iverksatt nødvendige tiltak

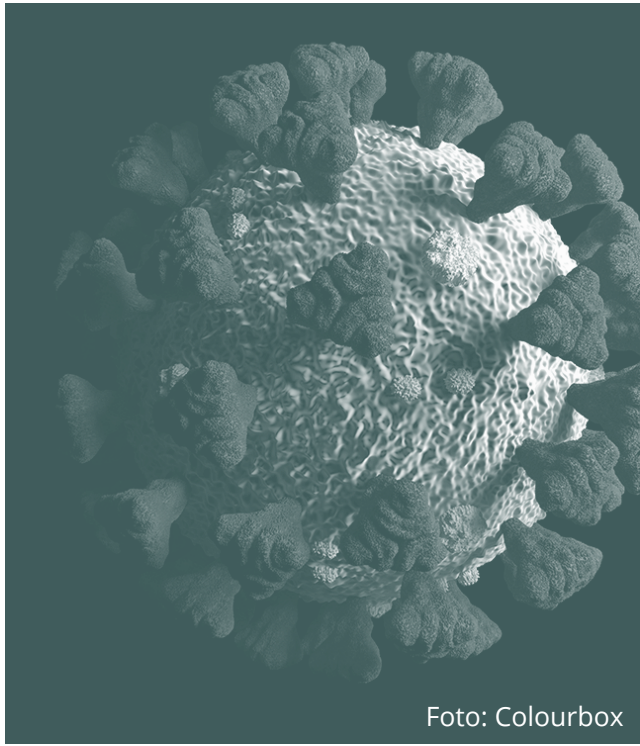
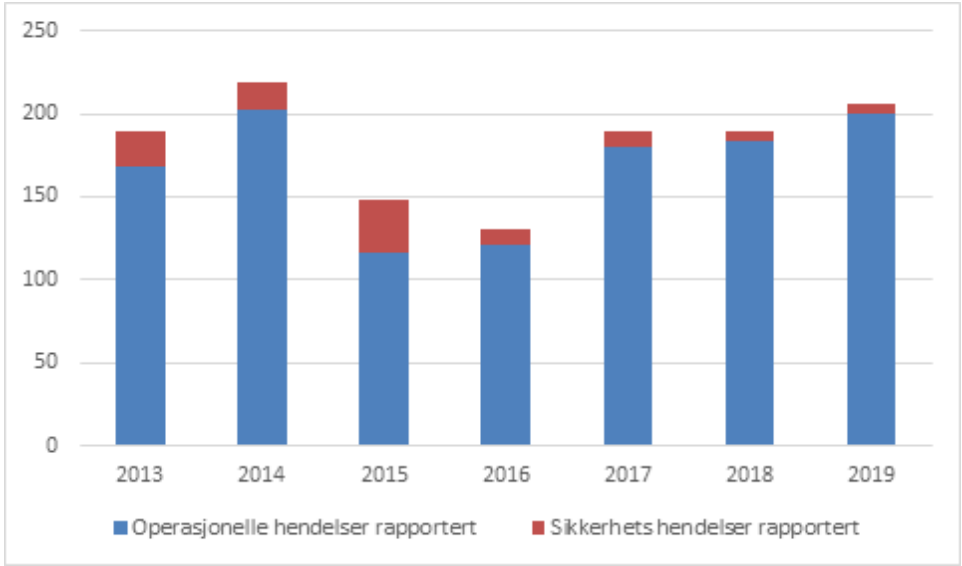


Foto: Colourbox

Rapporterte hendelser

Foretakene rapporterte 206 IKT-hendelser i 2019, som er 17 flere enn året før

- Antall rapporteringspliktige foretak økte fra 2018 til 2019
- Flere av de rapportert hendelsene gjaldt samme hendelse hos foretakenes felles leverandør



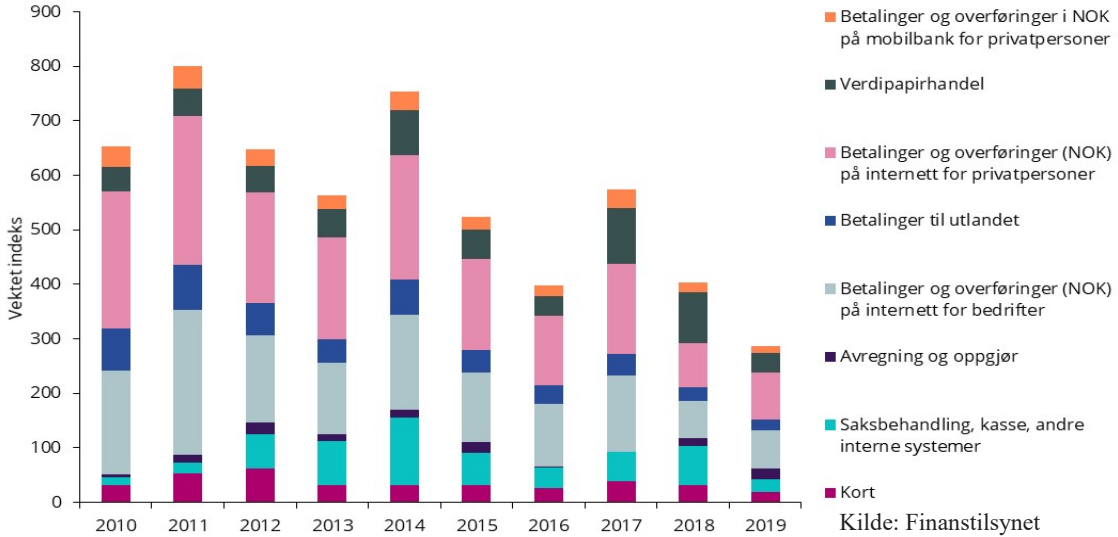
Kilde: Finanstilsynet

	Operasjonelle hendelser	Sikkerhets hendelser
2013	168	21
2014	202	17
2015	116	32
2016	121	10
2017	180	10
2018	184	5
2019	200	6

Hendelser – tilgjengelighet

- Ingen hendelser av lengre varighet rammet tilgjengeligheten til betalingstjenestene til mange banker samtidig
- Tilgjengeligheten til betalingstjenestene og øvrige kunderettede løsninger var noe bedre i 2019 enn i 2018

Dette er vurdert: antall brukere som er rammet, hendelsens varighet, i hvilken grad kunden lider skade som følge av hendelsen, alternative måter for å få tilgang til tjenesten.



Kilde: Finanstilsynet

Hendelser med spesielt alvorlige konsekvenser

Foto: Colourbox

- Nettverksproblem i Gjensidige Forsikring AS
- Vipps 17. mai
- Doble VISA-trekk
- Feil implementering av eFaktura-tjeneste
- Hendelser knyttet til bankenes elektroniske kunde- og transaksjonsovervåkningssystemer for å avdekke hvitvasking og terrorfinansiering (AML-systemer)
- BankID-hendelser
- Sikkerhetshendelser
- Rapporterte sårbarheter

Tap som følge av svindel ved bruk av betalingskort

Svindeltype betalingskort (beløp i hele tusen kroner)	2015	2016	2017	2018	1. halvår 2019
Misbruk av kortinformasjon, Card-Not-Present (Internett-handel m.m.)	98.410	137.015	102.908	114.932	76.546
Stjålet kortinformasjon (inkludert skimming):	51.117	43.122	17.935	14.507	3.911
Originalkort tapt eller stjålet:	39.132	26.366	24.748	19.293	14.009
Totalt	188.659	206.503	145.591	148.732	**94.466**

Kilder: Finanstilsynet og Bits AS

Transaksjonsverdi i hele tusen NOK	Transaksjoner i Norge	Grensekryssende transaksjoner i EØS	Grensekryssende transaksjoner utenfor EØS	2. halvår totale transaksjoner
Kortbetalinger (utsteder)				
Totalt transaksjonsbeløp	414.632.690	103.472.005	12.385.305	530.490.001
Hvorav svindel	7.091	67.236	20.354	**94.681**
Hvorav initiert elektronisk:				
Svindleren utsteder betalingen, hvorav	8.447	48.593	15.855	72.896
Svindleren endrer eller modifiserer betalingsordre	22	549	1.668	2.239
Svindleren manipulerer betaleren til en kortbetaling	49	6.886	393	7.328
Fjernbetaling uten sterk kundeautentisering				
Totalt transaksjonsbeløp	23.266.936	28.853.569	3.275.446	55.395.951
Hvorav svindel	2.500	34.749	12.033	49.282

Kilde: Finanstilsynet

Tap som følge av svindel ved bruk av nettbank

Svindeltype – nettbank (beløp i hele tusen kroner)	2015	2016	2017	2018	1. halvår 2019
Angrep ved bruk av ondartet programkode på kundens PC eller sikkerhetsmekanisme	3.055	2	727	1.252	201
Tapt/stjålet sikkerhetsmekanisme	963	8.758	1.892	1.959	69
Phishing og falske BankID-brukersteder	5.815	2.428	2.057	16.858	1.435
Annet/ukjent	2.715	7.444	2.911	6.723	1.932
Totalt	12.548	18.632	7.587	26.840	3.637

Kilder: Finanstilsynet og Bits AS

Kontooverføringer initiert elektronisk (beløp i hele 1000 kroner)	Transaksjoner i Norge	Grensekryss-ende i EØS	Grensekryss-ende utenfor EØS	2. Halvår totalt	Svindel-prosent
Totalt	188.219.191.694	25.188.476.543	5.978.582.637	219.386.250.875	
Svindel	41.716	130.886	129.027	301.629	0,00014
Hvorav ulike typer svindler:					
• Svindleren utsteder betalingen	21.297	9.700	10.876	41.873	
• Svindleren endrer eller modifiserer betalingsordren	475	4.069	0	4.544	
• Svindleren manipulerer betaleren til å utstede betalingsordren	19.944	117.944	118.151	256.039	

Kilde: Finanstilsynet

Tap som følge av svindel ved manipulering av betaleren

- Rapporterte tall indikerer tap på over 500 millioner kroner, mot i underkant av 300 millioner kroner i 2018

	2018	2019
Betaling for å leie et objekt mottager av pengene ikke eier	0,3 %	0,2 %
Innskudd etter løfter om store utbetalinger senere	3,1 %	2,4 %
Kjærlighet	29,7 %	8,7 %
Investeringer i falske selskaper	31,0 %	19,8 %
Betaling for varer som ikke leveres	4,0 %	0,8 %
Endret mottakerkonto	2,9 %	22,7 %
Direktørsvindel	11,4 %	37,6 %
Falsk faktura	11,1 %	4,1 %
Andre/nye typer	6,6 %	3,7 %

Kilder: Finanstilsynet og Bits AS

Digital kriminalitet

- Fortsatt betydelig økning i digitale angrep mot foretakene
- Foretakenes systemer for overvåking blir stadig bedre
- Angrepene avverges som oftest før de får konsekvenser for foretaket
- Ikke vært hendelser innen finansnæringen som kan kategoriseres alvorlig eller kritisk
- Skillet mellom trusselen fra organiserte kriminelle og fremmed etterretning viskes stadig mer ut
- Kriminelle aktører selger sine tjenester til statlige aktører
- PST og NSM peker på digital kartlegging og sabotasje av kritisk infrastruktur som en av de mest aktuelle truslene
- Arbeidet med å kartlegge risiko- og sårbarheter, iverksette preventive tiltak og forberede seg på å måtte håndtere angrep og følgeskadene av slike angrep må videreføres


Foto: Colourbox

Utkontraktering av IKT-virksomhet

- Behandlet i 2019 135 meldinger om ny eller endret utkontraktering av IKT, mot 161 meldinger i 2018
- Mer omfattende meldinger og kompleksiteten i utkontrakteringsforholdene har økt
- Foretakene blitt bedre til å håndtere utkontrakteringsavtalene
  - Risikoanalyser
  - Styrebehandling
  - Kvaliteten på avtalene
- Meldingene viser fortsatt klar tendens til økt bruk av skytjenester
- Økende kompleksitet i foretakenes løsninger pga. multi-sourcing
- For viktige leverandører bør foretakene etablere en samhandlingsmodell
- Kompleksiteten i samhandling mellom flere aktører utgjør en risiko
- Kontrollhandlingene ved utkontraktert virksomhet være minst like gode som ved egen intern virksomhet

Foto: Colourbox

Melding om systemer for betalingstjenester
Reautorisering og konsesjon til å yte betalingstjenester

- 21 meldinger om endrede eller nye betalingstjenester, bl.a.
  - Samarbeid mellom banker om betalingsløsninger
  - Nye løsninger for betaling med mobiltelefon
- 30 søknader knyttet til reautorisering og/eller konsesjon til å yte betalingstjenester
  - Flere foretak hadde på plass gode rutiner på IKT- og betalingstjenesterelaterte områder
  - Flere foretak hadde manglende forståelse av regelverket og behov for å vesentlig forbedre sine rutiner
- Fritak for reserveløsning iht PSD 2
- Utsatt frist for SKA ved bruk av betalingskort ved netthandel


Foto: Colourbox

Funn fra tilsynsvirksomheten

Banker

- Utilstrekkelig oppfølging av leverandører, spesielt etterlevelse av foretakets sikkerhetskrav
- Oppdatering og forbedring av sikkerhetsdokumentasjon. Manglende kontroll med at egne sikkerhetskrav etterleves
- Mangelfulle rutiner for informasjonsklassifisering og beskyttelse
- Risikoanalyser av IKT-virksomheten ikke avdekker reell risiko
- Svakheter i organisering av sikkerhetsarbeidet
- Svakheter i bankers kontinuitets- og kriseledelse
- Behov for bedre forberedelsene på å håndtere en evt. alvorlig cyber-hendelse
- Svakheter i kontrollen med uttrekk til AML-systemene

Betalingsforetak

- Risikoanalyser av IKT-virksomheten ikke avdekker reell risiko
- Utilstrekkelig oppfølging av leverandører, spesielt etterlevelse av foretakets sikkerhetskrav

Funn fra tilsynsvirksomheten

Verdipapirområdet

- Mangelfulle rutiner for informasjonsklassifisering og beskyttelse
- Mangler ved rutinene for sikkerhetstesting
- Mangler ved styring og kontroll med foretakets IKT-virksomhet og utkontraktert virksomhet
- Svakheter ved foretakets risikovurderinger for kritiske systemer
- Mangler ved foretakets beredskapsløsninger

Eiendomsmeglerforetak

- Systemstøttet kontroll av oppgjøret og kontroll av filer som overføres til nettbanken, er styrket siden tilsynet i 2016. Utbetalingsfilene krypteres, sikret mot tilsiktet manipulasjon.

Regnskap og revisjonsområdet

- Utkontraktert IKT-virksomhet uten at det foreligger skriftlige avtaler som i tilstrekkelig grad sikrer revisjonsselskapets styring, innsyn og kontroll
- Manglende retningslinjer for testing av forsvaret mot digital kriminalitet
- Vesentlige svakheter i revisjonsselskapers retningslinjer og rutiner for styring og kontroll med tilgang til konfidensiell informasjon

Foretakenes vurdering av risiko

- Økende kompleksitet i systemporteføljen medfører risiko og innebærer bl.a. følgende utfordringer:
  - Arbeidet med å utforme gode kriseløsninger kompliseres
  - Logger fra ulike systemer kan være vanskelig å sammenholde og svekker muligheten for å utnytte informasjonen i loggene
  - Etablere et helhetlig forsvar mot elektroniske angrep
  - Komplisert og tidkrevende feilsøking
  - Komplisert, omfattende og krevende arbeid med risikoanalyser
  - Manglende datakvalitet
- risikoen vurderes likevel som minkende
- Digitale angrep anses som en alvorlig og aktuell risiko
- Manglende sikkerhetsbevissthet øker faren for at angrep lykkes
- Leveransepresset anses som en risiko, men risikoen antas å bli dempet
- Omfanget av regulatoriske krav, herunder nye krav med kort frist for gjennomføring, som en betydelig utfordring og risiko


Foto: Colourbox

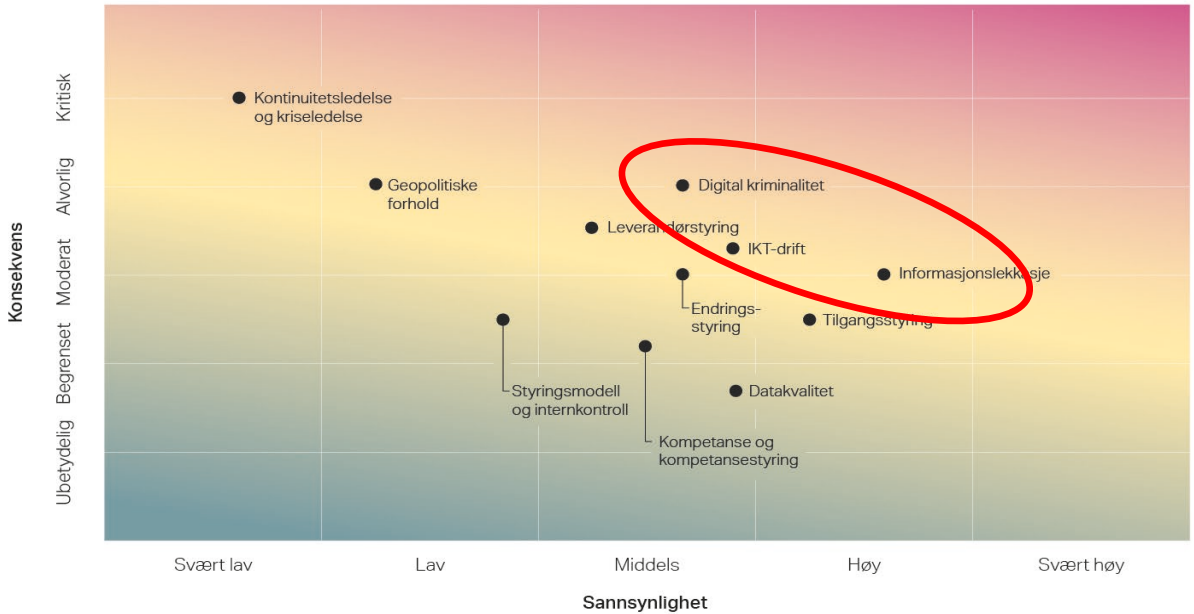
Risiko knyttet til kundenes tilgang til digitale tjenester

- BankID "universalnøkkel"
  - Effektivt
  - Den brede anvendelsen medfører risiko
- BankID brukes på mange forskjellige tjenester og ofte uten at det er lagt inn ytterligere kontroller for å forhindre misbruk
  - Skaper en sårbarhet for både kundene og foretakene
  - Risikoreduserende tiltak for ulike tjenester, tilpasset tjenestens egenart og potensialet for misbruk, bør vurderes
- De fleste finansielle tjenestene er basert på selvbetjening
- Stiller store krav til IKT-drift og informasjonssikkerhet
  - Tilgjengelighet
  - Konfidensialitet
  - Dataintegritet
- Krav til god oppfølging av kunder ved avvik i bruk av tjenestene
- Digitaliseringen har også gitt enkelte kundegrupper utfordringer
  - Det må etableres gode løsninger også for disse kundene


Foto: Colourbox

Oppsummerende vurdering av risikobildet knyttet til sårbarheter og trusler i foretakenes IKT-virksomhet

Finanstilsynets vurdering av risiko knyttet til sårbarheter og trusler



IKT-drift

Område	Sårbarheter og trusler som kan utgjøre en risiko for uønskede hendelser	Trend
IKT-drift	Kompleks integrasjon mellom systemer fra ulike leverandører, integrasjon mellom nye og gamle systemer, mange integrasjonspunkter mellom systemene, økt funksjonalitet i selvbetjente kanaler og økt bruk av skytjenester kan føre til utfordringer for sikker og stabil drift.	→

- Kompleks integrasjon mellom systemer fra ulike leverandører
- integrasjon mellom nye og gamle systemer
- mange integrasjonspunkter mellom systemene
- økt funksjonalitet i selvbetjente kanaler og
- økt bruk av skytjenester

kan føre til utfordringer for sikker og stabil drift


Foto: Colourbox

Digital kriminalitet

Område	Sårbarheter og trusler som kan utgjøre en risiko for uønskede hendelser	Trend
Digital kriminalitet	Manglende sikkerhetstester, sikkerhetsoppdateringer, opplæring og bevisstgjøring av ansatte samt mangelfull overvåking av aktiviteter i egen tekniske infrastruktur, herunder nettverk og systemer, kan føre til at kriminelle påfører foretaket skade gjennom digitale angrep.	↗

Manglende

- Sikkerhetstester
- Sikkerhetsoppdateringer
- Opplæring
- Bevisstgjøring
- Overvåking av teknisk infrastruktur; nettverk og systemer

kan føre til uønskede hendelser

Foto: Colourbox

Informasjonslekkasje

Område	Sårbarheter og trusler som kan utgjøre en risiko for uønskede hendelser	Trend
Informasjons-lekkasje	Manglende klassifisering av informasjon, herunder dokumentasjon, og kontroller for overvåking av informasjon som sendes ut på e-post, som kopieres til eksterne lagringsenheter eller kopieres til private skytjenester kan påføre foretaket eller dets kunder skade der uvedkommende får informasjonen i hende.	↗

Manglende

- klassifisering av informasjon
- kontroller for overvåking av informasjon som
  - sendes ut på e-post
  - kopieres til eksterne lagringsenheter
  - kopieres til private skytjenester

kan påføre skade der uvedkommende får informasjonen i hende

Foto: Colourbox

Geopolitiske forhold

Område	Sårbarheter og trusler som kan utgjøre en risiko for uønskede hendelser	Trend
Geopolitiske forhold	Utfordrende geopolitiske forhold eller brudd i kommunikasjonen mot utlandet, hvor leverandører blir forhindret fra å opprettholde leveranser av kritiske IKT-tjenester fra utlandet, kan føre til utfordringer med å opprettholde sikker og stabil drift.	↗

Utfordrende geopolitiske forhold og
Brudd i kommunikasjonen mot utlandet

- Leverandører blir forhindret fra å opprettholde leveranser av kritiske IKT-tjenester fra utlandet

Kan føre til utfordringer for sikker og stabil drift

Foto: Colourbox

Hovedtema for tilsynsvirksomheten på IKT- og betalingstjenesteområdet fremover

- Styring og kontroll med IKT-virksomheten
- Organisering av IKT-/cyber-sikkerhetsarbeidet
- Sikkerheten knyttet til foretakenes IKT-løsninger
- Beredskapsarbeid og testing av kontinuitets- og kriseløsninger
- Styring, kontroll og oppfølging av utkontraktert IKT-virksomhet
- Ytelse av betalingstjenester, herunder etterlevelse av det reviderte betalingstjenestedirektivet
- Sikkerheten i betalingstjenestene og kunderettede løsninger
- IKT-løsninger for å avdekke hvitvasking og terrorfinansiering
- Tilbud av kontanttjenester og kontantberedskap
- Oppfølging av IKT-hendelser
- Beredskapsarbeid rettet mot digital sårbarhet og digital sikkerhet
- Overvåke trusselbildet knyttet til digital kriminalitet

Oppsummering

- Den norske finansielle infrastrukturen er robust
- Tilgjengeligheten til tjenestene samlet sett bedre i 2019 enn i 2018
- Korona-situasjonen viste at de sentrale foretakene i den norske finansielle infrastrukturen har gode beredskapsplaner og kan raskt iverksette nødvendige tiltak
- Foretakene bør fortsatt styrke arbeidet innen IKT-området, både for å redusere sannsynligheten for avvik og for generelt å forbedre IKT-sikkerheten
- Foretakene har blitt bedre til å håndtere utkontrakteringsavtalene
- Svindel med sosial manipulering øker betydelig er for kriminelle den mest lukrative metoden
- Øvrig svindel øker. Utgjør liten andel av total transaksjonsverdi
- Kompleksiteten i den tekniske infrastrukturen øker og gir risiko på flere områder
- Fortsatt anses sårbarheter knyttet til foretaks forsvarsverk mot digital kriminalitet og informasjonslekkasje, samt IKT-drift, som de mest sentrale truslene knyttet til foretakenes bruk av IKT

FINANSTILSYNET

THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY