DI Analyse

Oktober 2025

Andreas Fernstrøm, chefanalytiker, afe@di.dk

To ud af tre har lav tillid til, at myndigheder kan efterforske eller retsforfølge cyberkriminelle

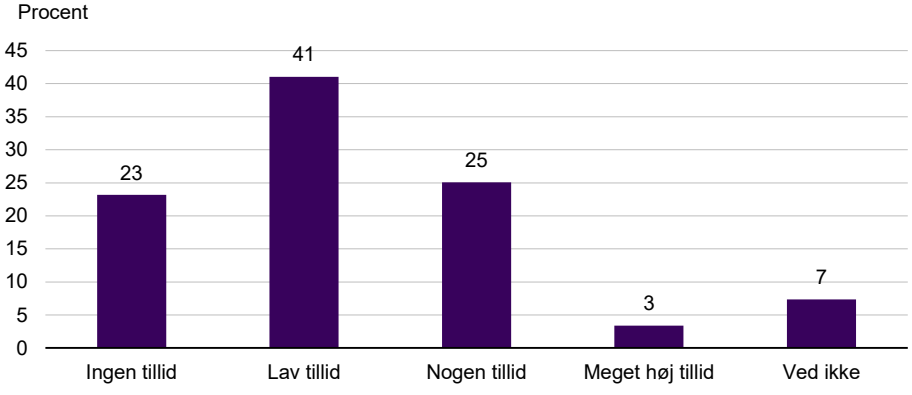
En ny analyse fra DI viser, at to ud af tre virksomheder har lav eller ingen tillid til, at politiet og øvrige myndigheder effektivt kan efterforske og retsforfølge cyberkriminalitet. Phishing og ransomware opfattes som de største trusler.

To ud af tre virksomheder har lav eller ingen tillid til politiets og øvrige myndigheders håndtering af cyberkriminalitet

Cyberkriminalitet er en relativt ny og stigende trussel mod erhvervslivet – men det er desværre også et fænomen, som er kommet for at blive. Det stiller store krav til politiet og myndighederne ift. at efterforske og retsforfølge

Ikke tillid til politiets muligheder inden for cyberkriminalitet

Hvor stor tillid har I til, at politiet og øvrige relevante myndigheder effektivt kan efterforske og retsforfølge sager inden for cyberkriminalitet?



Anm.: n = 475
Kilde: DI's virksomhedspanel, juni 2025

Dansk Industri

de kriminelle. Men det er krav, som erhvervslivet på nuværende tidspunkt ikke føler, at myndighederne effektivt kan løfte. Det er således to ud af tre virksomheder, som blot har lav eller ingen tillid til, at politiet eller andre myndigheder kan løfte opgaven, mens en ud af fire virksomheder har nogen tillid til, at de kan gøre det. Stort set ingen har høj tillid til myndighederne.

Resultat skal formentlig især ses i lyset af truslens grænseoverskridende karakter, vanskeligheder ved at slå effektivt ned på fødekæden af cyberkriminelle og virksomhedernes oplevelse af manglende respons efter anmeldelser af cyberkriminalitet, hvilket beskrives nærmere i whitepaperet fra DI og KPMG, der udfolder undersøgelsens resultater yderligere.[1]

Phishing og ransomware opfattes som de største trusler

Spørger man virksomhederne om, hvad der er de største trusler mod deres virksomhed, rettes spotlightet mod phishing blandt 60 pct. af dem, mens halvdelen peger på ransomware, hvor data krypteres og kun frigives mod løsesum. Færre end 10 pct. af virksomhederne ser ingen trussel fra cyberkriminalitet.

Store virksomheder ser flere trusler end mindre virksomheder

Samtidig er der relativt store forskelle, hvis man opdeler på størrelse. Det gælder særligt, når det kommer til ransomeware-angreb. Hver tredje af de mindste virksomheder ser det som en stor trussel, mens det er mere end 60 pct. for virksomheder med mindst 50 ansatte. Tilsvarende er der også en klar tendens til, at større virksomheder ser en trussel ved CEO-fraud. Det ses også, at virksomheder i bygge- og anlægsbranchen generelt ser lidt færre trusler.

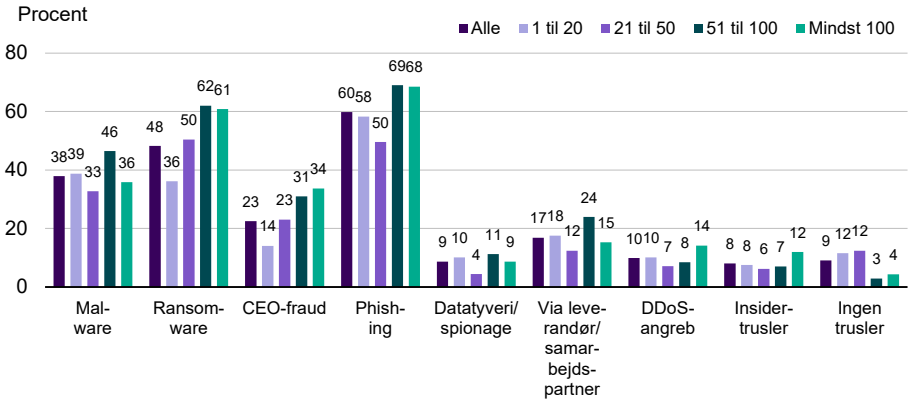
En af de i virksomhedernes øjne mellemstore trusler er usikkerheder via deres leverandører eller samarbejdspartnere, som 17 pct. peger på. Det interessante ved denne trussel er, at det er den trussel, som det europæiske agentur for cybersikkerhed peger på som den største trussel i 2030.[2]

1 Whitepaper findes på denne side, Løsninger i bekæmpelsen af cyberkriminalitet i Danmark

2 European Union Agency for Cybersecurity, Foresight Cybersecurity Threats for 2030 – Update, marts 2024.

Phishing og ransomware opfattes som de største trusler

Hvilke former for cyberkriminalitet vurderer I som de største trusler mod jeres forretning?



Anm.: Mulighed for op til tre svar. "Ved ikke" og "Andet" er ikke vist i figuren. n = 475
Kilde: DI's virksomhedspanel, juni 2025

Fire ud af ti har en beredskabsplan, en ekstern leverandør, der kan hjælpe eller en forsikring, der dækker ekstern hjælp

Hvis virksomhederne er under et cyberangreb, er der store forskelle på, hvilke muligheder de har for at afbøde angrebet. Der er dog nogle elementer i beskyttelsen, som går igen blandt godt 40 pct. af virksomhederne. Det er en beredskabsplan, en fast aftale med en ekstern leverandør, der kan hjælpe med at afbøde hændelser, og en cyberforsikring, der dækker ekstern hjælp. I den modsatte ende af skalaen har hver tiende virksomhed begrænset eller ingen forberedt reaktionskapacitet.[3]

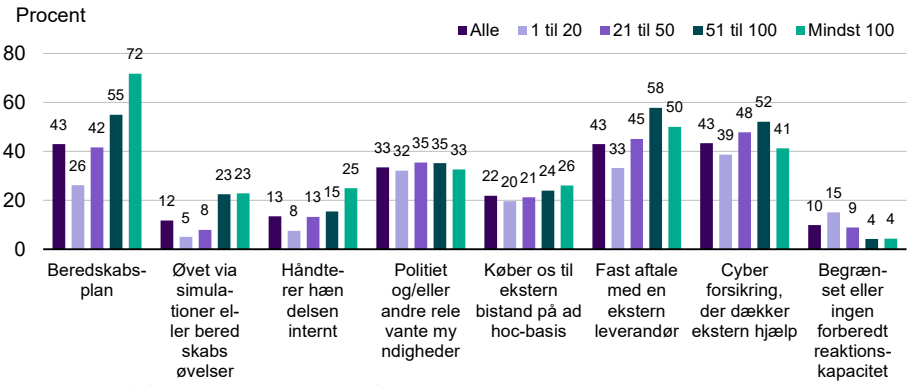
Større virksomheder har flere tiltag for at afbøde konsekvenser er cyberkriminalitet

Generelt gælder det, at de større virksomheder i højere grad end de mindre har forberedt sig på cyberkriminalitet. Især i udarbejdelsen af beredskabsplaner er der markante forskelle. Hver fjerde virksomhed med op til 20 ansatte har udarbejdet en beredskabsplan, mens det næsten er tre ud af fire af virksomhederne med mindst 100 ansatte.

I forhold til forsikringer mod cyberkriminalitet kunne man formode, at de virksomheder, der har tegnet sådan en, i mindre grad end andre virksomheder sikrer sig mod cyberkriminalitet på andre måder ud fra en tanke om, at man er "dækket ind". Det er dog ikke tilfældet. Vi ser i stedet det modsatte. Nemlig at virksomheder med en forsikring mod cyberkriminalitet i højere grad end andre virksomheder også foretager andre tiltag.

3 DI har tidligere offentliggjort en analyse, hvor der indgik tal for beredskabsplaner og om man har øvet sig. Her var tallet større. Årsagen er, at i den tidligere analyse, var resultatet vægtet med beskæftigelsen, da fokus var på hvor hårdt Danmark kunne blive ramt. I denne analyse er der ikke vægtet med beskæftigelse, da vi her har fokus på hvor stor en andel af virksomhederne, som er omfattet af de forskellige spørgsmål.

Flest har en beredskabsplan, forsikring eller bruger ekstern hjælp
I tilfælde af et alvorligt cyberangreb, hvilke muligheder har I for at reagere/afbøde



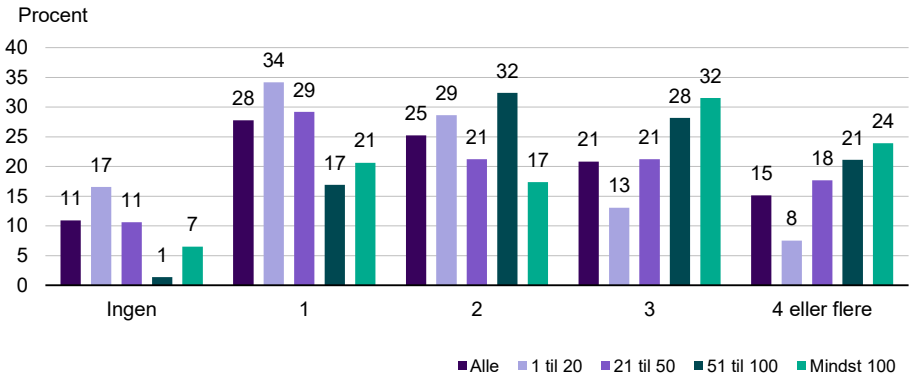
Anm.: Mulighed for flere svar. "Ved ikke" er ikke vist i figuren. n = 475
Kilde: DI's virksomhedspanel, juni 2025

Hver anden virksomhed har et eller to tiltag mod cyberkriminalitet

Ser man på antallet af tiltag mod cyberkriminalitet, som virksomhederne har sat i værk, ses det, at godt halvdelen har et eller to tiltag, mens ca. hver tredje virksomhed har tre eller flere tiltag. Godt hver tiende virksomhed har angivet, at de ikke har iværksat tiltag.

I forhold til antallet af foranstaltninger er der en markant forskel i forhold til virksomhedernes størrelse. Ca. hver anden virksomhed med mindst 50 ansatte har tre eller flere tiltag, mens det blot er hver femte for virksomheder med op til 20 ansatte.

Hver anden har en eller to foranstaltninger mod cyberangreb
Antal foranstaltninger for at reagere/afbøde hændelsen af cyberangreb?



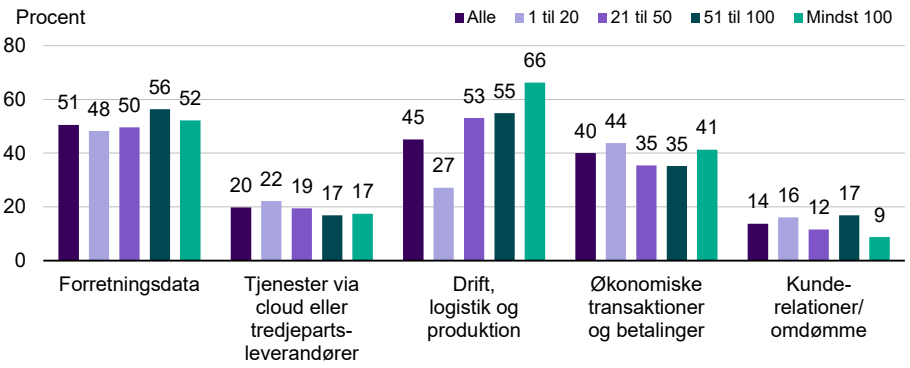
Anm.: Der er talt over de op til syv foranstaltninger, som ikke er Ingen eller ved ikke. n = 475
Kilde: DI's virksomhedspanel, juni 2025

Forretningskritisk data og driften er det vigtigste at beskytte for virksomhederne

Det er forretningskritiske data og driften, som er vigtigst for virksomhederne at beskytte. I omegnen af hver anden virksomhed peger på disse to elementer, som begge er vitale for at kunne fortsætte sin virksomhed, selvom man er udsat for cyberkriminalitet.

På de fleste områder af virksomhedernes kerneforretning er der ikke store forskelle, når der opdeles på størrelse. Det er der dog, hvis vi ser på drift og produktion, som er markant vigtigere for de største virksomheder. Det er således to ud af tre virksomheder med mindst 100 ansatte, der peger på driften som vigtigst at beskytte, mens det blot er hver fjerde virksomhed med op til 20 ansatte. Samtidig ses det også, at industrivirksomheder i højere grad end resten af erhvervslivet er bekymret for deres drift og produktion.

Forretningsdata og driften er det vigtigste at beskytte
Hvilke dele af jeres kerneforretning er det vigtigst for jer at beskytte mod



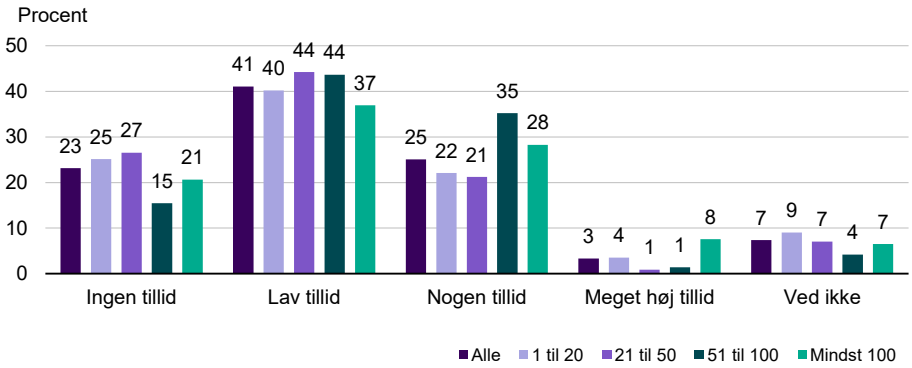
Anm.: Mulighed for op til to svar. "Ved ikke" er ikke vist i figuren. n = 475
Kilde: DI's virksomhedspanel, juni 2025

Store virksomheder har lidt større tillid til politiet og myndighederne end de mindre virksomheder

Som det blev vist i starten, er der en overvægt af virksomhederne, der ikke har tillid til, at politiet og relevante myndigheder kan løfte opgaven med at efterforske og retsforfølge de cyberkriminelle. Dykkes der ned i tallene, ses det, at de større virksomheder har lidt større tillid til politiet end de mindre virksomheder. Der er således op mod 40 pct. af de største virksomheder, der har nogen eller meget høj tillid, mens det blot er i omegnen af hver fjerde blandt mindre virksomheder. Der er til gengæld ikke de store forskelle i tilliden, hvis der opdeles på brancher.

Til gengæld ses det, at de virksomheder, som vil kontakte politiet, hvis de rammes af cyberkriminalitet også har større tillid til politiet, end dem der ikke vil kontakte politiet.

De større virksomheder har lidt større tillid til politiet
Hvor stor tillid har I til, at politiet og øvrige relevante myndigheder effektivt kan



Anm.: n = 475
Kilde: DI's virksomhedspanel, juni 2025

Sådan har vi gjort

Analysen bygger på en spørgeundersøgelse blandt DI's medlemmer foretaget mellem den 3. juni og 16. juni. 475 virksomheder, der til sammen repræsenterer 57.000 ansatte i Danmark, har svaret på undersøgelsen.

I indeværende analyse er der taget udgangspunkt i fire spørgsmål, som vises nedenfor. I figurerne kan svarmulighederne være forkortet af pladsmæssige hensyn, men de fremgår nedenfor i fuld længde.

Spørgsmål 1: Hvilke former for cyberkriminalitet vurderer I som de største trusler mod jeres forretning? (Sæt max 3 krydser)

- Malware-angreb (manipulation af digitale produkter/software)
- Ransomware-angreb (kryptering af data og krav om løsesum)
- CEO-fraud / Business Email Compromise (svindel via falske mails fra ledelsen)
- Phishing (falske e-mails)
- Datatyveri/spionage (fx persondata eller forretningshemmeligheder)
- Angreb via leverandør- eller samarbejdspartner
- DDoS-angreb (overbelastning af netværk og systemer)
- Insider-trusler (utilsigtede eller tilsigtede handlinger fra medarbejdere)
- Vi vurderer ikke cyberkriminalitet som en umiddelbar trussel mod vores forretning
- Ved ikke
- Andet

Spørgsmål 2: Hvilke dele af jeres kerneforretning er det vigtigst for jer at beskytte mod cyberkriminalitet? (Sæt max 2 krydser)

- Forretningsdata (fx kundeoplysninger, persondata og interne forretningsdata)
- Tjenester leveret via cloud eller tredjepartsleverandører
- Drift, logistik og produktion (fx ved ransomware eller systemnedbrud)
- Økonomiske transaktioner og betalinger (fx svindel eller misbrug)
- Kunderelationer/omdømme
- Ved ikke

Spørgsmål 3: I tilfælde af et alvorligt cyberangreb, hvilke muligheder har I for at reagere/afbøde hændelsen? (Angiv gerne flere svar)

- Vi har en beredskabsplan
- Vi har øvet håndteringen via simulationer eller beredskabsøvelser
- Vi håndterer hændelsen internt (f.eks. via et etableret SOC-team)
- Vi henvender os til politiet og/eller andre relevante myndigheder
- Vi kan købe os til ekstern bistand på ad hoc-basis
- Vi har en fast aftale med en ekstern leverandør, der kan hjælpe os med at håndtere hændelser
- Vi har en cyberforsikring, der dækker ekstern hjælp
- Vi har begrænset eller ingen forberedt reaktionskapacitet
- Ved ikke

Spørgsmål 4: Hvor stor tillid har I til, at politiet og øvrige relevante myndigheder effektivt kan efterforske og retsforfølge sager inden for cyberkriminalitet?

- Meget høj tillid – hurtig og kompetent indsats
- Nogen tillid – gode intentioner, men kapaciteten halter
- Lav tillid – mangler i højere grad ressourcer, ekspertise eller tempo
- Ingen tillid – myndighederne kan ikke håndtere opgaven
- Ved ikke