SVENSKT NÄRINGSLIV

BROTTS-BAROMETERN 2025

Förord

Svenska företag är motorn i tillväxt och sysselsättning – och en bärande del av landets välfärd, trygghet och motståndskraft. Näringslivet har en central roll i totalförsvaret och i att upprätthålla samhällsviktiga funktioner även vid kriser och krig. När företag drabbas av brott som bedrägerier, stölder, cyberattacker eller otillåten påverkan hotas inte bara deras verksamhet, utan hela samhällets stabilitet. Ett starkt företagande är därför en förutsättning för Sveriges försörjningsberedskap, tillväxt och säkerhet.

Mot denna bakgrund visar Brottsbarometern 2025 tydligt att brott mot företag är ett växande samhällsproblem. Fler än fyra av tio företag har utsatts för brott det senaste året, vilket leder till ekonomiska förluster, minskad konkurrenskraft och ökad otrygghet. Bedrägerier är vanligast – ett av fem företag har drabbats – och handeln är mest utsatt, med nästan sex av tio drabbade företag. Särskilt oroande är den låga anmälningsbenägenheten och det bristande förtroendet för polisens förmåga att hantera brott mot företag. Det riskerar att leda till att brottens verkliga omfattning inte synliggörs – och att samhällets insatser därför förblir otillräckliga i förhållande till problemens allvarlighetsgrad och omfattning.

Rapporten visar också att mer än vart tionde företag bedömer att deras verksamhet kan utsättas för otillåten påverkan, exempelvis hot, påtryckningar eller infiltration som syftar till att påverka beslut eller verksamhet inifrån.

Den visar att brottsligheten mot företag inte längre kan ses som enskilda händelser, utan som ett mönster som riskerar att försvaga företagens konkurrenskraft, tillväxt och förtroendet för rättsstaten. Konsekvenserna sträcker sig långt bortom de enskilda företagen till att påverka samhällsekonomin i stort. Det är därför avgörande att brott mot företag betraktas som ett samhällshot och inte reduceras till ett företags- eller branschproblem.

För att vända utvecklingen krävs en gemensam kraftsamling på nationell nivå där brott mot företag sätts högst på agendan. Näringsliv, myndigheter och kommuner måste arbeta tillsammans – förebyggande, långsiktigt och strategiskt. Samarbetet måste handla om att bygga motståndskraft, inte bara hantera konsekvenser

Svenskt näringsliv är fast besluten att vara en strategisk partner i det arbetet. Ett tryggt företagsklimat är en grundförutsättning för tillväxt, välfärd, försörjningsberedskap och nationell säkerhet. Denna rapport är ett underlag för handling – och en uppmaning till ansvarstagande – tillsammans.

Avslutningsvis vill jag framföra ett särskilt tack till Anna Thoursie, doktor i nationalekonomi, som med stor professionalism och gedigen expertis har sammanställt denna rapport. Hennes omfattande erfarenhet och analytiska förmåga har varit central för rapportens kvalitet och fördjupning.

Lena Nitz
Jurist, Expert brottslighet och trygghet,
Svenskt Näringsliv

Sammanfattning

Den brottslighet som drabbar företag i Sverige är ett samhällsproblem, inte ett företagsproblem. Svenskt Näringsliv nya rapport, Brottsbarometern 2025, visar hur brottsligheten nu tar sig uttryck, varför den är så allvarlig och vilka värden den hotar, och därmed varför bekämpningen av brott mot näringslivet behöver tas på ännu större allvar än hittills.

Brottslighet riktad mot företag – från enmansföretag till stora koncerner – är nu så vanligt att Brottsförebyggande rådet (Brå) skriver i sin rapport *Brott mot företag* (2025) att ”Risken för företag att utsättas för brott tycks därmed utgöra en inte oväsentlig del av företagens villkor.”

I denna rapport visar Svenskt Näringsliv bland annat följande.

Brottslighetens omfattning och mönster

- **UTSATTHET:** I genomsnitt har fler än 4 av 10 företag utsatts för brott under de senaste 12 månaderna.
- **BRANSCHER:** Mest drabbade är företag i handeln, där närmare 6 av 10 företag har utsatts för brott, följt av företag i besöksnäringen och byggbranschen, där nära hälften av företagen har varit brottsutsatta. Företag i transportbranschen, industrin och tjänstebranschen ligger något under genomsnittet, men även där är minst en dryg tredjedel drabbade.
- **BROTTSTYPER:** Vanligast är bedrägerier, där en så hög andel som ett av fem företag drabbats. Därefter följer ringa stöld/snatteri, inbrott/stöld, cyberbrott och skadegörelse. Efter det kommer hot, trakasserier, immaterialrättsliga intrång, utpressning, mutförsök, och i sällsynta fall våld och infiltration.
- **MÄNGDBROTT OCH ORGANISERAD BROTTSLIGHET:** Det finns en allt tydligare koppling mellan organiserad brottslighet och mängdbrott, främst stölder och bedrägerier.
- **GEOGRAFI:** Västmanland har högst andel brottsutsatta företag (55 procent). Utsattheten är högre i mellersta och södra Sverige, med närhet till storstäder och gränsöverskridande ligor.

Anmälningsbenägenhet och polisens kapacitet

- **LÅG ANMÄLNINGSBENÄGENHET:** Omkring hälften av de brottsutsatta företagen polisanmäler inte att de utsatts för brott. Det främsta skälet är en låg tilltro till att polisen ska klara upp brottet.
- **BRANSCHSKILLNADER:** Byggbranschen har högst anmälningsgrad, följt av transportbranschen. Branscherna handel och besöksnäring har lägst anmälningsgrad, delvis på grund av att snatteri är så vanligt och ofta upplevs som ”inte lönt att anmäla”. Men andelen företag som utsatts för hot och trakasserier är högst i handeln och besöksnäringen (nästan vart femte företag är utsatt). Rädsla för att möta gärningspersonerna i en (eventuell) rättegång kan dra ned viljan att polisanmäla.
- **NEGATIV SPIRAL:** En stor andel av brottsutsatta företag bedömer polisens hantering av mängdbrott som bristfällig. Det blir en negativ spiral som startar med polisens bristande kapacitet att klara upp brott: Låg uppklaringsgrad hos polisen → låg anmälningsbenägenhet hos brottsutsatta företag → sämre lägesbild av brottsligheten → felprioriteringar i polisens resursfördelning, vilket förstärker problemet med låg uppklaringsgrad.

Otillåten påverkan mot företag

- **BEDÖMD RISK:** I genomsnitt anser fler än 1 av 10 företag att de i hög eller ganska hög utsträckning kan utsättas för otillåten påverkan. Risken bedöms vara högst i byggbranschen och besöksnäringen. Fler än 6 av 10 företag bedömer dock att den utsträckning som de kan bli utsatta för otillåten påverkan är icke-existerande, mycket låg , eller ganska låg.
- **FÖREBYGGANDE ÅTGÄRDER:** Viktigast, enligt de företag som bedömer att de i hög eller ganska hög utsträckning kan utsättas för otillåten påverkan, är förbättrad IT-säkerhet, säkerhetsutbildning (t.ex. i digital säkerhet, social manipulation och påverkansförsök) samt bakgrundskontroller vid rekrytering. Rutiner för att upptäcka/hantera IT-attacker och försök till otillåten påverkan kommer strax därefter.
- **KUNSKAPSLUCKA:** Cirka vart tionde företag svarar att de inte vet om deras verksamheter kan bli utsatta för otillåten påverkan. Av de företag som bedömer att de i hög eller ganska hög utsträckning kan utsättas för otillåten påverkan är det närmare 1 av 10 som svarar att de inte vet vilka åtgärder som de tror är viktiga för att undvika otillåten påverkan. Det kan tyda på att många företag inte är tillräckligt förberedda på att otillåten påverkan kan drabba dem. Till skillnad från exempelvis inbrott eller skadegörelse handlar otillåten påverkan ofta om handlingar som är svårupptäckta – de är handlingar som är avsedda att inte synas.

Cyberbrott och gråzon mot otillåten påverkan

- **SÄLLAN ANMÄLT, OFTA KOSTSAMT:** Cyberbrott polisanmäls i mycket låg grad trots stora skador (bl.a. driftstopp, datastölder, utpressningsvirus och förlorat förtroende för företaget om dataläckan kommer ut till media). Små och medelstora företag är särskilt sårbara.
- **GRÅZON:** Det finns en gråzon mellan cyberbrott och otillåten påverkan som är svår att fånga i statistik. Gråzonen uppstår när cyberbrott används som en form av utpressning, t.ex. hot om att läcka data och överbelastningsattacker för att stressa fram beslut. Detta gör händelserna svåra att rubricera och leder till underrapportering.
- **HOTAKTÖRER:** Kriminella nätverk och främmande makt utnyttjar tekniska och mänskliga sårbarheter, ibland i kombination.

Framåtblickande:

- **PROGNOS:** Hälften av företagen tror att brottsligheten i samhället kommer att öka det kommande året.
- **VIKTIGA ÅTGÄRDER:** Den viktigaste åtgärden för att öka tryggheten för företagen och dess anställda är ökad närvaro av polis, väktare eller ordningsvakter. Tätt efter kommer snabbare och mer effektiv hantering av brottsanmälningar. På en delad tredjeplats kommer ökad samverkan mellan företag, kommun och polis samt bättre kameraövervakning.

Konsekvenser av brottslighet mot företag

50%

av företagen tror att brottsligheten i samhället kommer att öka det kommande året.

- **FÖR FÖRETAGEN:** Direkta förluster (i form av t.ex. intäktstapp, produktionsstopp och skador på egendom) och följdkostnader (i form av t.ex. säkerhetsinvesteringar och högre premier), samt försämrat kassaflöde—särskilt för små och medelstora företag. Psykologiska effekter (som oro och stress) påverkar produktivitet och beslut. Brott och otrygghet leder till inställda investeringar, rekryteringssvårigheter och i vissa fall nedläggningar.
- **FÖR SAMHÄLLET:**
  - Brott mot företag medför betydande samhällsekonomiska kostnader genom ökad belastning på rättsväsendet och minskad produktivitet i näringslivet. Företag tvingas omfördela resurser från investeringar till säkerhetsåtgärder, vilket på sikt hämmar tillväxt, sysselsättning och innovation.
  - När företag lämnar brottsutsatta områden urholkas det lokala näringslivet och en negativ spiral av ekonomisk stagnation och socialt förfall kan uppstå.
  - Särskilt allvarligt är otillåten påverkan, där hot, korruption eller trakasserier kan snedvrida företags beslut och undergräva principerna om fri konkurrens och rättssäkerhet.
  - Om den organiserade brottsligheten lyckas med att exploatera strategiska sårbarheter i näringslivet så kommer den att utgöra ett samhällshot och i förlängningen även ett systemhot.
  - Samhällshotande brottslighet påverkar människors tillit och trygghet. Den utgör betydande hot mot samhället eftersom den drabbar många individer och företag i vardagen men skyddsvärda samhällsfunktioner står kvar oskadda.
  - Systemhotande brottslighet är ett direkt angrepp mot skyddsvärda samhällsfunktioner, deras system eller företrädare samt påverkar deras beslut och hotar att skada institutionernas förmåga att fullgöra sina uppgifter.

Vad krävs?

En effektiv brottsbekämpning kräver ett tätt samarbete mellan stat, kommun, polis och näringsliv. Svenskt Näringsliv vill och kan vara en konstruktiv samarbetspartner i detta. Rapporten presenterar Svenskt Näringslivs 16 uppmaningar till beslutsfattare i regeringen och riksdagen, på Polismyndigheten samt på kommunal nivå. Några av dessa är.

- **REGERING OCH RIKSDAG:** Prioritera bekämpningen av mängdbrott; Stärk det förebyggande arbetet mot brott som drabbar näringslivet genom en nationell samordning; Skärp straffen för systematiskt begångna brott; Komplettera brottsstatistiken med brottskoder som identifierar brott mot företag; Förstärk cybersäkerhetssamverkan.
- **POLISMYNDIGHETEN:** Öka lokal polisnärvaro; Effektivisera anmälnings- och utredningsflöden; Prioritera mängdbrott; Tillsätt en specialiserad funktion för kartläggning av otillåten påverkan mot näringsliv och myndigheter samt en specialiserad funktion för näringslivskontakter.

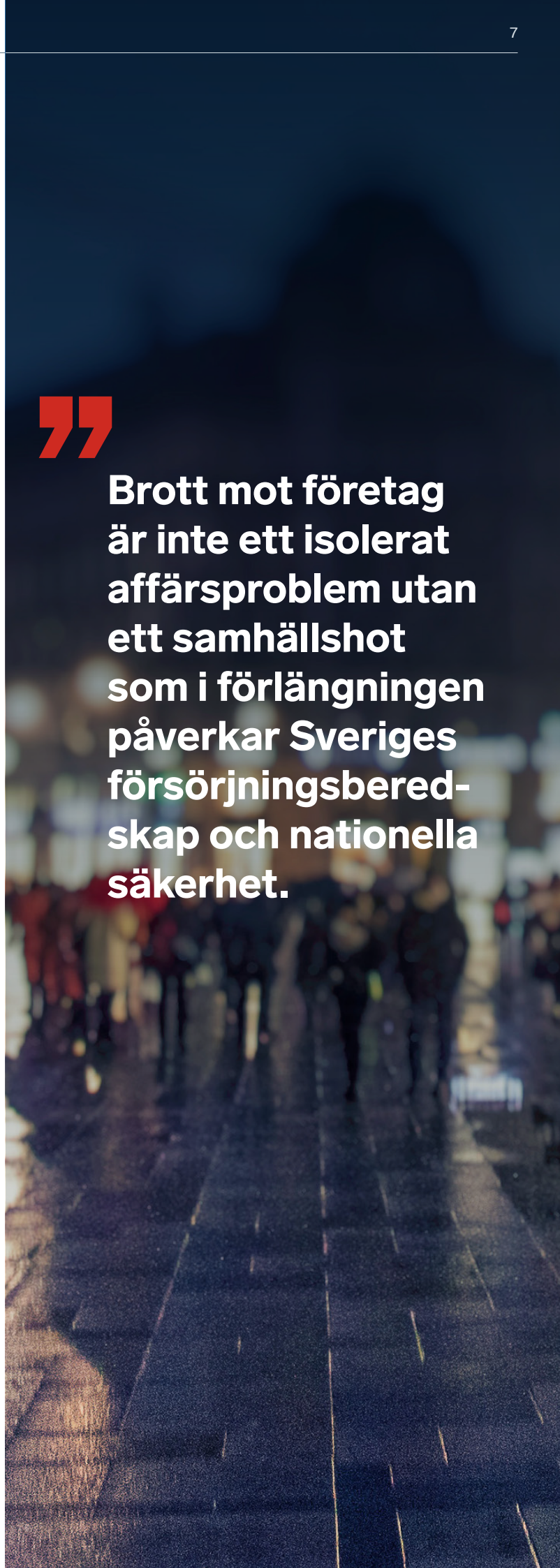
- **KOMMUNERNA:** Skapa kompletta lokala lägesbilder; Involvera näringslivet i lokala åtgärdsplaner; Integrera åtgärder mot brott och otrygghet som vitala delar av varje kommuns näringslivsstrategi.

Enskilda företag kan inte ensamma värna sig mot den kriminalitet som riktas mot näringslivet. Brott mot företag är inte ett isolerat affärsproblem utan ett samhällshot som i förlängningen påverkar Sveriges försörjningsberedskap och nationella säkerhet.

Försörjningsberedskapen bygger på att företag i hela landet – inom allt från transport och energi till livsmedel och digital infrastruktur – kan fungera även under påfrestning. När företag drabbas av brott, t.ex. cyberbrott, riskerar centrala flöden och funktioner att slås ut.

En samlad mobilisering krävs. Kommuner, regioner, polis, rättsväsende och statliga myndigheter behöver samarbeta med näringslivet i ett systematiskt och kunskapsbaserat brottsförebyggande arbete. Det handlar inte bara om att skydda enskilda verksamheter, utan om att stärka Sveriges resiliens och motståndskraft som helhet.

För att vända utvecklingen krävs ett gemensamt ansvarstagande och en tydlig nationell inriktning där företag ses som en integrerad del av landets säkerhetsarkitektur. Att skydda näringslivet från kriminalitet är att skydda Sveriges välfärd, beredskap och säkerhet.



Brott mot företag är inte ett isolerat affärsproblem utan ett samhällshot som i förlängningen påverkar Sveriges försörjningsberedskap och nationella säkerhet.

Innehåll

FÖRORD ... 3

SAMMANFATTNING ... 4

BROTT MOT FÖRETAG – ETT ALLVARLIGT PROBLEM MED SAMHÄLLSKONSEKVENSER ... 10

FÖRETAGENS UTSATTHET FÖR BROTT 2025 ... 13

- Fler än fyra av tio företag har utsatts för brott ... 13
- Handeln, besöksnäringen och byggbranschen mest utsatta för brott ... 13
- Bedrägerier, snatterier, stölder, inbrott och cyberbrott vanligaste brotten mot företag ... 14
- Högst andel brottsutsatta företag i Västmanland ... 18
- Omkring hälften av de brottsutsatta företagen polisanmäler inte ... 20
- Cyberbrott anmäls ytterst sällan men kan orsaka stora skador ... 24
- Otillåten påverkan riktad mot företag ... 26
- Gråzon mellan cyberbrott och otillåten påverkan ... 32
- Hälften av företagen tror att brottsligheten kommer att öka ... 34

VILKA BLIR KONSEKVENSERNA FÖR BROTTSUTSATTA FÖRETAG? ... 35

- Ekonomiska förluster och ökade kostnader ... 35
- En negativ spiral: Polisens bristande kapacitet att klara upp brott bidrar till att många brott mot företag aldrig anmäls ... 35
- Oro för eller utsatthet för brott ger effekter på investeringar och rekryteringar ... 37
- Osund konkurrens drabbar seriösa företag ... 37
- Ökad polisnärvaro och effektiv hantering av brottsanmälningar viktigast för ökad trygghet ... 38

VILKA BLIR KONSEKVENSERNA FÖR SAMHÄLLET AV BROTTSLIGHET MOT FÖRETAG? ... 39

- Kort- och långsiktiga konsekvenser ... 39
- Samhällshotande och systemhotande brottslighet ... 40

VAD KRÄVS FÖR EN FRAMGÅNGSRIK BROTTSBEKÄMPNING? ... 41

REFERENSER ... 43

BILAGA – DATA OCH METOD ... 45

Brott mot företag
– ett allvarligt problem med samhällskonsekvenser

Syfte

Rapportens syfte är att kartlägga omfattning och konsekvenser av brott mot företag i Sverige, att där så är möjligt jämföra utvecklingen över tid samt att belysa konsekvenserna för samhället av denna kriminalitet.

Brott mot företag i Sverige är i dag ett allvarligt problem som berör hela näringslivet – från små enmansföretag till stora koncerner. Brottsförebyggande rådet (Brå) skriver i sin rapport *Brott mot företag* att ”Risken för företag att utsättas för brott tycks därmed utgöra en inte oväsentlig del av företagens villkor.”[1]

Företag utsätts för ett stort antal brottstyper, som bedrägerier, stölder, snatterier, inbrott och cyberbrott samt otillåten påverkan i form av exempelvis hot och utpressning. Gemensamt är att de inte bara innebär direkta ekonomiska förluster utan också skapar en otrygghet som riskerar att hämma företagsamhet och investeringar. För många mindre företag kan ett enskilt brott få avgörande konsekvenser för verksamhetens fortlevnad.

När företag pressas av återkommande brottslighet minskar deras konkurrenskraft. Resurser som borde användas för innovation, sysselsättning och tillväxt tvingas i stället läggas på säkerhetsåtgärder. På lokal nivå kan kriminalitet dessutom underminera tilliten mellan aktörer i samhället – särskilt i mindre orter där företagare och kunder ofta är nära sammanlänkade. Företagare i utsatta områden är särskilt exponerade för brottslighet.

Förutom att leda till negativa ekonomiska konsekvenser får brott mot företag ofta psykologiska och sociala effekter, såväl för företagare som för deras anställda. Att bli utsatt för stölder, hot eller våld leder till en ökad oro i vardagen. Många brottsutsatta företagare väljer att inte polisanmäla för att de upplever att en anmälan inte leder någonstans. Vissa företagare avstår på grund av rädsla för repressalier. För de företagare som ändå anmäler

1 Brå (2025b), sid. 14 och 81.

uppstår ofta en administrativ börda i samband med polisanmälan, försäkringsprocess och skadereglering som förstärker den psykiska belastningen. Flera upplever en känsla av orättvisa och vanmakt över att rättssystemet inte förmår skydda dem eller beivra brotten.

Organiserad brottslighet exploaterar strategiska sårbarheter i näringslivet. Den utgör ett samhällshot och, om dess utbredning inte hindras, även ett systemhot. Samhällshotande brottslighet påverkar människors vardag, tillit och trygghet. Systemhotande brottslighet är organiserad kriminalitet som, genom, hot, våld, ekonomiska nätverk och parallella strukturer, underminerar samhällets grundläggande funktioner, skyddsvärda institutioner och deras legitimitet.

Mot denna bakgrund är det angeläget att analysera brott mot företag, inte enbart som affärsriskproblem, utan som ett samhällshot, och i förlängningen även ett systemhot. Rapporter från myndigheter, statliga utredningar, arbetsmarknadens parter och intresseorganisationer visar att den organiserade brottsligheten ökat i omfattning och hittat allt fler ingångar till reguljära marknader, till myndighetsutövande och till civilsamhället.[2] Under senare år har intresset för dessa frågor även från det samhällsvetenskapliga forskarsamhället ökat, exempelvis satsningen Sverige mot organiserad brottslighet, SMOB.[3]

Den ökade uppmärksamhet som riktats mot näringslivets sårbarhet för brott, och vad denna sårbarhet betyder för hela samhällets säkerhet och försörjningsberedskap, är välkommen men än så länge inte tillräcklig. Åtgärderna är ofta reaktiva snarare än förebyggande, och brottsutsatta företagare bedömer generellt polisens arbete som mycket ineffektivt. Det behövs en tydlig nationell inriktning med samordnade insatser mellan myndigheter och näringsliv för att stärka motståndskraften i de funktioner som är avgörande för Sveriges tillväxt, välfärd och nationella säkerhet.

Data och metod

Rapporten baseras på resultat från de digitala enkätundersökningar om brottslighet mot företag som årligen genomförs bland medlemsföretag i Svenskt Näringslivs Företagarpanel. Den senaste undersökningen i Företagarpanelen gjordes april–maj 2025.

Vidare ingår vissa resultat från den undersökning som Demoskop gjorde under februari–maj 2025 på uppdrag av Svenskt Näringsliv. I den kvantitativa delen låg fokus på att skatta andelen företag som utsatts för brott som innefattar olika typer av otillåten påverkan. I den kvalitativa delen låg fokus på att utforska och förstå upplevelser hos företag och företagare som utsatts för otillåten påverkan med särskilt tyngdpunkt på riskmedvetenhet, händelseförlopp, anmälningsprocess och framtida stödbehov.

Slutligen ingår några av resultaten från den lägesbild som tagits fram som en del av den samverkansöverenskommelse som slöts 2024 mellan Svenskt Näringsliv och Polismyndigheten. Lägesbilden fokuserar på hur otillåten påverkan drabbar privata företag.

Se vidare bilagan Data och metod för en utförligare beskrivning av undersökningarna.

2 Se t.ex. Brå (2025a, 2025b); Entreprenörskapsforum (2025); Europol (2025); Företagarna (2022, 2023, 2024); Konkurrensverket (2020); Myndighetsgemensam lägesbild (2023, 2025); Nationellt cybersäkerhetscenter (2024); Rostami & Mondani (2024); SOU 2023:8; Stockholms Handelskammare (2022); Svenskt Näringsliv (2023a, 2023b, 2024); Truesec (2025); Tryggare Sverige (2024).

3 SMOB (2024).

Brott företag i olika branscher utsatts för de senaste 12 månaderna

Handeln:

- Ringa stöld/Snatteri 35%
- Bedrägeri 26%
- Cyberbrott 10%

Besöksnäringen:

- Bedrägeri, 23%
- Ringa stöld/Snatteri 19%
- Skadegörelse 10%
- Trakasserier 10%
- Hot 10%

Byggbranschen:

- Inbrott/Stöld 22%
- Bedrägeri 17%
- Ringa stöld/Snatteri 12%

Transportnäringen:

- Bedrägeri 14%
- Inbrott/Stöld 13%
- Ringa stöld/Snatteri 11%

Industrin:

- Bedrägeri 18%
- Cyberbrott 11%
- Inbrott/Stöld 9%

Tjänstesektorn:

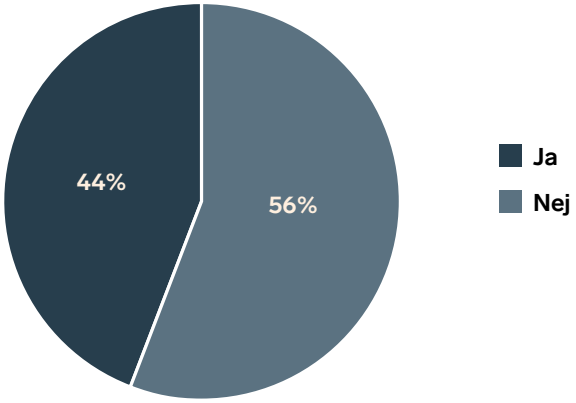
- Bedrägeri 17%
- Cyberbrott 10%
- Inbrott/Stöld 6%
- Skadegörelse 6%

Företagens utsatthet för brott 2025

Fler än fyra av tio företag har utsatts för brott

Resultaten från Företagarpanelen 2025 visar att fler än fyra av tio företag (44 procent) utsatts för brott. En jämförelse med 2024 visar att andelen brottsutsatta företag inte förändrats mellan åren.[4]

Figur 1. Har utsatts för brott de senaste 12 månaderna.



Källa: Svenskt Näringslivs Företagarpanel, april–maj 2025.

Handeln, besöksnäringen och byggbranschen mest utsatta för brott

Att cirka fyra av tio företag utsattes för brott de senaste 12 månaderna gäller alltså i genomsnitt. Utsattheten för brott är högst inom handeln, där nästan 6 av 10 företag svarat att de utsatts för brott, samt besöksnäring och bygg, där nära hälften av företagen svarat att de utsatts för brott.

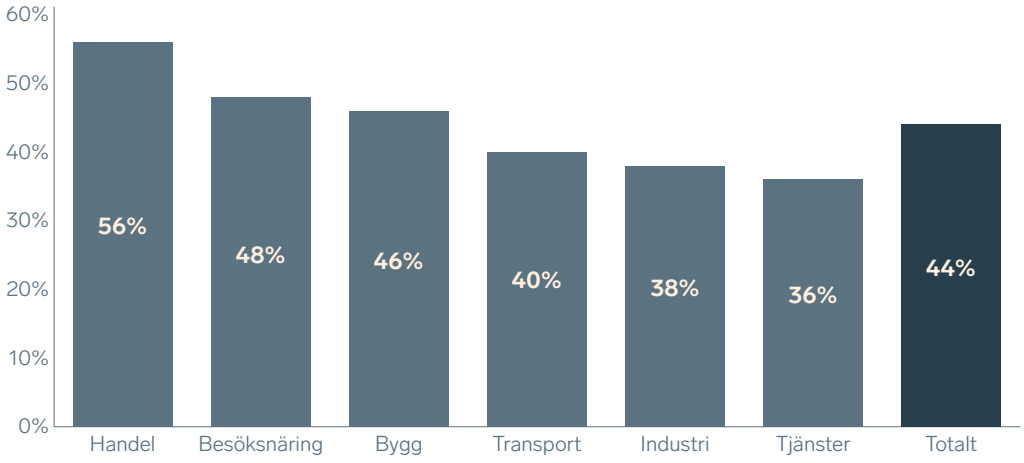
Andelarna företag inom branscherna transport, industri och tjänster som svarar att de utsatts för brott ligger något under genomsnittet, men även där är det fler än vart tredje företag som blivit utsatt för brott.

Jämfört med motsvarande undersökning 2024[5] är det samma branscher som är de mest brottsutsatta: handeln och besöksnäringen, följt av byggsektorn.

4 I *Brottsbarometern* 2024 (Svenskt Näringsliv, 2024) användes en annan metod för att vikta svaren från företagen. Om företagens svar för 2024 viktas för att vara jämförbara med företagens svar för 2025 blir resultatet att andelen brottsutsatta företag inte förändrats.

5 Svenskt Näringsliv (2024)

Figur 2. Utsatthet för brott bland företag i olika branscher de senaste 12 månaderna.



Källa: Svenskt Näringslivs Företagarpanel, april-maj 2025.

Bedrägerier, snatterier, stölder, inbrott och cyberbrott vanligaste brotten mot företag

Det vanligaste brottet som företag utsatts för är bedrägerier. Vart femte brottsutsatt företag i denna undersökning har utsatts för brott som falska fakturor, identitetskapning, försök att lura till sig betalning eller liknande. Bedrägerier har det gemensamt med cyberbrott att det ofta handlar om IT-relaterade brott. Definitionsmässigt hör dock bedrägeribrott till mängdbrott.

Mängdbrott

Brott som är vanligt förekommande kallas för mängdbrott och de brott som räknas till dessa är enligt polisen bland annat:

- Stöld till exempel av och ur bilar, cykelstöld och butiksstöld,
- Inbrott i bostad,
- Skadegörelse som till exempel klotter,
- Bedrägeri,
- Misshandel,
- Grov olovlig körning och rattfylleribrott.

Av det totala antalet anmälda brott utgör ungefär tre fjärdedelar mängdbrott.

Källa: https://polisen.se/om-polisen/polisens-arbete/mangdbrott/

Den myndighetsgemensamma lägesbilden 2025[a] visar en allt tydligare koppling mellan organiserad brottslighet och mängdbrott, främst stölder och bedrägerier. ”Det är inte längre vettigt och göra någon uppdelning mellan å ena sidan organiserad brottslighet, som man gärna tänker är grov, och skjutvapenvåld och liknande, och å andra sidan vardagsbrottsligheten.” säger Johan Olsson, chef för polisens Nationella operativa avdelning, NOA till SR Ekot, 2025-08-22.[b]

[a] Myndighetsgemensam lägesbild (2025)
[b] https://www.sverigesradio.se/artikel/polisen-organiserade-natverk-bakom-vardagsbrott

”De ska få jobba för det de stjäl”

Daniel Schönström driver S-Schakt AB, ett familjeföretag inom anläggningsbranschen som ligger i Hörby. Dieselstölder och stölder av verktyg hör till de brott som hans företag utsätts för. Det är en ständigt aktuell fråga att skydda maskiner och utrustning på arbetsplatserna.

Daniel Schönström konstaterar att läget faktiskt blivit något bättre det senaste året även om dieselstölderna fortsätter och är vanligt förekommande. Kanske kan minskningen bero på deras eget säkerhetsarbete:

– Vi har tagit tag i det på ett annat sätt nu. Låser in mer saker i containrar i stället för att bara kedja fast dem, har GPS-sändare och spårsändare på alla maskiner. Vi ställer till och med betongblock framför containrarna för att göra det svårare att stjäla ur dem. Problemet är att de som vill stjäla alltid hittar nya lösningar. Men vi gör det så svårt som möjligt för dem, säger Daniel.

> ”Det känns ofta som beställningsjobb. De som stjäl stör ut GPS-sändare, vet exakt vad de ska ta.”

Utmaningen är att anläggningsbranschens arbetsplatser ofta ligger på ensliga och folktomma platser som är extra utsatta nattetid.

Ofta måndagsoro: Vad har de tagit i helgen?

Konsekvenserna av stölderna går långt utöver det som faktiskt stjäls. Daniel beskriver en vanlig oroskänsla så här:

– Många måndagar kommer jag till jobbet och undrar vad som stulits den här helgen och vad det får för ekonomiska konsekvenser. Det handlar om självrisker på försäkringen, att vi kan behöva hyra eller köpa in nya verktyg, tanka upp våra maskiner och att arbetet blir stillastående om saker är borta.

Det blir kostsamt och det administrativa arbetet tar också tid och energi.

– Man måste skriva polisanmälningar, utreda vad vi har blivit av med, leta upp inköpskvitton, dokumentera för försäkringsbolaget med mera. Det är oro, ekonomi och tidskrävande hantering. Men det är tyvärr sådant man får ta, menar Daniel.

Trots att de flesta polisanmälningar läggs ner är Daniel noga med att polisanmäla allt.

– Om man inte anmäler så ser inte polisen att det är ett problem. Även om anmälningarna läggs ner så finns de i systemet och kan göra att polisen kanske kör en extra runda. Det är viktigt med statistiken. Det som inte anmäls, syns inte. Det försöker jag få ut till alla i branschen, säger Daniel.

De är smartare och fräckare nu

Daniel märker att brottsligheten har förändrats över åren. Även om de ”gamla dieseltjuvarna” – unga med EPA-traktorer och de som behöver pengar till mat och annat – fortfarande finns kvar, känns det ofta mer professionellt.

– Det känns ofta som beställningsjobb. De som stjäl stör ut GPS-sändare, vet exakt vad de ska ta. Med närhet till hamnar och broar är man snabbt ute ur landet.

Han berättar att de som stjäl verkar spana och ha koll på när nya maskiner kommer till arbetsplatserna. Inom skogsbranschen har han till och med hört om hot som också verkställts.

– ”Har du inte full tank nästa gång slår vi sönder din maskin”. Jag har inte själv blivit utsatt för det, men jag har hört om det från andra.

> ”De som stjäl är smartare och fräckare”.

GPS i maskinerna och kameror som avskräcker

För att skydda företaget har Daniel investerat i flera säkerhetslösningar. GPS-sändare sitter på nästan alla maskiner.

– Om maskiner förflyttar sig exempelvis nattetid får jag ett larm. Då kan jag se om de rör sig och ringa polisen. Dock verkar det som att de som stjäl kan ta bort sändare ganska lätt också.

Företaget har också satsat på kameraövervakning runt sina arbetsplatser. Det är främst i förebyggande och avskräckande syfte säger Daniel.

– Det handlar om att förhindra brott.

Hela tiden en avvägning mellan kostnad och risk

Men säkerhet kostar och Daniel beskriver att det ständigt behövs en avvägning:

– Det kostar många tusenlappar per kamera vi sätter upp och man får hela tiden väga kostnad mot risk. Är det värt att lägga de här extra pengarna? Det handlar förstås om att slippa att produktionen står stilla och nya inköp. Det är för vår egen skull. Har jag inga inbrott behövs inga polisanmälningar heller.

På frågan om vad politikerna borde göra lyfter Daniel tre saker. Enklare lagstiftning för kameraövervakning, skärpta straff och mer resurser till polis och tull.

– Det är inte kännbara straff för stölder och det är besvärliga regler för kameraövervakning. Både polisen och tullen behöver också resurser som gör att de kan prioritera stöldbrott högre.

Daniel hoppas också på det nya frivilliga maskinregistret. Han hade dock hellre sett ett tvingande register som en myndighet ansvarar för, liknande det Transportstyrelsen redan har för bilar, släp och trafikregistrerade maskiner.

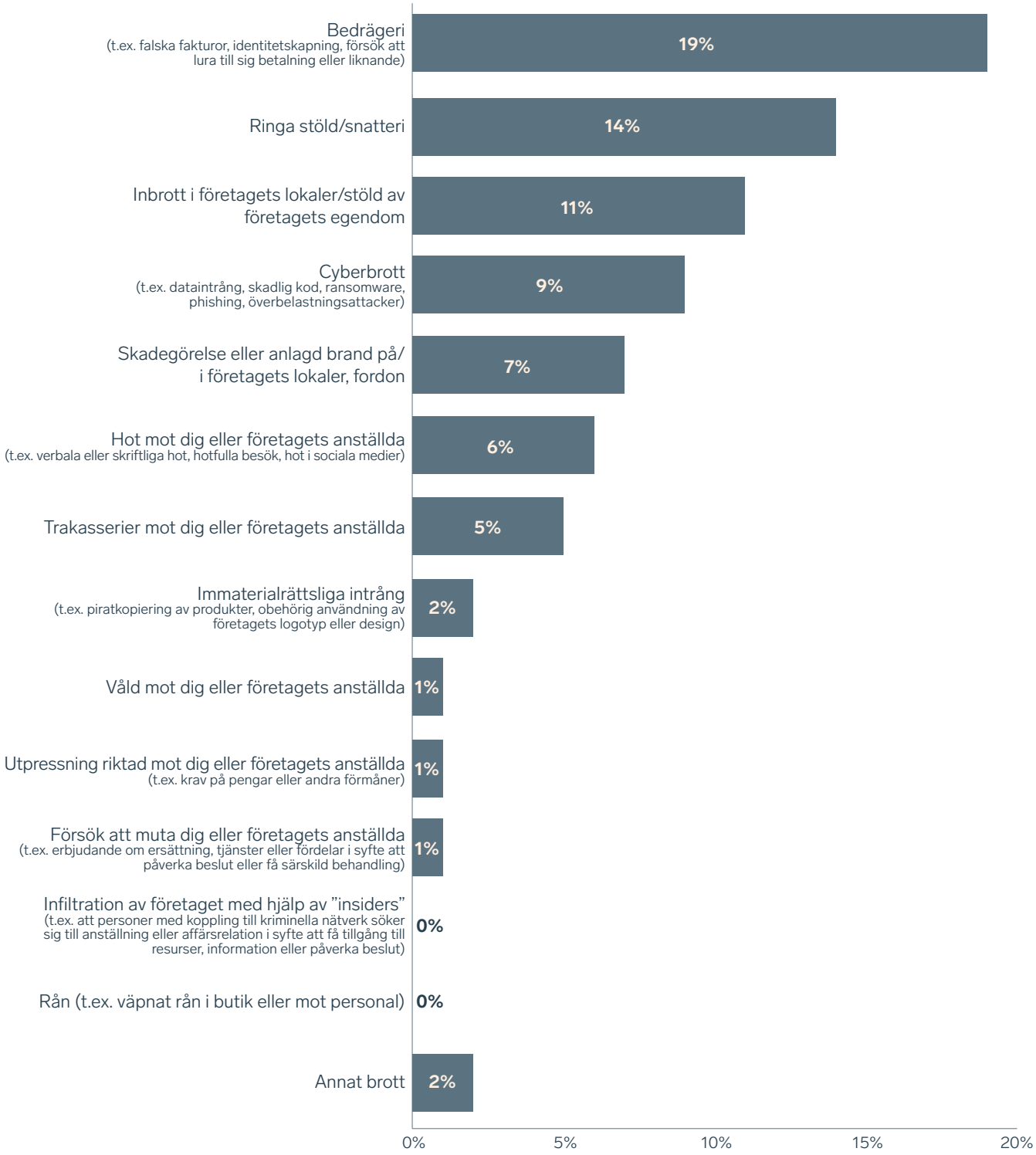
– Nu är det ett privat initiativ och frivilligt, men det är bättre än inget. På sikt kanske det kan leda till ett tvingande register.

Definitioner av vissa brott

I Svenskt Näringslivs enkätundersökningar har dessa brott definierats på följande sätt:

- Ringa stöld (snatteri) är när något stulits för ett värde understigande 1 250 kronor.
- Stöld (utan eller genom inbrott) är när något stulits eller skadats för ett värde på minst 1 250 kronor.
- Skadegörelse är klotter och anlagd brand, att fastigheter och/eller fordon skadats eller förstörts.
- Bedrägeri är att man uppsåtligen blivit vilseledd av någon och att det lett till skada för företaget. Exempel: bluffakturor eller phishing, det vill säga att någon på ett företag fått mejl eller sms och uppmanas klicka på en falsk länk eller ange/verifiera lösenord, ge koder eller bank- och kortuppgifter, eller att bedragare uppgett sig till exempel för att vara VD för ett företag och fått någon på ett företag att göra en pengaöverföring,
- Cyberbrott är IT-brottslighet som riktar sig mot datateknik eller brott som begås med hjälp av datateknik och datanät för att komma åt information och/ eller manipulera system.

Figur 3. Brott som företagen utsatts för de senaste 12 månaderna.



Not: Andelen som svarade ”Vet ej” uppgick till 3 procent.
Källa: Svenskt Näringslivs Företagarpanel, april-maj 2025.

Ringa stölder/snatterier är det näst vanligaste brottet som företagen utsatts för. 14 procent av företagen svarar att de utsatts för sådana brott. Andel företag som utsatts för inbrott samt stölder uppgår till 11 procent och för cyberbrott till 9 procent. Immaterialrättsliga intrång, t.ex. piratkopiering av produkter, obehörig användning av företagets logotyp eller design, uppgår till 2 procent.

Typer av brott som drabbar både företagare och anställda är de som har med hot, trakasserier, våld, utpressning eller mutförsök att göra. 6 procent av företagen rapporterar hot och 5 procent av företagen rapporterar trakasserier. 1 procent av företagen rapporterar våld och en lika stor andel rapporterar att de eller deras anställda blivit utpressade. Andelen företag som rapporterar mutförsök uppgår också till 1 procent.

Knappt en halv procent av företagen rapporterar att de utsatts för infiltration. Det är en låg siffra men inte förvånande. Infiltration är ju ett brott som är avsett att inte upptäckas. För att vara framgångsrika måste de som infiltrerar lyckas med att ”gå under radarn”, att inte synas. Det ovanligaste brottet i denna undersökning är rån – som ju är ett brott som syns – och som har drabbat knappt en kvarts procent av företagen.

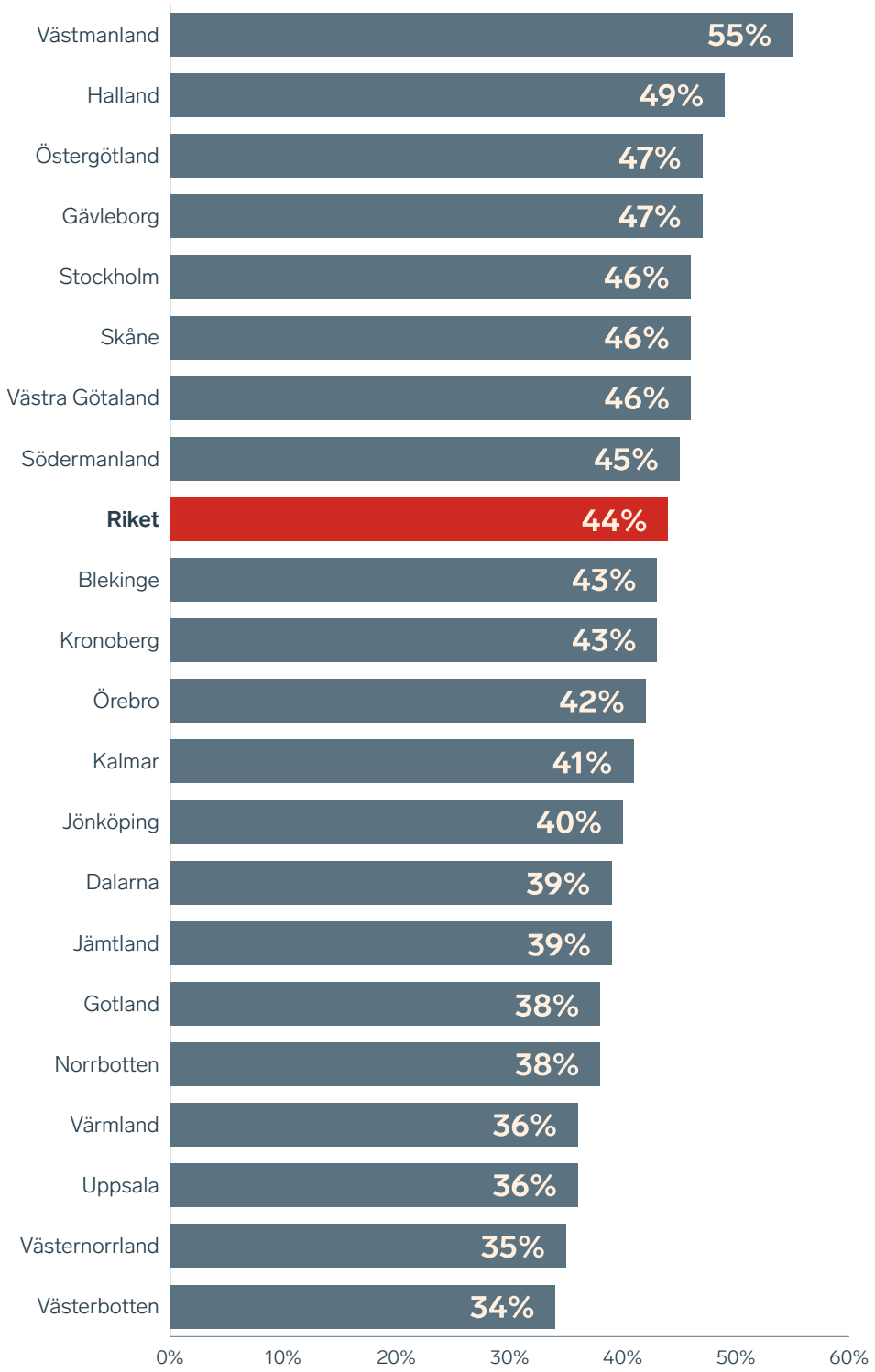
Handeln är den bransch som i störst utsträckning utsätts för ringa stölder och snatterier, vilket hänger samman med verksamhetens karaktär, medan inbrott och stölder är vanligast i byggbranschen. I alla branscher är bedrägerier bland de tre vanligaste brotten och det är det allra vanligaste brottet i industri-, transport- och tjänstebranscherna.

Högst andel brottsutsatta företag i Västmanland

Företagens utsatthet för brott varierar geografiskt, med tydliga skillnader mellan polisregioner, län och kommuner. När det gäller mängdbrott kan variationerna vara stora även inom enskilda kommuner. Skillnaderna rör inte bara omfattningen av brottsligheten utan också dess karaktär (Svenskt Näringsliv, 2023b).

I Västmanland är andelen företag som anger att de utsatts för brott högst i landet, 55 procent, alltså mer än vartannat företag. Näst mest utsatt är företag i Halland, där häften av företagen svarar att de utsatts för brott. Östergötland, Gävleborg, Stockholm, Skåne, Västra Götaland och Södermanland ligger ovanför genomsnittet.

Figur 4. Hur företag i olika delar av landet har utsatts för brott de senaste 12 månaderna.



Källa: Svenskt Näringslivs Företagarpanel, april-maj 2025.

Företag i landets mellersta och södra delar är i högre grad drabbade av brott. Detta hänger samman med att kriminaliteten i större utsträckning är koncentrerad till större städer samt med den geografiska närheten till kontinenten, vilket medför en ökad exponering för gränsöverskridande brottslighet, exempelvis organiserade stöldligor (Svenskt Näringsliv, 2023b).

Omkring hälften av de brottsutsatta företagen polisanmäler inte

Enligt Brottsförebyggande rådet, Brå, minskade antalet polisanmälda brott mot företag och organisationer från cirka 526 000 år 2018 till cirka 400 000 år 2023. Som andel av det totala antalet polisanmälda brott sjönk dessa brott från 33 procent år 2018 till 26 procent år 2023.[6] Det ska inte tolkas som att företagen blivit mindre brottsutsatta under denna tid. Flera tidigare undersökningar visar att det är vanligt att brottsutsatta företag inte polisanmäler detta.[7]

I flera studier ligger andelen företag som inte polisanmäler brott kring 40–50 procent, och så även i denna undersökning. Knappt hälften av de brottsutsatta företagen svarade att de inte polisanmält något av brotten. En knapp tredjedel av företagen anmälde samtliga brott och en dryg femtedel av företagen anmälde vissa av de brott de utsatts för enligt denna undersökning.

6 Brå (2025a). Det totala antalet polisanmälda brott uppgick till knappt 1,6 miljoner år 2018 respektive drygt 1,5 miljoner år 2023.

7 Enkätstudier visar att andelen brottsutsatta företagare som inte polisanmält samtliga brott varierar mellan drygt 30 till så högt som cirka 70 procent (Företagarna 2022, 2023, 2024; Svenskt Näringsliv 2022, 2023b, 2024; Tryggare Sverige 2024).

Varför har du inte polisanmält brott?

”Det är meningslöst att anmäla och tar bara tid via 114 14. **Anmälan läggs ner direkt**.”

”Det tar bara dyrbar arbetstid från mig och mina anställda **utan några konsekvenser för brottslingen**. Alla förundersökningar läggs ner av åklagare.”

”Förr anmälde vi mer och det är mot den bakgrunden vi upplever att **alla ärenden i vår bransch läggs ned**.”

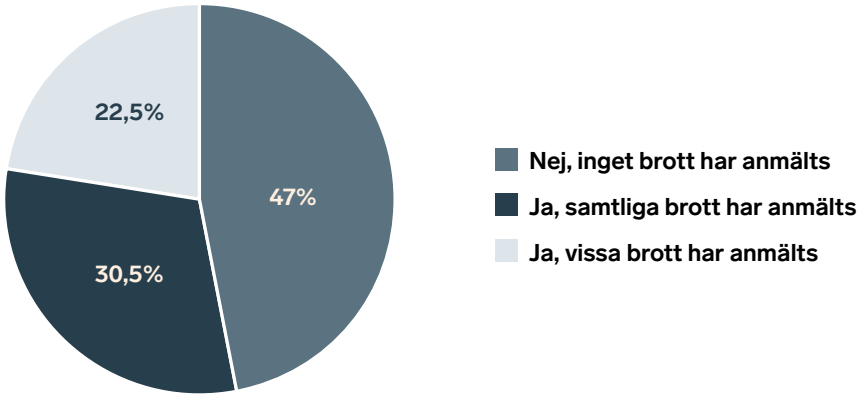
”Händer inget från polisen ändå.”

”Polisen lägger ned alla mindre ärenden samma timme som de anmäls.”

”Varför lägga tid på dokumentation, skicka bilder, etc. när polisen återkommer efter fem minuter med hänvisning till att ”anmälan lagts ned i brist på bevis”? **De har verkligen en lång väg för att återfå förtroendet ute hos oss företagare på landet.** ... Finns inget så förnedrande som polis som trots tydliga bevis och underlag lägger ned en utredning!”

”Det är viktigt för statistiken, men känns meningslöst.”

Figur 5. Har brott som inträffat de senaste 12 månaderna polisanmälts?



Not: Andelen som svarade ”Vet ej” uppgick till 2 procent.
Källa: Svenskt Näringslivs Företagarpanel, april-maj 2025.

Det känns fullständigt meningslöst att anmäla brott då inget görs utan man får bara ett besked om att undersökningen är nedlagd.”

För att inte förvärra situationen, då vi är placerade i ett utsatt område.”

Leder inte vidare tyvärr. Vi säkrar upp oss lokalt med systematiskt säkerhetsarbete för att motverka. Dock dyrt i längden.”

Risk för våld mot familjen.”

Känslan är att det inte är nån idé. Har anmält vissa brott, skadegörelse bland annat där vi haft viss info om vem som ligger bakom. Trots det, och **trots att DNA hittats, är känslan att det står still. Ingenting händer.** Så när saker försvinner, stjäls ur verkstad m.m. har vi inte orkat anmäla, för det läggs ändå bara ner.”

Har tidigare anmält två inbrott (varav ett fanns på film) och **hot mot ägare och anställda utan att polisen har gjort något**.”

Alla anmälningar läggs ner, så **vi kan inte lägga den tiden på anmälninga**r om det ändå bara leder till att den läggs ner.”

”Man kan inte förvänta sig att få hjälp”

Gerhard Bley är VD för Norrmejerier, det kooperativ som försörjer stora delar av Norrland med mejerivaror. I april 2024 drabbades de av ett cyberangrepp som hotade hela verksamheten. Produktionen stod still och myndigheternas agerande var passivt och i princip obefintligt.

”Notan för cyberangreppet landade på omkring **10 miljoner kronor**.”

Det började med att produktionsutrustningen på en av linjerna slutade fungera. Det är inget onormalt i sig, menar Gerhard Bley, men IT-teknikerna upptäckte snabbt att det var något annat. Det visade sig vara ett cyberangrepp.

– Vi tvingades stänga ner produktionen direkt. Det blev väldigt dramatiskt. Vi är ett kooperativ och den mjölk som produceras på gårdarna måste tas om hand direkt. Hela mejeriet stod still och det fick dramatiska konsekvenser.

300 000 liter mjölk varje dygn måste hanteras

Situationen var kritisk. Norrmejerier hanterar 300 000 liter mjölk varje dygn och cyberattacken som ledde till nedstängning gjorde att ingen mjölk från bönderna kunde tas emot.

– För bönderna som äger oss blev det stora ekonomiska konsekvenser. Notan för cyberangreppet landade på omkring 10 miljoner kronor och i början vi visste ju inte heller hur länge produktionen skulle stå stilla.

Externa experter kontaktades omedelbart och beskedet var nedslående.

– Vi fick veta att produktionen efter en sådan här attack kan stå stilla i ett antal veckor. Det hade inneburit att vi inte skulle ha överlevt.

64 timmar som räddade företaget

Men genom intensiva insatser och vad Gerhard kallar ”lite tur” lyckades de få igång produktionen inom 64 timmar.

– Inte fullt ut dock. Det tog en vecka innan vi var igång helt. Under tiden fick vi köra mjölk till andra mejerier i Sverige. Det var ett och ett halvt dygn som var mycket dramatiskt.

Norrmejeriers krisledningsgrupp arbetade dygnet runt tillsammans med ett externt cybersäkerhetsföretag. Mycket tyder på att angreppet kom österifrån som en del av ett systematiskt arbete.

– Vi fick kravbrev om att betala lösensumma men det gjorde vi inte.

Trots den akuta krisen lyckades företaget undvika långsiktiga skador.

– Vi lyckades ta oss ur det. Men det har lett till en massa ändringar internt, inte minst IT-säkerhetsmässigt.

Ett stort underbetyg åt myndigheterna

Gerhard är mycket kritisk till myndigheternas agerande.

– Myndigheterna agerade väldigt tafatt. Vi gjorde en polisanmälan men det var som att polisanmäla en cykel. Vi blev kontaktade av regeringskansliet, men det ledde inte till något.

Frustrationen är påtaglig över den uteblivna hjälpen.

– Det var beklämmande dåligt. Ett stort underbetyg åt myndigheterna. Kortsiktigt kanske de inte hade kunnat göra så mycket men det kostade oss och våra mjölkbönder många miljoner. Det var en valhänthet och en passivitet som är förvånande eftersom vi pratar så mycket om livsmedelsförsörjningen som en del av beredskapen.

Särskilt allvarligt är det eftersom Norrmejerier försörjer Norrbotten, Västerbotten, delar av Västernorrland och Jämtland med mejerivaror.

– Det var ett angrepp på vår livsmedelsförsörjning och det här borde vara högre prioriterat från myndigheternas sida.

Krisberedskap är A och O

Trots att företaget hade god IT-säkerhet från början har de förstärkt arbetet ytterligare.

– Ett av skälen till att vi klarade oss så bra var att vi hade god IT-säkerhet i grunden, men vi har täppt till fler luckor efteråt. Så länge vi har behov av internet finns det alltid risker.

Gerhards råd till andra företag är att ha en tydlig krisberedskap. När det händer något som en cyberattack, händer det så mycket på en gång. Ta extern hjälp av experter. På frågan om politiska åtgärder är han skeptisk men tydlig:

> **”Om det skulle hända något idag så känner jag inte att vi har några myndigheter som skulle vara till hjälp.”**

– Det finns inga begränsningar för hur många u-båtar vi kan köpa men att vi ska ha mat på bordet, där är det mer njuggt. I vårt fall är det mjölkbönderna som får ta smällen. Det borde kunna finnas ekonomisk stöttning.

Avslutningsvis konstaterar Gerhard:

– Om det skulle hända något idag så känner jag inte att vi har några myndigheter som skulle vara till hjälp.

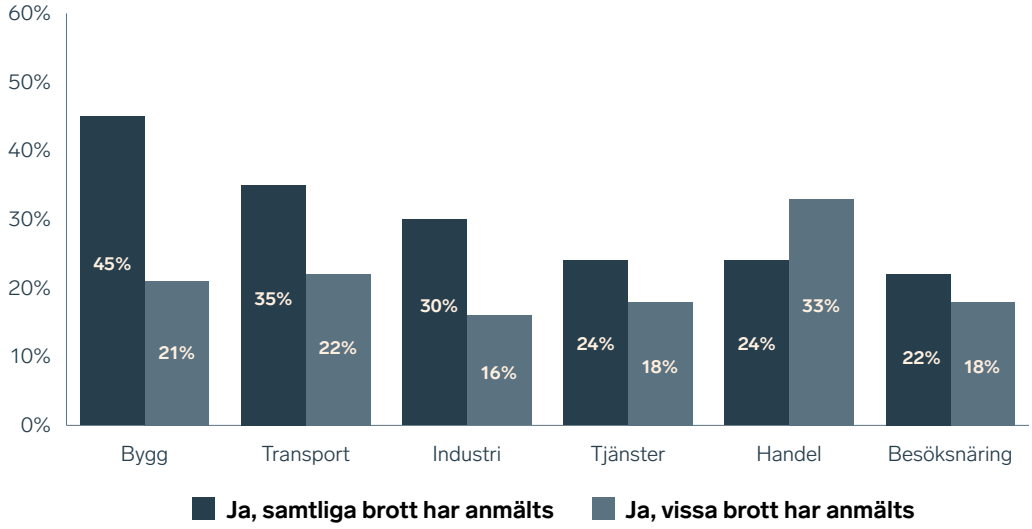
Vanliga svar i många studier där brottsutsatta företagare tillfrågas om varför de inte polisanmäler är att ”det är inte någon idé” eller ”det tar bara tid utan att ge något resultat”.[8] Även i denna undersökning framträder samma mönster: det stora antalet frisvar som anger att en polisanmälan upplevs som meningslös visar tydligt varför många företag väljer att avstå från att anmäla.

I en tidigare undersökning uppger endast drygt vart tionde företag att de är nöjda med polisens arbete med att utreda och klara upp de brott som drabbat dem under det senaste året. Hälften av företagen är missnöjda, medan en tredjedel varken är nöjda eller missnöjda.[9]

Benägenheten att polisanmäla brott varierar mellan branscher, vilket till stor del sannolikt beror på att olika typer av brott drabbar branscher olika mycket. Byggbranschen ligger högst i anmälningsbenägenhet. 45 procent av företagen svarar att de anmält samtliga brott och vart femte företag svarar att de anmält vissa brott. Troligen kan det kopplas till att inbrott och stölder är de vanligaste brotten i denna bransch.

8 Enligt Företagarna (2022, 2023 och 2024), är det viktigaste skälet, som företagen uppger till att inte anmäla, att de inte ser någon poäng med det, att ingenting kommer att hända.
9 Svenskt Näringsliv (2023b).

Figur 6. Har företag i olika branscher polisanmält brott som inträffat de senaste 12 månaderna?



Not: Andelen företag som svarade ”Vet ej” varierade mellan 1-2 procent per bransch.
Källa: Svenskt Näringslivs Företagarpanel, april-maj 2025.

Transportsektorn ligger näst högst i anmälningsbenägenhet, där 35 procent av företagen har polisanmält samtliga brott. Även där är inbrott och stölder de vanligast förekommande brotten men inte lika vanliga som i byggbranschen. Bedrägerier är nästan lika vanliga som inbrott och stölder i transportsektorn. På tredje och fjärde plats i anmälningsbenägenhet kommer industrisektorn respektive tjänstesektorn, två sektorer där bedrägeri och cyberbrott är de två vanligaste brotten.

Lägst anmälningsbenägenhet finns i handeln och besöksnäringen. Endast drygt vart femte företag i dessa branscher har anmält samtliga brott. En trolig delförklaring till den låga anmälningsbenägenheten är att ringa stölder och snatterier är de vanligaste brotten i dessa sektorer. Till skillnad från de övriga branscherna är andelen som anmält vissa brott högre i handeln, 33 procent, än andelen som anmält alla brott. Därmed kanske företagen inte ser vissa av de brott de utsatts för som tillräckligt allvarliga för att polisanmäla.

En betydligt mer allvarlig delförklaring kan vara att andelen företag som utsatts för hot och trakasserier är högst i handeln och besöksnäringen. Sammanlagt rapporterar nästan vart femte företag inom dessa branscher att hot och trakasserier drabbat dem själva eller företagets anställda. Rädsla för att möta gärningspersonerna i en (eventuell) rättegång kan dra ned viljan att polisanmäla.

Slutsatsen är att många brottsutsatta företag bedömer att det är i stort sett meningslöst att polisanmäla brotten, oavsett om det handlar om mängdbrott eller cyberbrott, och att dessa bedömningar varit vanliga under flera år.

Cyberbrott anmäls ytterst sällan men kan orsaka stora skador

Företagens benägenhet att polisanmäla brott är särskilt låg när det gäller cyberbrott, en brottstyp som är nära kopplad till organiserad brottslighet.[10] Flera av de personer som intervjuas i Brå:s undersökning *Polisanmälda dataintrång*[11] menar att många offer troligtvis aldrig upptäcker att de utsatts för dataintrång.

10 Stockholms Handelskammare (2022), Truesec (2025)
11 Brå (2022)

Emellertid polisanmäls i många fall inte upptäckta attacker som misstänks vara fientliga. Alla leverantörer av samhällsviktiga tjänster samt statliga myndigheter ska rapportera IT-incidenter som deras informationssystem utsätts för eller i tjänster som de tillhandahåller åt en annan organisation. Endast 27 procent av de IT-incidentrapporter med misstänkta antagonistiska angrepp som inkom till MSB under 2021 hade eller planerades att polisanmälas enligt uppgiftslämnarna.[12]

Enligt Stockholms Handelskammare anmäler endast 3–5 procent av de drabbade företagen sådana incidenter till polisen.[13] Skälen varierar: förutom att många upplever polisanmälan som meningslös, vill företag ofta undvika negativ publicitet som kan skada förtroendet om en anmälan uppmärksammas i media.

En intervjuperson som citeras i Stockholms Handelskammare (2022) säger att ”Företagets image kan skadas. Investerare och kunder kanske tror att företaget inte bryr sig tillräckligt om säkerheten. Det kan vara legala problem – du kan drabbas av böter om till exempel lagrade personuppgifter börjar spridas. Angriparna vet det här och utpressar företag med att de kommer offentliggöra känsliga personuppgifter på nätet om företaget inte kan betala lösensumman.”[14]

Enligt Svenskt Näringsliv (2023b) var cyberbrott den näst mest kostsamma brottstypen för svenska företag, med en uppskattad kostnad på cirka 9 miljarder kronor.

Threat Intelligence Report 2025. An In-Depth Analysis of the Cyber Threat Landscape

- Rapporten “Threat Intelligence Report 2025. An In-Depth Analysis of the Cyber Threat Landscape”[15] drar slutsatsen att cyberhoten fortsätter att utvecklas och ransomware (utpressningsvirus) fortfarande är det dominerande angreppssättet, ofta genom utnyttjade tekniska sårbarheter eller kapade inloggningar.
- Samtidigt ökar både datastölder och cyberspionage, där såväl statsaktörer som privata grupperingar av kriminella, som ofta hyr ut sina brottsliga tjänster, är aktiva. Geopolitiska konflikter, särskilt Rysslands krig mot Ukraina, driver på fler fall av cybersabotage. AI har blivit ett kraftfullt vapen för angripare – med phishing, deepfakes och snabbare utnyttjande av sårbarheter – men används också allt mer i försvar.
- Leverantörskedjor är en kritisk sårbarhet, vilket bland annat Tietoevry-attacken 2024 visade. Stora bolag ser nu fler ”tysta hot” i form av datastölder och spionage snarare än rena krypteringsattacker.
- När de större företagen stärker sitt skydd söker angriparna i stället enklare mål. Det gör små och medelstora företag är särskilt utsatta. Många tror felaktigt att de är för små för att vara intressanta, men begränsade resurser, föråldrade system och bristande IT-kompetens gör dem sårbara. Konsekvenserna kan bli höga kostnader, driftstopp och förlorat förtroende hos kunder.
- I den närmaste framtiden väntas Ryssland fortsätta använda cyberbrott som påtryckning mot väst, medan Kina intensifierar industrispionage och desinformation. AI-baserade attacker blir fler och mer avancerade. Samarbete mellan näringsliv och myndigheter är avgörande för samhällets motståndskraft.

12 MSB (2022)
13 Stockholms Handelskammare (2022)
14 Stockholms Handelskammare (2022), sid. 24.
15 Truesec (2025)

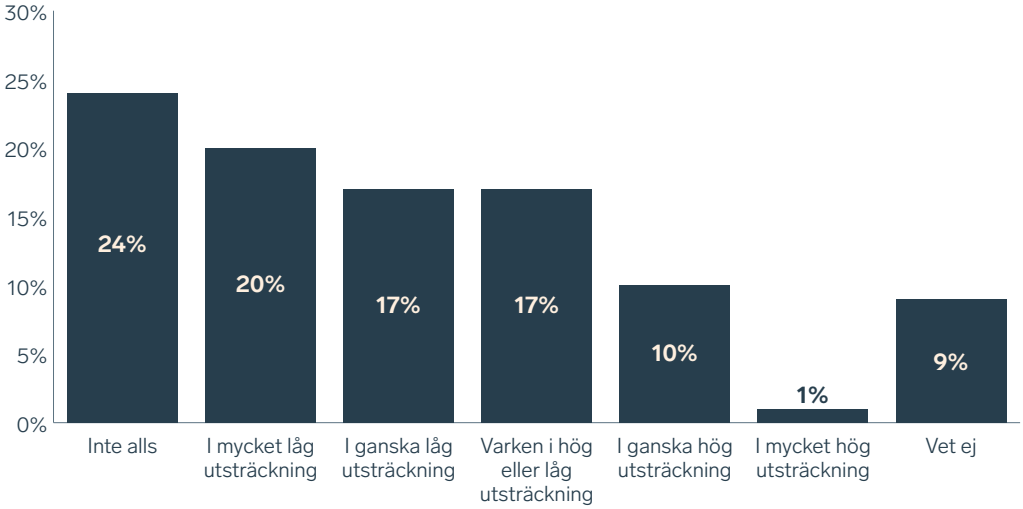
Otillåten påverkan riktad mot företag

För att få bättre bild av hur företag påverkas av hot, påtryckningar eller annan otillåten påverkan i sin verksamhet innehöll Svenskt Näringslivs Företagarpanel för april-maj 2025 frågor om otillåten påverkan, exempelvis om det funnits försök till otillåten påverkan i samband med upphandlingar eller affärsrelationer för att få beslutsfattare i företaget att ta beslut som annars inte skulle ha tagits eller infiltration, alltså att personer med otillbörliga avsikter tar sig in i eller rekryteras inne i ett företag och påverkar verksamheten inifrån på ett skadligt sätt.

I genomsnitt bedömer fler än vart tionde företag att deras verksamheter i mycket eller ganska hög utsträckning kan bli utsatt för otillåten påverkan.

Nästan vart fjärde företag bedömer att de inte alls kan bli utsatta för otillåten påverkan, vart femte att de i mycket låg utsträckning kan bli det, och knappt vart femte att de i ganska låg utsträckning kan bli det. Läggs dessa andelar ihop framkommer fler än 6 av 10 företag bedömer att den utsträckning som de kan bli utsatta för otillåten påverkan är icke-existerande, mycket låg , eller ganska låg. Knappt vart tionde företag svarar att de inte vet om deras verksamheter kan bli utsatta för otillåten påverkan.

Figur 7. I vilken utsträckning anser du att din verksamhet kan bli utsatt för otillåten påverkan?



Källa: Svenskt Näringslivs Företagarpanel, april-maj 2025.

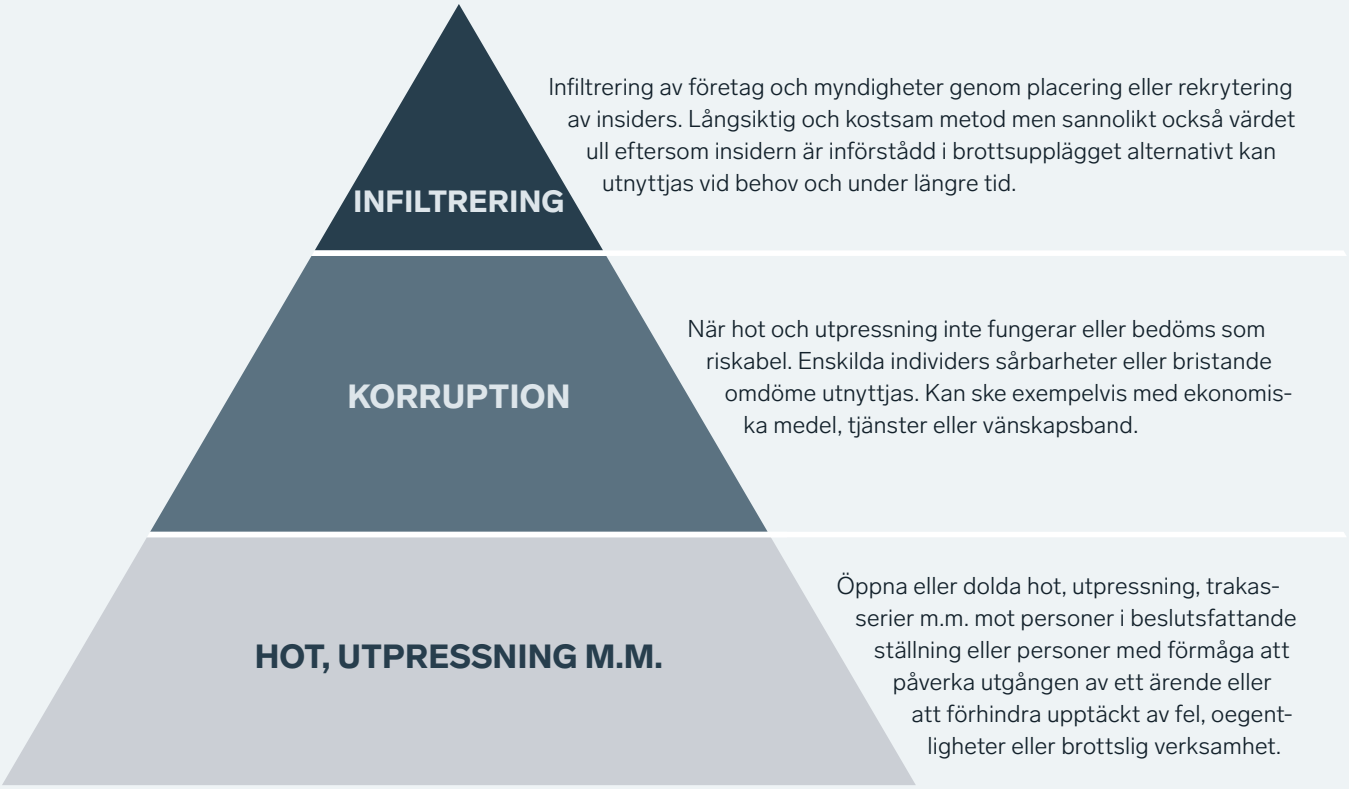
När dessa svar fördelas per bransch framkommer att högst andelar företag som bedömer att de i mycket eller ganska hög utsträckning kan bli utsatta för otillåten påverkan finns i byggbranschen och besöksnäringen (14 procent), följt av handeln (13 procent). Sedan kommer företag i tjänstebranschen (11 procent), industrin (10 procent) och sist transportbranschen (8 procent).

Vad är otillåten påverkan?

Otillåten påverkan är inte en juridisk brottsrubricering utan används här som ett samlingsnamn för illegala handlingar som syftar till att påverka hur någon agerar i sin yrkesroll eller sitt uppdrag.

Olika former av otillåten påverkan kan illustreras som en pyramid bestående av tre olika steg som speglar kriminella aktörers avsikt, förmåga och handlingsutrymme, se Figur 6. Ju högre upp i pyramiden, desto mer resurskrävande och långsiktig strategi krävs från aktörernas sida.

Figur 8. Otillåten påverkan.

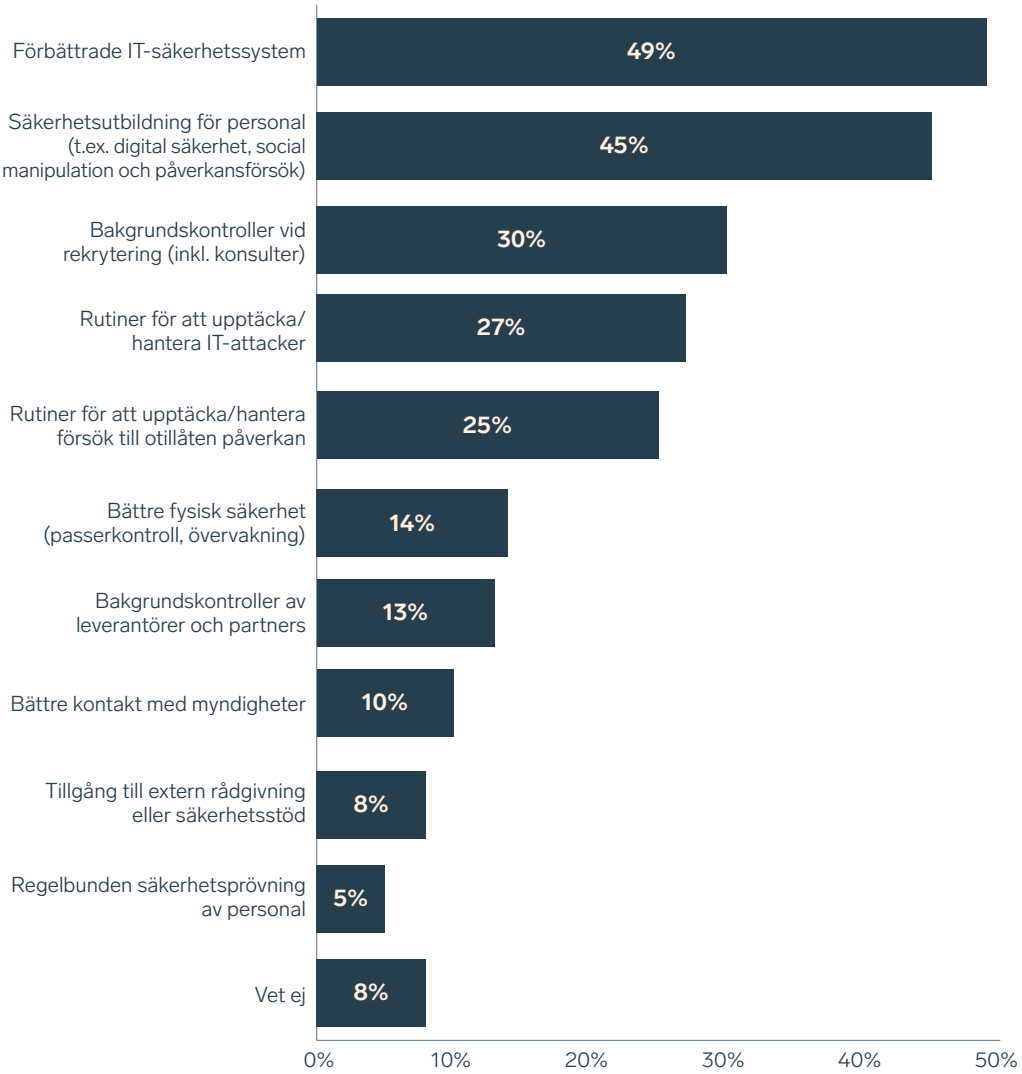


Källa: Myndighetsgemensam lägesbild (2023), s. 13.

På senare år har värvningar för ”engångsjobb” blivit vanligare. Exempelvis har de ryska underrättelsetjänsterna börjat använda sig av ”engångsspioner” eller ”förbrukningsagenter”. Till skillnad från klassiska spionvärvningar, som kan pågå under flera år, och därmed ligger högst i pyramiden, går dessa värvningar snabbt. Agenterna rekryteras via krypterade mobilapplikationer som Telegram och Signal, de ”får pengar, utför ett brott som ett sabotage eller en informationsstöld, för att sedan överges för gott.”[c]

[c] Sallinen & Ståhle (2025), sid. 370-371.

Figur 9. Vilka åtgärder tror du är viktiga för att hjälpa din verksamhet att undvika otillåten påverkan?



Not: Respondenterna är företag som på frågan ”I vilken utsträckning anser du att din verksamhet kan bli utsatt för otillåten påverkan?” svarat ”I mycket hög utsträckning” eller ”I ganska hög utsträckning”. De fick uppge upp till tre svarsalternativ. Andelen företag som svarade ”Annat” uppgick till 7 procent.
Källa: Svenskt Näringslivs Företagarpanel, april-maj 2025.

När dessa företag fick välja upp till tre av åtgärderna i Figur 9, som de bedömde vara viktiga för att hjälpa verksamheterna att undvika otillåten påverkan, kommer förbättrade IT-säkerhetssystem på första plats. Säkerhetsutbildning för personal, exempelvis i digital säkerhet, social manipulation och påverkansförsök, kommer på andra plats och på tredje plats kommer bakgrundskontroller vid rekrytering inklusive av konsulter. Nästan lika viktiga bedömdes rutiner för att upptäcka/hantera IT-attacker, samt rutiner för att upptäcka/hantera försök till otillåten påverkan, vara.

Sedan följer, i fallande ordning, bakgrundskontroller av leverantörer och partners, bättre kontakt med myndigheter, tillgång till extern rådgivning eller säkerhetsstöd, och sist en regelbunden säkerhetsprövning av personal. Andelen företag om svarade ”Vet ej” uppgick till 8 procent.

Regelbunden säkerhetsprövning av personal är resurskrävande och kostnaden upplevs sannolikt som alltför hög för de flesta små och medelstora företag. Många bedömer dessutom att deras verksamhet inte tillhör de mest utsatta branscherna. Det finns inte mycket information om hur vanligt förekommande det är med insiders i företag. Det är svårt att bedöma hur utbrett fenomenet är eftersom risken att upptäckas är låg.

Johanna Skinnari, biträdande enhetschef på Brå, säger i en intervju i tidskriften *Kvartal* att i de flesta fall rekryterar de kriminella nätverken personer som redan är anställda på den arbetsplats som gängen riktar sitt intresse mot.

> ”Den som blir insider kanske har köpt narkotika, den kan ha olika typer av andra missbruk som gör att den är närvarande i det kriminella nätverkets kontakter. Man kanske lånar pengar på grund av spelskulder eller köper sex. Och det man ska förstå om kriminella nätverk är att de lever på en väldigt hård marknad där varje kontakt är jätteviktig. Så när de frågar hur det är eller vad man jobbar med, så är det inte small talk. De samlar information och kan ha nytta av det någon annan gång.”[16]

En anställd behöver ju inte ha gjort någon av dessa handlingar för att ha en sårbarhet som kan utnyttjas av de kriminella nätverken. Andra exempel på sårbarheter kan vara att ha väldigt höga skulder för sitt boende, eller andra ekonomiska problem, eller att leva isolerat utan något starkt socialt stöd. Den viktiga slutsatsen är att kriminella nätverk är mycket skickliga på att upptäcka och utnyttja personers sårbarheter.

Nästan vart tionde företag som själva bedömer att de i mycket eller ganska hög utsträckning kan bli utsatta för otillåten påverkan svarade ”Vet ej” på frågan om vilka åtgärder som är viktiga för att skydda verksamheten. Bland samtliga företag var andelen nästan 30 procent.

> De kriminella nätverken **söker efter en sårbarhet hos de anställda som de kan dra nytta av**. När de frågar hur det är så är det inte vanligt small talk. De samlar information de kan dra nytta av senare. De är mycket skickliga på att upptäcka och utnyttja personers sårbarheter.

Det kan tyda på att många företag inte är tillräckligt förberedda på att otillåten påverkan kan drabba dem. Till skillnad från exempelvis inbrott eller skadegörelse handlar otillåten påverkan ofta om handlingar som är svårupptäckta – de är handlingar som är avsedda att inte synas.

I syfte att dels skatta andelen företag som utsatts för brott som innefattar otillåten påverkan, dels utforska och förstå upplevelser hos företag och företagare som utsatts för otillåten påverkan gjorde Demoskop, på uppdrag av Svenskt Näringsliv, en undersökning första halvåret 2025 där brottsutsatta företagare och säkerhetsexperter intervjuades. I den kvalitativa delen var fokus på riskmedvetenhet, händelseförlopp, anmälningsprocessen och framtida stödbehov.[17]

16 Johanna Skinnari intervjuad av Ellinore Levinsson, ”Så tar kriminella nätverk sig in i den lagliga världen”, ***Kvartal,*** 2025-09-11.
17 Svenskt Näringsliv (kommande).

”Stölder och bedrägerier hör tyvärr till vår vardag”

Mårten Tenne driver en ICA Maxi-butik i Nyköping. Stölder och snatterier pågår dagligen och innebär också risk för hotfulla situationer. En företagskapning utvecklades dessutom till en mardröm med utdraget rättsligt efterspel.

För Mårten Tenne och hans personal är stölder en del av vardagen även om dessa varken ökat drastiskt eller avtagit. Det är en konstant. Men stöldernas mönster har delvis förändrats.

– Stölder och snatterier hör till vardagen i butiken och självscanningsbedrägerierna har ökat kraftigt. Det har blivit vanligare med medvetet fusk, att betala för andra varor än de som man har lagt i varukorgen, eller att väga en vara för att sedan lägga i fler.

Mårten upplever också att de stölder som organiserade ligor står för har minskat men att de som trots allt sker, främst handlar om kött, kaffe, choklad och tekniksaker som har lokal avsättning.

Oavsett om det är snatterier eller organiserad brottslighet – konsekvenserna är flera

Konsekvenserna av stölder och bedrägerier är både ekonomiska och mänskliga. Mårten berättar att de förlorar cirka 0,6 procent av varorna varje år.

– Det handlar om drygt 3 miljoner kronor årligen. Även om inte allt kan härledas till stölderna står de för den absolut största delen.

Mårten konstaterar att alla stölder i slutänden betalas av kunderna, på varornas pris.

Men det är personalens arbetsmiljö som bekymrar mest.

– Stölder och bedrägerier är otrevliga situationer att hantera. Det kan vara utsatta människor, påtända eller ”vanliga” människor i en utsatt situation. Många försöker hota sig ur en stöldsituation. Hur reella hoten är vet man inte, men det finns ju vapen och knivar i omlopp. Det är jobbigt för personalen.

Företagskapning – nio månaders mardröm

En utdragen och svår händelse var den företagskapning som drabbade Mårtens butik. En internationell liga använde företagets uppgifter för att beställa varor från grossister i hela Europa.

– De skapade en domän med ett företagsnamn som liknade vårt och började beställa varor från Spanien, Tyskland, Tjeckien, Polen, Rumänien. Företag hörde av sig och frågade var de skulle skicka varorna.

> ”Alldeles för många polisanmälningar läggs ned. [...] Det gör ju att de här gärningspersonerna kan fortsätta begå brott.”

– Det beställdes och levererades varor för många hundra tusen kronor. Vi fick fakturor, de skickade varor till en lagerplats i Helsingborg. Det pågick i nio månader. Efter två år fick vi dessutom inkassokrav från ett företag från Polen och vi blev stämda i polsk domstol.

Utöver den tid som bedrägerierna pågick och den oro som företagskapningen ledde till, landade kostnaderna för att anlita advokater och rättegångskostnaderna på runt 150 000 kronor.

Polisanmälan lades ner med vändande post.

– Vi fick ingen hjälp av polisen utan fick ta hand om det själva med hjälp av advokater. Det är så klart komplext men vi blev helt ensamma i det här. Det är inte det här man vill hålla på med, att bestrida fakturor i Polen.

> Dagens tillträdesförbud är krångligt och verkningslöst.”

Personalen måste kunna känna sig trygg

För att hantera säkerhetsfrågorna lokalt har butiken skyddskommitté och säkerhetsansvarig. Mårten betonar att hela personalen måste vara involverad.

– Det handlar om tydliga säkerhetsrutiner som hela personalen måste känna till. Framför allt har vi fokus på personalens säkerhet. Det är ett ständigt arbete.

Tillträdesförbudet är helt verkningslöst

Trots aktivt deltagande i kommunens lokala brottsförebyggande råd, där dialog och kontaktnät fungerar bra, är Mårten frustrerad över bristen på att förhindra stöldbrott.

– Polis och åklagare måste ha resurser att ta stölder på allvar. Alldeles för många polisanmälningar läggs ned. Det är alldeles för många små brott som de kallar det, som läggs ned. Det gör ju att de här gärningspersonerna kan fortsätta begå brott.

Särskilt kritisk är Mårten mot Tillträdeslagen.

– Den är helt verkningslös. Jag vill kunna säga ”du är inte välkommen hit”, men en person måste vara dömd för brottet innan tillträdesförbudet ens kan gälla. Dagens tillträdesförbud är krångligt och verkningslöst.

Mårten pekar även på ett större samhällsproblem bakom mycket av den brottslighet som dagligvarubutiker utsätts för.

– Det är oroligt, många mår dåligt, har missbruk, men de beter sig samtidigt hotfullt och stjäl. I förlängningen kommer politiken och samhället in här. Det är ett samhällsproblem.

Undersökningen visar att otillåten påverkan är vanligt förekommande i brott mot företag, men att den ofta förbises eller underordnas mer konkreta brott som stöld, skadegörelse och hot. Framför allt mindre företag tenderar att fokusera på det mätbara, medan de subtila och emotionella påverkansmekanismerna glider undan uppmärksamheten.

Studien beskriver en påverkan i gråskalor, där kriminella aktörer medvetet balanserar på gränsen till det otillåtna – exempelvis genom antydningar, ”oskyldiga” frågor eller oväntade möten – vilket gör brotten svåra att definiera och anmäla. Detta skapar en hög risk för underrapportering, särskilt när påverkan lyckas och därför aldrig når myndigheternas kännedom.

Större organisationer har ofta system för att hantera sådana hot, medan mindre aktörer saknar resurser och kunskap. Rapportens belyser hur otillåten påverkan, trots att den ofta behandlas som ett sekundärt problem, i själva verket kan vara en drivande kraft bakom många brott som drabbar svenska företag.

Ytterligare en kunskapskälla om hur otillåten påverkan drabbar privata företag är den lägesbild[18] som tagits fram inom den samverkansöverenskommelse som Svenskt Näringsliv och Polismyndigheten slöt 2024. Syftet är att öka företagens motståndskraft och minska sårbarheten i de kritiska funktioner som kan exploateras av kriminella aktörer.

Den lägesbilden bygger på den information som framkommer i Demoskops undersökning, kompletterad med en kvantitativ analys som omfattar polisanmälda brott 2019–2024 mot privata företag.

I den kvantitativa analysen baserad på registerdata studeras särskilt:

- Antal företag med samhällsviktig verksamhet.[19]
- Antal företag som anmält brott vid upprepade tillfällen.
- Den kumulativa fördelningen av brott mellan företag.
- Företagens anmälningar i relation till beredskapssektorer.

Från denna analys dras följande huvudslutsatser:

- Det föreligger en överrepresentation av otillåten påverkan i företag som bedriver samhällsviktig verksamhet.
- Ett fåtal privata företag står för en stor andel av anmälningarna.
- Risken för att funktioner i företag utsätts för otillåten påverkan ökar när företaget utsätts vid upprepade tillfällen.
- Företag inom ett flertal samhällsviktiga områden och beredskapssektorer[20] är utsatta.

Gråzon mellan cyberbrott och otillåten påverkan

Studier, bl.a. från Säpo, MUST, MSB, Europol och FOI,[21] visar att det finns en gråzon mellan cyberbrott och otillåten påverkan, att den växer och är svår att fånga i statistik. Gråzonen uppstår när cyberbrott används inte bara för teknisk skada eller vinning, utan som en form av utpressning, psykisk press och styrning. Kriminella nätverk och främmande makter ligger bakom dessa brott, ibland i samarbete.

Säkerhets- och underrättelsetjänsterna i Ryssland, Kina och Iran har hög förmåga till att utföra cyberbrott och de har alla egna cyberenheter som genomför angrepp.[22] Ryssland är det största hotet och bedriver offensiv underrättelse- och påverkansverksamhet, inklusive sabotage. Kina arbetar långsiktigt för att anskaffa teknik, särskilt riktat mot svenska forskningsmiljöer, och påverka opinionen. Iran bedriver underrättelseverksamhet mot oppositionella och judiska mål, och har använt kriminella nätverk för våldsdåd.

18 Svenskt Näringsliv och Polismyndigheten (kommande).

19 Med samhällsviktig verksamhet avses verksamheter, tjänster eller infrastrukturer som upprätthåller eller säkerställer samhällsfunktioner nödvändiga för att tillgodose samhällets grundläggande behov, värden eller säkerhet, (se MSBFS 2024:9).

20 Det civila försvaret i Sverige är indelat i tolv beredskapssektorer, var och en ledd av en ansvarig myndighet. Syftet är att säkerställa samhällets funktionsförmåga vid kris eller krig. Myndigheter och företag som bedriver samhällsviktiga verksamheter kan tillhöra en eller flera sektorer, beroende på verksamhetens natur.

21 Se t.ex. MSB (2023), Jonsson, Eriksson, Ingemarsdotter, Rossbach & Wedebrand (2023), Säpo (2024), MUST (2024) och Europol (2025).

22 Säpo (2024)

1 CYBERBROTT SOM VERKTYG FÖR OTILLÅTEN PÅVERKAN

- **Informationsstöld** kan användas för att utpressa företag eller beslutsfattare (t.ex. hot om att läcka känsliga uppgifter om man inte följer kriminellas krav).
- **Ransomware** (utpressningsvirus), DDoS-attacker (överbelastningsattacker) eller dataintrång kan riktas mot företag eller myndigheter för att stressa fram beslut eller visa makt.
- **Deepfakes** (AI-genererade förfalskningar) och desinformation används för att skada rykten, skapa osäkerhet eller splittring.

2 SUBTILA PÅVERKANSOPERATIONER I DIGITAL MILJÖ

- **Kriminella** nätverk och främmande makter använder sociala medier, hackade konton och anonyma forum för att sprida hotfulla budskap utan att det blir tydliga brottsrubriceringar.
- **Gränsen** mellan trakasserier, hot och påverkanskampanjer blir suddig när de sker digitalt och kan maskeras som ”vanlig nätaktivitet”.

3 SVÅRIGHETER ATT AVGRÄNSA

- **Juridiskt** klassas ofta cyberbrott som dataintrång, bedrägeri eller sabotage – medan den psykologiska dimensionen av påverkan inte lyfts fram.
- **Brottsoffren** upplever däremot ofta både tekniska och emotionella effekter: ett intrång kan samtidigt vara ett sätt att visa makt, inge rädsla och styra handlingsmönster.

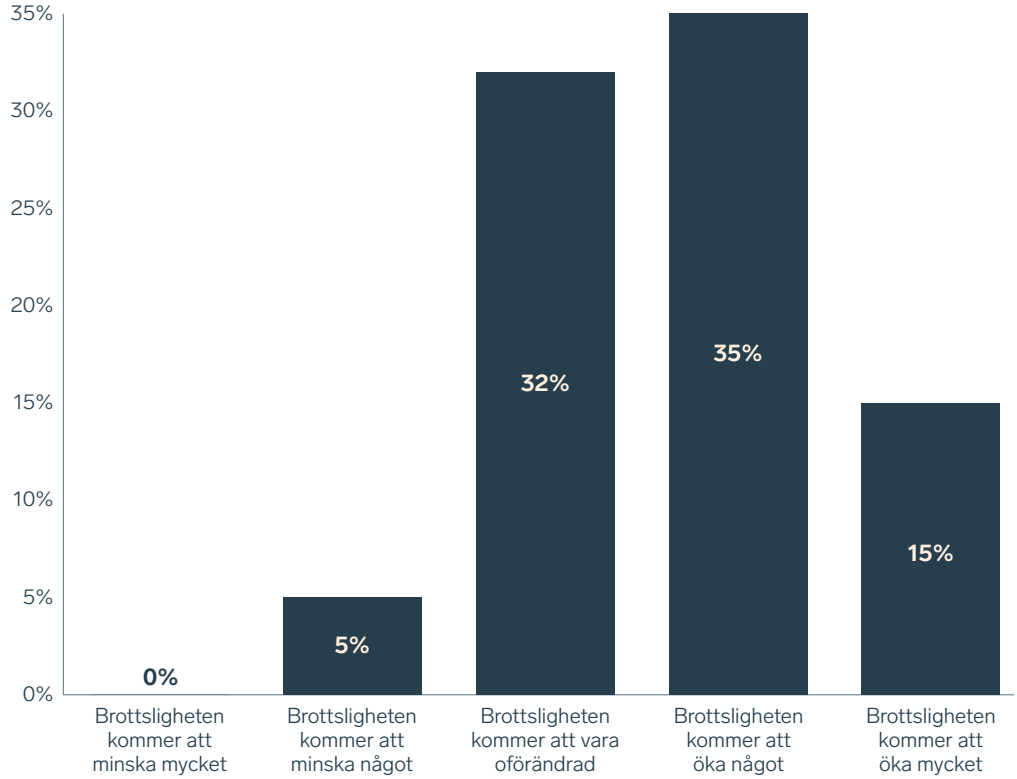
4 KONSEKVENSER

- **Gråzonen** innebär en hög risk för underrapportering, eftersom företag kan uppfatta cyberbrottet som ”bara ett IT-problem” snarare än ett försök till påverkan.
- **Denna gråzon** gör det också svårt för myndigheter att prioritera rätt åtgärder: ska det hanteras som IT-säkerhet, brottsbekämpning eller skydd mot otillåten påverkan?

Hälften av företagen tror att brottsligheten kommer att öka

Hälften av företagen tror att brottsligheten i samhället kommer att öka mycket eller något det kommande året. En tredjedel tror att den kommer att vara oförändrad. Endast 5 procent av företagen tror att brottsligheten i samhället kommer att minska något och mindre än 1 procent tror att den kommer att minska mycket.

Figur 10. Hur tror du brottsligheten i samhället kommer att förändras det kommande året?



Not: Andelen företag som svarade ”Ingen uppfattning” uppgick till 13 procent.
Källa: Svenskt Näringslivs Företagarpanel, april-maj 2025.

Inom handel och transport är det närmare 6 av 10 företag som tror att brottsligheten kommer att öka mycket eller något. Inom byggindustrin tror drygt hälften av företagen på en ökande brottslighet. Inom tjänstesektorn är det knappt hälften och inom besöksnäring samt industri är det cirka 4 av 10 företag som tror att brottsligheten kommer att öka.

Vilka blir konsekvenserna för brottsutsatta företag?

Ekonomiska förluster och ökade kostnader

Att bli utsatt för brott orsakar inte enbart omedelbara ekonomiska förluster för företagen, utan också följdkostnader, ofta långvariga.

Till att börja med tillkommer kostnader för egna brottsförebyggande åtgärder: investeringar i larm, kameraövervakning, IT-säkerhet, personalutbildning och, i vissa fall, väktartjänster. En hög brottsexponering leder dessutom ofta till höjda försäkringspremier, och i värsta fall till att företag nekas försäkring på rimliga villkor.

För små och medelstora företag kan brottsligheten få omedelbara effekter på likviditeten. Ett fakturabedrägeri, en större stöld eller omfattande skadegörelse kan snabbt undermine-ra kassaflödet. Till skillnad från större bolag har mindre företag ofta begränsade reserver och sämre möjligheter att sprida riskerna, vilket gör att en enskild händelse kan hota hela verksamhetens överlevnad.

Enligt Entreprenörskapsforum (2025) uppger nystartade företag i betydligt högre grad än etablerade verksamheter att brottsligheten påverkar dem negativt – oavsett om det gäller investeringar, inköp, expansionsplaner eller den långsiktiga utvecklingen. Nästan en tredje-del av de brottsutsatta nyföretagarna har till och med valt att lägga ned sin verksamhet.

Nästan

1/3

av de brottsutsatta nyföretagarna har valt att lägga ned sin verksamhet på grund av brottslighet.

På längre sikt riskerar brott att försvaga företagens konkurrenskraft och tillväxtförmåga. Osäkerhet kring tryggheten kan leda till att investeringar skjuts upp, att verksamheter flyt-tas eller läggs ned, och att rekrytering försvåras.

Kostnaderna förknippade med brott är dock inte enbart ekonomiska. Minst lika allvar-liga är de psykologiska kostnaderna – de icke-monetära följder som drabbar företagare och deras personal. Det handlar om oro, ångest, sömnproblem, känslor av otrygghet och nedstämdhet, och i svårare fall posttraumatiskt stressyndrom (PTSD). Dessa effekter kan bestå långt efter själva händelsen och påverkar både produktivitet, beslut och viljan att fortsätta driva verksamheten.

En negativ spiral: Polisens bristande kapacitet att klara upp brott bidrar till att många brott mot företag aldrig anmäls

Riksrevisionen (2023) konstaterade att Polismyndigheten inte hanterar mängdbrott effek-tivt. Trots ökade anslag och bättre förutsättningar för rekrytering och kompetensutveckling är den operativa förmågan fortsatt bristfällig, enligt Riksrevisionen, och detta beror främst på tre faktorer: resurser dräneras ständigt från lokalpolisområdena för att hantera grova brott på andra nivåer, nödvändig kompetensutveckling och spridning av goda arbetssätt uteblir, samt ett internt beslut begränsar anställningen av civil personal som annars skulle kunna avlasta poliser i centrala uppgifter.

Polismyndigheten fick därför i regleringsbrevet för 2024 i uppdrag att redovisa vilka åtgärder som myndigheten vidtagit för att förstärka utredningsförmågan kopplat till mängdbrott. Polismyndighetens bedömning var att merparten på olika sätt var relevanta och redan adresserades i Polismyndighetens löpande utvecklingsarbete, och gav olika exempel på detta, som framtagande av en mer enhetlig ledningsstruktur för utredningsverksamheten, utveckling av en nationell ordning för sortering och prioritering, och inventering av behov för en effektiv kompetensförsörjning.[23]

Riksrevisionen (2025) granskade om Polismyndigheten har arbetat effektivt för att uppnå målen med den stora omorganisationen 2015, då 21 länspolismyndigheter, Statens kriminaltekniska laboratorium och Rikspolisstyrelsen slogs ihop till en myndighet. Reformen syftade till ökad kvalitet, effektivitet, flexibilitet och bättre resultat i polisens verksamhet. Riksrevisionens slutsats är att dessa intentioner inte har uppnåtts. Till exempel minskar antalet uppklarade brott trots att personalstyrkan vuxit betydligt och anslaget nästan fördubblats sedan 2015.

> Att företagen inte polisanmäler brott bidrar till att brott mot företag underskattas och osynliggörs. **Följden blir en ofullständig och troligen alltför ljus bild av företagens brottsutsatthet.** Det blir en negativ spiral som startar med polisens bristande kapacitet att klara upp brott.

Att företagen inte polisanmäler brott de varit utsatta för är allvarligt eftersom det signalerar ett långvarigt, lågt förtroende för polisen och bidrar till att brott mot företag underskattas och osynliggörs. Följden blir en ofullständig och troligen alltför ljus bild av företagens brottsutsatthet, och detta kan vidare ge konsekvenser i form av en snedvridning av polisens resursfördelning som en följd av den ofullständiga informationen. Det blir en negativ spiral som startar med polisens bristande kapacitet att klara upp brott.

Svenskt Näringsliv betonar vikten av att företag polisanmäler alla brott. Genom anmälningarna kan polisen och andra beslutsfattare få en mer fullständig bild av brottslighetens omfattning, utveckling och konsekvenser. Detta är också en förutsättning för att gärningspersoner ska kunna ställas till ansvar och hindras från att begå nya brott. Om anmälningsnivån är låg riskerar brottsbekämpningen att bli ineffektiv, och politiska beslut som skulle kunna göra insatserna mer träffsäkra kan utebli. Följden kan bli att företagen drabbas hårdare och att förtroendet för samhällskontraktet gradvis undergrävs.

23 Polismyndigheten (2024), sid. 52.

Oro eller utsatthet för brott ger effekter på investeringar och rekryteringar

I genomsnitt uppger ett av tjugo företag, oavsett bransch, att de under det senaste året på grund av oro för eller utsatthet för brott

- övervägt att lägga ned delar av eller hela verksamheten,
- avstått från investeringar, eller
- haft svårt att rekrytera personal.

Ser man till enskilda branscher framträder vissa skillnader. Handeln är mest utsatt när det gäller nedläggnings- och investeringsbeslut: 7 procent av företagen har övervägt att lägga ned verksamhet och 8 procent har avstått från investeringar. När det gäller rekrytering är transportbranschen hårdast drabbad: 10 procent av företagen uppger att oro för eller utsatthet för brott försvårat möjligheten att anställa.

Osund konkurrens drabbar seriösa företag

Osund konkurrens uppstår när företag bryter mot lagar, regler eller avtal och därmed skaffar sig orättvisa fördelar. Seriösa företag som blir drabbade av osund konkurrens är inte brottsutsatta i lagens egentliga mening men de destruktiva effekterna som osund konkurrens har på marknaderna undergräver förtroendet för deras funktionssätt. Seriösa företag i utsatta branscher kan tvingas “anpassa sig nedåt” eller lämna marknaden vilket ger effekter på branschstruktur samt utbud av varor och tjänster.

Den osunda konkurrensen drivs av flera faktorer:[24]

- kriminella aktörer som använder företag för vinning eller penningtvätt,
- ”grå” företag som medvetet rundar regelverk,
- myndigheter som inte kontrollerar tillräckligt effektivt,
- politiker som inte ger rätt verktyg eller resurser,
- seriösa företag som brister i kontrollen av sina affärspartners,
- upphandlare som, av resursbrist eller rädsla för överprövning, inte följer upp leverantörer.

Redan 2013 pekade Riksrevisionen på offentlig upphandling som ett speciellt riskutsatt område.[25] Sju år senare, 2020, understryker Konkurrensverket samma sak, att offentlig upphandling är ett riskområde.[26] Ett särskilt problem är att många offentliga upphandlare ensidigt fokuserar på lägsta pris. Det står upphandlarna fritt att göra det, men det resulterar i problem att konkurrera på sunda villkor. Enligt en undersökning från Almega 2024 avstår cirka 40 procent av medlemsföretagen från offentlig upphandling.[27] Dessa företag uppger att den enskilt viktigaste orsaken till att inte delta är att det är för stort fokus på lägsta pris.

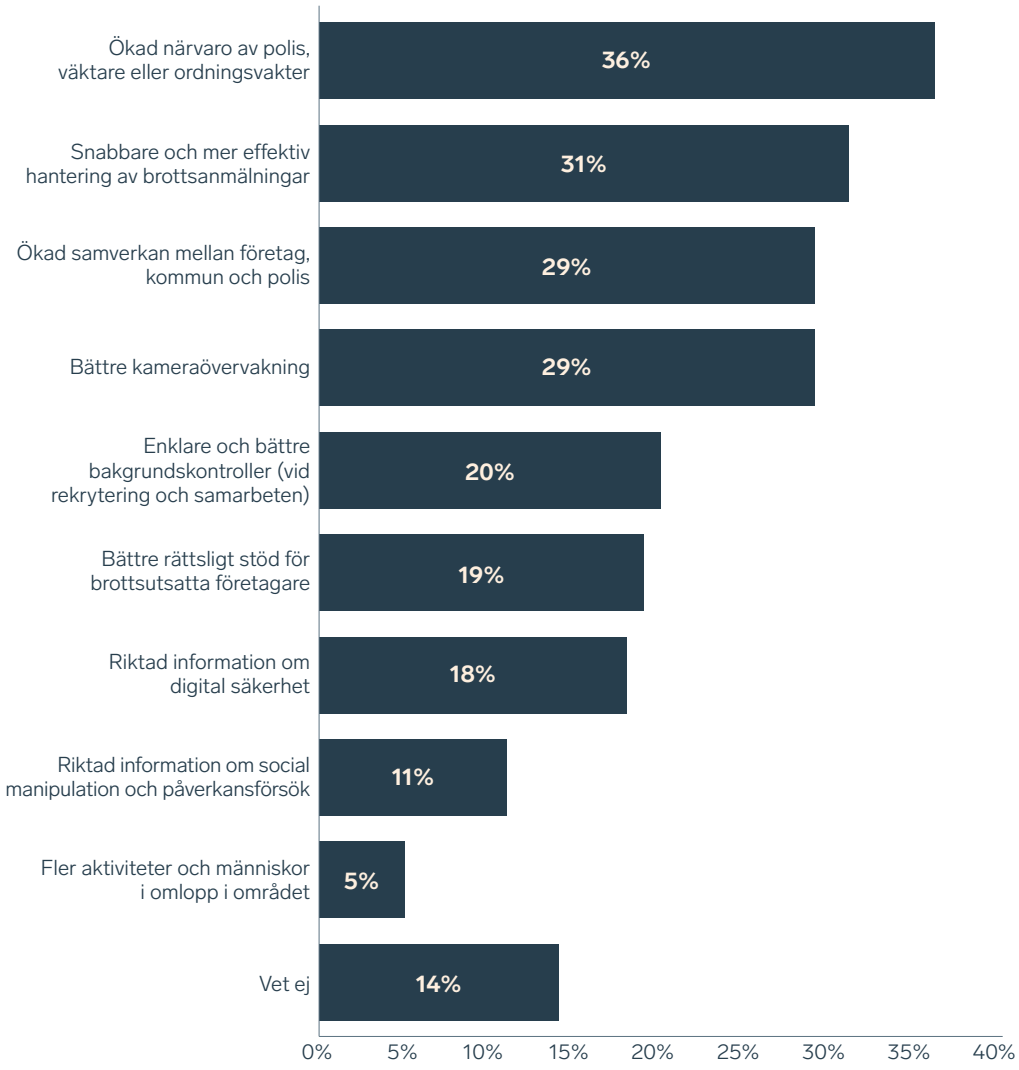
24 Svenskt Näringsliv (2023a)
25 Riksrevisionen (2013)
26 Konkurrensverket (2020)
27 Almega (2024)

Ökad polisnärvaro och effektiv hantering av brottsanmälningar viktigast för ökad trygghet

Enlig svaren i Svenskt Näringslivs Företagarpanel är den viktigaste åtgärden för att öka tryggheten för företagen och dess anställda ökad närvaro av polis, väktare eller ordningsvakter. Tätt efter kommer snabbare och mer effektiv hantering av brottsanmälningar. På en delad tredjeplats kommer ökad samverkan mellan företag, kommun och polis samt bättre kameraövervakning.

Enklare och bättre bakgrundskontroller vid rekrytering och samarbeten samt bättre rättsligt stöd för brottsutsatta företagare kommer en bit längre ned på delad fjärde plats. På femte plats kommer riktad information om digital säkerhet. En bit längre ned, på sjätte plats, kommer riktad information om social manipulation och påverkansförsök. Sist kommer fler aktiviteter och människor i omlopp i området, som ett sätt att öka tryggheten. Andelen företag som svarade att de inte visste vilka de trygghetsskapande åtgärder de helst skulle vilja se uppgick till 14 procent.

Figur 11. Vilka åtgärder skulle du helst vilja se för att öka tryggheten för företagen och dess anställda?



Not: Respondenterna fick uppge upp till tre svarsalternativ. Andelen företag som svarade ”Annan åtgärd” respektive ”Finns inga särskilda behov” uppgick till 3 procent respektive 7 procent.
Källa: Svenskt Näringslivs Företagarpanel, april-maj 2025.

Vilka blir konsekvenserna för samhället av brottslighet mot företag?

Kort- och långsiktiga konsekvenser

När företag drabbas av mängdbrott – såsom stölder, skadegörelse och bedrägerier – uppstår inte bara kostnader för de enskilda företagen utan också för samhället i stort. Rättsväsendet belastas av fler polisutredningar, fler åtal och ett växande tryck på domstolar och kriminalvård.

På kort sikt leder brottslighet till att företagens resurser måste omfördelas: Mer måste läggas på skadehantering, säkerhetsåtgärder och försäkringspremier; mindre kan läggas på produktiva investeringar.

Detta får stor betydelse på lång sikt: Företagens möjligheter att växa, anställa och utveckla nya produkter och tjänster minskar därmed. Följderna blir lägre sysselsättning, minskade skatteintäkter och förlorade innovationsmöjligheter – vilket hämmar både produktivitet och BNP-tillväxt.

Utöver dessa följder tillkommer betydande dynamiska effekter. Brottslighetens långsiktiga konsekvenser sprider sig genom ekonomin och påverkar tillväxtförutsättningarna över tid. När företag drar sig ur brottsutsatta områden eller branscher försämras det lokala näringslivets struktur och konkurrenskraft.

I områden som redan präglas av socioekonomisk utsatthet blir effekterna särskilt tydliga. När butiker, gym, restauranger och frisörer tvingas stänga till följd av brottslighet och otrygghet försvinner inte bara arbetstillfällen utan även centrala funktioner som bidrar till vardagsservice, lokalt kapital och socialt liv. Det skapar en negativ spiral där ekonomisk stagnation, minskad attraktivitet och fortsatt kriminalitet förstärker varandra – och där samhällets kostnader ökar i takt med att de förebyggande funktionerna minskar i betydelse.

En särskild samhällsrisk uppstår när företag utsätts för otillåten påverkan. Även om det förfaller vara en minoritet av företag som berörs kan konsekvenserna bli omfattande, eftersom själva beslutsfattandet i företagen riskerar att snedvridas under påtryckningar. När hot, trakasserier eller korrupta erbjudanden påverkar vilka affärsrelationer som upprätthålls, vilka leverantörer som anlitas eller vilka upphandlingar man deltar i, rubbas principerna om fri konkurrens och likabehandling. Företag kan börja fatta beslut som inte bygger på ekonomisk rationalitet eller kvalitet, utan på rädsla, lojalitetstvång eller beroende av kriminella aktörer.

När företag drar sig ur brottsutsatta områden eller branscher **försämras det lokala näringslivets struktur och konkurrenskraft**.

Samhällshotande och systemhotande brottslighet

Organiserad brottslighet exploaterar strategiska sårbarheter i näringslivet. Den utgör ett samhällshot och i förlängningen även ett systemhot. Polismyndigheten har inga formella definitioner av begreppen ”samhällshotande brottslighet” och ”systemhotande brottslighet”, men man använder och beskriver dem i enlighet med hur dessa brottslighetstyper påverkar samhället och dess institutioner.

Brottslighet som är samhällshotande påverkar människors tillit och trygghet. Den utgör betydande hot mot samhället eftersom den drabbar många individer och företag i vardagen – ofta med hög grad av organisatorisk effektivitet – men skyddsvärda samhällsfunktioner står kvar oskadda.

Systemhotande brottslighet är ett direkt angrepp mot skyddsvärda samhällsfunktioner, deras system eller företrädare samt påverkar deras beslut och hotar att skada institutionernas förmåga att fullgöra sina uppgifter. Kriminalitetens institutionaliserande roll innebär att den utvecklas till ett alternativt system för styrning och reglering, där brottsliga normer och strukturer i praktiken får samma funktion som samhällets officiella institutioner. “Den organiserade brottsligheten hatar […] allt vad individuell frihet och individuella rättigheter heter. Målet är en tyst, undergiven skrämd massa som inte ser, hör eller lägger sig i. Bara tjänar.” skriver Bo Wennström, professor emeritus i rättsvetenskap, i boken *Att vända bort blicken : Om underminering – dess filosofi, politik och praktik*.[28]

	Samhällshotande brottslighet	Systemhotande brottslighet
Kännetecken	Organiserad brottslighet som får breda negativa konsekvenser för samhället, men utan att direkt hota skyddsvärda samhällsfunktioner.	Organiserad brottslighet, kriminella nätverk och/eller främmande makt, som riktas mot eller undergräver skyddsvärda samhällsfunktioner och demokratins funktionssätt.
Effektnivå	Skapar otrygghet, snedvrider fri konkurrens och urholkar tilliten till myndigheter och marknader.	Hotar själva samhällsordningen och statens förmåga att fungera samt upprätthålla legitimitet.
Exempel	Arbetslivskriminalitet, organiserade swtölder, omfattande bedrägerier, vissa cyberbrott, bombdåd, miljöbrott, storskalig narkotikahandel.	Infiltration av myndigheter, spioneri, korruption, vissa cyberbrott, otillåten påverkan mot politiker eller tjänstemän.
Konsekvens	Minskad tillväxt, försämrat företagsklimat, långvarigt ökade offentliga utgifter, urholkade skattebaser, möjligheterna till såväl skattesänkningar som utgiftshöjningar blir mindre.	Förtroendekris för staten, risk för parallella maktstrukturer, ett normativt vakuum där rättsstaten uppfattas som frånvarande.

28 Wennström (2025), sid. 101.

Vad krävs för en framgångsrik brottsbekämpning?

Brott mot företag är ett samhällsproblem som kräver ett gemensamt ansvarstagande. Regering och riksdag måste ge tydliga mandat, resurser och rättsliga verktyg för att möjliggöra ett effektivt brottsförebyggande arbete. Polis och kommuner har huvudrollen i det lokala genomförandet, men insatserna blir verkningsfulla först när de sker i samarbete med näringsliv och civilsamhälle.

Enskilda företagare kan inte ensamma skydda sig mot brott och otrygghet. För att förebygga brott krävs ett strukturerat samarbete mellan företag, branschorganisationer, myndigheter och andra relevanta aktörer,[29] med stöd av en tydlig nationell inriktning. Bara genom gemensamma insatser kan brottsutsatthet och oro motverkas.

När fler aktörer involveras blir åtgärderna både mer träffsäkra och mer förankrade. Svenskt Näringsliv vill och kan vara en konstruktiv samarbetspartner för förändring. För att stärka tryggheten för företagare och anställda, och för att värna ett näringsliv med sund konkurrens kommer här våra 16 viktigaste uppmaningar till beslutsfattare i regeringen och riksdagen, på Polismyndigheten samt på kommunal nivå.

UPPMANINGAR TILL REGERINGEN OCH RIKSDAGEN

1. Prioritera bekämpningen av mängdbrott: Dessa brott drabbar företag och bidrar till att finansiera organiserad kriminalitet. Effektiva och uthålliga resurser på detta område minskar samhällskostnader, stärker företagsklimatet och ökar tryggheten för både företag och medborgare.
2. Öka möjligheterna för näringslivets engagemang att stärka samhällets gemensamma resurser mot kriminalitet: Förbättra skattereglerna om avdragsrätt för sponsring.
3. Stärk det förebyggande arbetet mot brott som drabbar näringslivet: Inrätta en nationell samordnare med tydligt uppdrag – med långsiktiga strategier, tydligare styrning och ett mer sammanhållet brottsförebyggande arbete.
4. Förstärk förtroendet för rättsväsendet och skapa verkningsfulla brottsförebyggande effekter: Skärp straffen för systematiskt begångna brott.
5. Öka möjligheterna att identifiera och förebygga kriminalitet: Förbättra förutsättningarna för informationsdelning mellan kommuner, polis, andra myndigheter och i vissa fall näringslivet.
6. Synliggör och skapa en tydligare bild av företagens utsatthet för brott: Revidera och komplettera brottsstatistiken med brottskoder som särskilt identifierar brott mot företag.
7. Förbättra företagens förmåga att motverka cyberhot och öka därmed cybersäkerheten i hela samhället: Stärk samarbetet och öka informationsdelningen mellan Nationella cybersäkerhetscentret och näringslivet.

29 Se t.ex. Svenskt Näringsliv, Polismyndigheten, Brå & Länsstyrelserna (2025) samt Ekobrottsmyndigheten (2022).

UPPMANINGAR TILL POLISMYNDIGHETEN

8. Förebygg brott och öka tryggheten: Stärk den lokala polisnärvaron.
9. Höj företagares förtroende för polisens kapacitet att hantera brottsanmälningar: Ge effektivisering av hanterande av brottsanmälningar högsta prioritet.
10. Motverka normalisering av brott och rekrytering av barn och unga till kriminalitet: Inför nolltolerans mot brott och prioritera mängdbrotten.
11. Synliggör förekomsten av otillåten påverkan: Tillsätt en specialiserad funktion för kartläggning av otillåten påverkan mot näringsliv och myndigheter. I dag sprids ärenden på flera enheter (korruption, bedrägeri, demokratibrott), vilket gör att otillåten påverkan lätt försvinner bland mängdbrotten. En nationell specialistresurs kan kunna analysera mönster, ge operativt stöd till lokalpolisområden, bygga kompetens hos utredare och samla statistik.
12. Stärk samarbetet med näringslivet och möjliggör en mer kunskapsbaserad och proaktiv bekämpning av brott mot företag: Tillsätt en specialiserad funktion för näringslivskontakt inom polisen.
13. Förbättra bekämpningen av cyberbrott: Främja samarbete mellan offentliga och privata aktörer inom IT-säkerhet och inrätta ett råd vid polisens nationella IT-brottscentrum, liknande det som finns vid European Cybercrime Center.

UPPMANINGAR TILL KOMMUNERNA

14. Skapa så kompletta lokala lägesbilder som möjligt: Kartlägg företagens utsatthet för brott och upplevda otrygghet i varje kommun.
15. Gör de lokala brottsförebyggande åtgärderna mer effektiva: Involvera näringslivet i upprättandet av lokala åtgärdsplaner, arrangera återkommande dialogmöten mellan näringsliv, kommun och polis och bjud in näringslivsrepresentanter till det lokala brottsförebyggande rådet.
16. Förbättra det lokala företagsklimatet: Integrera åtgärder mot brott och otrygghet som vitala delar av varje kommuns näringslivsstrategi.

Kommunernas ansvar

Med den nya lagen (SFS 2023:196) har kommunerna fått ett utökat ansvar för att göra det brottsförebyggande arbetet mer kunskapsbaserat och effektivt. Kommunerna ansvarar för två centrala samverkansformer.

1) De ska leda ett strategiskt råd (även kallat lokalt brottsförebyggande råd) med relevanta aktörer och fungera som en styrgrupp för det lokala brottsförebyggande arbetet.

2) De ska teckna samverkansöverenskommelser mellan kommunen och relevanta aktörer.

Kommunerna är också skyldiga att ta fram en lägesbild över brottsligheten i området och utifrån den besluta om en åtgärdsplan med konkreta insatser för att förebygga brott. Enligt Brå upplever kommunerna att lagen gett arbetet ökad legitimitet och högre politisk prioritet. Samverkan med polisen har förbättrats, men samarbetet med andra aktörer, särskilt näringslivet, är fortfarande svagt. Brist på resurser lyfts som största hinder, framför allt i mindre kommuner, där en person ofta måste hantera flera roller samtidigt. Endast 15 procent av kommunerna samverkar med näringslivet i enlighet med lagen, och färre än en av tio uppfyller samtliga lagstadgade krav.

Referenser

Almega (2024). Offentlig upphandling ur tjänsteföretagens perspektiv.

Brå (2022). Polisanmälda dataintrång. Karaktär, utmaningar, utvecklingsområden. Rapport 2022:8.

Brå (2025a). Statistik om brott mot företag och organisationer. Rapport 2025:12.

Brå (2025b). Brott mot företag. Rapport 2025:16.

Ekobrottsmyndigheten (2022). Checklista: ”Så undviker du oseriösa aktörer”.

Entreprenörskapsforum (2025). Entreprenörskap i Sverige. Nationell GEM-rapport 2025.

Europol (2025). European Union Serious and Organised Crime Threat Assessment – The changing DNA of serious and organised crime, Publications Office of the European Union, Luxembourg.

Företagarna (2022). Brott mot företagare 2022.

Företagarna (2023). Brott mot företagare 2023.

Företagarna (2024). Brottsanmälan saknad. Hur får vi företagare att anmäla brott?

Jonsson, D. K.; Eriksson, C.; Ingemarsdotter, J.; Rossbach, N. H. & Wedebrand, C. (2023). Gråzonslägen i krig och fred, FOI, Rapport FOI-R--5447—SE.

Konkurrensverket (2020). Korruption och osund konkurrens i offentlig upphandling. Rapport 2020:1.

Levinsson, E. (2025). Intervju med Johanna Skinnari, ”Så tar kriminella nätverk sig in i den lagliga världen”, *Kvartal,* 2025-09-11.

MSB (2022). En inblick i Sveriges cybersäkerhet. Årsrapport it-incidentrapportering 2021.

MSB (2023). Motståndskraft i gråzon. (Utförare: Totalförsvarets forskningsinstitut, FOI)

MSBFS 2024:9. Föreskrifter om vilka samhällsviktiga verksamheter som omfattas av lagen (2023:560) om granskning av utländska direktinvesteringar.

MUST (2024). Årsöversikt 2024.

Myndighetsgemensam lägesbild (2023). Organiserad brottslighet 2023.

Myndighetsgemensam lägesbild (2025). Organiserad brottslighet 2025.

Nationellt cybersäkerhetscenter (2024). Cybersäkerhet i Sverige 2024.

Polismyndigheten (2024). Årsredovisning 2024.

Riksrevisionen (2013). Statliga myndigheters skydd mot korruption. RiR 2013:2.

Riksrevisionen (2023). Polisens hantering av mängdbrott – en verksamhet vars förmåga behöver förstärkas. RiR 2023:2.

Riksrevisionen (2025). Polisreformen 2015 – intentionerna ännu inte nådda. RiR 2025:26.

Rostami, A. & Mondani, H. (2024). Kriminella entreprenörer. – en studie av den organiserade brottslighetens kopplingar till näringslivet. På uppdrag av Stockholms Handelskammare.

Sallinen, J. & Ståhle, M. (2025). *Främmande makt. Utländska spioner på svensk mark*. Albert Bonniers Förlag.

SMOB (2024). Sverige mot organiserad brottslighet. Södertörns högskola.

SOU 2023:8. Arbetslivskriminalitet: arbetet i Sverige, en bedömning av omfattningen, lärdomar från Danmark och Finland. Delbetänkande av Delegationen mot arbetslivskriminalitet.

Stockholms Handelskammare (2022). Cyberbrott mot svenska företag – hur bygger vi en säkrare framtid?

Svenskt Näringsliv (2022). Brottslighetens kostnader 2022.

Svenskt Näringsliv (2023a). Arbetsmarknadskriminalitet – hur påverkas företagen och vad behöver göras?

Svenskt Näringsliv (2023b). Brottslighetens kostnader 2023.

Svenskt Näringsliv (2024). Brottsbarometern 2024.

Svenskt Näringsliv (kommande). Otillåten påverkan – lägesbild 2.0.

Svenskt Näringsliv och Polismyndigheten (kommande). Lägesbild 2025. Otillåten påverkan mot privata företag.

Svenskt Näringsliv, Polismyndigheten, Brå & Länsstyrelserna (2025). Tillsammans med näringslivet mot brott och otrygghet.

Säpo (2024). Säkerhetspolisen 2024 –2025.

Truesec (2025). Threat Intelligence Report 2025. An In-Depth Analysis of the Cyber Threat Landscape.

Tryggare Sverige (2024). Företagens trygghetsundersökning 2024.

Wennström, B. (2025). *Att vända bort blicken : Om underminering – dess filosofi, politik och praktik*. Jure Förlag AB.

Bilaga
– Data och metod

För att kartlägga företagens utsatthet för brott har Svenskt Näringsliv under våren 2025 genomfört tre undersökningar.

Den första undersökningen är en enkät som gått via e-post till medlemsföretagen i Svenskt Näringslivs Företagarpanel under perioden 29 april – 16 maj 2025. Frågorna rörande om företag blivit utsatta för brottslighet under de senaste 12 månaderna och om (eventuella) brott polisanmälts skickades ut till 13 600 medlemsföretag. 5 739 företag besvarade enkäten, vilket ger en svarsfrekvens på 42 procent. Övriga frågor om brottslighet som besvarades av Företagarpanelen skickades ut till en undergrupp i urvalet på 3 346 medlemsföretag. 1 376 företag besvarade dessa frågor, vilket ger en svarsfrekvens på 41 procent. Svaren har vägts på sektor och region.

Den andra undersökningen har Demoskop genomfört på uppdrag av Svenskt Näringsliv och Polismyndigheten. Målgruppen bestod av företag/företagare som har varit utsatta för brott som innefattar otillåten påverkan, både de som har anmält brott och de som inte har anmält brott, samt säkerhetsexperter från olika branscher. Undersökningen bestod av en kvantitativ webbenkät och kvalitativa djupintervjuer. Totalt genomfördes 1 239 intervjuer i den kvantitativa webbenkäten samt 18 djupintervjuer i den kvalitativa delen under februari–maj 2025. Svaren i den kvantitativa undersökningen har vägts på antal anställda och stad/landsbygd.

Den tredje undersökningen är den lägesbild som tagits fram som en del av den samverkansöverenskommelse som slöts 2024 mellan Svenskt Näringsliv och Polismyndigheten. Lägesbilden som fokuserar på hur otillåten påverkan drabbar privata företag och bygger samma data som Demoskops undersökning kompletterad med en kvantitativ studie som omfattar registerdata avseende polisanmälda brott mot privata företag under perioden 2019–2024.

www.svensktnaringsliv.se
Storgatan 19, 114 82 Stockholm
Telefon 08-553 430 00