omega point.

# Svenskt Säkerhetsindex® 2025

En årlig kartläggning av säkerhetsläget inom samhällsviktig verksamhet

I samarbete med

Radar.

# Innehåll


En alltjämt ökande oro ..... 4

En positiv negativ mognadsutveckling? ..... 8

Fler spår en ökad säkerhetsbudget ..... 10

Ett ökande gap mellan upplevd hotbild och förmåga ..... 16

Svenska befolkningen mer positiva till Nato ..... 18

Leveranskedjan – en exponentiellt ökande risk ..... 22

Samverkan stärker totalförsvarsförmågan ..... 26

Allmänhetens oro både ökar och minskar ..... 30

De tre viktigaste sakerna att fokusera på ..... 35

Om kartläggningen ..... 36

Om Omegapoint ..... 38

# Högre medvetenhet ger hopp

Årets Svenskt Säkerhetsindex beskriver förutom den upplevda hotbilden även hur allmänheten och beslutsfattare bygger upp insikt om hotbildens uppbyggnad och innehåll. Allt fler beslutsfattare blir medvetna om den kompetens som behövs för att adressera hot och hur man just nu kartlägger behov och gap som behöver stängas med ny förmåga.

Här kommer samverkan vara en viktig framgångsfaktor både internt och externt. Årets fördjupning handlar om leveranskedjor (supply chain) och Sveriges inträde i Nato.

Den upplevda hotbilden 2025 understödjer den långsiktiga trend där andelen som upplever en försämrad hotbild ökar – detta gäller både hos allmänheten och hos beslutsfattare.

Samtidigt visar allmänheten en fortsatt minskad tilltro till att beslutsfattare har förmåga att skydda viktig infrastruktur. Det är en bekymmersam utveckling när totalförsvarsförmågan i Sverige skall byggas upp. Högst tilltro har allmänheten till försvaret och blåljusorganisationerna. Försvaret verkar även ha fått en signifikant boost av tilltro genom medlemskapet i Nato.

En anmärkningsvärd paradox är att trots allmänhetens sjunkande tilltro till myndigheternas förmåga har man en mycket hög förväntan (9 av 10) av stöd från samma myndigheter i händelse av kris.

Samtidigt anser beslutsfattarna att de upplever en ökad förmåga i sina organisationer att identifiera och analysera hotbilden och sårbarheten. De har med andra ord blivit bättre på att kartlägga gap mellan befintlig förmåga och behov av ny förmåga. En konsekvens av detta blir att årets mätning av mognad sjunker jämfört med fjolårets. Det är en “positiv negativ utveckling” och ett nödvändigt steg för att bygga en faktisk förmåga som stänger gapet mellan hotbild och sårbarhet.

Som norra Europas ledande konsultbolag inom cybersäker digitalisering ser vi det som vår skyldighet att belysa situationen och aktivt arbeta för att sprida kunskap samt skapa debatt som gemensamt kan bidra till ett säkert och robust samhälle.

Hoppas du finner rapporten insiktsfull!

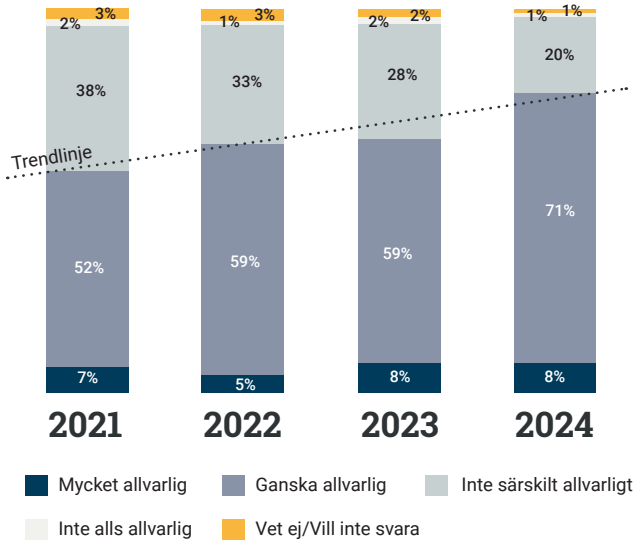
**Johan Malmliden**
Koncernchef Omegapoint

# En alltjämt ökande oro

## Hos beslutsfattare

Verksamheter och organisationer i statlig, offentlig och privat sektor upplever att hotbilden mot Sverige och samhället är ökande. Den mätningen följer samma fyråriga ökande trend som allmänheten nedan.

När andelen som upplever en allvarlig och mycket allvarlig hotbild slås samman är utfallet ungefär lika stort för både allmänheten och organisationer (allmänhet 76%, beslutsfattare 79%). Det finns därmed en samsyn kring upplevd hotnivå mellan dessa båda grupper.

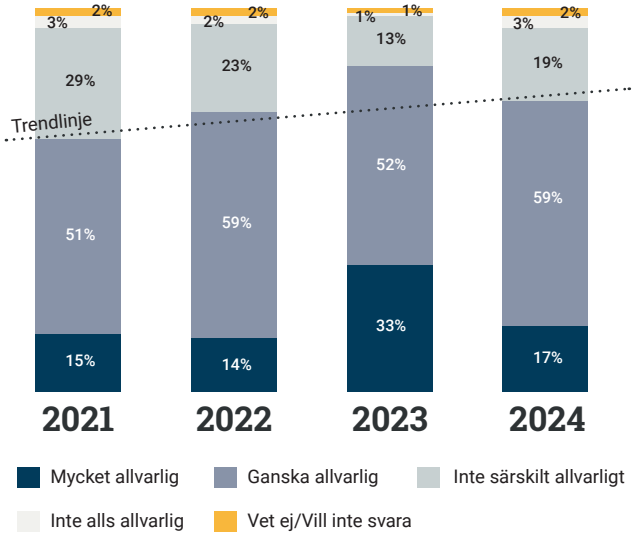



## Bland allmänheten

Allt fler anger att hotbilden mot Sverige är allvarlig eller mycket allvarlig idag, jämfört med för 4 år sedan. Det är en ökande trend, sett över åren 2021-2024.

Genom att titta på de som anger att hotbilden mot Sverige är allvarlig eller mycket allvarlig är det fler idag som svarar detta än vad de var för 4 år sedan.

Årets mätning visar dock att förra året (2023) markerar en topp och att nivån för 2024 har sjunkit något. Tappet är dock inte så stort att det hamnar under 2022 års nivå och därmed är den övergripande trenden baserad på 4 års mätningar att allmänheten upplever att hotbilden mot Sverige är ökande.




Den observerade toppen för allmänheten under 2023 kan möjligen förklaras av dramatiska geopolitiska och omdanande händelser som sammanföll med förra årets mätperiod. Den utmanande geopolitiska och säkerhetspolitiska utvecklingen har sedan dess fortsatt, men skapar möjligen inte lika skarpa reaktioner då det finns en ökad insikt om att ett allvarligt hotläge är en del av det nya normalläget.

Allmänhetens upplevelse av hotbild är intressant att tolka, men är troligen inte lika välgrundad som för beslutsfattarna. Beslutsfattare inom samhällsviktiga verksamheter har en dokumenterad erfarenhet och kunskap inom området med tillgång till data och rådgivning. Att denna grupp ser en mycket eller ganska allvarlig hotbildsutveckling har därmed en annan tyngd och är en oroväckande utveckling för samhället.

# Tydlig ökning i samhällsviktiga verksamheter

Den upplevda hotbilden mot samhällsviktiga verksamheter har ökat avsevärt under det senaste året. I årets mätning anser 8 av 10 (76%) respondenter att hotbilden är allvarlig, jämfört med 7 av 10 (67%) i föregående mätning. Den största förändringen återfinns i andelen som bedömer hotbilden som “ganska allvarlig”, vilket signalerar en brett förankrad ökning av riskmedvetenheten.

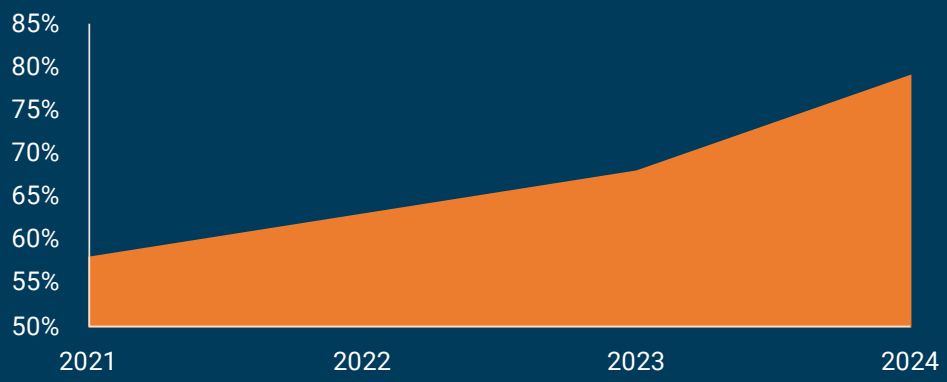
Generellt sett kan man utgå ifrån att samhällsviktiga verksamheter har högre kompetens, mognad och förmåga att bedöma och följa upp hot än andra verksamheter. De har högst troligt ett mer systematiskt och utvecklat förhållningssätt att analysera gap mellan sårbarhet och hot jämfört med befintlig förmåga.

Därmed är det intressant att årets mätning understödjer trenden över tid om en ökande upplevd hotbild hos beslutsfattare i samhällsviktiga verksamheter. Ökningen är signifikant i årets mätning med tanke på att det högst troligt är väl insatta beslutsfattare i ämnet.

En kompletterande delanalys kan också vara att dagens hotlandskap utgörs av hot och hotaktörer som för tillfället prioriterar samhällsviktig verksamhet. Kort och gott är exponeringsnivån högre i denna sektor just nu och det ökade hotet märks av tydligare för dessa verksamheter.

**8/10** upplever att hotbilden är allvarlig

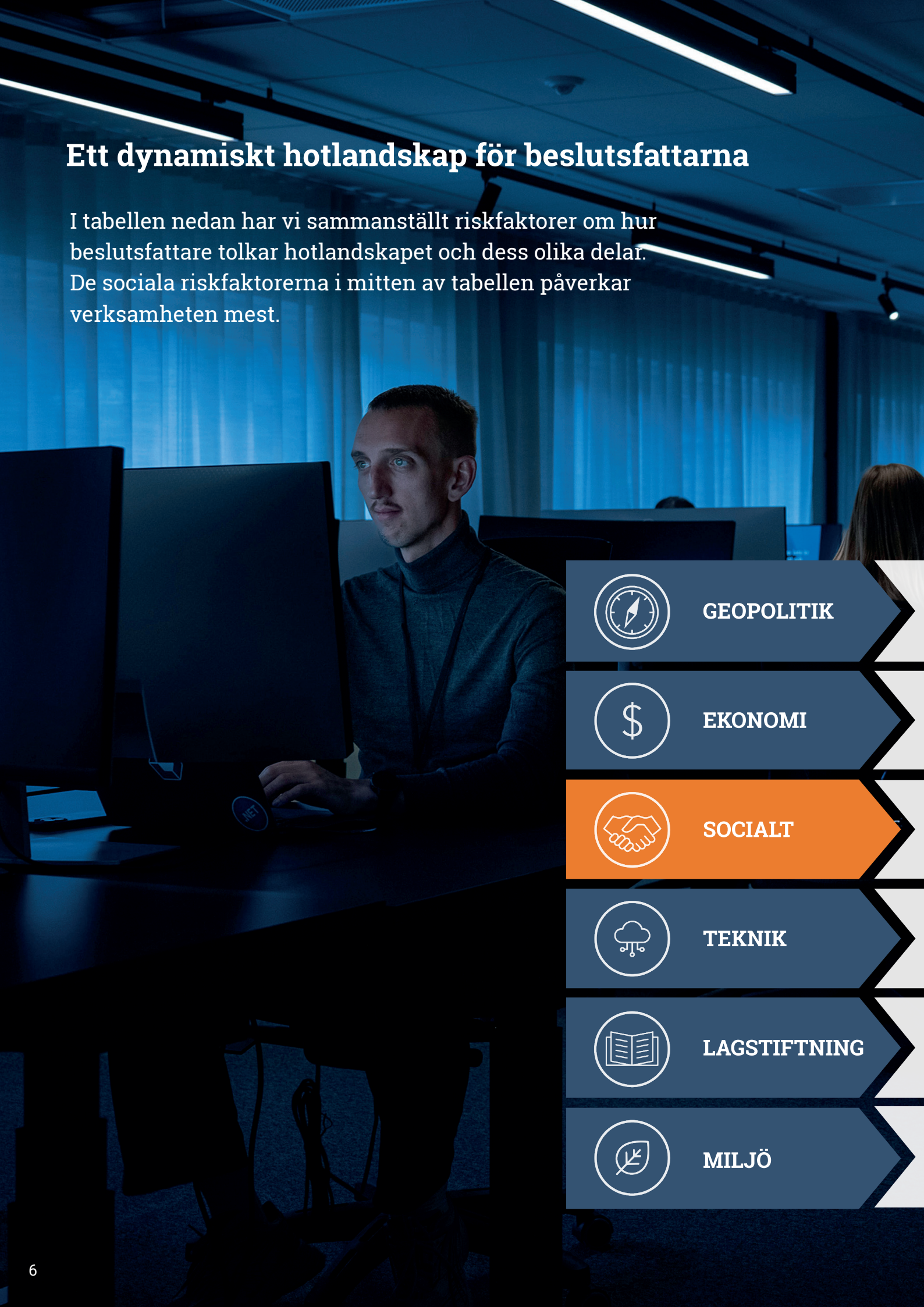
## Beslutsfattares* upplevda hotbild trend 2021–2024




*) Beslutsfattare för samhällsviktig verksamhet som svarar “mycket allvarlig” och “ganska allvarlig”.

# Ett dynamiskt hotlandskap för beslutsfattarna

I tabellen nedan har vi sammanställt riskfaktorer om hur beslutsfattare tolkar hotlandskapet och dess olika delar. De sociala riskfaktorerna i mitten av tabellen påverkar verksamheten mest.



- Ny president i USA
- Kina 2049 – partiprogram
- Globala försörjningskedjor
- Biologisk & teknisk krigsföring
- Splittrat Europa (försvagat)
- Sveriges roll och tillgång till EU & NATO
- Ryssland, Iran, Kina, Israel, Indien, Nordkorea

- Handelskrig och tullar
- Inflation
- Monopol
- Ekonomisk ställning påverkar säkerhetsmöjligheter (=ojämlika förutsättningar)

- Bred kompetensbrist
- Bristande tilltro till ledning
- Ojämn krisberedskap & naivt samhälle
- Säkerhetschefer bränns ut
- Låg tilltro till myndigheter
- Personalsäkerhet underskattas
- Bristande samverkan
- Bristande ledningsengagemang
- Allmänheten ser minskad hotbild
- Ej skalbar förmåga (befolkning)
- Gängkrim & smittspridning

- AI som hot och lösning
- Ny teknik vs säkerhetsförmåga
- IT/OT och OT-säk underskattat
- Exponentiellt ökande komplexitet
- Datahantering
- Ökad innovation & automation
- Antagonister snabbare på att dra nytta av ny teknik

- Små och medelstora bolag omfattas inte och får inte samma stöttning
- Sverige & NATO ej harmoniserande
- NIS2: otydlig
- CER: ej starkt fokus
- SSL: upplevs mer konkret men något utdaterad

- Olja och gas
- Minskat fokus/prioritering av hållbarhet
- Klimatomställning

# En positiv negativ mognadsutveckling?

### Mognadskriterier backar

I tidigare kartläggningar av har vi identifierat 11 nyckelområden för att bedöma säkerhetsmognaden inom verksamheter, där 6 områden anses särskilt kritiska (markerade med fetstilt). I år har 4 av dessa 6 kritiska områden uppvisat en negativ utveckling, vilket skulle kunna indikera att svenska verksamheter blivit mindre mogna.

Jämfört med 2024 års mätning ser vi relativt små rörelser. Samtliga beslutsfattare upplever att man till viss mån har handlingsplaner för att återställa system och verksamhet så snabbt som möjligt. Vi ser också att allt fler verksamheter blir bättre på att säkerställa sin leverantörskedja genom att utföra säkerhetskontroller på externa samarbetspartners. En mer negativ utveckling ser vi i antalet verksamheter som faktiskt har, och övar på en krisplan regelbundet samt har en fungerande och fullt implementerad policy kring informationssäkerhet.

### Positiv negativ utveckling

Den negativa utvecklingen kan även tolkas som ett tecken på att svenska verksamheter har blivit mer mogna i sitt säkerhetsarbete och tagit till sig av föregående kartläggningar. Genom att genomföra mer strukturerade sårbarhetsanalyser har verksamheterna utvecklat en högre intern förmåga att bedöma sina egna brister.

”Verksamheterna är numera medvetet inkompetenta” är ett uttryck som dykt upp i djupintervjuerna. De har blivit mer insiktsfulla och därmed kritiska till sin egen förmåga. Självklart hade det varit bättre med en positivt trendande utveckling, men det är även viktigt med en grundad och realistisk uppfattning om var basnivån ligger som utgångspunkt för fortsatt arbete.

Den positivt negativa utvecklingen stärker även tesen om att det finns ett gap mellan verksamheters försvarsförmåga och antagonisternas förmåga att attackera dem. När vi tror att vi har uppnått en god nivå har antagonisterna hittat nya attackmetoder. Det innebär att mognaden alltid är relativ. Även fast vi gör mer idag än vi gjorde igår flyttas målet hela tiden fram.

> ”Verksamheterna är numera medvetet inkompetenta”

Det ska även sägas att vissa kategorier, som att alltid ha den senaste och bästa tekniska it-säkerheten, är svåra att svara “Ja, fullt ut” på, vilket också kan påverka resultaten.

# Allt färre verksamheter har ett heltäckande verksamhetsskydd

Fråga: I vilken utsträckning stämmer följande in på din verksamhet?

| | 2023 | 2024 | |
|---|---|---|---|
| **Har till viss mån handlingsplaner för att återställa system/verksamhet så snabbt som möjligt** | 89% | 100% | ▲ |
| Utbildar personalen regelbundet om it-säkerhetsfrågor | 93% | 96% | ▲ |
| Utvärderar verksamhetens it-säkerhet med viss regelbundenhet | 92% | 91% | ▼ |
| Det finns till viss mån en kontinuitetsplan för att hålla verksamheten i drift efter en allvarlig störning. | 93% | 91% | ▼ |
| **Arbetar med riskhantering (har riskhaneringsplaner med beskrivning av aktiviteter och åtgärder för att upptäcka, bedöma och minimera risker i verksamheten)** | 97% | 90% | ▼ |
| Säkerställer att man alltid har den senaste och bästa tekniska it-säkerheten | 83% | 86% | ▲ |
| **I samband med rekryteringar säkerställs det att medarbetaren inte utgör en säkerhetsrisk** | 81% | 82% | ▲ |
| **Har tydliga rutiner för hur verksamheten ska återställas efter ett it-haveri** | 85% | 82% | ▼ |
| Gör en säkerhetskontroll på alla externa samarbetspartners | 63% | 82% | ▲ |
| **Har en fungerande och fullt implementerad policy kring informationssäkerhet** | 86% | 77% | ▼ |
| **Har en krisplan som övas med viss regelbundenhet** | 81% | 68% | ▼ |

Ovanstående är sammanvägda svar bestående av "ja" och "ja, till viss del".

**Definition**

För att ha ett heltäckande verksamhetsskydd har vi definierat elva kriterier som måste uppfyllas. Dessa kriterier spänner över informationssäkerhet, personalsäkerhet och fysisk säkerhet och utgår från ett kontinuerligt och systematiskt arbetssätt. Genom att uppfylla samtliga kriterier anser vi att man har ett heltäckande verksamhetsskydd. Det finns sex kriterier (av de totalt elva) som är helt avgörande. Om någon av dessa sex kriterier **inte** är uppfyllda, bedöms organisationen ha ett 'otillräckligt verksamhetsskydd'.

# Fler spår en ökad säkerhetsbudget

En majoritet av beslutsfattarna tror på större säkerhetsbudgetar det kommande året. Närmare bestämt tror 68% på en högre budget, vilket är en ökning med +10% från föregående år. Andelen som tror att budgeten kommer att vara oförändrad uppgår till 23% vilket är en minskning med -12% från förra året. De som menar att budgeten istället kommer att minska är 9% vilket innebär en ökning med +7% sedan förra mätningen.

### Delad syn på verksamheternas organisation

Den största andelen beslutsfattare upplever att organiseringen vad gäller beslut och budget för säkerhetsskydd är ganska bra (35%) eller mycket bra (12%). Runt en fjärdedel upplever sammantaget att organiseringen är ganska eller mycket dålig (24%), medan nästan en tredjedel (29%) har en neutral inställning. Värst är det inom offentlig sektor, där en fjärdedel (24%) upplever att de är dåligt organiserade när det gäller beslut kring säkerhetsskydd och ägande av budget.

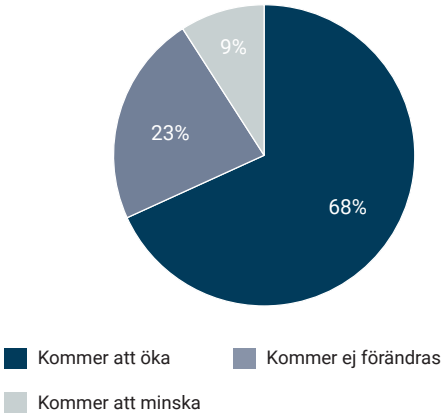
### Framgångsfaktorer

Framgångsfaktorer som lyfts för att lyckas inom detta är tydliga rapporteringsvägar med starkt ägarskap över säkerhetsbudgeten och tydlighet i roller och ansvar. Vidare betonas vikten av ledningens engagemang och att sätta tydliga mål, bedriva ett tydligt riskarbete samt genomföra omvärldsbevakning. Det uppges vara viktigt att säkerhetsarbetet är väl förankrat i ledningen där mandat finns för att fatta nödvändiga beslut.

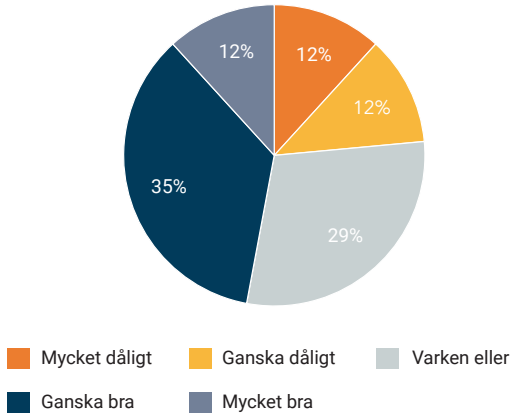
### Hindrande faktorer

Inom organisationen uppges hindrande faktorer vara otydlighet i ansvar och bristande implementering av säkerhet i styrning och mål. Även otillräcklig krisberedskap och avsaknad av samordnade övningar mellan berörda organisationer, förvaltningar och leverantörer som behöver samarbeta vid genomförandet av säkerhetsskydd utgör en betydande utmaning.

**Hur tror du att er säkerhetsbudget kommer förändras under det kommande året?**




**Hur tycker du att ni är organiserade när det gäller beslut kring säkerhetsskydd och ägande av budget?**



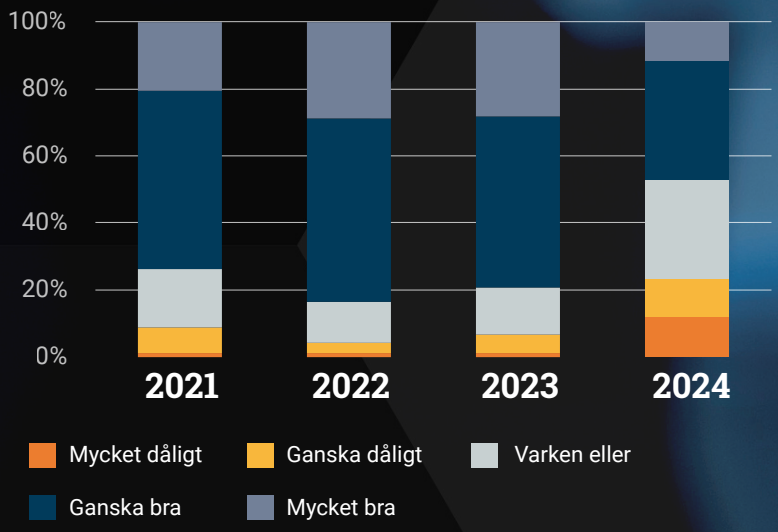
# Stor diskrepans mellan budget och beslut

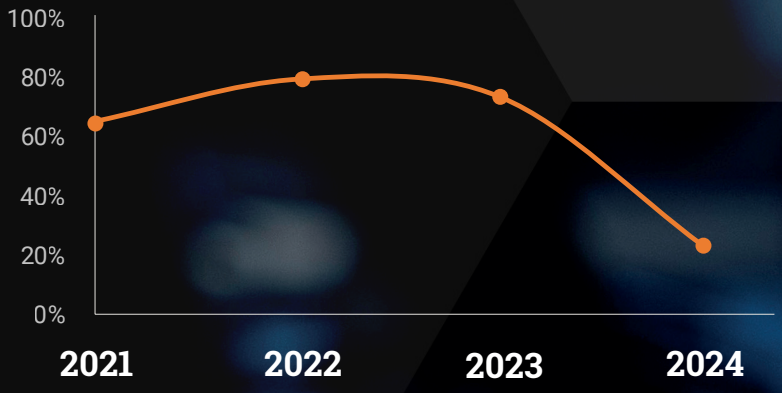
Sedan förra årets mätning har upplevelsen av organisation runt beslut och budget för säkerhetsskydd sett en betydande försämring. Från att ha legat relativt stabilt mellan 2021–2023, så visar årets resultat ett tydligt trendbrott.

Andelen som uppger att organisation kopplad till budget och beslut är mycket dålig har ökat med +10% från förra året, samtidigt som andelen som uppger mycket bra har minskat med -16%.

Beslutsfattare uppger att det finns diskrepanser och brist på samverkan vad gäller budget och beslut kring säkerhetsskydd för it, fysiskt skydd eller personalsäkerhet. Som tidigare nämnt finns just nu ett större fokus på informationssäkerhet bland samtliga roller, och säkerhetschefer som vill investera i utökat fysiskt skydd eller personalsäkerhet upplever att de får argumentera hårdare för att motivera sina investeringar inom de områdena.

**Hur tycker du att ni är organiserade när det gäller beslut kring säkerhetsskydd och ägande av budget?**




Den indexerade grafen bredvid utgår från extremvärdena där vi har tagit bort svarsalternativet ”varken eller”, enligt samma princip som ett NPS-värde. Formeln är (”Mycket bra” + ”Ganska bra”) – (”Mycket dålig + ”Ganska dåligt”).

**“Den största utmaningen just nu är att få ledningens förståelse och insikt för säkerhetsfrågor, dom är inte där ännu.”**

– Informationssäkerhetschef, Bank & finanssektor

# Det är inte bara en fråga om pengar längre

Tidigare års kartläggningar visar att man med mer resurser i form av högre budget tror sig kunna bygga och skala förmåga.

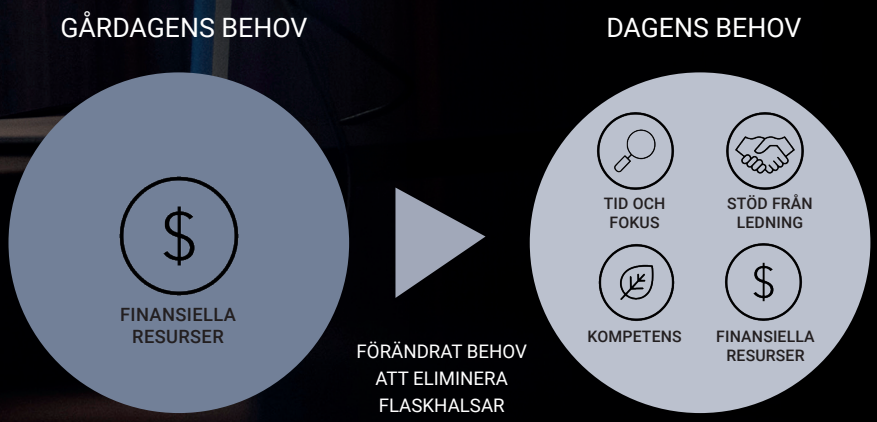
I denna års mätning anger respondenterna tydligare att de har ett bredare behov som även innefattar:

- Tid och fokus
- Stöd från ledning
- Kompetens
- Finansiella resurser (fortsatt behov)

Trenden visar att organisationer ytterligare har kartlagt sitt behov men även befintlig förmåga. Att skala upp sin förmåga är komplext och kräver breda insatser. Mer och fler resurser behövs.

Det förändrade behovet återspeglar även en ökad mognad. För att få ut tänkt värde och effekt av genomförda investeringar så behöver det finnas vissa organisatoriska förutsättningar på plats.

## Skattad prioritering av behov för att bygga förmåga i organisation




**TID OCH FOKUS**

Behov av tid att kunna fokusera, samverka, bygga förmåga och utbilda.

**STÖD FRÅN LEDNINGEN**

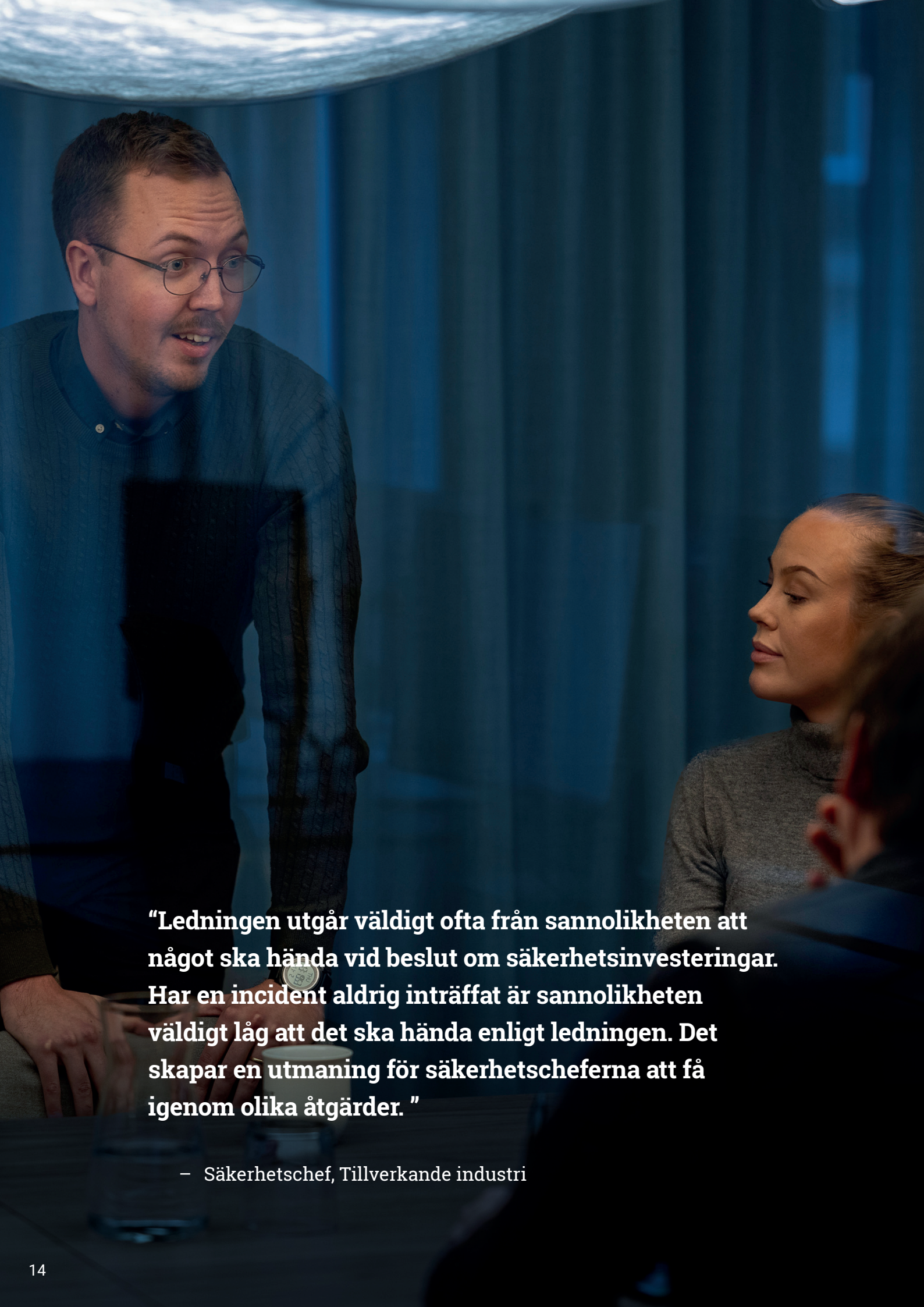
Stöd från ledning för att etablera ny kultur, skapa prioritering och insikt av betydelse.

**KOMPETENS**

Att bygga ny och skala befintlig kompetens är A och O för att nå nödvändig förmåga.

**FINANSIELLA RESURSER**

Viktigt men inte viktigast och mest prioriterad just nu. Ledning har insikt om kostnads- och investeringsbehov.



**“Ledningen utgår väldigt ofta från sannolikheten att något ska hända vid beslut om säkerhetsinvesteringar. Har en incident aldrig inträffat är sannolikheten väldigt låg att det ska hända enligt ledningen. Det skapar en utmaning för säkerhetscheferna att få igenom olika åtgärder. ”**

– Säkerhetschef, Tillverkande industri

# Det regulatoriska landskapet och digitalisering av säkerhetsskyddsklassificerade system

Digitalisering har förändrat hur organisationer hanterar information och säkerhet, särskilt inom områden med höga krav på skydd av känsliga data. I Sverige regleras säkerhetsskyddsklassificerade system av ett strikt regelverk som skyddar nationella intressen och förhindrar att känslig information hamnar i orätta händer. Regelverket bygger på både nationell lagstiftning och internationella överenskommelser.

**Regulatoriskt ramverk**
Säkerhetsskyddslagen (2018:585) och dess förordning (2018:658) utgör grunden för hanteringen av säkerhetsskyddsklassificerad information i Sverige. Dessa regler ställer krav på analyser, avtal och tillsyn för att förebygga hot som spioneri och sabotage. EU-direktivet NIS2 (cybersäkerhetslagen i Sverige) påverkar också hur kritisk infrastruktur och digitala tjänster skyddas.

**Bedömning av hot**
En nyckelfaktor i hanteringen av säkerhetsskyddsklassificerade system är hotbedömning. Det innebär att identifiera hotaktörer, deras förmågor och möjliga konsekvenser. Hoten kan inkludera statliga aktörer, cyberkriminella nätverk och insiders med illvilliga avsikter.

Bedömning av hot omfattar också analys av sårbarheter i it-system, mänskliga faktorer och externa beroenden. Effektiva metoder inkluderar:

- **Sårbarhetsanalyser:** Identifiera och åtgärda risker i system och processer.
- **Omvärldsbevakning:** Håll dig uppdaterad om nya hotmetoder.
- **Konsekvensbedömningar:** Prioritera åtgärder utifrån allvarlighetsgrad.

**Fokus på informationssäkerhet**
Årets kartläggning ger en tydlig fingervisning om beslutsfattarnas bedömning av olika säkerhetsskyddsåtgärder. Alla sektorer pekar konsekvent på att informationssäkerhet är det mest allvarliga hotet. Detta belyser en generell medvetenhet om cybersäkerhetsrisker. Undersökningen visar att personal- och fysisk säkerhet inte tas på lika stort allvar som informationssäkerhet, mycket på grund av att man som verksamhet känner ett lugn med att man har jobbat med dessa frågor under en längre tid och har processer på plats.

**Civilt försvar kräver fokus på samtliga områden**
Det faktum att personal- och fysisk säkerhet inte ges samma fokus som informationssäkerhet riskerar att leda till sårbarheter på sikt. Antagonister letar konstant efter vägar in och avancerade hybridhot där olika attackmetoder tillämpas och kombineras är just nu ökande. Det är förväntat att nya regulatoriska krav såsom lagen om motståndskraft hos kritiska verksamhetsutövare (CER-direktivet) kommer att driva ett utökat fokus på personal- och fysisk säkerhet de kommande åren.

**Utmaningar vid digitalisering**
Digitalisering av säkerhetsskyddsklassificerade system innebär flera utmaningar. En av de största är att balansera effektivitet och innovation med behovet av strikt säkerhet. För att uppnå detta måste organisationer säkerställa att de digitala lösningarna uppfyller både funktionella krav och säkerhetskrav. En annan utmaning är att hantera det ökande hotet från cyberangrepp, där aktörer blir alltmer sofistikerade och utnyttjar sårbarheter i komplexa system.

Vidare innebär digitalisering ofta att organisationer blir beroende av tjänster och externa leverantörer. Detta kräver noggranna bedömningar av leverantörens säkerhetsåtgärder och juridiska överenskommelser som säkerställer att svensk lagstiftning följs, även om data hanteras utanför landets gränser.

**Möjligheter och framtidsutsikter**
Trots utmaningarna erbjuder digitalisering betydande fördelar. Automatisering av säkerhetsprocesser kan minska mänskliga fel och förbättra incidenthantering. Artificiell intelligens och maskininlärning används alltmer för att upptäcka och motverka hot i realtid. Dessutom möjliggör digitala verktyg effektivare samordning mellan myndigheter och företag, vilket stärker det nationella säkerhetsskyddet.

Framtiden för digitalisering av säkerhetsskyddsklassificerade system ligger i att skapa flexibla och robusta lösningar som snabbt kan anpassas till förändrade hotbilder och nya tekniska möjligheter. Detta kräver kontinuerlig utbildning av personal, investeringar i forskning och utveckling, samt ett nära samarbete mellan offentlig och privat sektor.

Sammanfattningsvis är det regulatoriska landskapet kring säkerhetsskyddsklassificerade system utformat för att möta de höga krav som digitalisering medför. Genom att kombinera strikt efterlevnad av lagstiftningen med innovativa teknologier och en noggrann hotbedömning kan organisationer både skydda känslig information och dra nytta av digitaliseringens potential.

Mikael Nordelind

*Säkerhets- och säkerhetsskyddschef, Omegapoint*

# Ett ökande gap mellan upplevd hotbild och förmåga

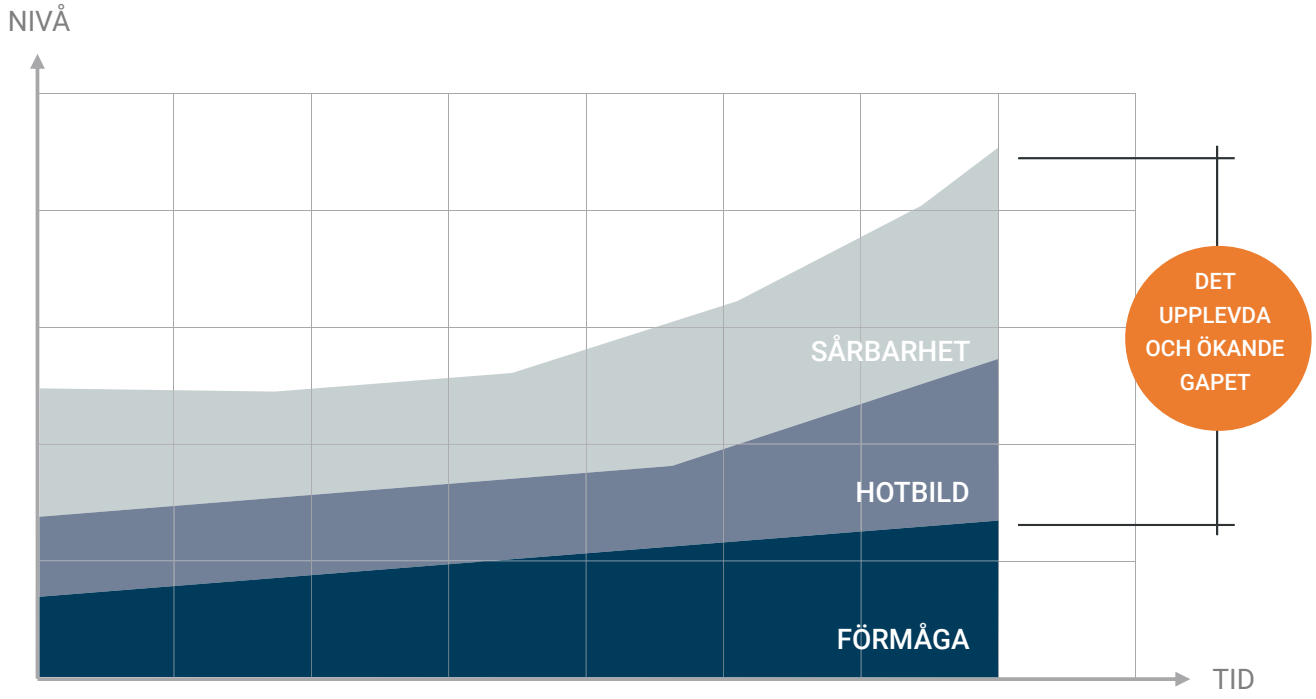
Det ligger en paradox i att Sveriges totalförsvarsförmåga ökar samtidigt som hotbilden mot Sverige ökar ännu mer.

Respondenterna i undersökningen anger att de upplever ett ökat gap mellan sårbarhet och hot å ena sidan och verksamhetens förmåga att bygga säkerhetsförmåga och motståndskraft å andra sidan.

Även om Sverige investerar och bygger upp sin totalförsvarsförmåga anpassar hotaktörerna sitt beteende och intensitet. Sårbarheten ökar – pådrivet av utvecklingen inom ny teknik, leveranskedjor, nya beteendemönster och ökade krav.

Det är därför av yttersta vikt för det fortsatta arbetet att göra rätt prioriteringar och att fokus på förmågeutveckling är stark och tydlig.

## Hur upplever du utveckling mellan sårbarhet, hotbild och utvecklingen av egen förmåga?



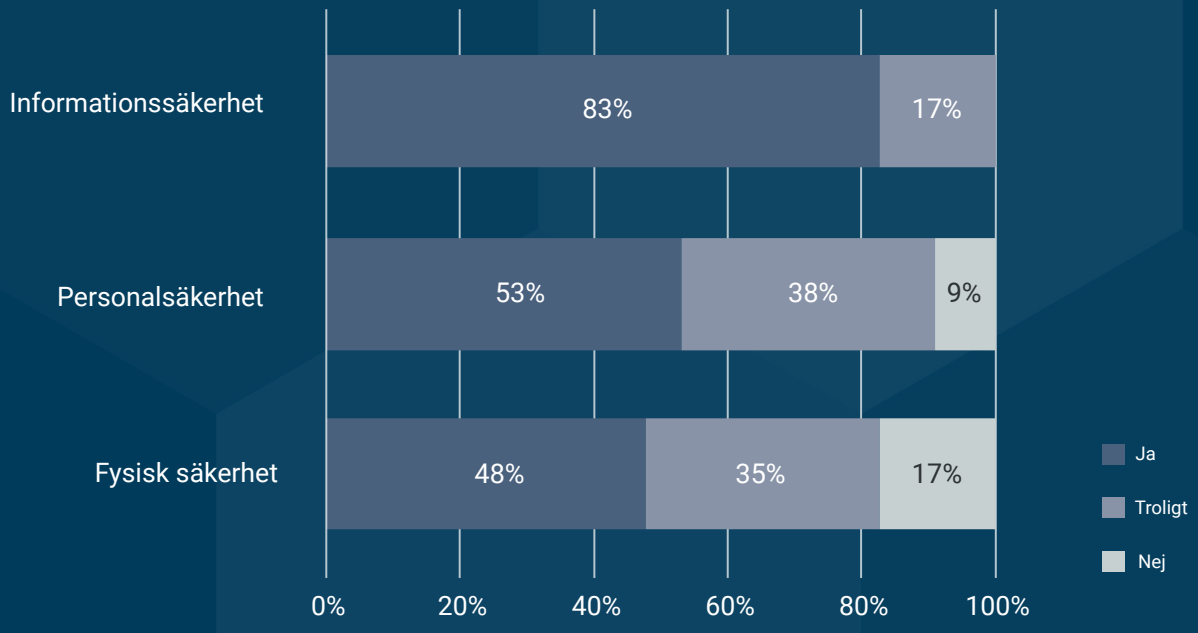
# Störst behov av åtgärder för att hantera informationssäkerhet

Det råder en bred samstämmighet om att det skyddsvärda oftast är digitalt och kopplat till informationshantering (informationssäkerhet). Det är även inom detta område som hoten utvecklats mest. Med en ökad digitalisering, som på senare tid i allt större utsträckning drivs på av linjeorganisationen och där it-avdelningen allt mer hamnar i en stöttande position trots sin kompetens blir konsekvensen att säkerhet och robusthet kan komma i kläm.

I denna undersökning ser vi en tydlig samsyn om att insatser på bred front behövs för att förstärka informationssäkerheten. Samtliga respondenter anger att det behövs eller troligen behövs ytterligare åtgärder in i verksamheter (offentliga + privata) för att säkra de skyddsvärda informationstillgångarna.

I djupintervjuerna framkommer ett mönster om att respondenterna förutser att personalsäkerhet troligtvis behöver stärkas ytterligare för att möta framtidens hot mot informationssäkerheten. Exempelvis infiltration och korruption via personal bedöms vara ökande hot framöver. Det finns även ett behov av att stärka personalsäkerheten från andra typer av hot, såsom misstag genom social manipulation (social engineering) som blir allt mer komplext och sofistikerat med utvecklingen av ny teknik.

## Verksamheter anger att de har behov av att vidta åtgärder mot hot kopplat till följande



# Svenska befolkningen mer positiva till Nato

Den svenska befolkning har, givet förändringen av det geopolitiska läget under året, en mer positiv inställning idag till Nato än vid själva inträdet under våren 2024.

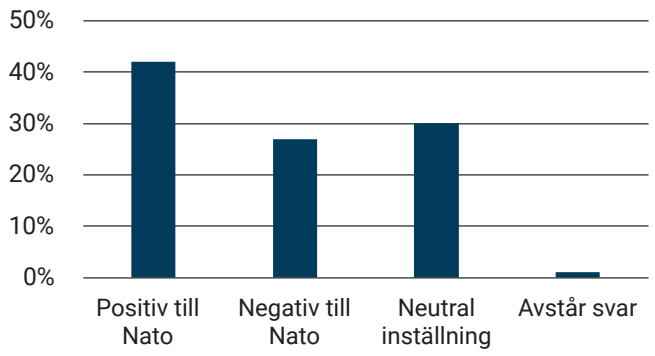
Innan det svenska Nato-inträdet var 42% av respondenterna positiva till ett svenskt Nato-medlemskap och endast 27% emot.

Efter 8 månader har samma respondenter kollektivt blivit mer positiva till Nato. De som inte har ändrat uppfattning alls, blivit mer eller mycket mer positiva till Nato utgörs av 86% av respondenterna.

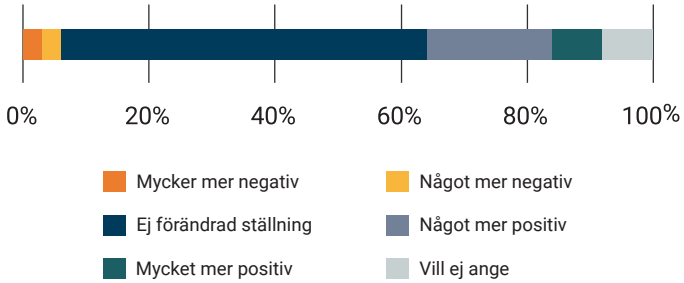
Delförklaringar till denna positiva förändring kan vara (berörs ej i enkätunderlaget):

- Rysslands fortsatta anfallskrig mot Ukraina
- Pågående påverkansoperationer och hybridkrigsföring mot Sverige
- Den ökade mediala bevakningen av hotbilden emot Sverige
- Att Sveriges inrangeringsprocess i Nato går planenligt
- Det uppfattas positivt att se Sverige delta och samöva inom ramen för Nato
- Det svenska narrativet om att bygga upp totalförsvaret växer

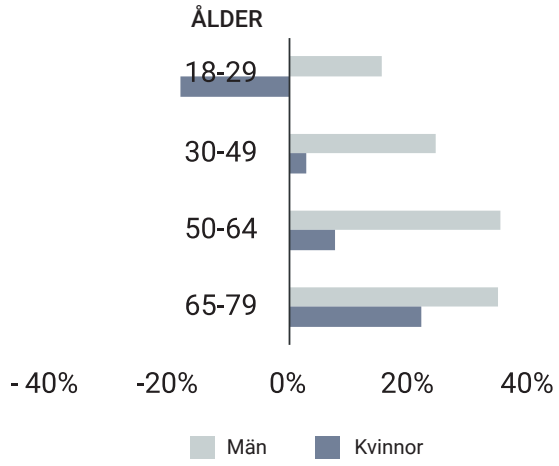
### Inställning till Nato innan inträde




### Förändrad inställning till Nato efter inträde




INDEXERAT MÄN & KVINNOR




Inställningen till Nato har en tydlig korrelation till ålder och kön. Män i alla åldrar var mer positiva än negativa till Nato före inträdet. Minst positiva män återfanns i de yngre åldrarna (18-29 år).

I den kvinnliga målgruppen fanns en större betydligt spridning. Den yngre målgruppen (18-29 år) var mest negativa eller tveksamma till ett Nato-medlemskap medans de två äldre åldersgrupperna (50-64 år och 65-79 år) hade en positiv inställning till Nato före inträdet.

# För verksamheterna återstår ett gediget integrationsarbete

Svenska organisationer har uppfattningen att det är ett omfattande arbete att integrera Sverige in i ett fullvärdigt medlemskap i Nato. På en direktfråga är uppfattningen att det kommer ta minst 5 år för Sverige att nå en acceptabel nivå av integration in i Nato.

De upplevda anledningarna till att det kommer ta tid är bland annat:

1. **Sveriges historik som fristående och neutral nation medför att mycket skall byggas upp från noll**
2. **Många formella befattningar att tillsätta**
3. **Anpassning av svensk standard och praxis**
4. **Uppbyggnad och anpassning av den svenska civila delen som ingår i Nato**
5. **Skapa förståelse och insikt om hur Nato nyttjar både statlig och privat verksamhet**
6. **Skapa förståelse och insikt för svenska verksamheter runt hur Nato genomför upphandlingar**
7. **Anpassa sig och ta del av Natos (positiva) syn till att nyttja innovation och ny teknik vilket är en stark svensk förmåga**

## Samlad och skattad tids-uppfattning för Sveriges integration in i Nato

**“Vi litar väldigt mycket på människor och vill inte tro ont om dem. Här är vi sårbara, vilket nog tyvärr kommer vara något som utnyttjas mer framöver. Kommer man inte åt information med digitala medel kommer man börja jobba mer mot individer.”**

– Generalsekreterare,
Statlig branschorganisation

# Nato innebär både möjligheter och utmaningar för vår civila beredskap

Att Sveriges medlemskap i Nato innebär en grundläggande förändring för Försvarsmakten råder det ingen tvekan om. Vad som däremot inte är fullt lika diskuterat eller bevakat är vad medlemskapet innebär för det svenska samhället i övrigt. Årets rapport påvisar ett kompakt stöd för Sveriges medlemskap, t.o.m. en viss ökning under våra första åtta månader som medlem. Rysslands krigföring i Ukraina och Nordkoreas inträde i kriget spelar så klart en stor roll. Putinregimens allt mer aggressiva och risktagande hybridaktiviteter i Sverige och i våra grannländer, förstärker troligtvis upplevelsen av en närvarande och aktiv rysk hotbild.

Ett Natomedlemskap har en avsevärt djupare räckvidd in i det svenska samhället utöver det militära försvaret. Det ger oss nya förutsättningar för att utveckla det svenska civila försvaret och därmed totalförsvaret. Med Nato kommer krav på det civila samhällets förmåga att skydda civilbefolkning, stärka försvarsvilja och att stödja det egna och andra länders försvarsmakter. Dessa krav är likställiga med kraven på vår militära förmåga. Den Resilienskommitté som förvaltar Natos sju grundläggande riktlinjer för civil förmåga, är hieratiskt jämbördig med Natos militärkommitté.

Det är en rad nya Natoregelverk som beskriver hur Sverige förväntas arbeta med det civila försvaret som våra länsstyrelser, tillsammans med sektorsansvariga myndigheter, lusläser och tolkar just nu. Allt kommer däremot inte att vara nytt. Samtliga Natos sju förmågeområden har sina motsvarigheter i Sveriges tio beredskapssektorer. Sverige har även som medlem i Natos Partnerskap för fred (PFP) sedan början av 1990-talet varit engagerad i Natos strukturer för civilförsvar.

Men med Natomedlemskapet kommer även en helt annan kultur och förväntan när det gäller offentlig och privat samverkan än vad vi kanske är vana vid i Sverige. Det här kommer förhoppningsvis innebära en knuff i ryggen och nya möjligheter för effektiv och innovativ samverkan mellan statlig, offentlig och privat verksamhet inom ramen för svensk civil beredskap. Den upplevda hotbild som skapas genom media och fikarumssamtal kommer däremot att behöva balanseras med välgrundade hotbildsbedömningar från myndigheter och kunskapsbärande organisationer. Detta kommer att utgöra en framgångsfaktor för den samverkan som mycket av vår civila beredskap ska vila på.

Ett annat spännande område är innovation och forskning som inom Nato utgör ett prioriterat fokusområde. Här är Sverige en strategisk aktör med vår försvarsindustri och vår forskning. Faktum är att arbetet med Natos nya forskningsstrategi kommer att ledas av FOIs generaldirektör, Jens Mattsson. Det borde ses som ett erkännande av svensk förmåga inom området. Men även här har vi en resa att göra när det gäller arbetet med att skydda svensk forskning och innovation mot totalitära stater och deras ambitioner att nyttja svenska och europeiska forskningsframsteg för egna syften.

Det ska sammanfattningsvis bli mycket intressant att se hur nästa års Svenskt Säkerhetsindex kommer att se ut kring temat Nato. Inte minst när det gäller upplevelsen av hur svensk implementering av Natos regelverk går och integreringen i Natos lednings- och samverkansstrukturer.

**Thom Thavenius**

*Säkerhetsskyddsspecialist och f.d. senior analytiker vid Säkerhetspolisen*

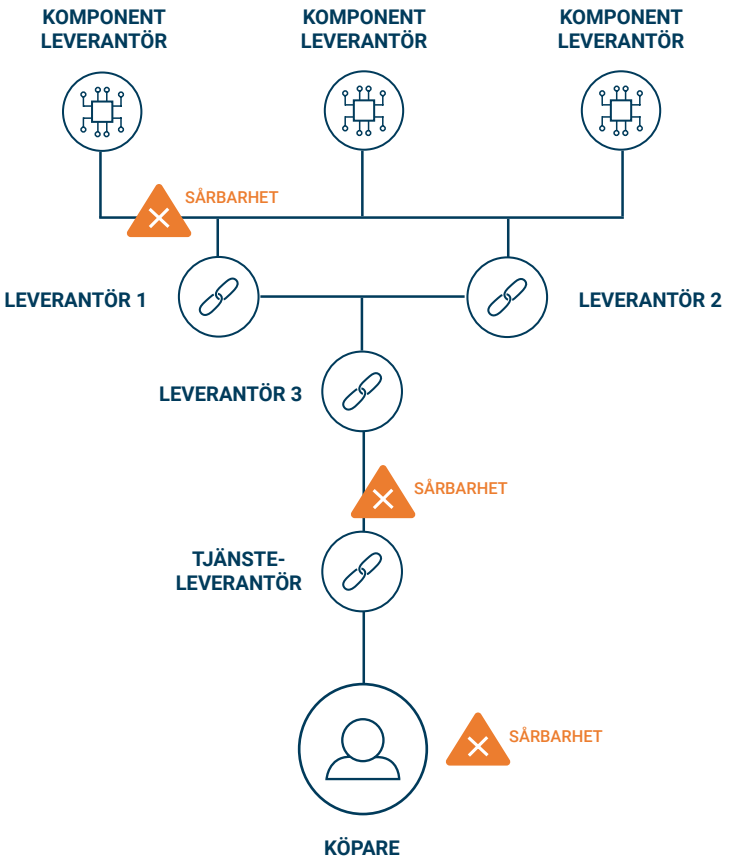
# Leveranskedjan – en exponentiellt ökande risk

I takt med att verksamheter blir mer uppkopplade och sammankopplade ökar beroenden och risk. De nya regulatoriska kraven ställer högre krav på verksamheter att ta ansvar för sina egna leveranskedjor.

En allt större del av de skyddsvärda tillgångarna är dessutom digitala, vilket följaktligen medför att de antagonistiska aktörerna blir alltmer digitala. En ökad grad av industrialisering inom it och en historisk outsourcingtrend har medfört att verksamheter minskat sin egenproduktion av bland annat it för att uppnå skalfördelar och större effektivitet. Konsekvensen blir en högre grad av specialisering, där olika aktörer i ekosystemet fokuserar på vad man gör bäst i sin del av kedjan och så skapar man beroenden till andra aktörer för att tillgodose resten. I takt med att antalet leverantörerna växer, beroenden blir fler och digitala sårbarheter fördjupas så ökar risken för angrepp mot leveranskedjor exponentiellt.

I ett nära sammankopplat och komplext ekosystem är det problematiskt när det finns svaga länkar. Små och medelstora verksamheter är alltid en del av värdefulla leveranskedjor, och som grupp är mindre bolag ofta sämre rustade att möta komplexa cyberhot. Mindre verksamheter möter samma hotbild men har helt andra förutsättningar för att hantera den. De har ofta begränsade budgetar och resurser för att arbeta med säkerhet. Resursstarka och motiverade antagonister som vill åsamka stor skada har insett potentialen i att attackera leveranskedjor och detta gör att mindre aktörer möter en oproportionerlig risk – de måste bygga ett försvar mot aktörer som kanske inte har ett intresse för dem själva givet sin storlek, men där de kan utnyttjas för att komma åt fler aktörer längre bort i kedjan.

**Sårbarheter i leveranskedjan kan uppstå i flera olika led.**



# Ökat tryck skapar konsekvens för relationen

En ökad insikt om tredjepartsrisker kombinerat med ett högre tryck på att säkra leveranskedjan från nya regulatoriska regelverk, ger frågan ett högt fokus.

Resiliens i digitala produkter och tjänster, samt säkerhetsbedömningar av leverantörer och dess processer dyker i högre grad upp som en del av kravställningar. En dryg fjärdedel (24%) uppger att man kommer att utvärdera och konsolidera sitt leverantörslandskap som ett sätt att hantera sin risk. Det här ställer krav på helt nya sätt att arbeta tillsammans med sitt leverantörsled. Vi ser en stor andel verksamheter som lägger sitt huvudsakliga fokus på kontrakt, avtal och inköpsprocesser. Närmare och mer strategiska relationer kommer att premieras.

### Ökat behov av att kunna ta sig ur avtal

En aktuell diskussion kopplat till leveranskedjan är koncentrationsrisk och inlåsningseffekter. Båda är exempel på något att undvika och något som allt fler verksamheter tar i beaktande i sin riskhantering.

Att inkludera mekanismer för avslut av avtal blir allt vanligare, och märks särskilt i offentliga upphandlingar kring digitala tjänster som levereras utanför Sveriges gränser. Instabila geopolitiska och regulatoriska förutsättningar skapar behov för ökad agilitet och flexibilitet hos verksamheter.

## Verksamhetens hantering av tredjepartsrisk

*(Källa: Radar Svensk cybersäkerhet 2024)*

# Små och medelstora bolag utmanas och utmanar

Kartläggningen visar att små och medelstora bolag (SME) lyfts fram som en utmanande faktor i leveranskedjan. Mindre verksamheter klarar inte av att arbeta i samma tempo, den generella säkerhetsmognaden är lägre och man träffas inte av regulatoriska ramverk på samma sätt som i många större verksamheters säkerhetsarbete. Detta har skapat ett gap i verksamheternas förmåga som fortsätter att öka. SME är samtidigt en del i olika leveranskedjor, så de blir därmed en sårbarhet för hela ekosystemet.

Mindre verksamheter saknar dessutom i högre grad en policy för leverantörshantering. Man är även mer benägen att förlita sig på certifieringar som ett led i att säkra sin leveranskedja som ett sätt att kompensera för brist på kompetens och resurser.

Eftersom mindre verksamheter alltid är en del av värdefulla leveranskedjor, betraktas de som en risk och sårbarhet av beslutsfattare i olika samhällsviktiga verksamheter.

**Andel verksamheter som förlitar sig på certifieringar för att hantera sin tredjepartsrisk**

*(Källa: Radar Svensk cybersäkerhet 2024)*




Små & medelstora företag




Större företag

**Andel verksamheter där leverantörshanterings-policy saknas, eller saknas men är under införande**

*(Källa: Radar Svensk cybersäkerhet 2024)*


Små & medelstora företag

Större företag

# Samverkan stärker totalförsvarsförmågan

Strax över en tredjedel (36%) av beslutsfattarna uppger att man i hög grad samverkar med myndigheter eller andra aktörer (såsom länsstyrelser, beredskapsmyndigheter, kommuner) för att skydda sin verksamhet. Hälften av de svarande menar att samverkan sker till viss del, medan en knapp tiondel uppger att samverkan inte sker alls.

Trots att en dryg tredjedel av beslutsfattarna (vänstra diagrammet) upplever en hög grad av samverkan, betonar man särskilt vikten av samverkan mellan statliga aktörer. Det ses som kritiskt för samhällets försvarsförmåga.

### Samverkan fokus i nya regelverk

Tidigare analyser påvisar ett tydligt samband mellan grad av samverkan och nivå av säkerhetsskydd, där en högre grad av samverkan korrelerar med ett heltäckande verksamhetsskydd. Samverkan blir också allt mer kritiskt för att hantera ens externa beroenden och som är en av de största säkerhetsutmaningarna kommande år.

### Offentlig verksamhet är snäppet bättre

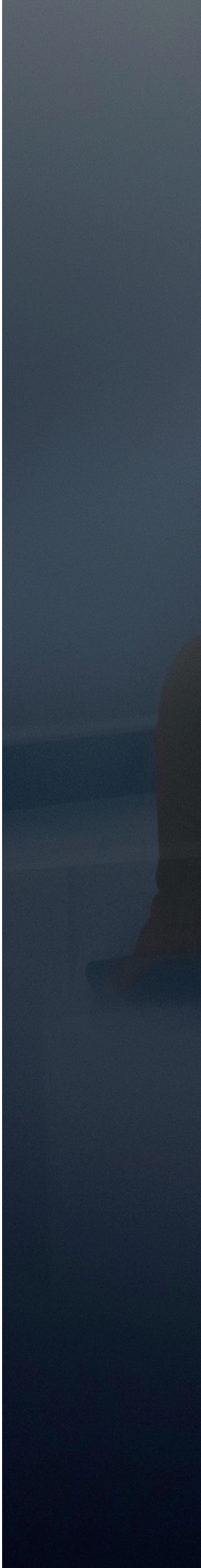
I tabellen till höger ser vi att offentliga verksamheter i högre utsträckning samarbetar med andra myndigheter eller aktörer för att stärka sin säkerhet. Detta kan förklaras av existerande samverkansforum där gemensamma frågeställningar lyfts och arbetas med. Trots detta efterfrågar offentliga verksamheter en tydlig plattform för samverkan som innefattar:

- Resurspool
- Kunskapsdelning
- Samplanering

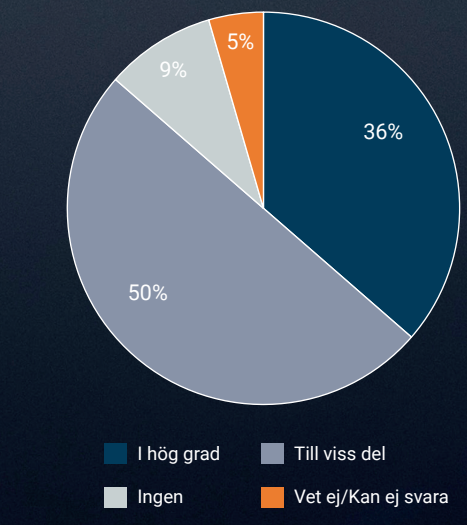
På så sätt kan verksamheter med tuffare förutsättningar stärka sin förmåga på ett mer resurseffektivt sätt.

### Behov av samverkan mellan privat och offentlig sektor

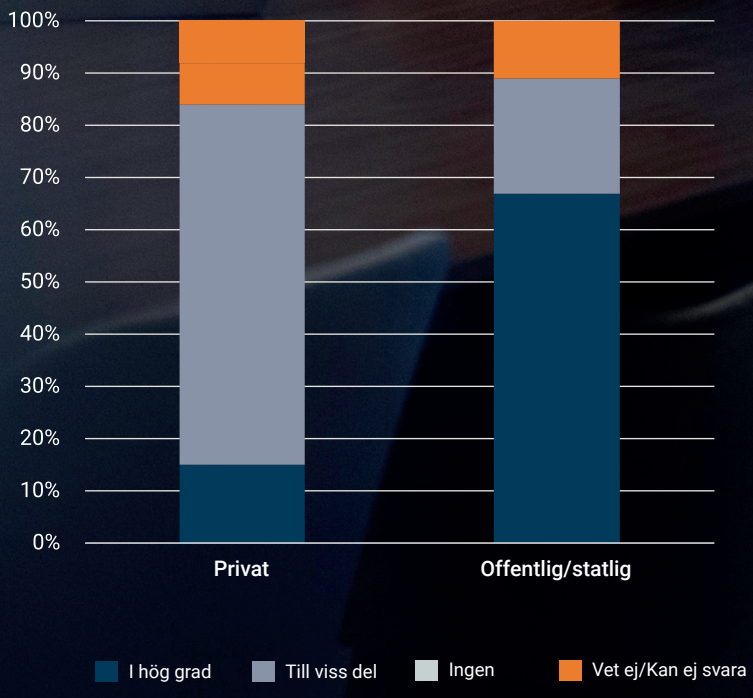
En gemensam insikt är att det finns ett stort behov av att öka graden av samverkan mellan det privata och offentliga för att stärka totalförsvarsförmågan. Ökad samverkan ses som ett sätt att hantera en brist på resurser och gynnar därmed särskilt mindre organisationer.



## I vilken utsträckning samverkar ni med myndigheter eller andra aktörer?




## I vilken utsträckning samverkar ni med myndigheter eller andra aktörer?



**“Jag ser ett behov av större samverkan mellan olika aktörer – framförallt mellan statlig och offentlig sektor. Vi måste stärka möjligheten till samverkan och samplanering istället för att alla ska uppfinna själva på sin egen kammare. Det är inte det bästa för Sveriges säkerhet.”**

– It-chef, Myndighet

# Samverkan minskar risker i leveranskedjans beredskap

Resursstarka och motiverade antagonister som vill åsamka stor skada, har insett potentialen i att attackera svaga punkter i sammankopplade och komplexa leveranskedjor. Mindre aktörer fungerar ofta som ingångspunkter i större system och kan utnyttjas för att komma åt större organisationer längre bort i kedjan. Samma hotbild som drabbar stora aktörer överförs därför till mindre verksamheter med begränsade resurser att investera i nödvändiga säkerhetsåtgärder.

En resursstark antagonist kan använda olika attackvektorer för att nå sitt mål. Phishing-attacker eller att utnyttja sårbarheter i mjukvara eller system som inte är uppdaterade på grund av begränsade resurser hos mindre företag är vardagsmat.

En angripare kan också använda sig av attacker, där de placerar skadlig kod i produkter eller system som senare distribueras till större aktörer. Ett annat exempel är social engineering, där angriparna manipulerar människor att omedvetet hjälpa till i attacken. Angrepp som ovan kan vara särskilt effektiva mot mindre aktörer som kanske inte har rätt utbildning av personalen eller tillräckliga rutiner för att upptäcka hot.

**Stora aktörer kan hjälpa mindre leverantörer**

Förutom de tekniska riskerna står företag inför betydande compliance-risker kopplade till de regelverk som styr leveranskedjor och cybersäkerhet. Regelverk som DORA och NIS2 inom EU ställer höga krav på hur data hanteras och skyddas. Om små och medelstora verksamheter inte uppfyller dessa krav riskerar de inte bara ekonomiska sanktioner, utan också att förlora affärsrelationer med större aktörer som kräver efterlevnad av regelverken.

På kort sikt kan större aktörer bidra genom att dela med sig av kunskap och resurser, exempelvis genom att dela med sig av hotinformation och varningar till sina leverantörer. De kan t ex ta fram gemensamma planer för incidenthantering som inkluderar alla aktörer i leveranskedjan och genomföra övningar för att simulera cyberattacker och identifiera svagheter i samarbetet. Initiativ från EU och svenska myndigheter kan också spela roll genom att ge ekonomiska incitament för mindre företag att investera i säkerhet.

**Cybersäkerhet är ett gemensamt ansvar**

Ett ekosystem är bara så starkt som sin svagaste länk. En framgångsrik attack mot mindre företag kan leda till förtroendeförluster, ekonomiska skador och till och med samhällsstörningar. Genom att investera i ett helhetsperspektiv och betrakta cybersäkerhet som en kritisk del av leveranskedjan kan vi säkerställa inte bara enskilda verksamheters överlevnad utan också hela ekosystemets stabilitet. Genom att skapa samarbeten och förbättra informationsdelning kan vi bygga ett mer robust försvar som skyddar alla aktörer – stora som små.

**Jonas Rehn**

*Senior advisor, Omegapoint*

# Allmänhetens oro både ökar och minskar

Allmänhetens upplevda hotbild mot samhället är hög. Under årets mätning anger hela 76% av de tillfrågade att den externa hotbilden är allvarlig eller mycket allvarlig*. Resultatet är i paritet med beslutsfattare i verksamheter där motsvarande siffra är 79%.

Resultatet underbygger en fyraårig trend om att fler och fler anser att hotbilden är allvarlig eller mycket allvarlig.

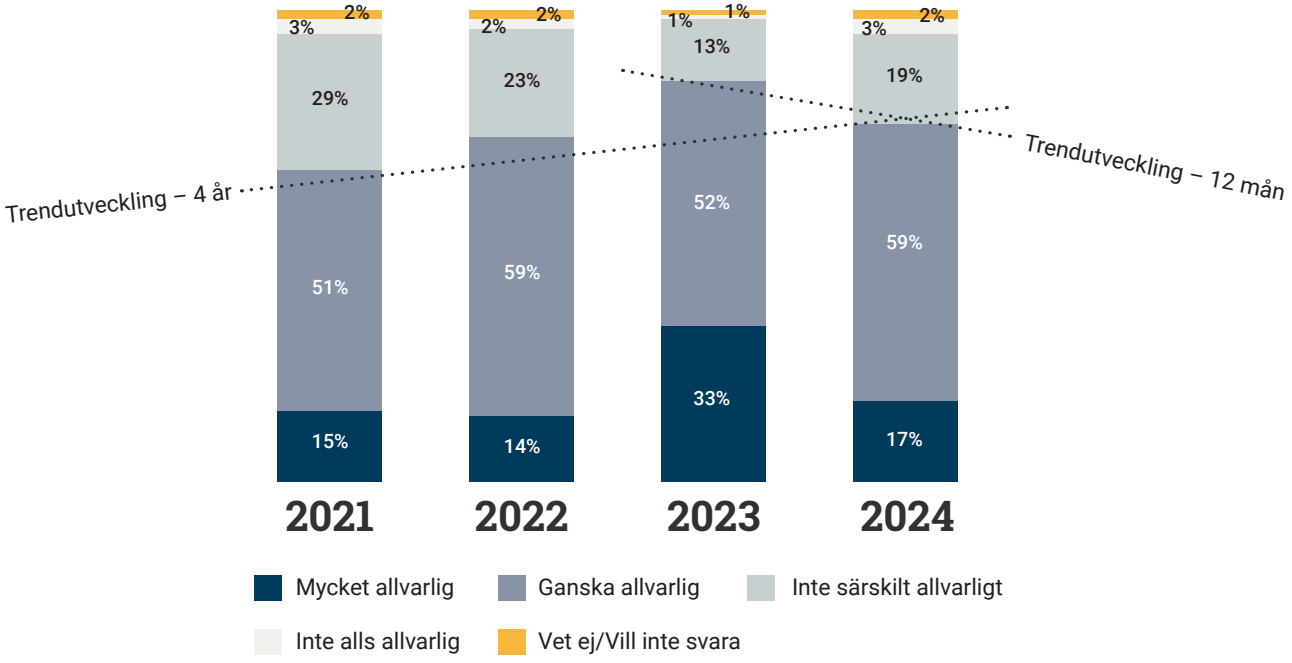
Dock är det ett trendbrott om man bara tittar på de senaste 12 månaderna, där det har skett en minskning sedan förra året med hela nio procentenheter i gruppen som inte tycker att hotbilden är allvarlig eller mycket allvarlig.

Beslutsfattare i organisationer instämmer inte i den minskande förtroendetrenden hos allmänheten utan ser istället en ökning med tolv procentenheter jämfört med förra årets mätning.

Den troliga analysen är att det under 2023 (förra årets kartläggning) var en toppnotering hos allmänheten kopplat till upplevd hotbild. Denna topp kan sannolikt kopplas till geopolitiska händelser som rönt stor uppmärksamhet. Den mest stabila insikten som kan dras ut ur data på denna bild är att det finns en fyraårig trend om en ökad upplevd hotbild.

* Sammantaget: mycket allvarlig + ganska allvarlig
Källa: Kantar
Bas: Allmänheten (1002)

## Hur upplever du den externa hotbilden mot samhället idag?



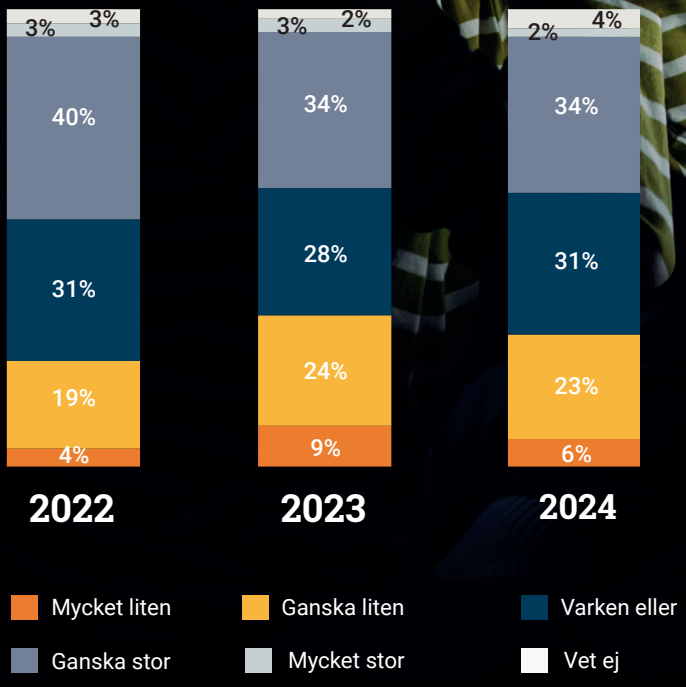
# Allmänheten får lägre förtroende för beslutsfattarna

Den andel av allmänheten som som har mycket liten eller ganska liten tilltro till att beslutsfattare kan skydda viktigt infrastruktur växer över tid med en 'negativ' trend (andelen ökar) om man tittar ur ett tre års perspektiv (2022 – 2024).

Här finns en nödvändig förbättringspotential. Det är avgörande för rikets totalförsvarsförmåga att allmänheten har tilltro till Sveriges förmåga att skydda och snabbt återställa viktig infrastruktur.

Det är även intressant att allmänhetens tilltro till beslutsfattare följer en likartad trendutveckling som bedömningen av deras upplevda hotbild.

## Vilken tilltro har du till beslutsfattarnas förmåga att skydda viktig infrastruktur?



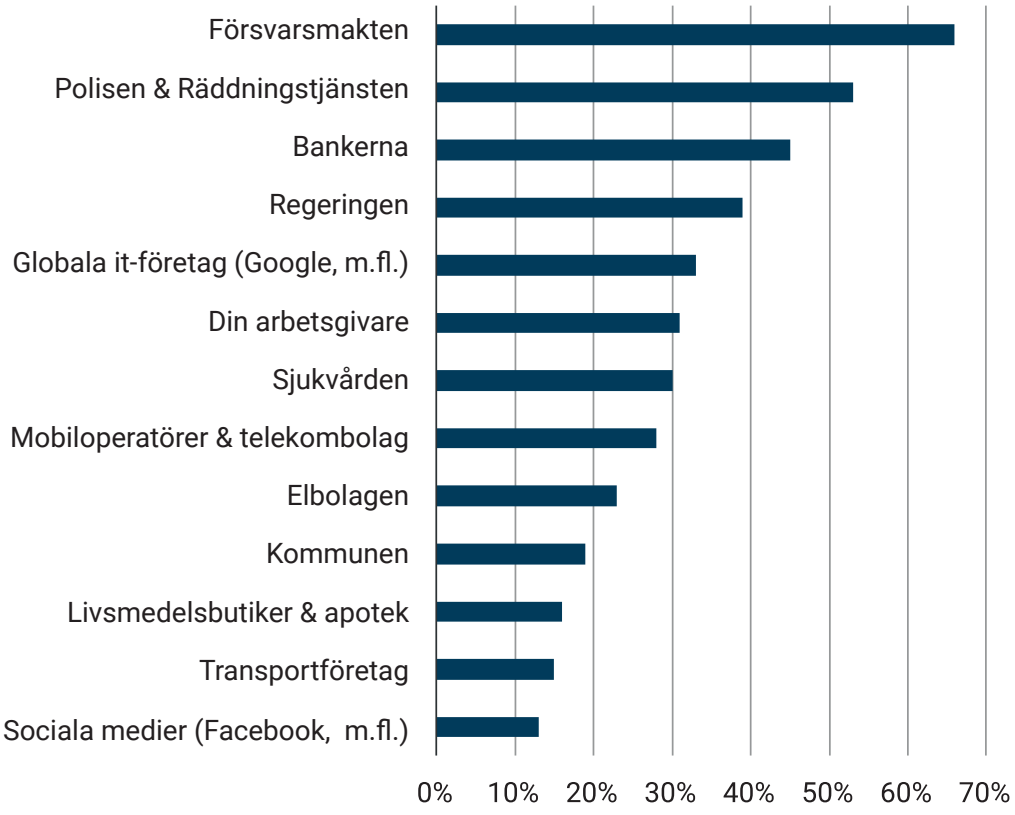
# Förtroendet för kommuner på samma nivå som sociala medier

Beslutsfattarna beskriver i kartläggningen att hotbilden mot både samhället och verksamheterna är mest utmanande kopplat till informationssäkerheten.

När vi ber allmänheten rangordna de beslutsfattare som upplevs ha bäst förmåga till informationssäkerhet (skydda sig emot it-haveri och/eller cyberattacker) hamnar försvaret och blåljusverksamhet högst upp.

I andra änden av skalan hittar vi kommuner tillsammans med bland annat sociala medier och elbolag. Det faktum att samhällsviktiga verksamheter placeras i samma fack som sociala medier förstärker bilden av att allmänhetens tilltro till vissa myndigheter och liknande aktörer med viktig infrastruktur är låg. Globala it-företag hamnar i mitten av skalan.

## Upplevd tilltro till att beslutsfattare gör vad de kan för att skydda sig mot it-haveri eller cyberattacker



# Trots minskad tilltro lägger allmänheten sin trygghet i myndigheternas händer

Det sker ingen större förflyttning hos allmänheten mellan förra årets mätning (Svenskt Säkerhetsindex 2024) och årets mätning (Svenskt Säkerhetsindex 2025) när det kommer till att ta eget ansvar och förbereda sig inför en potentiell kris.

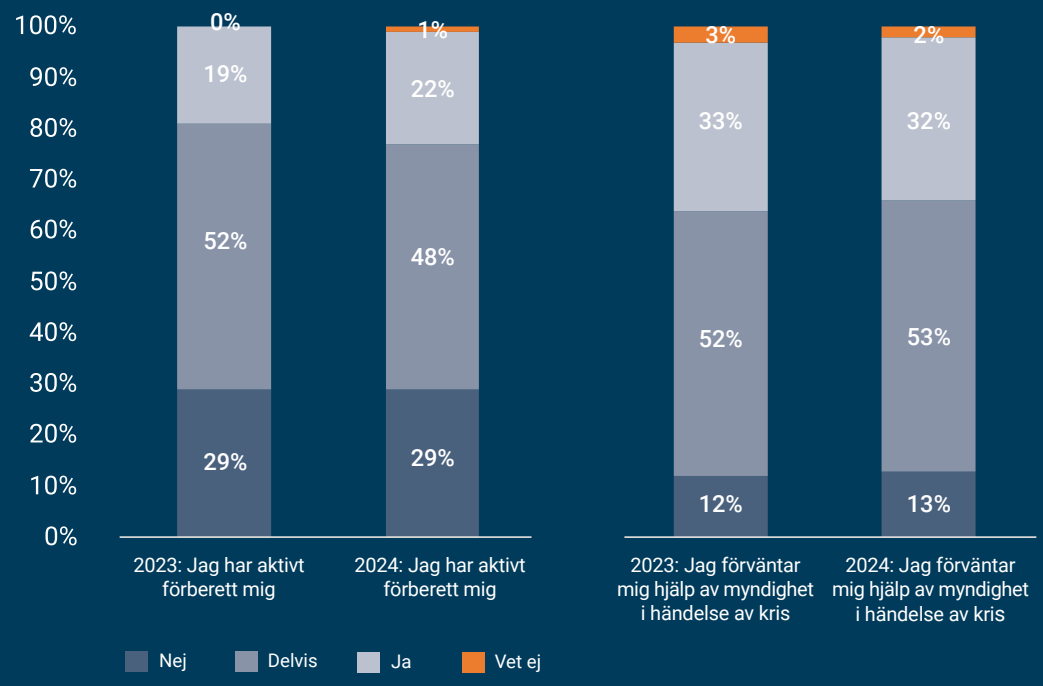
Den åldersgrupp med flest andel (79%) som helt eller delvis förberett sig för en potentiell kris är åldersgruppen 50–64 år. Det är den åldersgrupp som också har störst andel av dem som anser att hotbilden mot Sverige är mycket eller ganska allvarlig.

Den åldersgrupp som förberett sig i minst utsträckning är den yngsta åldersgruppen 18–29 år till en andel om 51%.

Allmänhetens förväntan på stöd från myndigheter i händelse av kris är mycket stor, nästan 9 av 10 (85%) har förväntan om stöd eller delvis stöd från myndigheter. Ingen nämnvärd förändring från föregående års mätning.

Det är en intressant motsägelse att allmänheten har stor förväntan om stöd från myndigheter i händelse av kris samtidigt som man har en låg tilltro till samma myndigheters förmåga att skydda kritisk infrastruktur (föregående sida). Här råder heller ingen förflyttning gentemot resultatet i fjol.

### Allmänhetens egna förberedelser (bygga förmåga) och förväntningar på myndigheter i händelse av kris



**”Hade man bara behövt lägga pengar på sin säkerhet hade det inte varit ett svårt problem att lösa. Utmaningen är snarare att hitta kompetens och säkerställa att det finns nog med tid att hantera säkerheten. Tid och kompetens är jättesvårt att få ihop.”**

– It-chef, Trossamfund

**”Säkerhetsskyddschefens placering i organisationen är en kritisk fråga. Rollen hamnar ofta i skymundan, bildligt i en källare, när kompetensen snarare behövs i ledningsgrupper eller ännu högre upp i organisationen.”**

– Försvarsdirektör, Region

# De tre viktigaste sakerna att fokusera på

Utifrån de kvalitativa och kvantitaiva intervjuer som Radar har genomfört med beslutsfattare är Omegapoints rekommendation att fokusera på nedanstående tre områden:

1

## Ledningsförmåga

Samtliga verksamheter behöver prioritera att bygga ledningsförmåga. Som visats i rapporten är situationen komplex, under förändring och med en stor potentiell påverkan. Konkret handlar det om att bygga insikt och kompetens inom domänområdet samt förstå den interna och externa omvärlden som är relevant för stunden. Den önskade effekten är att beslutsfattare skall få förmåga att kunna analysera och ytterst bli rådig och beslutsmässig.

2

## Kompetens

I rapporten framgår även att det kommer behövas byggas ny förmåga på bred front. Att bygga förmåga kommer kräva mer och ny kompetens. Med all säkerhet kommer kompetens bli en holistisk och bred flaskhals som kommer medföra en lägre takt. Konsekvensen kommer bli hårdare prioriteringar för att möta en oönskad (digital) affärsrisk inom vissa områden.

3

## Samverkan

Fokus och resurser behöver läggas på att bygga en kultur där samverkan är naturlig. Både internt och externt. En stark samverkanskultur kommer medföra bättre underrättelse, bidra till mer träffsäker analys, starkare beslutsunderlag och slutligen ett mer proaktivt förhållande till den ständigt föränderliga framtiden och hotbilden. Samverkansnivån kommer att öka i samhället då de regulatoriska ramverken och förordningarna prioriterar samverkansförmåga.

# Om kartläggningen

Kartläggningen har gjorts av Omegapoint tillsammans med dotterbolaget Basalt, i samarbete med Radar*. Den baseras på dels djupintervjuer med beslutsfattare inom samhällsviktig verksamhet och dels webbaserad enkät. Samtliga personer som har deltagit är medlemmar i verksamhetens ledningsgrupp och/eller ansvarar för alternativt påverkar beslut kring it och/eller säkerhetsfrågor.

Under samma tidsperiod genomfördes en webbundersökning i Sifopanelen gentemot den svenska allmänheten. I webbundersökningen deltog 1002 personer från ett riksrepresentativt urval i åldrarna 18-79 år.

*Radar är Nordens ledande leverantör av lokala- och oberoende datadrivna insikter för it-ekosystemets alla aktörer. Bland kunderna finns en majoritet av de största it-bolagen, mindre it-leverantörer, riskkapitalbolag och it-köpande organisationer inom både privat- och offentlig sektor.

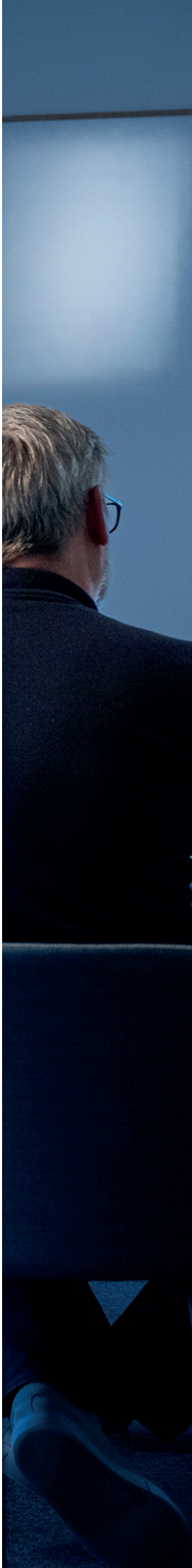
## Beslutsfattare

| | |
|---|---|
| **Metod** | Djupintervjuer, online/telefon |
| **Antal intervjuer** | 32 |
| **Genomförd av** | Radar |
| **Metod** | Webbaserad enkät |
| **Antal svarande** | 155 |
| **Genomförd av** | Radar |
| **Period** | Oktober–november 2024 |

## Allmänheten

Svenska allmänheten i åldrarna 18-79 år från ett riksrepresentativt urval

| | |
|---|---|
| **Metod** | Online i Kantar Medias webbpanel (Sifopanelen) |
| **Antal svarande** | 1002 |
| **Genomförd av** | Kantar |
| **Period** | 30 september–7 oktober 2024 |



# Om Omegapoint

Omegapoint är norra Europas ledande konsultbolag inom cybersäker digitalisering. Med en vision om en framtid där vi fullt ut kan lita på teknik använder Omegapoint sin expertis för att utveckla och skydda sina kunders verksamheter.

Koncernen har 950 anställda i Sverige, Norge, och Danmark, omsätter 1 400 MSEK och ägs delvis av medarbetare, delvis av FSN Capital.

Vårt helägda dotterbolag Basalt är ett av Sveriges ledande säkerhetsföretag med en stark position inom säkerhetsskydd. Rapporten Svenskt Säkerhetsindex har genomförts av Basalt mellan 2020–2024. Sedan 2025 genomförs Svenskt Säkerhetsindex i Omegapoint-koncernens regi och fungerar som ett strategiskt beslutsunderlag för samhällsviktiga verksamheter.


Cybersäkert från grunden


omega
point.
I samarbete med
Radar.