

# Små företags syn på cybersäkerhet

En undersökning från  
SSF Stöldskyddsföreningen, dec 2025



# Förord

I denna rapport presenterar vi resultaten av vår uppföljande undersökning där småföretag i Sverige bedömer sin cybersäkerhet. Undersökningen är en fortsättning på vår mätning från 2024 och ger en aktuell bild av hur företagen ser på sin oro, motståndskraft och upplevda utsatthet för cyberrelaterade angrepp.

Resultaten visar ett tydligt och delvis motsägelsefullt mönster: många företag uppger att de känner oro inför cyberhot, men de som har vidtagit minst skyddsåtgärder är ofta också minst oroliga. Samtidigt är det uppenbart att merparten av småföretagen behöver stärka sitt skydd för att stå bättre rustade i en allt mer komplex digital miljö.

Detta pekar på ett mer grundläggande problem i hur hot uppfattas, värderas och omsätts i praktiskt handlande. I vardagen är vi vana att hantera risk. I trafiken, till exempel, har vi en uppfattning om både faror och sannolikheter och kan väga risk mot nytta, som vid en omkörning. I dagens digitala miljöer rör sig företag däremot inte bara i ett sådant risklandskap, utan även i ett osäkerhetslandskap där hoten är föränderliga, sammanlänkade och svåra att överblicka. Det gör det svårt att avgöra vad som är viktigast att prioritera och vilka åtgärder som faktiskt ger effekt.

I detta landskap uppstår det som vi här kallar osäkerhetsstress. Begreppet knyter an till forskning om hur människor och organisationer fattar beslut i situationer präglade av osäkerhet, otydliga hotbilder och begränsat beslutsunderlag. Med osäkerhetsstress menar vi ett tillstånd där organisationer vet att de är utsatta för hot, men saknar tillräcklig överblick för att kunna värdera riskerna och fatta välgrundade beslut om vad som är rimligt att göra. De lever med en känsla av att något kan inträffa, utan att riktigt veta vilket skydd som är tillräckligt. Osäkerhetsstress försämrar beslutsförmågan och leder i praktiken ofta till att beslut skjuts upp, att åtgärder vidtas på svagt underlag eller att resurser läggs på insatser som främst skapar en känsla av kontroll snarare än verklig säkerhet. Att minska osäkerhetsstress handlar inte om att skrämma fram fler åtgärder eller att skapa mer oro. Det handlar om att hjälpa företag att prioritera rätt. När osäkerhet ersätts av tydlighet och komplexitet delas upp i hanterbara steg, blir säkerhetsarbetet både mer effektivt och mer genomförbart.

Det är precis detta som vi på SSF Stöldskyddsföreningen arbetar med varje dag. Vårt mål är att hjälpa företag att stärka sin motståndskraft mot cyberrelaterade angrepp, både under och efter en incident.

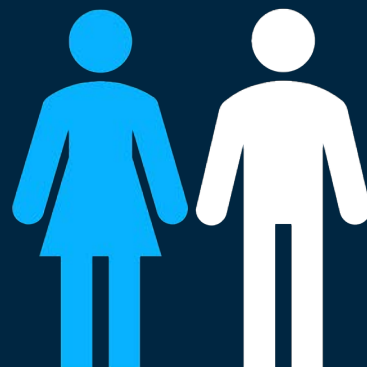


# Om undersökningen

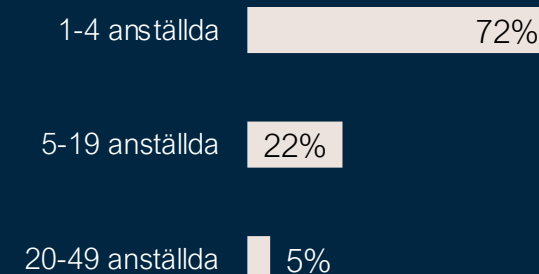
|                  |   |
|------------------|---|
| Syfte            | SSF Stöldskyddsföreningen har gett Demoskop i uppdrag att genomföra denna undersökning bland små och medelstora företag. Syftet är att kartlägga deras oro, beredskap och utsatthet när det gäller cybersäkerhet. Undersökningen är en uppföljning av motsvarande undersökning genomförd 2024, och är finansierad av dåvarande MSB, nu Myndigheten för civilt försvar, MCF. Vissa frågor har formulerats om, vilket gör att eventuella jämförelser bör tolkas med försiktighet. |
| Metod            | Webbintervjuer  |
| Målgrupp         | Vd/ägare i små och medelstora företag (1-49 anställda)  |
| Antal intervjuer | 573 intervjuer  |
| Vägning          | Resultatet är vägt med avseende på antalet anställda  |
| Fältperiod       | 28 oktober – 13 november 2025   |
| Ansvariga        | Ulrika Hallesius, SSF Stöldskyddsföreningen och Per Hörnsten, Demoskop  |

# Demografi\*

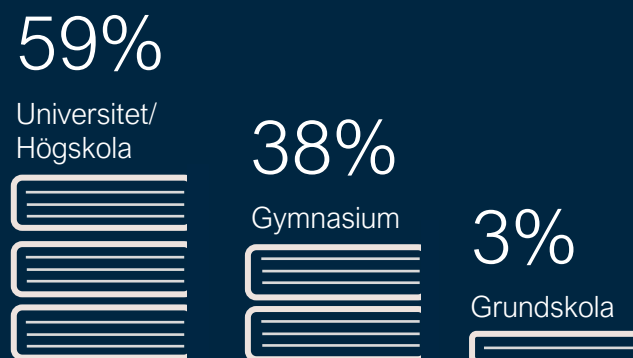
## Bransch



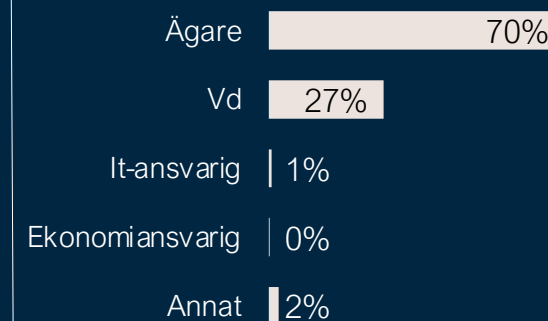
## Antal anställda



## Utbildning



## Befattning



\*Vägd data

# SSF:s prioriteringar

SSF Stöldskyddsföreningen arbetar systematiskt för att förebygga cyberbrottslighet och stärka cybersäkerheten för privatpersoner och mindre företag.

Denna undersökning tar sin utgångspunkt i små och medelstora företags upplevda situation. Med stöd i resultaten har SSF Stöldskyddsföreningen identifierat tre prioriterade områden som kommer att vara i fokus under det kommande året.

Samtidigt görs en utveckling och uppdatering av SSF:s normer som berör cybersäkerhet.

## 1. Ökad medvetenhet om hot, risker och affärskrav

Trots att medvetenheten om cyberhot har ökat de senaste åren uppger fortfarande över hälften av de tillfrågade företagen att de inte är särskilt oroade för att drabbas av cyberbrott eller dataintrång. Samtidigt finns en växande insikt om krav från både kunder och leverantörer – men denna insikt omsätts i begränsad utsträckning i konkreta säkerhetshöjande åtgärder.

På sikt riskerar detta att resultera i att företag inte klarar de krav som ställs på leverantörskedjor enligt den nya cybersäkerhetslagen.

SSF Stöldskyddsföreningen kommer att arbeta för att öka företagens medvetenhet och förståelse för risker, regulatoriska krav och affärsmässiga möjligheter. En central del är att tydligare synliggöra affärsnyttan med stärkt cybersäkerhet, till exempel ökad tillit, konkurrenskraft och leveransförmåga. Arbetet kommer bland annat att ske med Säkerhetskollen som grund och genomföras som riktade informationsinsatser, kampanjer och samverkan med branschorganisationer.

## 2. Stärka företagets förmåga att hantera och överleva en cyberattack

Undersökningen visar att två av tre företag saknar en policy för informationssäkerhet, och att över hälften saknar åtgärdsplaner för hur en cyberincident ska hanteras. Samtidigt tar färre än

hälften stöd av externa leverantörer inom cybersäkerhet.

Att vara förberedd genom planering, tydliga roller och övning är avgörande för att minska konsekvenserna av en attack och möjliggöra snabb återhämtning.

Under året kommer SSF Stöldskyddsföreningen att stärka stödet till mindre företag i frågor som rör incidentberedskap och kontinuitetshöjande åtgärder. Ett första steg är att via Säkerhetskollen ta fram lättillgängliga guider, checklistor och rekommendationer för hur företag kan förbereda sig, öva och hantera en cyberattack.

SSF Stöldskyddsföreningen kommer även att verka för att skapa förutsättningar för att sprida information om pågående cyberattacker till små och medelstora företag.

## 3. Cybersäkerhetsutbildning för personal

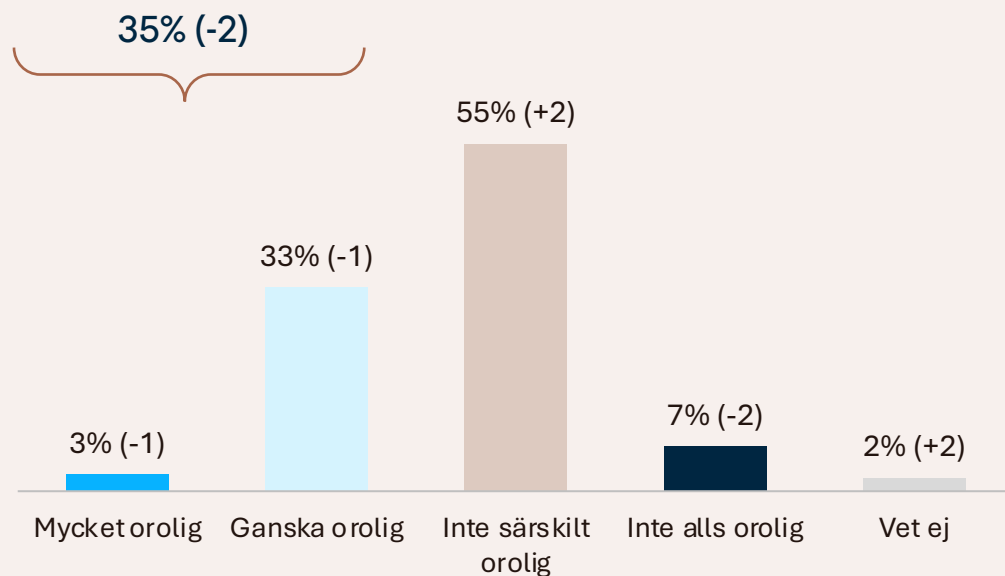
Endast 17 procent av företagen uppger att de genomför cybersäkerhetsutbildning för sin personal. Detta trots att medarbetare och chefer ofta utgör en mycket viktig pusselbit för ett effektivt och systematiskt cybersäkerhetsarbete.

Samtidigt är personalen även privatpersoner, vilket innebär att kompetenshöjande insatser i arbetslivet också bidrar till en bredare höjning av den samhälleliga cybersäkerheten, och vice versa.

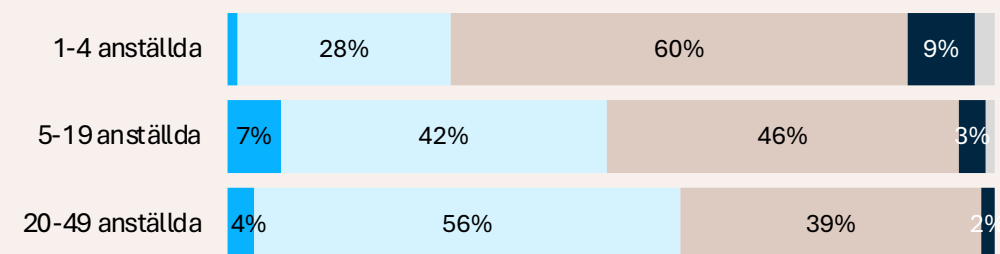
Personal kommer att vara en prioriterad målgrupp. SSF Stöldskyddsföreningen kommer att verka för att företag enkelt ska kunna erbjuda sina medarbetare grundläggande cybersäkerhetsutbildning. Säkerhetskollen är ett centralt verktyg i detta arbete, inte minst eftersom samma eller liknande utbildningsinnehåll kan användas både i arbetslivet och för privatpersoner.

# Drygt 1 av 3 företag känner oro över att bli utsatt för cyberrelaterade brott

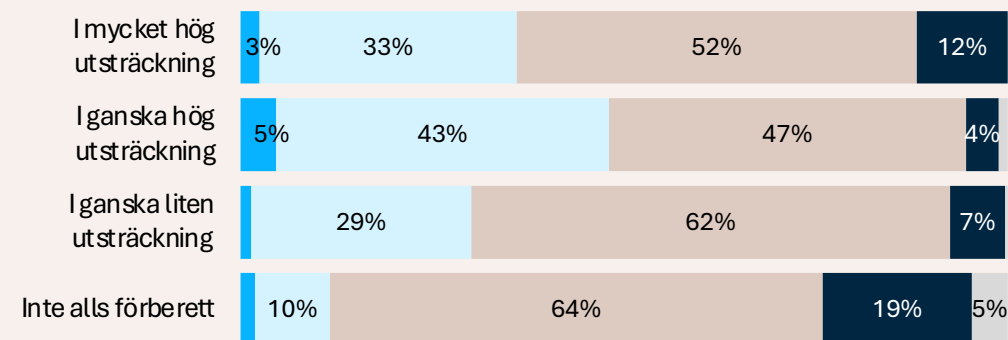
Diagrammet nedan visar övergripande svar på frågan samt svaren nedbrutna efter företagsstorlek (antal anställda) till höger.



■ Mycket orolig ■ Ganska orolig ■ Inte särskilt orolig ■ Inte alls orolig ■ Vet ej



I vilken utsträckning är ert företag förberett för att stå emot cyberrelaterade attacker?



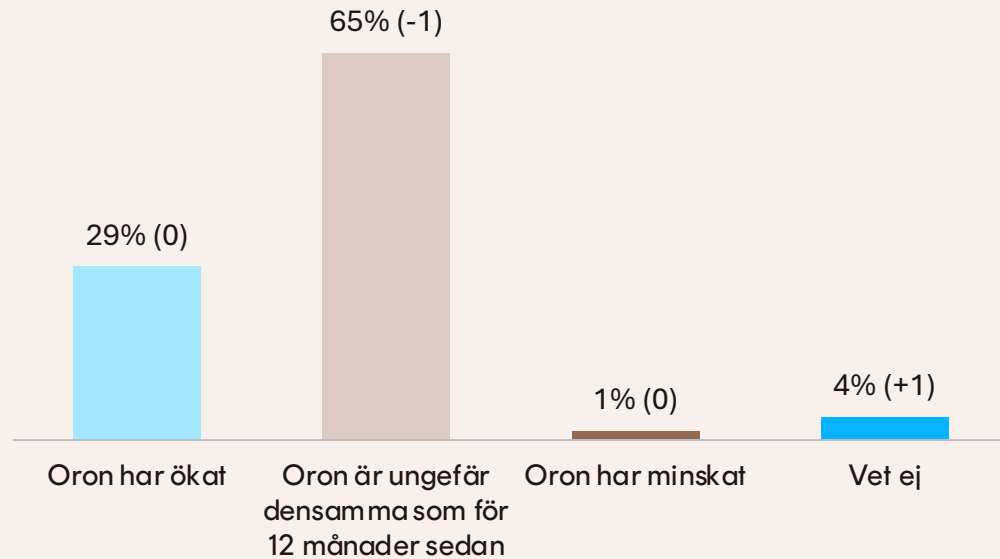
**Fråga:** Hur orolig är du för att ert företag ska utsättas för cyberrelaterade brott?

**Bas:** Samtliga, 573 intervjuer  
Skilnad i jämförelse med 2024 anges med (+/- x)

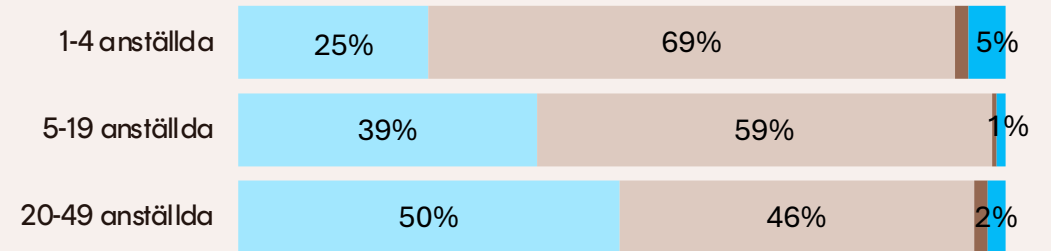
**Fråga 2024:** Hur orolig är du att ditt företag ska bli utsatt för it-relaterade eller digitala brott?

# 3 av 10 företag känner en ökad oro

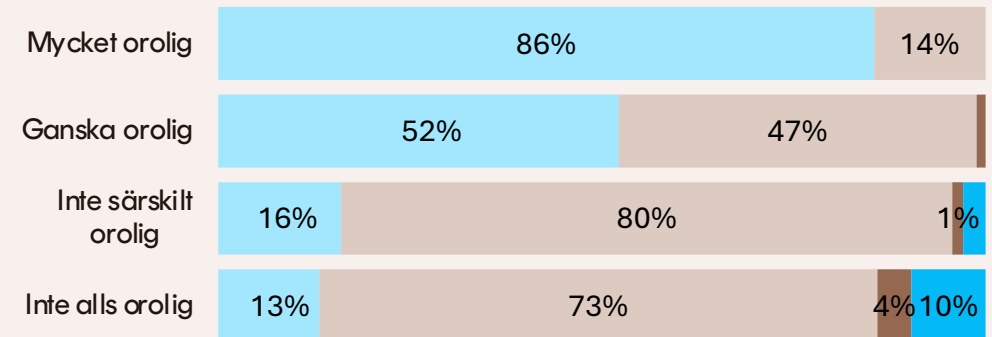
Diagrammet nedan visar övergripande svar på frågan samt svaren nedbrutna efter företagsstorlek (antal anställda) till höger.



- Oron har ökat
- Oron är ungefär densamma som för 12 månader sedan
- Oron har minskat
- Vet ej



Hur orolig är du för att ert företag ska utsättas för cyberrelaterade brott?

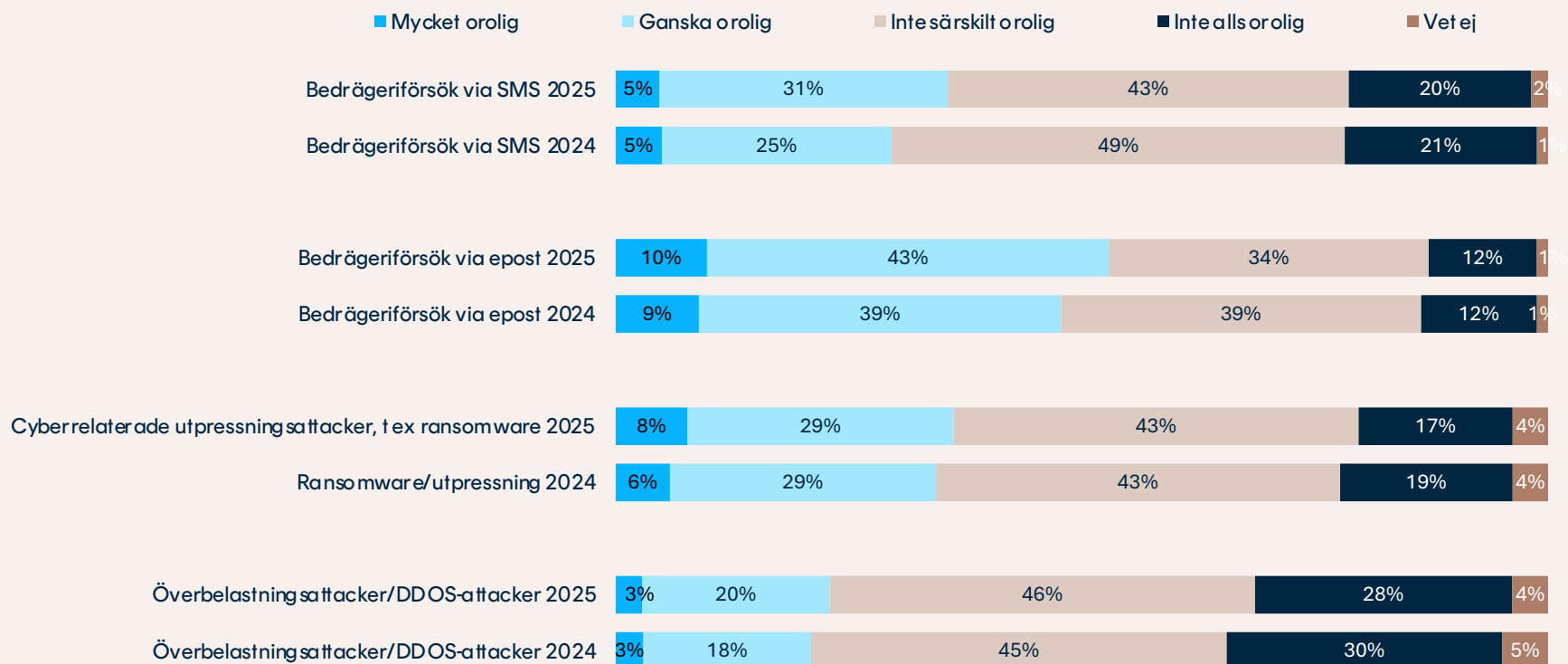


**Fråga:** Har din oro ökat eller minskat jämfört med förra året?

**Bas:** Samtliga, 573 intervjuer  
Skillnad i jämförelse med 2024 anges med (+/- x)

**Fråga 2024:** Skulle du säga att oron har ökat eller minskat i jämförelse med 12 månader bakåt i tiden när det gäller potentiella it-relaterade och digitala brott på det företag du arbetar på?

# Oron för bedrägeriförsök via SMS och e-post ökar mest

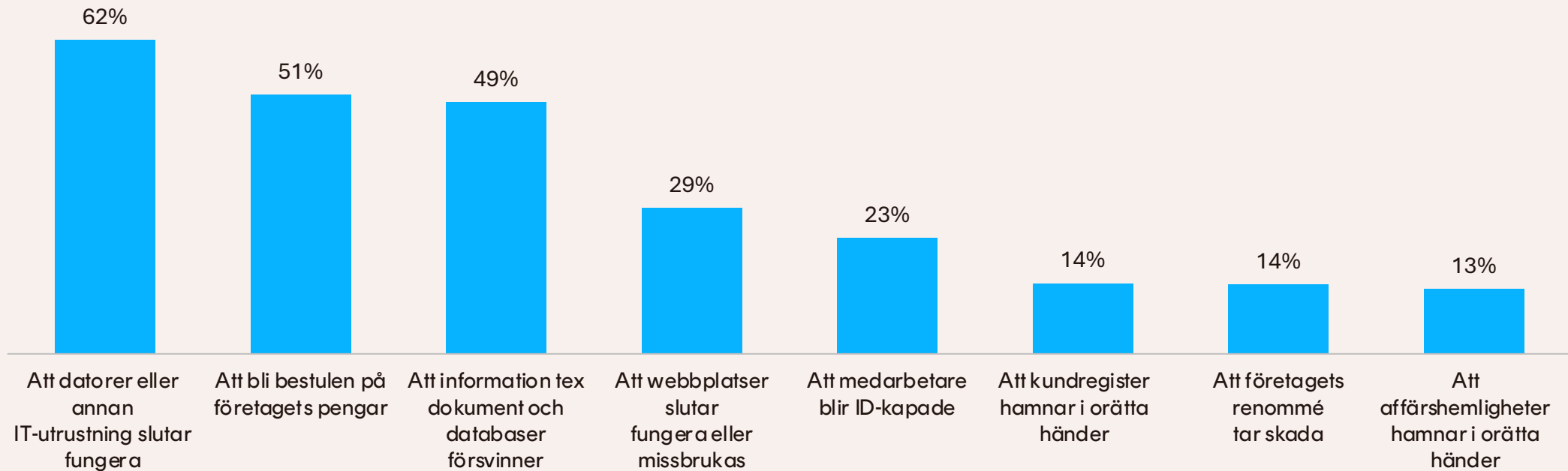


**Fråga:** Hur orolig är du för att ert företag ska utsättas för något av följande?

**Bas:** Samtliga, 573 intervjuer

**Fråga 2024:** Hur orolig är du att ditt företag ska utsättas för någon av följande?

## 6 av 10 oroar sig mest för att it-utrustningen ska sluta fungera

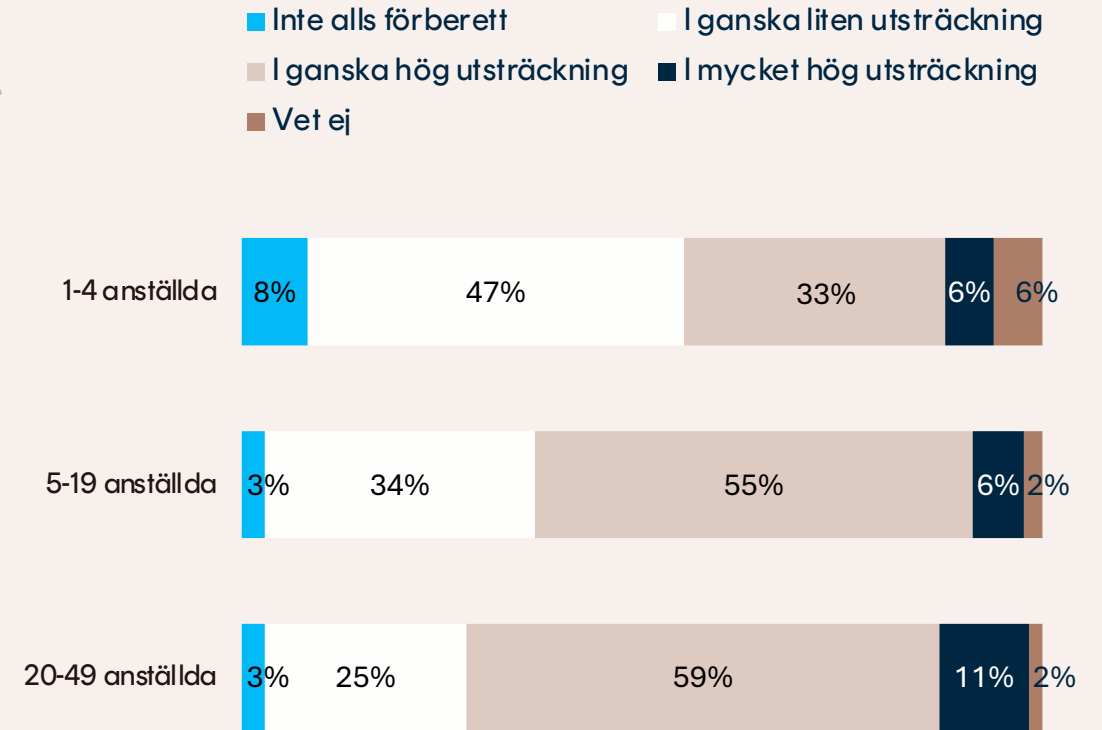
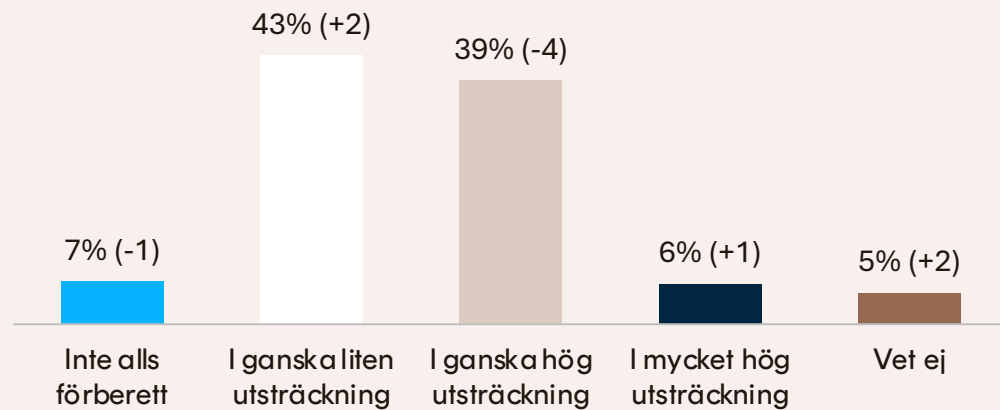


**Fråga:** Vilken konsekvens är du mest orolig för vid en cyberrelaterad attack? (Max 3 svar möjliga)

**Bas:** Samtliga, 573 intervjuer

# Vartannat företag är dåligt förberett för att möta en cyberrelaterad attack

Diagrammet nedan visar övergripande svar på frågan, samt svaren nedbrutna efter företagsstorlek (antal anställda) till höger.



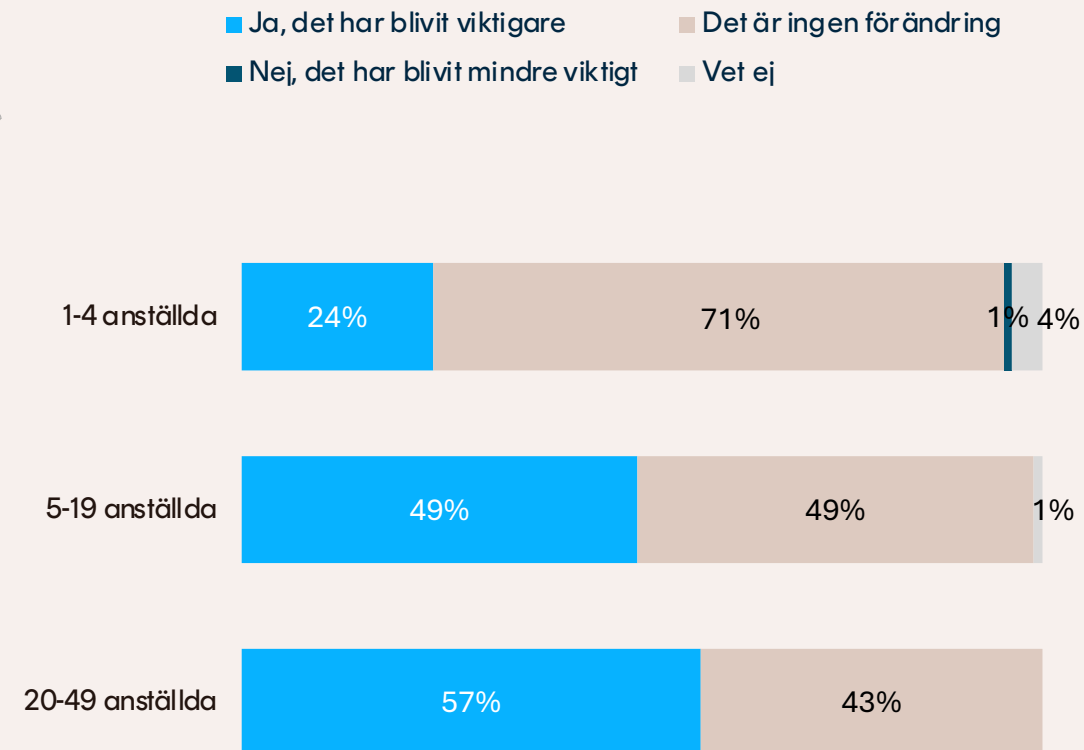
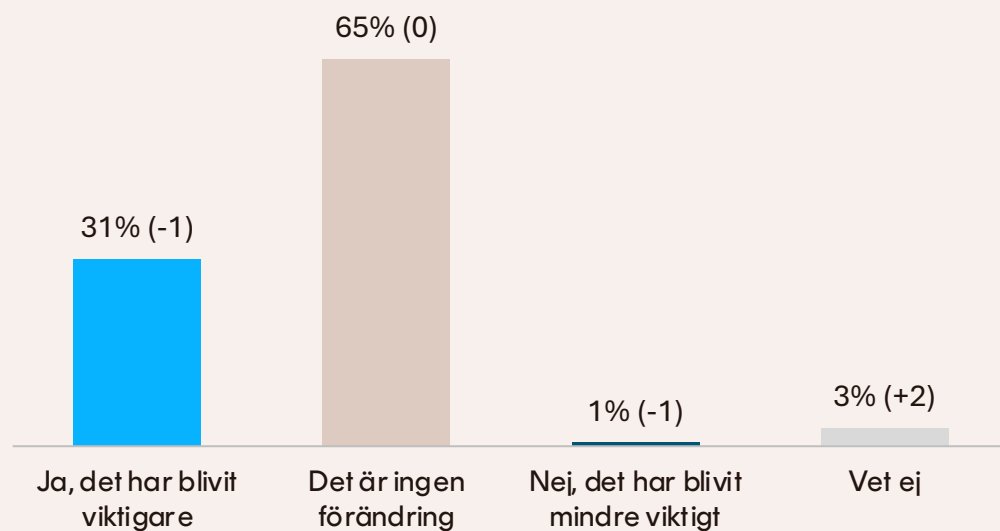
**Fråga:** I vilken utsträckning är ert företag förberett för att stå emot cyberrelaterade attacker?

**Bas:** Samtliga, 573 intervjuer  
Skillnad i jämförelse med 2024 anges med (+/- x)

**Fråga 2024:** I vilken utsträckning anser du att ditt företag är förberett för att möta attacker mot it-system och andra digitala hot?

# 65 procent uppger att cybersäkerheten inte har blivit viktigare det senaste året

Diagrammet nedan visar övergripande svar på frågan, samt svaren nedbrutna efter företagsstorlek (antal anställda) till höger.



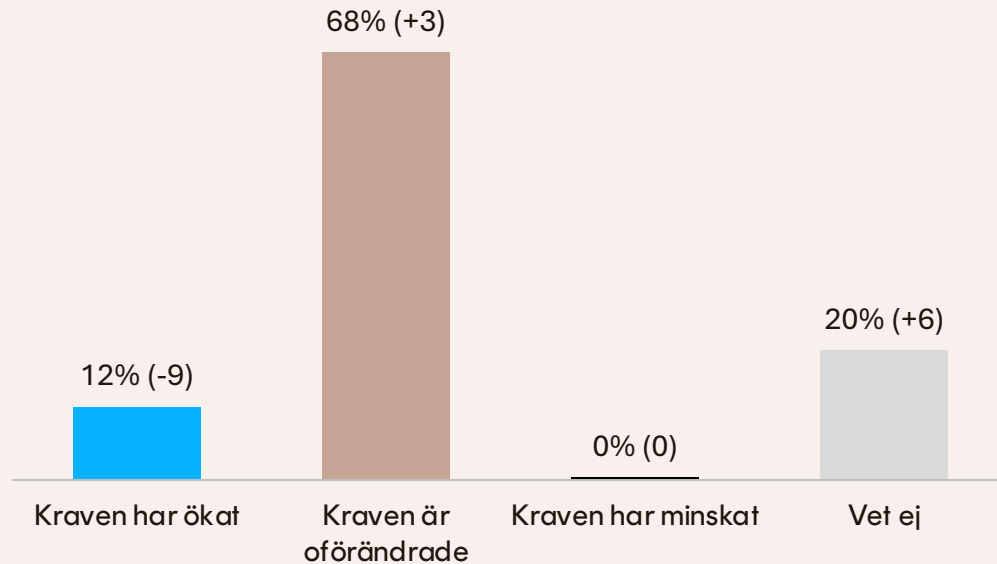
**Fråga:** Har cybersäkerhet blivit viktigare för er verksamhet jämfört med förra året?

**Bas:** Samtliga, 573 intervjuer  
Skillnad i jämförelse med 2024 anges med (+/- x)

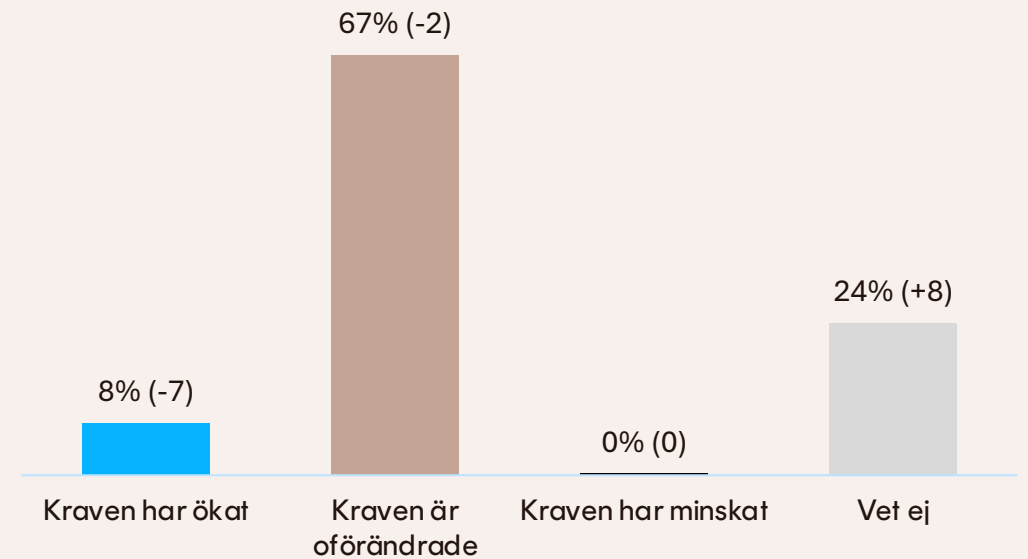
**Fråga 2024:** Har digital säkerhet blivit viktigare för er verksamhet under de senaste 12 månaderna?

# Runt 1 av 10 företag har fått ökade krav på cybersäkerhet från kunder eller från leverantörer

... kunders krav på ert företags cybersäkerhet har förändrats jämfört med förra året?



... leverantörers krav på ert företags cybersäkerhet har förändrats jämfört med förra året?



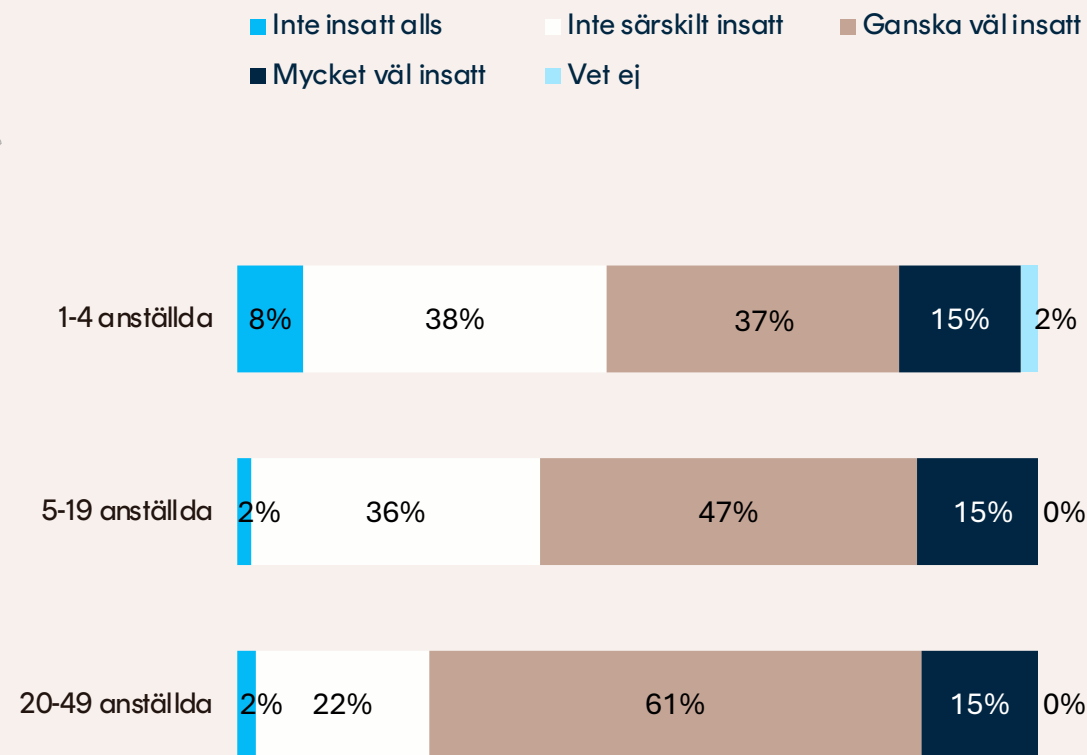
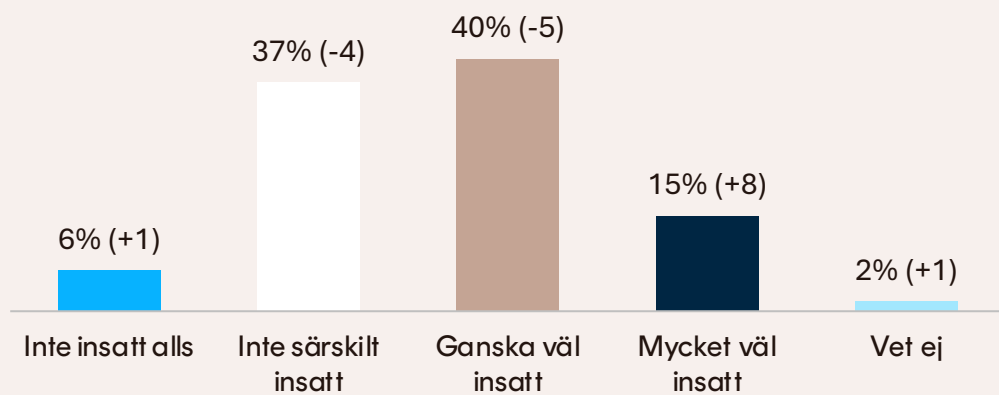
**Fråga:** Anser du att era...?

**Bas:** Samtliga, 573 intervjuer  
Skillnad i jämförelse med 2024 anges med (+/- x)

**Fråga 2024:** Om du tänker på de senaste 12 månaderna. Anser du att era...? ... kunders krav på digital säkerhet har förändrats respektive ... leverantörers krav på digital säkerhet har förändrats

# Bara hälften av respondenterna känner sig insatta i cybersäkerhetsfrågor

Diagrammet nedan visar övergripande svar på frågan, samt svaren nedbrutna efter företagsstorlek (antal anställda) till höger.



**Fråga:** Hur insatt är du i frågor som berör cybersäkerheten i ert företag?

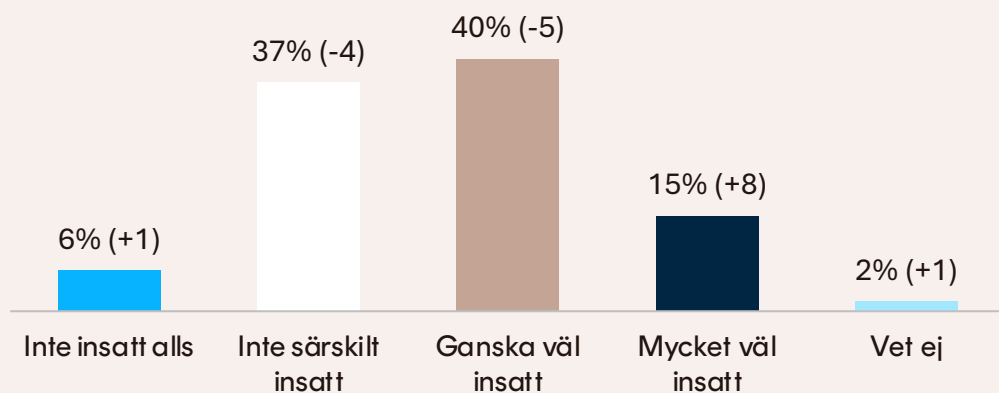
**Bas:** Samtliga, 573 intervjuer

Skillnad i jämförelse med 2024 anges med (+/- x)

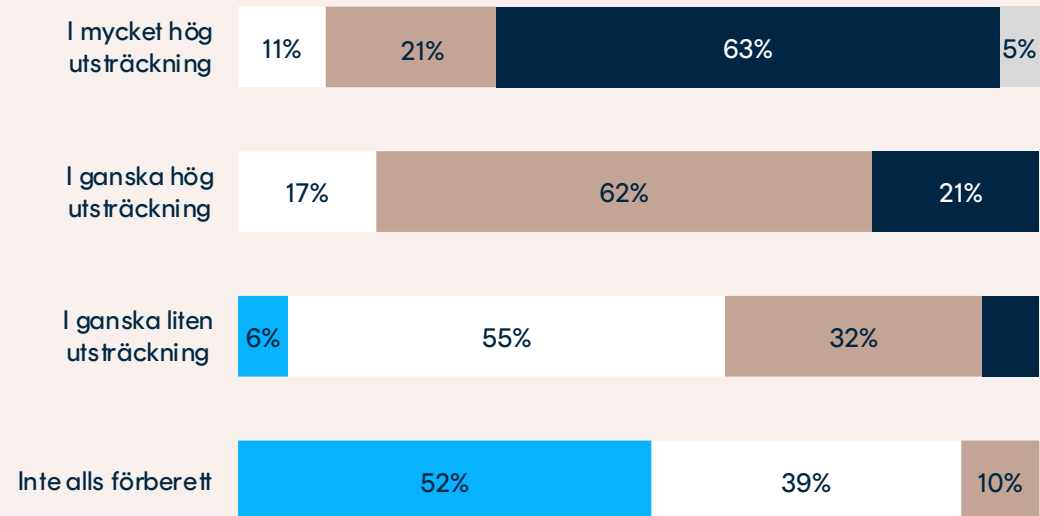
Fråga 2024: Hur väl skulle du säga att du är insatt i frågor som rör skydd mot digitala hot i ditt företag?

# Bara hälften av respondenterna känner sig insatta i cybersäkerhetsfrågor

Diagrammet nedan visar övergripande svar på frågan, medan resultatet till höger visar hur dessa svar fördelar sig beroende på hur förberedda företagen anser sig vara mot cyberrelaterade attacker.



I vilken utsträckning är ert företag förberett för att stå emot cyberrelaterade attacker?



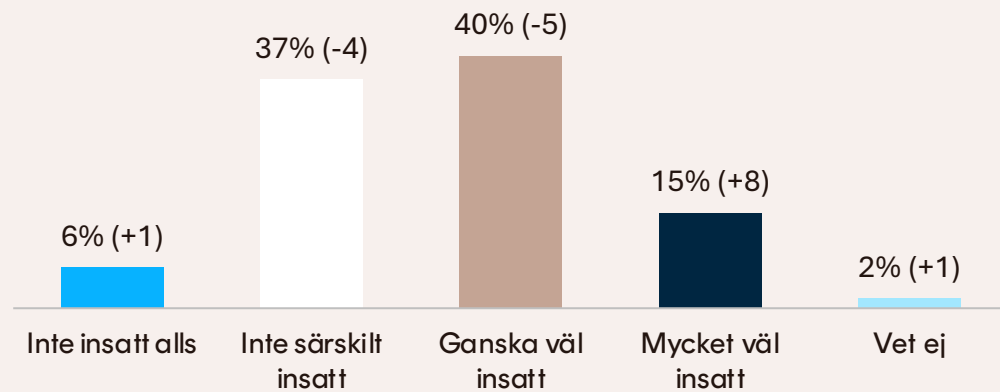
**Fråga:** Hur insatt är du i frågor som berör cybersäkerheten i ert företag?

**Bas:** Samtliga, 573 intervjuer  
Skillnad i jämförelse med 2024 anges med (+/- x)

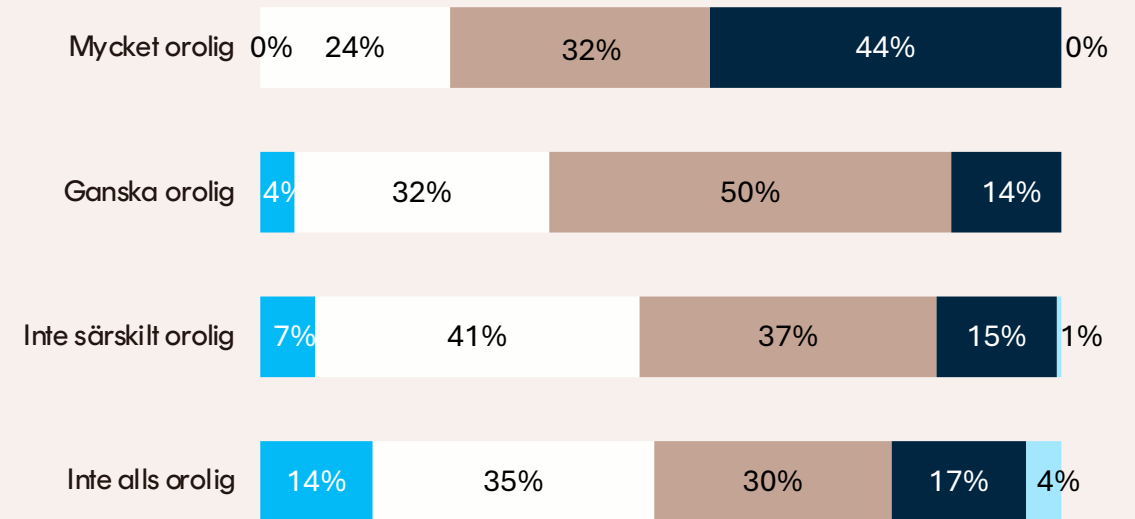
**Fråga 2024:** Hur väl skulle du säga att du är insatt i frågor som rör skydd mot digitala hot i ditt företag?

# Bara hälften av respondenterna känner sig insatta i cybersäkerhetsfrågor

Diagrammet nedan visar övergripande svar på frågan, medan resultatet till höger visar hur svaren fördelar sig utifrån företagets oro för att utsättas för cyberrelaterade brott.



Hur orolig är du för att ert företag ska utsättas för cyberrelaterade brott?



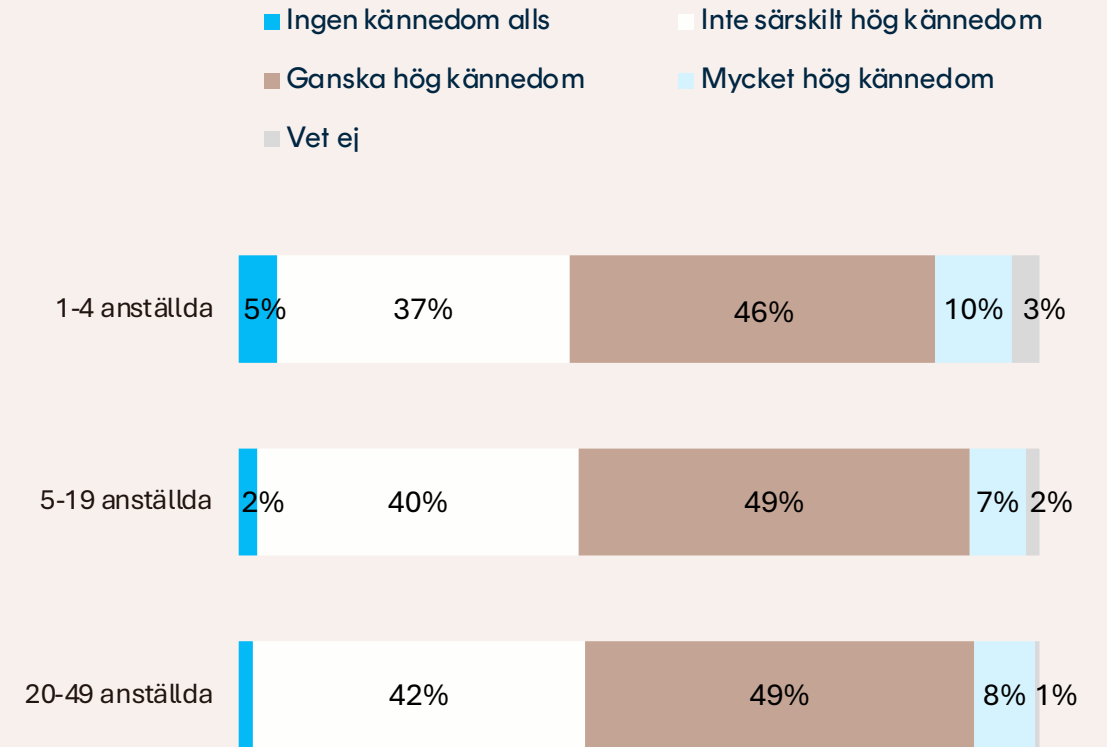
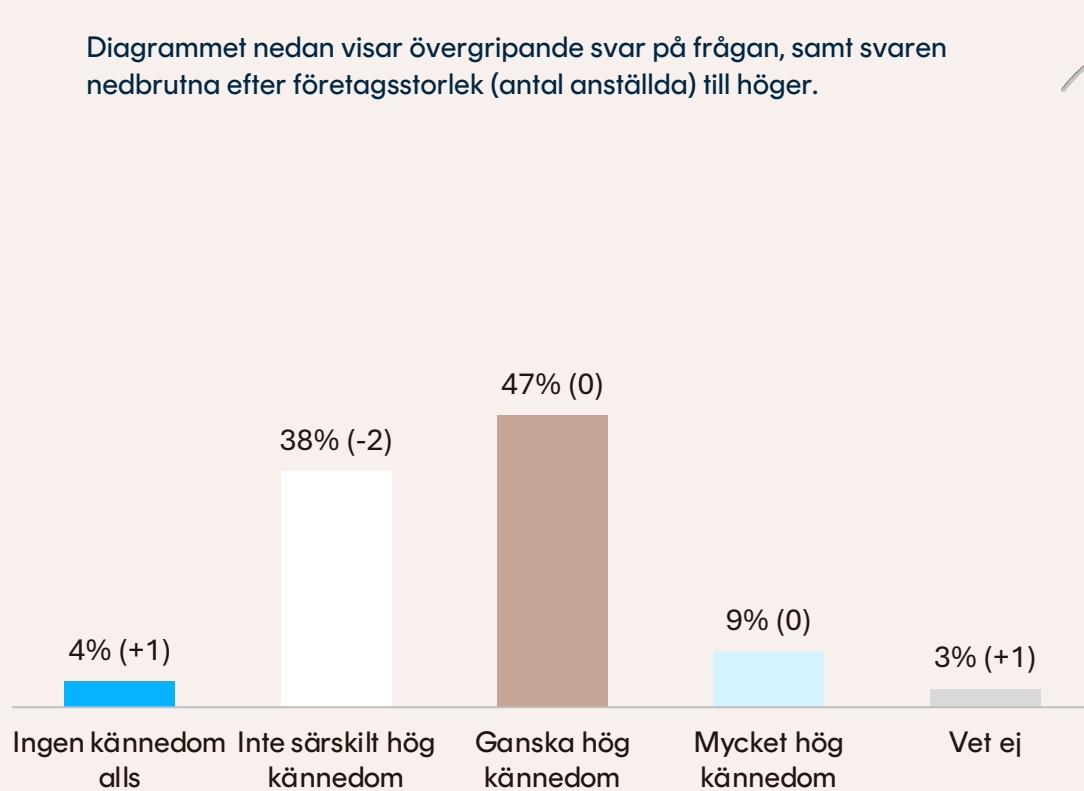
**Fråga:** Hur insatt är du i frågor som berör cybersäkerheten i ert företag?

**Bas:** Samtliga, 573 intervjuer  
Skillnad i jämförelse med 2024 anges med (+/- x)

**Fråga 2024:** Hur väl skulle du säga att du är insatt i frågor som rör skydd mot digitala hot i ditt företag?

# 4 av 10 anser att kunskapen om digital säkerhet är låg på arbetsplatsen

Diagrammet nedan visar övergripande svar på frågan, samt svaren nedbrutna efter företagsstorlek (antal anställda) till höger.



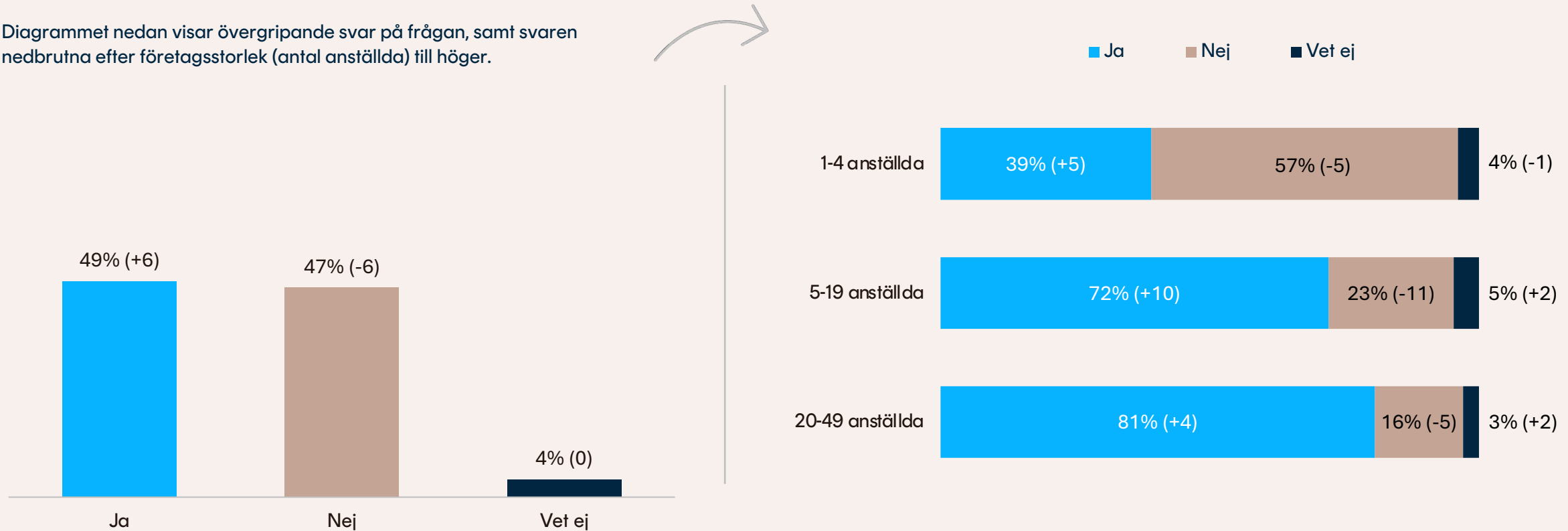
**Fråga:** Hur stor kännedom skulle du säga det är kring digital säkerhet generellt på din arbetsplats?

**Bas:** Samtliga, 573 intervjuer  
Skillnad i jämförelse med 2024 anges med (+/- x)

**Fråga 2024:** Generellt sett, hur stor kännedom skulle du säga det är kring digital säkerhet inom din arbetsplats?

# Hälften av företagen anlitar extern leverantör för att skydda företagets information och it-system

Diagrammet nedan visar övergripande svar på frågan, samt svaren nedbrutna efter företagsstorlek (antal anställda) till höger.

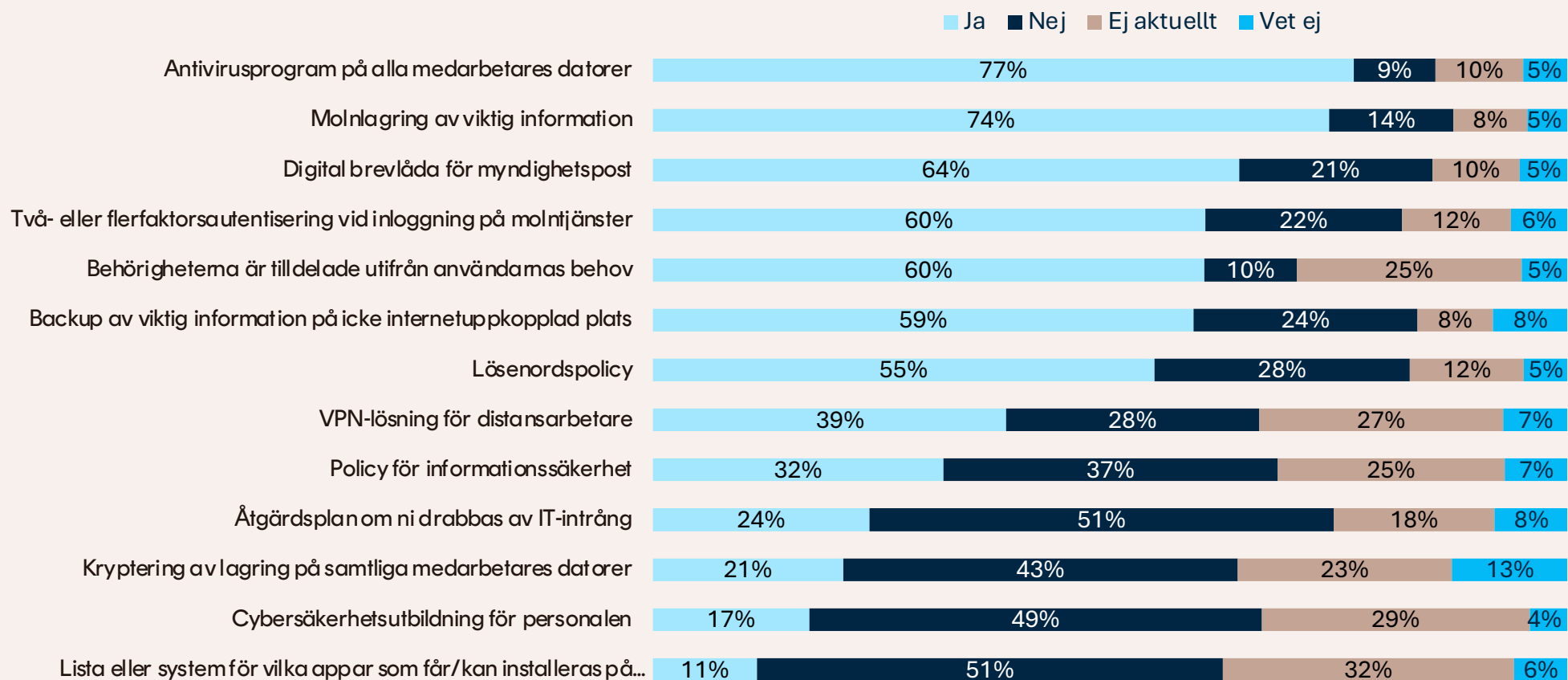


**Fråga:** Anlitar ni någon extern leverantör för att skydda företagets information och it-system?

**Bas:** Samtliga, 573 intervjuer  
Skillnad i jämförelse med 2024 anges med (+/- x)

**Fråga 2024:** Samverkar ni med någon eller några externa aktörer i digitala säkerhetsfrågor för skydd av företagets information och system?

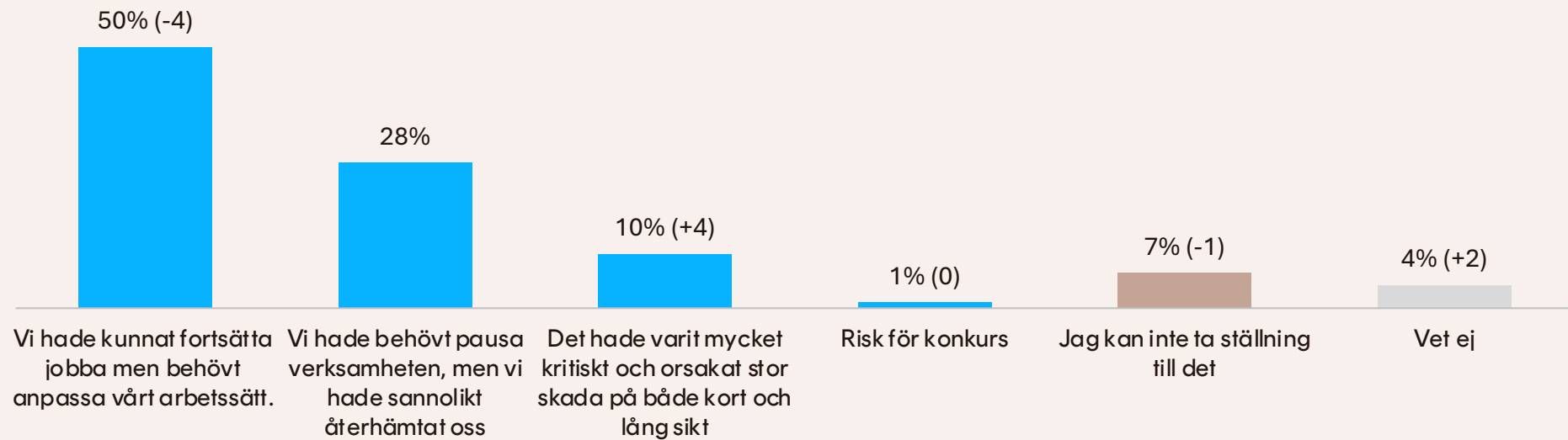
# Inte ens två företag av tio arbetar med cybersäkerhetsutbildning för personal



**Fråga:** Vad av följande tillämpar ni för att stärka er cybersäkerhet?

**Bas:** Samtliga, 573 intervjuer

# Ett it-avbrott på upp till fem dagar skulle stoppa verksamheten hos vart tredje företag



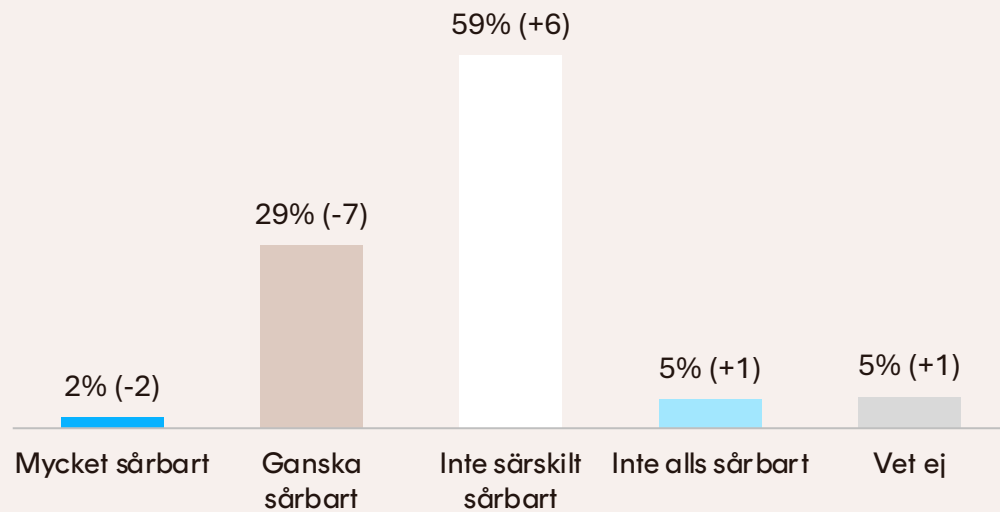
**Fråga:** Hur kritiskt skulle det vara om era it-system blev helt eller delvis otillgängliga under fem dagar?

**Bas:** Samtliga, 573 intervjuer  
Skillnad i jämförelse med 2024 anges med (+/- x)

**Fråga 2024:** Föreställ dig att ditt företag blir utsatt för en attack mot företagets it-system som varar under fem dagar. Hur kritiskt hade det varit för ditt företag om it-systemen helt eller delvis var otillgängliga under denna tid?

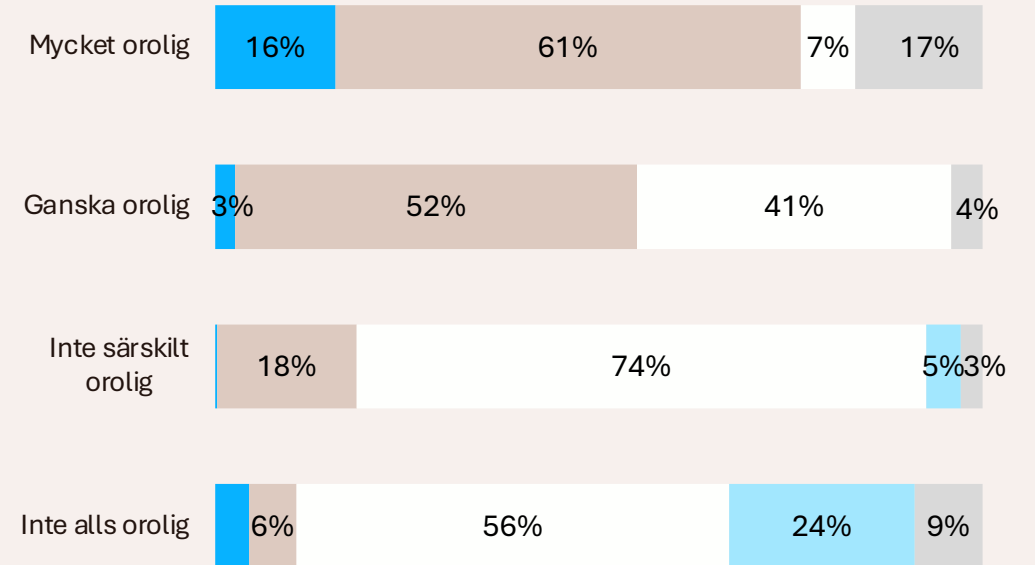
# 3 av 10 företag upplever att de är sårbara mot cyberrelaterade brott

Diagrammet nedan visar övergripande svar på frågan, medan resultatet till höger visar hur svaren fördelar sig utifrån företagets oro för att utsättas för cyberrelaterade brott.



■ Mycket sårbart ■ Ganska sårbart ■ Inte särskilt sårbart ■ Inte alls sårbart ■ Vet ej

Hur orolig är du för att ert företag ska utsättas för cyberrelaterade brott?



**Fråga:** Hur sårbart anser du att ert företag är för cyberrelaterade brott?

**Bas:** Samtliga, 573 intervjuer  
Skillnad i jämförelse med 2024 anges med (+/- x)

**Fråga 2024:** Hur sårbart anser du att ditt företag är för digitala och it-relaterade brott?

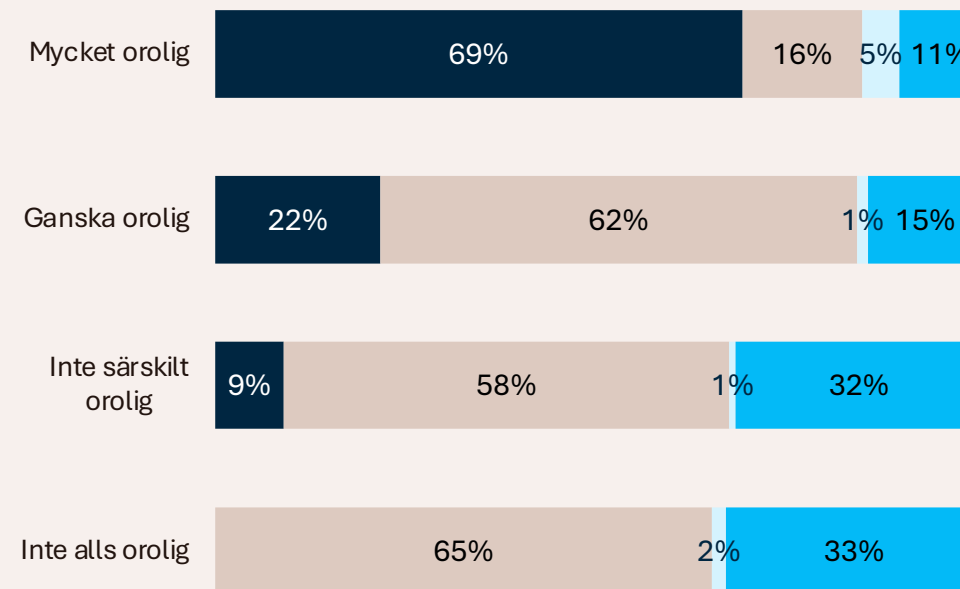
# Ökat antal attacker skapar stor oro

Diagrammet nedan visar övergripande svar på frågan, medan resultatet till höger visar hur svaren fördelar sig utifrån företagets oro för att utsättas för cyberrelaterade brott.



■ Det har ökat ■ Det är oförändrat ■ Det har minskat ■ Vet ej

Hur orolig är du för att ert företag ska utsättas för cyberrelaterade brott?

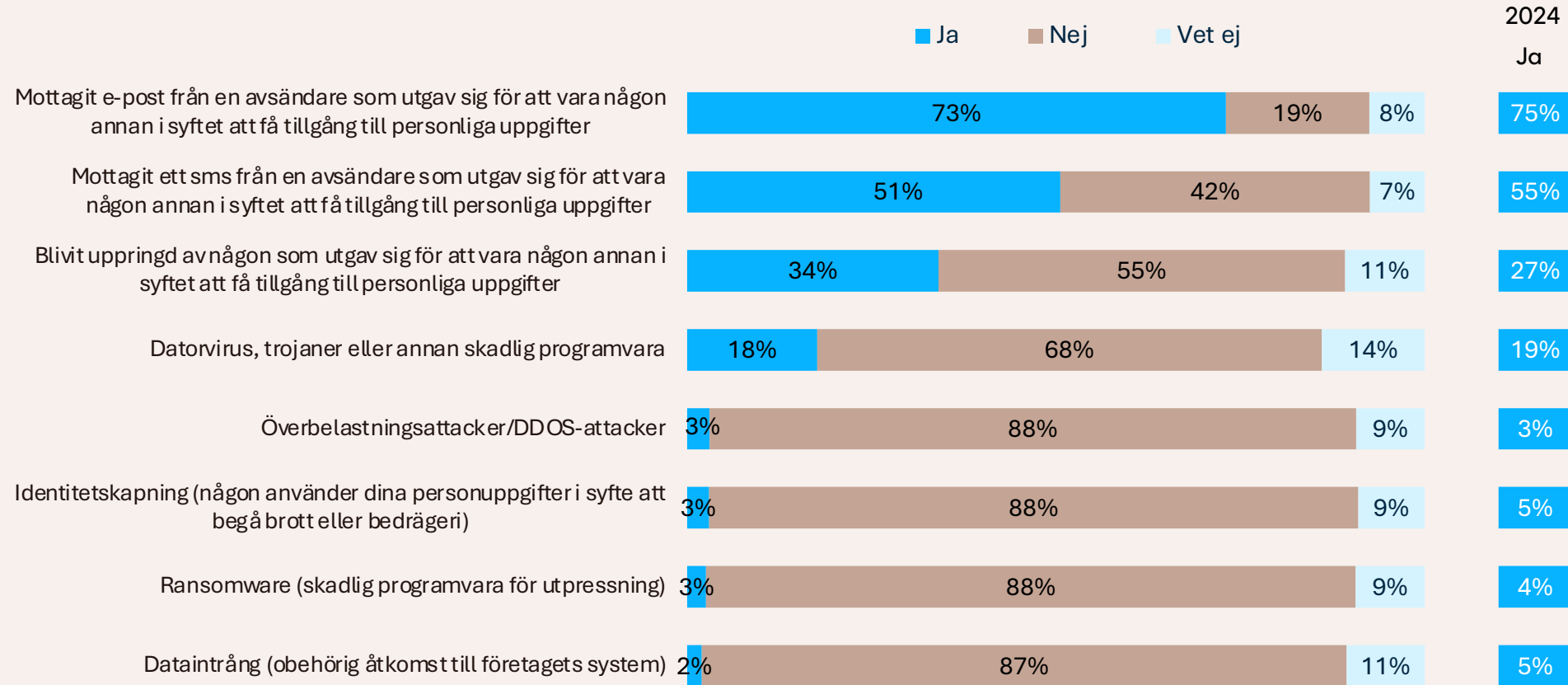


**Fråga:** Upplever du att antalet cyberrelaterade attacker mot ert företag har ökat, minskat eller varit oförändrat jämfört med föregående år?

**Bas:** Samtliga, 573 intervjuer  
Skillnad i jämförelse med 2024 anges med (+/- x)

Fråga 2024: Upplever du att antalet it- och digitala attacker mot ditt företag har ökat, minskat eller varit oförändrat de senaste 12 månaderna?

# Bedrägeriförsök via e-post är vanligaste incidenten

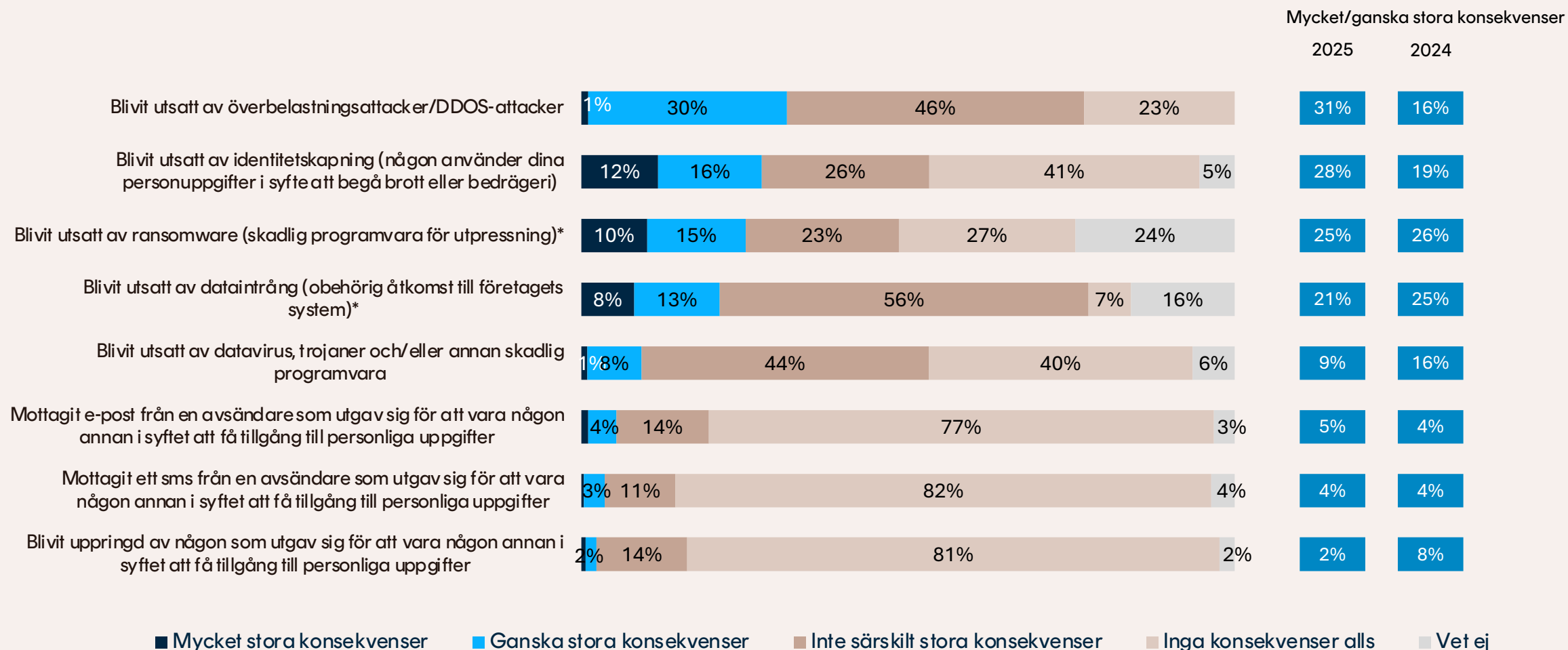


**Fråga:** Har ert företag blivit utsatt för något av följande under det senaste året?\*

**Bas:** Samtliga, 573 intervjuer

\* Frågelydelse 2024: Har ditt företag blivit utsatt för någon av följande incidenter under det senaste året?\*

# Ransomware och dataintrång skapar störst skada för företagen

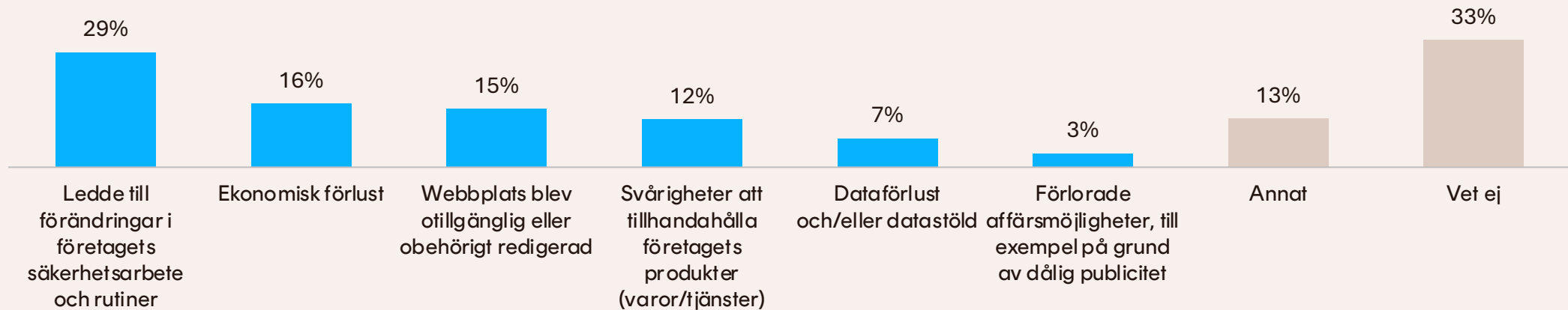


**Fråga:** Vilka konsekvenser fick det för företaget att ni...?

**Bas:** Blivit utsatt för incident/er, 11-419 intervjuer

\* Låg bas: Under 30 intervjuer

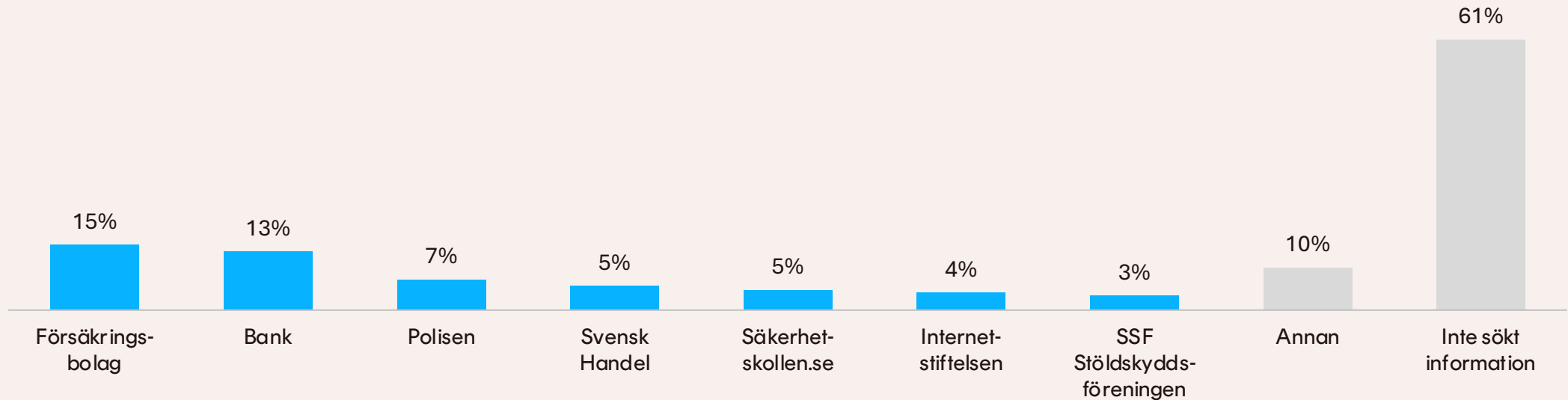
# Förändringar i säkerhetsarbete och rutiner är den vanligaste följden av cyberrelaterade brott



**Fråga:** På vilket sätt påverkade de cyberrelaterade brotten ert företag? (Flera svar möjliga).

**Bas:** Blivit utsatt för incident/er som gett konsekvenser, 136 intervjuer  
Skillnad i jämförelse med 2024 anges med (+/- x)

## Sex av tio företag har inte sökt information eller stöd för att skydda sig mot bedrägerier



**Fråga:** Har du sökt information hos någon eller några av dessa företag/organisationer för att få hjälp med att skydda dig mot bedrägerier?

**Bas:** Samtliga, 573 intervjuer

# Stöldskyddsföreningen – stöd för ett tryggare digitalt företagande

## Om SSF Stöldskyddsföreningen

SSF Stöldskyddsföreningen är en oberoende, icke vinstdrivande organisation som arbetar för att förebygga brott och stärka tryggheten i samhället. Vi stödjer företag och organisationer i arbetet med säkerhet, både i den fysiska och digitala miljön.

I takt med att hotbilden blir allt mer komplex möter vi dagligen företag som vill göra rätt, men som har svårt att avgöra vad som är viktigast att prioritera. Vårt arbete utgår från att göra säkerhetsfrågor mer begripliga, mer hanterbara och mer genomförbara.

Genom kunskap, vägledning och konkreta verktyg hjälper vi företag att steg för steg stärka sin motståndskraft mot cyberrelaterade brott under och efter en incident. Den här rapporten är en del av det arbetet.

Undersökningen *Små företags syn på cybersäkerhet* genomfördes i december 2025 av SSF Stöldskyddsföreningen i samarbete med dåvarande Myndigheten för samhällsskydd och beredskap (MSB), idag Myndigheten för civilt försvar (MCF).

För kontakt: [info@stoldskyddsforeningen.se](mailto:info@stoldskyddsforeningen.se)

Vill ni veta hur ert företag ligger till?

Gör vårt test på: [Säkerhetskollen](#)