

Cybersäkerhet

Mognadsrapport 2026

Vi som skrivit rapporten



Matti Olofsson

Co-founder & CEO, OneMore Secure

Matti Olofsson är medgrundare och VD för OneMore Secure och har över 20 års erfarenhet av entreprenörskap, digitalisering, lärande och cybersäkerhet.



Robert Willborg

Co-founder & CSO, OneMore Secure

Robert Willborg är medgrundare och Chief Security Officer på OneMore Secure och är en cybersäkerhetsevangelist och senior rådgivare. Han är medlem i Altinget, Security Advisory Board och skapare av den internationellt använda STAR-modellen för säkerhetsmedvetenhet.

Utgiven av OneMore Secure AB

Utgåva 2 – Oktober 2026

© OneMore Secure 2026. Alla rättigheter förbehållna.

www.onemoresecure.com

Innehåll

Förord	4
Om vår data	5
Cyberlandskapet	6
Attacker mot leveranskedjan	7
Övergripande insikter	8
Cybersäkerhetsmognad efter bransch	8
Cybersäkerhetsmognad efter område	10
Efter bransch och område	11
NIS2	13
Säker utveckling	15
Leverantörers och kunders mognadsgrad	20
Förändringar över tid	21
Insikter om specifika kontroller	23
Tolv kontroller, en per sida	24
Cybersäkerhetsmognad i Europa	36
Referenser	37
Slutord från PwC	38

Förord

”Vi känner redan till svagheterna. Det avgörande är om vi är beredda att göra något åt dem.”

Förtroende är svårt att bygga och lätt att förlora. Det gäller för en enskild verksamhet, och det gäller för ett land. I en tid då cybersäkerhet i allt högre grad avgör vem som får göra affärer med vem, vem som litar på vem och vem som klarar sig när trycket ökar, blir frågan om hur vi faktiskt mäter och förstår det förtroendet allt viktigare.

Hotbilden har verkligen inte stått still. Utpressningstrojaner fortsätter att kosta verksamheter veckor av driftstörning. Nätfiske riktar sig fortfarande mot människor snarare än system, särskilt i tider av stress och förändring. Statsstödda aktörer har på allvar börjat rikta in sig på leveranskedjor och kritisk infrastruktur, inte för att skada en enskild verksamhet utan för att nå den tillit som håller hela ekonomier samman. Samtidigt har regelverket gått från riktning till skarpt krav. Cybersäkerhetslagen är svensk lag, DORA gäller för finanssektorn och Cyber Resilience Act är på ingående. Cybersäkerhet är därför inte längre en teknisk stödfunktion som kan skjutas åt sidan. Det är en ledningsfråga och det är en kulturfråga. Och i grunden är det en fråga om förtroende. Mellan affärspartners. Mellan myndigheter och medborgare. Mellan Sverige och de partners som förväntar sig att vi håller vår del av kedjan säker.

Cybersäkerhet Mognadsrapport 2026 baseras på data från 1515 verksamheter. Den bekräftar något jag möter i nästan varje styrelserum och ledningsgrupp, att styrka sällan är jämnt fördelad. Vissa bär ett större ansvar än de är rustade för, i synnerhet när vi pratar om leverantörskedjor. Vissa förmågor är starkare än vi tror, andra svagare än vi vill erkänna. Rapporten pekar ut var förtroendet i dag faktiskt håller och var det är tunnare än vi skulle önska, utan att göra någon del av bilden mindre sann än den andra.

Jag väljer att läsa det rapporten belyser, och som kan uppfattas som en varningssignal, som en möjlighet. Varje mätning, oavsett vad den visar, är en chans att se sig själv i spegeln tydligare, mer ärligt. Först när vi har en tydlig bild kan vi fatta rätt beslut utifrån rätt information. Den här rapporten är inte till för att skuldbelägga. Den är tänkt att ge Sverige, verksamhet för verksamhet, ett gemensamt underlag att bygga motståndskraft från.

Robert Willborg

Cybersäkerhetsexpert, rådgivare och sakkunnig

Ett av landets mest omfattande underlag om cybersäkerhetsmognad

1 515

verksamheter

I OneMore Secures (OMS) saas-tjänst för säkerhet i leveranskedjan visualiseras risker och sårbarheter i leveranskedjan. Både kunder och leverantörer svarar på en säkerhetsdeklaration för att åskådliggöra verksamhetens mognadsgrad när det gäller cybersäkerhet. Verksamheten får ett säkerhetsindex (mellan 0 och 5), ett Key Performance Indicator (KPI), som är jämförbart mellan verksamheter. Uppföljningen är automatiserad under hela avtalsperioden.

Rapportens underlag omfattar 1 515 verksamheter. Det gör rapporten till ett av de mest omfattande dataunderlagen om cybersäkerhetsmognad i landet. Analysen fokuserar på svenska verksamheter, så att resultaten blir jämförbara och användbara för svenska beslutsfattare. När det är relevant jämförs resultaten även med andra länder.

Säkerhetsdeklarationen innehåller kontroller som täcker säkerhetskultur, informationssäkerhet, IT-säkerhet och integritetsskydd (GDPR). Det finns även tilläggskontroller för efterlevnad av NIS2, DORA, Säker utveckling, AI-förordningen och OT-säkerhet. I denna rapport redovisar vi data för NIS2 samt för Säker utveckling, då övriga tilläggskontroller för närvarande innehåller för få svar för att vi ska kunna dra tillförlitliga slutsatser. Kontrollerna i tjänstens säkerhetsdeklaration är mappade mot standarder och ramverk såsom ISO 27001, NIST och CIS18. Dessutom är de formulerade med tydlighet och utan onödigt komplexa formuleringar.

All data bygger på självskattningar från verksamheter, vilket ger en bred men subjektiv lägesbild. I takt med att tillämpningen av NIS2 och DORA mognar, väntas tredjepartsvalidering bli ett allt vanligare krav och OMS bedömning är att efterfrågan på oberoende verifiering kommer att öka i omfattning.

Cyberlandskapet

Hotbilden mot vårt digitala samhälle fortsätter att utvecklas snabbt, driven av alltmer sofistikerade cyberhot, geopolitiska spänningar och utbredda svagheter inom de globala leveranskedjorna. Verksamheter i alla sektorer står i dag inför ett flertal samtidiga och överlappande hot.

Utpressningstrojaner (ransomware) fortsätter att vara det mest kostsamma hotet globalt, med driftstörningar som ofta sträcker sig över flera veckor för drabbade verksamheter och kostnader som stiger år för år. Nätfiske, phishing, utgör fortsatt den initiala angreppsmetoden till många incidenter och riktar sig främst mot mänskliga sårbarheter, särskilt i tider av organisatorisk stress eller förändring. Överbelastningsattacker (DDoS) används både som störning i sig och som distraktion vid mer komplexa angrepp. Attacker mot leveranskedjan fortsätter visa att sårbarheter hos tredje part ofta fungerar som språngbräda in i annars skyddade miljöer. Detta är en utveckling som konkretiserades under en rad attacker sommaren 2026 och som visade hur snabbt en enskild svag länk i mjukvaruförsörjningen kan spridas vidare. Avancerade ihållande hot och statligt stödd cyberkrigföring har fortsatt öka i omfattning, där kritisk infrastruktur, media och finanssektorer utgör prioriterade mål.

Samtidigt har geopolitiska spänningar ökat de statligt sponsrade cyberattackerna som riktar sig mot kritisk infrastruktur och känsliga sektorer, vilket förstärker behovet av robusta cybersäkerhetsramar och proaktiva försvarsmekanismer. I Sverige delades MSB (numera Myndigheten för Civil Försvar– MCF) och CERT-SE upp den 1 juli 2026, då CERT-SE:s verksamhet gick in i Nationella cybersäkerhetscentret. Det är en strukturell förändring väl värd att känna till för alla verksamheter som behöver rapportera incidenter eller söka vägledning framöver.

Sammantaget kan vi konstatera att cybersäkerhet inte längre är en teknisk stödfunktion eller en kostnadspost, utan en strategisk förutsättning och investering för stabil verksamhetskontinuitet. Det krävs en grundläggande cyberhygien för att få göra affärer, licence to operate. Den ökade kopplingen mellan hotaktörer och nationella intressen innebär dessutom att hoten är samhällspolitiska och inte bara ekonomiska.

Attacker mot leveranskedjan

Attacker mot leveranskedjan är en realitet där angriparen utnyttjar asymmetrin mellan små leverantörers svaga skydd och större kunders beroende av dem. Angripare riktar in sig på tredjepartsaktörer med bristfälliga cybersäkerhetsrutiner, för att komma åt deras kunders data.

Kända incidenter som SolarWinds, Kaseya och MOVEit står ännu som talande exempel på hur en enskild sårbar leverantör kan bli systemhotande för en verksamhet. I en alltmer sammankopplad värld räcker det att en aktör i ekosystemet är oskyddad för att hela kedjan ska bli sårbar. Enligt ENISA (Europeiska cybersäkerhetsmyndigheten) kan en majoritet av de cyberattacker som drabbar större verksamheter härledas till tredje part. Angreppen sker ofta via bristande segmentering, svaga autentiserings- och uppdateringsrutiner, eller bristfälligt krypterad dataöverföring mellan parter.

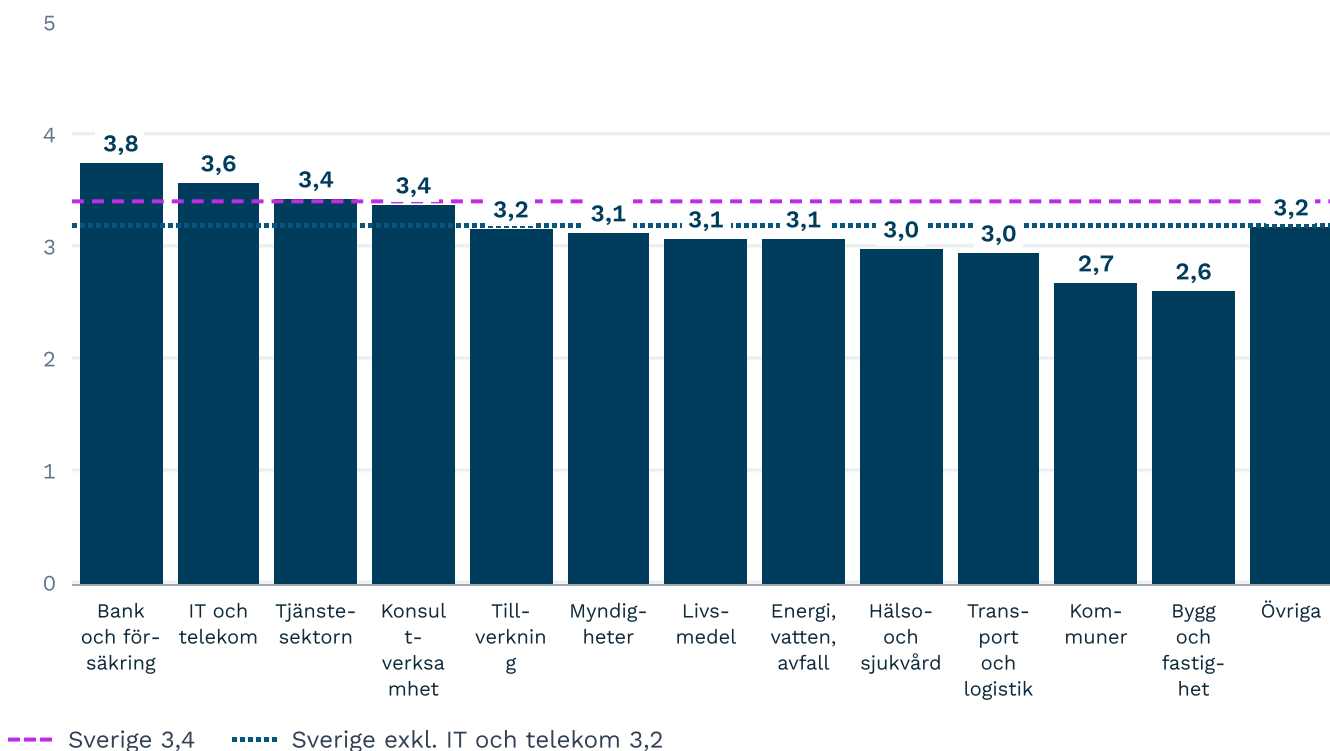
Det är mot den bakgrunden som årets resultat väcker särskild oro: mognadsgraden för säkra leveranskedjor är i dag den enskilt svagaste kontrollen i hela rapporten. Drygt 44 procent av de svenska verksamheterna har en låg mognadsgrad på området, och skillnaden mellan branscher är liten. Detta tyder dessvärre på att det verkar röra sig om en genomgående nationell svaghet snarare än ett nischproblem hos enskilda sektorer. OMS bedömning är att detta till stor del hänger samman med att leverantörsstyrning kräver samordning över organisatoriska gränser, något som är svårare att äga och resurssätta än interna kontroller. Och att många verksamheter fortfarande saknar en systematisk process för att klassificera och följa upp sina leverantörers säkerhetsnivå.

EU:s NIS2-direktiv, sedan 15 januari 2026 svensk rätt genom Cybersäkerhetslagen och Cyber Resilience Act ställer explicita krav på att verksamheter tar ansvar för säkerheten i sin leveranskedja, både juridiskt och operativt. Riskklassificering av leverantörer, tydliga säkerhetskrav i avtal och löpande uppföljning är därmed inte längre frivilliga åtgärder utan rättsliga skyldigheter. Att mognadsgraden ändå ligger så lågt är enligt OMS bedömning en anmärkning som branschen och lagstiftaren behöver ta på störst allvar. Konsekvenserna är konkreta. En osäker leveranskedja underminerar den grundläggande cyberhygien i hela ekosystemet, eftersom en enskild svag länk kan sprida en attack vidare till annars välskyddade verksamheter. Det försvagar också samhällets samlade förmåga till kontinuitet, eftersom kritiska funktioner i praktiken är beroende av leverantörer vars säkerhetsnivå sällan är verifierad. Och det påverkar ytterst konkurrenskraften. Svenska verksamheter som inte kan styrka en säker leveranskedja riskerar att förlora affärer till svenska såsom utländska aktörer, som kan visa att de har kontroll, samtidigt som internationella kunder och partners i allt högre grad ställer denna typ av krav som villkor för samarbete.

Cybersäkerhetsmognad efter bransch

Den samlade mognadsgraden bland svenska verksamheter uppgår till 3,4 för 2026. IT- och telekombranschen drar upp genomsnittet eftersom de visar en högre mognadsgrad samt utgör en stor andel av underlaget; exkluderas branschen landar den svenska mognadsgraden på 3,2. Det är den senare siffran som enligt OMS bedömning bäst speglar det bredare svenska näringslivets faktiska mognadsnivå, eftersom IT- och telekomsektorns starka resultat annars riskerar att dölja svagheter i övriga delar av ekonomin.

Figur 1 Mognadsgrad per bransch, 2026



Skillnaden mellan branscher är stor, från ett snitt på 2,6 till 3,8 på en femgradig skala. Bank och försäkring visar högst mognadsgrad med 3,8, en nivå som enligt OMS bedömning sannolikt speglar att de skärpta kraven under DORA blottlägger brister i självskattningen som tidigare inte syntes lika tydligt, snarare än att den faktiska säkerhetsnivån försämrats. Näst högst ligger IT och telekom 3,6, följt av tjänstesektorn och konsultverksamhet 3,4.

I den andra änden av skalan har bygg- och fastighetsbranschen den lägsta mognadsgraden av alla branscher, med ett snitt om 2,6. Kommuner kommer strax efter med 2,7.

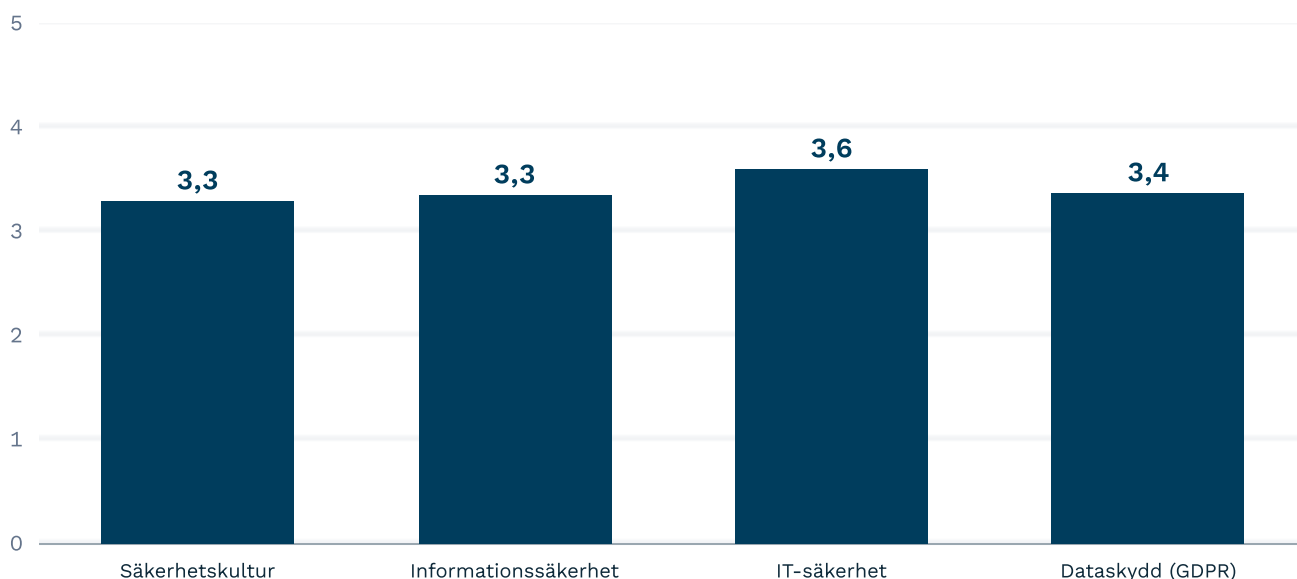
Cybersäkerhetsmognad efter bransch (forts.)

En bild OMS ser som ett tecken på systematiskt underinvesterade säkerhetsfunktioner snarare än enstaka eftersläntrare. Transport och logistik samt hälso- och sjukvård med 3,0 hanterar omfattande samhällskritiska funktioner respektive känslig persondata utan att mognadsgraden i dag speglar det ansvaret. Energi, vatten och avfall samt livsmedelsindustrin med 3,1 ligger också under riksgenomsnittet, vilket är särskilt bekymrande givet att dessa sektorer utgör en del av samhällets kritiska infrastruktur och står inför förhöjda risker från både kriminella och statsstödda aktörer. Sammantaget innebär den breda spridningen mellan branscher att Sveriges samlade motståndskraft är ojäm: kedjan är inte starkare än sin svagaste sektor och flera av de lägst rankade branscherna levererar funktioner som resten av samhället är beroende av.

Cybersäkerhetsmognad efter område

Bryter vi ner resultatet per område är IT-säkerhet det område där svenska verksamheter presterar bäst, med en mognadsgrad på 3,6. Dataskydd enligt GDPR följer på 3,4, tätt följt av informationssäkerhet och Säkerhetskultur med 3,3. Mönstret är tydligt: den mjuka, organisatoriska sidan av cybersäkerhet halkar efter den tekniska.

Figur 2 Mognadsgrad per område, Sverige 2026



Att just säkerhetskultur är svagast är särskilt bekymmersamt eftersom det är det område som i störst utsträckning avgör hur väl tekniska skyddsåtgärder faktiskt används i praktiken. En brandvägg eller kryptering hjälper föga om verksamheten inte förstår varför den finns eller hur den ska hanteras. Enligt OMS bedömning är detta glapp mellan teknisk och organisatorisk mognad en av de mest underskattade riskerna i svenskt näringsliv i dag: det urholkar den vardagliga cyberhygien, eftersom även välinvesterad teknik i praktiken kringgås av mänskligt beteende. Det gör investeringar i teknisk säkerhet mindre lönsamma än de borde vara, vilket i förlängningen påverkar verksamheters konkurrenskraft när säkerhetsbudgeten inte ger fullt utbyte.

OMS bedömning

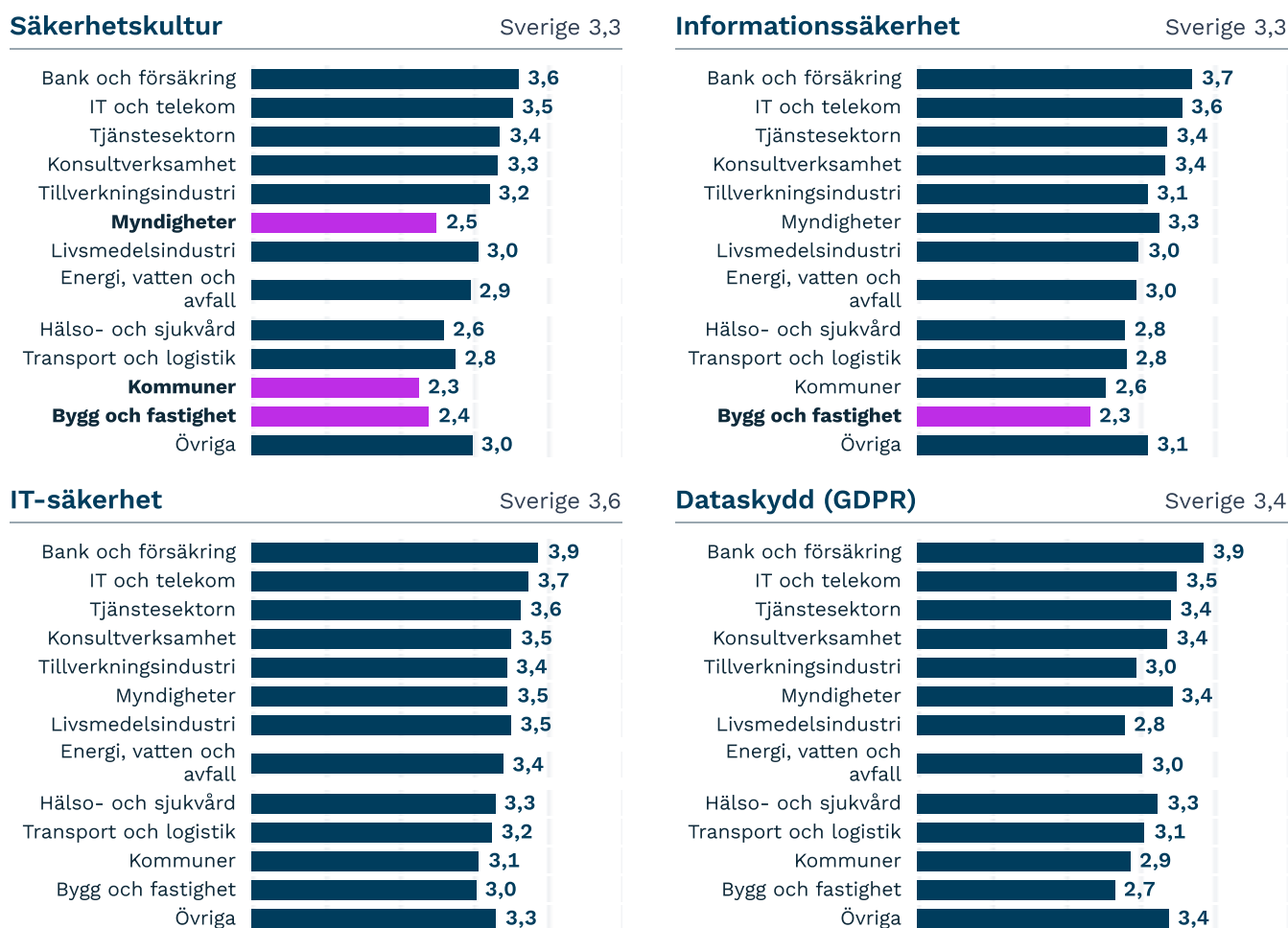
Glappet mellan teknisk och organisatorisk mognad är en av de mest underskattade riskerna i svenskt näringsliv i dag: även välinvesterad teknik kringgås i praktiken av mänskligt beteende.

Cybersäkerhetsmognad efter bransch och område

Bryter vi ner data per bransch och område sticker kommuner, bygg- och fastighetsbranschen samt myndigheter ut särskilt negativt inom säkerhetskultur, samtliga med en mognadsgrad under 2,6 på det området. Att myndigheter och kommuner återfinns i botten av den här listan är anmärkningsvärt givet den roll offentlig förvaltning spelar för medborgarnas förtroende: en myndighet med svag säkerhetskultur riskerar inte bara egna incidenter utan urholkar tilliten till digital offentlig service i stort.

Inom dataskydd är det bygg- och fastighetsbranschen som uppvisar lägst mognadsgrad, med livsmedelsindustrin och kommuner strax därefter. Alla med ett snitt under 3,0. Det är anmärkningsvärt eftersom GDPR har varit i kraft sedan 2018. Att flera branscher, åtta år senare, fortfarande inte närmat sig en godtagbar nivå tyder, enligt OMS bedömning, snarare på strukturellt låg prioritering och bristande resurssättning än på att en pågående mognadsresa förklarar avståndet. Konsekvensen är direkt: bristande dataskydd innebär förhöjd risk för sanktioner, förtroendeskada och i en tid då persondata alltmer används i geopolitiska syften, en sårbarhet som sträcker sig bortom det rent regulatoriska.

Figur 3 Mognadsgrad per bransch och område



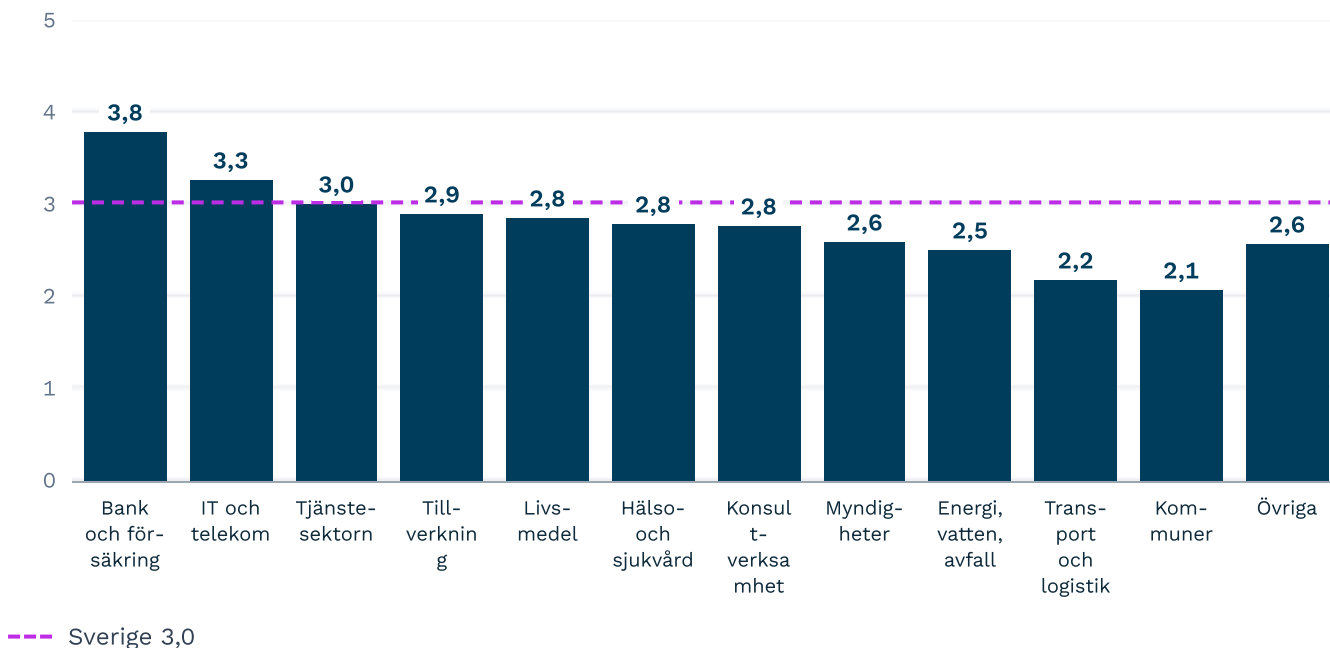
■ Mognadsgrad ■ Under 2,6 Branscherna står i samma ordning i alla fyra delar. Skala 0–5.

NIS2

NIS2, implementerat i Sverige som Cybersäkerhetslagen, är sedan den 15 januari 2026 gällande rätt. Mognaden i det här avsnittet mäts mot ett regelverk som faktiskt måste efterlevas, inte en förväntad kravbild, vilket gör siffrorna särskilt relevanta att ta på allvar.

Den samlade NIS2-mognaden bland svenska verksamheter är 3,0. Kommuner har ett snitt på 2,1 och transport- och logistikbranschen med 2,2. I den andra änden toppar bank och försäkring listan med 3,8, följt av IT och telekom på 3,3. Att bank och försäkring ligger högst, vilket enligt OMS bedömning, speglar att dessa branscher redan omfattas av närliggande regelverk såsom DORA och därför har längre erfarenhet av strukturerad regelefterlevnad.

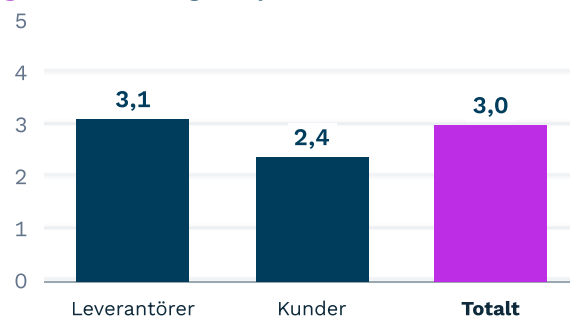
Figur 4 NIS2-mognad per bransch



NIS2 (forts.)

Det finns också en tydlig skillnad mellan olika verksamheter: leverantörer har en NIS2-mognad på 3,1, medan kunderna ligger på 2,4. Gapet kan delvis förklaras med att många leverantörer är IT-företag som generellt uppvisar en högre mognadsgrad, men det är ändå värt att uppmärksamma, eftersom det i grunden är kundernas ansvar enligt NIS2 att ställa krav nedåt i sin leveranskedja. Ett stort mognadsgap gör det arbetet svårare i praktiken och riskerar att skapa en falsk trygghet hos kunder som förlitar sig på sina leverantörer utan att själva ha förmåga att bedöma eller följa upp leverantörers säkerhetsnivå, vilket i förlängningen är en fråga om både cyberhygien och nationell motståndskraft.

Figur 5 NIS2-mognad per roll



Säker utveckling

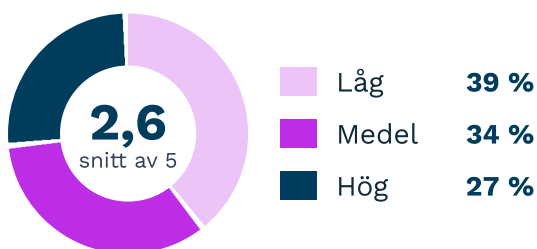
Digitaliseringen har gjort mjukvara till en grundläggande komponent i nästan alla verksamhet. Programvara finns inte längre bara i traditionella IT-system, utan också i fordon, industrisystem, medicinteknik, energisystem, fastigheter, uppkopplade produkter och samhällskritisk infrastruktur. Det innebär att sårbarheter som introduceras under utvecklingen kan få konsekvenser långt utanför det enskilda systemet eller den organisation som utvecklat det.

Säker utveckling handlar därför om att flytta cybersäkerheten från slutet av utvecklingsprocessen till hela produktens och mjukvarans livscykel. Säkerhetskrav behöver definieras redan när ett system eller en produkt planeras, följas upp under utvecklingen och kompletteras med kontinuerlig testning, hantering av tredjepartsberoenden och sårbarheter samt säkra processer för förändringar och uppdateringar.

Årets data visar att svenska verksamheter fortfarande har en rad utmaningar framför sig vad gäller sin cyberförmåga.

Den genomsnittliga mognadsgraden för Säker utveckling bland svenska verksamheter är 2,6 av 5. Av samtliga svar på de tio kontrollerna ligger 39 procent på en låg mognadsnivå och 34 procent på medelnivå, medan endast 27 procent når en hög nivå. Det visar att säker utveckling fortfarande inte är en fullt etablerad och systematisk process hos en majoritet av de verksamheter som ingår i underlaget.

Figur 6 Andel svar per mognadsnivå, samtliga tio kontroller



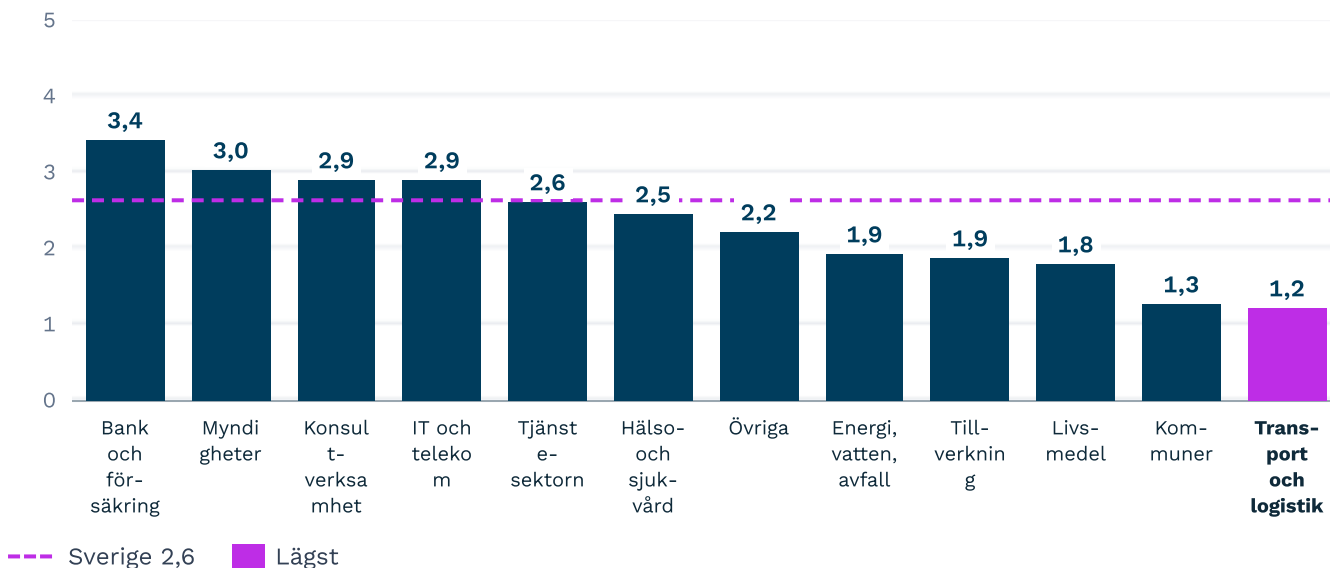
Stora skillnader mellan branscher

Skillnaderna mellan branscherna är betydande. Bank och försäkring har högst mognadsgrad med 3,4, medan IT och telekom ligger på 2,9. Att inte ens IT- och telekomsektorn når nivå 3 i genomsnitt är värt att uppmärksamma eftersom just denna sektor utvecklar och förvaltar en stor del av de digitala tjänster som andra verksamheter är beroende av.

Säker utveckling (forts.)

Betydligt lägre nivåer finner vi bland annat inom energi och samhällsnyttiga tjänster 1,9, tillverkningsindustrin 1,9, livsmedelsindustrin 1,8, kommuner 1,3, samt transport och logistik 1,2. Mönstret är tydligt. Flera av de sektorer där digitala system har stor betydelse för fysisk verksamhet och samhällskritiska funktioner uppvisar samtidigt låg mognad inom säker utveckling.

Figur 7 Säker utveckling per bransch



Detta sammantaget skapar en särskild typ av risk. När digitalisering och uppkoppling ökar snabbare än förmågan att utveckla och förvalta systemen på ett säkert sätt, riskerar teknisk skuld och säkerhetsskuld att byggas upp i samhällets digitala infrastruktur.

Automatiserad säkerhetstestning är den största svagheten

Bryter vi ner resultaten på de tio kontroller som ingår framträder ytterligare ett tydligt mönster.

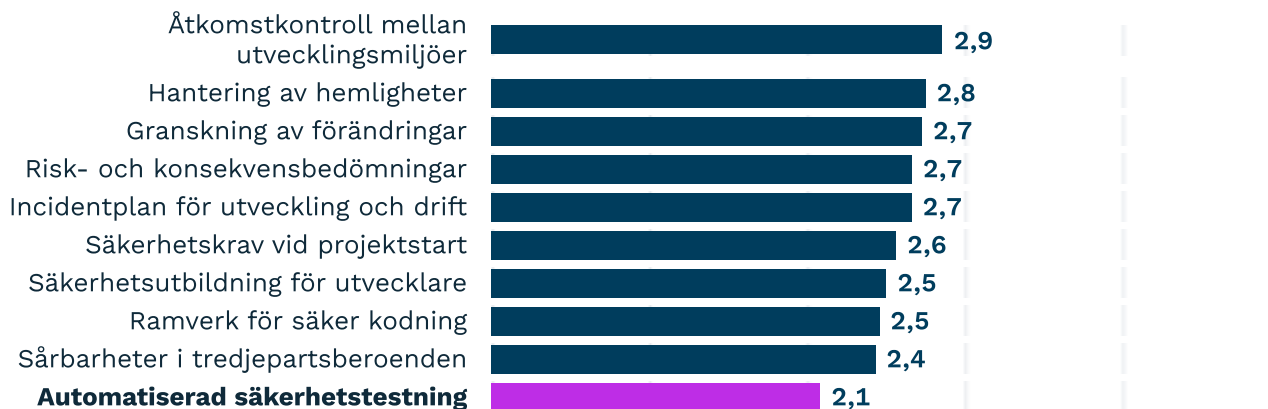
Den kontroll som visar på svagast mognad är om automatiserad säkerhetstestning integrerad i utvecklings- och förändringsprocessen, med en genomsnittlig mognadsgrad på endast 2,1. 27 procent av verksamheterna svarar att de helt saknar detta.

Även standardiserade ramverk (som OWASP eller SANS Top 25 eller motsvarande) för säker kodning är lågt med 2,5 och hantering och övervakning av sårbarheter i tredjepartsberoenden 2,4 ligger på en låg nivå. Den senare är särskilt viktigt i moderna utvecklingsmiljöer, där en betydande del av en applikation ofta består av komponenter, bibliotek och paket som verksamheten inte själv har utvecklat.

Säker utveckling (forts.)

Något bättre ser det ut när det gäller åtkomstkontroller mellan separerade utvecklingsmiljöer 2,9 och säker hantering av hemligheter och autentiseringsuppgifter 2,8. Men inte heller här når genomsnittet minimikravet på grundläggande cyberförmåga.

Figur 8 Mognadsgrad per kontroll



27 procent saknar helt automatiserad säkerhetstestning. Skala 0–5.

Resultaten pekar därmed på ett bredare problem än enskilda tekniska säkerhetskontroller. Säkerhet är ännu inte konsekvent integrerad i själva utvecklingsprocessen.

Från DevOps till DevSecOps

Under lång tid har utveckling framför allt handlat om att kunna leverera nya funktioner snabbare. DevOps har gjort det möjligt att korta utvecklingscyklerna genom automation och tätare integration mellan utveckling och drift. Nästa steg är att säkerheten får samma naturliga plats i processen.

Det är kärnan i DevSecOps: säkerheten ska inte vara en kontrollstation före produktionsättning. Det ska vara en integrerad och kontinuerlig del av hela utvecklingsprocessen.

Säkerhetskrav behöver finnas med från projektstart. Kod och komponenter behöver kunna testas automatiskt. Tredjepartsberoenden behöver identifieras och följas upp. Hemligheter som API-nycklar och autentiseringsuppgifter måste hanteras säkert. Förändringar måste vara spårbara och riskbedömningar behöver genomföras kontinuerligt. Utvecklare behöver dessutom ha rätt säkerhetskompetens.

Ju senare en sårbarhet upptäcks, desto större blir normalt både kostnaden och komplexiteten för att åtgärda den. Säker utveckling är därför inte bara en säkerhetsfråga, det är också en fråga om kvalitet, effektivitet och affärsrisk.

Cyber Resilience Act förändrar spelplanen

Behovet av säker utveckling förstärks kraftigt genom EU Cyber Resilience Act (CRA). Förordningen innebär att cybersäkerhet för produkter med digitala element i betydligt större utsträckning blir ett produktansvar.

CRA ställer krav på cybersäkerhet genom produktens livscykel. Från planering, design och utveckling, till underhåll och hantering av sårbarheter. Produkter med digitala element ska utvecklas med en cybersäkerhetsnivå som är lämplig utifrån riskerna och regelverket ställer bland annat krav på säker standardkonfiguration, hantering av sårbarheter och möjligheten att distribuera säkerhetsuppdateringar.

Tidplanen gör frågan särskilt aktuell under 2026. CRA skyldigheter att rapportera aktivt utnyttjade sårbarheter och allvarliga säkerhetsincidenter började tillämpas den 11 september 2026. Huvuddelen av CRA börjar därefter tillämpas den 11 december 2027.

Det innebär att organisationer som utvecklar produkter med digitala element inte kan vänta till 2027 med att påbörja arbetet. Förmågan att identifiera, dokumentera, hantera och rapportera sårbarheter förutsätter processer, kompetens och tekniska verktyg som behöver byggas upp långt tidigare.

Säker utveckling blir en leveranskedjefråga

CRA bör dessutom ses tillsammans med NIS2. Medan NIS2 i stor utsträckning ställer krav på hur verksamheter hanterar sina cyberrisker och sina leverantörskedjor, flyttar CRA ansvaret närmare de produkter och den mjukvara som kedjan faktiskt består av.

Detta skapar två perspektiv av samma ansvar.

Organisationer behöver kunna ställa krav på säkerheten i de digitala produkter och tjänster de köper. Tillverkare och utvecklare behöver samtidigt kunna visa att säkerheten har varit en integrerad del av utvecklingen och att sårbarheter hanteras under produktens livscykel.

Säker utveckling blir därmed också en central del av säkerheten i leveranskedjan. En organisation kan ha hög intern cybersäkerhetsmognad men ändå exponeras för betydande risk om den bygger sin verksamhet på mjukvara, komponenter eller digitala produkter som utvecklats utan motsvarande säkerhetsnivå.

Från att skydda systemen till att bygga dem säkra

Årets resultat visar ett tydligt gap mellan hur beroende Sverige har blivit av mjukvara och hur systematiskt vi arbetar med säkerheten när denna mjukvara utvecklas.

Det är ett gap som blir allt svårare.

Historiskt har cybersäkerhet till stor del handlat om att skydda redan driftsatta system genom brandväggar, antivirus, övervakning och andra skyddslager. Det kommer fortsatt att behövas, men det räcker inte. När samhället blir alltmer beroende av mjukvaror och applikationer av olika slag måste säkerheten börja tidigare.

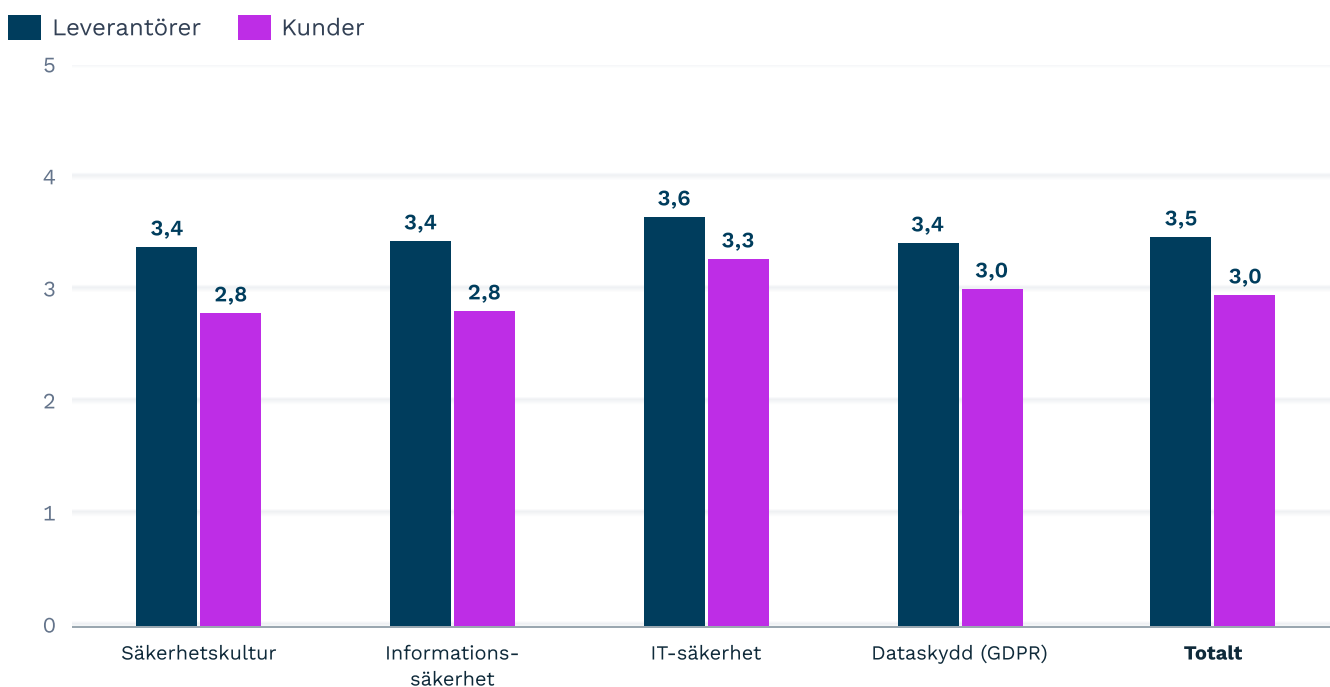
Vi behöver gå från att försöka skydda det vi redan har byggt till att bygga det säkert från början.

Cyber Resilience Act innebär att dessa säkerhetskrav blir lagstadgade. Årets mognadsrapport visar att det för många svenska verksamheter fortfarande återstår mycket att göra.

Leverantörers och kunders mognadsgrad

Fördjupar vi oss i skillnaderna generellt ligger leverantörernas mognadsgrad i dag på 3,5, medan kundernas ligger på 3,0. Att båda grupperna befinner sig under den nivå som skulle krävas för att med god marginal möta NIS2 och angränsande regelverk stärker OMS bedömning att det rör sig om ett brett, delat mönster i den svenska marknaden snarare än en enskild gruppssärskilda utmaning.

Figur 9 Leverantörer och kunder per område

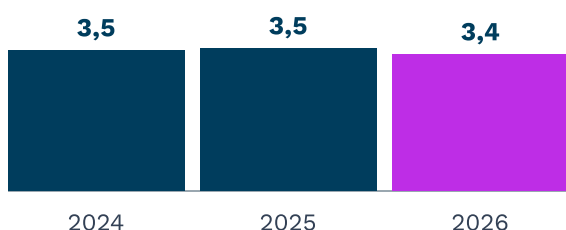


De som är registrerade som leverantörer har högre mognadsgrad än kunderna i plattformen inom samtliga fyra områden, vilket delvis kan förklaras med att många leverantörer är IT-företag som generellt har en högre mognadsgrad, medan kunderna återfinns i alla branscher. Skillnaden mellan kunder och leverantörer är minst inom IT-säkerhet, vilket tyder på att den tekniska lägstanivån är mer jämnt spridd i marknaden än den organisatoriska och kulturella mognaden. Det gap som ändå kvarstår är en påminnelse om att kedjan bara är så stark som den svagaste länken; för kunder som själva ligger lågt är det svårt att ställa trovärdiga krav uppåt eller nedåt i sin egen leveranskedja, vilket håller tillbaka hela ekosystemets samlade motståndskraft.

Förändringar över tid

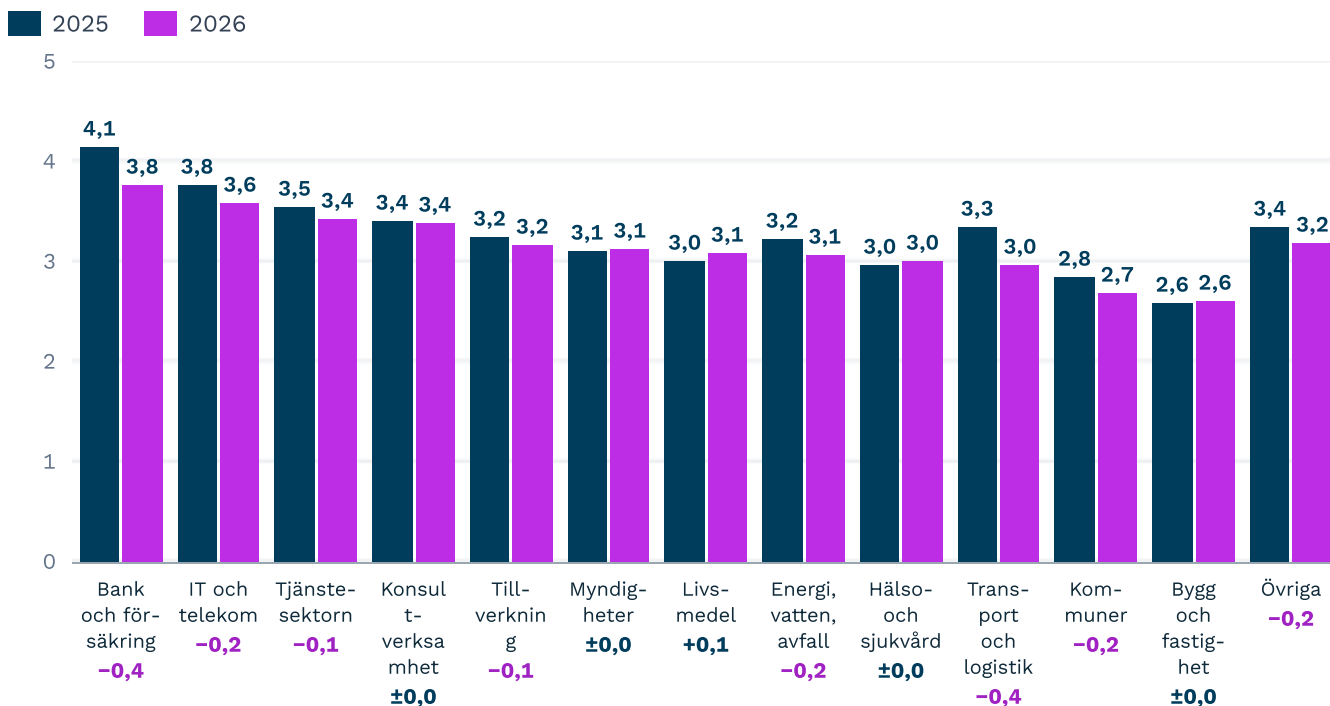
Efter att mognadsgraden bland svenska verksamheter steg marginellt mellan 2024 och 2025, har den sjunkit mellan 2025 och 2026, från 3,5 till 3,4. Detta beror sannolik en del på att kontrollerna i OneMore Secures deklaration inte bara förfinats och preciserats, utan också att det har tillkommit kontroller med hänsyn till omvärlds- och regulatoriska krav. Men nedgången beror till stor del att mer data nu är tillgänglig och en tydligare bild av mognaden, nationellt och internationellt, nu går att analysera.

Figur 10 Sverige totalt



Nedgången är bred och syns i nästan samtliga branscher. Bank och försäkring samt transport och logistik har tappat mest i absoluta tal, båda med omkring 0,4 enheter, medan endast livsmedelsindustrin visar en positiv utveckling, om än en svag sådan.

Figur 11 Förändring per bransch, 2025 till 2026



Siffran under varje bransch visar förändringen.

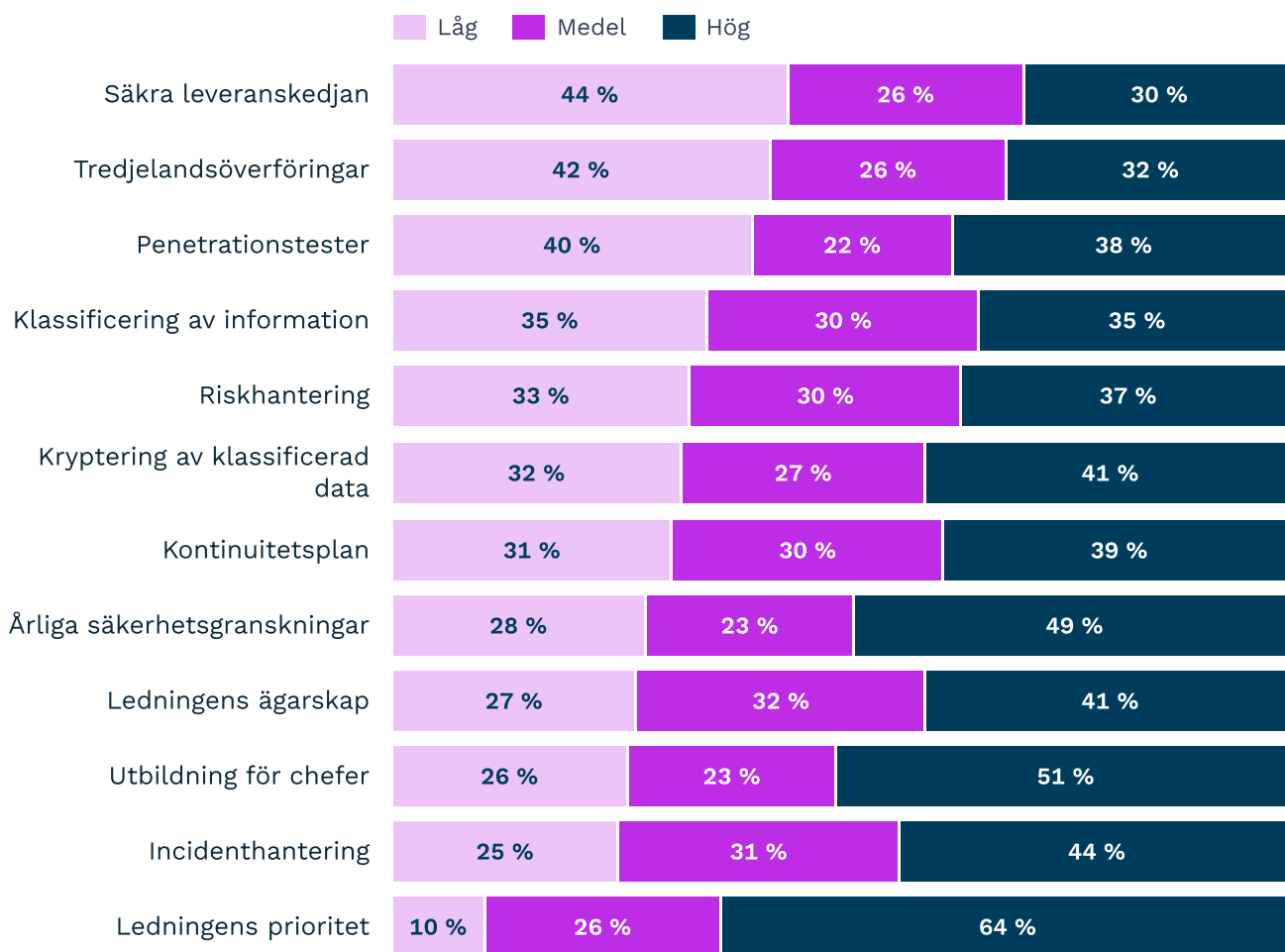
Förändringar över tid (forts.)

Vi vill vara transparenta kring en möjlig delförklaring: årets underlag är betydligt större än förra årets och en stor andel nya verksamheter har tillkommit i populationen under året. Om de nytillkomna verksamheterna i genomsnitt har en lägre mognadsgrad än de som redan fanns med i fjolårets underlag, väger de ner det samlade genomsnittet även om enskilda, redan etablerade verksamheter fortsatt förbättrar sig. Vi kan utifrån denna rapports data inte fastställa exakt hur stor del av nedgången som förklaras av detta jämfört med en faktisk försvagning hos befintliga verksamheter, men vi bedömer att det sannolikt är en delförklaring, inte hela förklaringen, givet hur brett nedgången slår även bland etablerade branscher och kontroller. Detta är precis den typ av begränsning i självskattningsdata vi flaggade för redan i förra årets rapport och den förtjänar att tas på största allvar när resultaten tolkas.

Insikter om specifika kontroller

Rapporten fokuserar på ett urval av kontroller som belyser mognadsgraden inom några specifika och avgörande områden. Vi analyserar nuläget, möjliga bakomliggande faktorer och vilka konsekvenser utvecklingen kan få.

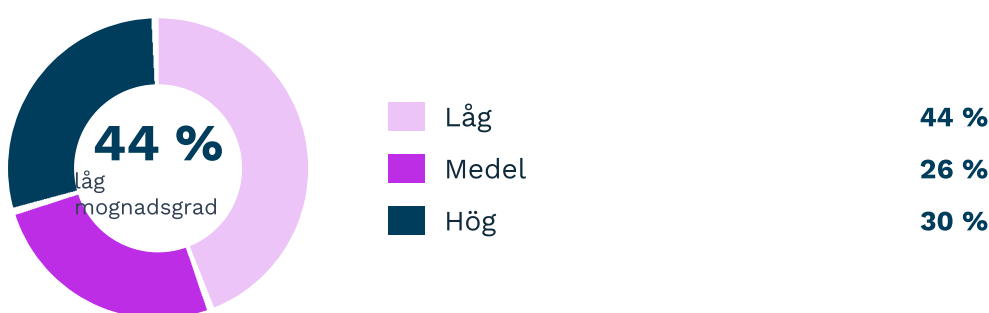
Figur 12 Andel verksamheter per mognadsnivå och kontroll



Säkra leveranskedjan

Kontrollen för säkra leveranskedjor sticker ut som en av de allra svagaste i hela rapporten. Drygt 44 procent av de svenska verksamheterna har en låg mognadsgrad och endast 30 procent når en hög mognadsgrad. OMS bedömning är att detta till stor del beror på att leverantörsstyrning kräver strukturer, avtal och uppföljningsrutiner som sträcker sig utanför den egna organisationen, vilket gör kontrollen svårare att äga och resurssätta än rent interna säkerhetsåtgärder.

Figur 13 Mognadsnivå, säkra leveranskedjan



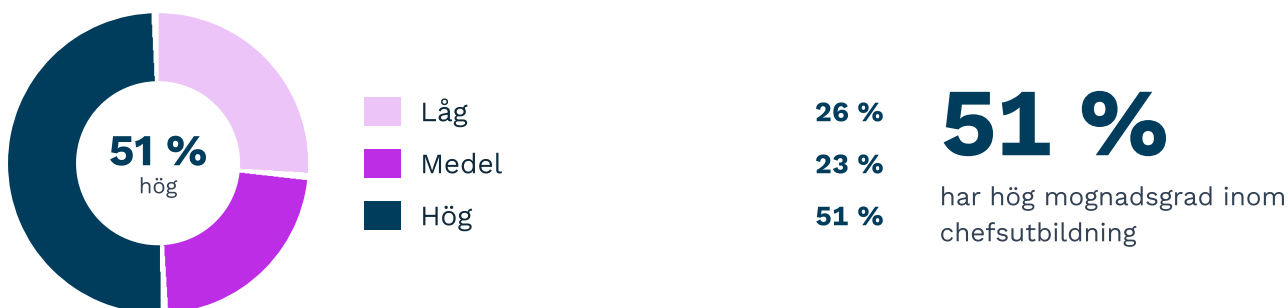
Detta är särskilt allvarligt i ett läge där cybersäkerheten blivit ett geopolitiskt verktyg. Statliga och statsstödda aktörer riktar sig i allt högre grad mot leverantörer i väst för att nå in i samhällskritisk infrastruktur, det såg vi inte minst i incidenten kring Miljödata. I en sådan omvärld kan Sveriges verksameters låga mognad vad gäller säkerhet i leveranskedjan inte försvaras. Det handlar inte längre bara om regelefterlevnad enligt NIS2 och DORA, utan om nationell motståndskraft. Konsekvenserna är flerdimensionella: för den enskilda verksamheten innebär det försämrade cyberhygien, eftersom osäkra leverantörer i praktiken blir en okontrollerad ingång till den egna miljön. För samhället i stort innebär det en försvagad förmåga till kontinuitet, eftersom kritisk infrastruktur ofta är beroende av just de leverantörsled som visar sig svagast. Och för näringslivet är det en konkurrensfråga: verksamheter som inte kan styrka en säker leveranskedja riskerar att förlora upphandlingar och partnerskap till aktörer som kan det, samtidigt som internationella kunder i allt högre grad kräver sådan dokumentation som villkor för affärsrelationen. Att den här kontrollen idag är en av rapportens svagaste är, enligt OMS bedömning, årets enskilt viktigaste varningssignal. NIS2 är dessutom särskilt tydlig på denna punkt genom artiklarna 21, 22 och 23.

OMS bedömning

Att den här kontrollen idag är en av rapportens svagaste är årets enskilt viktigaste varningssignal. NIS2 är särskilt tydlig på denna punkt genom artiklarna 21, 22 och 23.

Utbildning för chefer

Figur 14 Mognadsnivå, utbildning för chefer

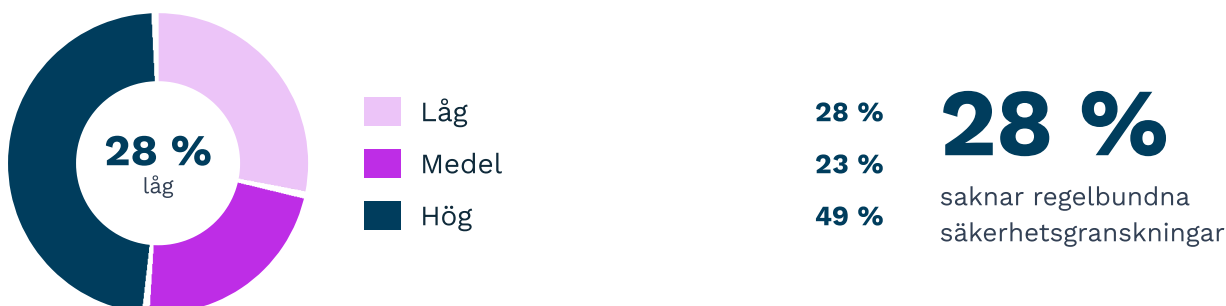


Att chefer förstår cybersäkerhetsrisker kopplade till sina roller är avgörande, eftersom beslutsfattande under tidspress eller osäkerhet ofta är den svagaste länken vid incidenter. I dag har 51 procent av verksamheterna en hög mognadsgrad inom chefsutbildning, vilket lämnar knappt hälften av det svenska näringslivet med ett ledarskap som saknar tillräcklig träning i att fatta rätt beslut när en incident inträffar.

Sverige befinner sig i ett skärpt säkerhetsläge, där påverkan och kognitiv manipulation blivit ett allt vanligare inslag vid cyberoperationer, vilket enligt OMS bedömning gör bristen på chefsutbildning särskilt allvarlig just nu: chefer som inte är tränade i att känna igen och hantera denna typ av påverkan riskerar att fatta ogenomtänkta beslut i skarpa lägen. NIS2 betonar dessutom behovet av ledningsansvar och personlig ansvarsskyldighet vid säkerhetsbrister, vilket gör chefsutbildning till ett konkret ansvar enligt EU-rätt snarare än en god vilja. Konsekvensen av att så många chefer i dag saknar tillräcklig utbildning är att den grundläggande cyberhygien brister redan på ledningsnivå, att verksamheternas kontinuitetsförmåga försvagas eftersom kritiska beslut i en kris riskerar att fattas utan rätt kunskap och att svenska verksamheter riskerar personligt ansvar och förtroendeskada som i förlängningen påverkar konkurrenskraften gentemot aktörer med bättre rustat ledarskap.

Årliga säkerhetsgranskningar

Figur 15 Mognadsnivå, årliga säkerhetsgranskningar

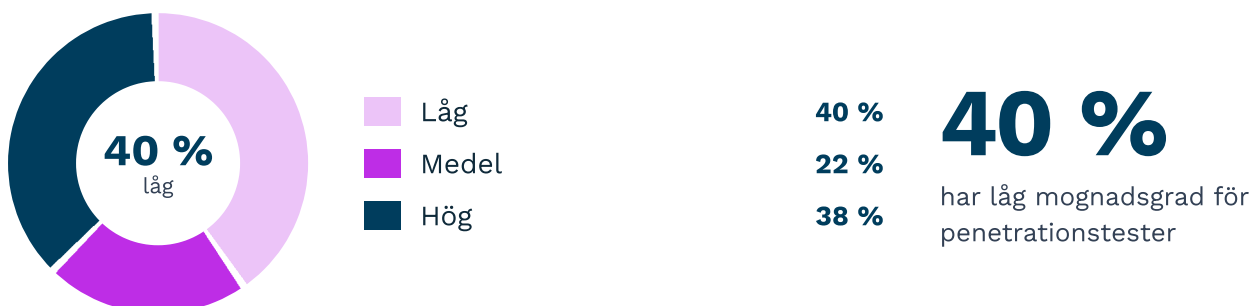


28 procent av verksamheterna saknar i dag regelbundna säkerhetsgranskningar, vilket innebär att mer än var fjärde aktör står helt utan årlig kontroll. Säkerhetsgranskningar är inte en formalitet. De är navet i det kontinuerliga förbättringsarbetet och utan dem saknas både lägesbild och kontroll över om identifierade brister faktiskt åtgärdas.

Från ett riskperspektiv är detta särskilt oroande eftersom hotbilden förändras snabbt, både tekniskt och geopolitiskt. Både NIS2 och kända ramverk ställer krav på löpande intern kontroll, dokumentation och uppföljning, men våra data visar att detta fortfarande inte är en självklar del av den operativa kulturen i många svenska verksamheter. Det tyder det på att säkerhetsarbetet i stor utsträckning fortfarande är reaktivt snarare än förebyggande: brister upptäcks när något redan har hänt, inte innan. Det är en svag grund för cybersäkerhet i vardagen och gör det svårare att lita på att en verksamhets kontinuitetsförmåga faktiskt håller när den provas.

Penetrationstester

Figur 16 Mognadsnivå, penetrationstester

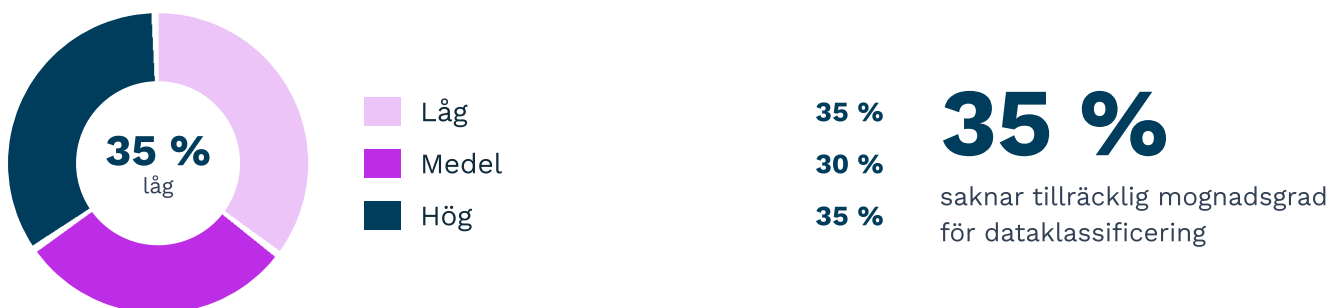


Nästan 40 procent av verksamheterna har i dag en låg mognadsgrad avseende penetrationstester. Det är oroväckande med tanke på vilken central roll dessa säkerhetstester spelar för att upptäcka sårbarheter innan en angripare gör det.

Penetrationstester är en etablerad metod för att simulera verkliga attacker och validera försvarsförmågan i praktiken. Det räcker inte att ha säkerhetssystem på plats; det är minst lika viktigt att testa om de faktiskt håller. Flera incidenter har visat att brister ofta upptäcks först efter att skadan är skedd, brister som hade kunnat förhindras med regelbundna tester. Att så många verksamheter saknar denna grundläggande kontroll innebär enligt OMS bedömning att sårbarheter i praktiken förblir okända tills de utnyttjas, vilket urholkar cyberhygien, förlänger återställningstiden när en incident väl inträffar och därmed försvagar den samlade kontinuitetsförmågan. Att vara förberedd är i dag inte bara en teknisk fråga. Det är en ledningsfråga, ett ansvar och en direkt indikator på verksamhetens motståndskraft.

Klassificering av information

Figur 17 Mognadsnivå, klassificering av information

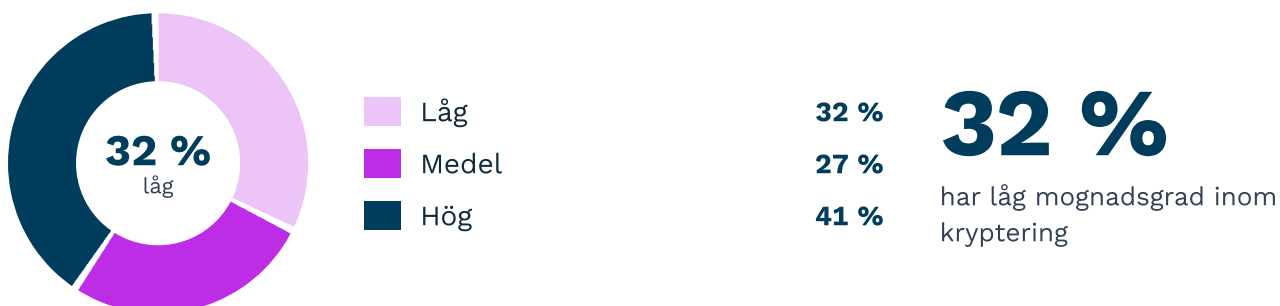


Dataklassificering är grunden för att kunna skydda information på rätt sätt. Utan den vet man inte vilka tillgångar som är mest skyddsvärda, vilket gör det omöjligt att prioritera insatser. I dag saknar drygt en tredjedel av verksamheterna en tillräcklig mognadsgrad kopplad till dataklassificering.

Det innebär att en betydande andel av verksamheterna riskerar att behandla känslig information som vilken data som helst, vilket ökar risken för läckor, felaktig åtkomst och bristande efterlevnad av regelverk som GDPR och NIS2. Informationsläckor utnyttjas idag både för ekonomisk vinning och som påverkansmedel i hybridkonflikter. Bristande dataklassificering är därför en nationell sårbarhet, inte enbart en intern kvalitetsfråga.

Kryptering av klassificerad data

Figur 18 Mognadsnivå, kryptering av klassificerad data

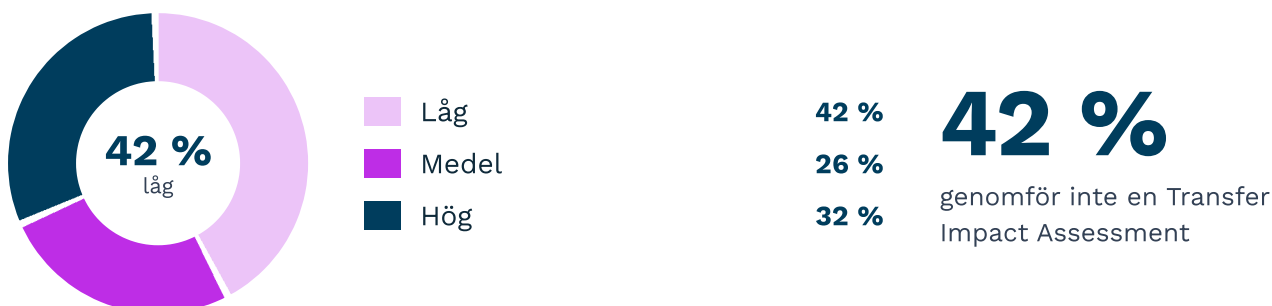


Kryptering är en av de mest grundläggande teknikerna för att skydda känslig information, både i vila och under överföring. I dag har närmare 32 procent av verksamheterna en låg mognadsgrad inom kryptering. Det är en oroande siffra, särskilt med tanke på att det inte bara är en rekommendation utan ett krav enligt både GDPR och NIS2.

Att lämna data okrypterad innebär att ett intrång snabbt kan leda till full exponering av personuppgifter, affärshemligheter eller systeminformation. I ett förhöjt geopolitiskt läge, där cyberoperationer ofta syftar till just stöld av data och informationspåverkan, blir konsekvenserna ännu mer allvarliga. Krav enligt artikel 32 i GDPR och artikel 21 i NIS2 är tydliga: känsliga uppgifter ska skyddas med starka tekniska och organisatoriska åtgärder. Att så pass många verksamheter ändå ligger under en godtagbar nivå, visar enligt OMS bedömning på ett glapp mellan lagstiftning och praktisk implementering som behöver stängas snabbt. Ett glapp som direkt försämrar cyberhygienen och som i en skärpt hotbild också blir en fråga om Sveriges förmåga att skydda samhällsviktig information.

TredjELandsöverföringar

Figur 19 Mognadsnivå, tredjELandsöverföringar

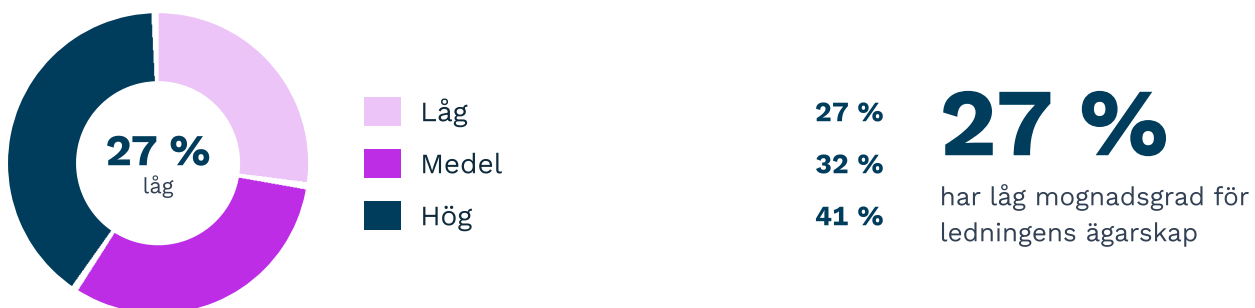


Mer än fyra av tio verksamheter, 42 procent, genomför i dag inte en Transfer Impact Assessment om överföring av personuppgifter till tredjELand. Det gör tredjELandsöverföringar till en av de två svagaste kontrollerna i hela rapporten, tillsammans med säkra leveranskedjor.

En sådan bedömning är avgörande för att identifiera om den mottagande staten har lagar eller praxis som undergräver skyddet av personuppgifter, en central fråga sedan EU-domstolens vägledande dom i Schrems II. I ett omvärldsläge där persondata allt oftare används som råvara i geopolitiska intressen, inklusive massövervakning, profilering och påverkan, är bedömningen av tredjELandsrisk enligt OMS bedömning inte bara en juridisk fråga utan även en strategisk. Att så stor andel av verksamheterna saknar en sådan bedömning är en tydlig signal om att efterlevnaden inom tredjELandsöverföring behöver förbättras. Det räcker inte att lita på standardavtal eller tredjepartsförsäkringar. Riskerna måste analyseras och hanteras konkret, annars riskerar svenska verksamheter både sanktioner och att bli en svag länk i internationella affärsrelationer där dataskydd är en förutsättning för fortsatt samarbete.

Ledningens ägarskap

Figur 20 Mognadsnivå, ledningens ägarskap

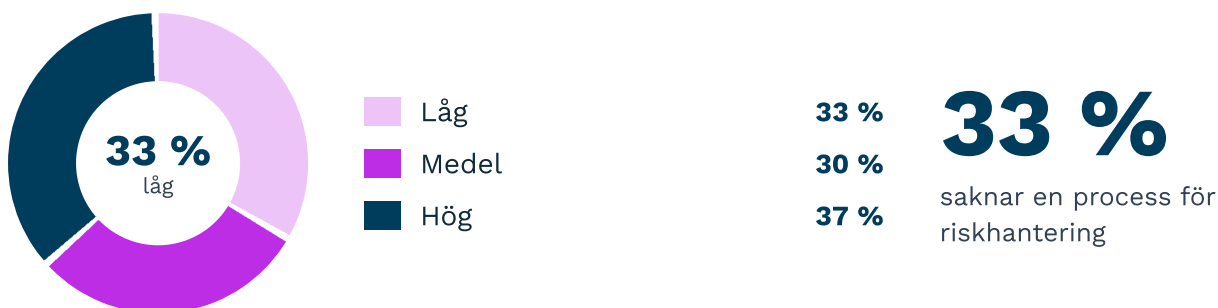


NIS2 tydliggör att det inte längre räcker att delegera säkerhetsansvar nedåt i verksamheten. Ledningen måste enligt direktivet aktivt uppfylla kraven och kan hållas personligen ansvarig enligt nationell rätt. Drygt 40 procent visar en hög mognadsgrad, medan omkring 27 procent ligger på en låg nivå.

I ett osäkert geopolitiskt läge, där kritisk infrastruktur är ett strategiskt mål för statsstödda cyberangrepp, är detta en bräcklig grund att stå på. Felbedömningar i ledningsrummet kan få lika allvarliga konsekvenser som tekniska sårbarheter och nu när NIS2 är gällande rätt väger det personliga ansvaret tungt. Ledningens förmåga att förstå, väga och agera på cybersäkerhetsrisker är i dag en förutsättning för både regelefterlevnad och affärskritisk motståndskraft, och en svag mognad på denna punkt riskerar att sprida sig nedåt i organisationen: om ledningen inte äger frågan blir det svårare att få gehör och resurser för säkerhetsarbetet i övrigt.

Riskhantering

Figur 21 Mognadsnivå, riskhantering

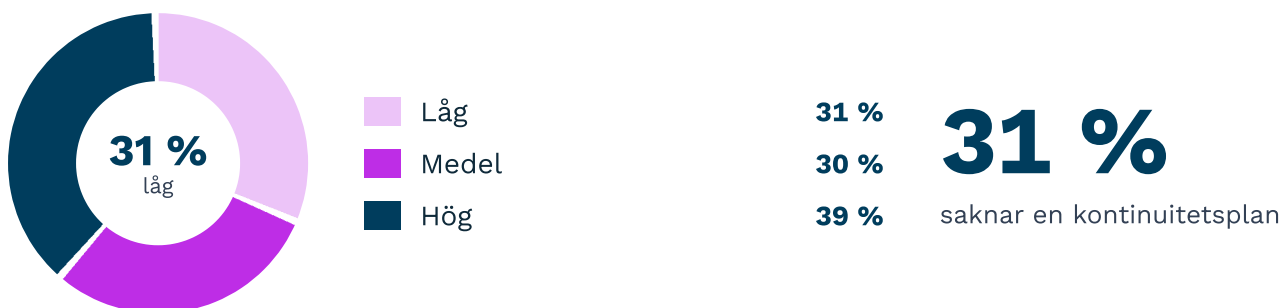


Enligt NIS2 ska verksamheter ha formella policyer och rutiner för att identifiera, hantera och följa upp risker, inte bara inom IT, utan ur ett helhetsperspektiv för hela verksamheten. Det innebär ett allriskangreppssätt där cyberhot bedöms i relation till affärsverksamhet, drift, leverantörsberoenden och samhällspåverkan. Trots det saknar i dag omkring en tredjedel av verksamheterna en process för riskhantering.

I dagens läge, där hybridpåverkan, desinformation och cyberangrepp alltmer smälter samman, krävs en samlad bild för att förstå hur olika hot samverkar och påverkar verksamheten strategiskt. Frånvaron av helhetsrutiner gör det svårt att fånga just dessa kopplingar och ökar risken att allvarliga sårbarheter förblir osynliga tills de materialiseras som incidenter. Enligt OMS bedömning är detta en av dagens mest underskattade risker. Utan en samlad riskbild blir cyberhygienen fragmenterad, kontinuitetsplaneringen felaktig och verksamheten investerar i fel skydd - vilket skapar en direkt konkurrensnackdel.

Kontinuitetsplan

Figur 22 Mognadsnivå, kontinuitetsplan

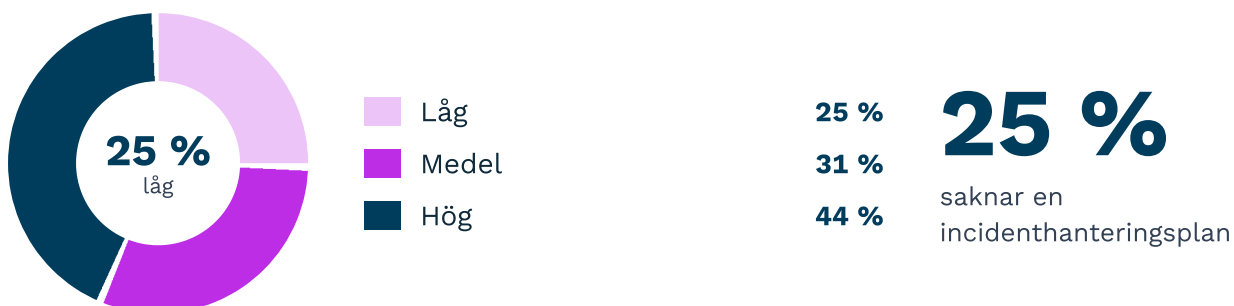


Cyberhygien och förmåga till motståndskraft och kontinuitet ställer krav på att verksamheter har en dokumenterad plan för att upprätthålla och säkerställa kontinuitet vid störningar, inklusive backup, krishantering och återställning efter incidenter. Trots detta saknar i dag omkring en tredjedel av verksamheterna en sådan plan.

Det geopolitiska läget kräver förmåga att hantera konsekvenserna av angrepp och återgå till drift på ett kontrollerat sätt. Att sakna en plan för detta är inte bara ett brott mot NIS2, det är en strategisk sårbarhet. Ransomware-attacker är ett tydligt exempel där frånvaron av fungerande kontinuitetsplaner förlänger tiden hela eller delar av verksamheten ligger nere, ofta med veckor. Kontinuitetsplanen är en kärnkomponent i verksamhetens motståndskraft och att en tredjedel av det svenska näringslivet saknar en sådan plan innebär enligt OMS bedömning att samhällets samlade förmåga att stå emot och återhämta sig från allvarliga störningar i dag är svagare än den behöver vara. Detta med direkta konsekvenser för både leveranssäkerhet och konkurrenskraft när verksamheter inte kan garantera driftskontinuitet gentemot sina kunder och partners.

Incidenthantering

Figur 23 Mognadsnivå, incidenthantering

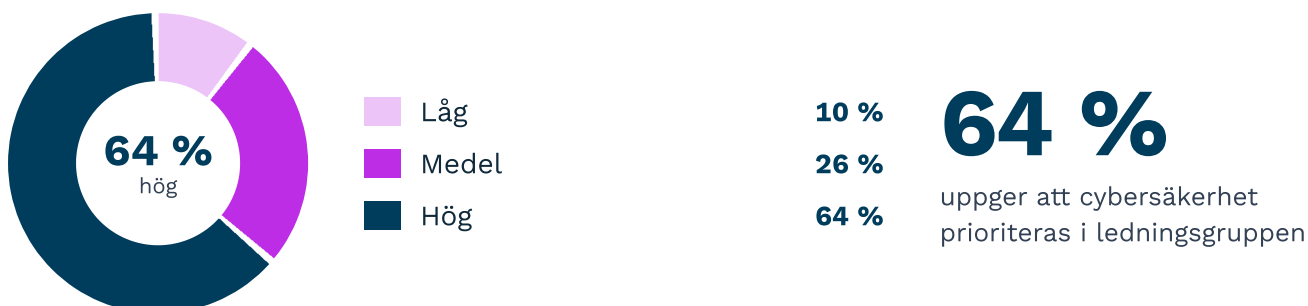


Enligt NIS2 ska alla verksamheter ha en dokumenterad incidenthanteringsplan som omfattar både tekniska och organisatoriska åtgärder. Planen ska testas och granskas regelbundet och personalen ska veta exakt vad som förväntas av dem vid en incident. I dag saknar ungefär en fjärdedel av verksamheterna en sådan plan.

I takt med att attackerna blivit mer koordinerade och komplexa har också kraven på incidentrespons ökat. Angripare använder sig av taktiker som överbelastning, desinformation och samtidig påverkan av flera system. Utan en fungerande plan ökar risken för felbeslut på grund av informationsbrist, vilket leder till längre återställningstider, sämre cyberhygien under själva krisen och en svagare samlad kontinuitetsförmåga. En incidentplan är ett verktyg för att skydda verksamheten när något går fel. I dagens läge är det inte längre en fråga om, utan när.

Ledningens prioritet

Figur 24 Mognadsnivå, ledningens prioritet



Detta är en ny kontrollfråga i årets underlag, och resultatet är på ytan hoppfullt: nästan två tredjedelar av verksamheterna uppger en hög mognadsgrad när det gäller att cybersäkerhet faktiskt prioriteras i ledningsgruppen, medan bara en av tio ligger på en låg nivå.

Det är den enskilt starkaste siffran i hela rapporten och den är värd att lyfta fram. Samtidigt är det värt att hålla den bredvid resultaten för chefsutbildning, riskhantering och ledningens ägarskap, som alla visar en betydligt svagare bild. Att ledningen säger sig prioritera cybersäkerhet är ett nödvändigt första steg, men dagens data tyder på att den prioriteringen ännu inte fullt ut har omsatts i konkret utbildning, ägarskap och operativ riskhantering. Enligt OMS bedömning är just detta glapp mellan avsikt och genomförande en nyckel till att förstå varför den operativa cyberhygien fortfarande brister trots att viljan finns i ledningsrummet. Detta är ett glapp vi kommer att följa med stort intresse i kommande rapporter.

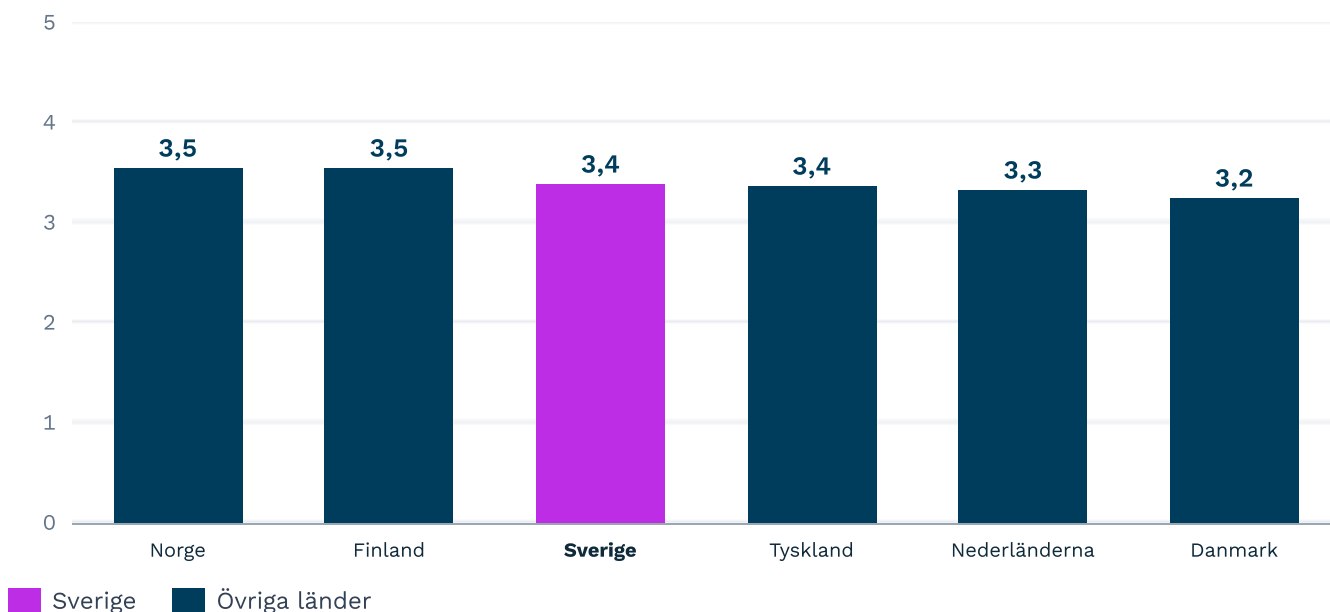
Cybersäkerhetsmognad i Europa

Genom en geografisk analys kan vi identifiera signifikanta mognadsskillnader mellan de nordiska länderna och några europeiska länder. Datamaterialet för länder utanför Norden är fortsatt begränsat, vilket gör att resultaten bör tolkas med försiktighet och inte kan generaliseras.

Norge och Finland är i dag de ledande nordiska länderna med en mognadsgrad på 3,5. Sverige ligger på tredje plats bland de jämförda länderna, med en mognadsgrad på 3,4. Svenska verksamheter följer i allmänhet grundläggande cybersäkerhetsregler, men behöver enligt OMS bedömning öka takten när det gäller införandet av omfattande säkerhetsbedömningar och proaktiva funktioner för upptäckt av hot. Att stå på tredje plats i en jämförelse där Norge och Finland ligger före är inte bara en fråga om nationell stolthet: det är en konkurrensfråga för svenska verksamheter som verkar internationellt och en fråga om Sveriges attraktionskraft som handelspartner och investeringsdestination i en tid då säkerhetsnivå alltmer vägs in i affärsbeslut.

Danska verksamheter bör prioritera att stärka cybersäkerhetsåtgärderna, förbättra regel efterlevnaden och avsevärt öka medvetenheten för att minska sårbarheter och förbättra den övergripande cybersäkerhetsmognaden.

Figur 25 Mognadsgrad per land, 2026



Danmark uppvisar den lägsta cybersäkerhetsmognaden i denna jämförande analys.

Referenser

ENISA. (2021). Threat Landscape for Supply Chain Attacks. European Union Agency for Cybersecurity. <https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks>

ENISA. (2026). NIS360. European Union Agency for Cybersecurity. <https://www.enisa.europa.eu/news>

ENISA. (2026). Cyber Europe 2026. European Union Agency for Cybersecurity. <https://www.enisa.europa.eu/news>

Europeiska kommissionen. (2022). Direktiv (EU) 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå inom hela unionen (NIS2). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555>

Europeiska kommissionen. (2026). Vägledning inför Cyber Resilience Act. <https://digital-strategy.ec.europa.eu/en/news>

MSB & Nationellt cybersäkerhetscenter. (2024). Lägesbild cybersäkerhet: Kritisk infrastruktur och nationella hotaktörer. <https://www.ncsc.se>

Nationellt cybersäkerhetscenter. (2026). CERT-SE:s övergång till NCSC. <https://www.cert.se/nyheter/>

Riksdagen. (2025). Cybersäkerhetslagen (2025:XX). I kraft sedan 15 januari 2026.

Slutord från PwC

PwC ser samma övergripande utveckling globalt som OneMore Secure lyfter i rapporten: cyberrisk är i allt högre grad en fråga om hela det digitala ekosystemet, inte enbart den egna organisationens interna säkerhet. När verksamheter blir mer beroende av externa leverantörer, molntjänster, SaaS-lösningar, mjukvara, dataflöden och AI ökar också exponeringen mot risker som ligger utanför den egna direkta kontrollen. Det innebär att organisationers motståndskraft i praktiken påverkas av hur väl deras leverantörer och partners kan förebygga, upptäcka och hantera cyberhot.

I PwC:s globala analyser ser vi att den förändrade hotbilden, ökade regulatoriska krav och mer komplexa leverantörskedjor gör tredjepartsrisk till en allt viktigare fråga för ledning och styrelse. För att möta dessa utmaningar krävs ett mer strukturerat, kontinuerligt och riskbaserat arbetssätt för att identifiera, prioritera och hantera kritiska beroenden. Ett sådant arbetssätt bör även inkludera teknisk validering av faktisk säkerhetskfiguration och säkerhetsförmåga, för att verifiera att identifierade kontroller inte bara finns dokumenterade utan också fungerar i praktiken.

OneMore Secures rapport belyser vikten av ökad transparens kring cybersäkerhetsmognad i leveranskedjan. Den typen av insikter kan bidra till bättre prioriteringar, stärkt regelefterlevnad och ökad digital motståndskraft i ett samhälle där organisationer är mer sammankopplade än någonsin.

Henrik Petré

Partner, PwC Sverige



OneMore Secure är en Digital Trust Hub för Supply Chain Security som hjälper verksamheter att förstå, följa upp och stärka säkerheten i sina leverantörskedjor.