

JULI 2023

OT enligt Sverige

Allmänhetens och svenska företags syn
på framtiden, teknologins utveckling,
beredskap och OT-säkerhet.

Innehållsförteckning

Bakgrund **3**

Allmänheten 4

Företagen 5

Allmänheten **6**

01 Framtidssyn och oro 7

02 Beredskap 13

03 Teknikens framsteg 20

04 Kunskap om OT 27

Företagen **34**

05 Framtidssyn 35

06 Beredskap 40

07 Teknik 47

08 OT-säkerhet 54

Appendix **73**

Bakgrund



Allmänheten

Syfte

Denna studie fokuserar på den svenska befolkningens syn på framtiden, oro, krisberedskap, teknikens roll i samhället och begreppet operativ teknik (OT).

Målet är att förstå svenskarnas syn på framtiden, individuell krisberedskap, samhällets och svenska industriers förmåga att motverka hot, samt att undersöka attityder till ny teknik, innovation och forskning och deras påverkan på framtiden.

Målgrupp

Undersökningen riktade sig mot alla i Sverige över 18 år.

Metod

Undersökningen genomfördes genom en onlinepanel (CAWI) via Norstat. Totalt deltog 1014 respondenter.

Period

Datainsamlingen genomfördes under vecka 27, 2023.

Företagen

Syfte

Undersökningen fokuserar på Operational Technology (OT), den digitala teknologin för att styra och övervaka fysiska system i industrier och infrastruktur, med betoning på OT-säkerhet mot hot och cyberattacker.

Målet är att förstå företags syn på framtiden, deras beredskap för hot och attacker samt deras inställning till ny teknik, innovation, forskning och dess påverkan på OT-miljö och OT-säkerhet.

Målgrupp

Undersökningens målgrupp består av följande nyckelpersoner: CIO (IT-chefer), CTO (IT-direktörer),

CISO (säkerhetschefer inom IT) samt Säkerhetsansvarig (utan chefsbefogenheter) vid större eller medelstora företag verksamma i Sverige.

Metod

Undersökningen genomfördes genom en onlinepanel (CAWI) via Norstat. Totalt deltog 28 respondenter. Eftersom basen är begränsad bör en vara försiktig med att dra alltför breda slutsatser från de procentuella resultat som presenteras i denna rapport. Dessa resultat ger dock en värdefull indikation.

Period

Datainsamlingen genomfördes under vecka 27 och 28, 2023.

Allmänheten



01

Framtidssyn och oro

Sammanfattning framtidssyn och oro

Detta avsnitt undersöker hur Sveriges befolkning betraktar framtiden och de potentiella faror som kan präglade deras tankar. Vi utforskar deras nivå av oro, frekvensen av deras reflektion över framtida hot, deras medvetenhet om globala utmaningar samt deras tro på mänsklighetens förmåga att hantera dessa utmaningar.

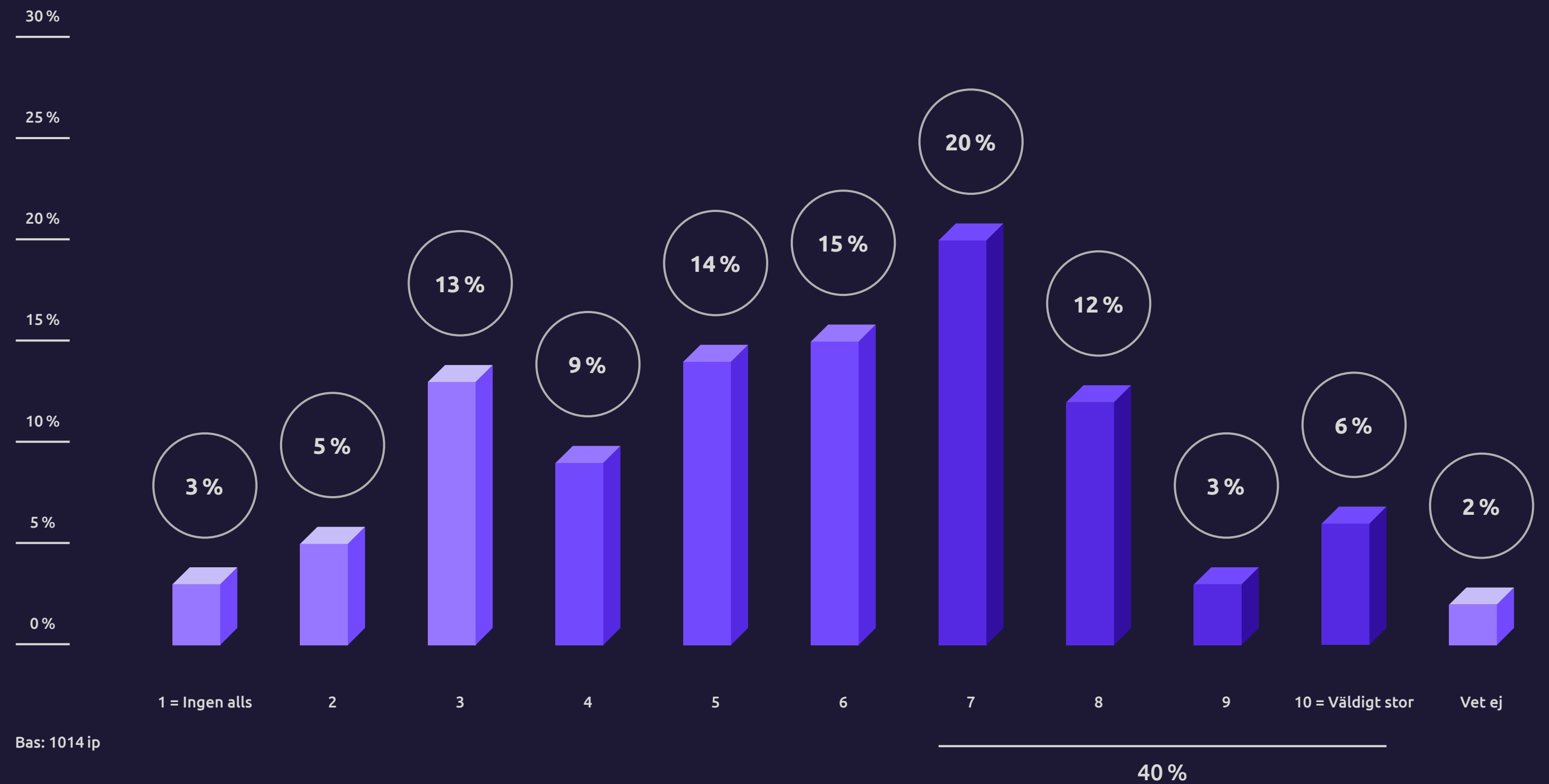
01.1

4 av 10 känner *stor* eller *väldigt stor* oro för framtiden

Det är 40 % som känner viss eller väldigt stor oro för framtiden. Oron är högst bland kvinnor samt de yngre åldersgrupperna.

21 % av respondenterna känner knappt någon eller ingen oro alls.

Oro för framtiden



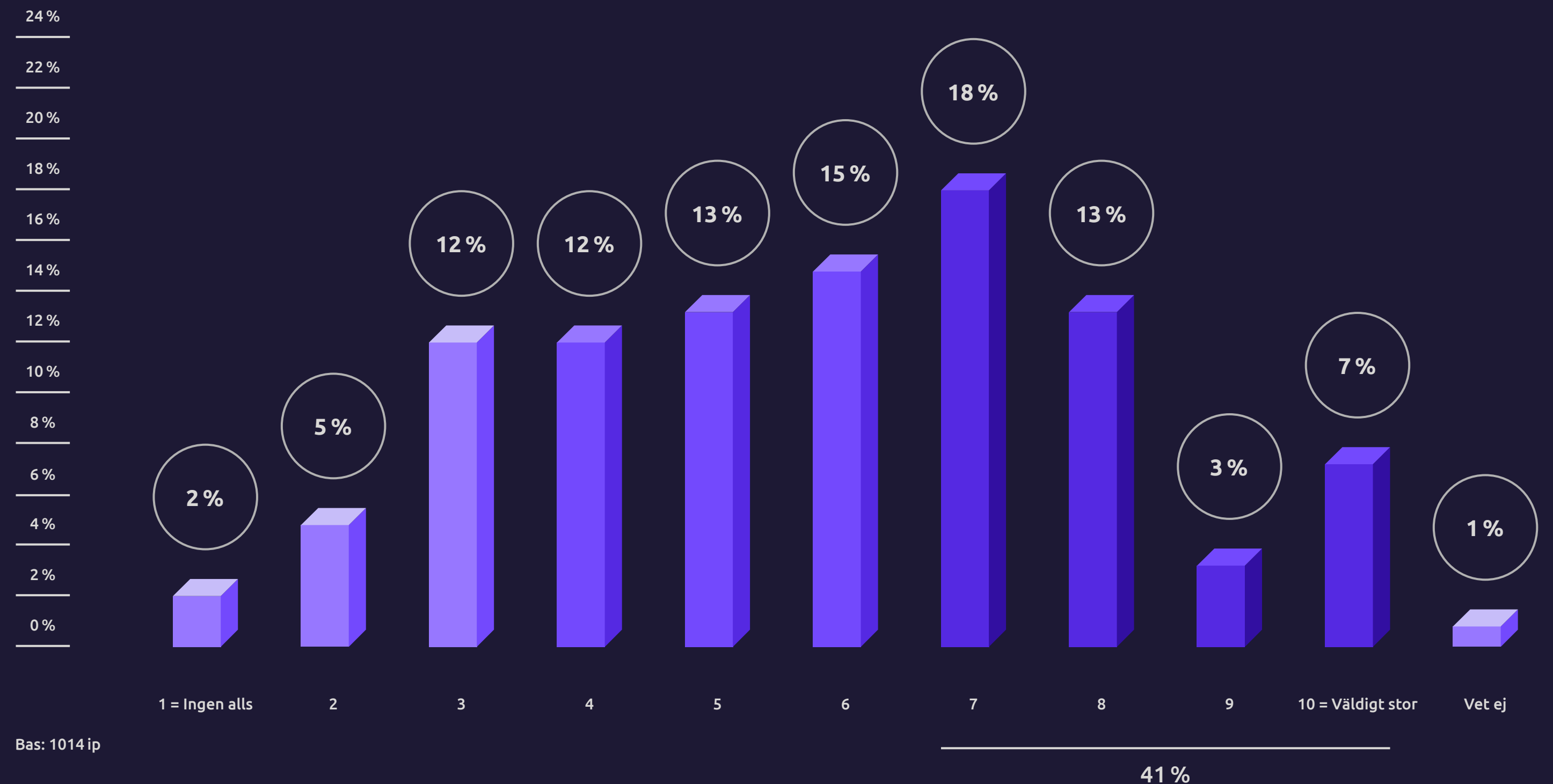
01.2

4 av 10 tänker *ofta* eller *väldigt ofta* på framtiden och de potentiella risker eller hot som kan uppstå

Det är en högre andel kvinnor och yngre åldersgrupperna som tänker på detta.

19 % av respondenterna tänker nästan aldrig eller aldrig på framtida risker och hot.

Tankar på framtida potentiella risker och hot

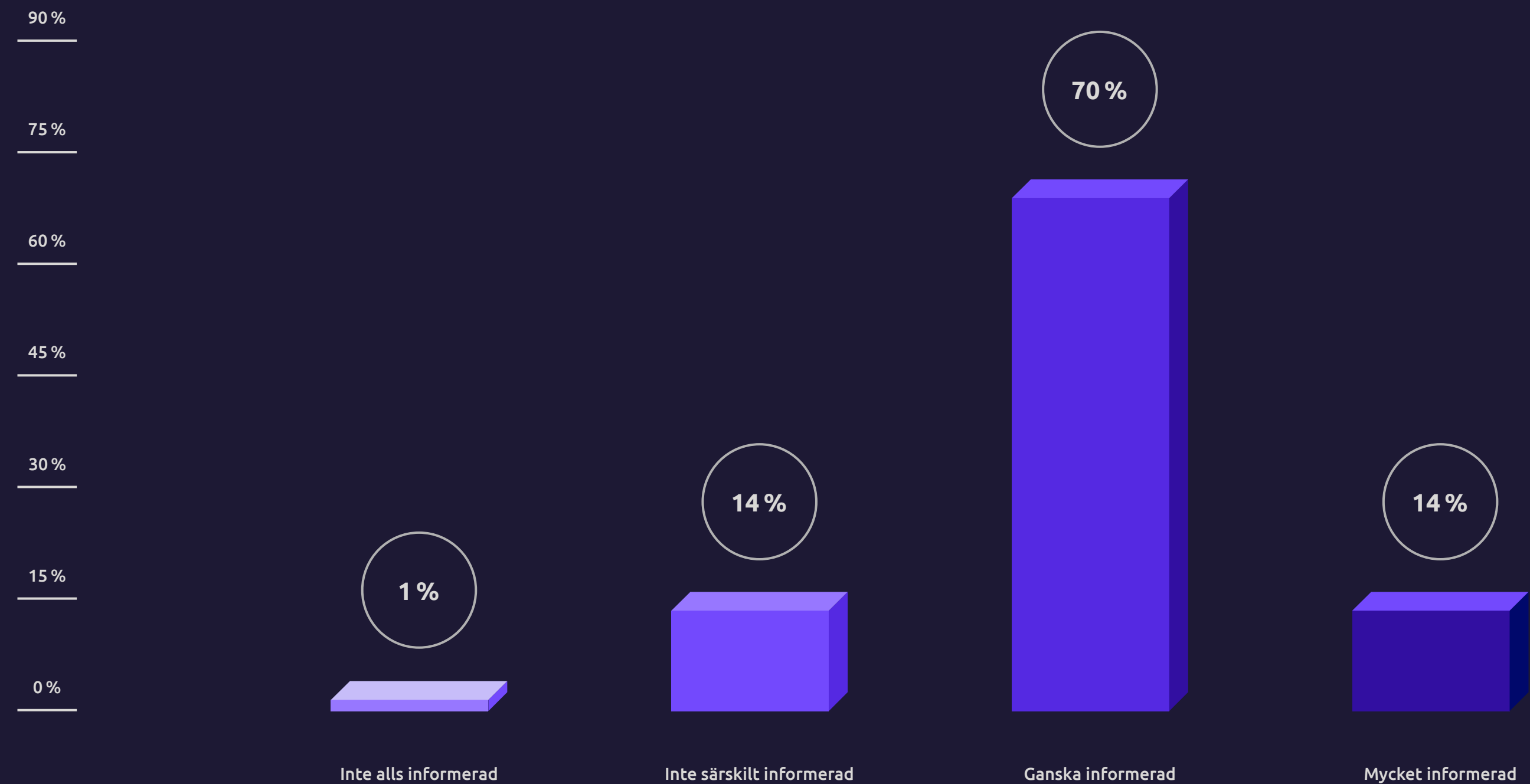


01.3

Majoriteten är *ganska informerad* om globala utmaningar som kan påverka framtiden

14 % uppger att de är mycket informerade. Lika stor andel säger att de inte är särskilt informerade. 1 % är inte alls informerade.

Hur väl informerad en är om globala utmaningar



Bas: 1014 ip

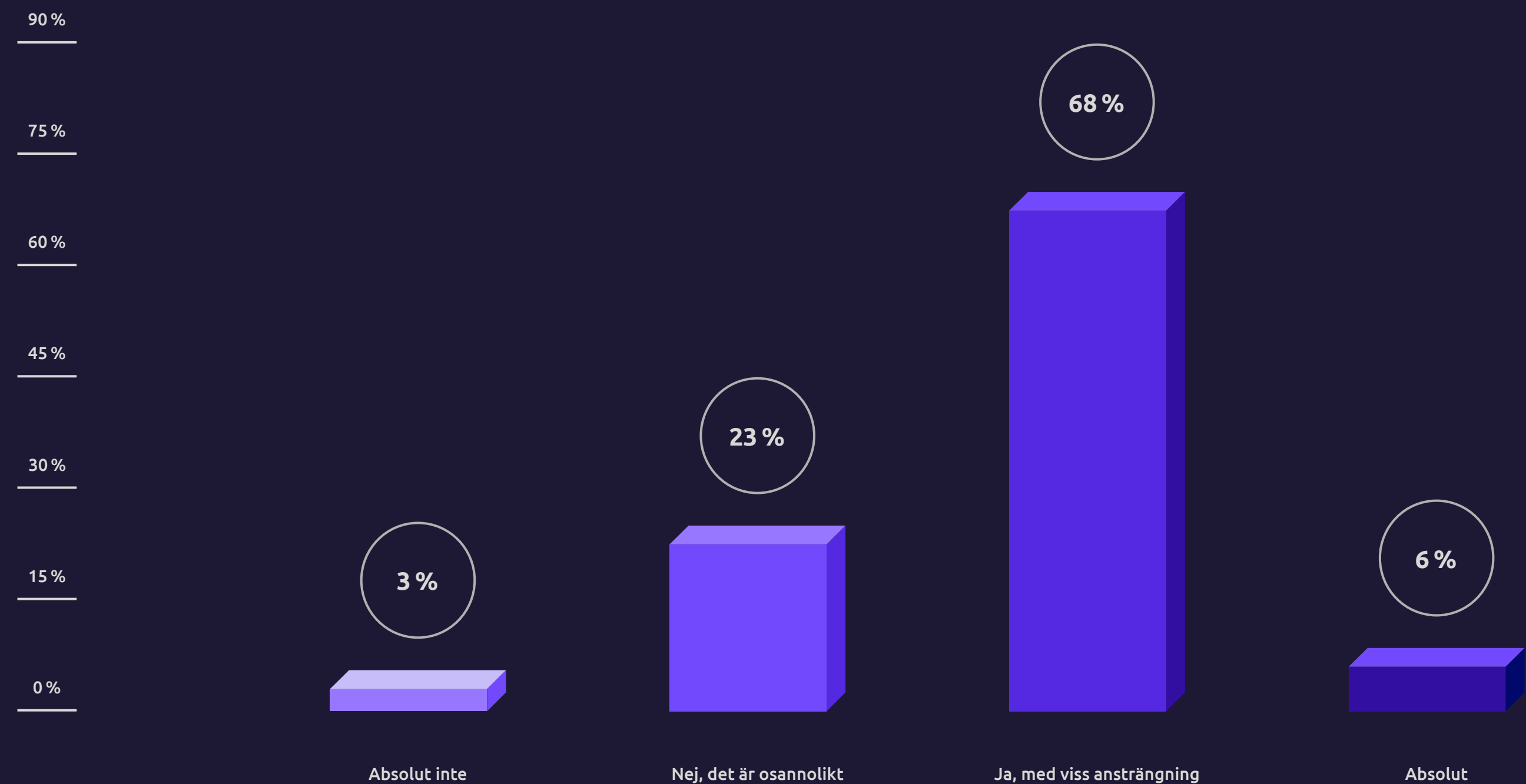
01.4

Två tredjedelar av respondenterna tror att vi människor *har förmågan* att lösa utmaningarna *med viss ansträngning*

6 % uppger att de absolut tror på människans förmåga att lösa de utmaningar som kan uppstå i framtiden.

23 % svarar att det är osannolikt och 3 % absolut inte.

Tron på förmågan att lösa framtida utmaningar



Bas: 1014 ip

02

Beredskap

Sammanfattning beredskap

Det kommande kapitlet analyserar svenskarnas syn på beredskap inför kriser och nödsituationer. Vi granskar deras personliga nivå av förberedelse på kris- eller nödsituation samt deras bedömning av samhällets och företags beredskapsnivå. Vi undersöker även deltagarnas syn på framtiden och de samhälleliga faktorer som kan komma att påverka den.

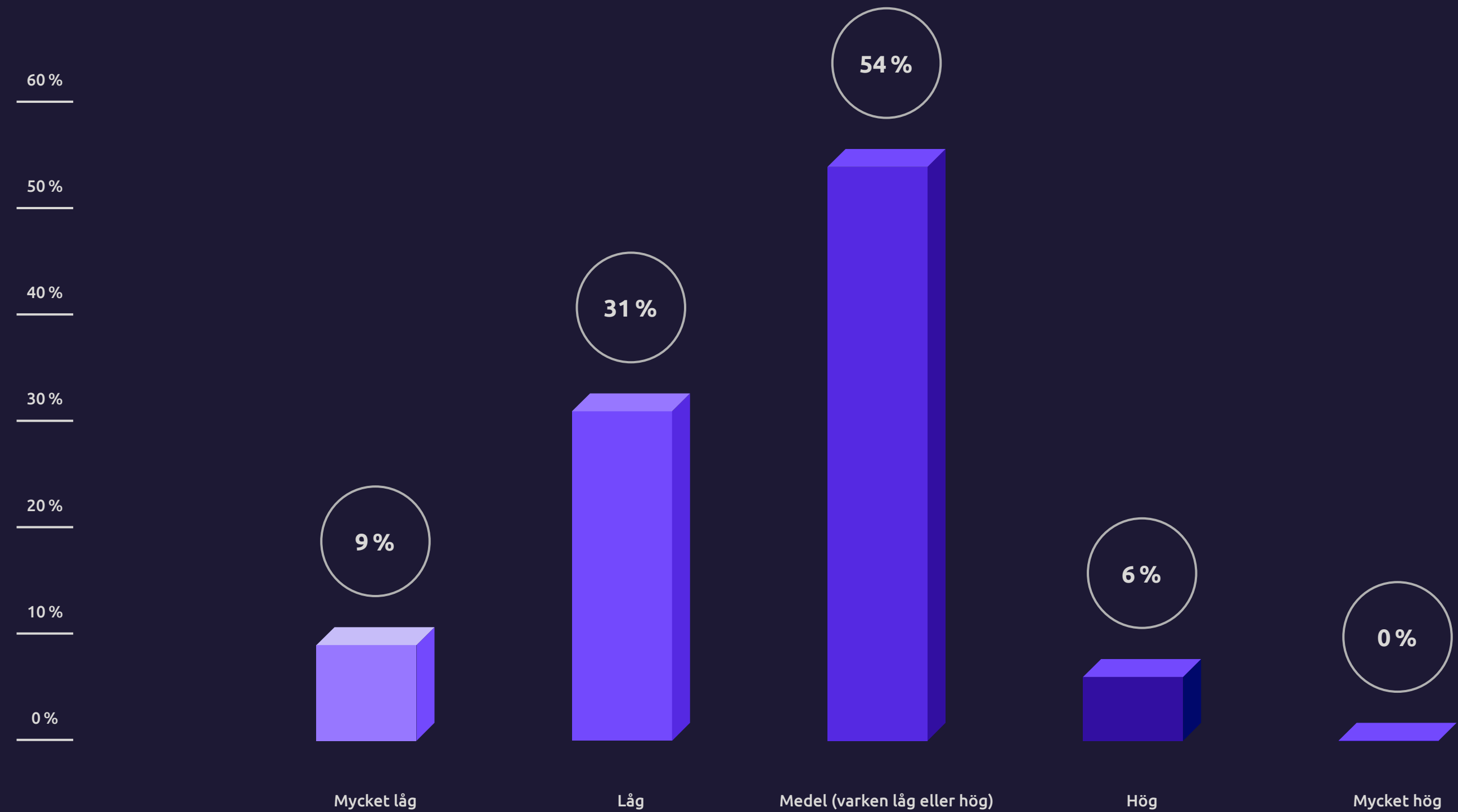
02.1

Drygt hälften (54 %) upplever samhällets beredskapsnivå som *varken låg eller hög*

6 % av respondenterna svarar att samhällets beredskapsnivå för att hantera eventuella kriser eller nödsituationer är hög.

31 % anser att beredskapsnivån är låg och 9 % mycket låg.

Samhällets beredskapsnivå



Bas: 1014 ip

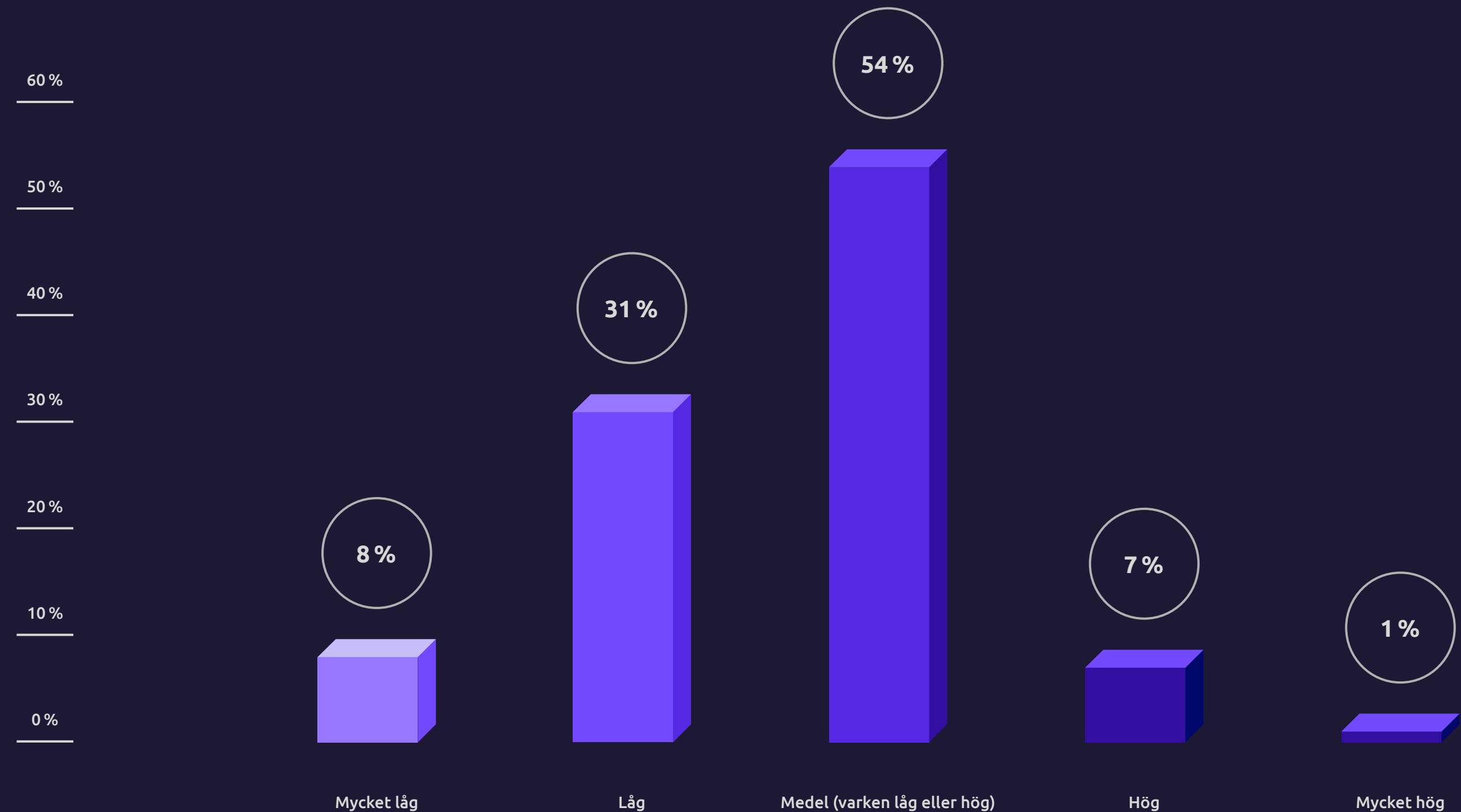
02.2

54 % bedömer svenska industriföretags beredskapsnivå som *varken låg eller hög*

7 % respondenterna svarar att svenska industriföretags beredskapsnivå för att hantera eventuella kriser eller nödsituationer är hög. Endast 1 % svarar mycket hög.

31 % anser att beredskapsnivån är låg hos svenska industriföretag och 8 % uppger att den är mycket låg.

Svenska industriföretags beredskapsnivå



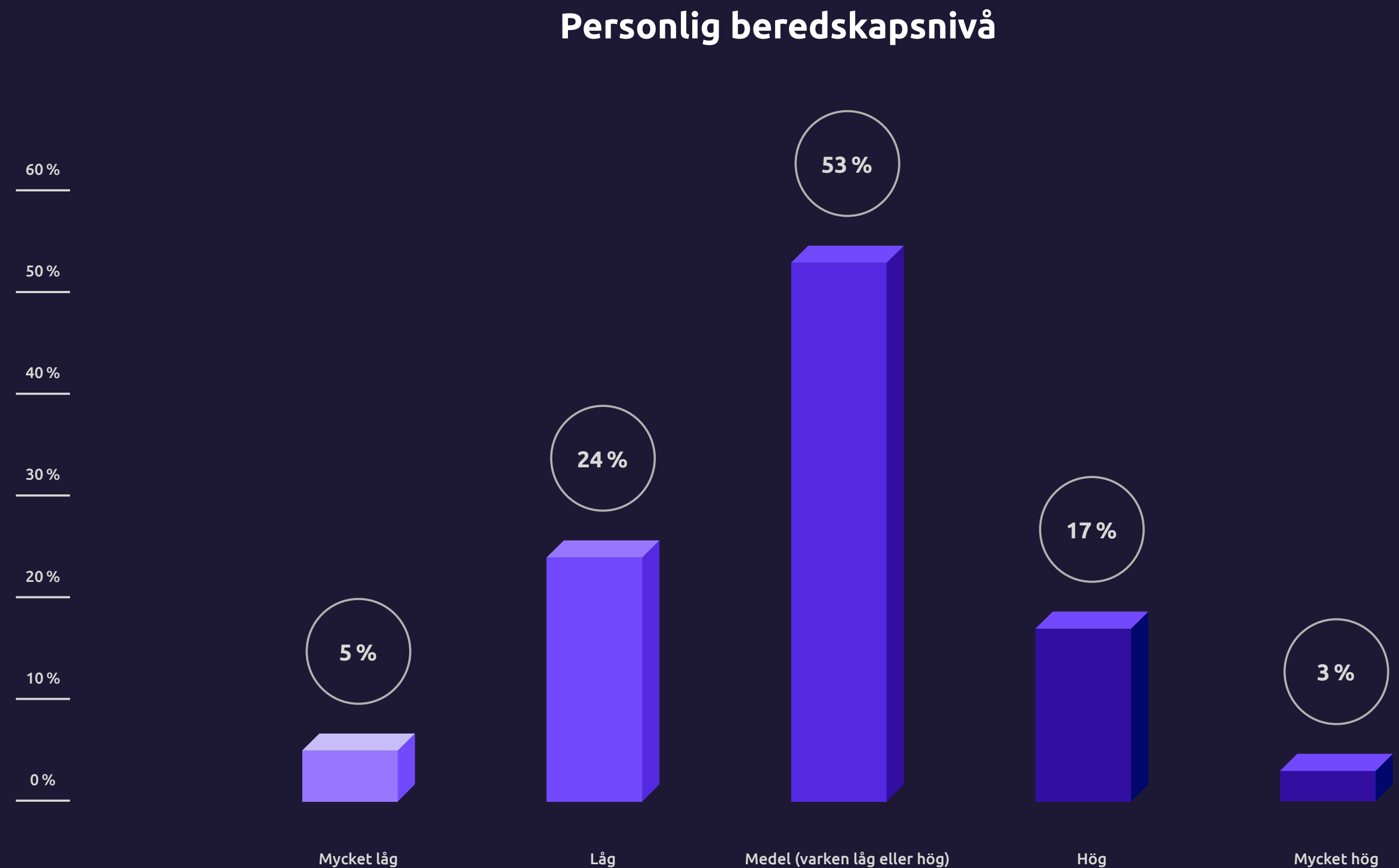
Bas: 1014 ip

02.3

53 % anser att deras egna personliga beredskapsnivå ligger på *medelnivå*

17 % av respondenterna svarar att deras egna beredskapsnivå för att hantera eventuella kriser eller nödsituationer är hög. 3 % svarar mycket hög.

24 % anser att deras beredskapsnivå är låg och 5 % uppger att den är mycket låg.



Bas: 1014 ip

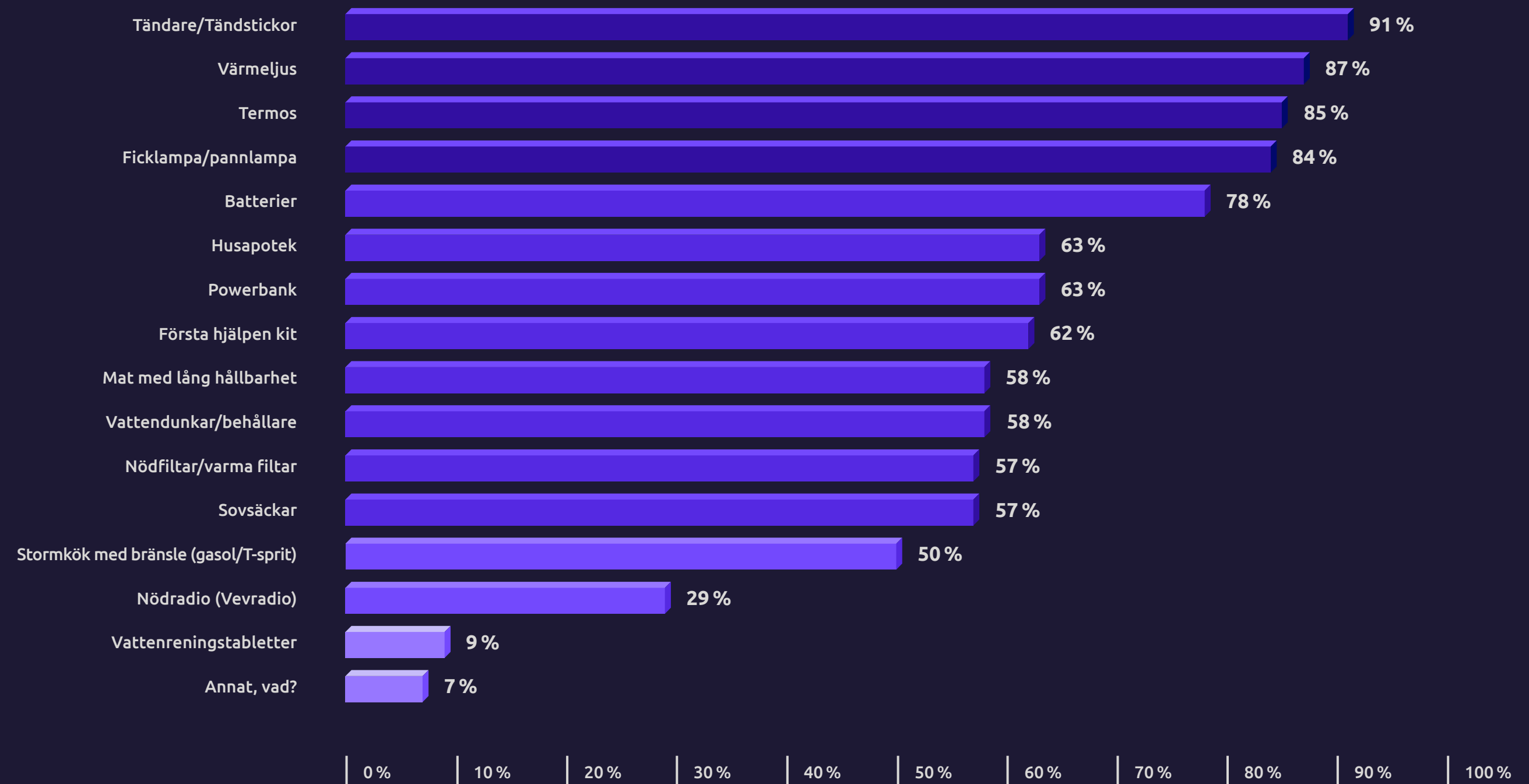
02.4

Tändare/tändstickor, värmeljus, termos, ficklampa och batterier är vanligast förekommande att ha hemma

63 % uppger att det finns ett husapotek och Powerbank hemma.

Det är 58 % som har mat med lång hållbarhet och vattendunkar. Endast 29 % har en nödradio och 9 % vattenreningstabletter.

Finns i hushållen idag



Bas: 1014 ip

02.5

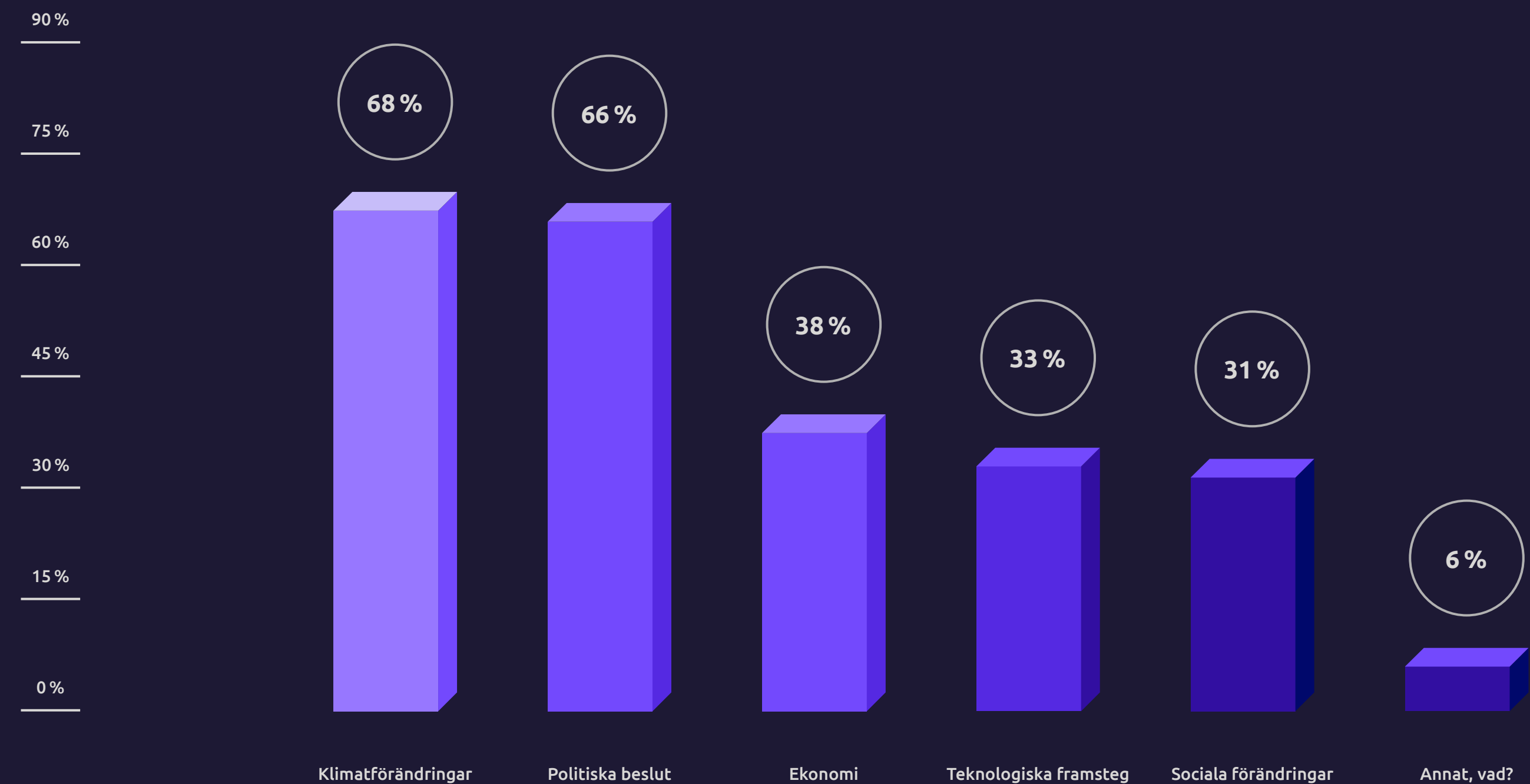
2 av 3 respondenter tror att *klimatförändringar* och *politiska beslut* är det som främst kommer påverka hur framtiden blir

Det är 38 % som uppger att ekonomin kommer påverka mest och 33 % svarar teknologiska framsteg.

De som valt "Annat" nämner framför allt samhällliga och kulturella faktorer, följt av faktorer inom säkerhet och konflikt, miljörelaterade faktorer och demografiska faktorer.

För alla svarsalternativ "Annat", se appendix 1 på sida 74.

Faktorer som kan påverka framtiden



Bas: 1014 ip

03

Teknikens framsteg

Sammanfattning teknikens framsteg

I det här kapitlet undersöks hur svenskarna förhåller sig till modern teknologi. Vi undersöker hur mycket de förlitar sig på modern teknik i vardagen, deras syn på teknologins inverkan på samhället samt deras kunskap om nya teknologier som AI och IoT. Deras åsikter om teknikens framtida potential och synen på samhällets förmåga att hantera teknologiska frågor belyses.

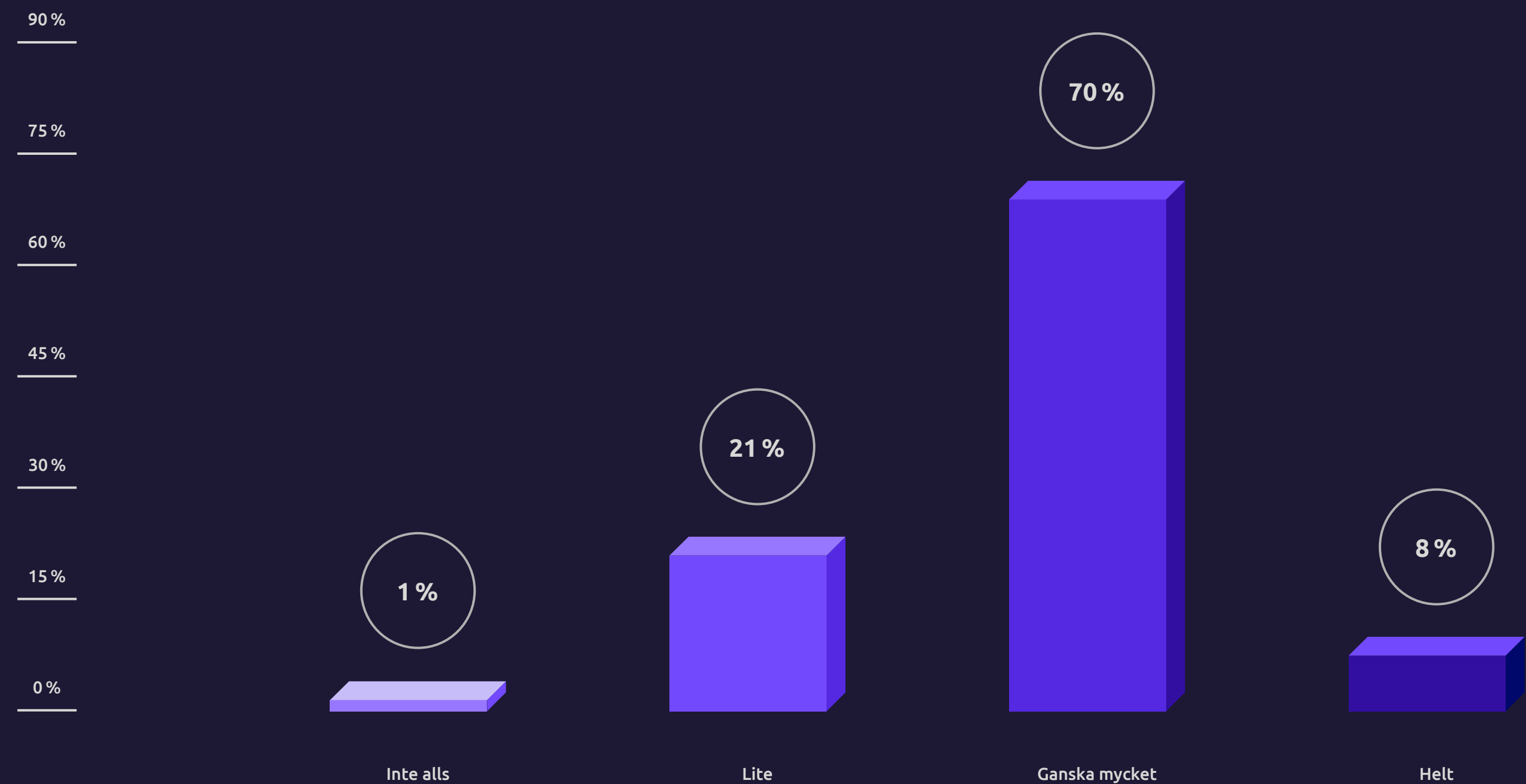
03.1

Merparten av svenskarna förlitar sig *ganska mycket* på modern teknik i sitt dagliga liv

70 % av respondenterna menar att de förlitar sig ganska mycket och 8 % säger att de förlitar sig helt på modern teknik i sitt dagliga liv.

21 % uppger att de förlitar sig lite och endast 1 % förlitar sig inte alls på modern teknik.

Hur mycket en förlitar sig på modern teknik



Bas: 1014 ip

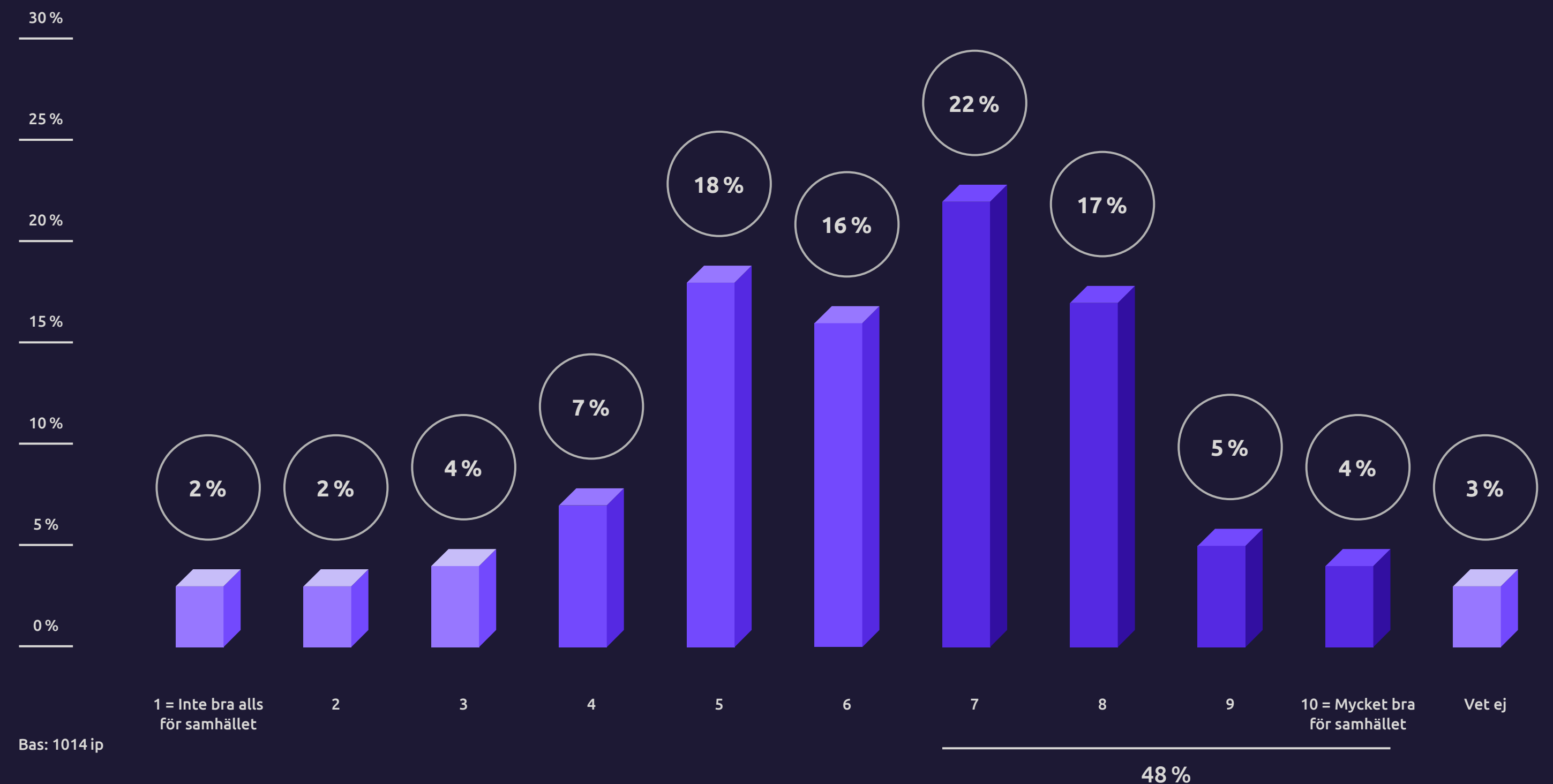
03.2

Nästan hälften anser att den moderna teknikens påverkan är *bra för samhället*

Svaren visar att män och de yngre åldersgrupperna (18–29 år och 30–44 år) i högre grad är positiva till den moderna teknikens påverkan på samhället än övriga respondenter.

8 % tycker att den moderna tekniken inte är bra för samhället.

Syn på modern teknologi



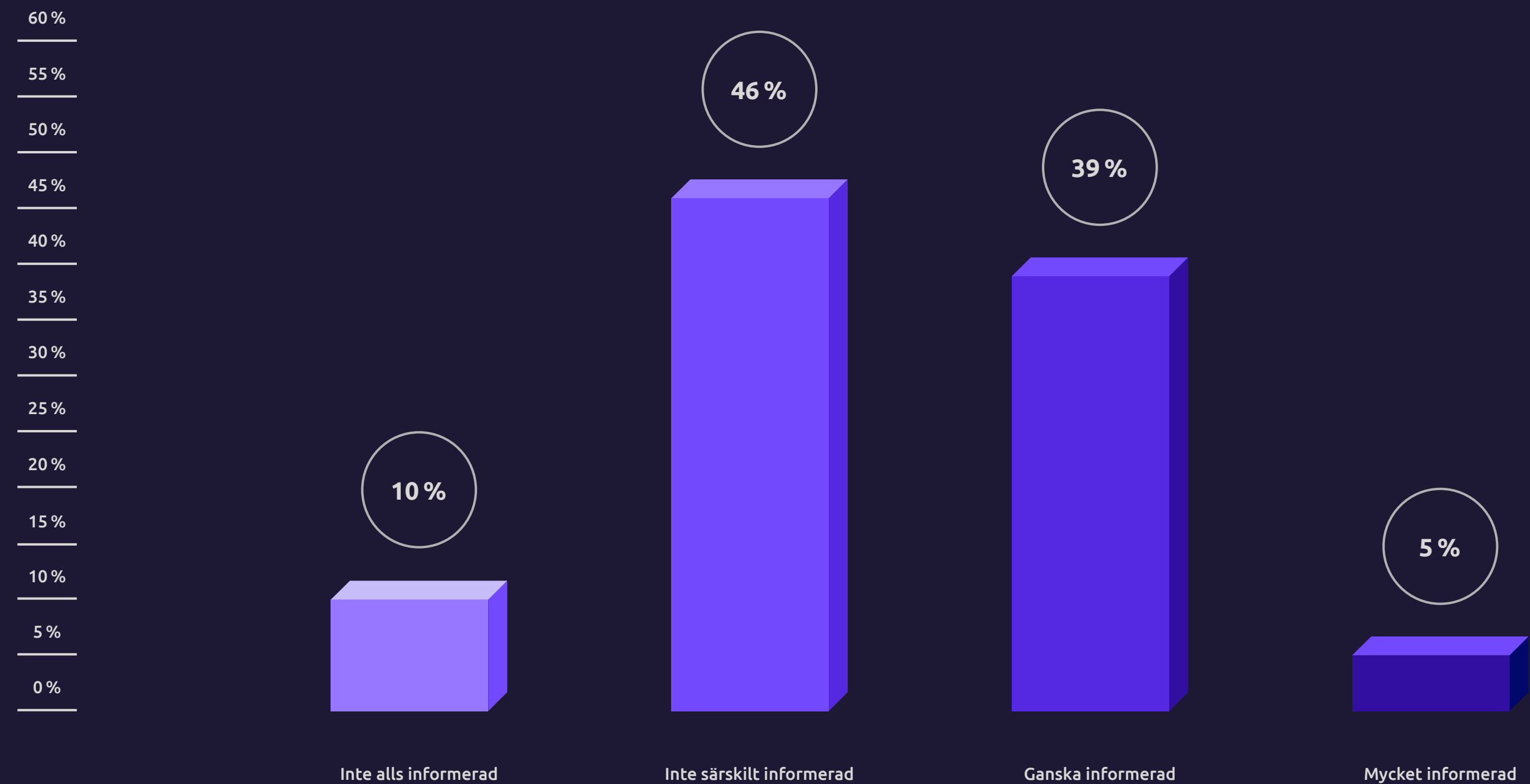
03.3

Nästan 6 av 10 känner sig *inte särskilt informerade* om nya teknologier

39 % anser sig vara ganska informerade kring nya teknologier som artificiell intelligens, blockchain, Internet of Things och 5 % svarar att de känner sig mycket informerade.

Andelen som känner sig ganska eller mycket informerad är högre bland männen och de yngre åldersgrupperna.

Informationsnivå kring nya teknologier



Bas: 1014 ip

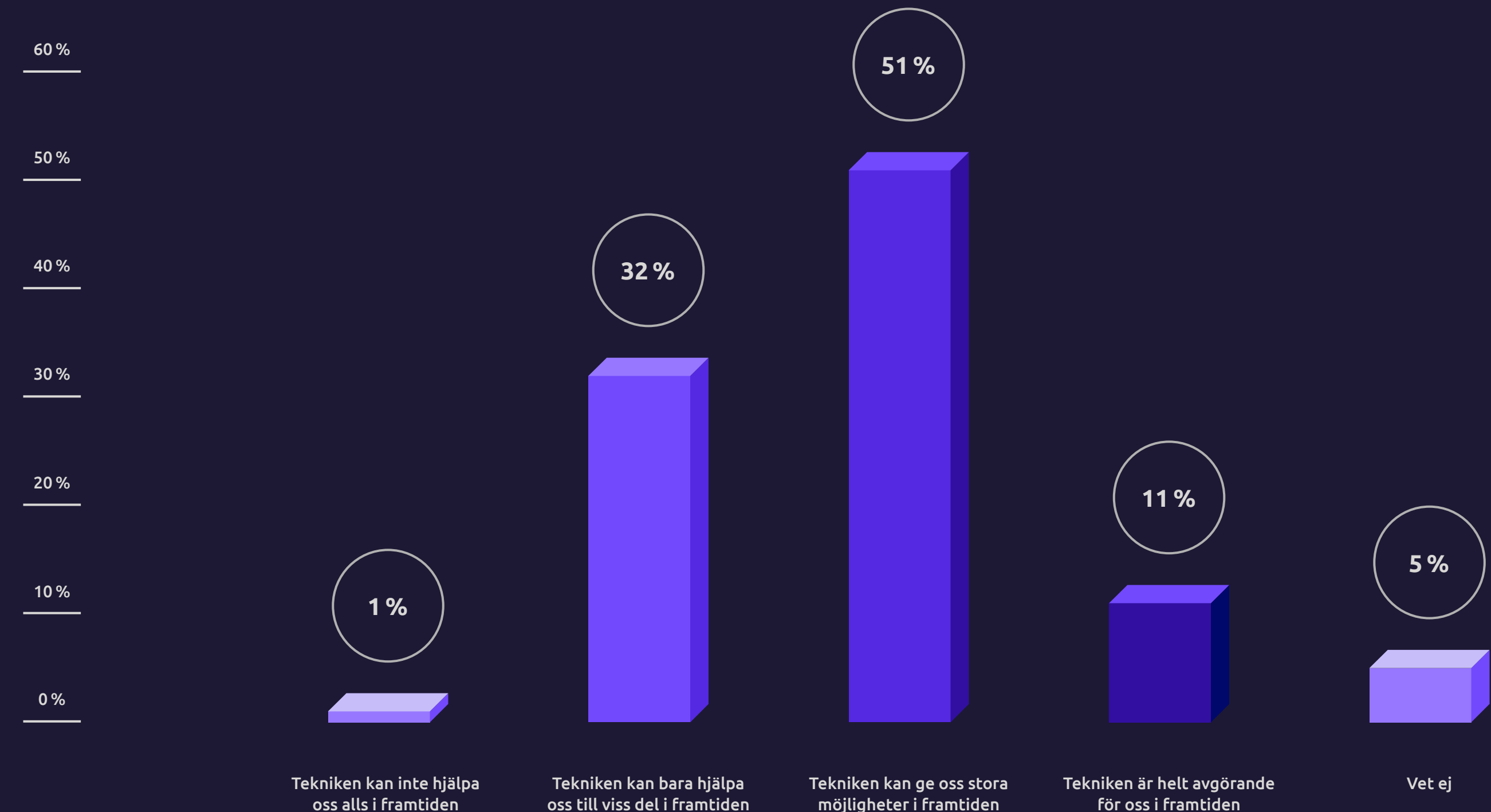
03.4

2 av 3 respondenter menar att tekniken kan ge oss stora eller avgörande möjligheter i framtiden

51 % anser att tekniken har potentialen att skapa stora eller avgörande möjligheter, medan 11 % anser att tekniken är helt avgörande för framtiden. Denna uppfattning är mer utbredd bland män och yngre åldersgrupper.

Endast 1 % uppger att tekniken inte alls kan hjälpa oss i framtiden.

Syn på möjligheter teknologin kan ge oss



Bas: 1014 ip

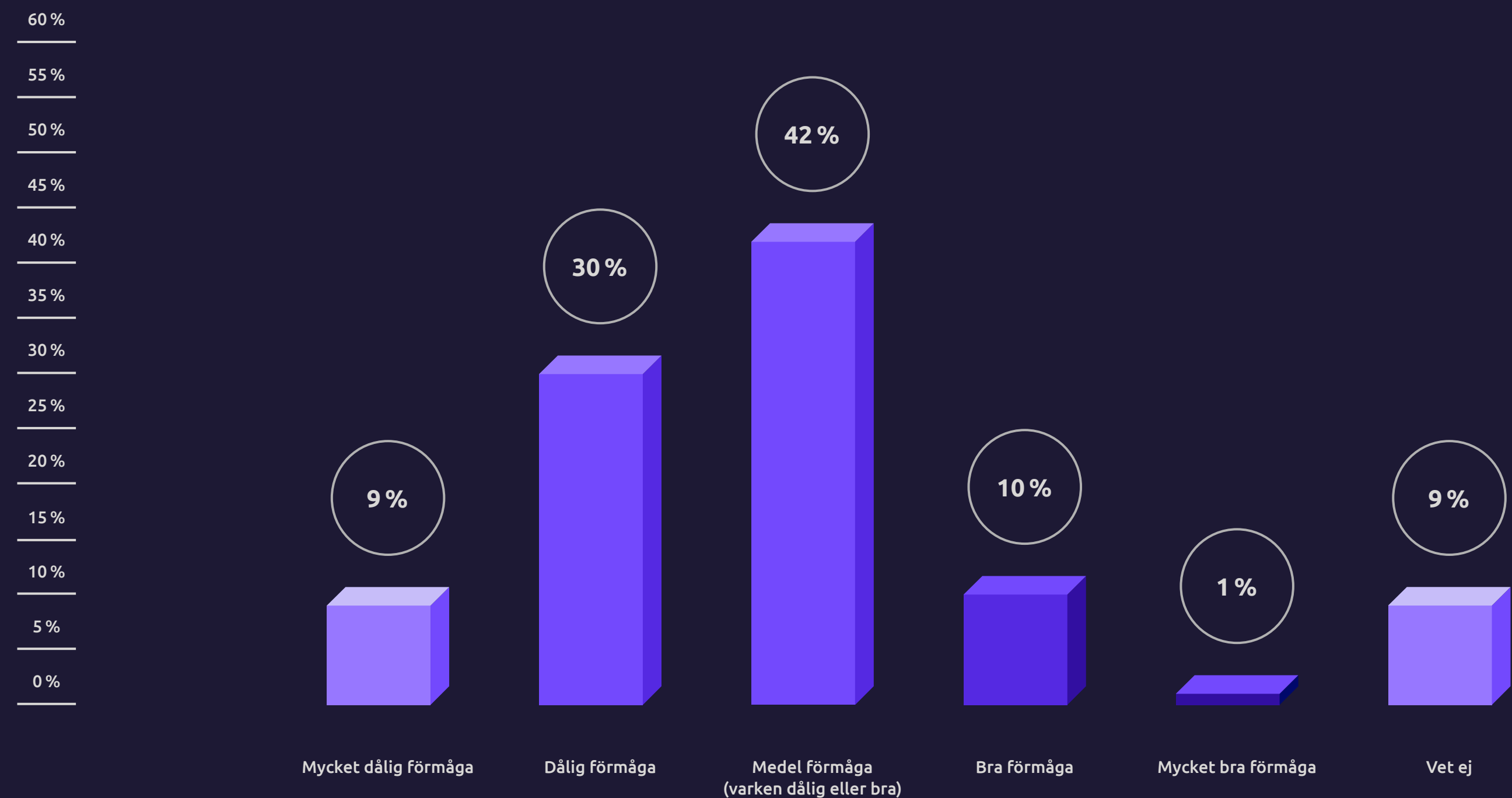
03.5

Det råder *låg tilltro* till samhällets hantering av etiska och rättsliga frågor kring teknologisk utveckling.

39 % anser att samhället har dålig eller mycket dålig förmåga i detta avseende. För 42 % är neutrala i frågan.

Endast 11 %, en grupp som är överrepresenterad i åldersgruppen 18–29 år, anser att förmågan är bra eller mycket bra.

Åsikter om samhällets förmåga att hantera etiska och rättsliga frågor



Bas: 1014 ip

04

Kunskap om OT

Sammanfattning kunskap om OT

Det kommande kapitlet undersöker svenskarnas uppfattning om operativ teknologi (OT) och dess säkerhet. Vi granskar deras kännedom om IT- och OT-säkerhet, hur viktigt de tycker att det är att Sverige tar en ledande roll inom området och hur väl allmänheten upplever samhället och svenska industrier skyddar kritisk infrastruktur och verksamheter idag.

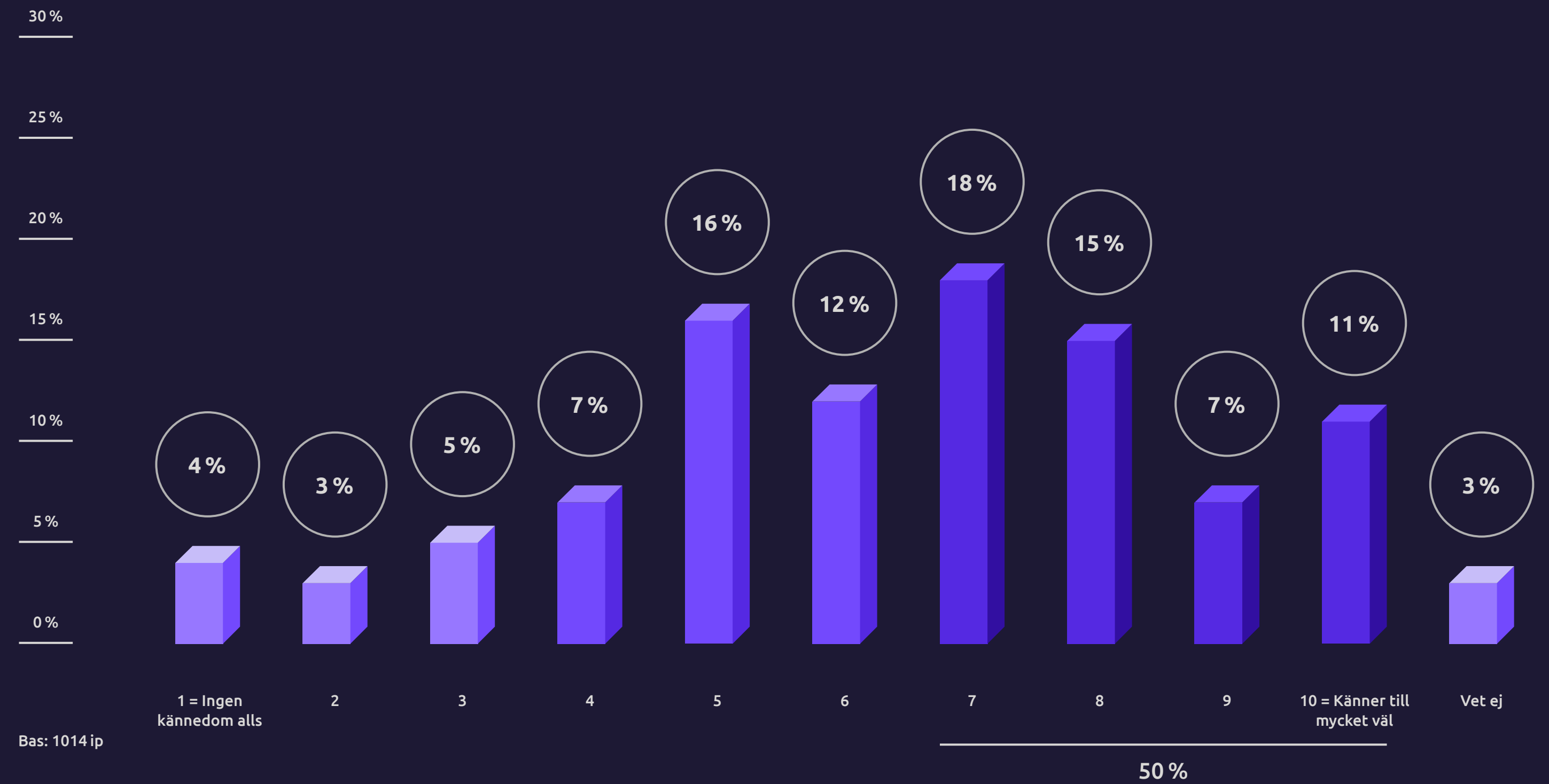
04.1

Hälften av respondenterna känner *väl* eller *mycket väl* till uttrycket IT-säkerhet

Kännedomen om IT-säkerhet är relativt hög och män är överrepresenterade i denna grupp.

Bara 12 % svarar att de känner till uttrycket lite eller inte alls.

Kunskap om IT-säkerhet

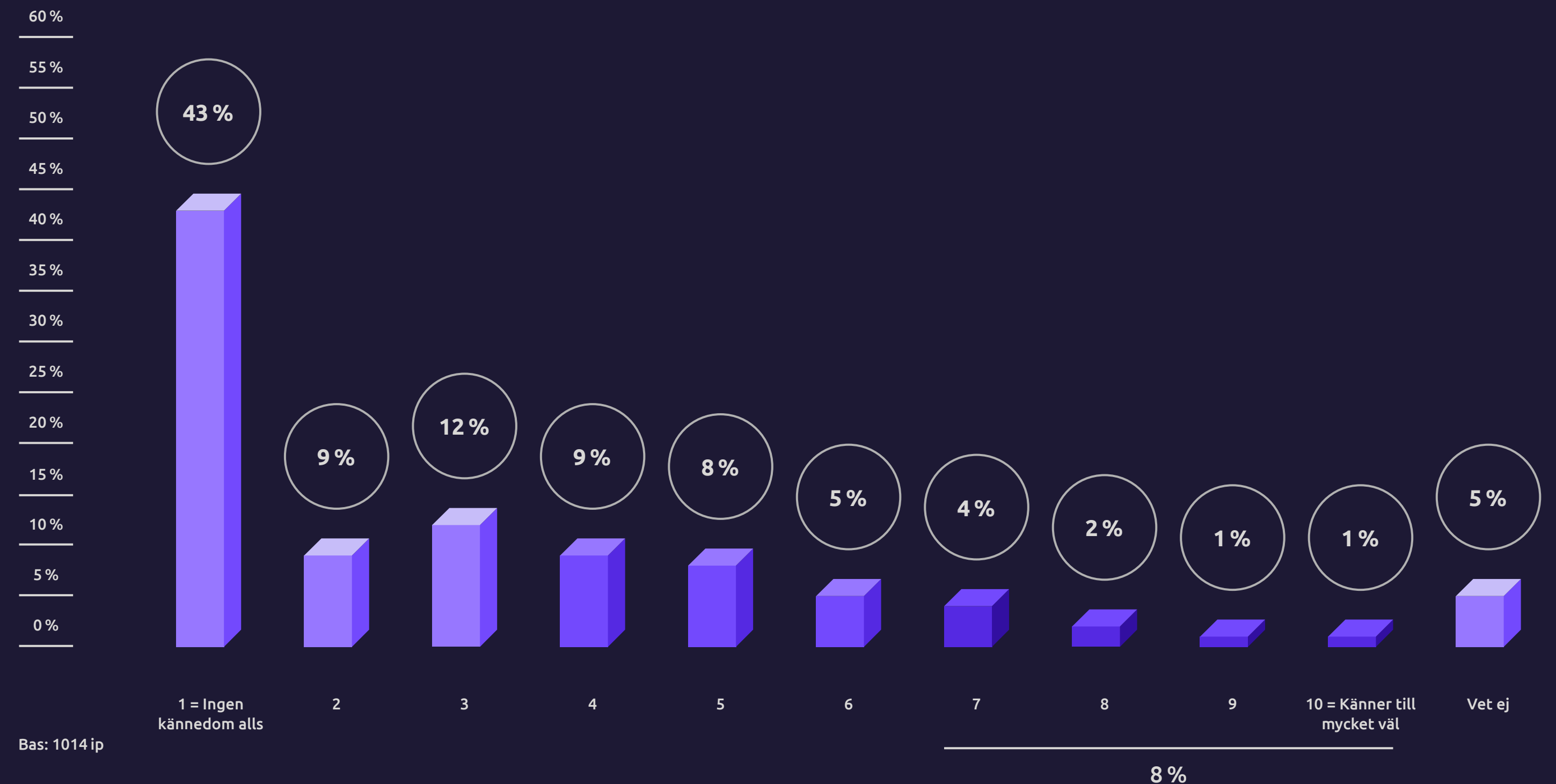


04.2

Kunskapen kring uttrycket OT-säkerhet är *låg*, betydligt lägre än om IT-säkerhet

Kännedomen om OT-säkerhet är generellt låg. 43 % svarar att de inte har någon kännedom alls. Endast 8 % svarar att de känner till uttrycket ganska eller mycket väl. Kännedomen är högre bland männen och bland de yngre åldersgrupperna.

Kunskap om OT-säkerhet

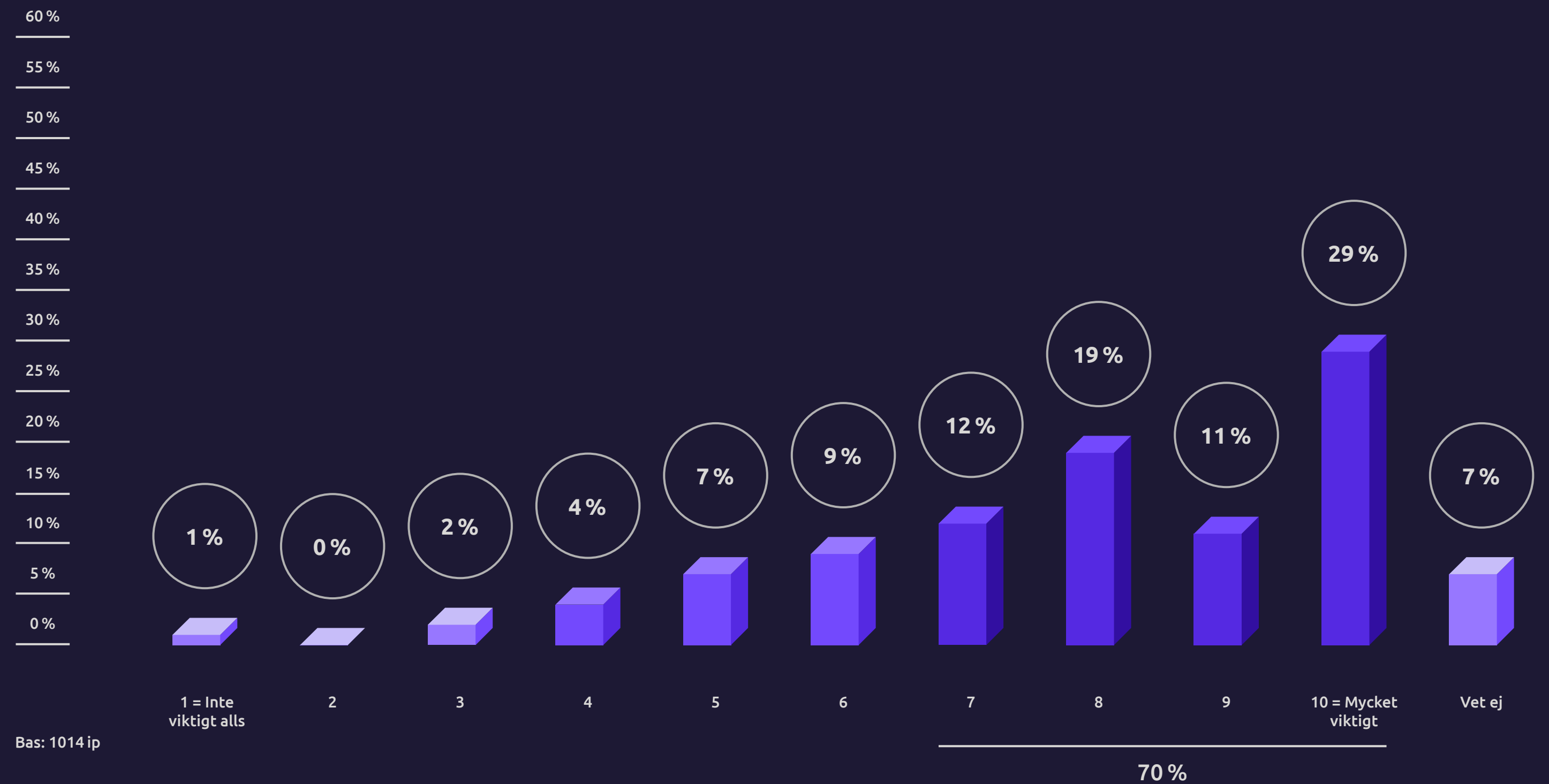


04.3

En majoritet anser att det är *viktigt* att Sverige ligger i framkant kring OT-säkerhet

Efter att ha läst en informationstext om OT-säkerhet anser 70 % av respondenterna att det är viktigt eller mycket viktigt att Sverige är ledande inom detta område.

Syn på vikten av OT-säkerhet



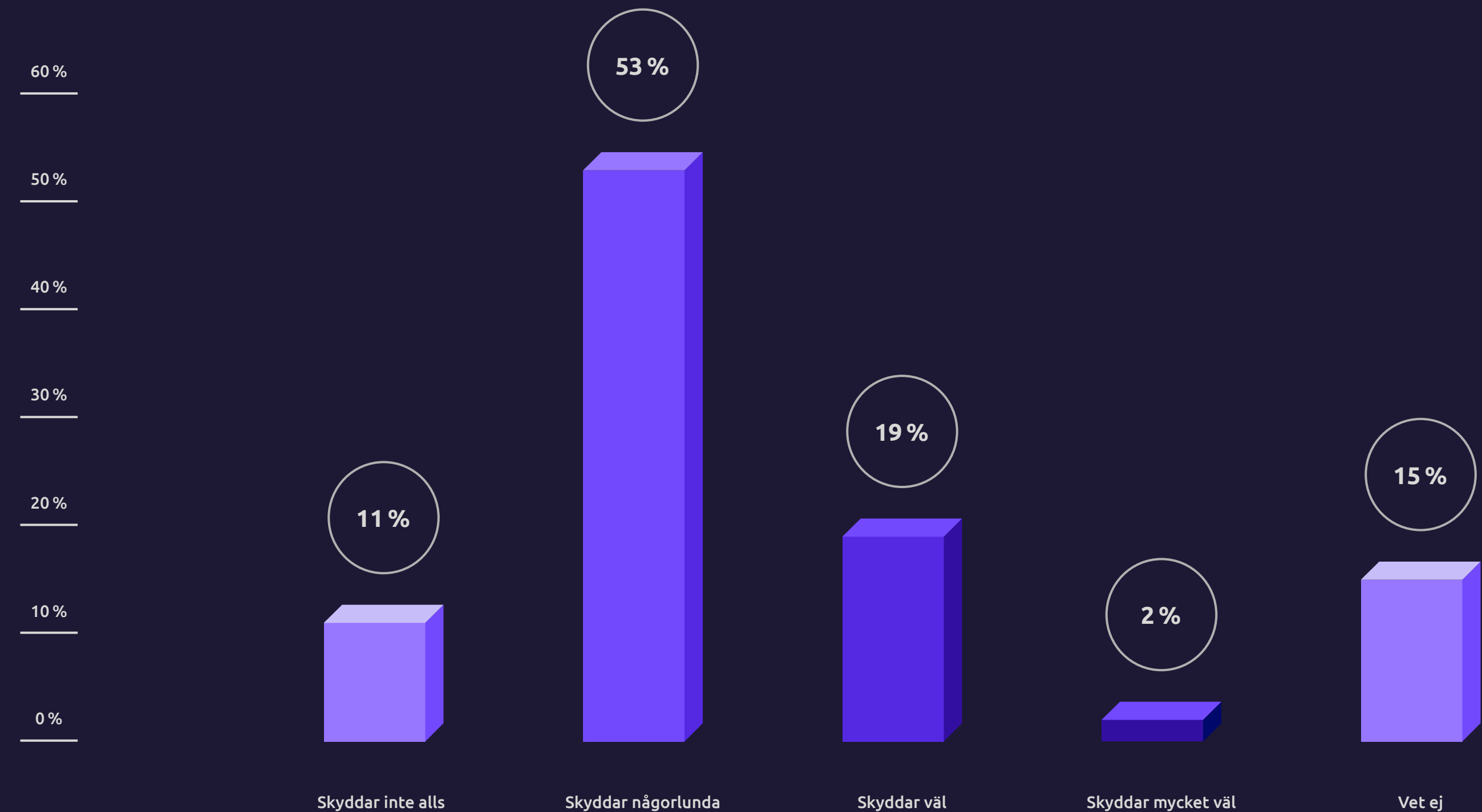
04.4

En övervägande majoritet anser att Sverige *inte säkerställer* tillräckligt skydd för sin kritiska infrastruktur idag

64 % anser att skyddet är otillräckligt, medan 21 % anser att skyddet är tillräckligt eller mycket bra. Denna uppfattning är mer uttalad i gruppen 18–29 år.

15 % svarar att de inte har en klar uppfattning.

Syn på samhällets skydd av kritisk infrastruktur



Bas: 1014 ip

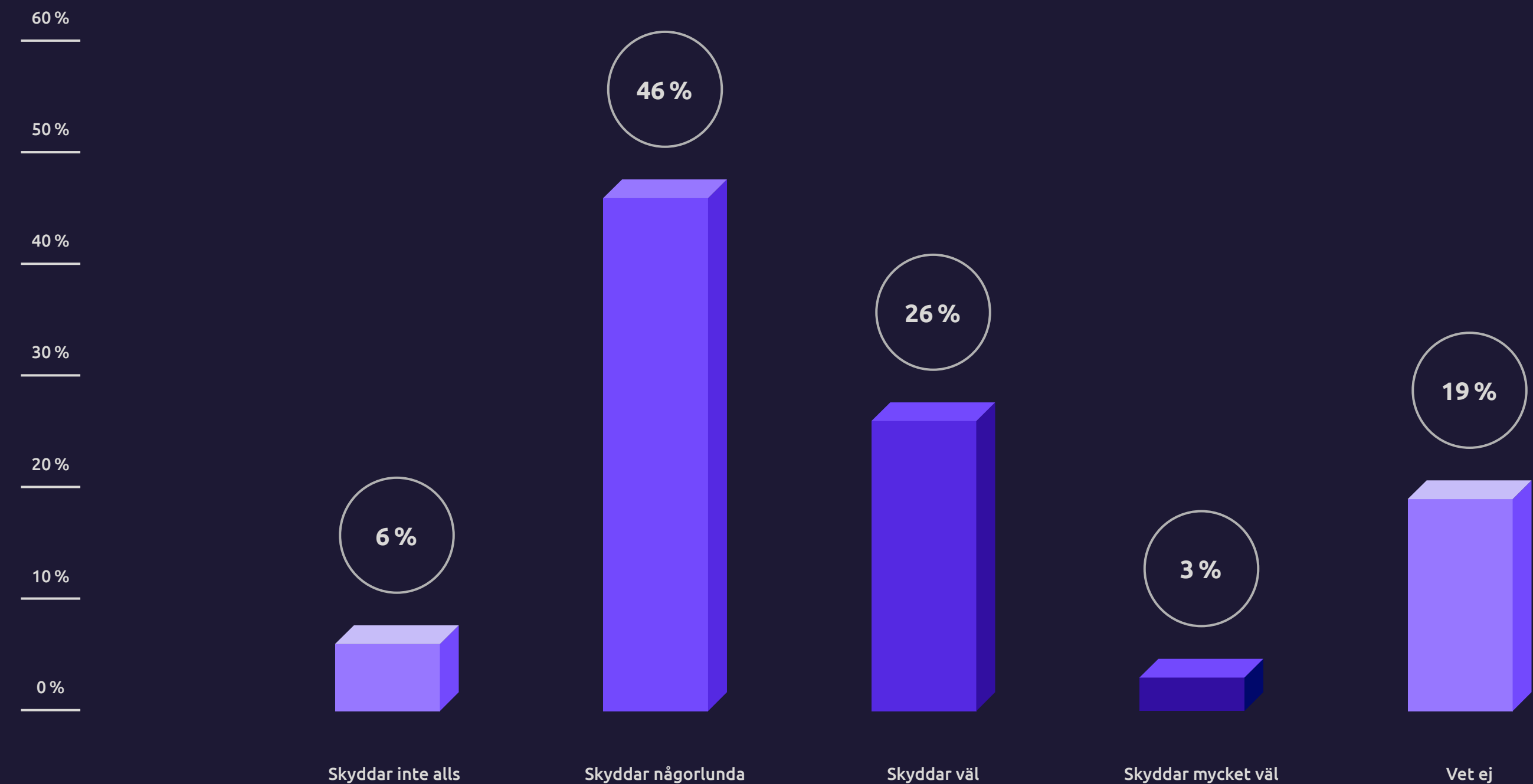
04.5

Lite över hälften anser att svenska industrier *inte tillräckligt* säkrar sina verksamheter idag

52 % anser att svenska industrier inte erbjuder tillräckligt skydd för sina verksamheter. Å andra sidan anser 29 % att svensk industri erbjuder god eller mycket god säkerhet för sina verksamheter. Denna åsikt är mer utbredd bland individer i åldersgruppen 18–29 år.

19 % har svarat "vet ej".

Syn på industriers verksamhetsskydd



Bas: 1014 ip

Företagen



05

Framtidssyn

Sammanfattning framtidssyn

Det kommande kapitlet granskar svenska företags perspektiv på operativ teknik (OT) och dess påverkan. Vi undersöker deras oro för avancerade cyberattacker, deras uppfattning om framtida utmaningar inom OT och deras syn på innovationens roll i framtiden.

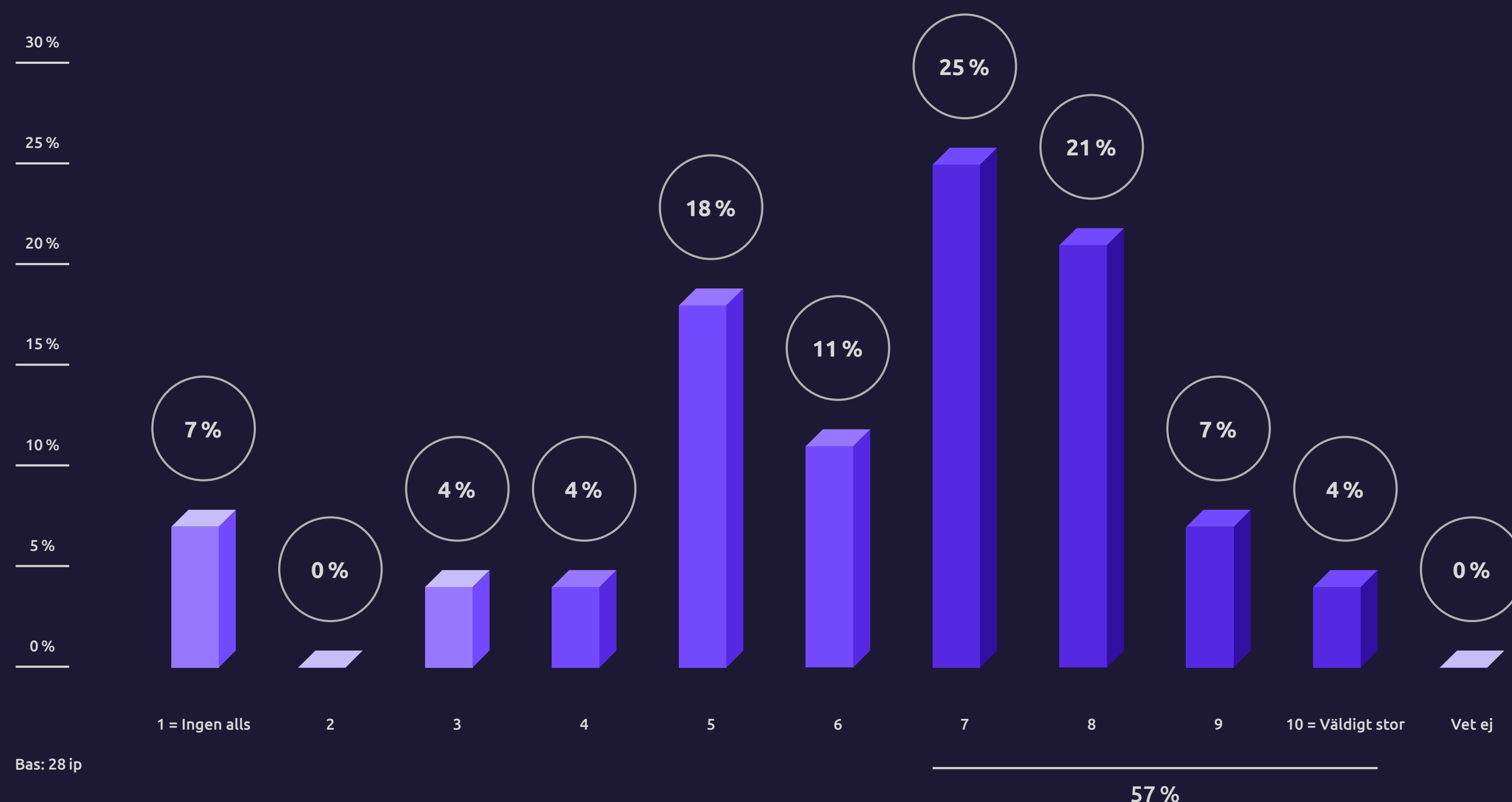
05.1

6 av 10 företag känner *stor* eller *väldigt stor* oro för att drabbas av cyberattacker

57 % känner stor eller väldigt stor oro för möjligheten att drabbas av avancerade och sofistikerade cyberattacker inom deras industri.

Det är främst respondenter med verksamhet inom offentlig sektor, sjukvård och smart factory som anger att de känner stor eller väldigt stor oro för att drabbas.

Oro för att drabbas av cyberattacker



05.2

Respondenterna identifierar att de kan stå inför utmaningar inom säkerhet & skydd, tekniska utmaningar och framtid & innovation.

Respondenterna betonar behovet av bättre IT-säkerhet och att förebygga ransomware. Utmaningarna inkluderar ekonomisk lönsamhet, övergång från stordatorer och att hantera användarnas sårbarhet. Framtiden ser positiv ut med AI och hållbarhet, men det finns oro för nya attacker och kompetensbehov. Osäkerhet råder kring produktion och framtiden.

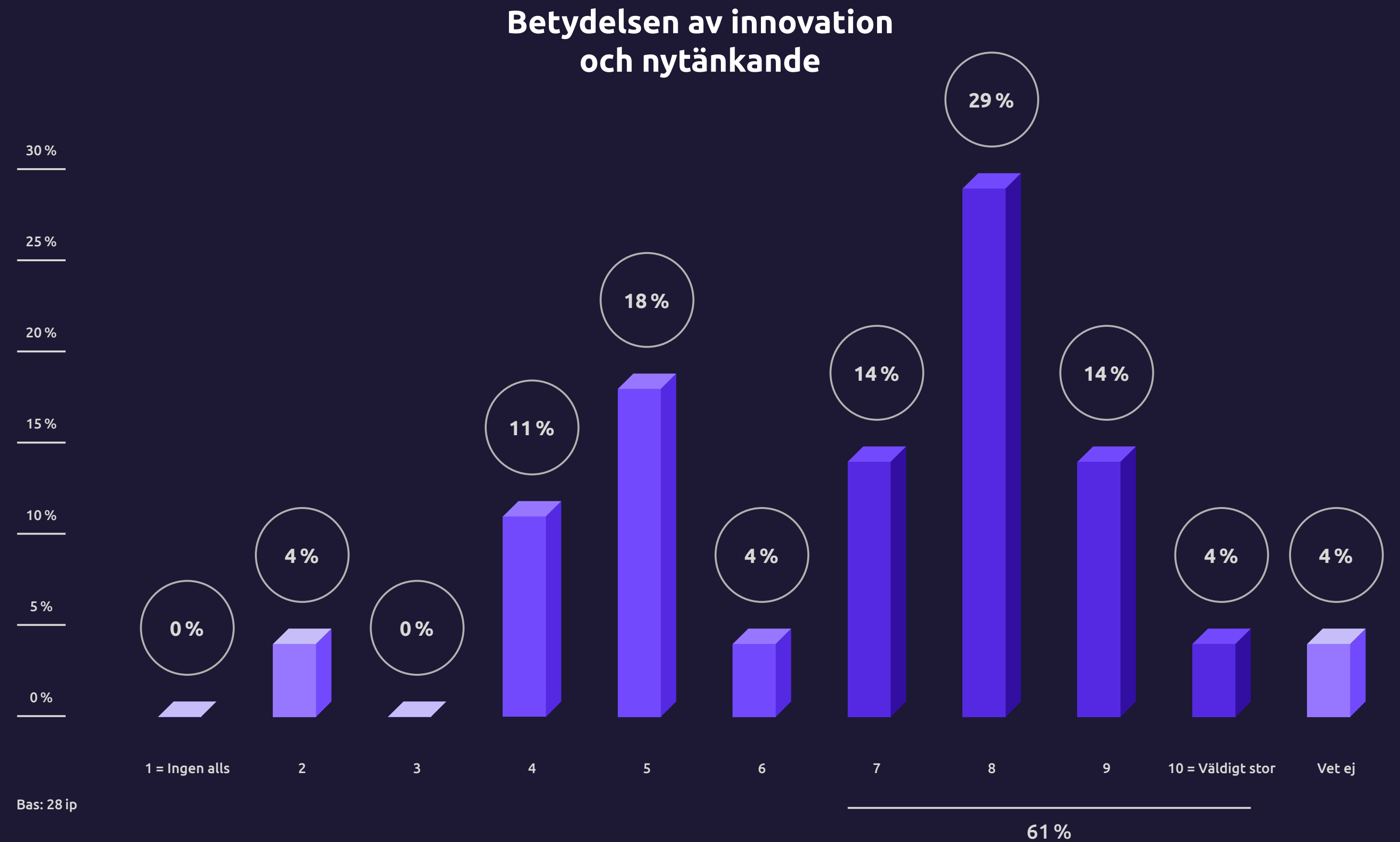
För alla svarsalternativ, se appendix 2 på sida 75.

05.3

6 av 10 anser att innovation och nytänkande kommer ha en stor betydelse för deras industris framtid

En majoritet, 61 %, menar att innovation och nytänkande kommer att ha en stor eller väldigt stor betydelse för sin industris framtid med tanke på utvecklingen som sker inom operativ teknik (OT).

Det är främst respondenter med verksamhet inom offentlig sektor, sjukvård och tillverkning som anser att innovation och nytänkande kommer ha stor eller mycket stor betydelse för industrins framtid.



06

Beredskap

Sammanfattning beredskap

I detta kapitel undersöks hur svenska företag hanterar operativ teknik (OT) och cybersäkerhet, graden av etablerade säkerhetsprotokoll, hur de utvärderar säkerhet och utbildar personal. Deltagarna bedömer även betydelsen av regleringar och standarder för industrins hantering av OT och cybersäkerhet i framtiden.

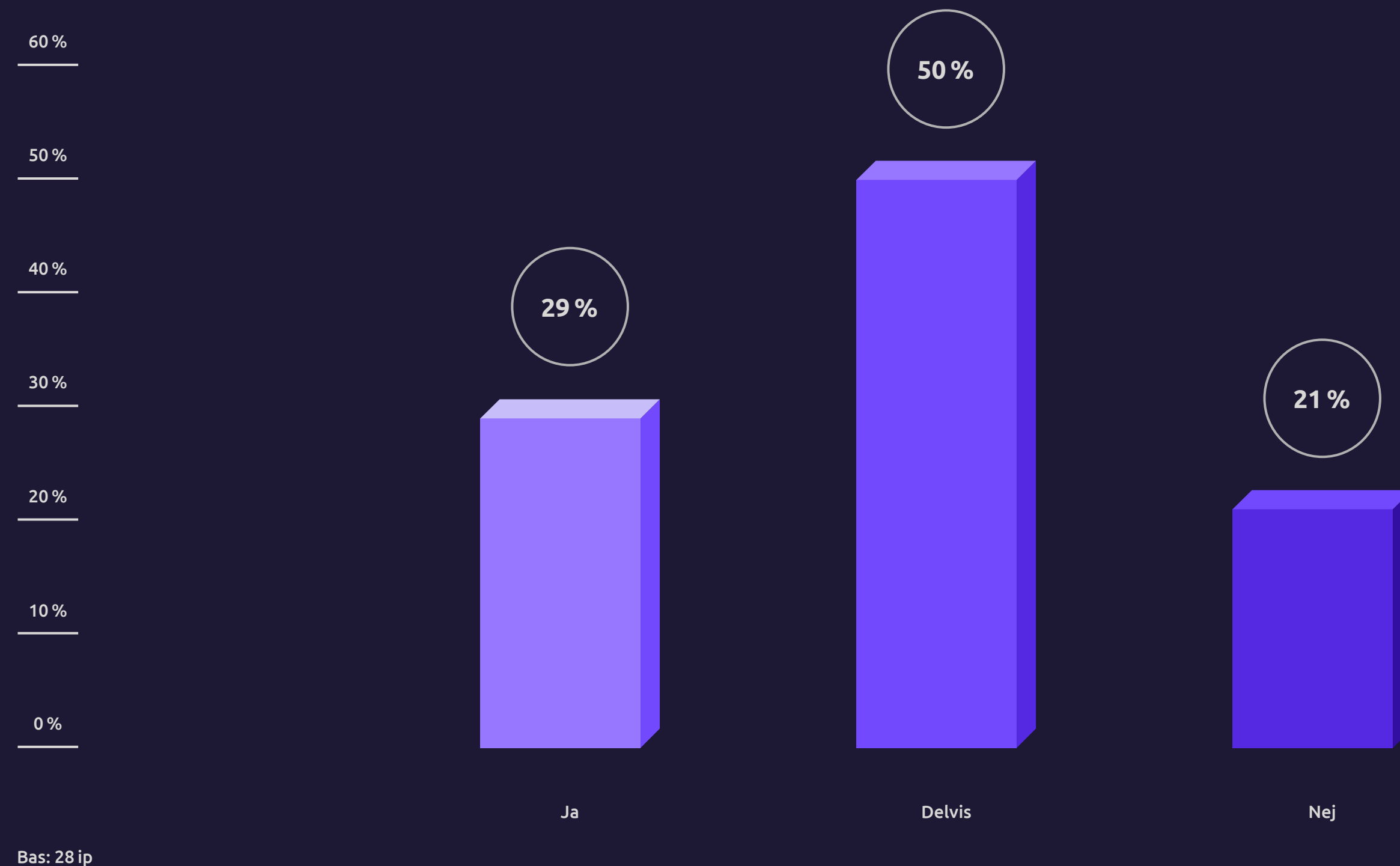
06.1

Var femte företag har idag *inte etablerat* specifika åtgärder för eventuella OT-hot och attacker

Av de tillfrågade företagen har 21 % inte etablerat några säkerhetsprotokoll och planer för eventuella OT-hot och attacker.

50 % svarar att deras företag delvis har etablerat specifika säkerhetsprotokoll och planer för detta och endast 29 % av respondenterna svarar att deras företag helt har etablerat specifika säkerhetsprotokoll och planer för att hantera potentiella OT-hot och attacker.

Etablerade säkerhetsprotokoll för OT-miljön



06.2

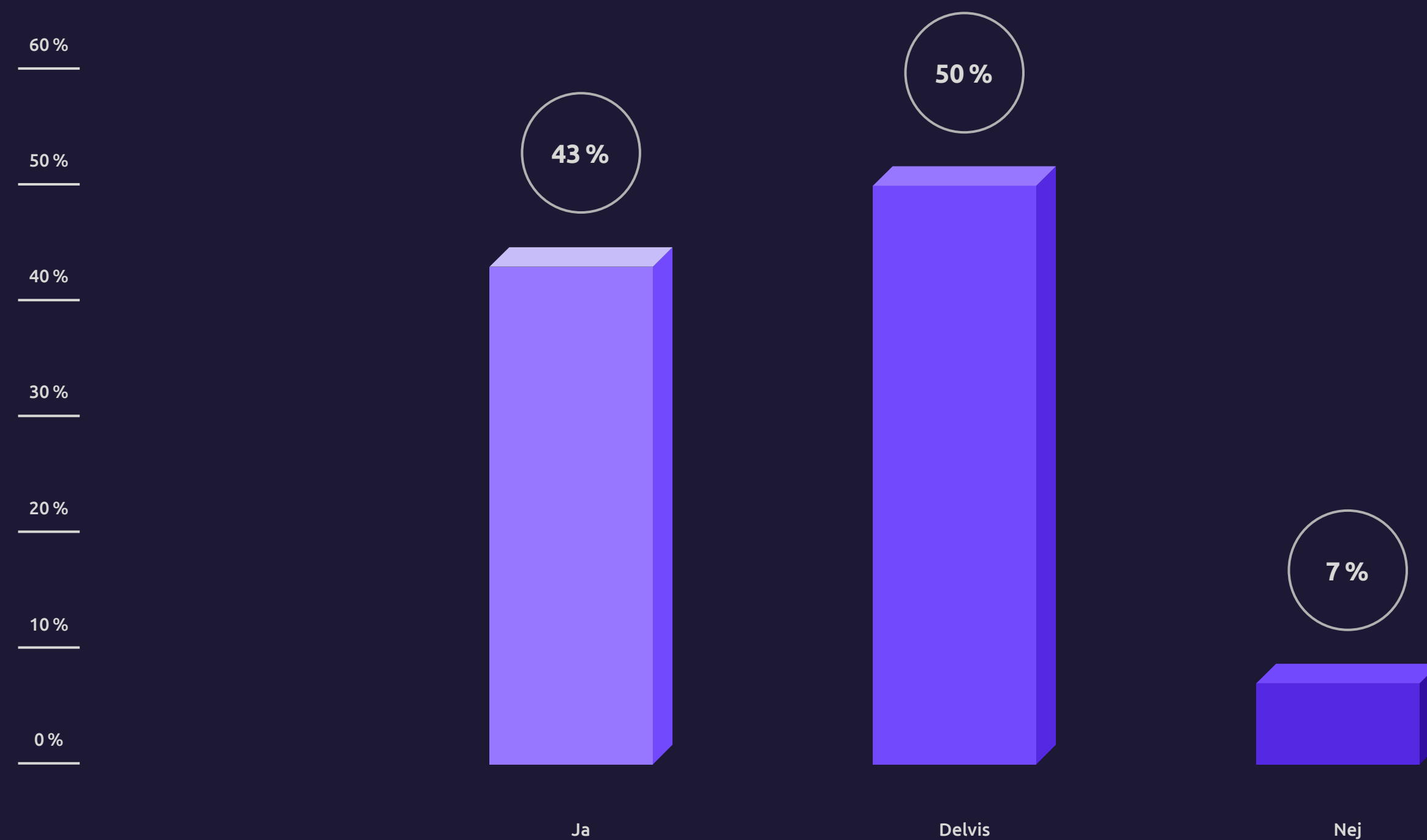
Lite mindre än hälften av företagen har *helt etablerat* specifika säkerhetsprotokoll och planer för IT-hot och attacker

43 % av respondenterna svarar att deras företag har etablerat specifika säkerhetsprotokoll och planer för att hantera potentiella IT-hot och attacker.

Hälften av respondenterna (50 %) svarar att deras företag delvis har etablerat specifika säkerhetsprotokoll och planer för sin IT-miljö.

7 % har inte etablerat något alls.

Etablerade säkerhetsprotokoll för IT-miljön



Bas: 28 ip

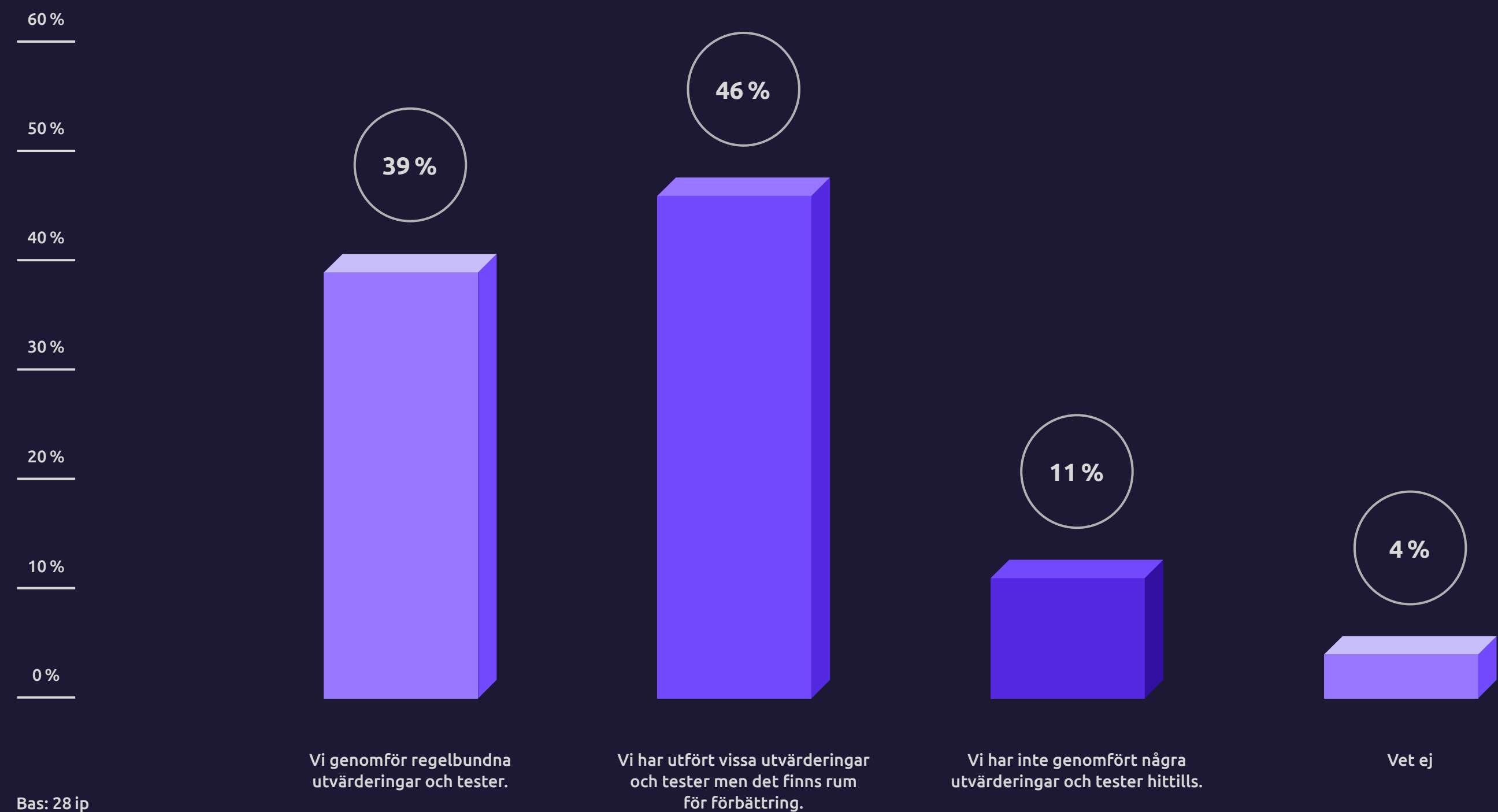
06.3

4 av 10 företag genomför regelbundna utvärderingar och tester i sina operativa tekniksystem

Dessa företag genomför regelbundna utvärderingar och tester för upptäcka och åtgärda potentiella sårbarheter i deras operativa tekniksystem.

46 % svarar att deras företag har utfört vissa utvärderingar och tester, men att det finns rum för förbättring och 11 % har hittills inte genomfört några utvärderingar eller tester.

Frekvens på säkerhetsutvärderingar och tester i OT-miljön



Q: Hur regelbundet genomför ni säkerhetsutvärderingar och penetrationstester för att upptäcka och åtgärda potentiella sårbarheter i era operativa tekniksystem?

06.4

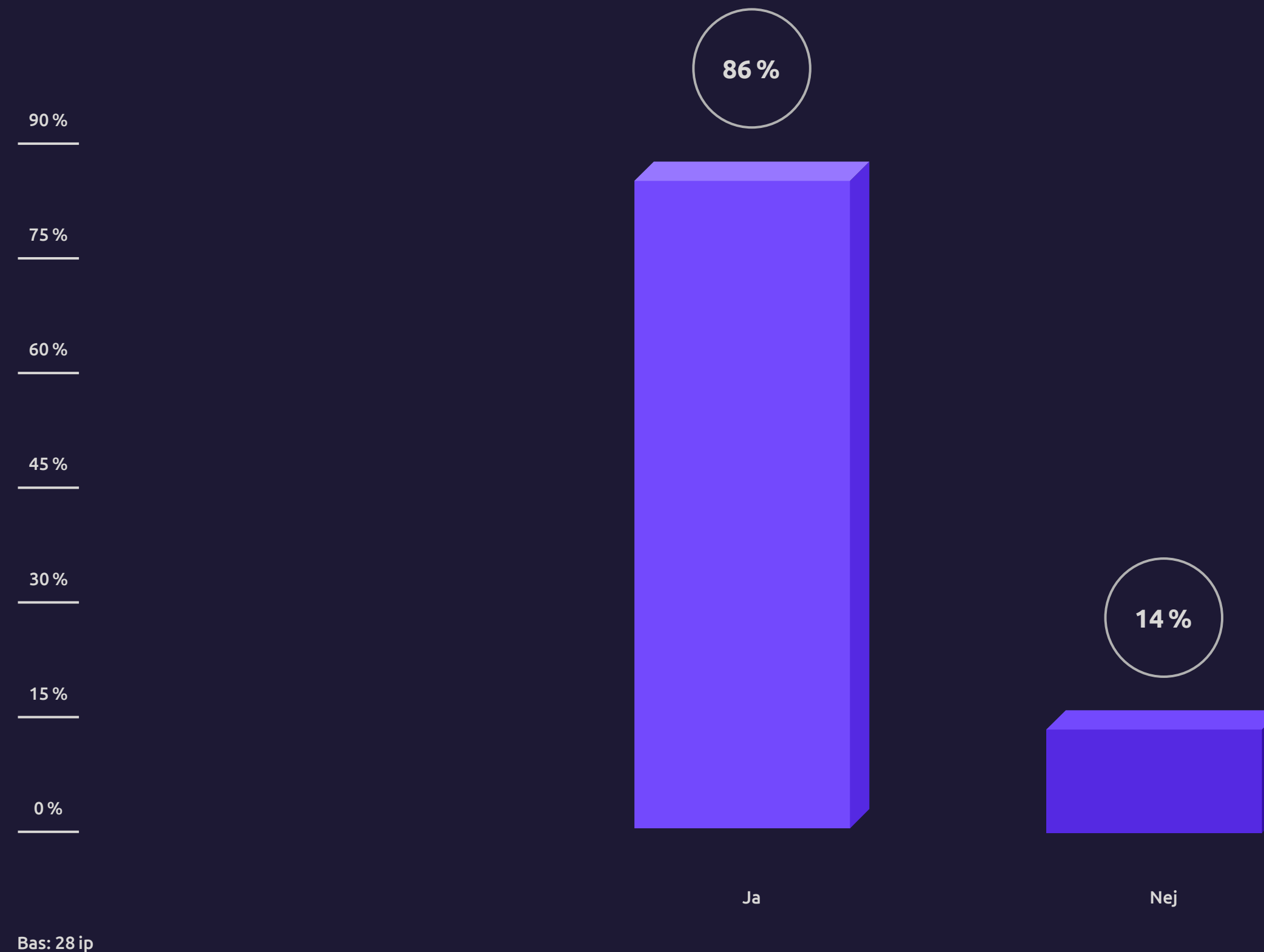
Majoriteten av företagen utbildar sin personal i säkerhetsfrågor idag

86 % av respondenterna svarar att deras företag utbildar deras personal i säkerhetsfrågor.

Att utbilda sin personal i säkerhetsfrågor är mest vanligt inom tillverkningsindustrin, offentlig sektor, sjukvården och smart factories. De företag som utbildar sin personal gör det genom interna och externa utbildningar och kurser, oftast via en tredje part. De som svarar att de inte utbildar sin personal i säkerhetsfrågor anger att anledningarna till detta är oförståelse hos ledningen, tidsbrist eller otillräcklig ekonomi.

För alla svarsalternativ, se appendix 2 på sida 76.

Utbildning av personal i säkerhetsfrågor



Q: Utbildar ni er personal i säkerhetsfrågor?

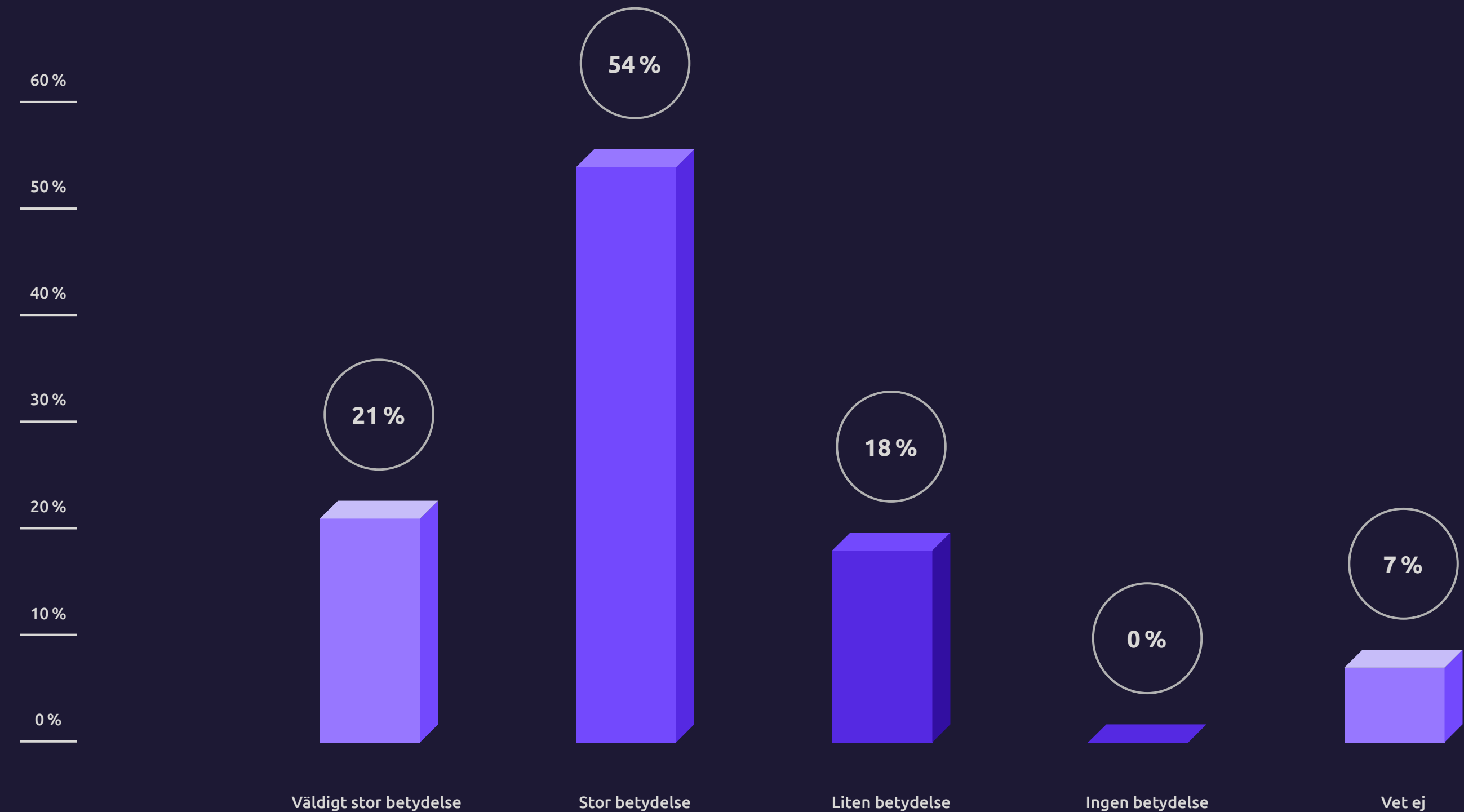
06.5

3 av 4 företag tror att regleringar och standarder kommer ha *stor* eller *väldigt stor* betydelse i framtiden

75 % av respondenterna svarar att regleringar och standarder kommer att ha stor eller väldigt stor betydelse för deras industris hantering av operativ teknik (OT) och cybersäkerhet i framtiden.

Endast 18 % anser att det har en liten betydelse.

Betydelsen av regleringar och standarder



Bas: 28 ip

Q: Hur stor betydelse tror ni att regleringar och standarder kommer att ha för er industris hantering av operativ teknik (OT) och cybersäkerhet i framtiden?

07

Teknik

Sammanfattning teknik

Detta kapitel undersöker svenska företags syn på att hålla sig uppdaterad om trender och hur de förbereder sin verksamhet för framväxande teknologier. Respondenterna bedömer även hur viktigt de tycker att det är att investera i innovation och forskning för att möta framtida utmaningar.

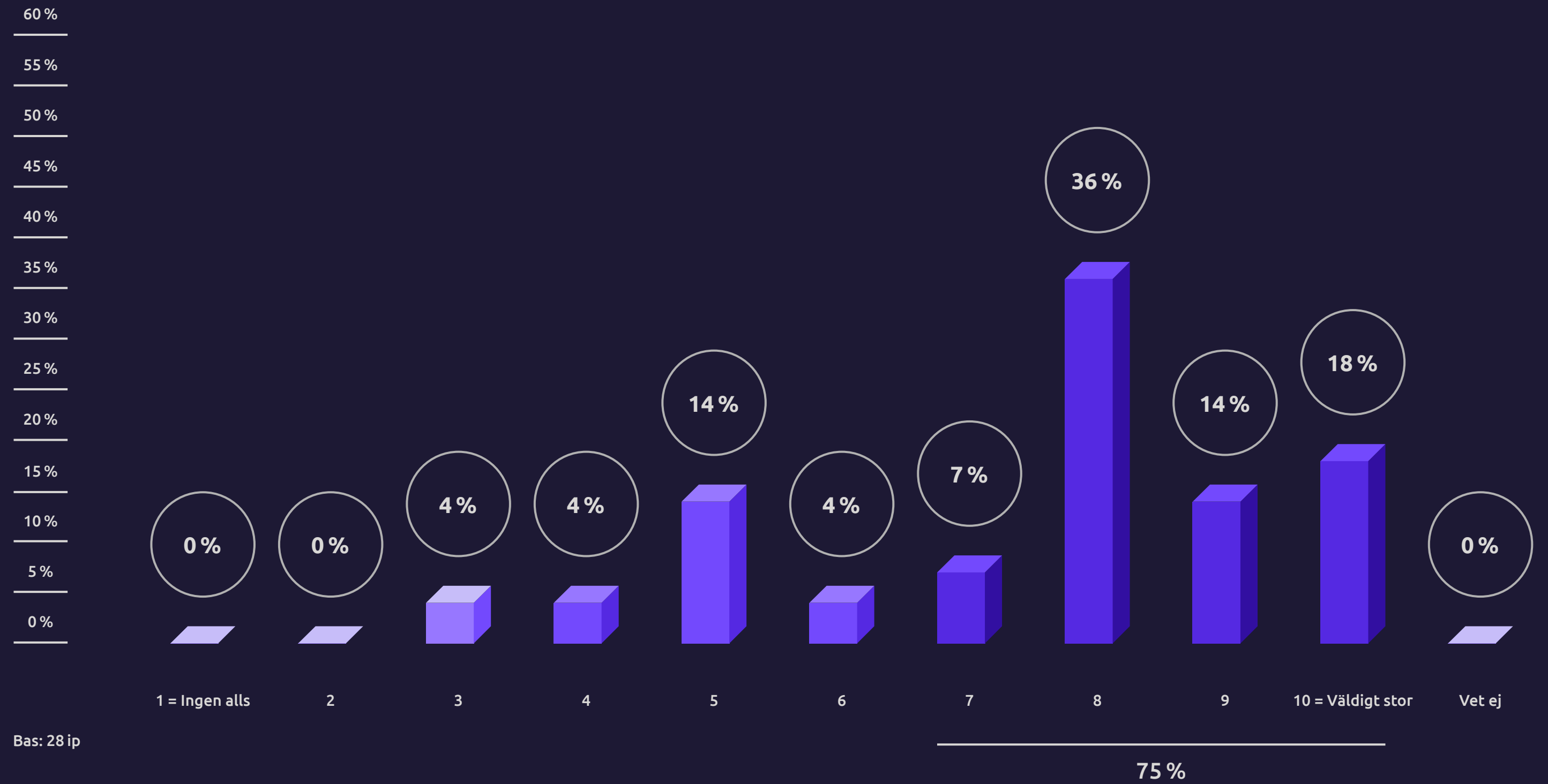
07.1

En stor majoritet anser att det är *viktigt* eller *mycket viktigt* att hålla sig uppdaterad om de senaste trenderna inom IT

Av respondenterna är det 75 % som anser att det är viktigt eller mycket viktigt att hålla sig uppdaterad kring de senaste trenderna inom IT.

Endast 4 % av respondenterna finner inte detta viktigt.

Vikten av att hålla sig uppdaterad om trender inom IT



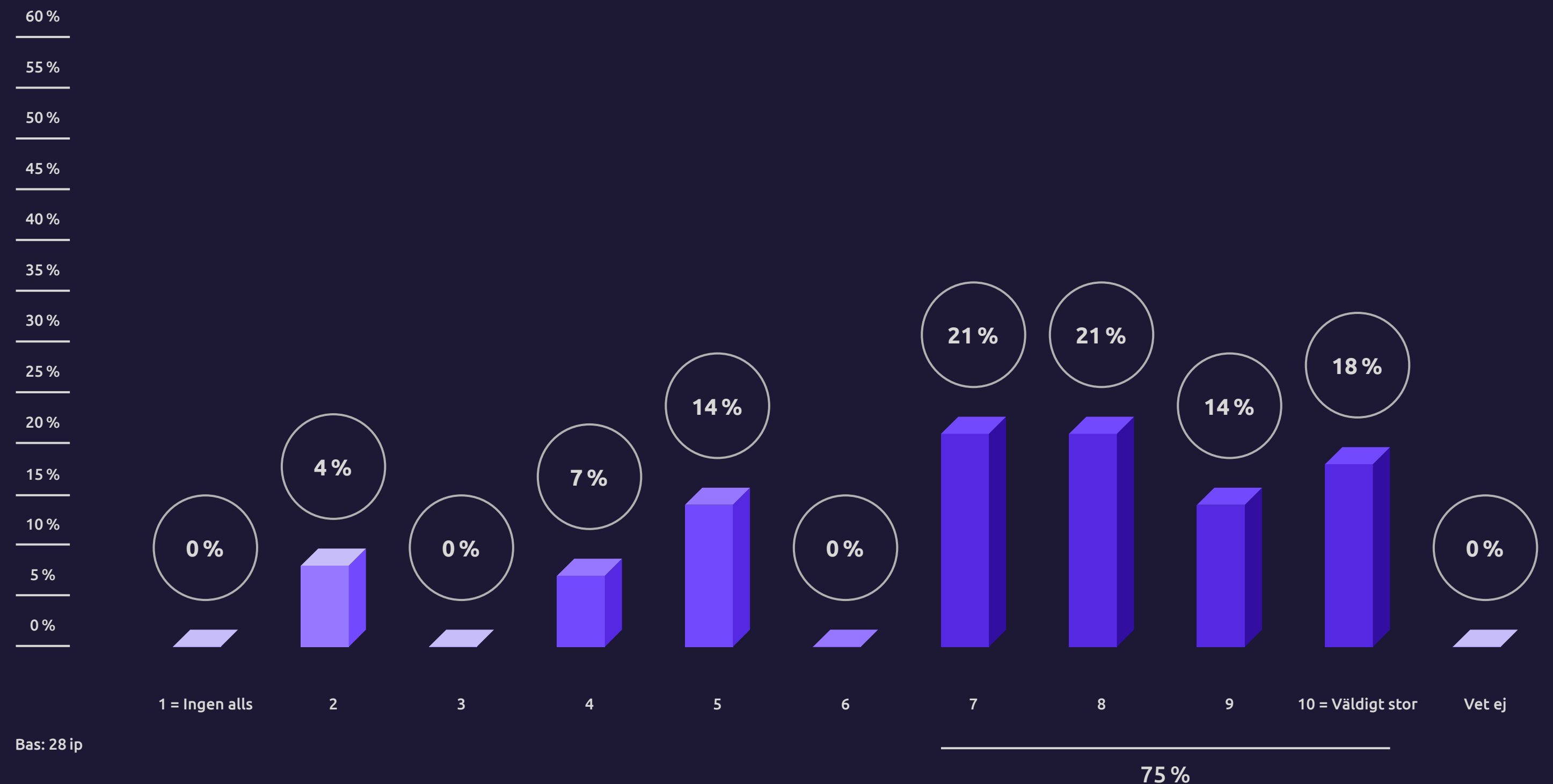
07.2

Majoriteten anser att det är *viktigt* eller *mycket viktigt* att hålla sig uppdaterad om de senaste trenderna inom OT

75 % anger att det är viktigt eller mycket viktigt att hålla sig uppdaterad om trender inom OT.

Endast 4 % av respondenterna finner inte detta viktigt.

Vikten av att hålla sig uppdaterad om trender inom OT



07.3

Majoriteten av företagen har ännu *inte implementerat* alla framväxande teknologier

Det är 43 % som uppger att de har implementerat några av de nämnda teknologierna och planerar fortsätta implementera övriga teknologier framöver.

Endast 14 % har implementerat alla teknologier, lika många (14 %) håller på med att undersöka och planera för implementering och 7 % har inga specifika planer på att implementera dessa teknologier.

Förberedelser för framväxande teknologier



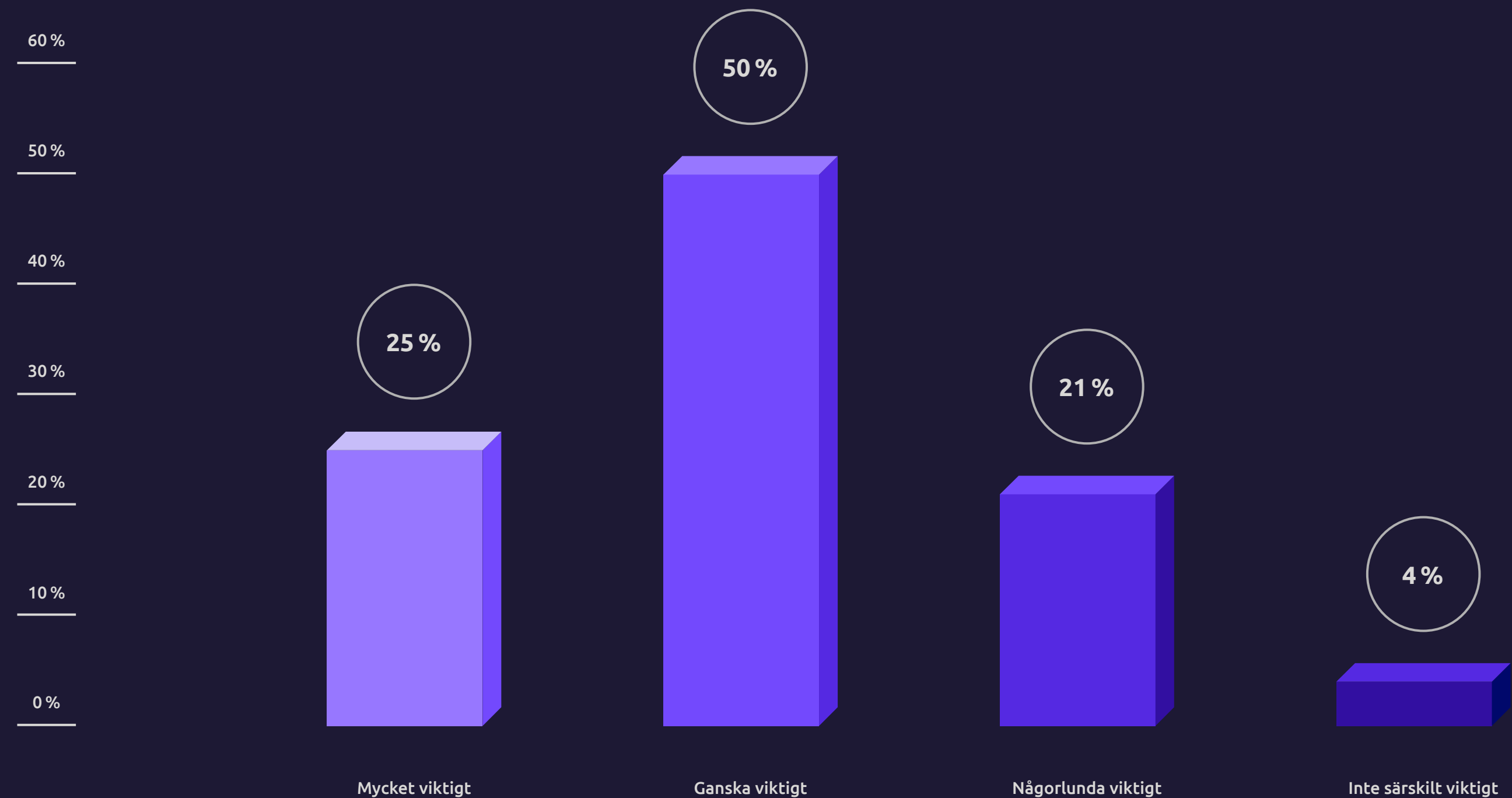
07.4

Majoriteten av företag anser att det är *ganska* eller *mycket viktigt* att investera i innovation och forskning kring OT

Det är 50 % som anser att det är ganska viktigt och 25 % att det är mycket viktigt att investera i innovation och forskning kring OT för att möta framtida utmaningar kopplade till OT inom sin industri.

4 % anser att det inte är särskilt viktigt.

Vikten av att investera i innovation och forskning kring OT



Bas: 28 ip

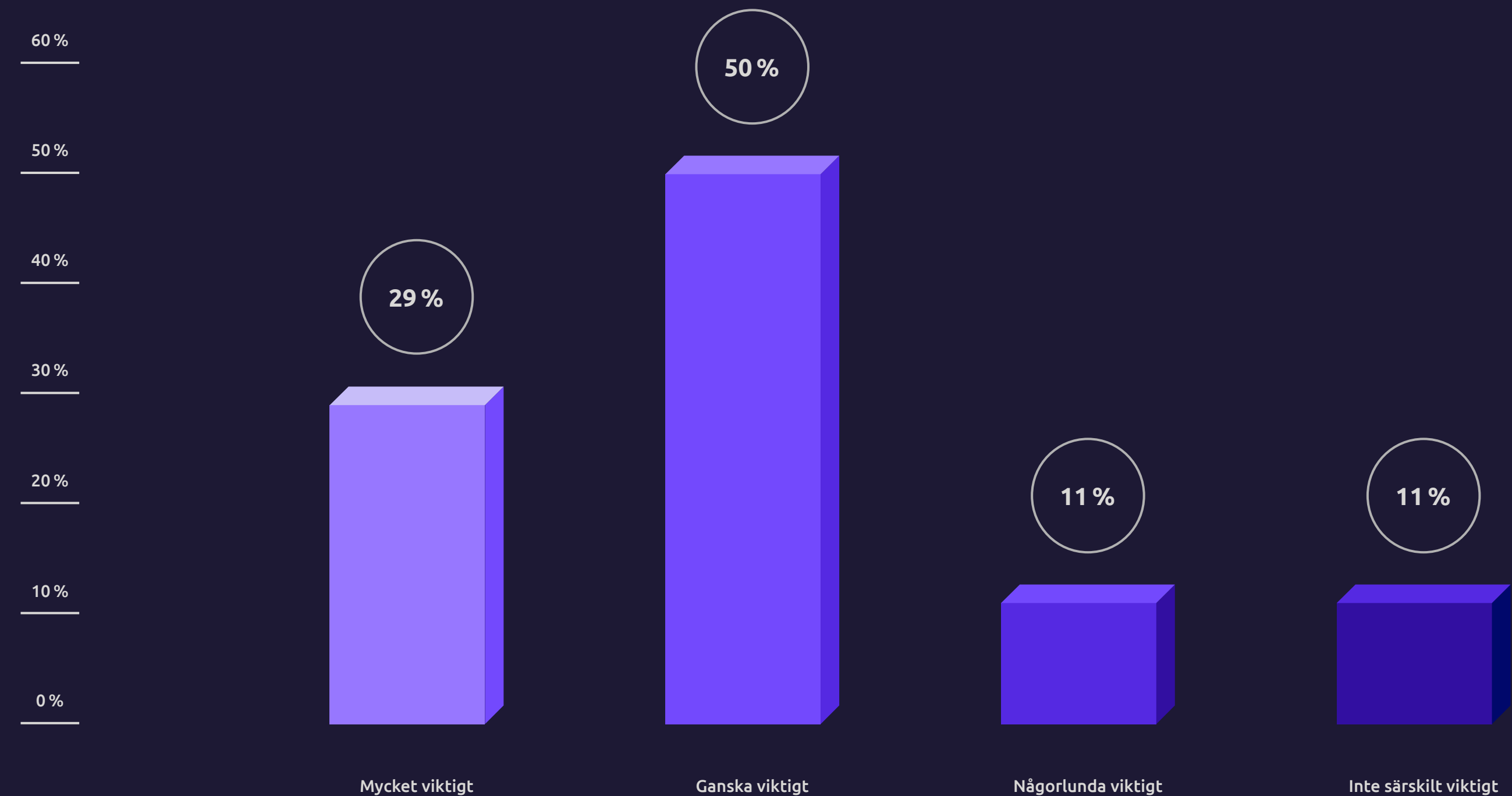
07.5

Majoriteten av företag anser att det är *ganska* eller *mycket viktigt* att investera i innovation och forskning kring IT

Det är 50 % som anser att det är ganska viktigt och 29 % att det är mycket viktigt att investera i innovation och forskning för att möta framtida utmaningar kopplade till IT inom sin industri.

11 % anser att det inte är särskilt viktigt.

Vikten av att investera i innovation och forskning kring IT



Bas: 28 ip

08

OT-säkerhet

Sammanfattning

OT-säkerhet

Det kommande kapitlet utforskar hur svenska företag hanterar operativ teknik (OT) och dess säkerhet. Vi undersöker deras syn på framtida förändringar inom OT, och deras strategier för att förbättra både säkerhet och effektivitet. Kapitlet inkluderar även deras beredskap, investeringar, prioriteringar, och hinder när det gäller OT-säkerhet.

08.1

61 % har haft minst 2–3 säkerhetshot eller cyberattacker de senaste 12 månaderna.

Det är 21 % av företagen som haft 2–3 säkerhetshot eller cyberattacker de senaste 12 månaderna. Lika många har haft fler än 20 säkerhetshot eller cyberattacker de senaste 12 månaderna.

18 % av respondenterna vet inte om de haft några säkerhetshot eller cyberattacker de senaste 12 månaderna.

Antal säkerhetshot/cyberattacker senaste 12 mån



Bas: 28 ip

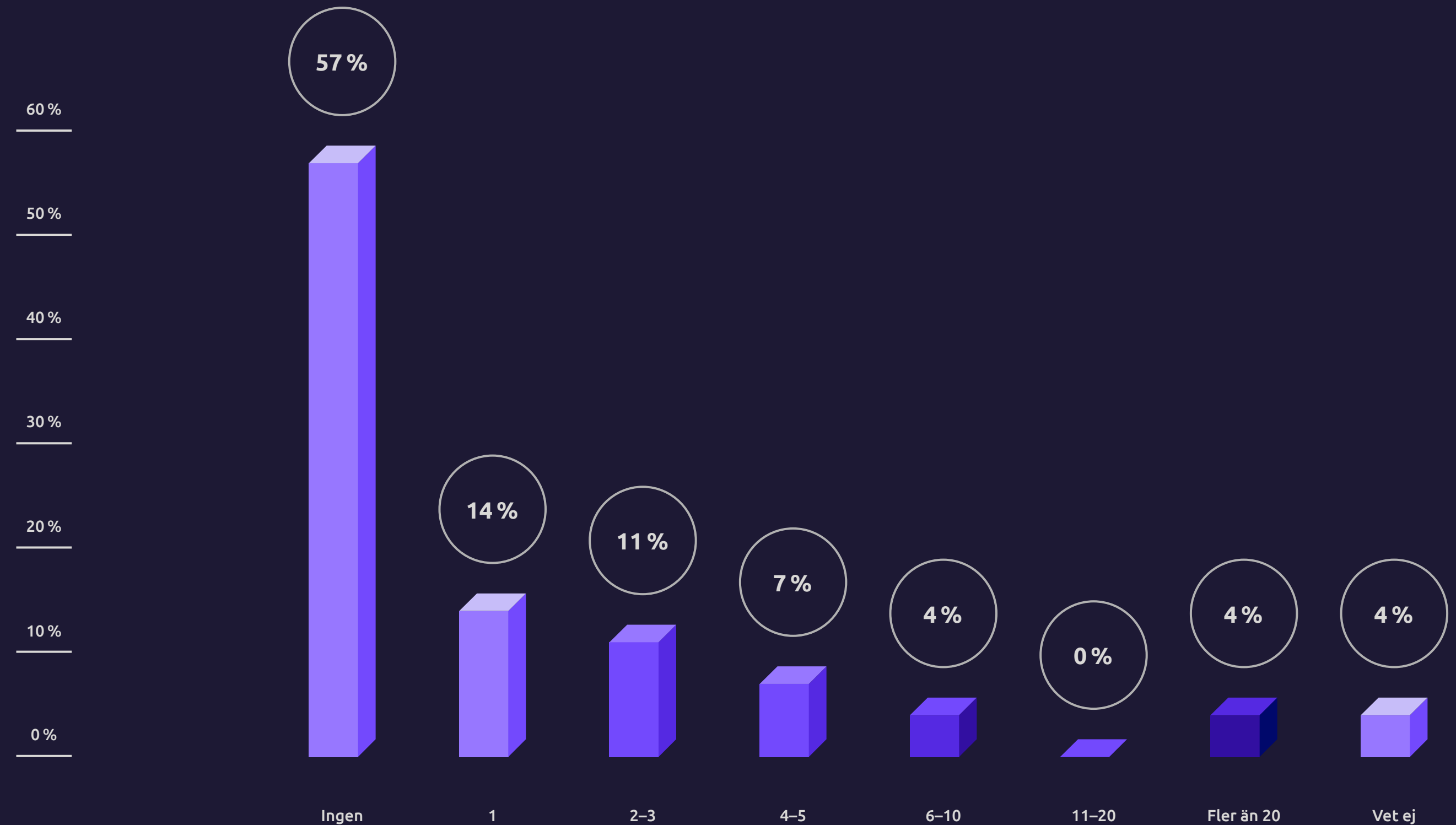
08.2

Det är 4 av 10 företag som haft *minst en incident* som lett till allvarliga konsekvenser

Det är även 15 % av företagen som uppger att de haft 4–5 eller fler allvarliga incidenter som orsakat större ekonomiska förluster eller fysisk skada de senaste 12 månaderna.

57 % av företagen har inte haft någon allvarlig incident som lett till större konsekvenser.

Antal allvarliga incidenter



Bas: 28 ip

Q: Hur många av dessa skulle du uppskatta har lett till allvarliga incidenter som orsakat större ekonomiska förluster eller fysisk skada de senaste 12 månaderna?

08.3

Majoriteten av de nämnda incidenterna är cybersäkerhetsrelaterade, endast några få nämner fysiska säkerhetsincidenter.

Incidenterna inkluderar cyberattacker från utländska länder, försök till lösenordsattacker, GDPR-relaterat läckage, intrångsförsök, mailattacker och överbelastningsattacker. Det har även förekommit fysiska incidenter som rån, stölder och inbrott.

Konsekvenserna var för många marginella men vissa anger att de fått stopp i produktion eller sanktioner.

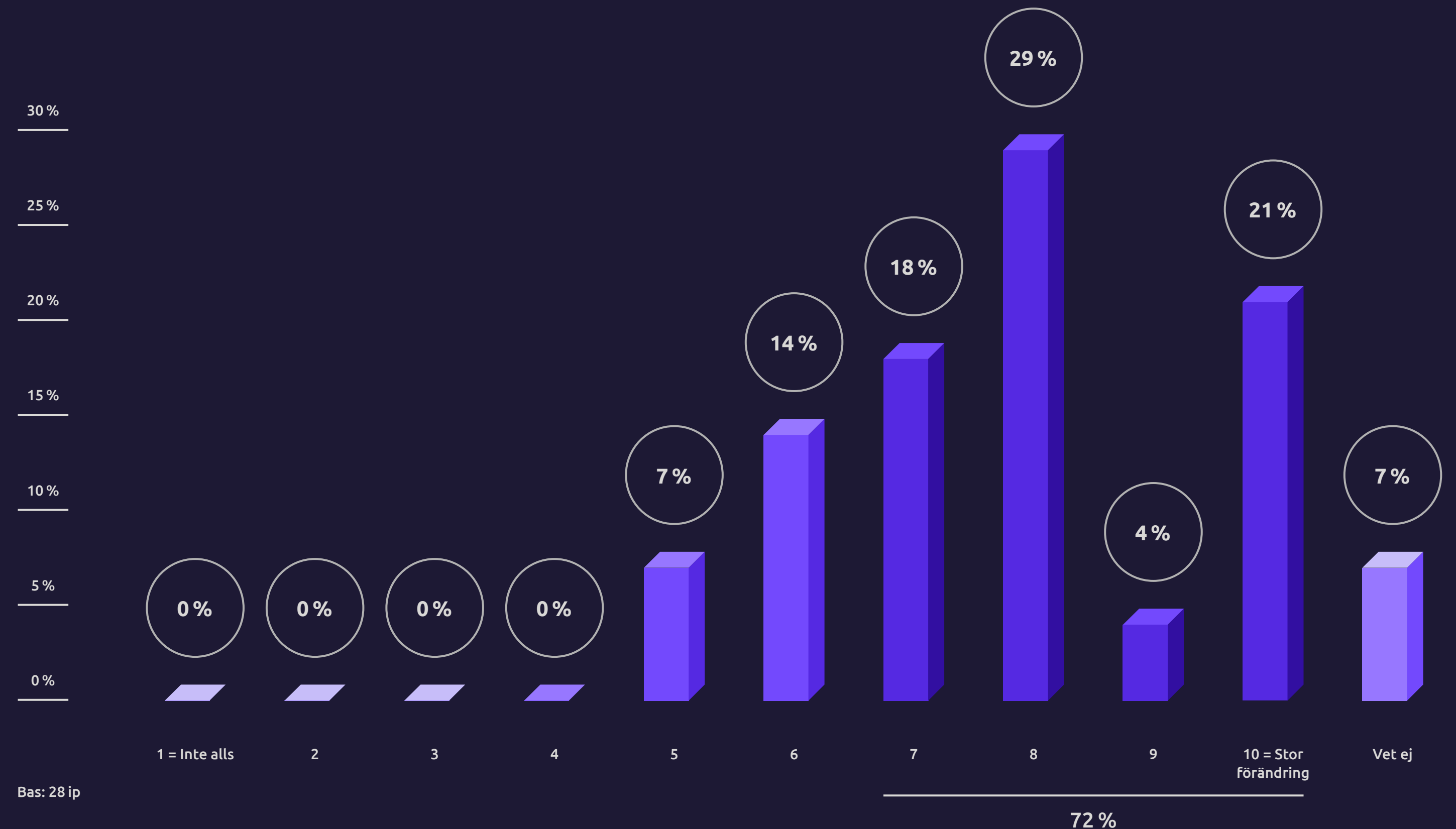
För alla svarsalternativ, se appendix 4 på sida 77.

08.4

Majoriteten tror att OT-landskapet kommer förändras och utvecklas framöver

Totalt är det 72 % som tror att OT-landskapet kommer genomgå en förändring eller en stor förändring framöver. Det är 21 % som svarar en 10:a.

Förändring och utveckling av OT-landskapet framöver



08.5

Respondenterna tror att de kan dra nytta av de framväxande teknologierna på flera sätt

Respondenterna tror på förbättrad säkerhet genom säkrare mjukvara och system, vilket möjliggör ostörd och säker arbetsmiljö. De ser också fördelar i teknologiska framsteg, särskilt genom att teknikverktyg blir mer allmänt tillgängliga, vilket gynnar även mindre företag. Att följa trender och utnyttja IT-synergier är i fokus, liksom att dra nytta av AI och automatisering för att öka effektiviteten och generera ökad efterfrågan och vinst.

För alla svarsalternativ, se appendix 5 på sida 78.

08.6

4 av 10 företag har en *robust och omfattande säkerhetsstrategi* och implementerar kontinuerliga åtgärder

Hälften av företagen uppger att de har genomfört vissa säkerhetsåtgärder, men att det finns utrymme för att göra vissa förbättringar.

11 % har inte genomfört några säkerhetsåtgärder alls.

Skydda och säkra operativa teknikersystem



Bas: 28 ip

08.7

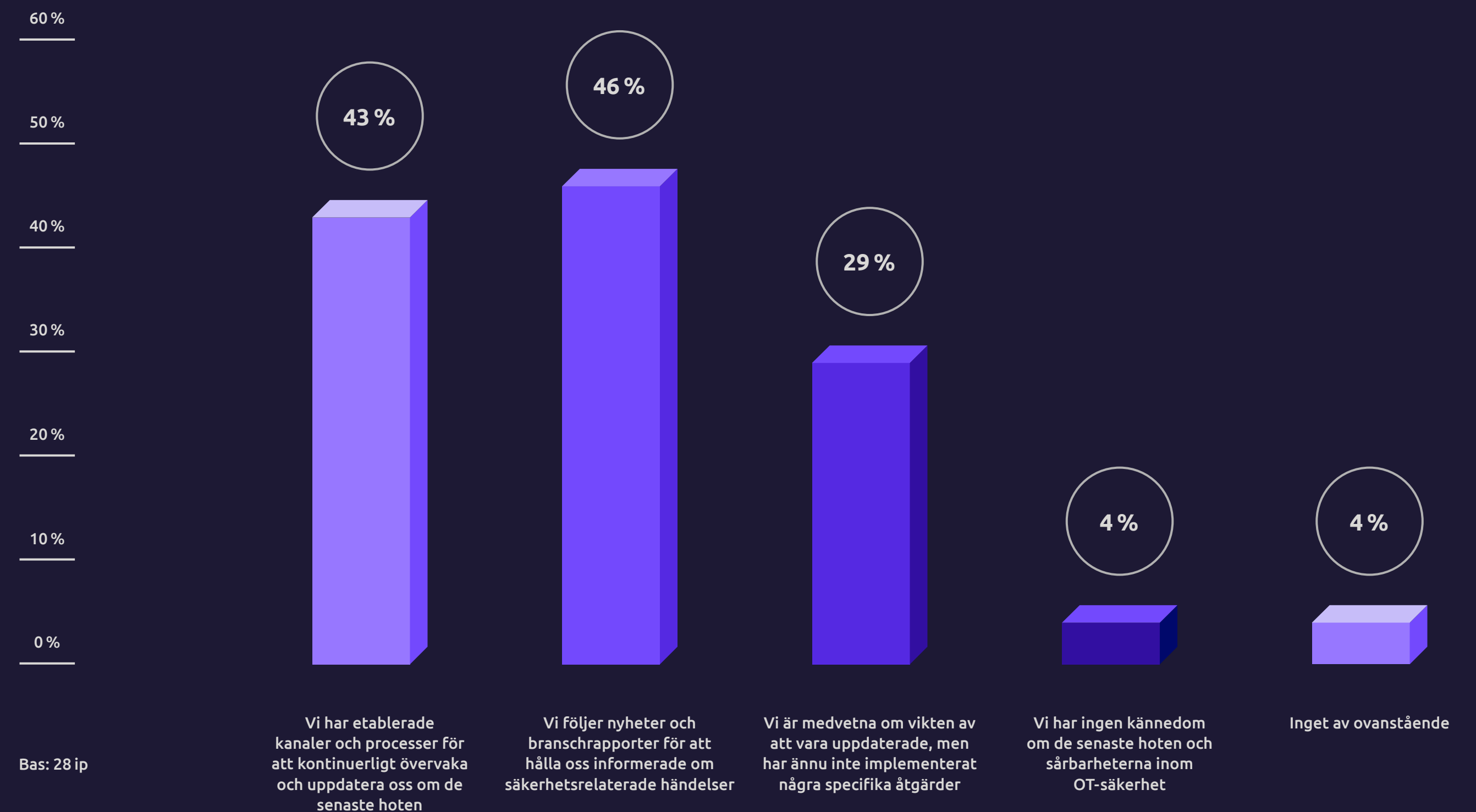
4 av 10 företag har etablerade sätt för att övervaka och uppdatera sig om de senaste hoten inom OT-säkerhet

46 % av företagen uppger att de följer nyheter och branschrapporter för att hålla sig informerade om säkerhetsrelaterade händelser.

29 % har inte implementerat några specifika åtgärder ännu för att hålla sig uppdaterade. De är dock medvetna om vikten av att göra det.

4 % har ingen kännedom alls kring senaste hoten inom OT-säkerhet.

Hur de håller sig uppdaterade om hot och sårbarhet inom OT



08.8

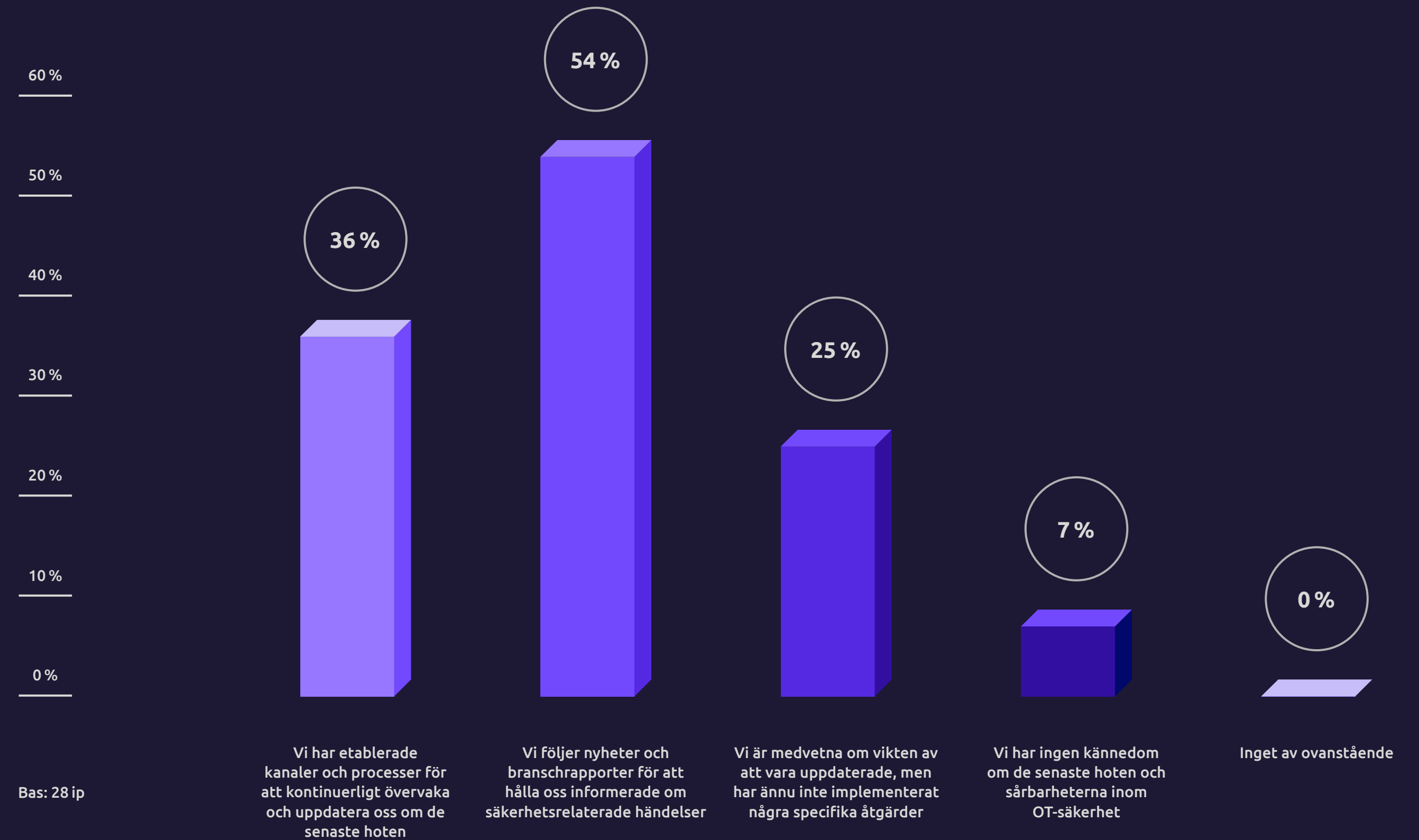
Drygt en tredjedel av företagen har etablerade kanaler och processer för att övervaka och uppdatera sig om senaste hoten inom IT-säkerhet

54 % av företagen uppger att de följer nyheter och branschrapporter för att hålla sig informerade om säkerhetsrelaterade händelser.

25 % har inte implementerat några specifika åtgärder ännu. De är dock medvetna om vikten av att göra det.

7 % har ingen kännedom alls kring senaste hoten inom IT-säkerhet.

Hur de håller sig uppdaterade om hot och sårbarhet inom IT



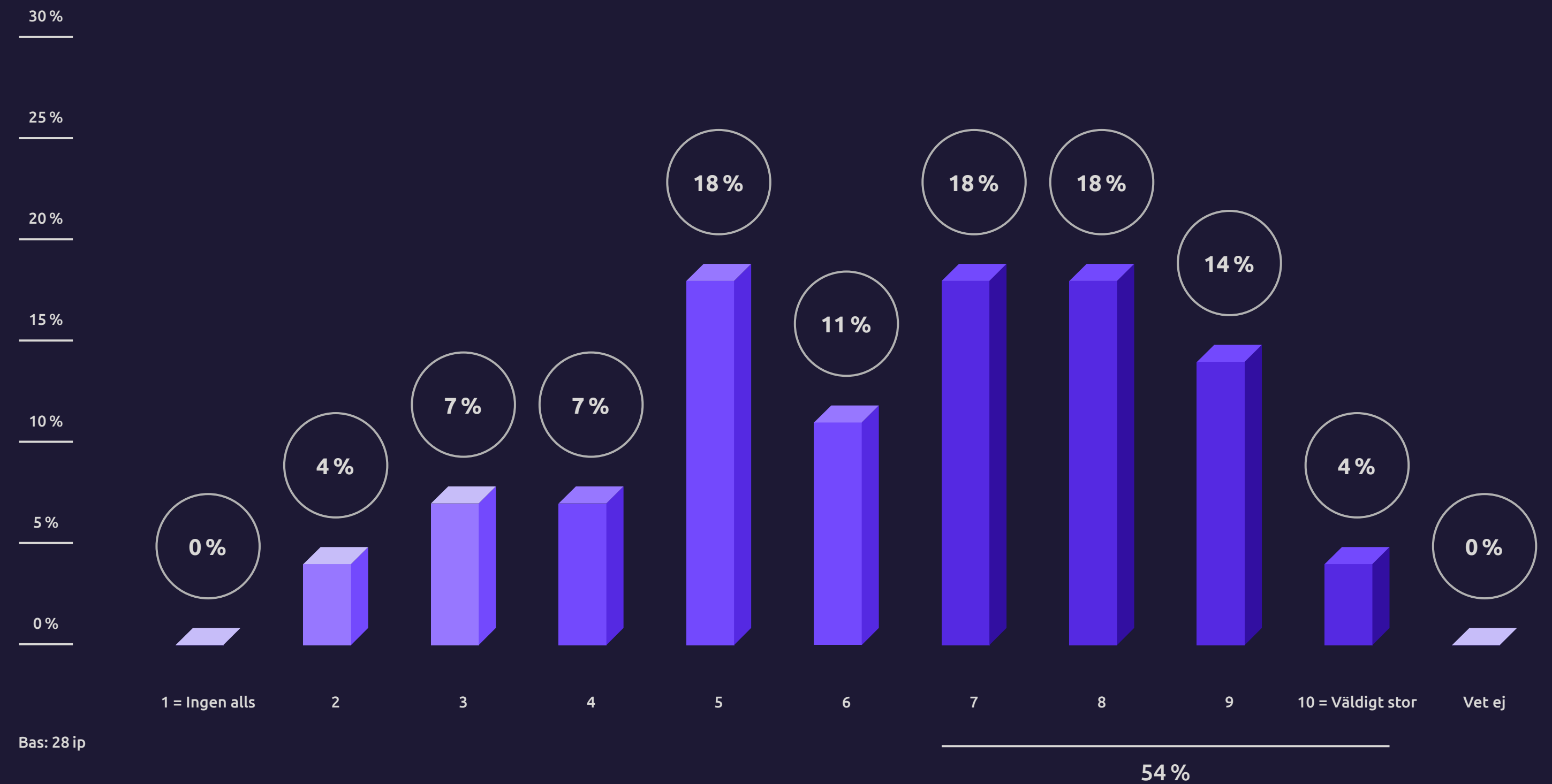
08.9

Lite mer än hälften av företagen är *ganska* eller *helt förberedda* på att hantera en storskalig cyberattack idag

Det är endast 4 % som anger en 10:a på skalan, vilket betyder att de är helt förberedda på att hantera en storskalig attack.

11 % svarar att de inte är särskilt väl förberedda för hantera en storskalig cyberattack.

Hur förberedda de är på att hantera en storskalig attack



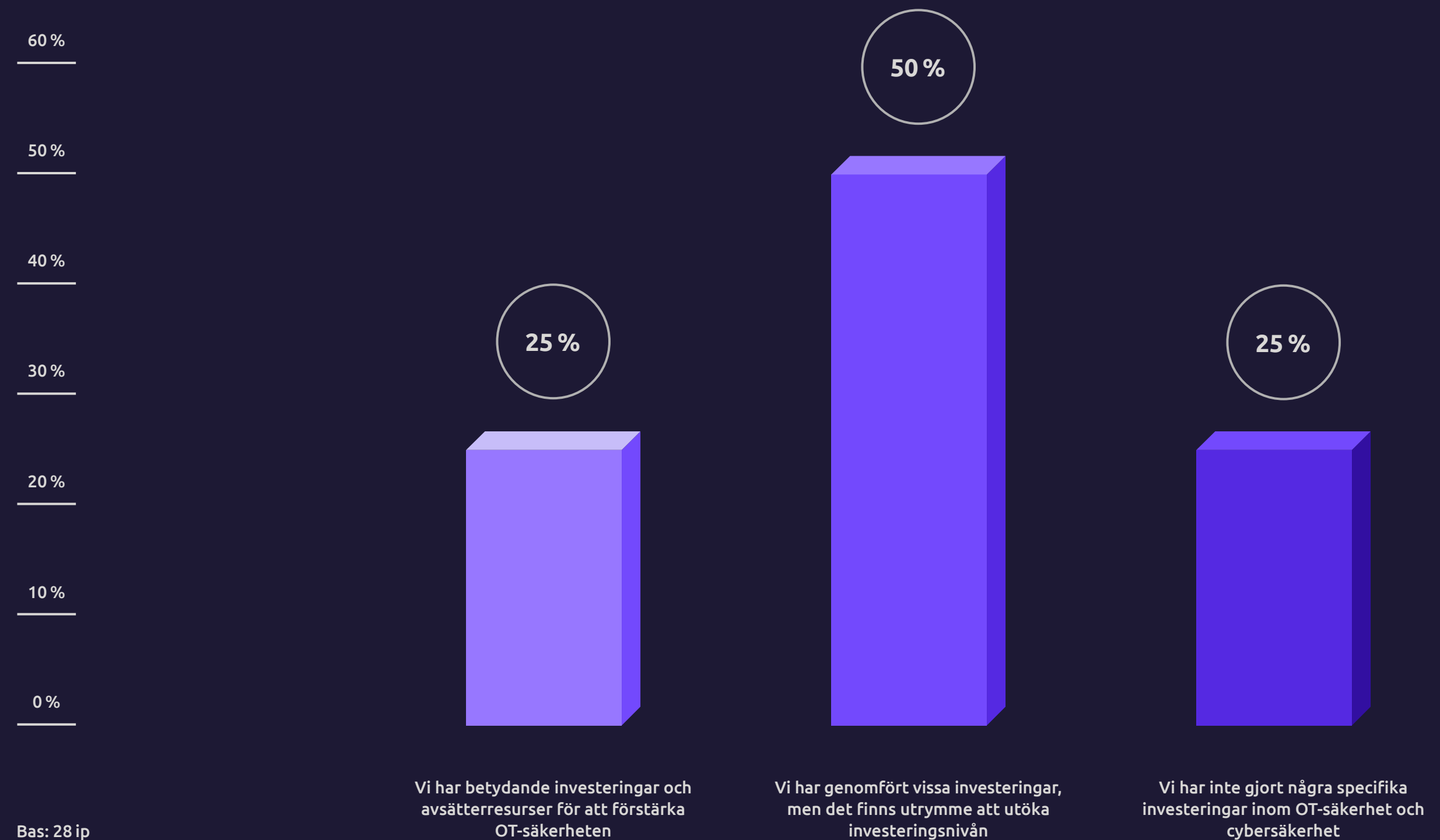
08.10

Hälften av företagen har genomfört *vissa investeringar*, men det finns utrymme att utöka investeringsnivån

25 % av företagen uppger att de har betydande investeringar och avsätter resurser för att stärka OT-säkerheten.

25 % har inte gjort några specifika investeringar kring detta ännu.

Investeringsnivå för säkerhetsåtgärder



Bas: 28 ip

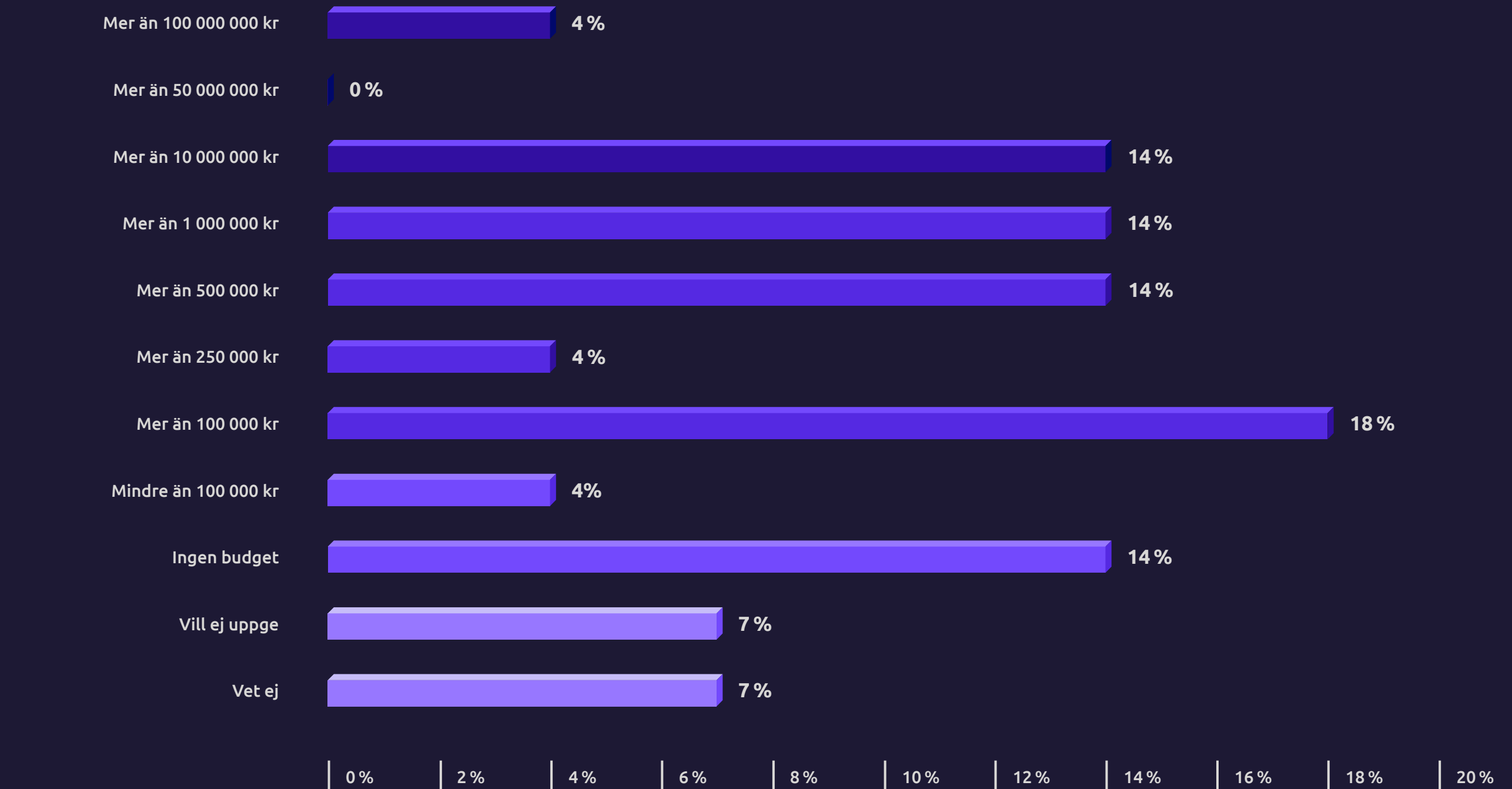
08.11

En tredjedel av företagen har en årlig budget på mer än 1 miljon kronor för OT-säkerhet och cybersäkerhet

De största budgetarna för OT-säkerhet återfinns inom tillverkningsindustrin, tätt följt av sjukvården.

14 % uppger att de inte har någon budget.

Årlig budgetnivå för OT-säkerhet



Bas: 28 ip

08.12

36 % har att skydda kontinuerlig drift som sin främsta prioritet i deras OT-miljö

18 % av företagen uppger att deras främsta prioriteringen är att skydda den fysiska säkerheten av fabriken.

32 % har att skydda anställdas fysiska säkerhet som främsta prioritet.

Främsta prioritet för cybersäkerhet i OT-miljön



Bas: 28 ip

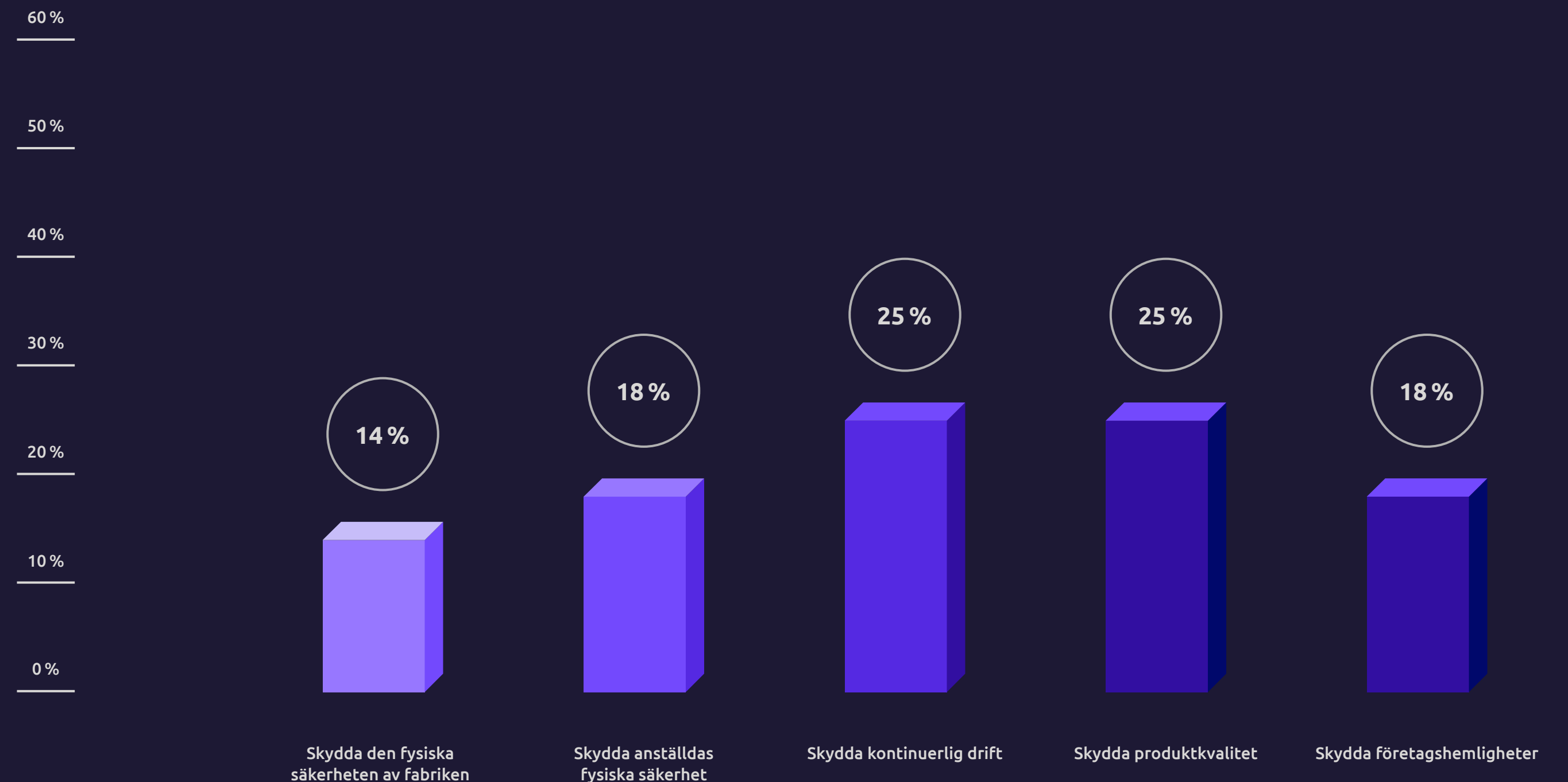
08.13

25 % har att skydda kontinuerlig drift och skydda produktkvalitet som prioritet 2 i deras OT-miljö

14 % av företagen uppger att deras näst främsta prioritering är att skydda den fysiska säkerheten av fabriken.

18 % har att skydda anställdas fysiska säkerhet som näst främsta prioritet.

Andra prioritet för cybersäkerhet i OT-miljön



Bas: 28 ip

08.14

32 % har att skydda produktkvalitet som prioritet 3 i deras OT-miljö

21 % av företagen uppger att deras tredje främsta prioritering är att skydda företagshemligheter.

18 % har att skydda kontinuerlig drift eller den fysiska säkerheten av fabriken som tredje främsta prioritet.

Tredje prioritet för cybersäkerhet i OT-miljön



Bas: 28 ip

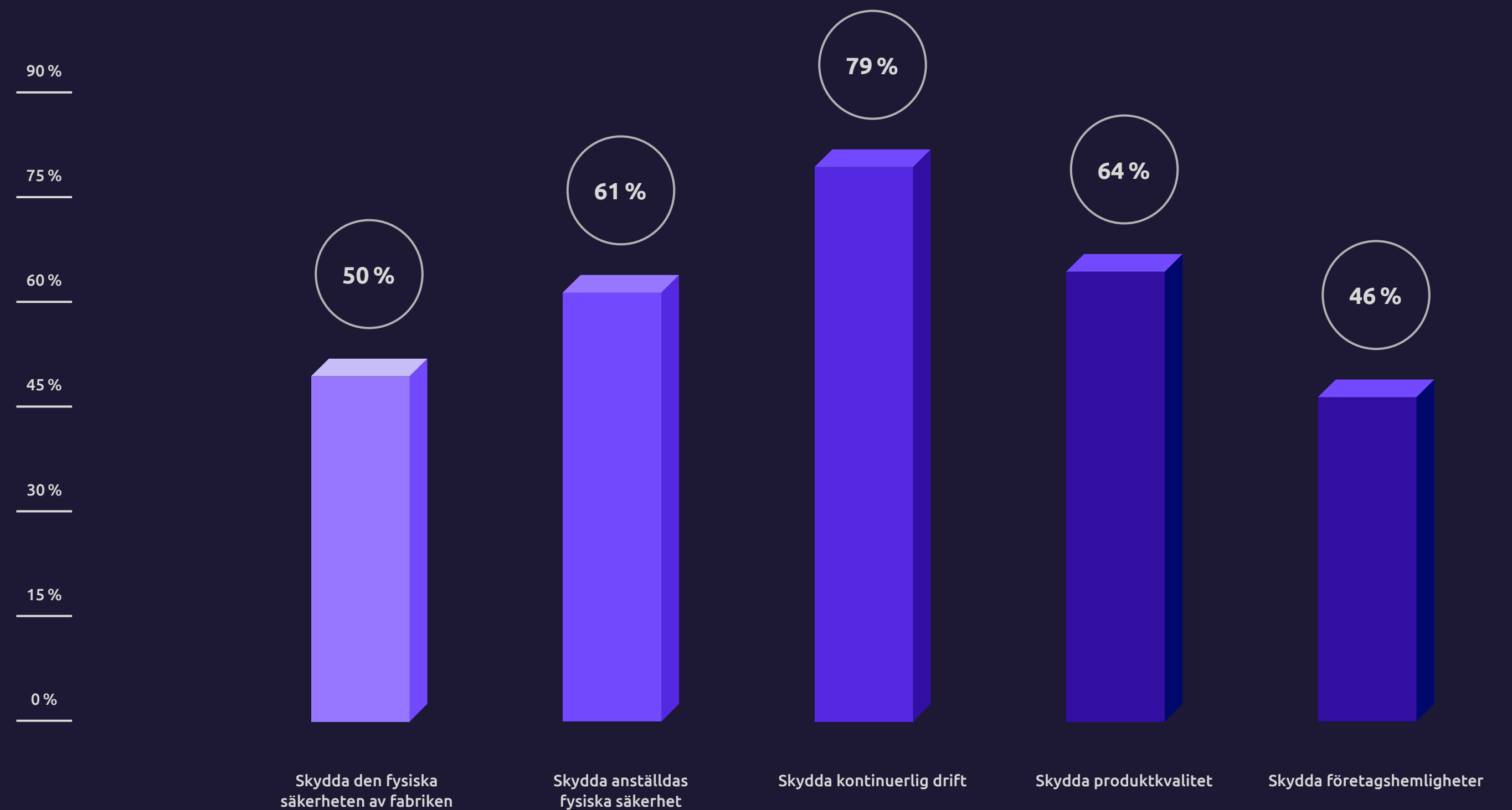
08.15

79 % av företagen har att skydda kontinuerlig drift som prioritet 1–3 i deras OT-miljö

64 % av företagen uppger att deras främsta prioriteringar (1–3) är att skydda sin produktkvalitet.

61 % har att skydda anställdas fysiska säkerhet som främsta prioriteringar (1–3).

Första till tredje prioritet för cybersäkerhet i OT-miljön



Bas: 28 ip

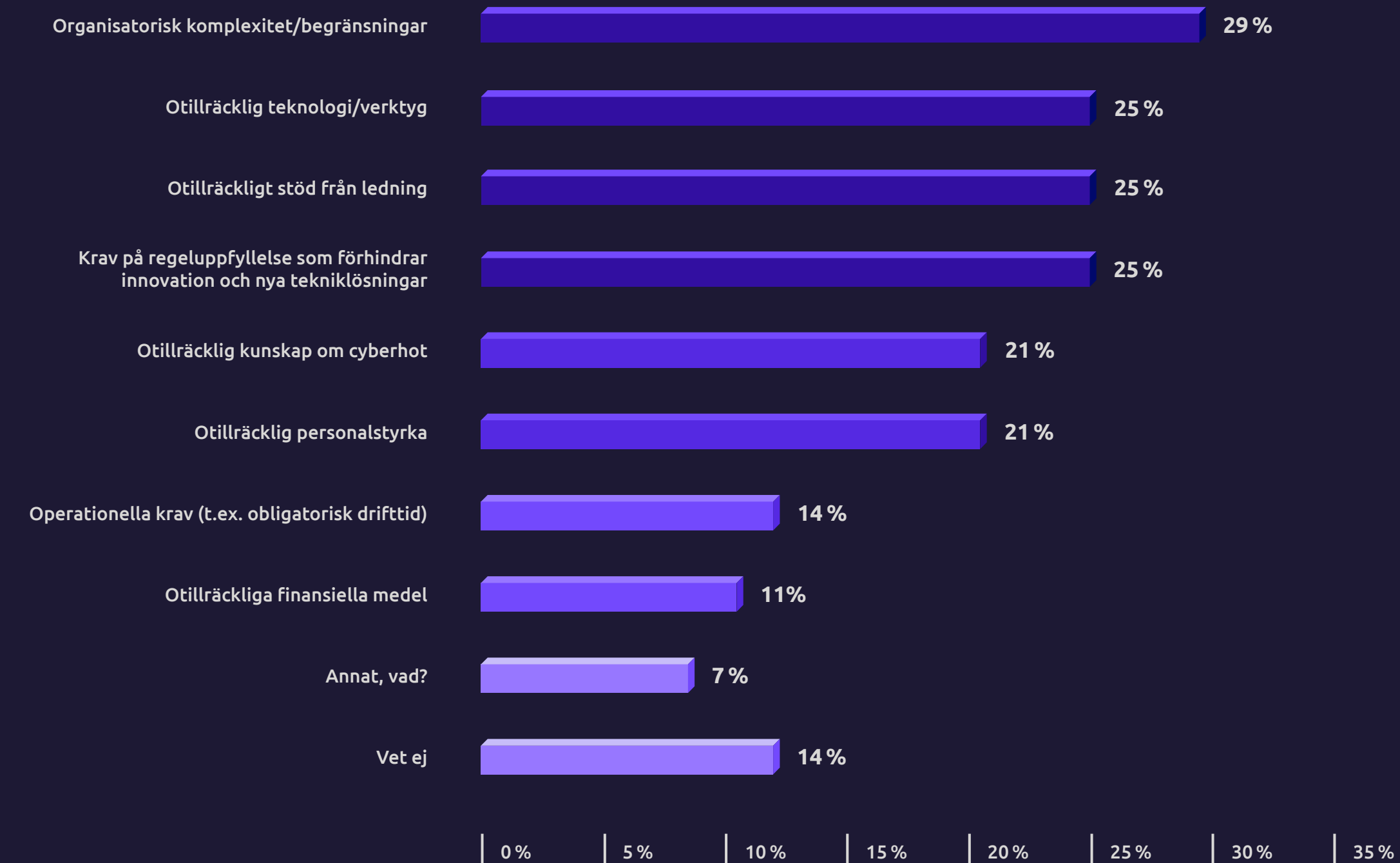
08.16

Organisatorisk komplexitet och begränsningar är största hindret för att minska attackytan i företags OT-miljö

29 % nämner detta som största hinder. Nästan lika många (25 %) nämner otillräcklig teknologi/verktyg, brist på ledningsstöd och krav på regeluppfyllelse som förhindrar innovation och nya tekniker för att minska attackytan.

Under "Annat" nämns att det är svårt i stora företag med många komplexa affärsområden samt att gamla system är dyra att byta ut.

Främsta hindren för att minska attackytan för cybersäkerhet



Bas: 28 ip

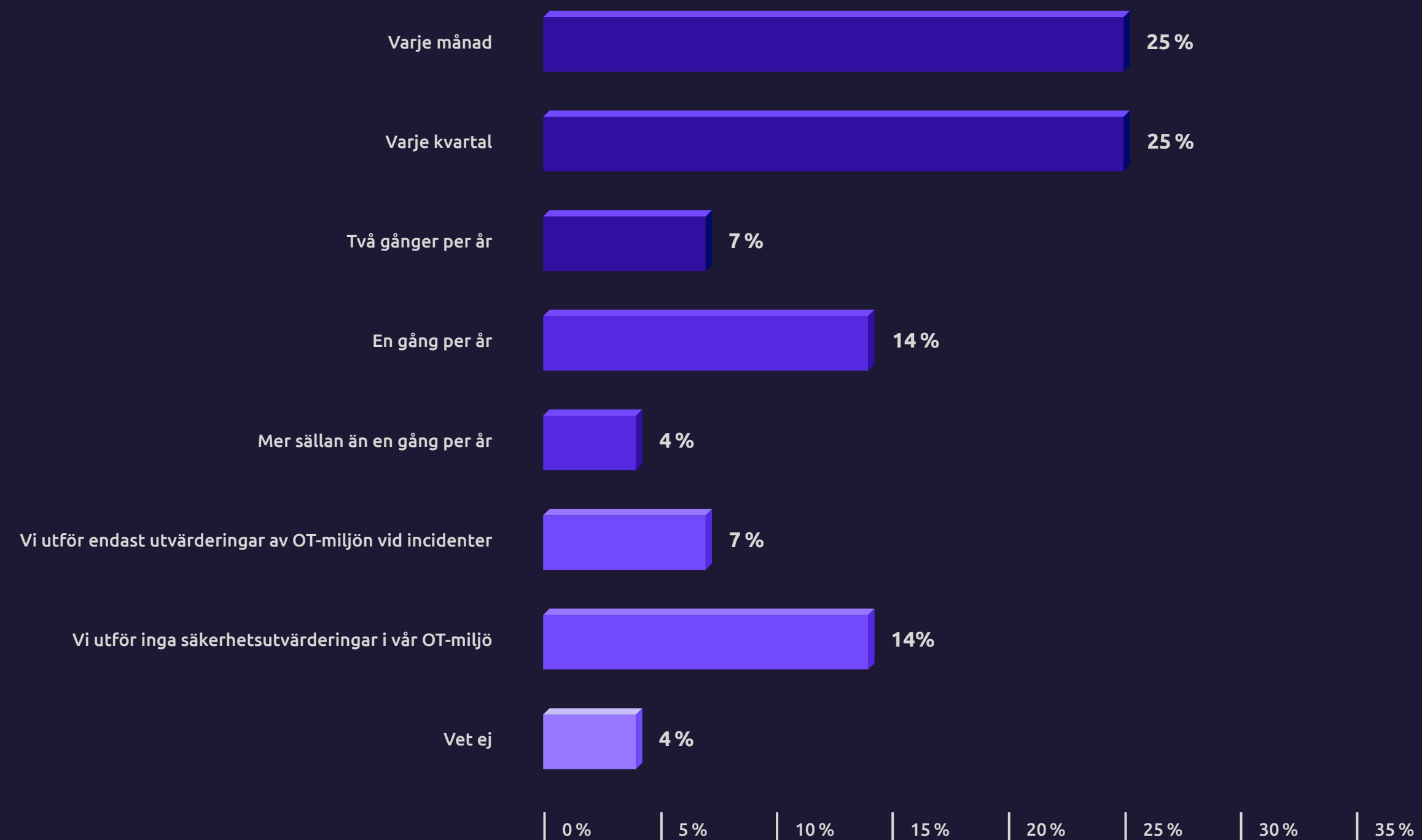
08.17

Hälften av företagen utför utvärderingar *minst en gång per kvartal* eller oftare

Av dem är det 25 % som utför utvärderingar varje månad.

Det är 7 % av företagen som utför endast utvärderingar av OT-miljön vid incidenter. 14 % svarar att de inte utför några säkerhetsutvärderingar alls i sin OT-miljö.

Hur ofta organisatoriska utvärderingar utförs



Bas: 28 ip

Appendix



Appendix 1

02.5

Faktorer som kommer påverka hur framtiden ser ut

- Befolkningssammansättning, åldersstruktur.
- Begränsade naturresurser.
- Bomb.
- Cyberattacker mot el- och vattenförsörjning.
- Demografin, för mycket folk.
- Droger.
- Folks inställning.
- Fotogenvärmare.
- Global ojämlikhet.
- Global politik och krig.
- Grundvattnet.
- Hatet mellan människor. Respektlöshet. Krig.
- Hälsa.
- Höga el- och drivmedelspriser.
- Konflikter.
- Konflikter.
- Korkade politiska beslut.
- Krig.
- Krig föder krig.
- Kriget i Ukraina.
- Kriminella gäng.
- Läget i världen.
- Matproduktion.
- Människors vilja/ovilja till förändring. Bl. a. hur villig många är att sänka sin standard, inkomst, dela med sig till mindre bemedlade i samhället, dra ner på semesterar, inköp, ombyggnad p.g.a. av att personer tröttnat på inredning mer än att det faktiskt fysiskt är dags att byta p.g.a. av materialets livslängd.
- Nedskräpning.
- Omvärldens påverkan.
- Omvärldsläget.
- Pengar.
- Psykopatiska narcissistiska ledare.
- Rasism och fattigdom.
- Religion.
- Ryssland.
- Samhället står inför stora utmaningar som är kopplade till nyliberalismen och vår oförmåga att bibehålla ett solidariskt hållbart samhälle. Det går att ändra på och detta är nödvändigt för människornas överlevnad. Jorden klarar sig alltid men inte mänskliga samhällen.
- Överbefolkningen.

Appendix 2

05.2

Utmaningar industrin står inför i samband med OT

- AI.
- Att AI-tekniken hjälper till med hacking.
- Att få användarna att tänka på säkerhet.
- Att få sömlös integration mellan alla våra bolag.
- Att garantera säkerheten.
- Bara positivt.
- Bättre skydd mot attacker, användarna är den svagaste länken.
- Framtiden.
- Hantera övergång från stordatorer till PC.
- Hantering av säkert data och cyber.
- Inga större.
- Integritet.
- Kompetens.
- Möjlighet till fler former av attacker.
- Na.
- Operative words and difficulties.
- Osäker.
- Osäkert i dagsläget, har dock ingen produktion.
- Ransomware.
- Små volymer i liten bransch är dyrt. Svårt att skapa lönsam utveckling.
- Stora utmaningar.
- Säkerhet IT.
- Säkerheten.
- Säkerhetsaspekten inom de snabbt förändrade teknikerna samt lagarna. GDPR och ChatGPT.
- Tänka mer hållbar och miljövänlig.
- Vet inte.
- Visibility och kunskap.

Appendix 3

06.4

Hur utbildas personalen i säkerhetsfrågor

- Artificial intelligence and terror risk.
- De får en utbildning en gång per år.
- Dels internutbildning och dels externa utbildningar.
- Externa utbildningar som vi köper in.
- Fysiskt och digitalt.
- Genom att beskriva instruktioner i säkerhetsfrågor.
- Genom tredje part.
- Hantering av ämnet.
- Interna informationskanaler, digitala utbildningar.
- Internt i företaget.
- Intranät.
- IT.
- Kontinuerligt.
- Med intranät utbildning som skickas i din mailadress.
- Med kurser.
- Obligatoriska onlineutbildningar. Tester med phishing mails etc.
- Olika utbildningar med konsulter som är experter.
- Onlinekurser från cybergate.
- Specialister Utbildning inom sitt område genom branschutveckling eller leverantörsutbildning.
- Säkerhetsprotokoll.
- Vi använder Nimblr, det har fått igång diskussionen om säkerhet.
- Via 'read and understood' dokument.
- Webbaserad digital utbildning cirka 5 minuter varje månad.

Appendix 4

08.3

Typ av incidenter och vilka konsekvenser de fått

- Attacker från flera olika utländska länder.
- Avbrott på nätet.
- Brute force attacker för att komma åt lösenord, överbelastningsattacker.
- Cyberattacker med marginella konsekvenser.
- Företaget läckte GDPR.
- Skyddade uppgifter till en nära anhörig. Vi fick sanktioner.
- Försök till cyberattacker. Men stordatorer är mindre drabbade.
- Hackers and trespassing.
- Hoten har upptäckts i tid och kunnat förhindras.
- Informationsläckage.
- Intrång.
- Intrång.
- Känner inte till några incidenter.
- Mailattack.
- Någon planterade ett USB-minne i nätverket.
- Rån stölder inbrott.
- Stopp i produkter.
- Säkerhet.
- Överbelastning.

Appendix 5

08.5

Hur industrin kan dra nytta av trender

- Allt blir säkrare.
- Automatisering.
- Bli mer effektiv.
- Bättre och säkrare mjukvara.
- Bättre skydd.
- Bättre säkerhetssystem.
- Framförallt att diverse verktyg blir mer "allmänna" och därmed tillgängliga för mindre företag.
- Framförallt för effektivisering.
- Följa trender.
- Inget särskilt.
- Kan jobba ostört och säkert.
- Kontinuerlig omvärldsspaning och utbildning är ett måste.
- Mer beställning.
- Mycket.
- Nej.
- Ok.
- På många vis.
- Synergier med IT.
- Use.
- AI to our benefit.
- Vet ej.
- Vet ej.
- Vet ej.
- Vet inte.
- Vill ej svara.
- Vinst.
- Väldigt bra.

Kontakt

Carl-Johan Dahlgren

Business Development Director Northern Europe
carl-johan_dahlgren@txone.com

Samanta Hollis Franco

Marketing Director Northern Europe
samanta_hollis@txone.com