



Fastly Global Security Research 2023

Nordics Findings

November 2023

Research conducted by
SAPIO Research



Project overview and methodology

- The survey was conducted among **209** IT Decision Makers (more than 2/3 respondents directly make or influence cybersecurity decisions) in organisations with 500+ across the Nordics. Participants hold a wide range of roles across the infrastructure including cloud operations, IT management, application architect and security operations analyst.
- At an overall level results are accurate to $\pm 6.8\%$ at 95% confidence limits assuming a result of 50%.
- The interviews were conducted online by Sapio Research in **August, September & October 2023** using an email invitation and an online survey.

Respondent demographics summary

Demographics

Total respondents: 209

Country of residence



Department

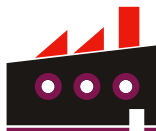


Size of company



# of employees	250 - 499	500 to 999	1,000 to 5,000	5,001 to 10,000	10,001 to 25,000	25,000 to 75,000	75,000+
% of respondents	15%	34%	28%	12%	8%	3%	11%

Industry



Company sectors – top 3:



Decision making (cyber security)



- 71% make or influence cybersecurity decisions
- 18% are fully aware of decisions regarding cybersecurity
- 11% are somewhat aware of cybersecurity decisions

Key stats

32% predict '**GenAI**' and '**data breaches and data loss**' as the biggest cybersecurity threats over the next 12 months

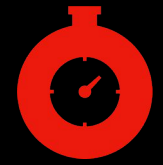
On average, businesses lose **10%** of their annual income as a result of **cyber attacks**

41% of respondents feel there is gap among the current talent pool in terms of the lack of relevant **technical skills**

Making cybersecurity more accessible (**33%**) and improving cybersecurity skills (**28%**) are the main security priorities over the next year

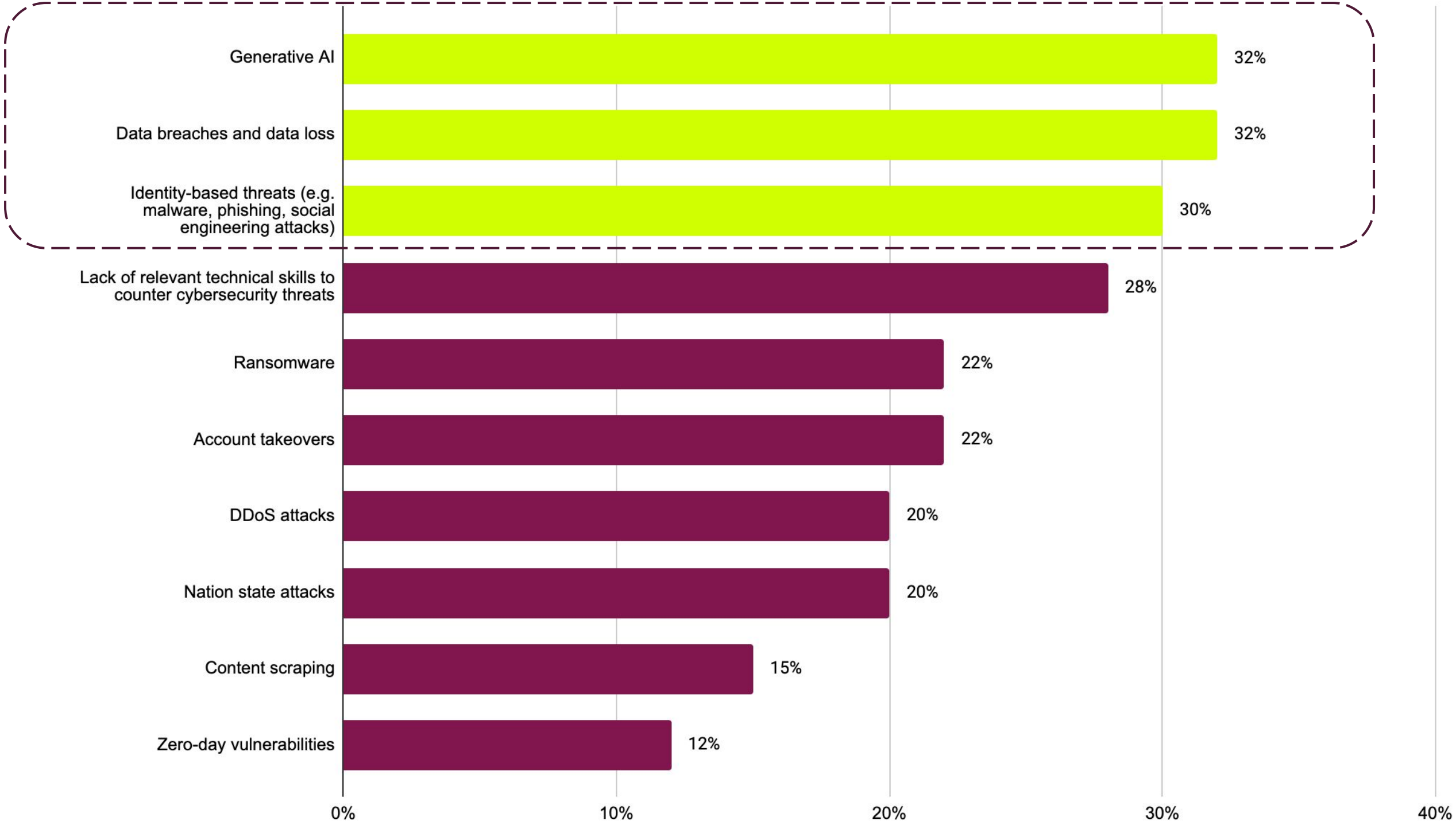
50% say that their organisations cybersecurity strategy has **hampered business innovation**

On average, **46%** of cybersecurity tools are fully deployed/active



Main Findings

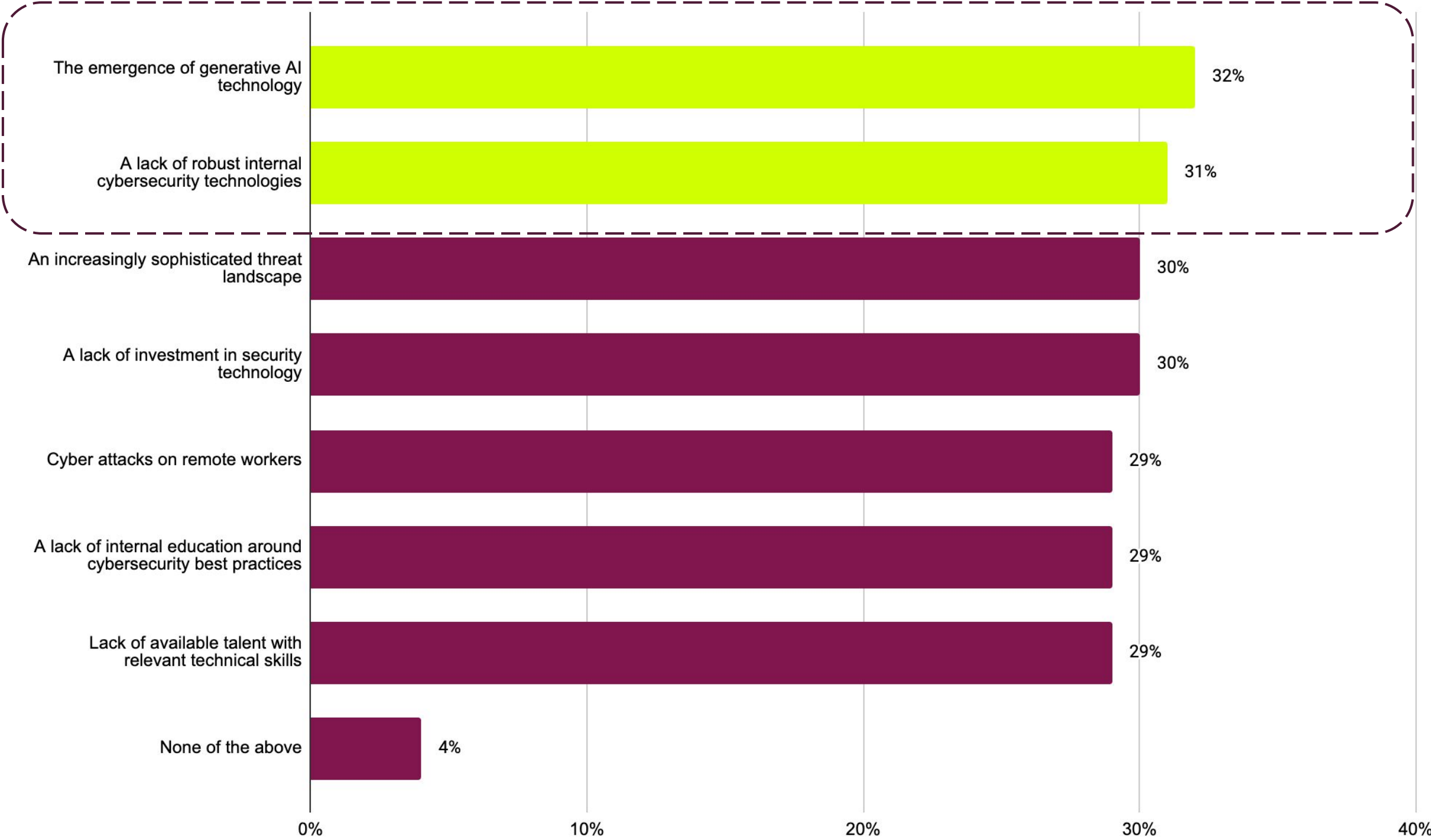
Generative AI and data breaches and data loss (both 32%), and Identity-based threats (30%), are viewed as the biggest cybersecurity threats to organisations over the next 12 months



Q1. What do you predict will be the biggest cybersecurity threat to your organisation over the next 12 months? Select top three

Base: 209

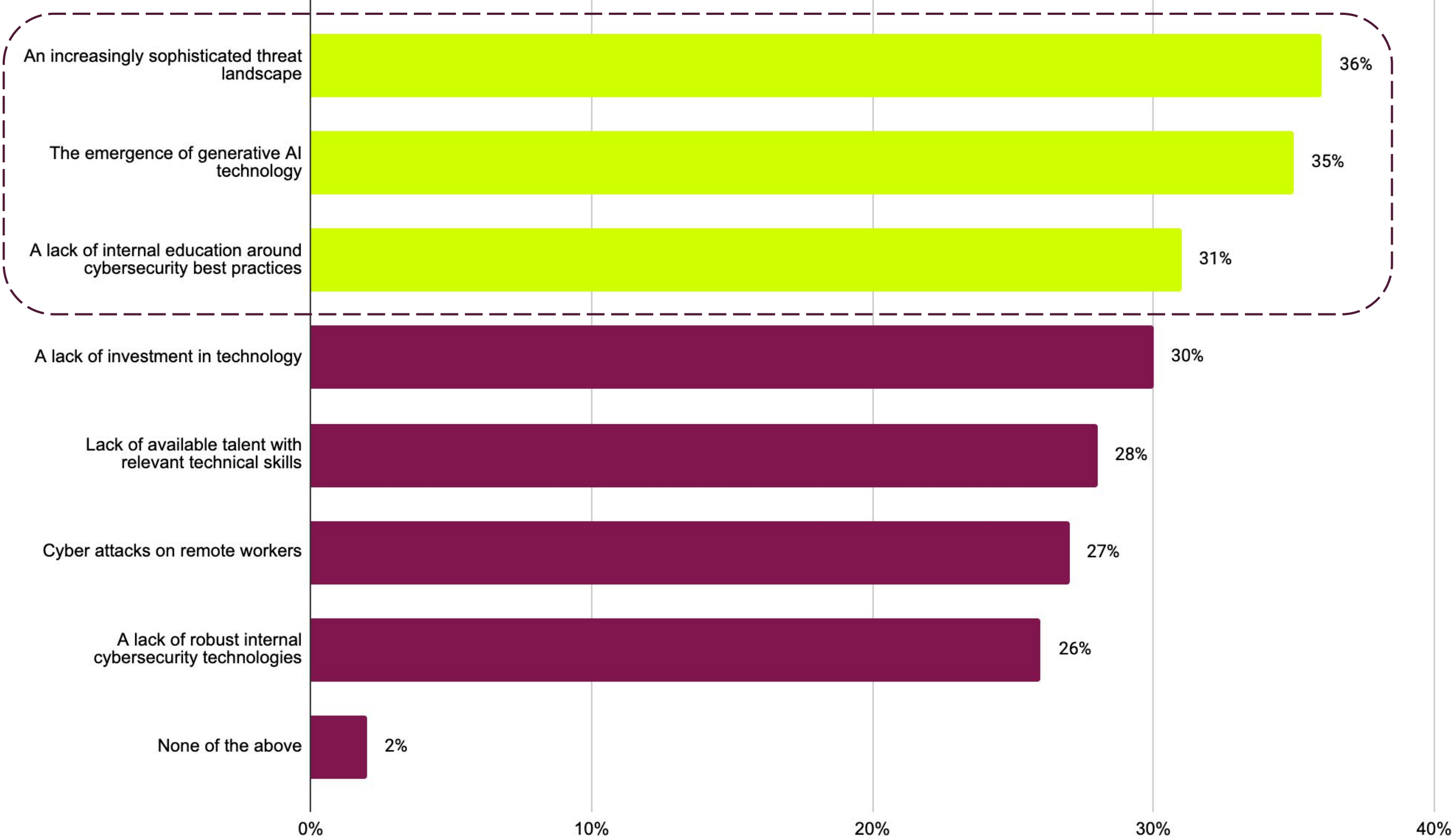
Over the last 12 months, the emergence of generative AI (32%) and a lack robust internal cybersecurity tech (31%) were the main drivers of cybersecurity threats



Q2a. Which of the following, if any, have driven cybersecurity threats to your business over the past 12 months?
Select top three

Base: 209

Over the next 12 months, an increasingly sophisticated threat landscape (36%), the emergence of generative AI (35%), and a lack of internal education around cybersecurity best practices (31%) are still main drivers of cybersecurity threats

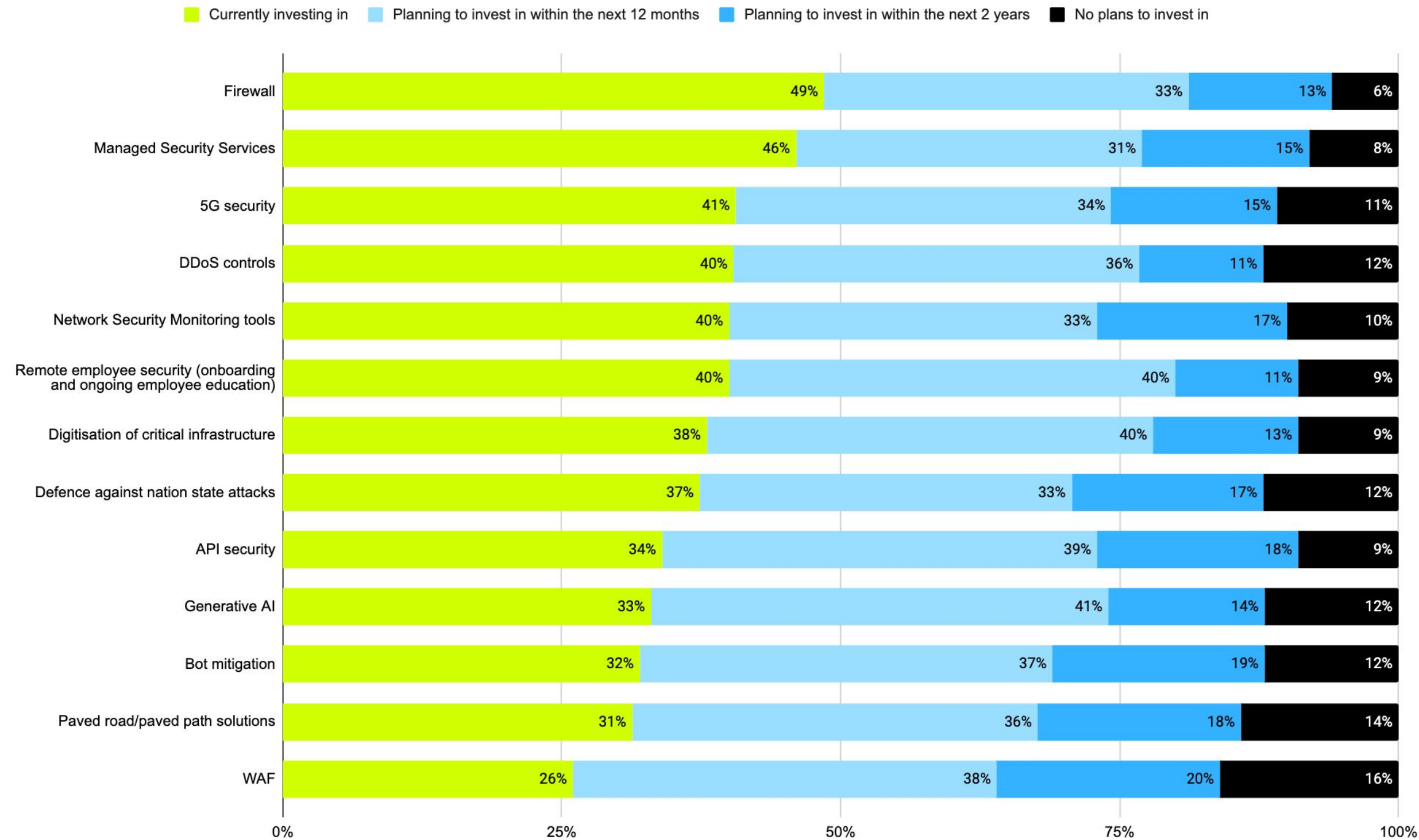


Q2b. Which of the following do you predict will drive cybersecurity threats to your business over the next 12 months?
Select top three

Base: 209

49% are currently investing in 'Firewall' technology, and around half are investing in 'Managed security services' (46%)

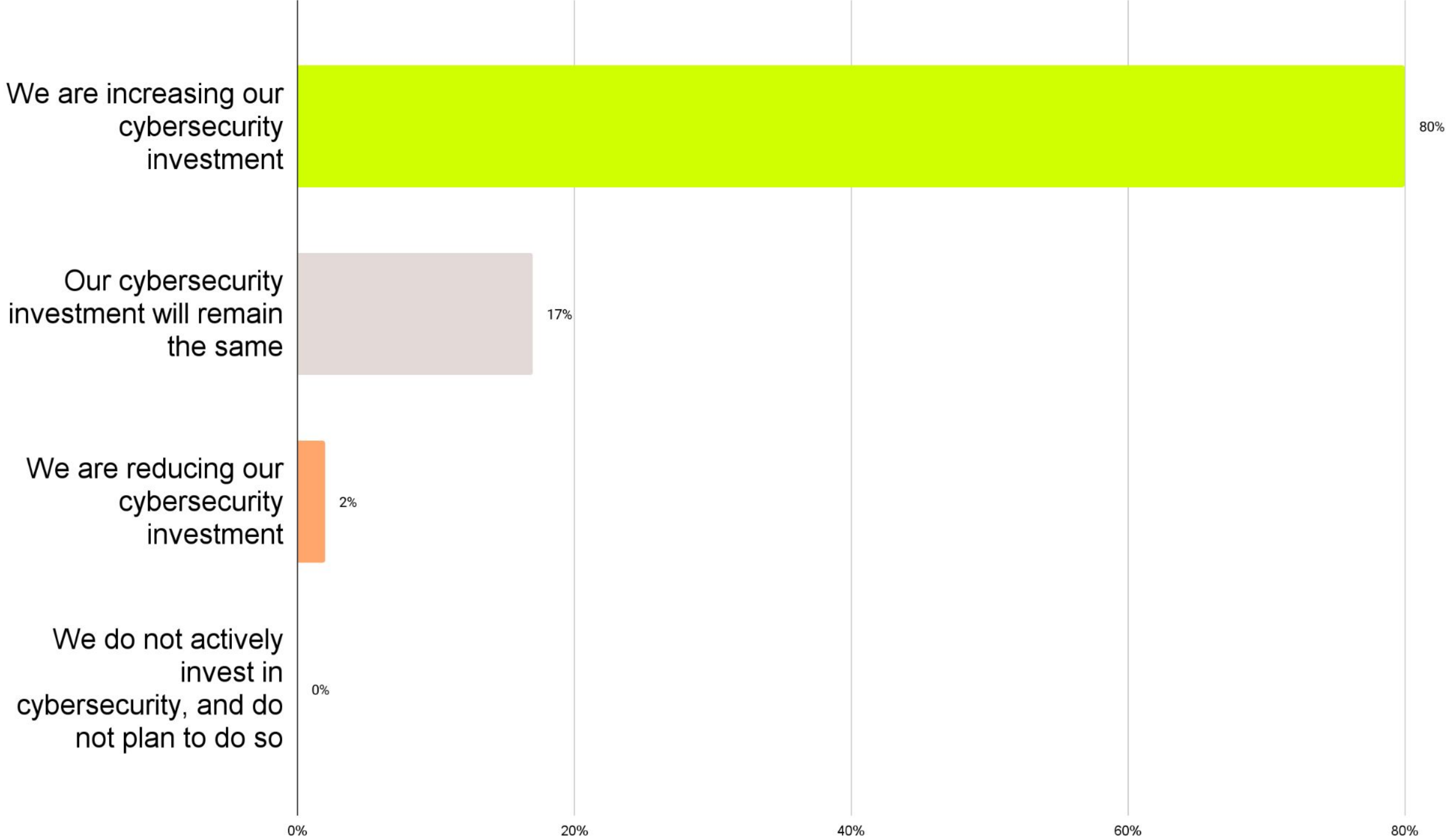
16% have no plans to invest in WAF



Q3. Which technologies and/or services is your organisation currently investing in/planning to invest in/have no plans to invest in?

Base: 209

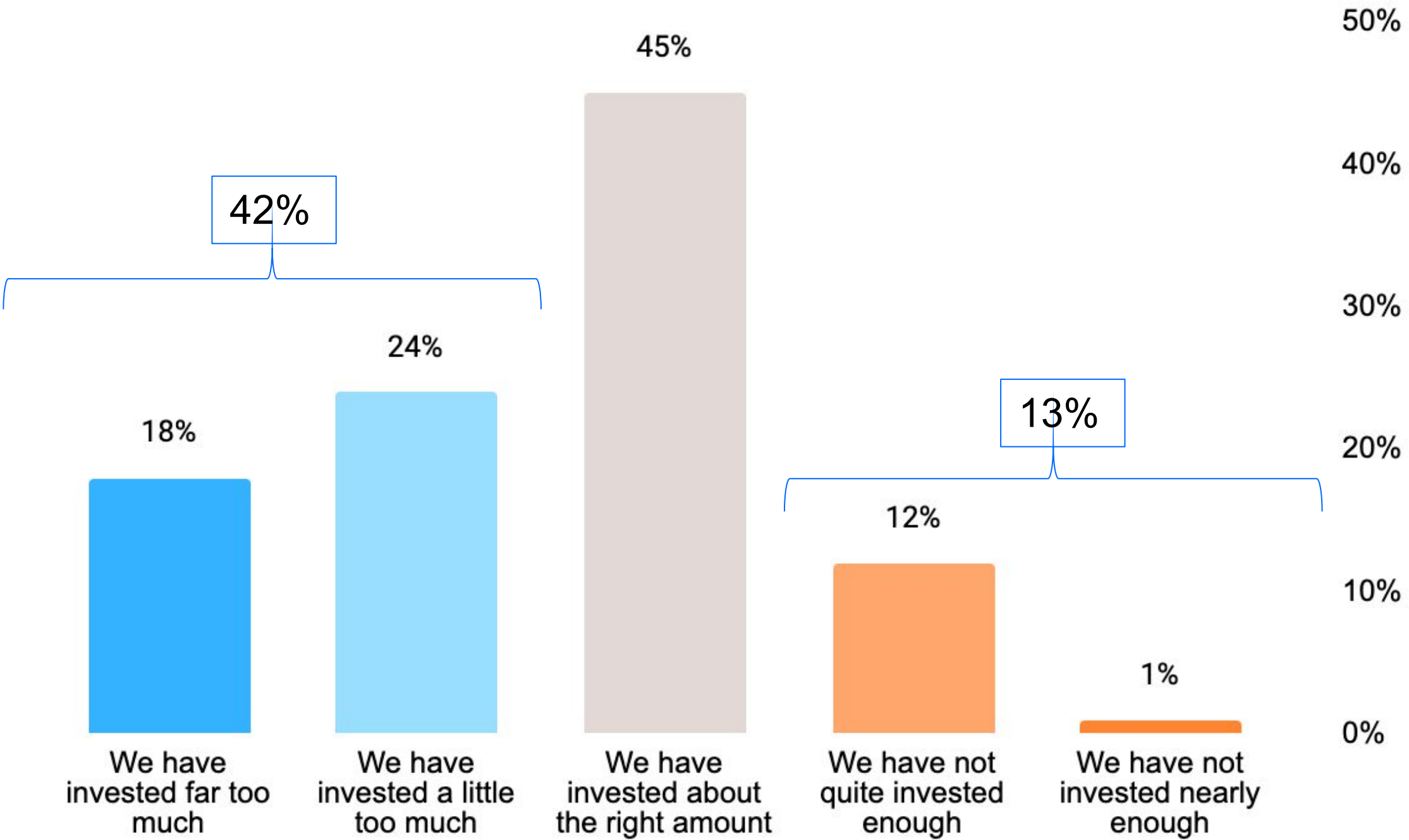
80% of respondents are increasing their cybersecurity investment



Q4a. When it comes to investment, which of the following best describes how your organisation is preparing for future cybersecurity risk over the next 12 months? Select one

Base: 209

42% of respondents have invested too much into cybersecurity over the past 12 months
45% say they have invested about the right amount

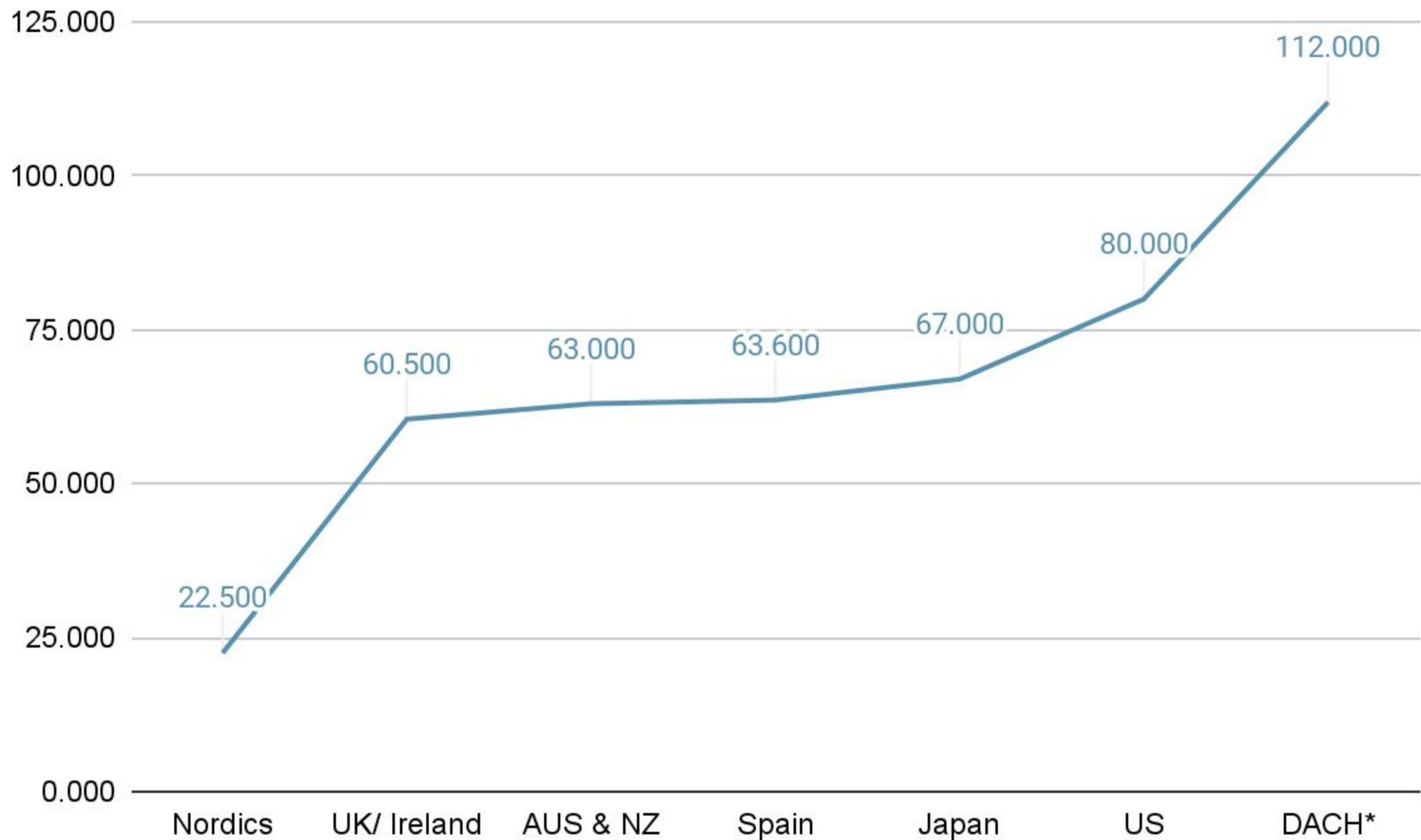


*only asked to those who invest in cybersecurity

Q4b. Thinking about the investment you made to prepare for cybersecurity risk over the past 12 months, which of the following best applies to your organisation? Select one

Base: 208*

On average (median), \$22,500 USD are spent per year on web application and API security control/tools in the Nordics



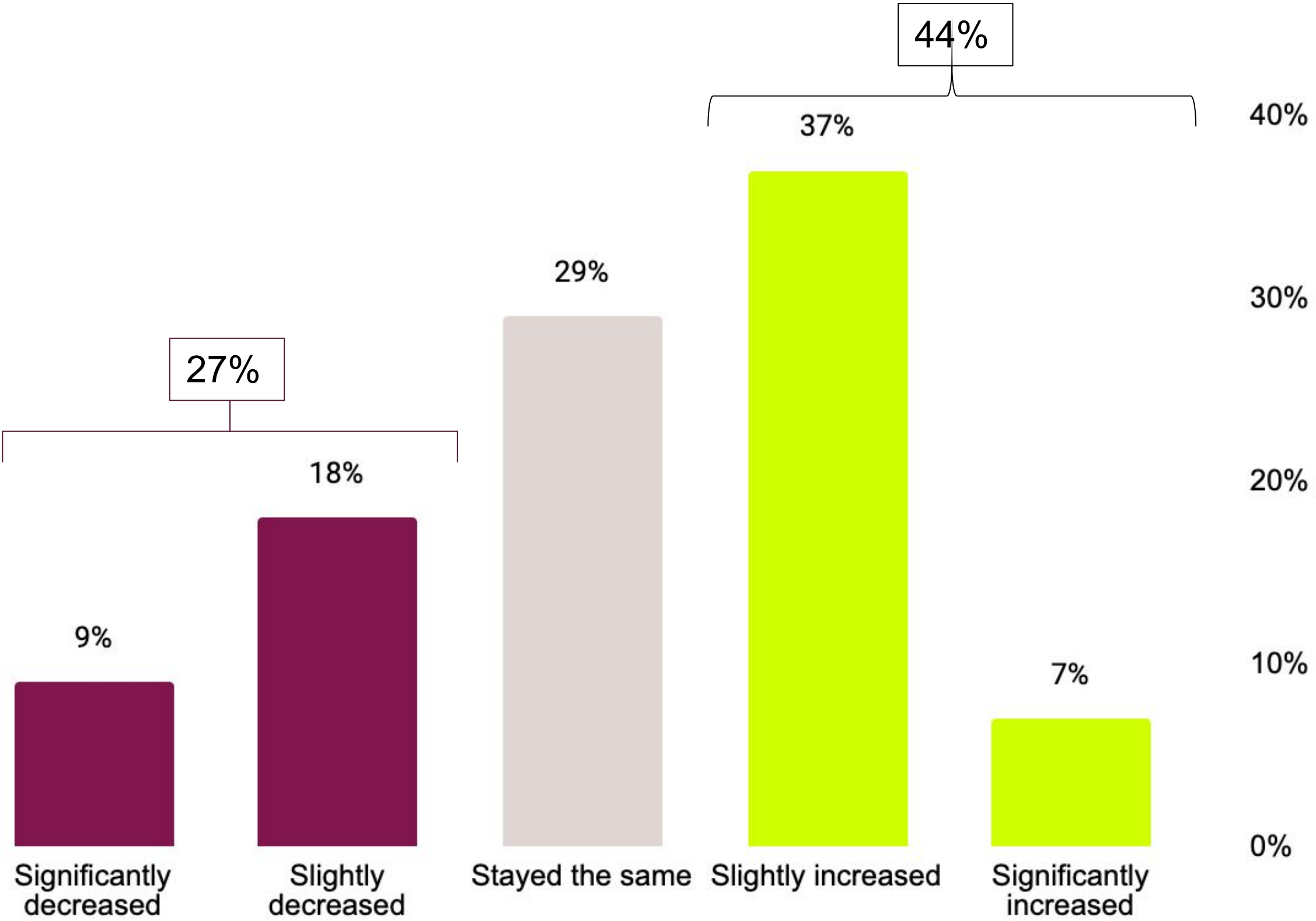
*The sample for DACH countries had a larger proportion of companies with more than 75,000+ employees

2022 Survey:	
Nordics	22,990
Spain	48,150
US	50,000
UK & Ireland	54,030
AUS & NZ	64,900
DACH	65,000
Japan	69,300

Q5a. Approximately how much would you estimate your organisation spends per year on web application and API security controls/tools (i.e., inclusive of licences, subscriptions, appliances, and support costs)?

Base: 1484

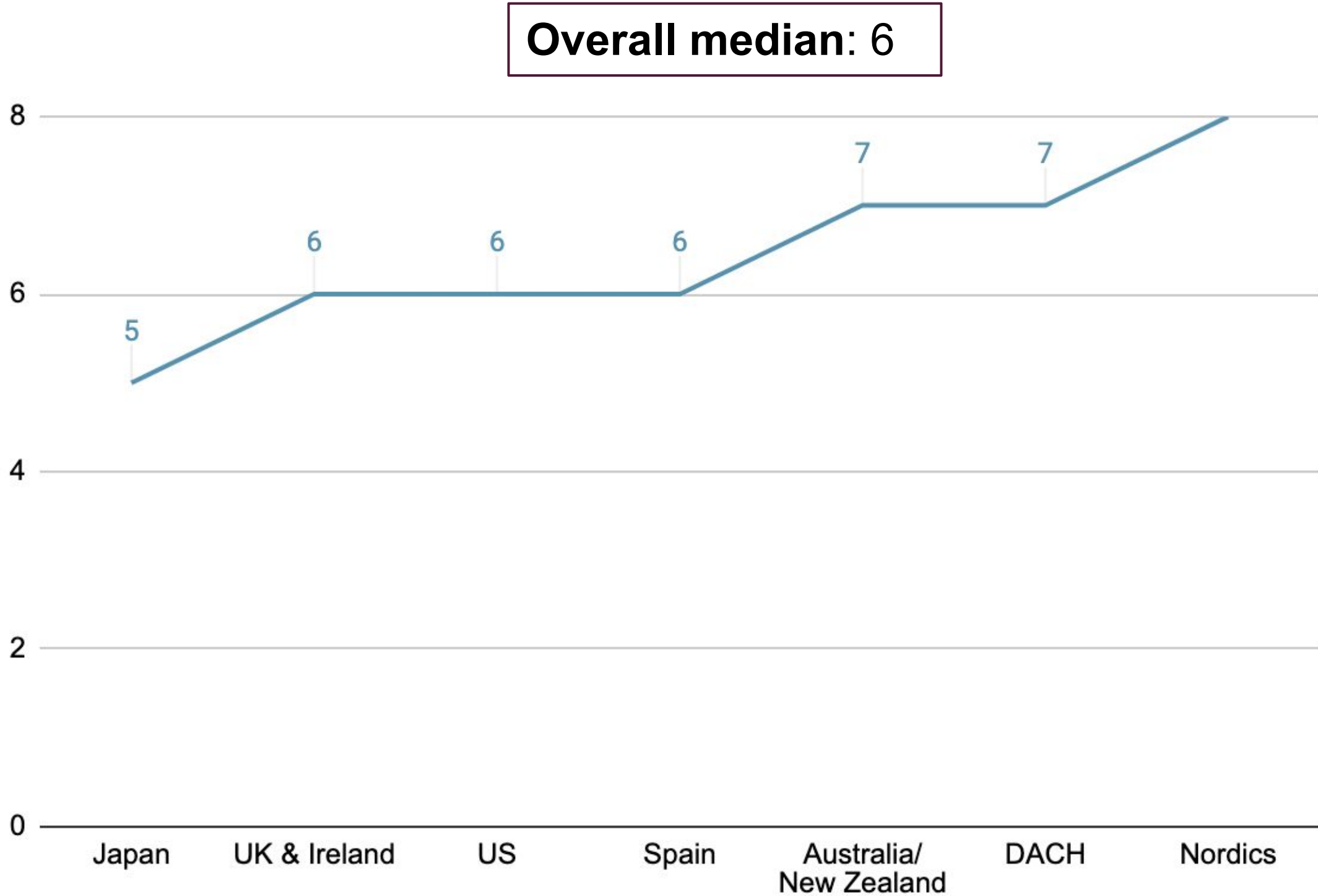
44% of respondents have increased talent spending, with only 27% having decreased talent spending



Q5b. How has your talent spending (e.g. new hires, wages) for cybersecurity changed, if at all? Select one

Base: 209

On average (median), organisations in the Nordics rely on 8 network and application cybersecurity solutions

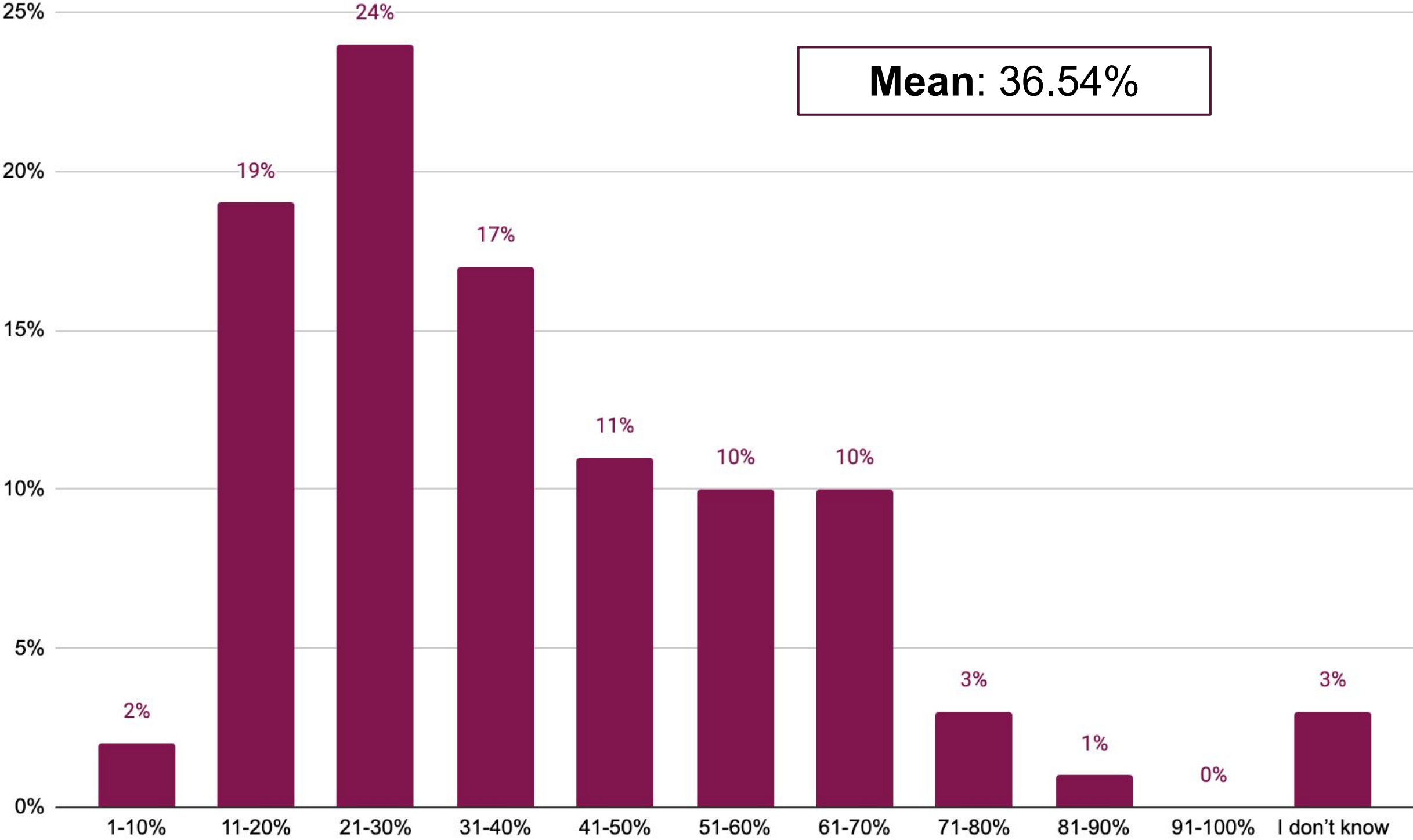


2022 Survey:
Japan **4**
Spain **5**
US **5**
UK & Ireland **6**
AUS & NZ **5**
DACH **5**
Nordics **7**

Q6a. Approximately, how many network and application cybersecurity solutions does your organisation rely on?
Please enter your best estimate below

Base: 1484

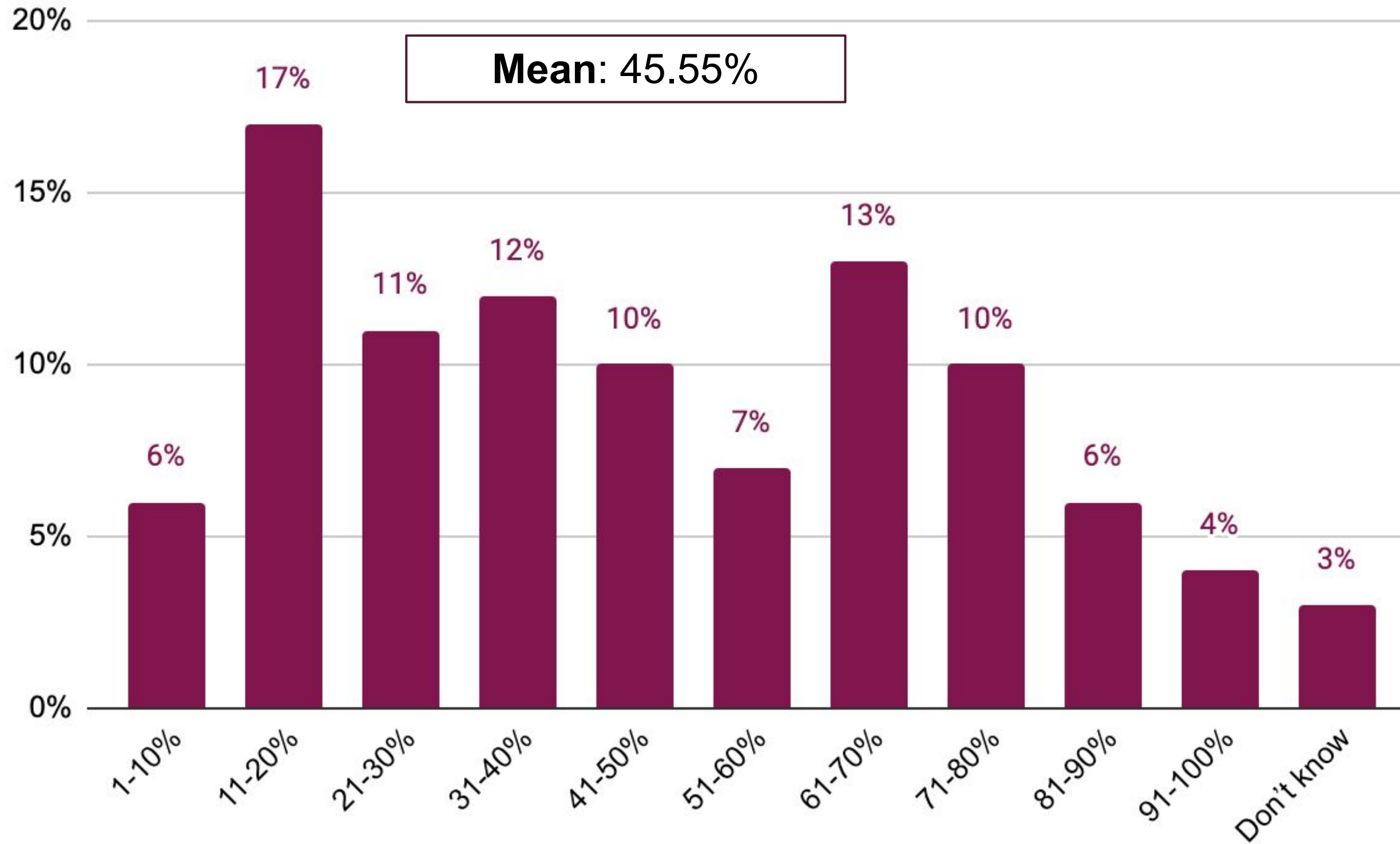
On average, 37% of network and application cybersecurity solutions overlap



Q6b. And roughly, how many of these solutions overlap in covering the same threats? Select one

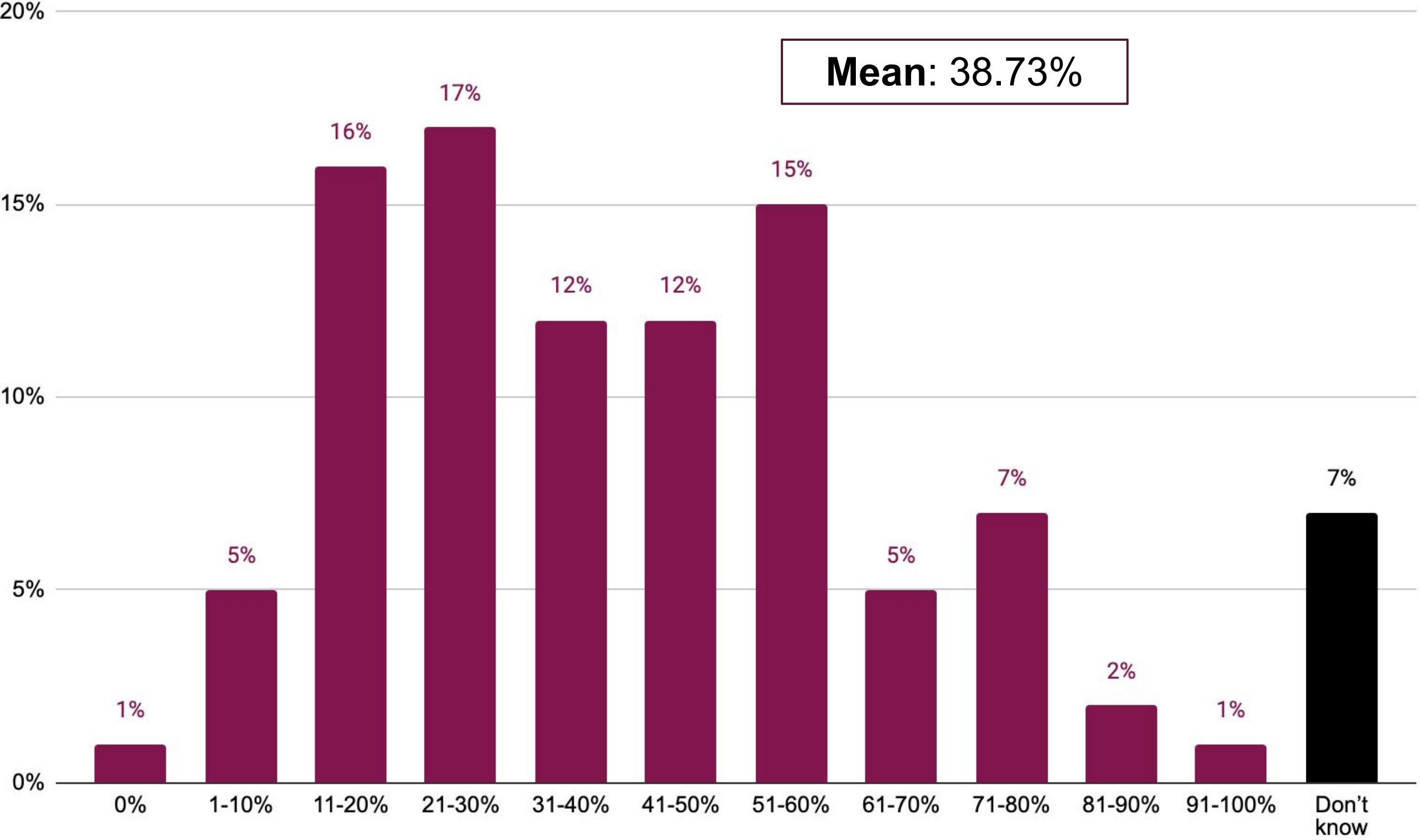
Base: 209

On average, only 46% of cybersecurity tools are fully active/ deployed



Q7. What percentage of your cybersecurity tools are fully active/deployed? Select one

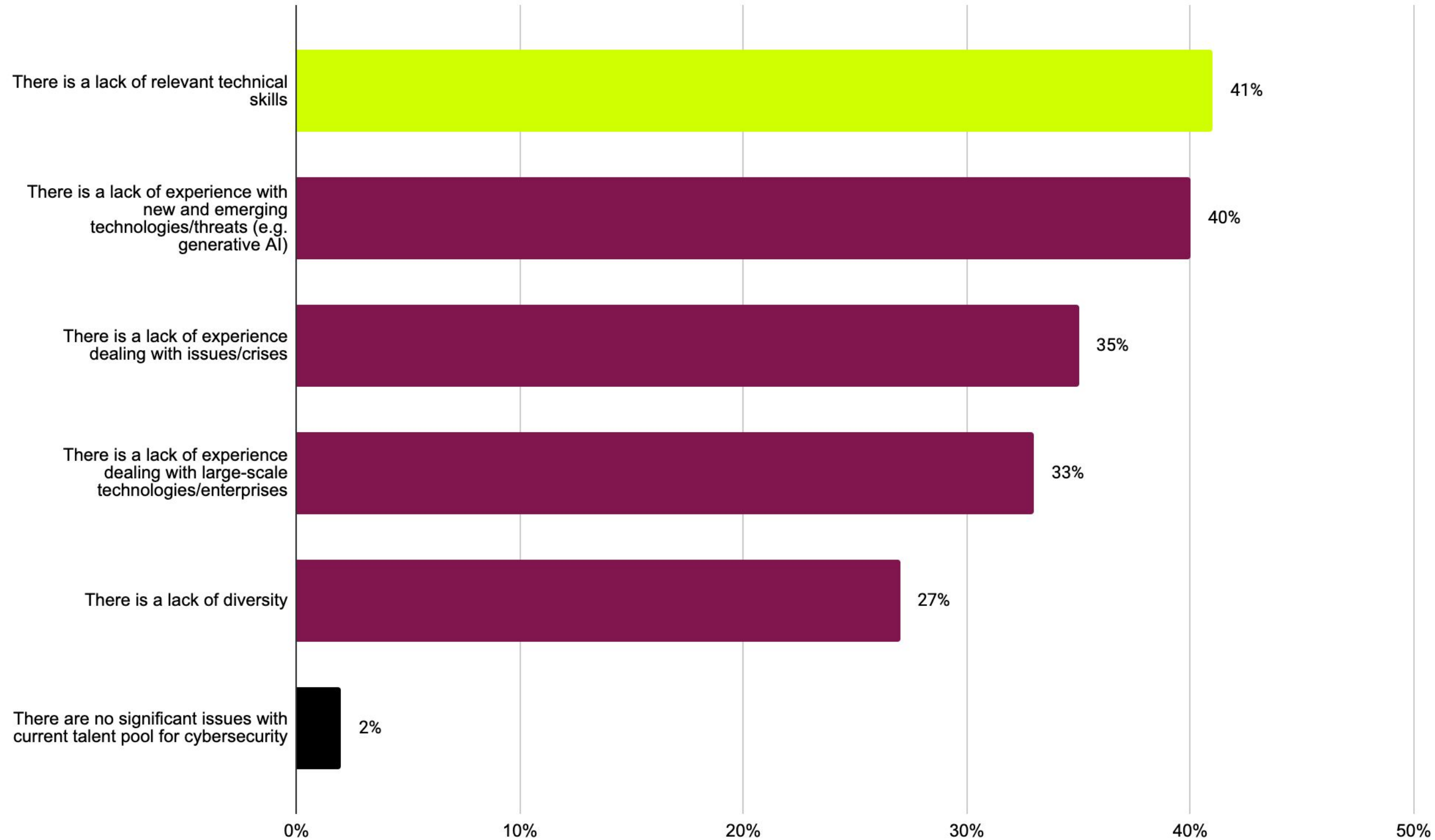
On average, 39% of security alerts detected by an organisations WAF are false alerts



Q8. What proportion of security alerts detected by your organisation's WAF are false alerts? Select one

Base: 209

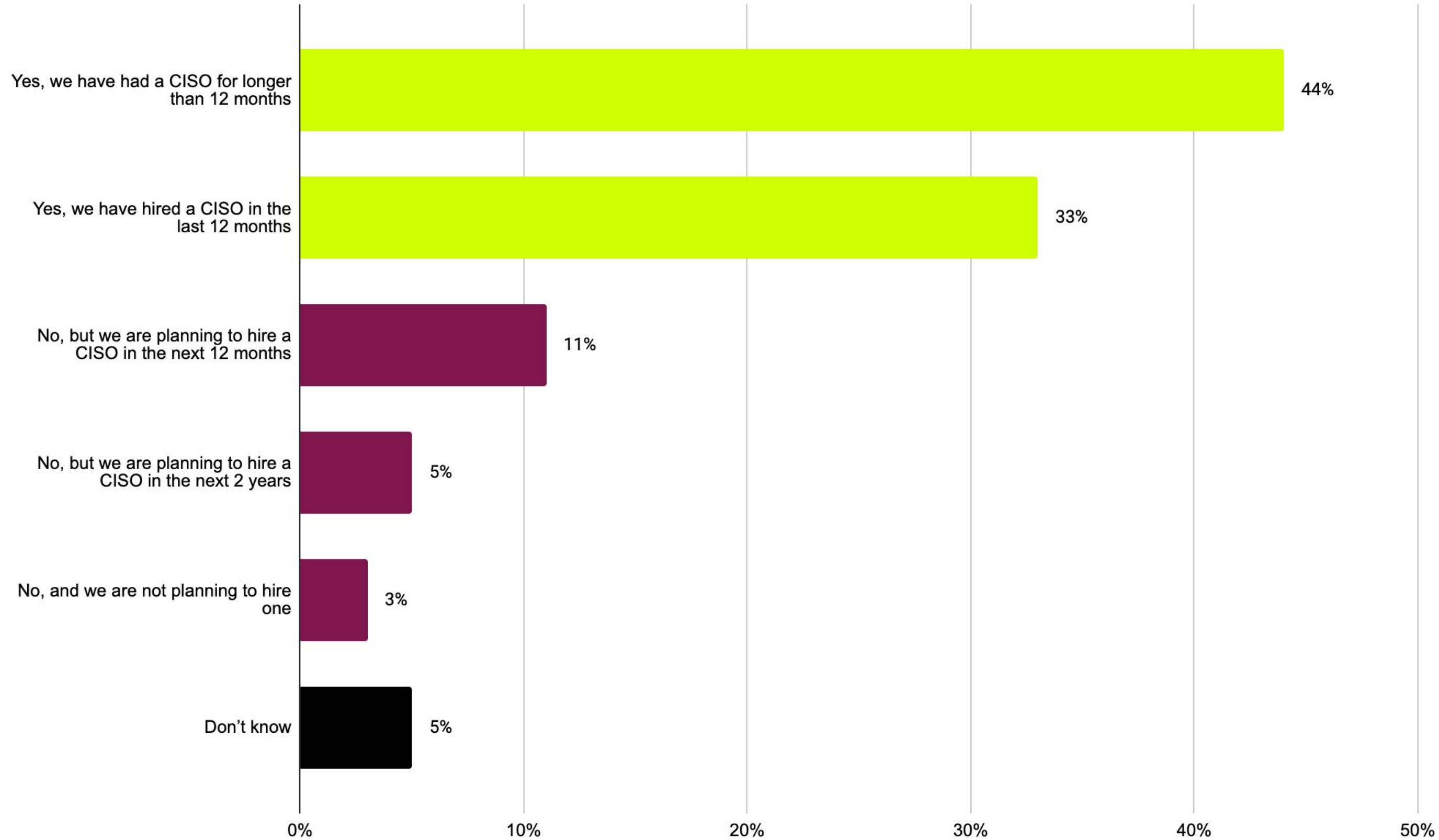
Respondents feel that the biggest gap among the current talent pool is the lack of relevant technical skills (41%)



Q9. Where do you feel there are gaps among the current talent pool when it comes to cybersecurity? Select all that apply

Base: 209

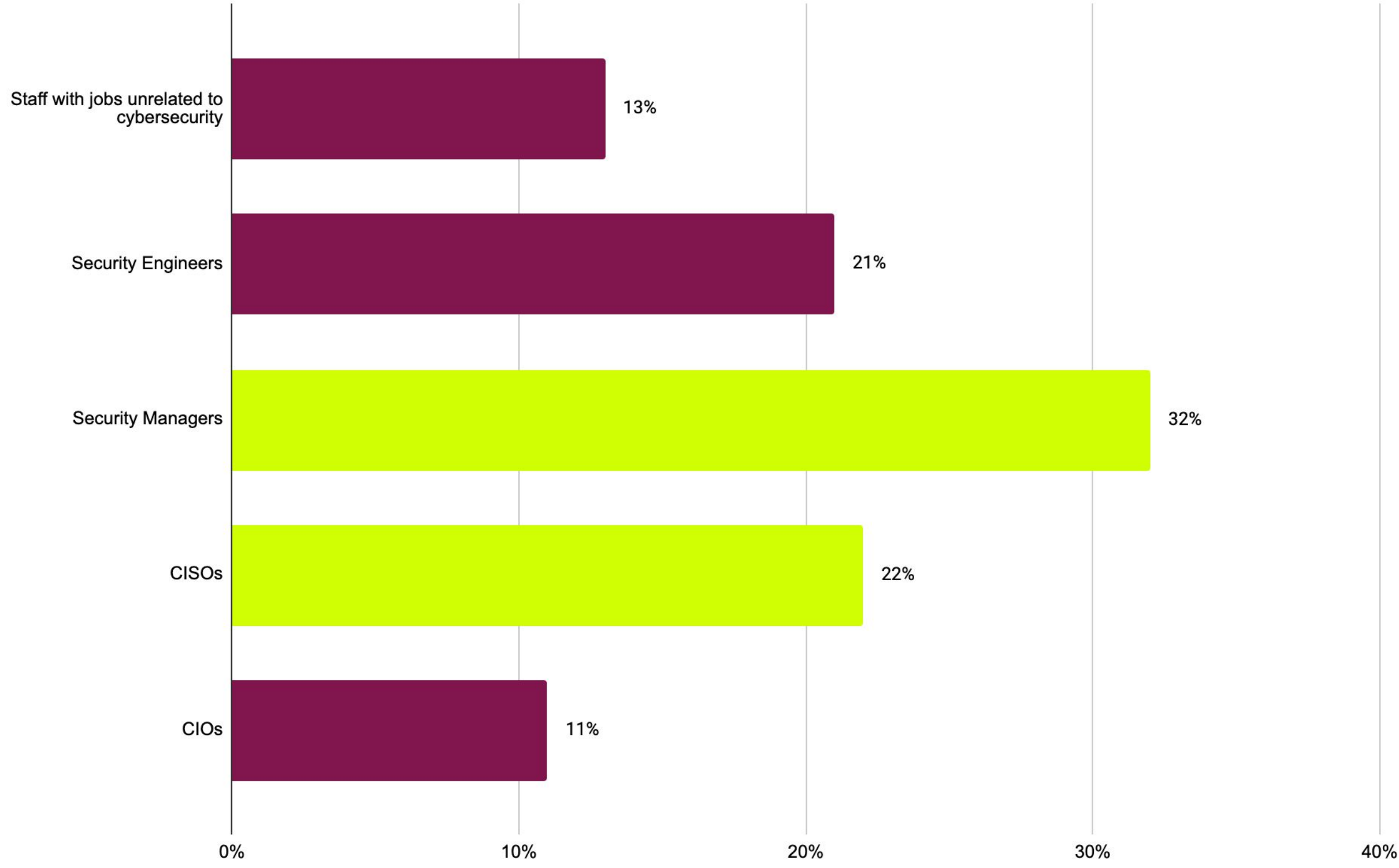
77% of respondents have hired a CISO, 33% of those within the last 12 months



Q9. Where do you feel there are gaps among the current talent pool when it comes to cybersecurity? Select all that apply

Base: 209

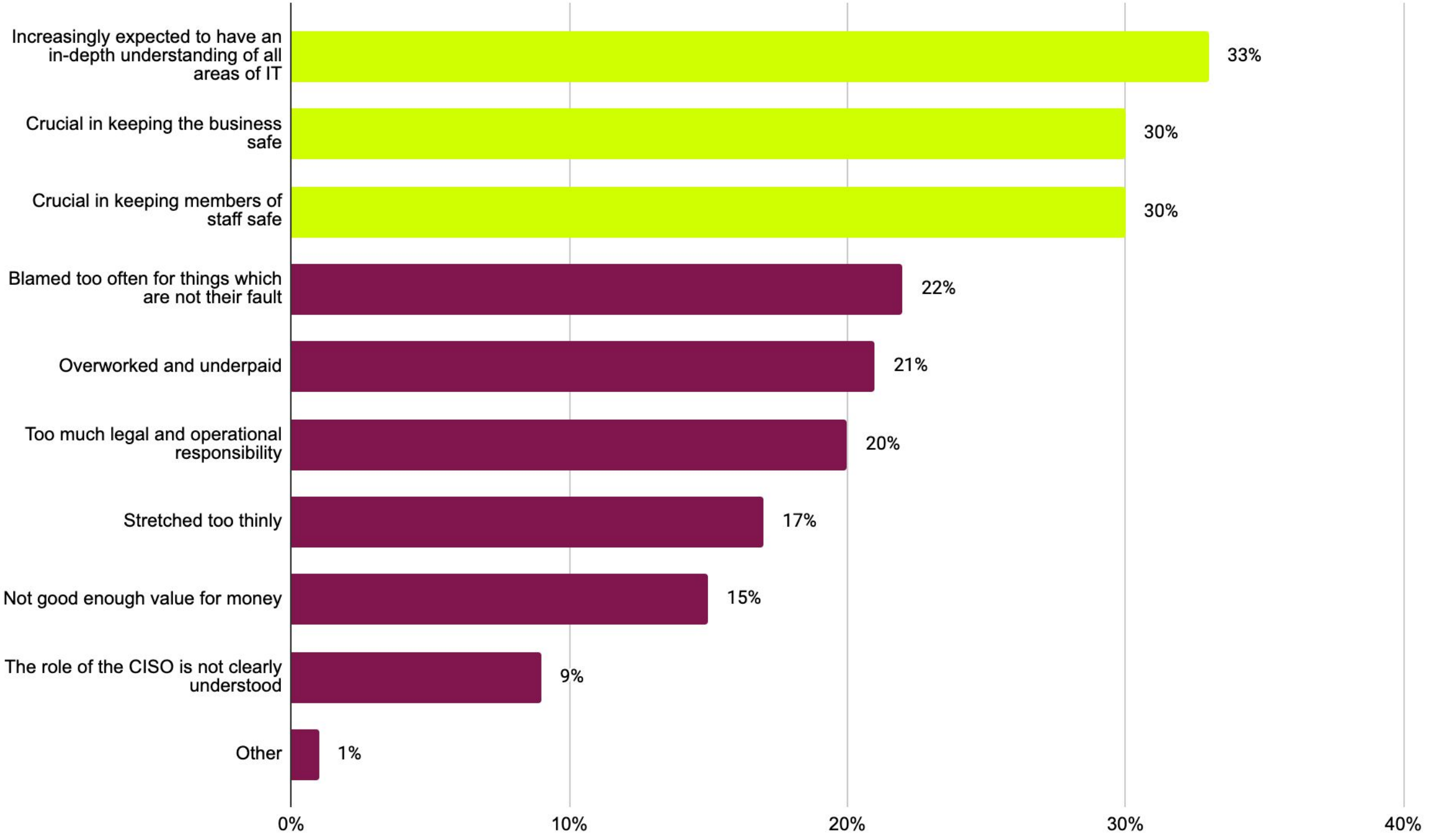
32% of respondents think Security managers are often held responsible for cybersecurity incidents, 22% think CISOs are often held responsible



Q11. Who do you feel is most often held responsible for cybersecurity incidents in your organisation? Select one

Base: 209

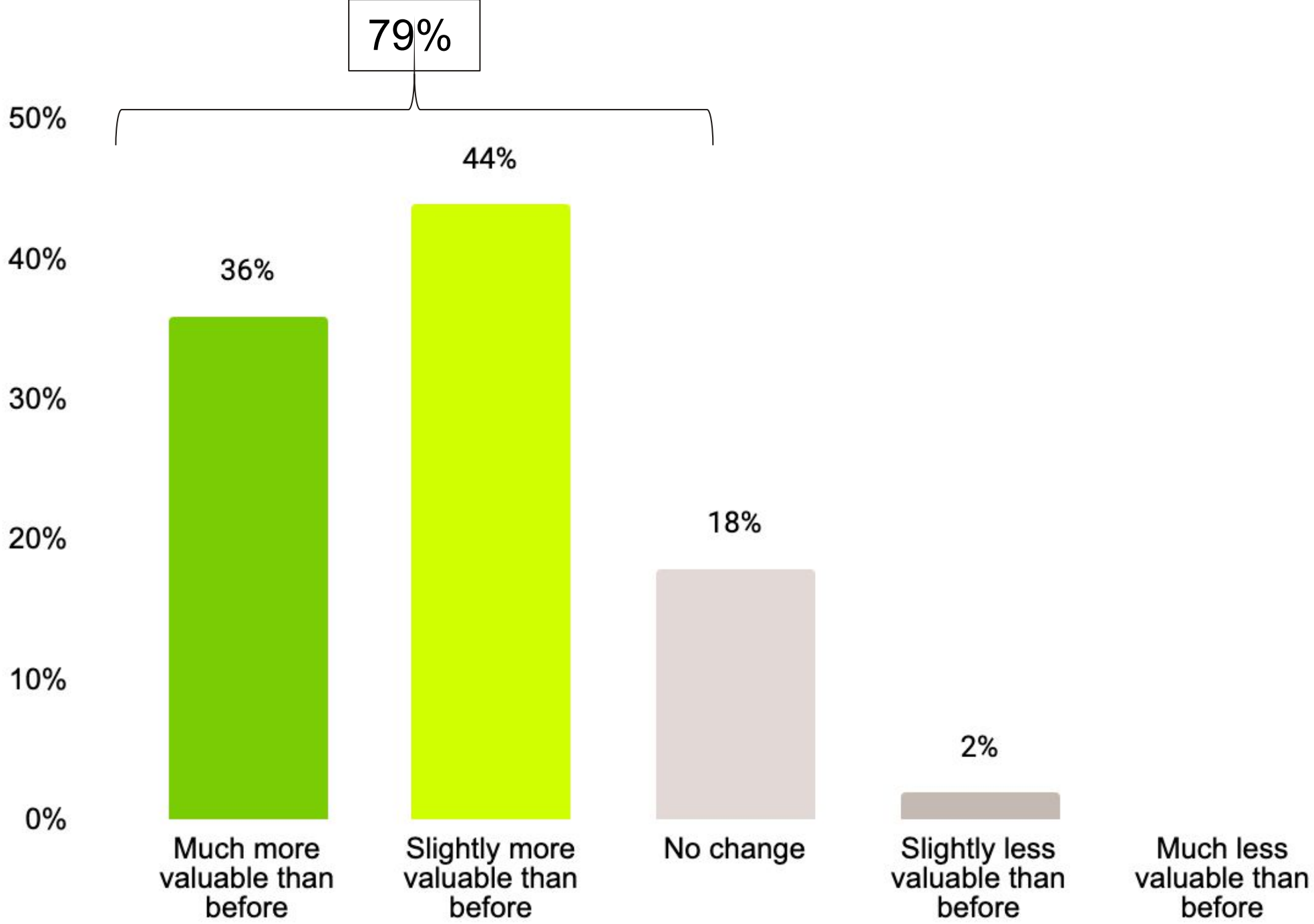
CISOs are viewed as having an in-depth understanding of all areas of IT (33%), crucial in keeping the business safe (30%), and crucial in keeping members of staff safe (30%)



Q12a. How do you think the role of the CISO is viewed by your wider organisation? Select top three

Base: 209

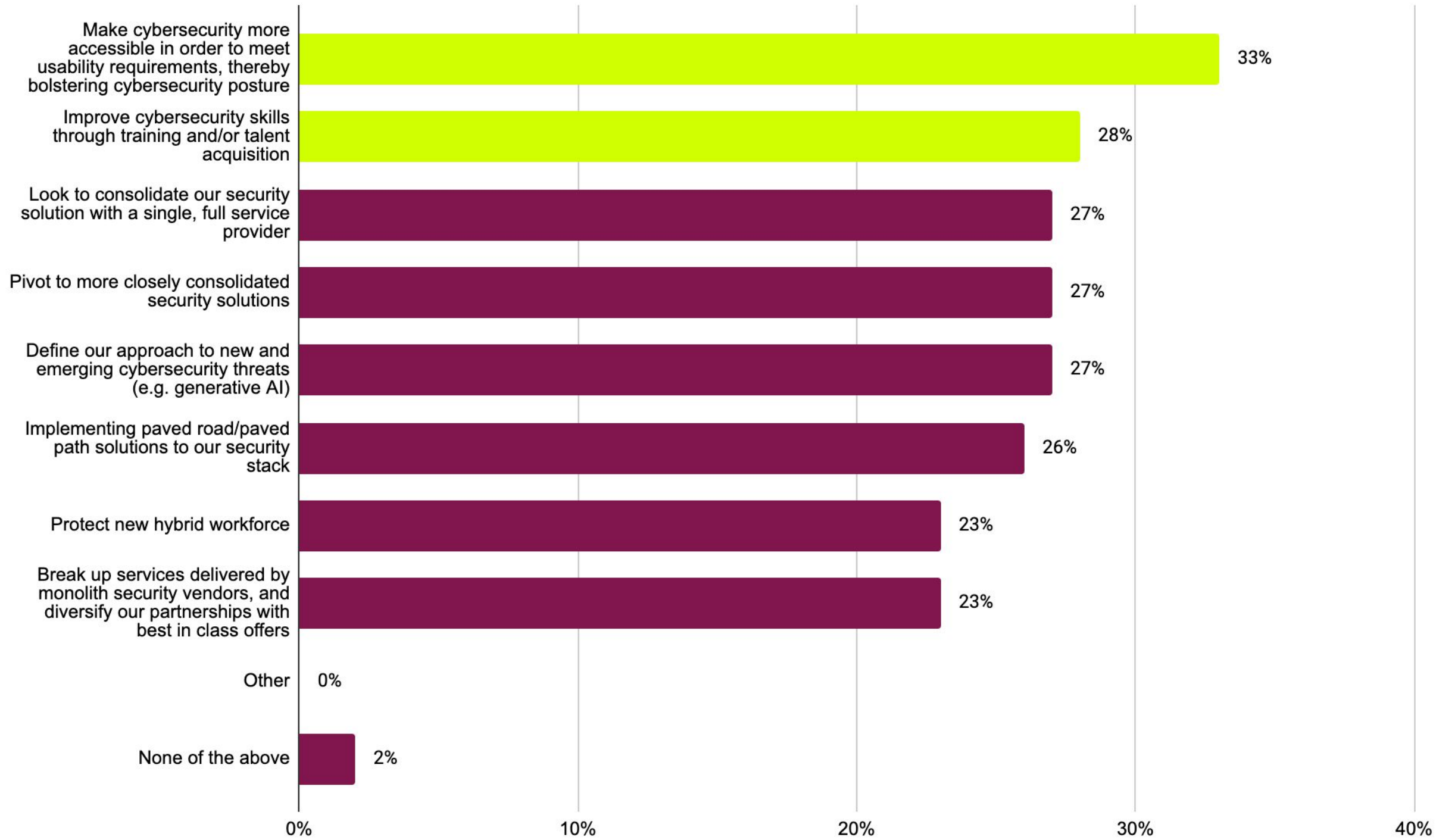
79% of respondents think their cybersecurity programme has become more valuable over the last 12 months



Q12b. How do you feel your organisation's perception of the value of your cybersecurity programme has changed over the last 12 months? Select one

Base: 209

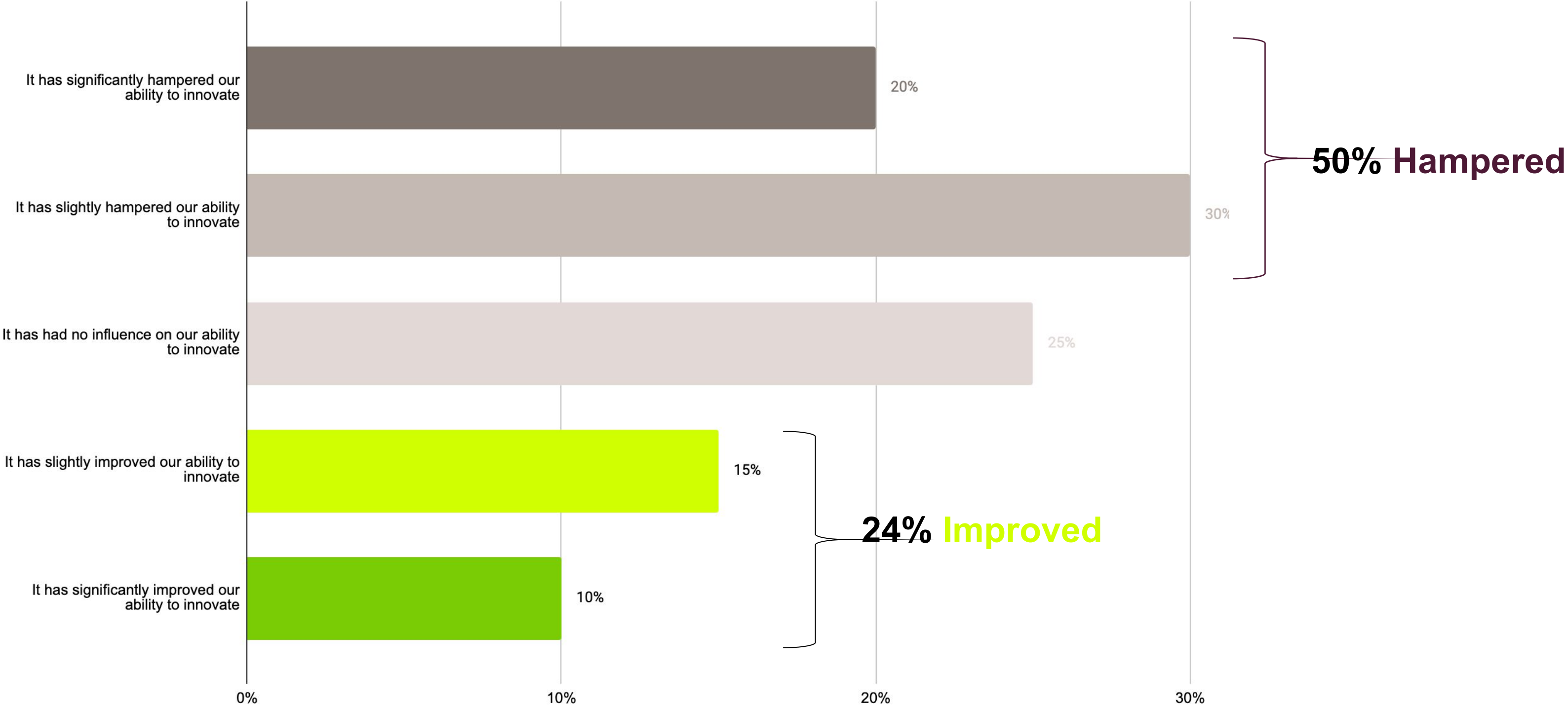
Making cybersecurity more accessible (33%) and improving cybersecurity skills (28%) are the main security priorities over the next year



Q13. What are your organisation's security priorities over the next year? Select top three

Base: 209

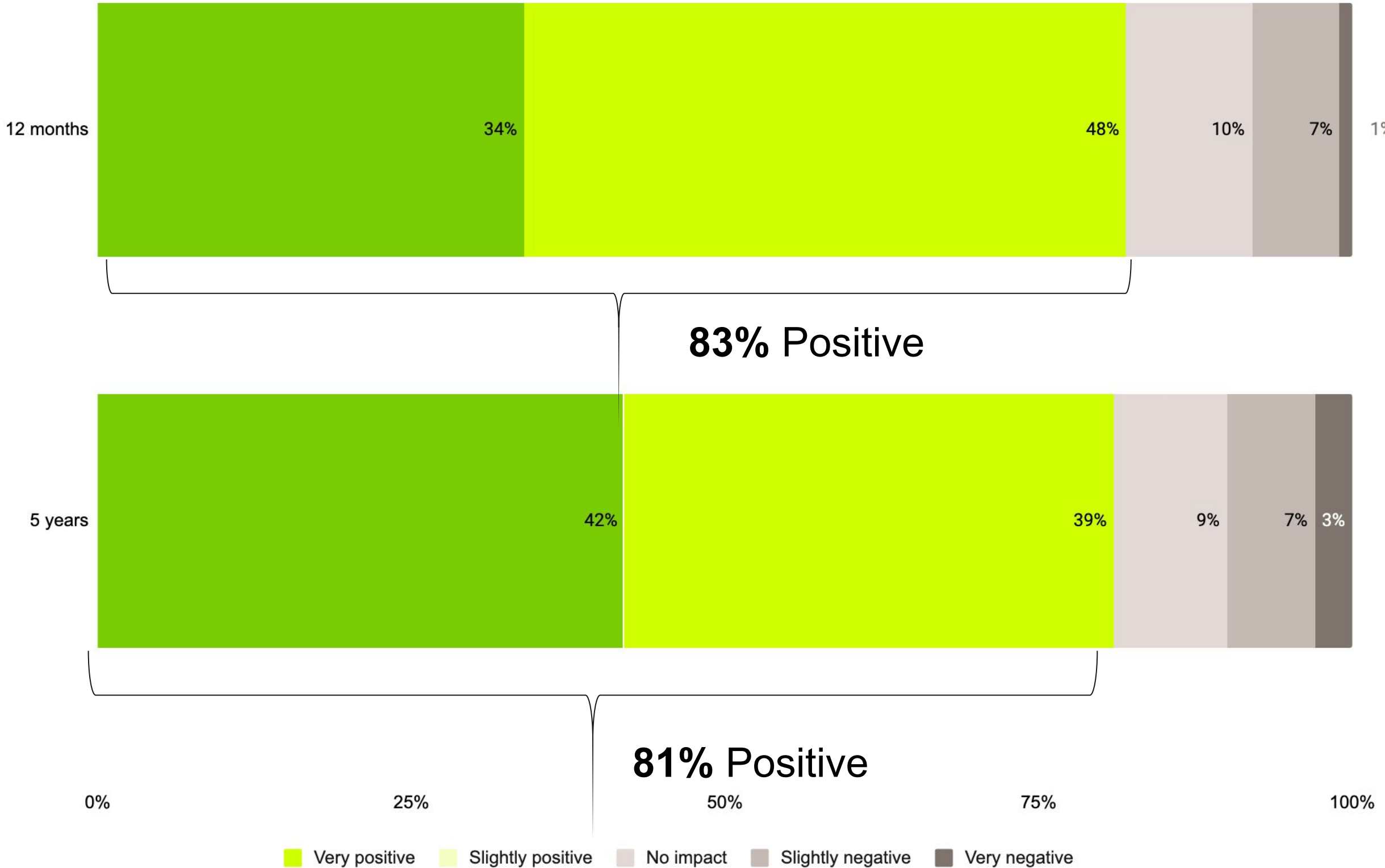
50% say that their organisations cybersecurity strategy has hampered business innovation Only a quarter say it has improved innovation (24%)



Q15. What impact has your organisation's cybersecurity strategy had on business innovation? Select one

Base: 209

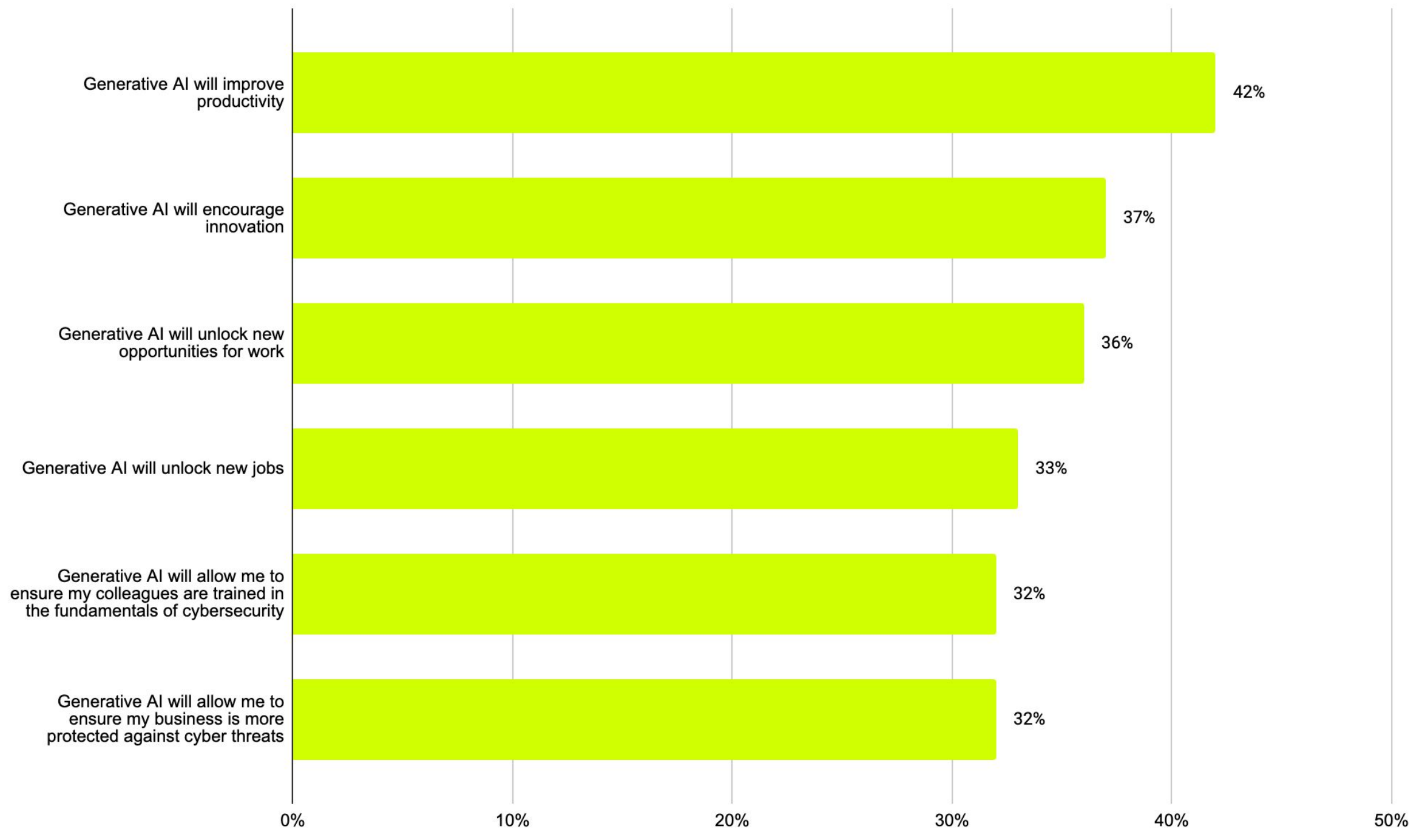
83% predict that Generative AI will have a positive impact on cybersecurity over the next 12 months
81% predict it will have a positive impact over the next 5 years



Q16. What do you predict will be the impact of Generative AI on cybersecurity over the next...

Base: 209

Improving productivity (42%), encouraging innovation (37%) and unlocking new opportunities for work (36%) are the main positive impacts of Generative AI

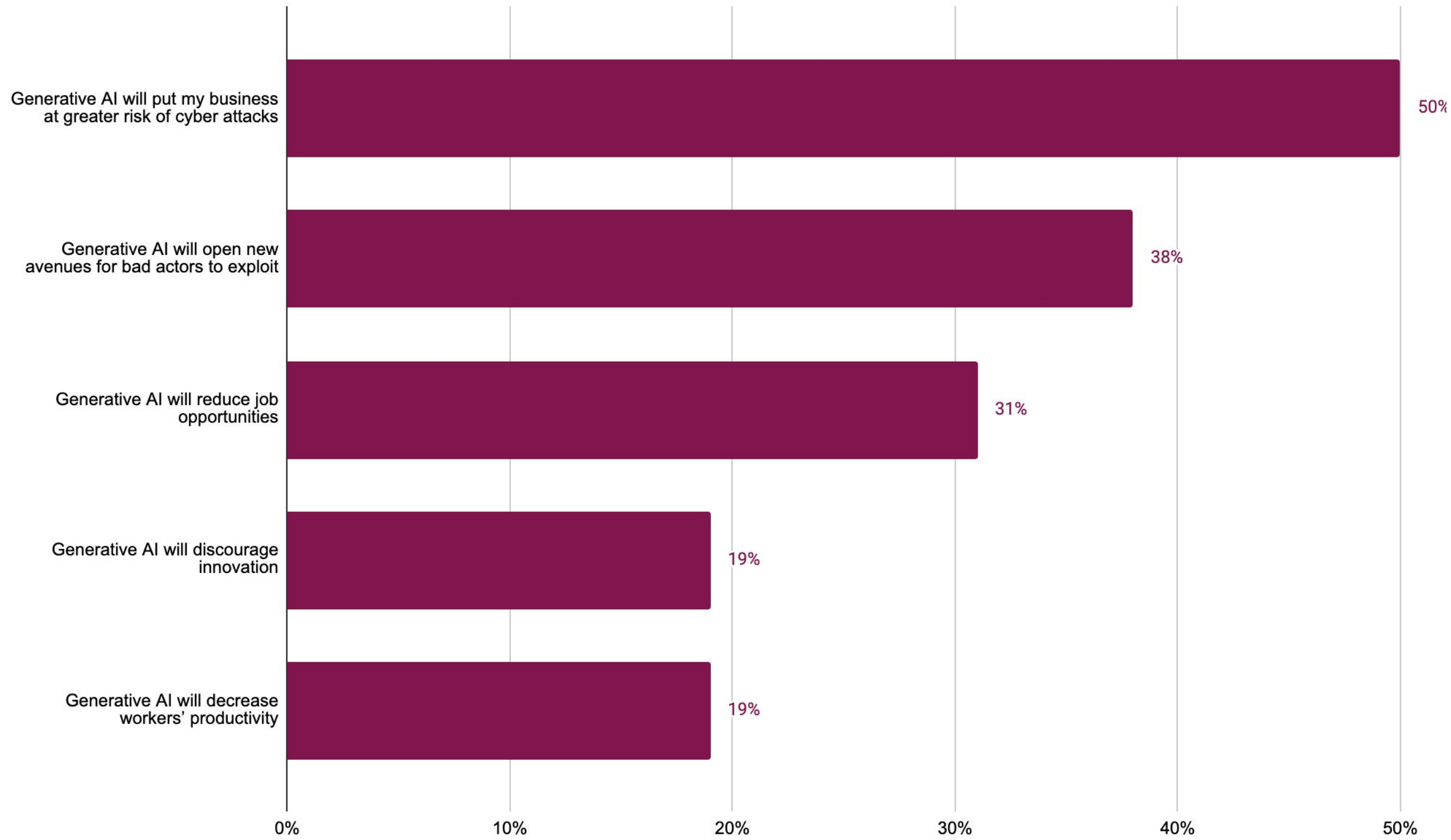


*only asked to those who said generative AI will have a positive impact in the next 12 months

Base : 173*

Q17a. You mentioned generative AI will have a positive impact over the next 12 months? Which of the following are the most likely reasons for this? Select all that apply

There are fears that Generative AI will put businesses at greater risk of cyber attacks (50%)

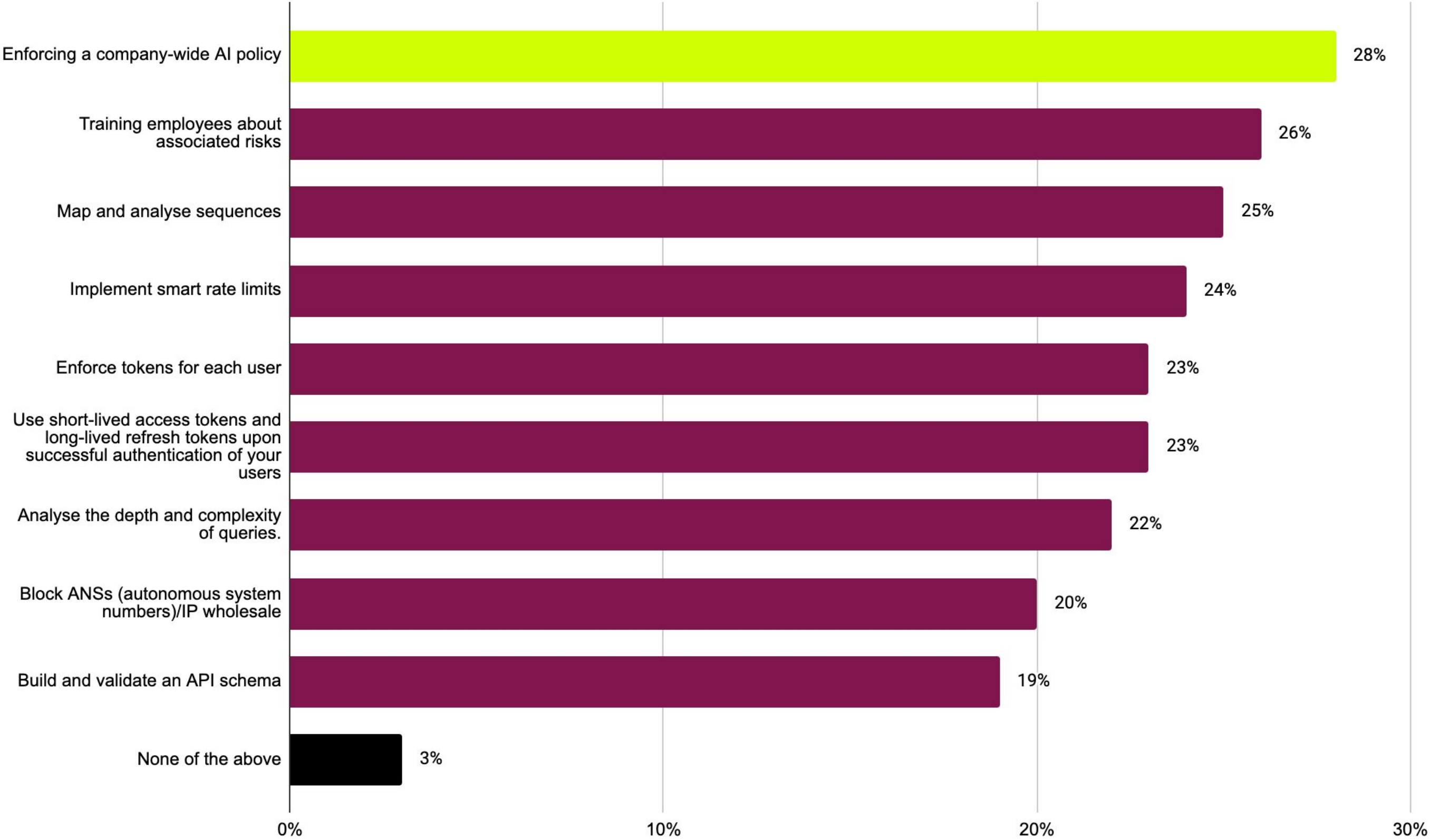


*only asked to those who said generative AI will have a negative impact in the next 12 months

Base: 16*

Q17b. You mentioned generative AI will have a negative impact over the next 12 months? Which of the following are the most likely reasons for this? Select all that apply

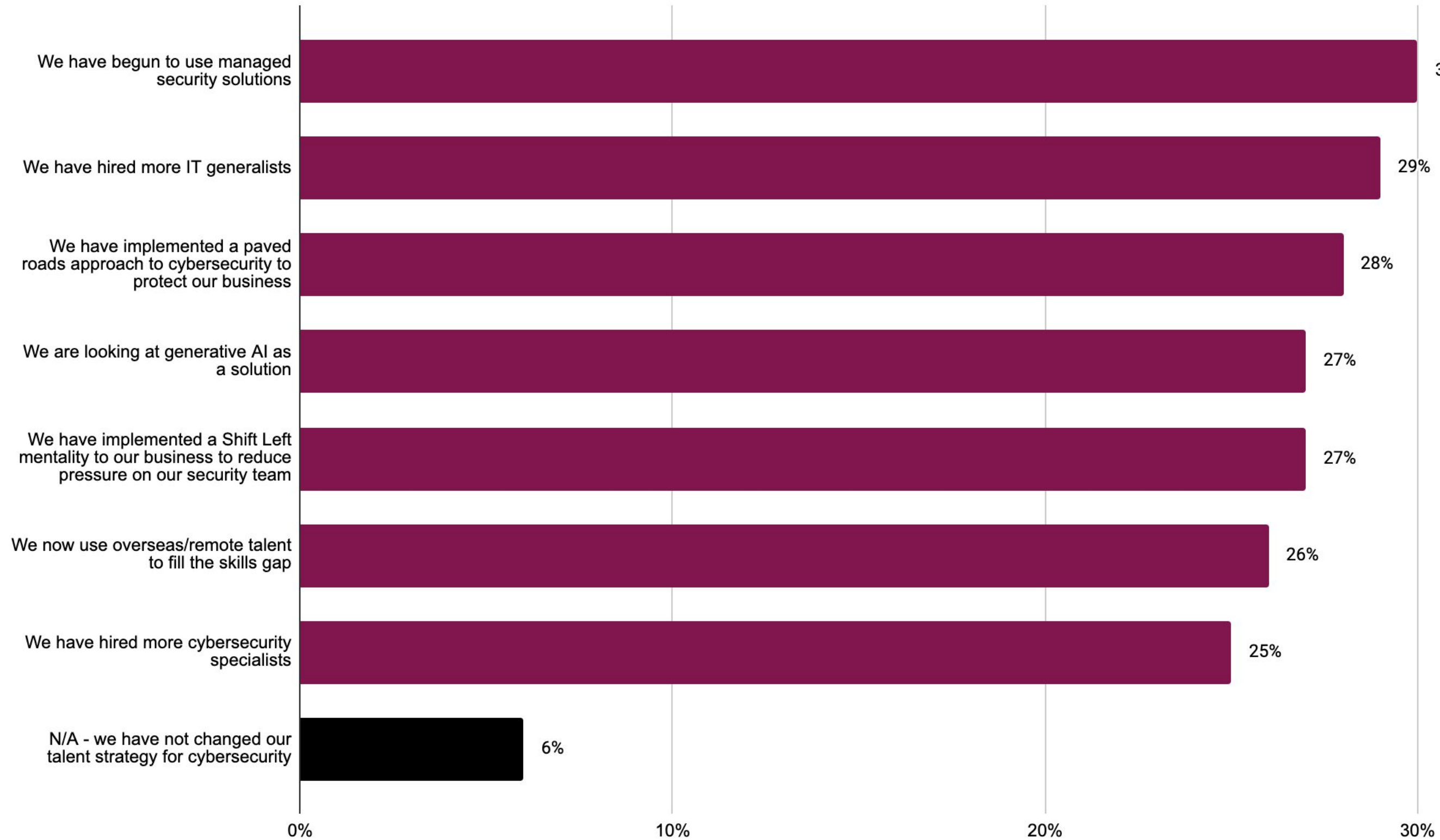
Enforcing a company-wide AI policy (28%) is the top step companies are taking to mitigate generative AI security threats



Q18. What steps is your organisation taking to mitigate generative AI security threats? Select top three

Base: 209

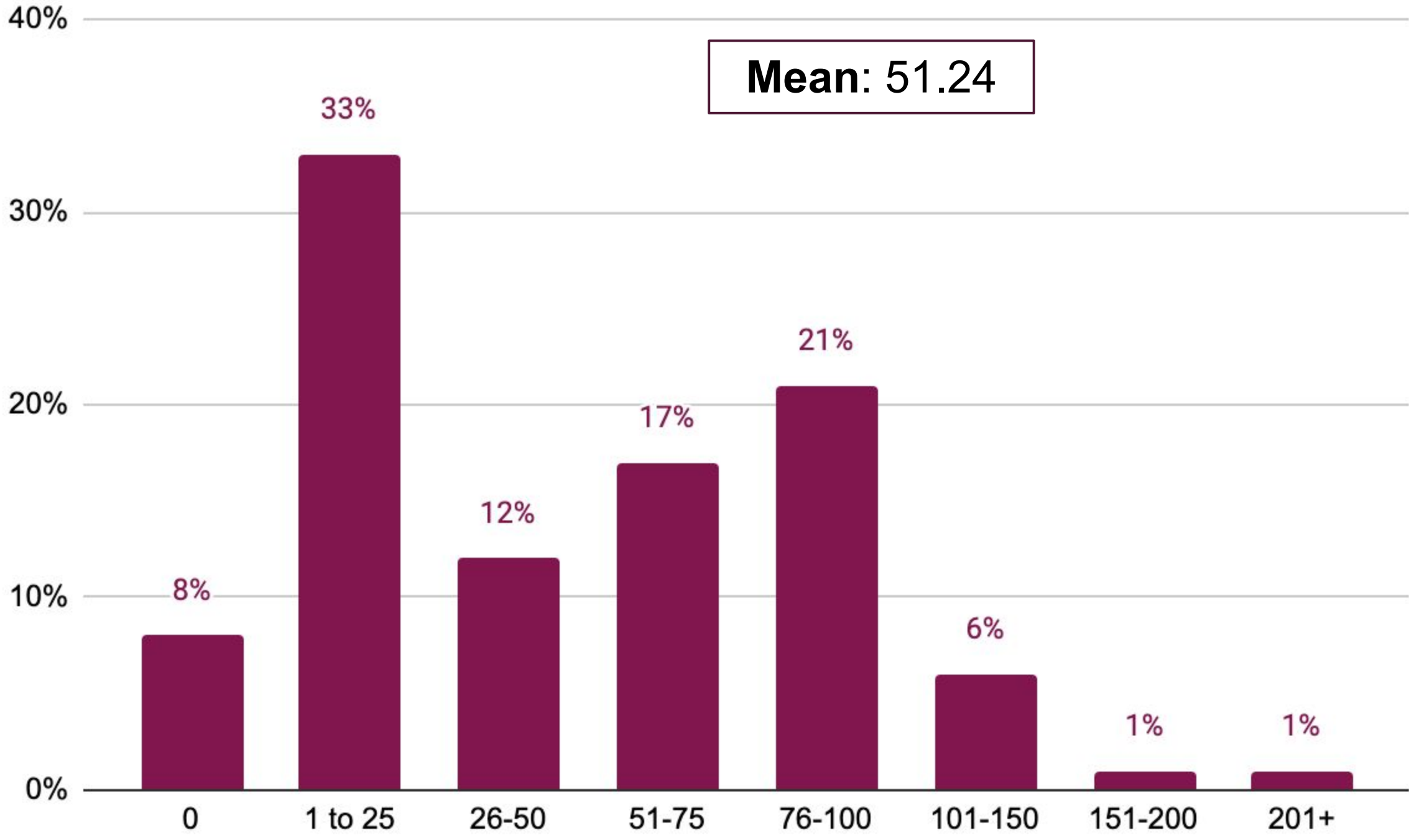
30% of companies have begun to use managed security solutions over the last 12 months



Q19. Thinking back to 12 months ago, how has your talent strategy for cybersecurity changed, if at all? Select all that apply

Base: 209

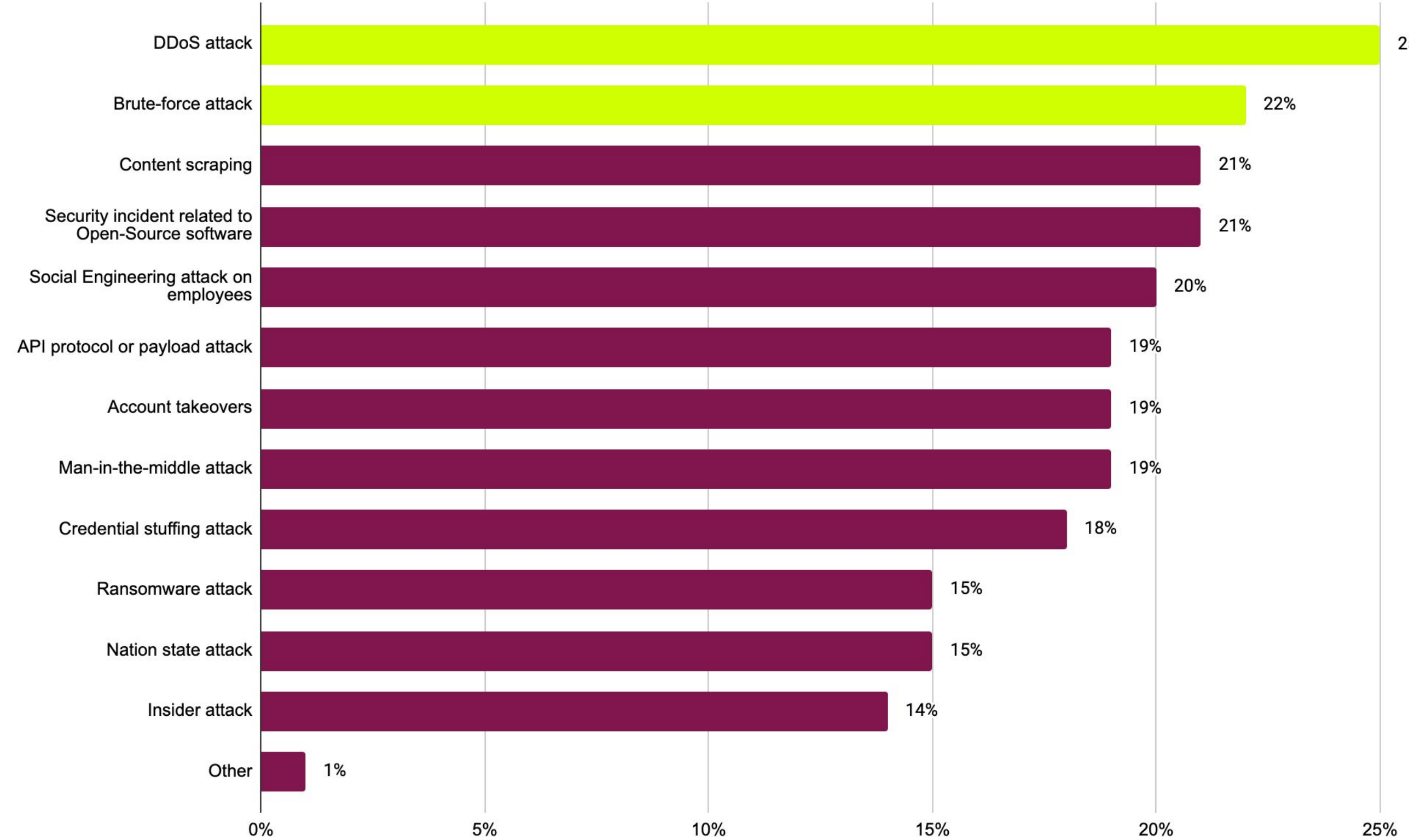
On average, businesses have suffered 51 cyberattacks in the past 12 months



Q20. How many cyber attacks has your business suffered in the past 12 months? Select one

Base: 209

The most common types of cyberattacks were DDoS attacks (25%), security related to open-source software and brute-force attacks (both 22%)

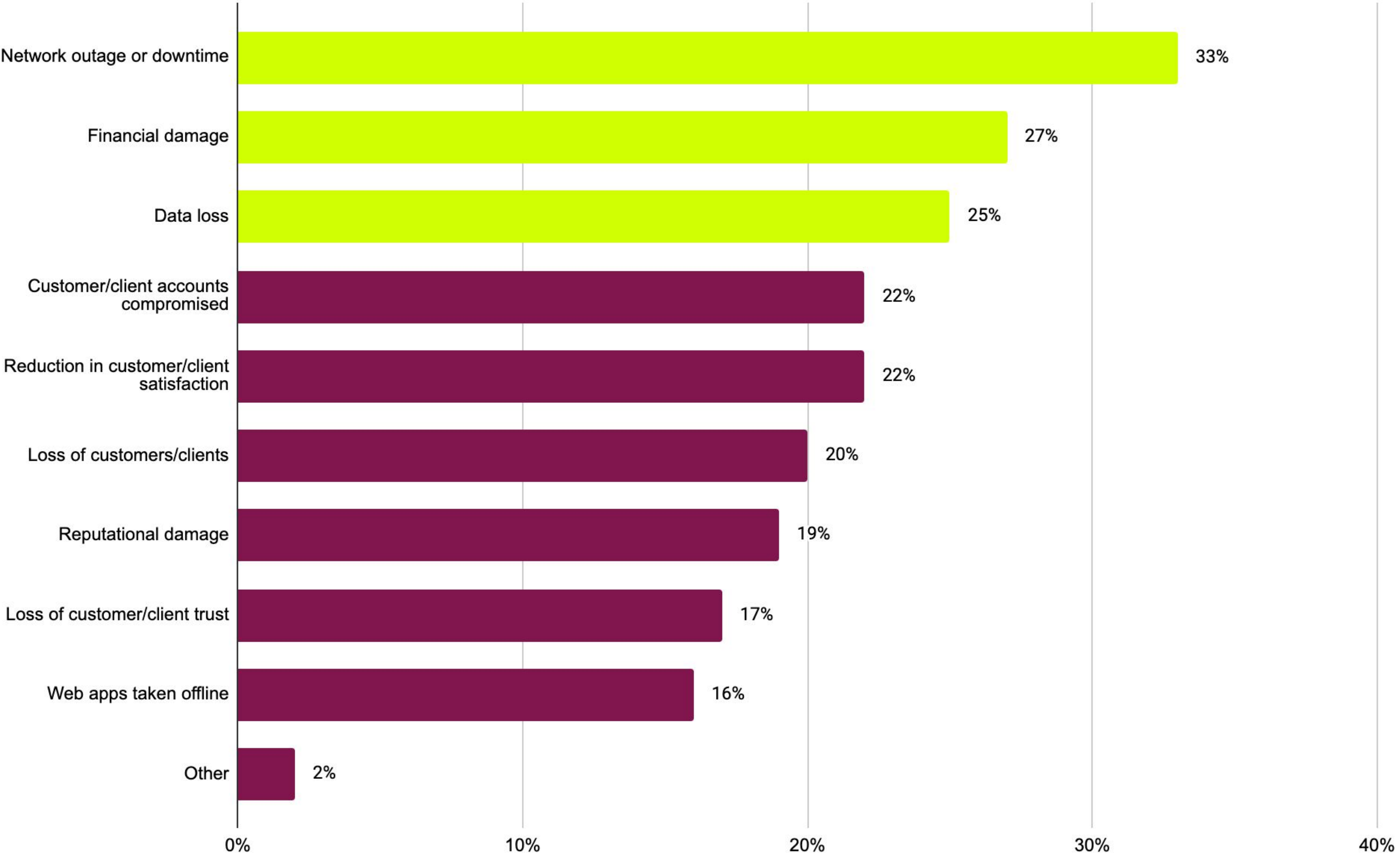


*only asked to those who have experienced a cyber attack

Q21. What kind of cyber attack was it? If you had more than one cyber attack, please select all that apply

Base: 192*

Network outages or downtime (33%), financial damage (27%), and data loss (25%) were the main impacts of cyber attacks

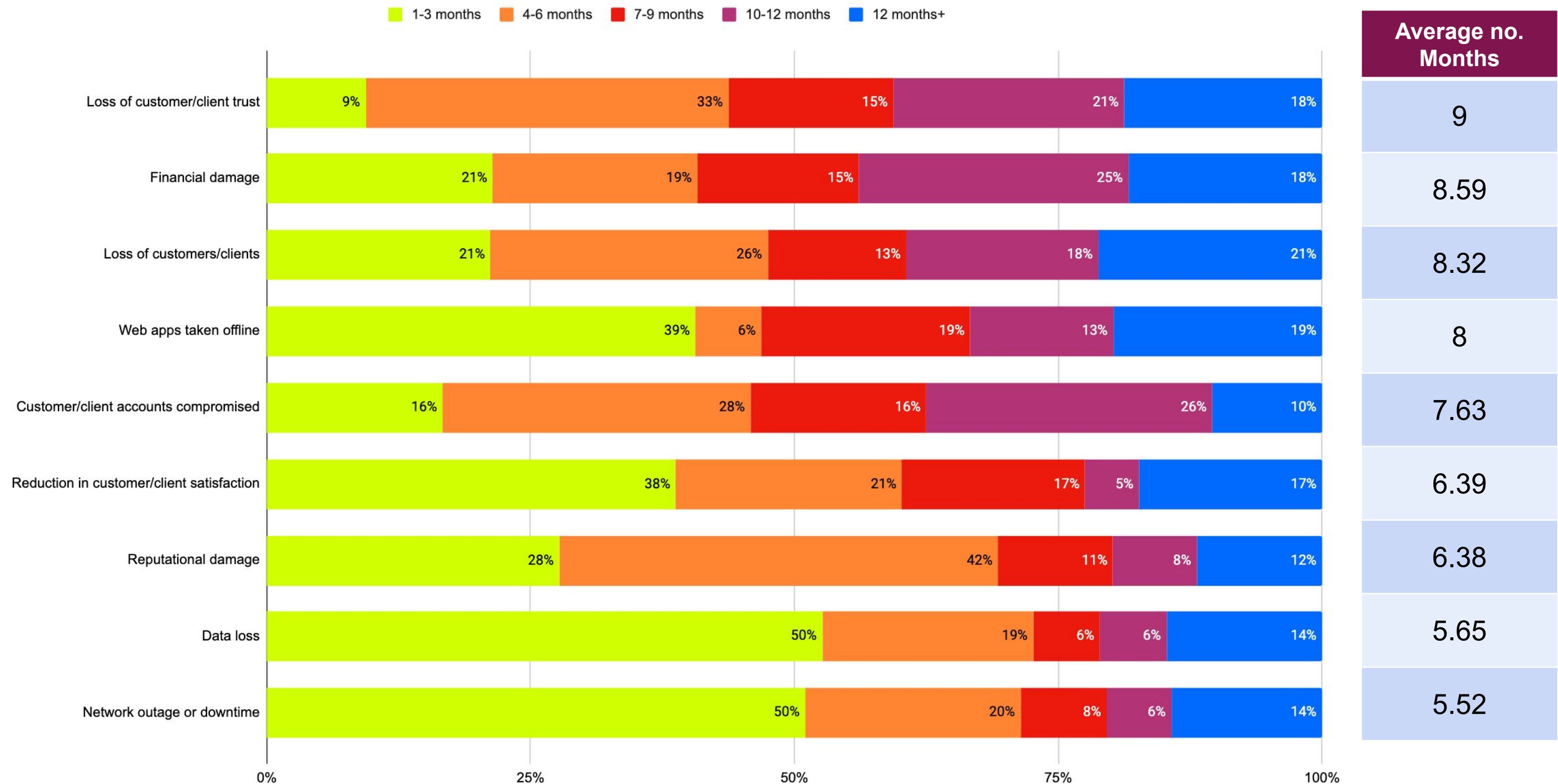


*only asked to those who have experienced a cyber attack

Q21. What kind of cyber attack was it? If you had more than one cyber attack, please select all that apply

Base: 192*

On average, it will take businesses 9 months to recover from the loss of customers/ clients trust and financial damage as a result of a cyber attack

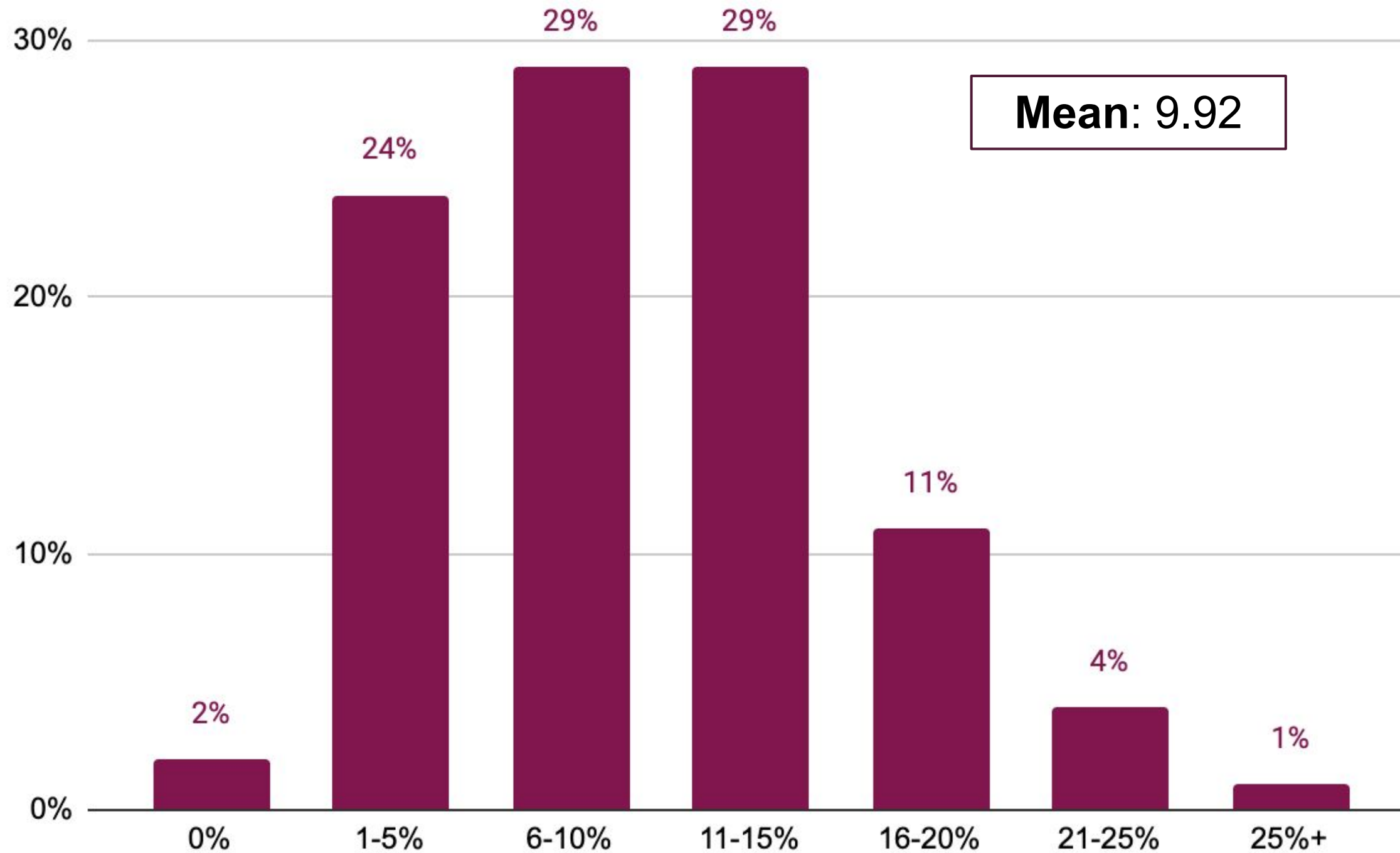


*only asked to those who had experienced each impact at Q22

Q23. How long has it taken, or how long do you expect it to take, to fully recover from each of these impacts?

Base: varies*

On average, businesses lose 10% of their annual income as a result of cyber attacks



*only asked to those who had experienced each impact at Q22

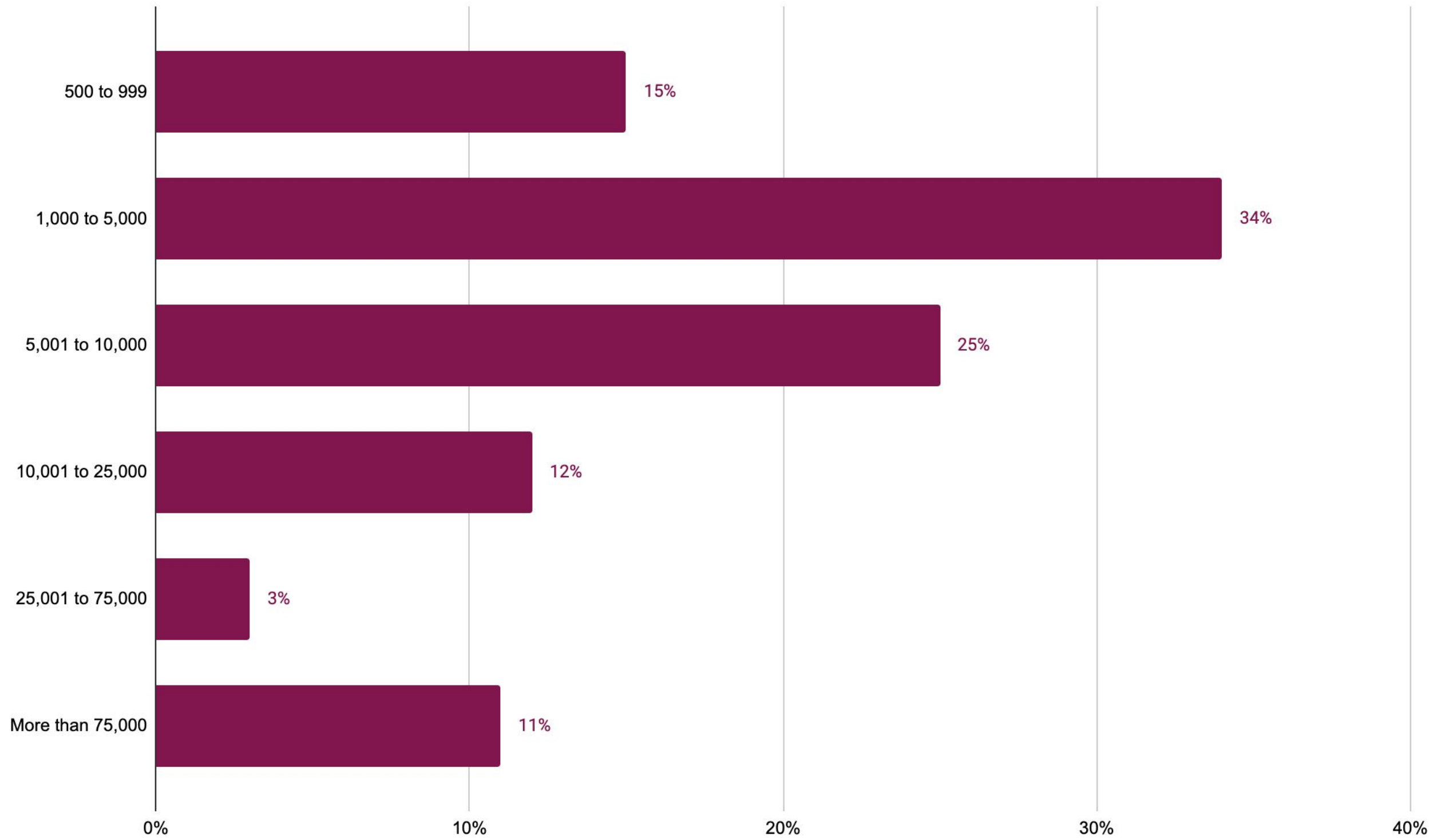
Base: 192*

Q24. As a percentage of your business's overall revenue, what would you estimate to be the financial impact of these attacks in the past 12 months? Select one



Demographics

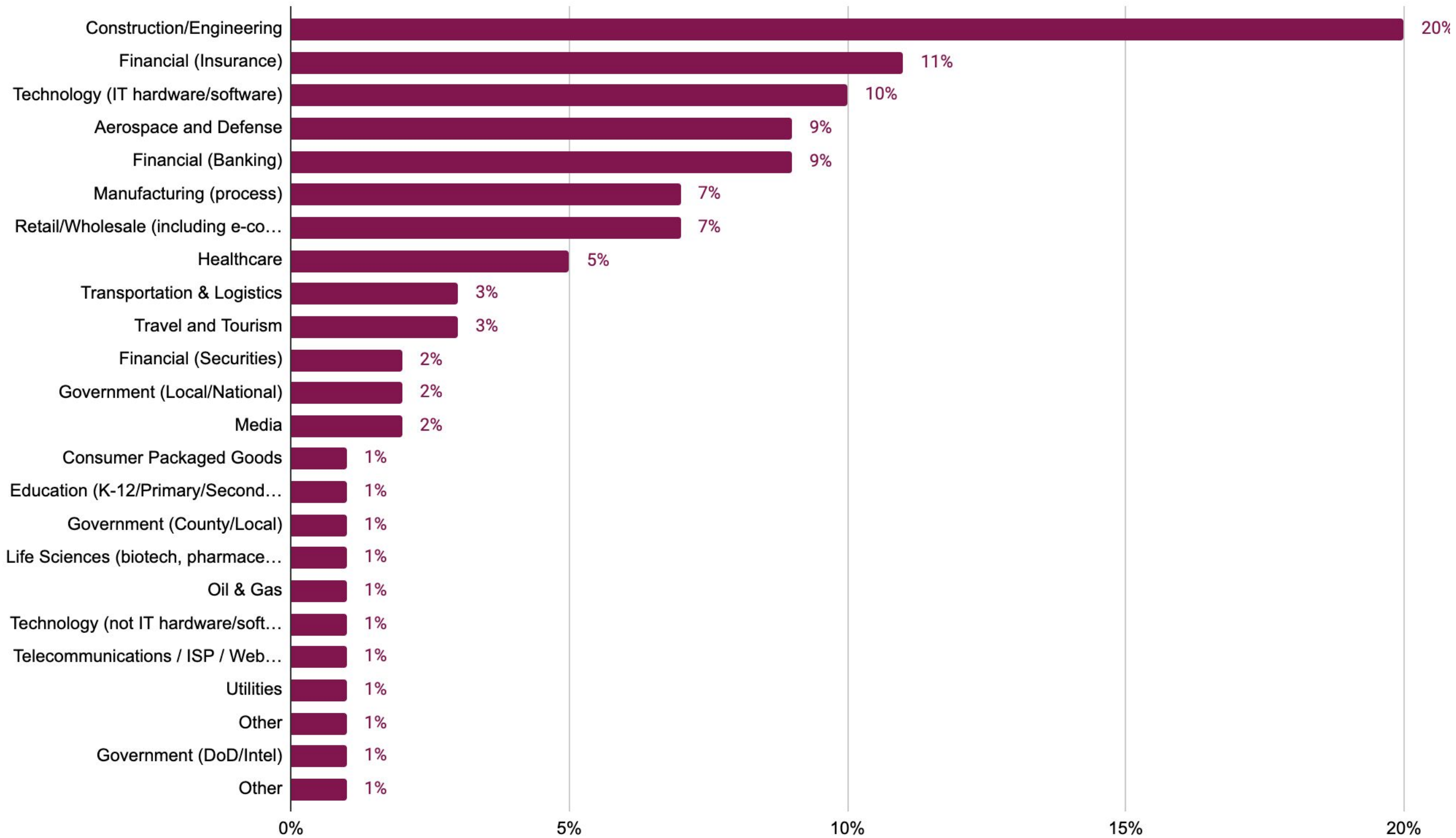
Size



S1. How many employees does your organisation have? Select one

Base: 209

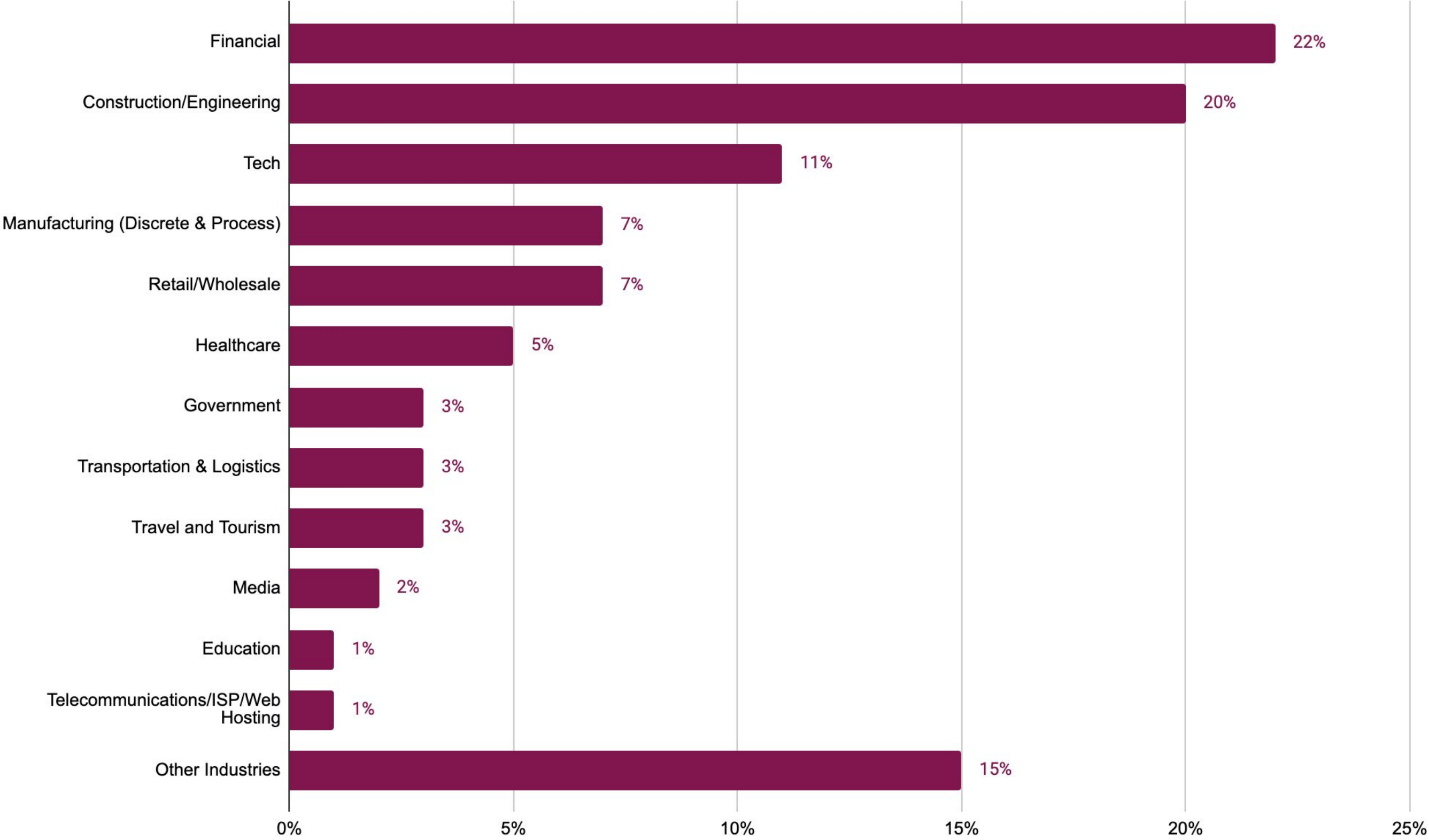
Industry



S2. What is your company's primary industry? Select one

Base: 209

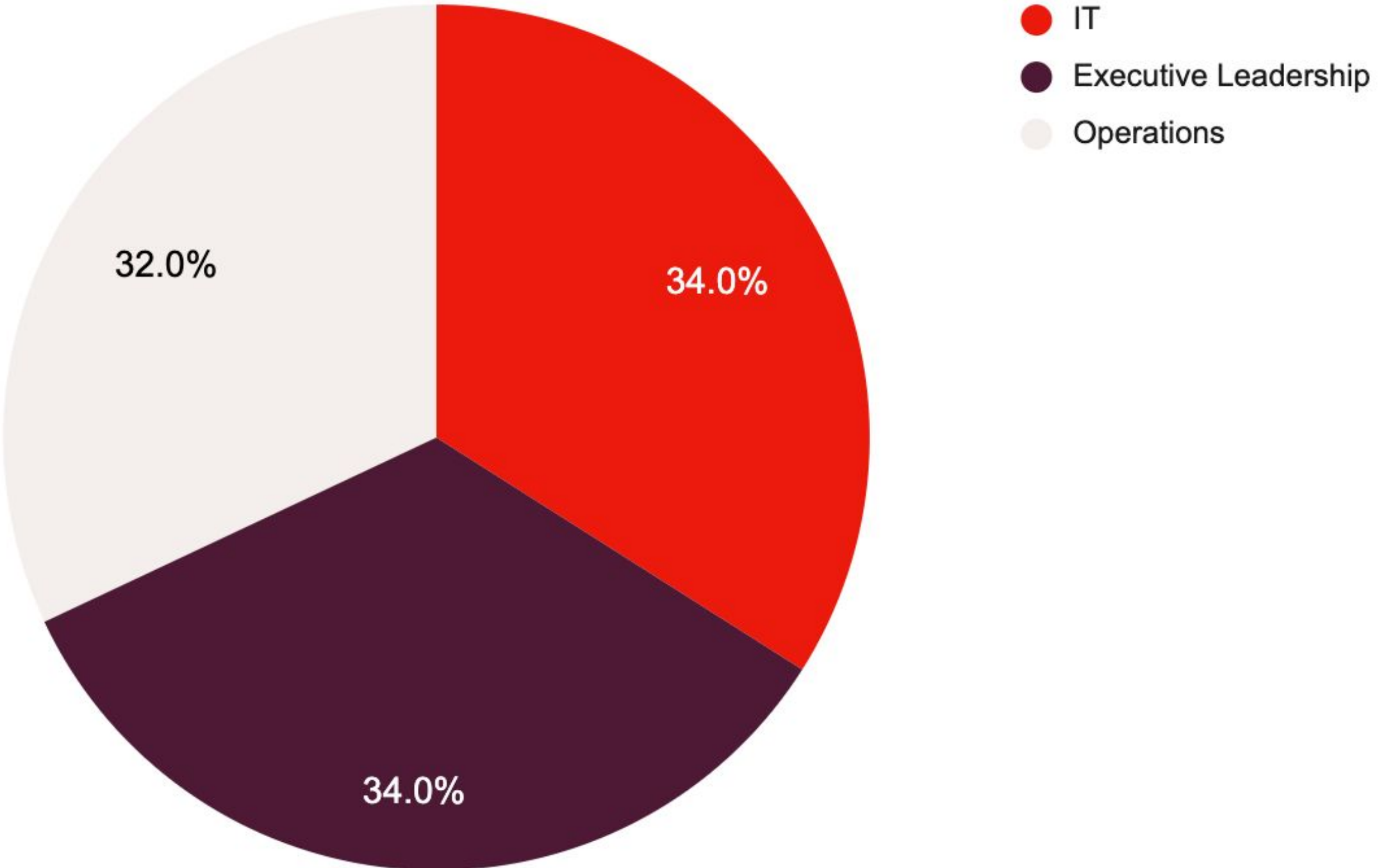
Industry - focus



S2. What is your company's primary industry? Focus

Base: 209

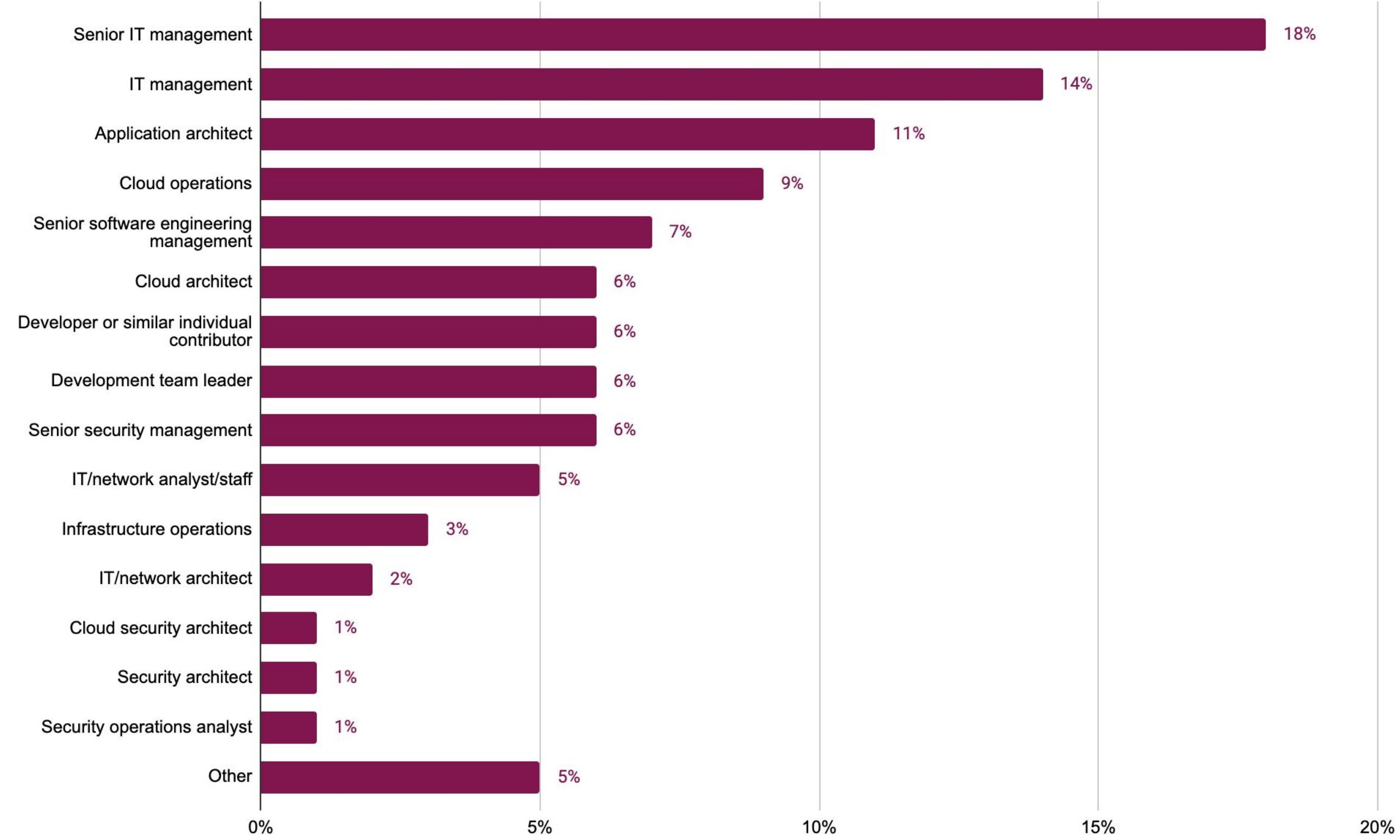
Department



S3. Which of the following best describes the department you sit within? Select one

Base: 209

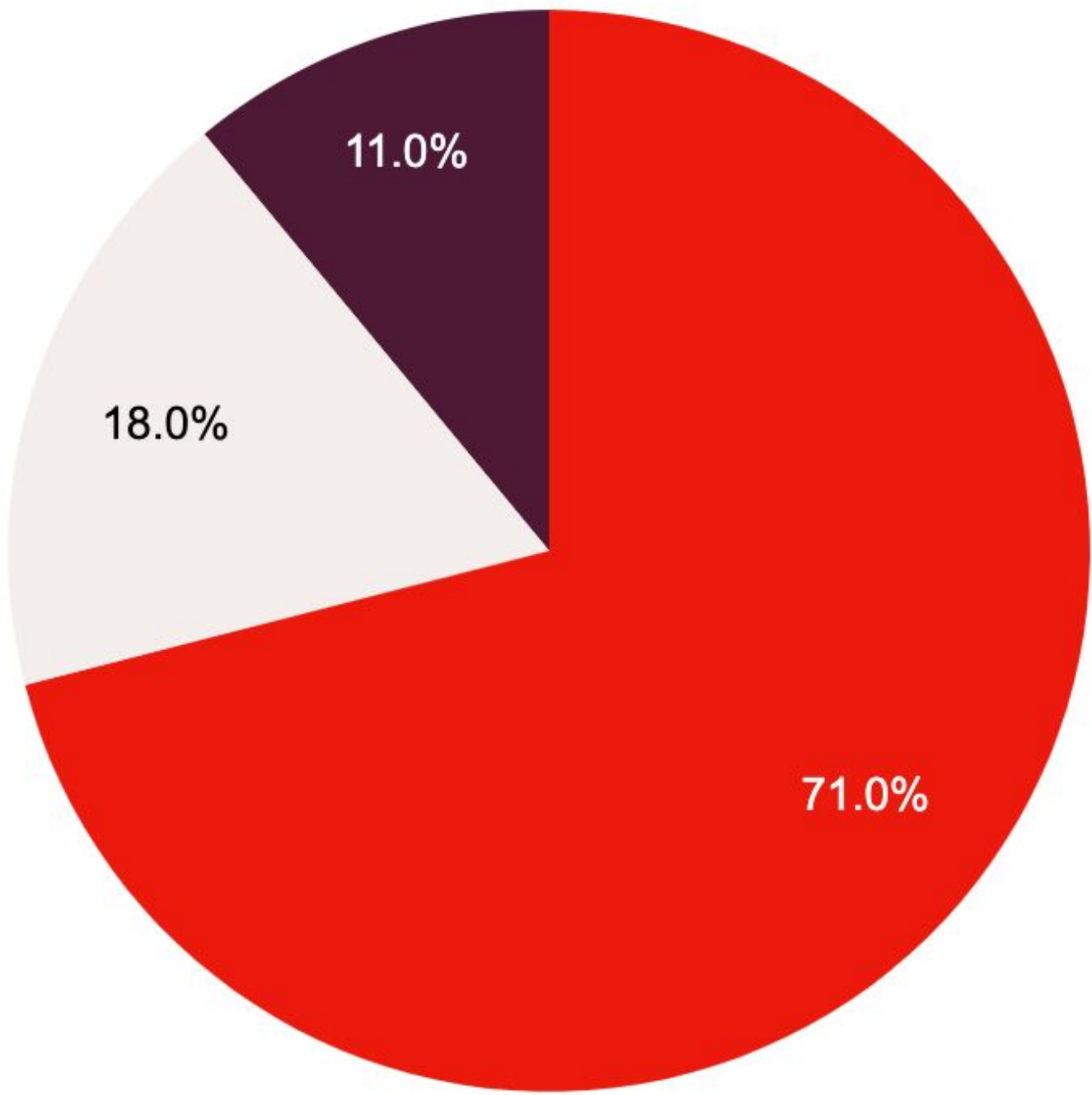
Current responsibility



S4. Which of the following best describes your current responsibility within your organisation? Select one

Base: 209

Cyber security decision making



- Yes, I make or influence decisions regarding this
- Yes, I am fully aware of this
- Yes, I am somewhat aware of this

S5. Within your current job role, are you aware of or do you make or influence decisions regarding cybersecurity within your organisation? Select one

Base: 209

Thank you!

fastly[®]