Fastly Global Security Research 2023

Australia and New Zealand Findings

November 2023

Research conducted by
SAPIO Research

Project overview and methodology

- The survey was conducted among **211** IT Decision Makers (more than 2/3 respondents directly make or influence cybersecurity decisions) in organisations with 250+ in Australia and New Zealand. 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 ± **6.7**% at 95% confidence limits assuming a result of 50%.

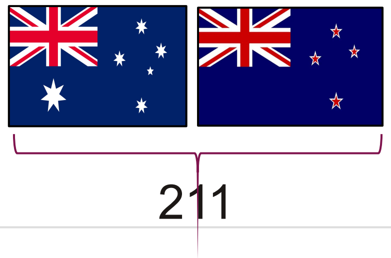
- The interviews were conducted online by Sapio Research in **August, September & October 2023** using an email invitation and an online survey.

Respondent demographics summary

Demographics

Total respondents: 211

Country of residence



Department

IT: 43%

Ops: 36%

Executive Leadership : 21%

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	9%	18%	18%	17%	15%	8%	14%

Industry

Company sectors – top 3:

Construction / Engineering: 23%

Financial (banking): 18%

Manufacturing: 16%

Decision making (cyber security)

- 81% make or influence cybersecurity decisions
- 12% are fully aware of decisions regarding cybersecurity
- 7% are somewhat aware of cybersecurity decisions

Key stats

42% predict **‘data breaches and data loss’** as the biggest cybersecurity threat over the **next 12 months**

On average, businesses lose **9%** of their annual income as a result of **cyber attack**

39% of respondents feel there is gap among the current talent pool **in experience** with new and emerging technologies / threats such as **generative AI**

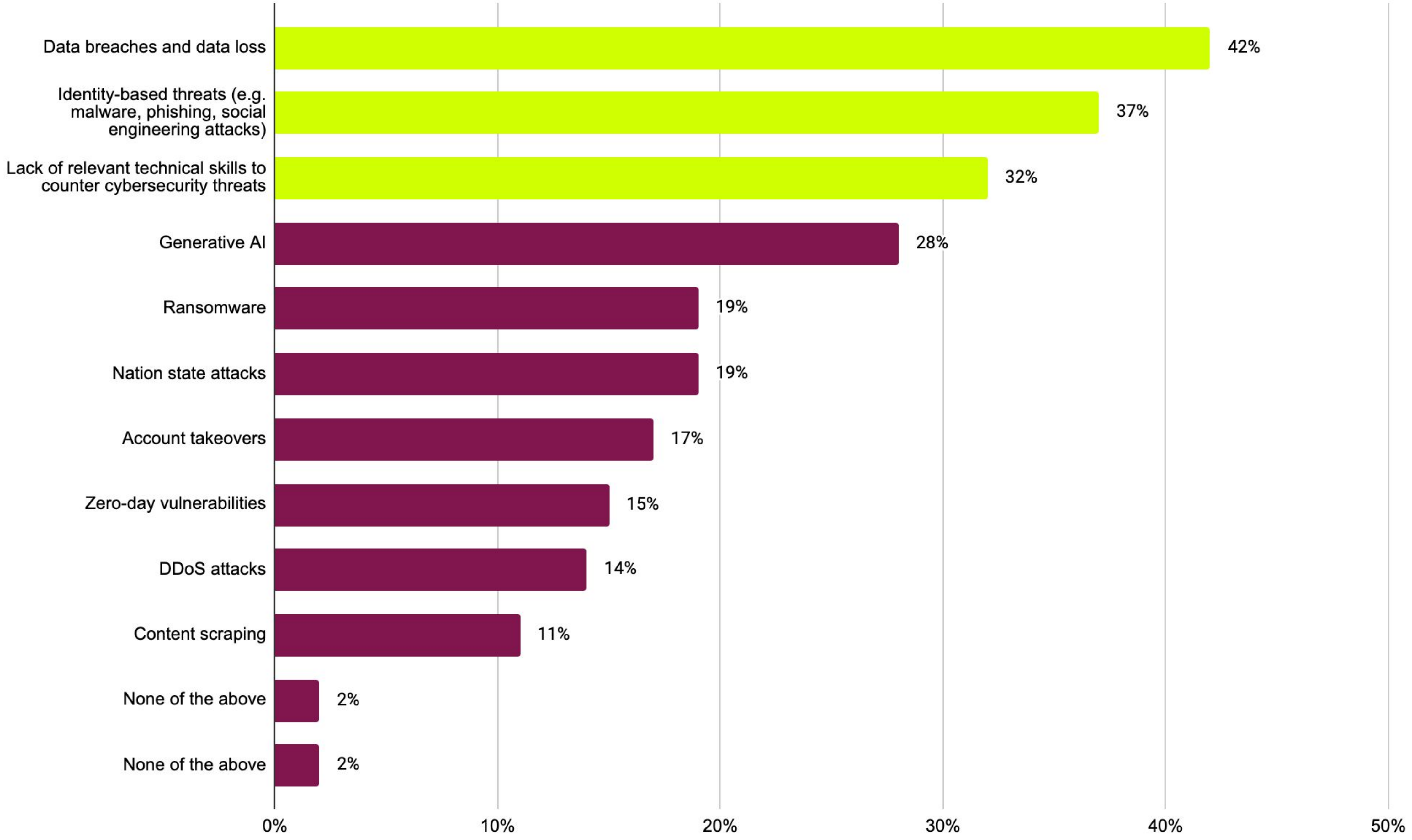
Making **cyber security more accessible (41%)**, **defining their approach (38%)**, and **improving cyber security skills through training (33%**) are the main security priorities **over the next year**

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

On average, **47%** of cybersecurity tools are fully deployed / active

Main Findings

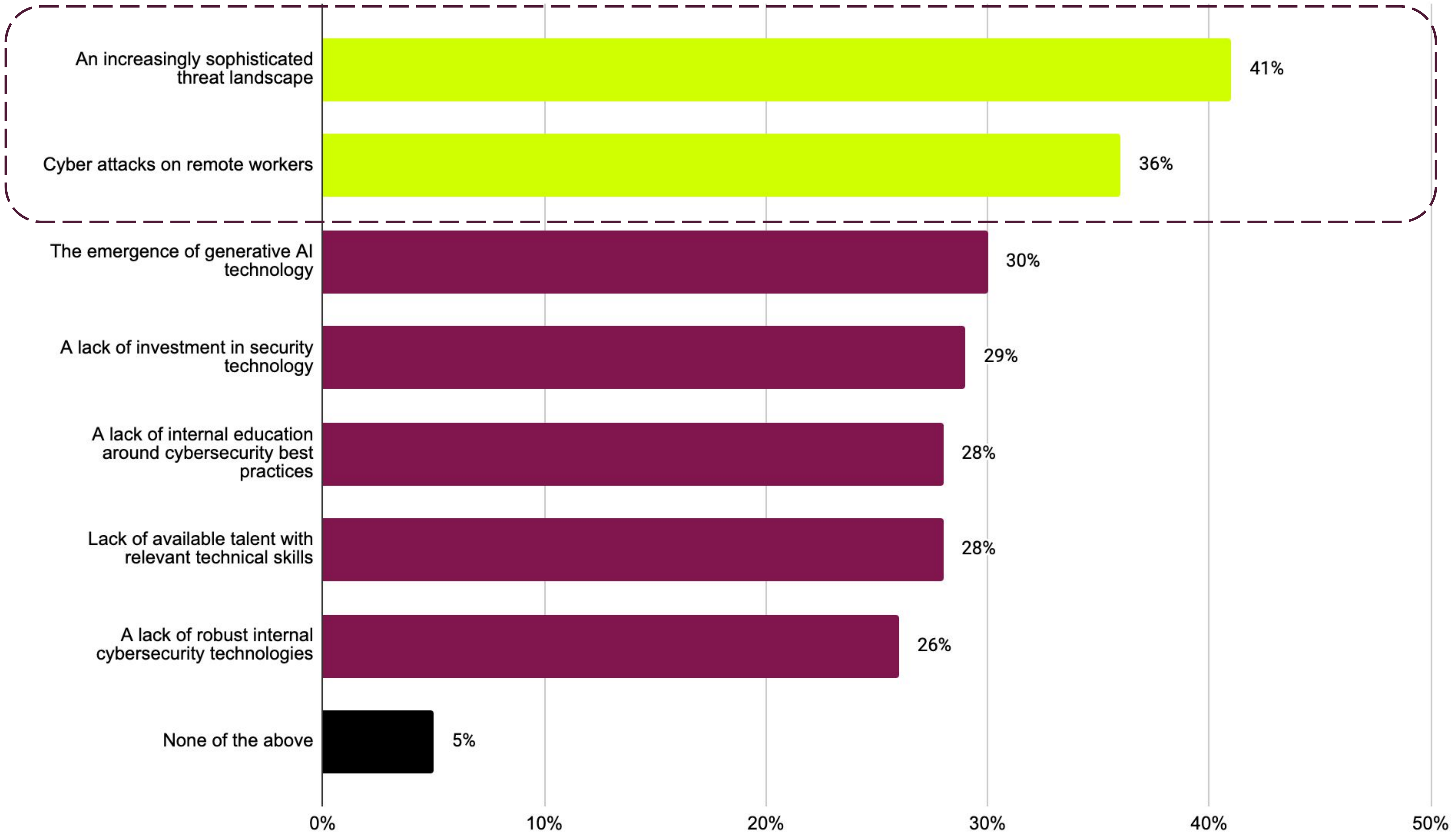
Data breaches and data loss (42%), identity-based threats (37%), and lack of relevant technical skills to counter cybersecurity threats (32%), are viewed as the biggest cybersecurity threats to organisations over the next 12 months



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

Base: 211

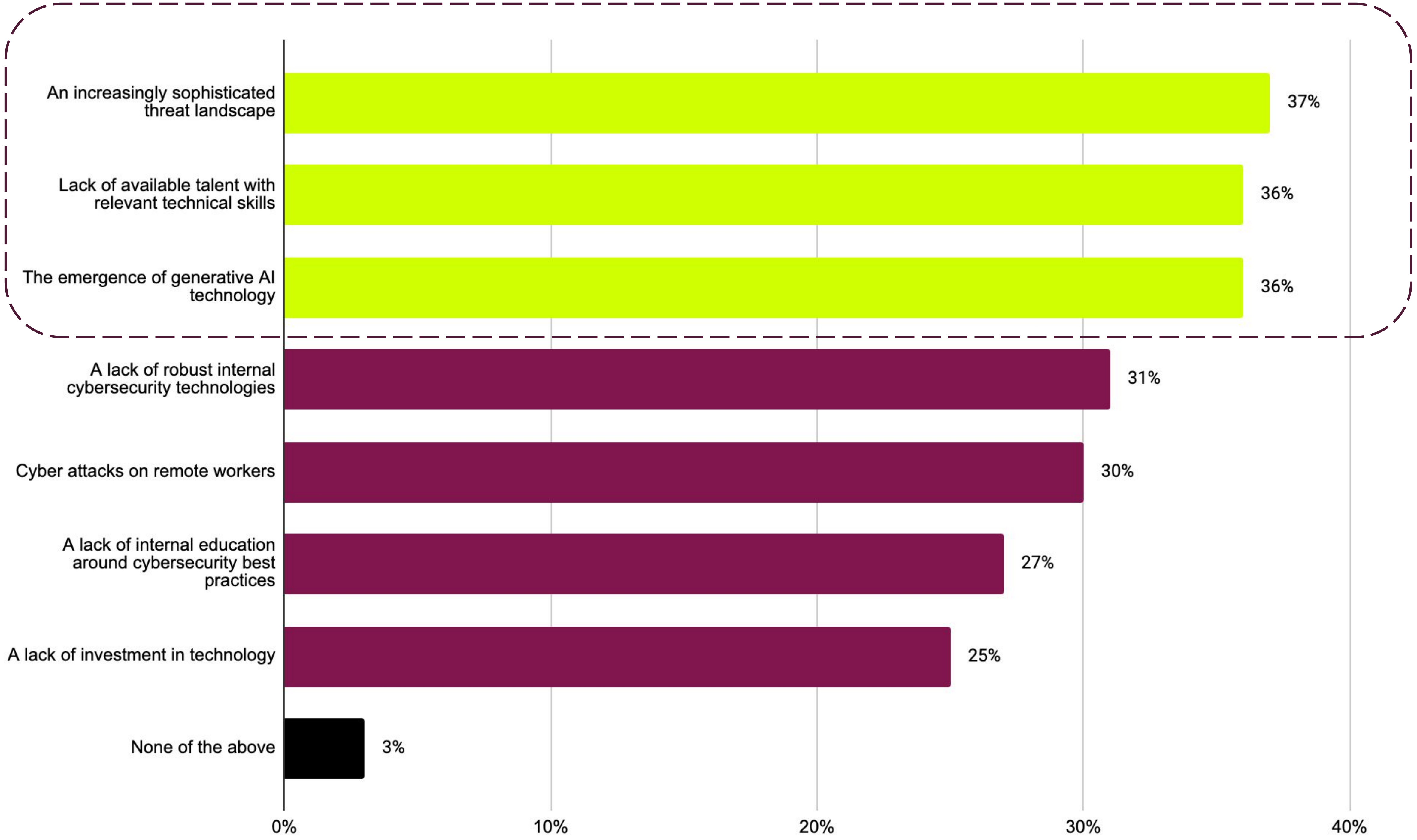
Over the last 12 months, an increasingly sophisticated threat landscape (41%) and cyber attacks on remote workers (36%) were the main drivers of cybersecurity threats



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

Base: 211

Over the next 12 months, an increasingly sophisticated threat landscape (37%), lack of talent and the emergence of generative AI technology (both 36%) are predicted to be the main drivers of cybersecurity threats

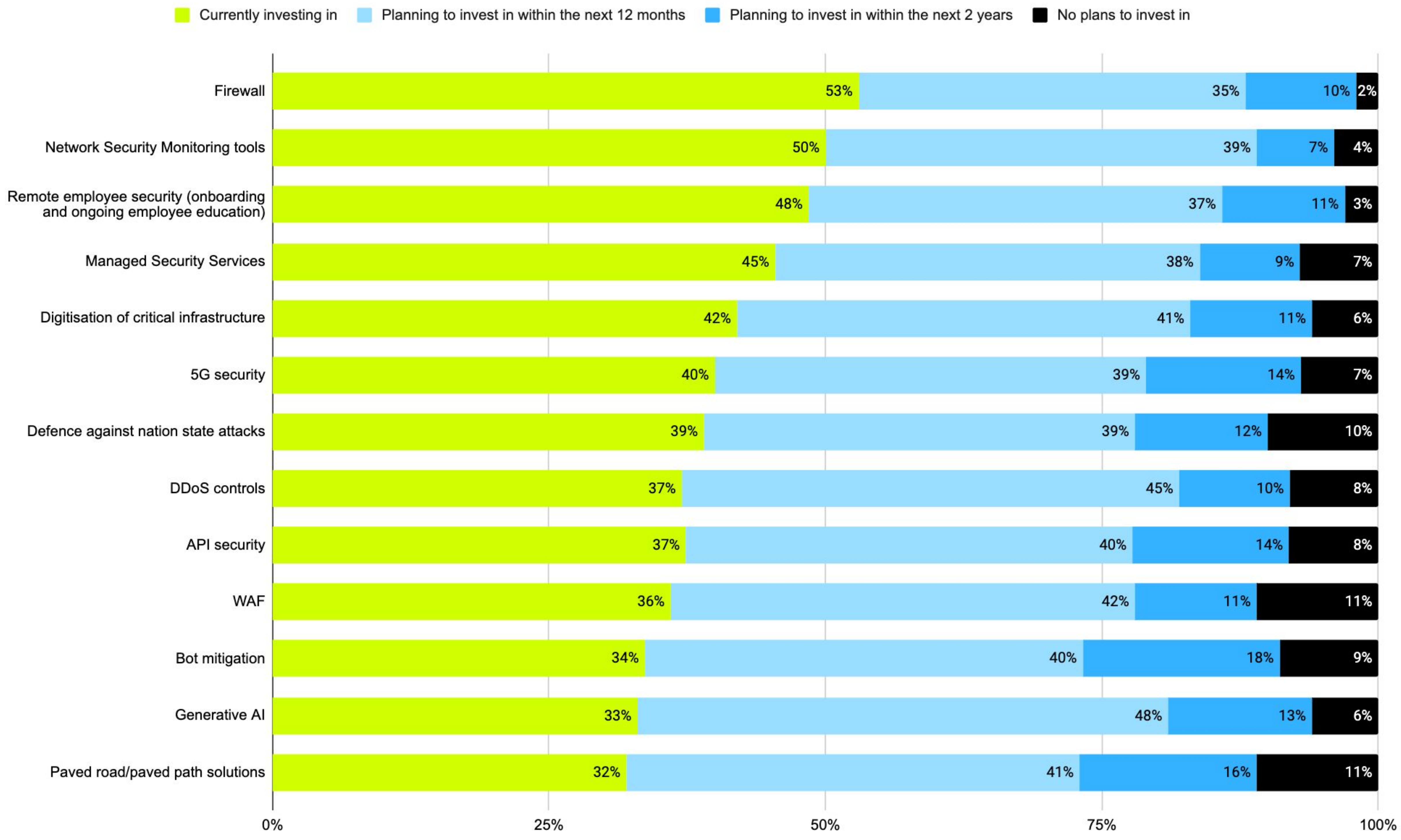


Q2b. Which of the following do you predict will drive cybersecurity threats to your business over the next 12 months? Select top three

Base: 211

53% are currently investing in ‘Firewall’ technology, and around half are investing in ‘Network Security Monitoring tools’ (50%) and ‘Remote employee security’ (48%)

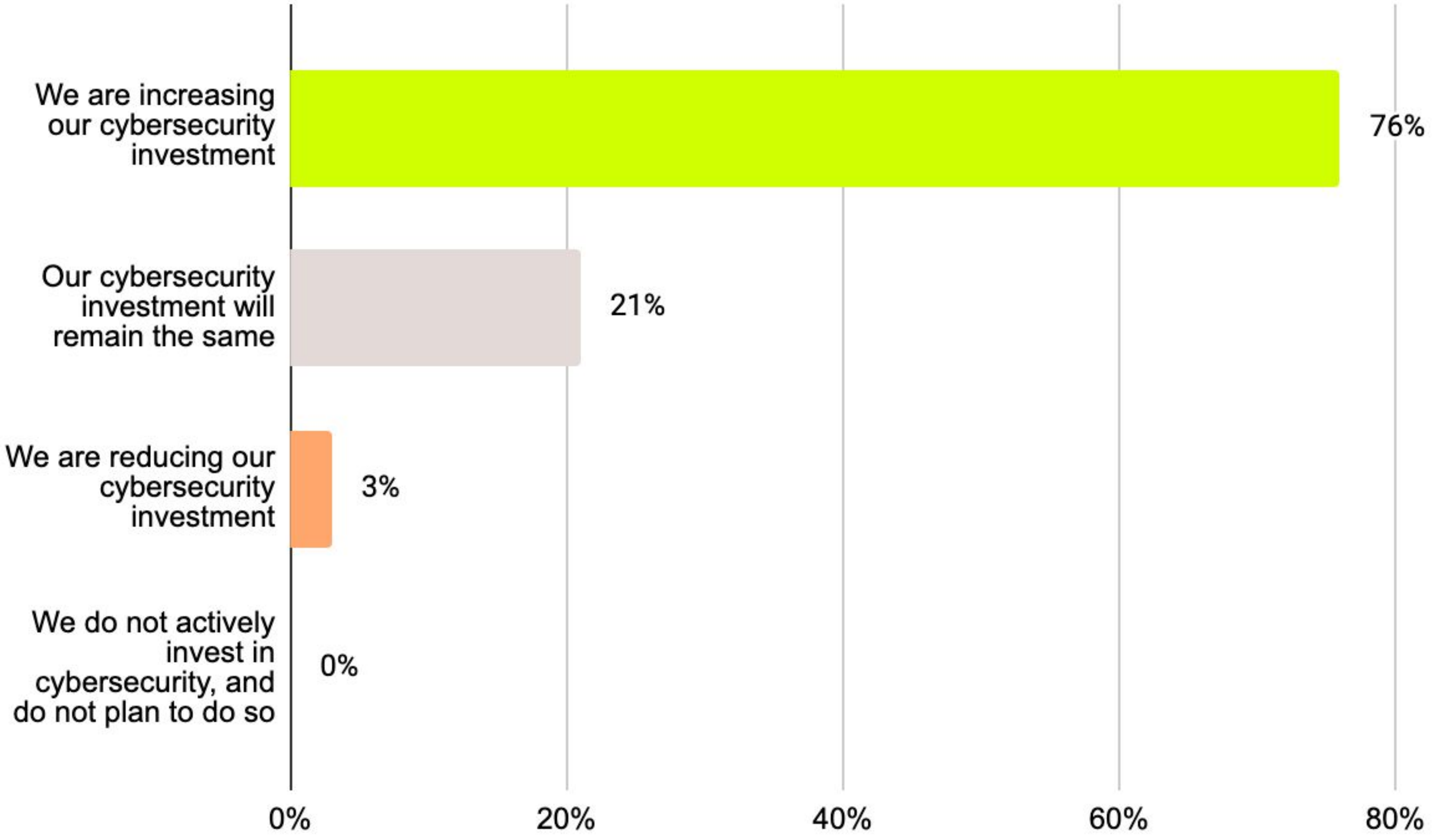
11% have no plans to invest in paved road/ paved path solutions or WAF



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

Base: 211

76% of respondents are increasing their cybersecurity investment

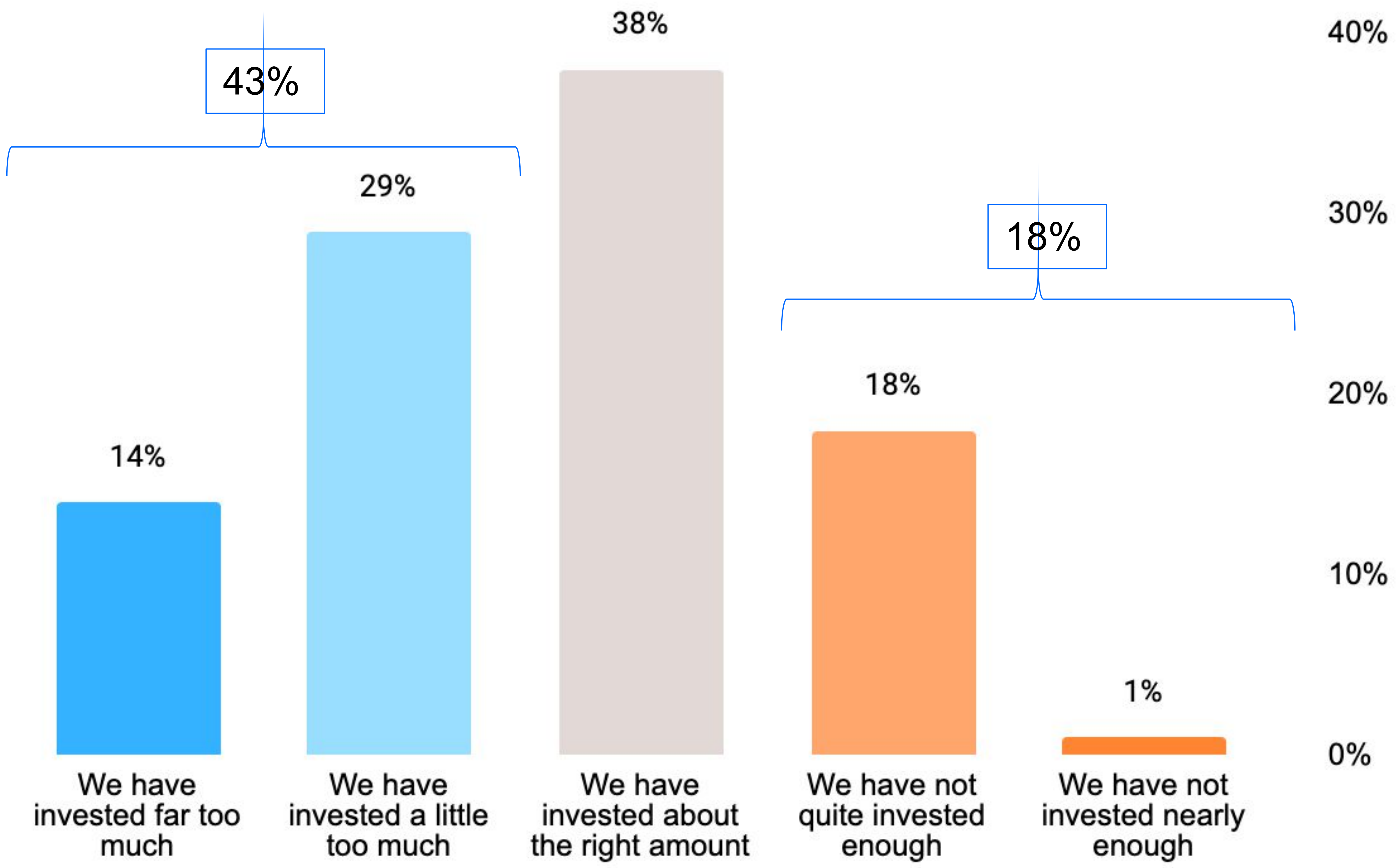


Q4a. When it comes to investment, which of the following best describes how your organisation is preparing for future cybersecurity risk over the next 12 months? Select one

Base: 211

43% of respondents have invested too much into cybersecurity over the past 12 months

18% say they have not invested enough

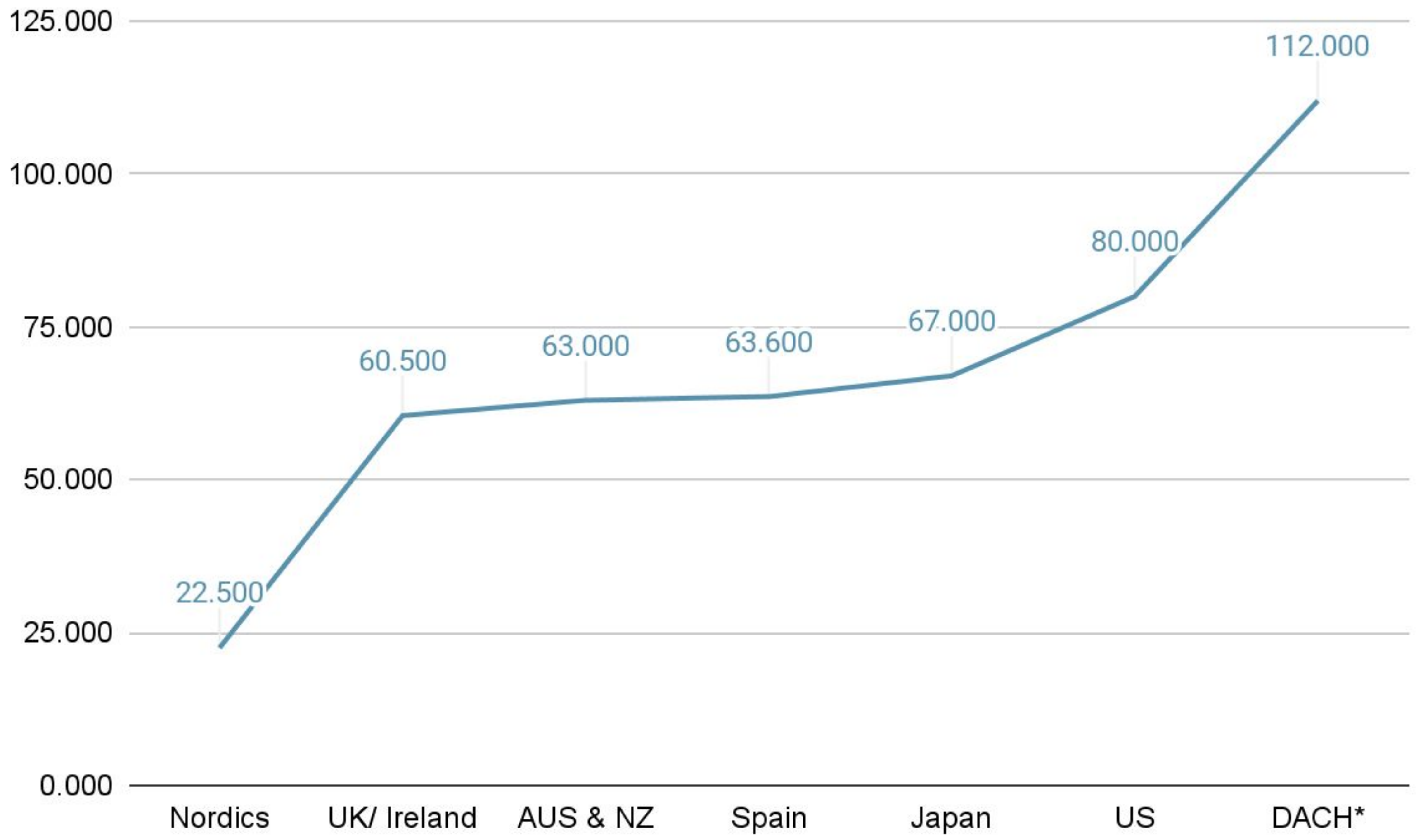


*only asked to those who invest in cybersecurity

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: 211*

On average (median), $63,000 USD are spent per year on web application and API security control/tools in Australia and New Zealand



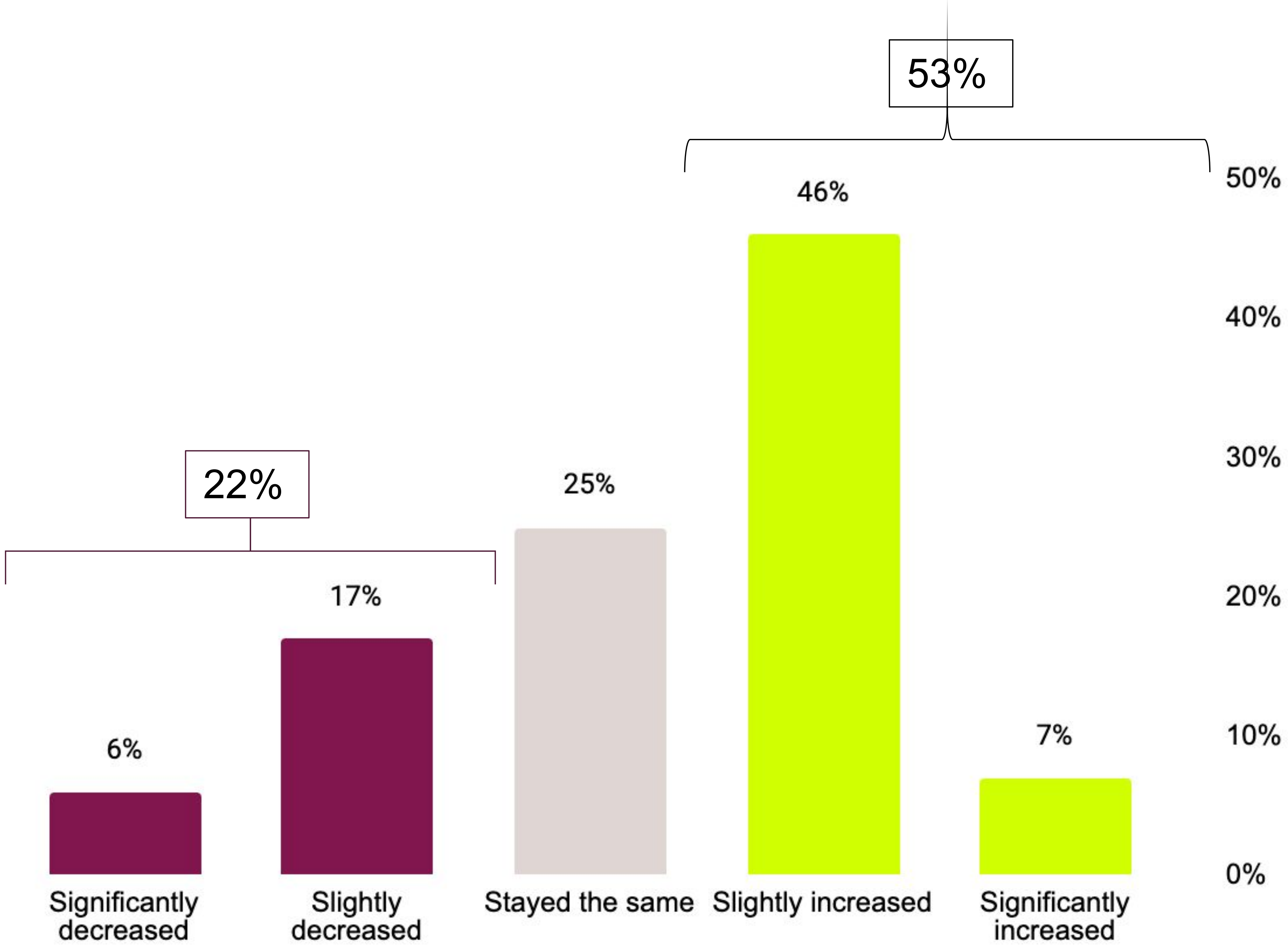
*The sample for DACH countries had a larger proportion of companies with more than 75,000+ employees

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

53% of respondents have increased talent spending, with only 22% having decreased talent spending

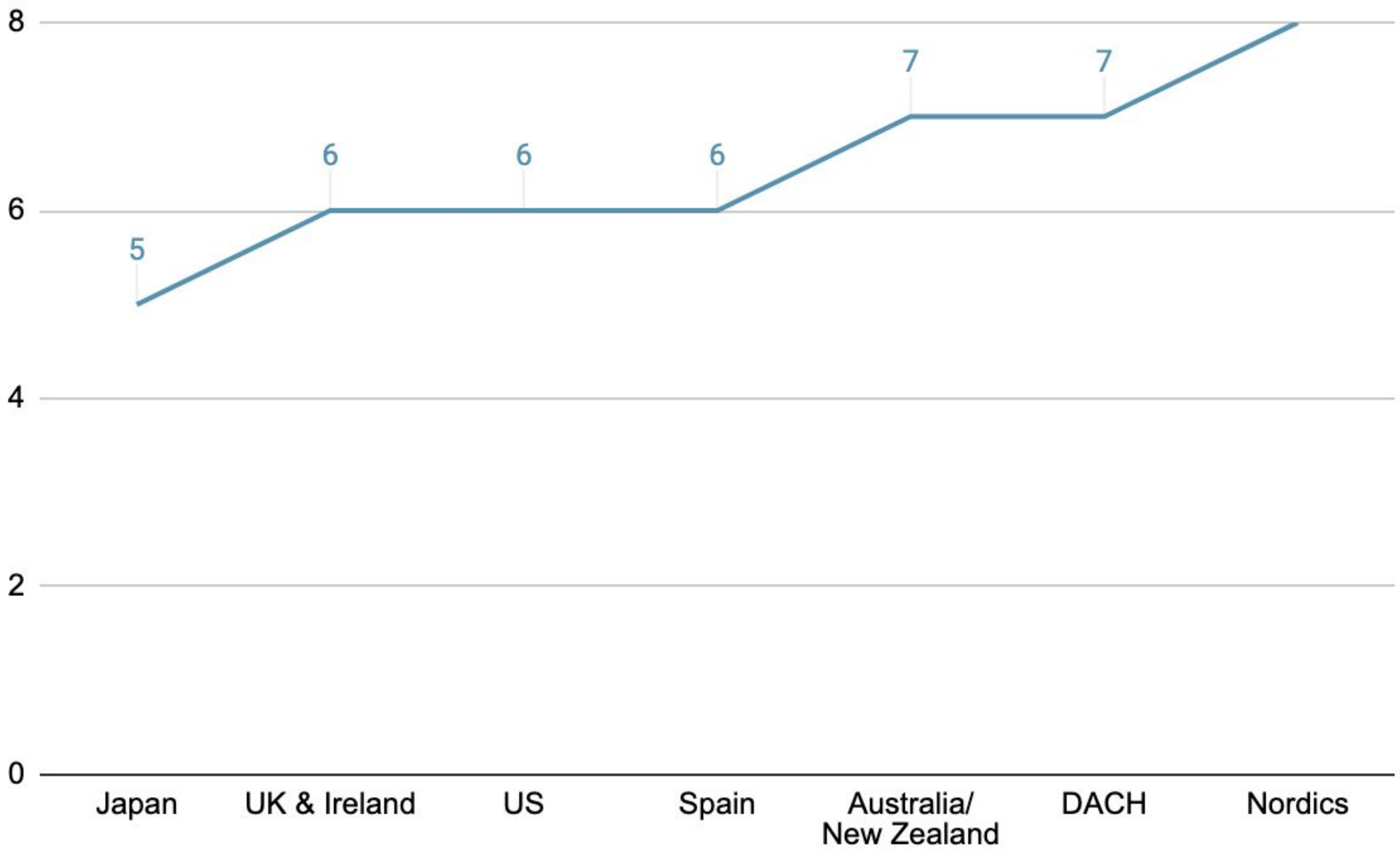


Q5b. How has your talent spending (e.g. new hires, wages) for cybersecurity changed, if at all? Select one

Base: 211

On average (median), organisations in Australia and New Zealand rely on 7 network and application cybersecurity solutions

Overall median: 6

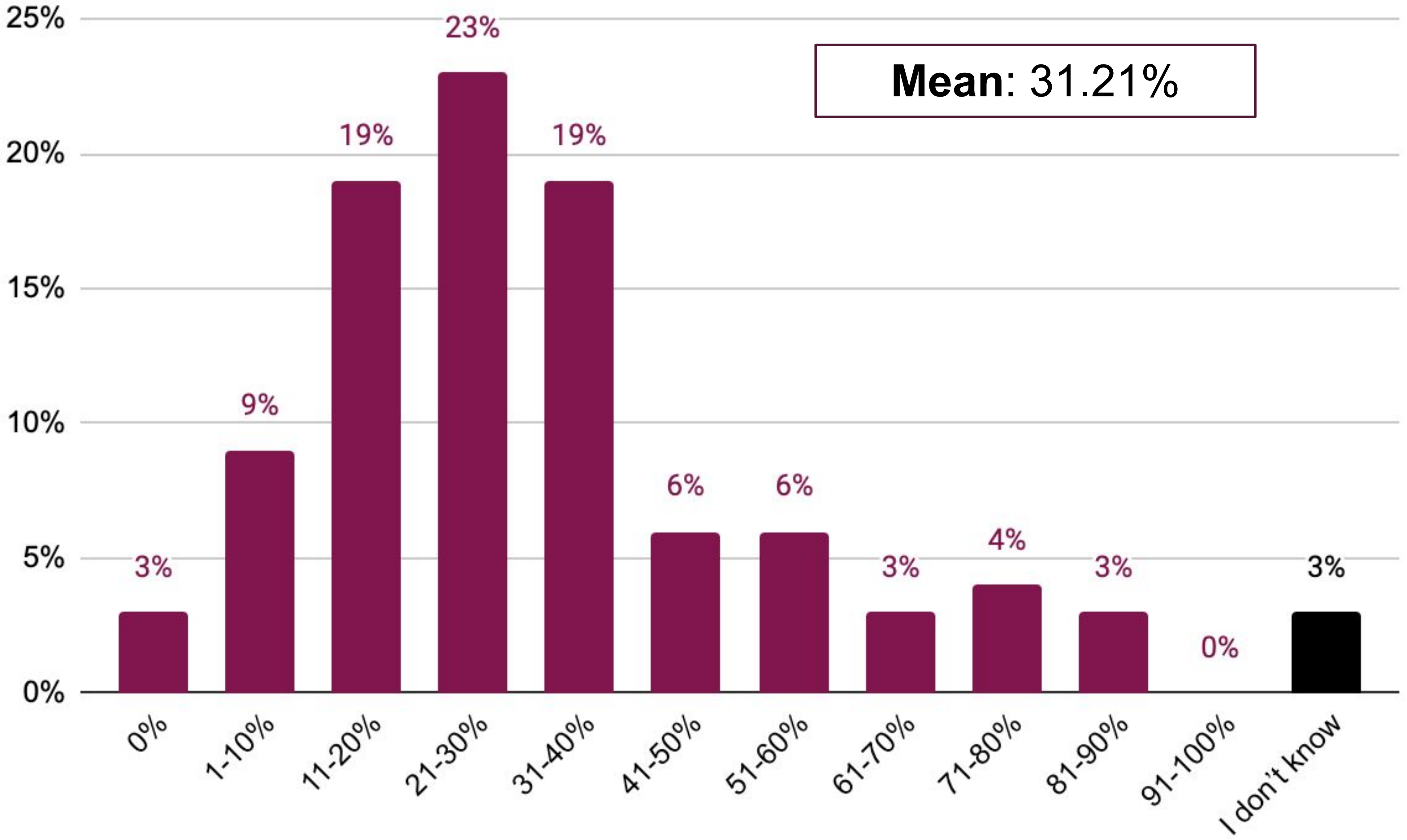


2022 Survey:
Japan **4**
Spain **5**
US **5**
UK & Ireland **6**
AUS & NZ **5**
DACH **5**
Nordics **7**

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

Base: 1484

On average, 31% of network and application cybersecurity solutions overlap

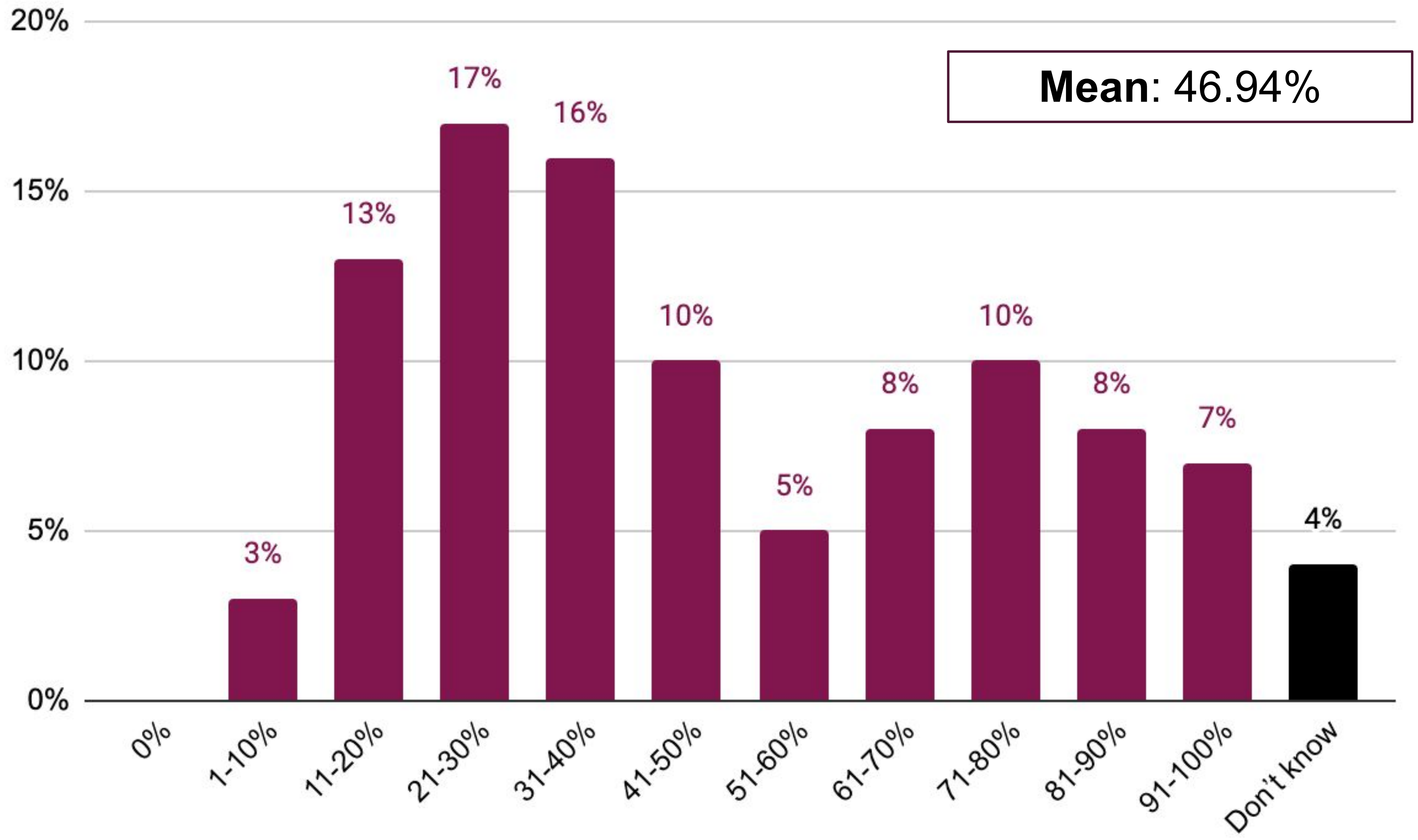


Mean: 31.21%

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

Base: 211

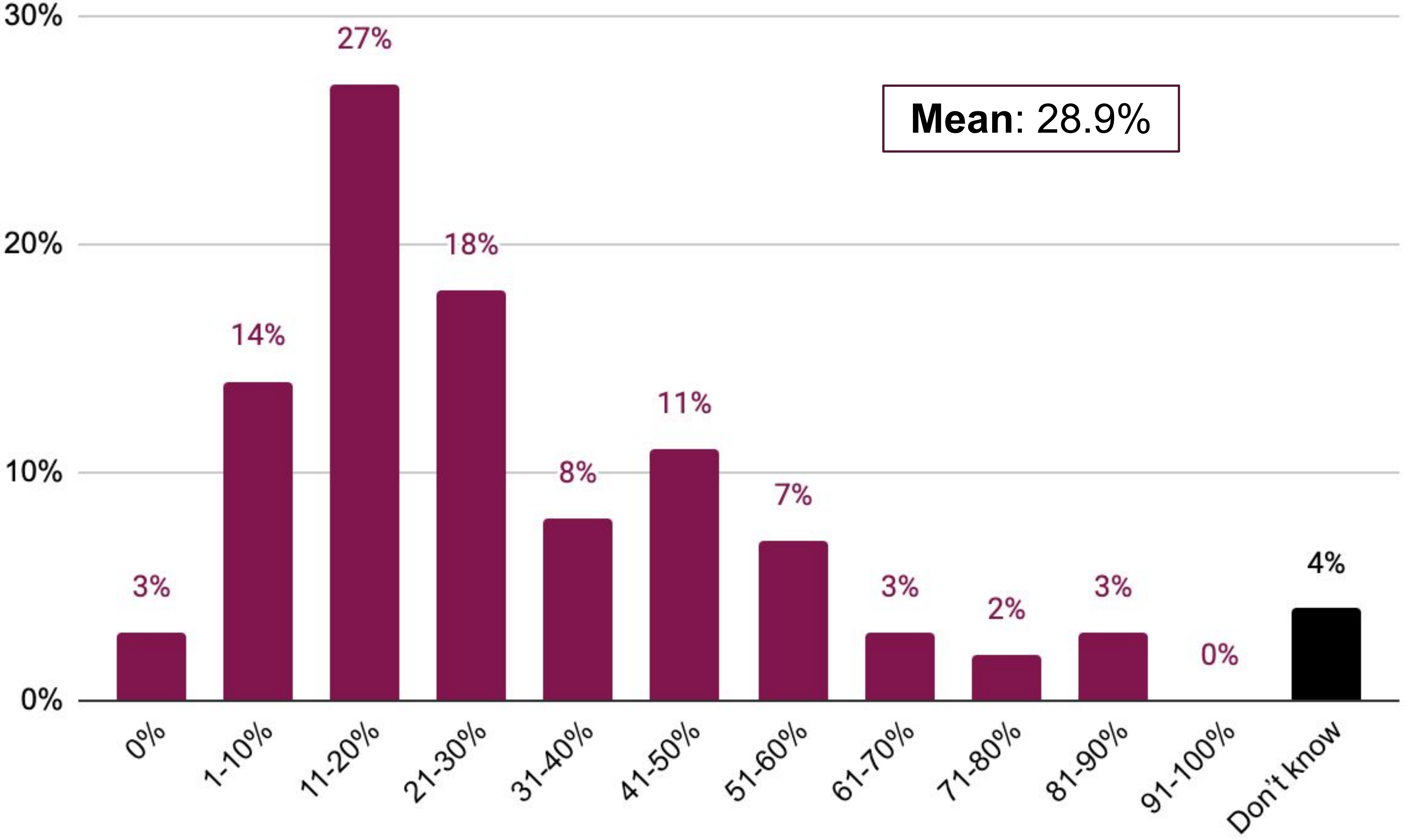
On average, only 47% of cybersecurity tools are fully active / deployed



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

Base: 211

On average, 29% of security alerts detected by an organisations WAF are false alerts

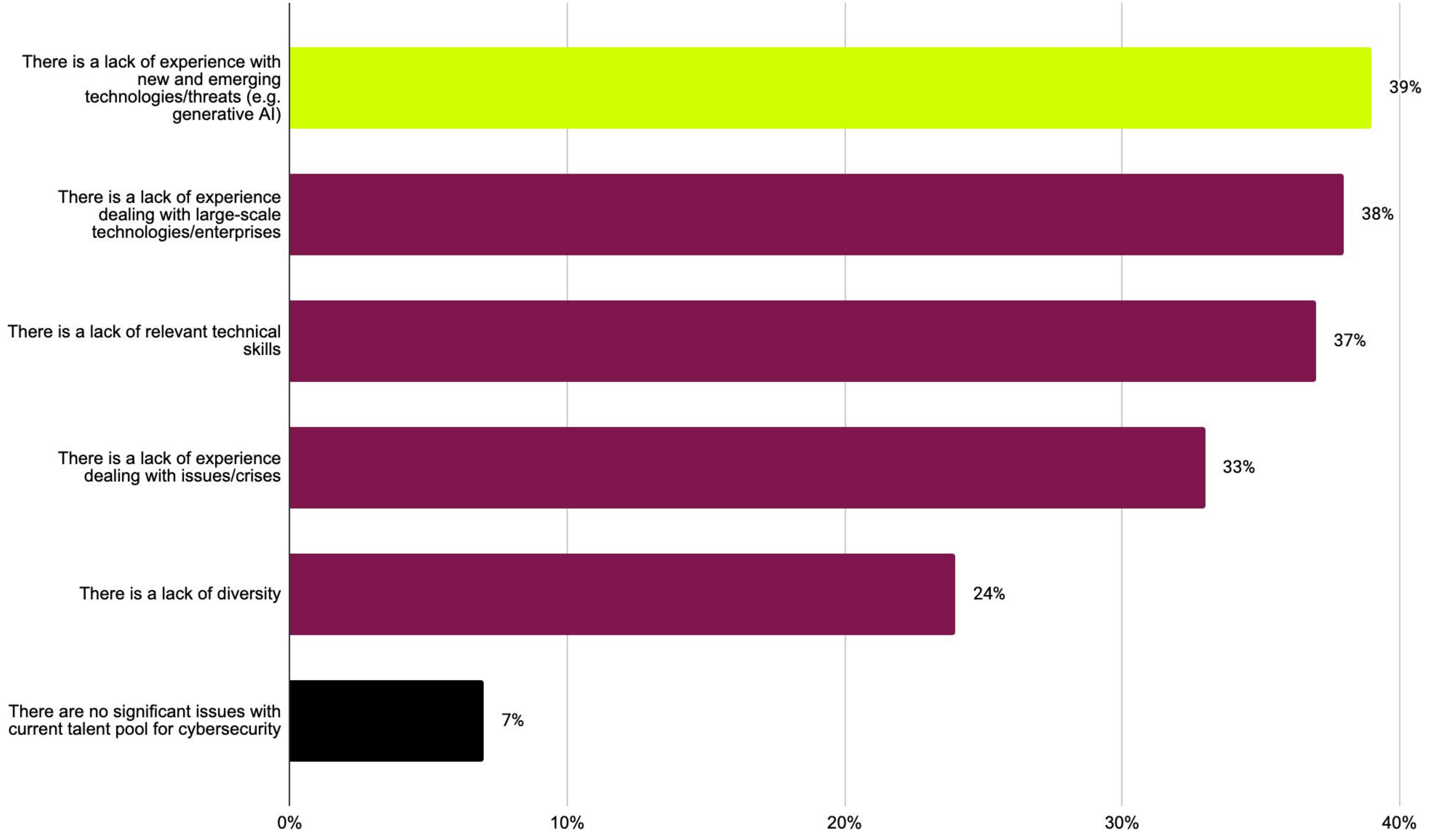


Mean: 28.9%

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

Base: 211

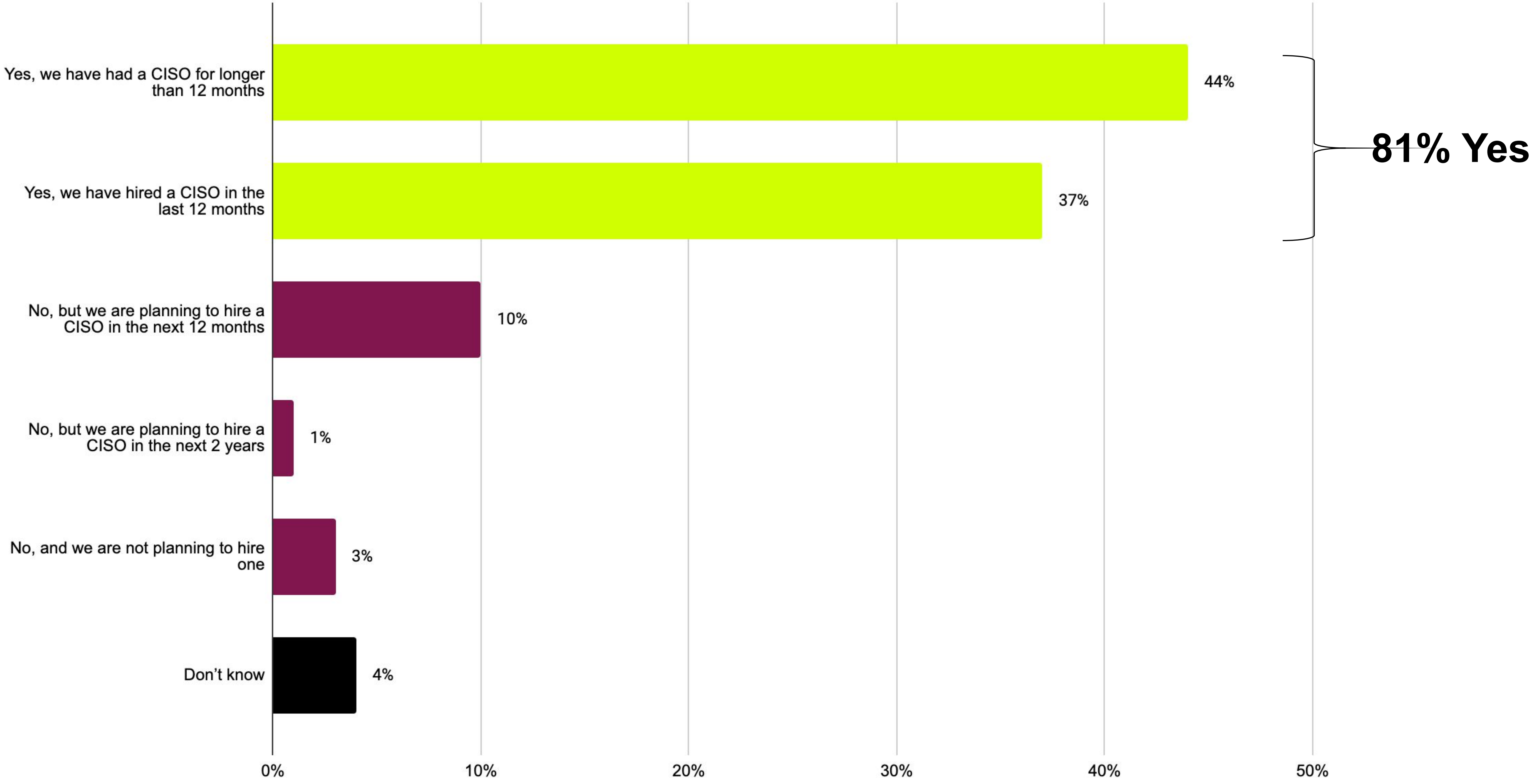
Respondents feel that the biggest gap among the current talent pool is experience with new and emerging technologies / threats such as generative AI (39%)



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

Base: 211

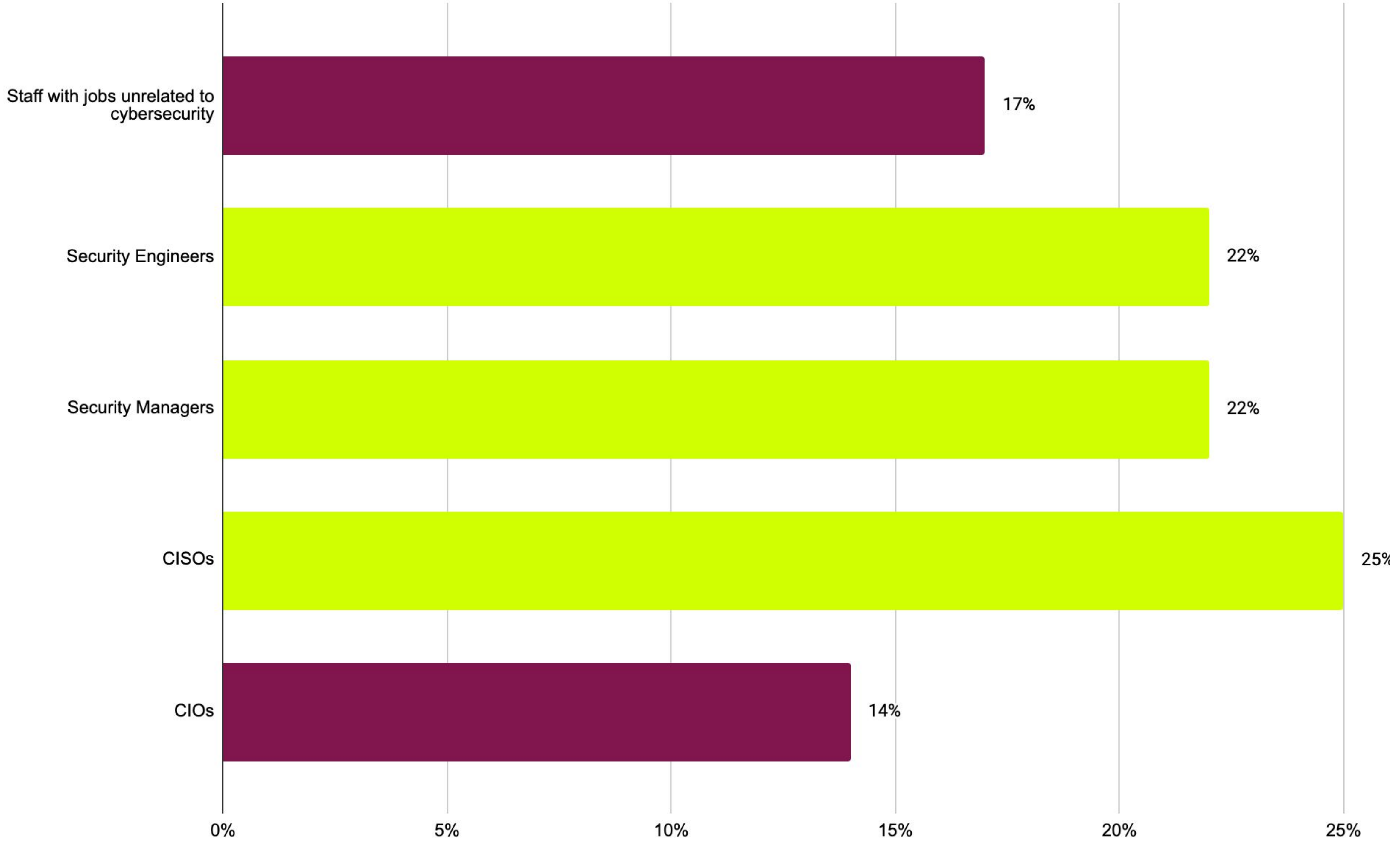
81% of respondents have hired a CISO, 37% of those within the last 12 months



Q10. Does your organisation have a CISO? Select one

Base: 211

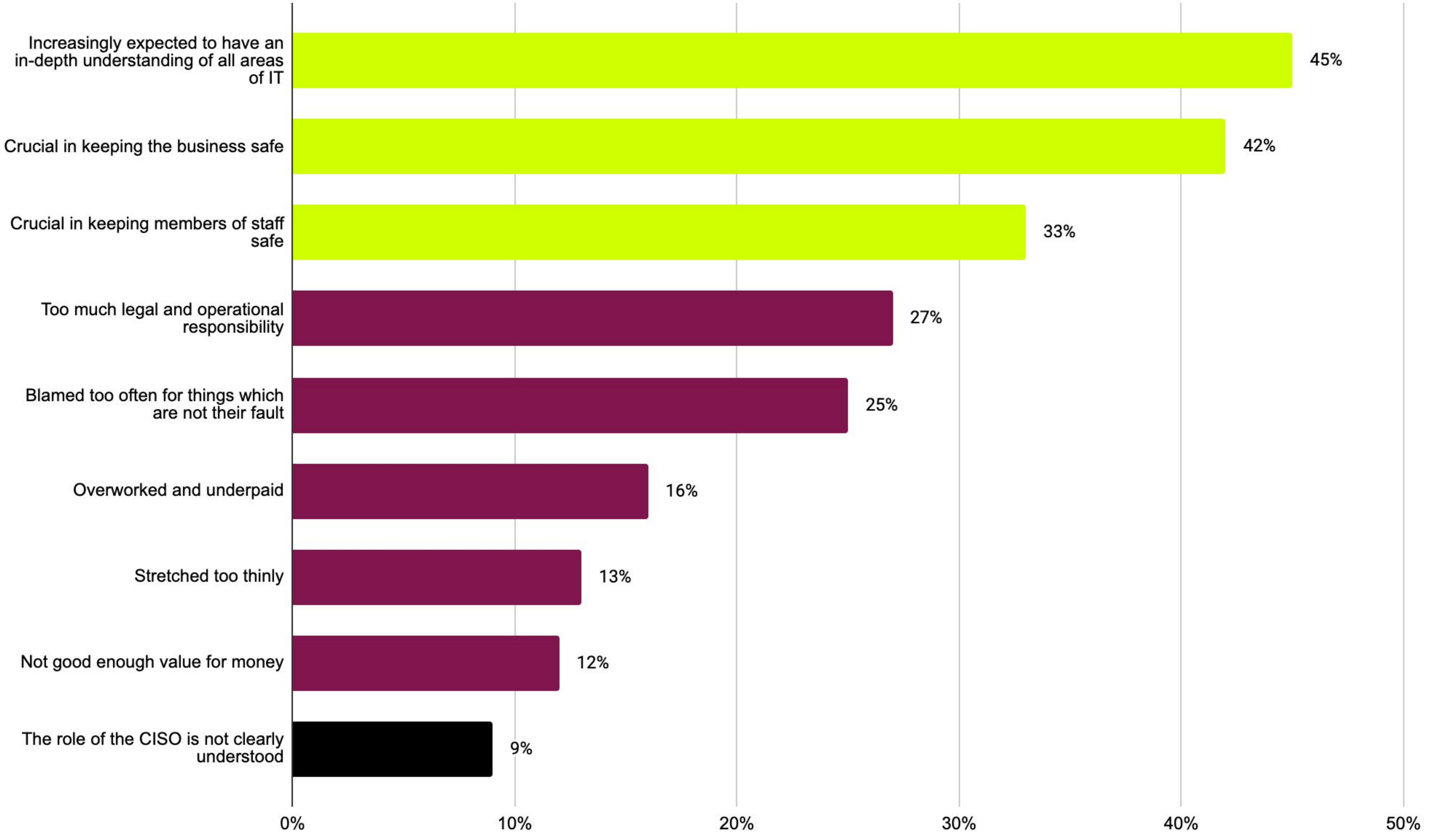
25% of respondents think CISOs are often held responsible for cybersecurity incidents, 22% think security managers and security engineers are often held responsible



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

Base: 211

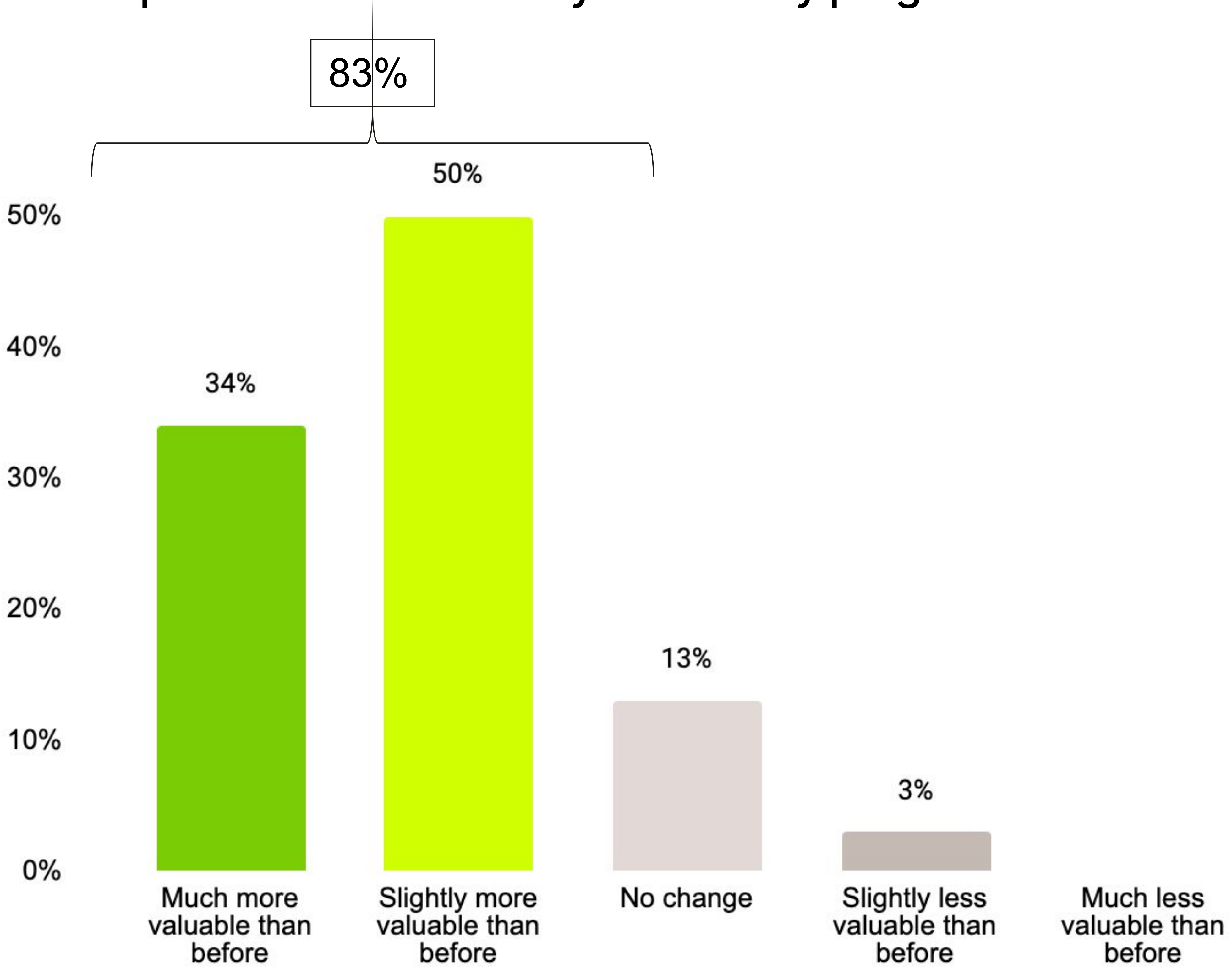
CISOs are viewed as having an in-depth understanding of all areas of IT (45%), crucial in keeping the business safe (42%), and crucial in keeping members of staff safe (33%)



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

Base: 211

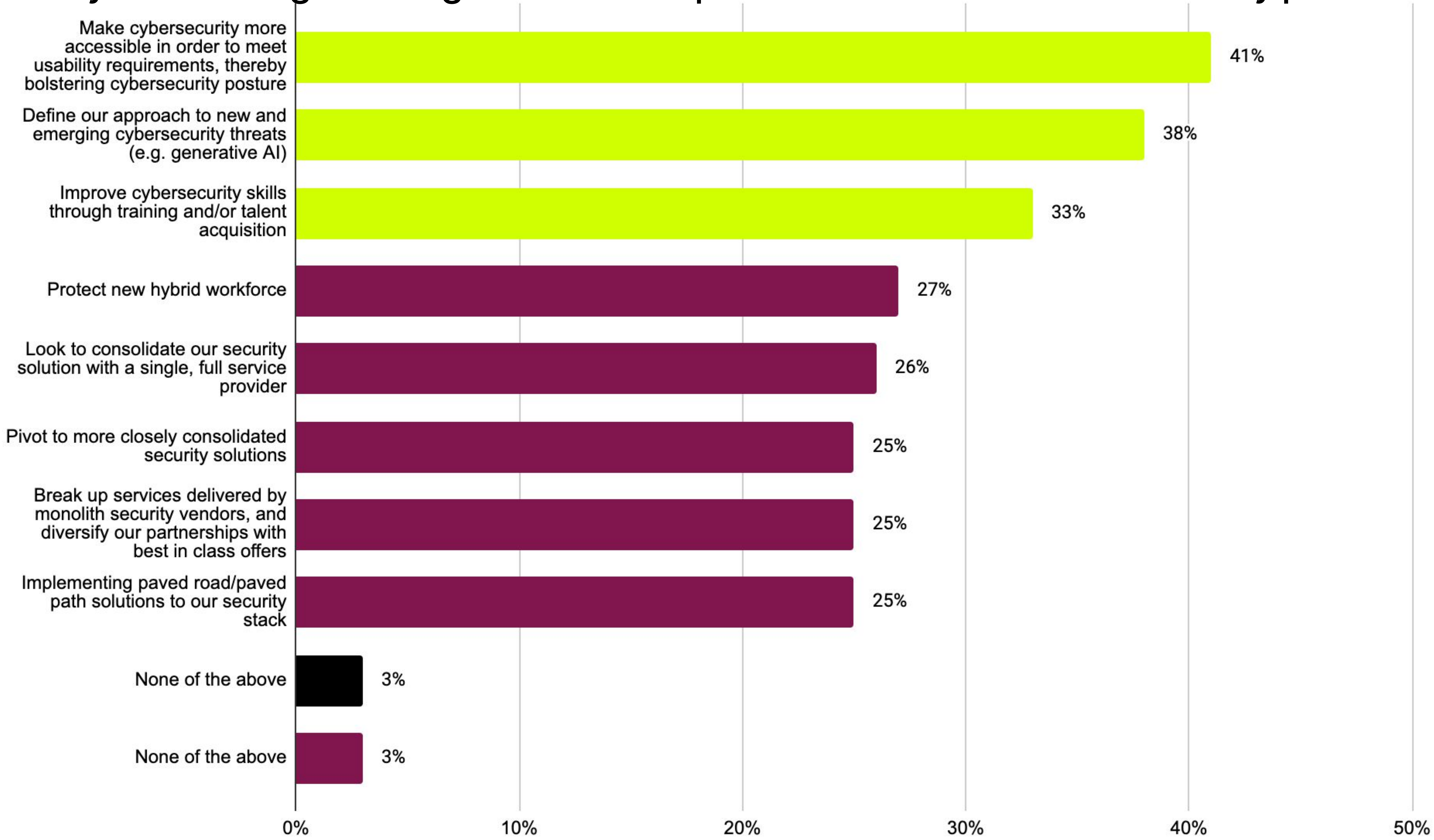
83% of respondents think their cybersecurity programme has become more valuable over the last 12 months



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: 211

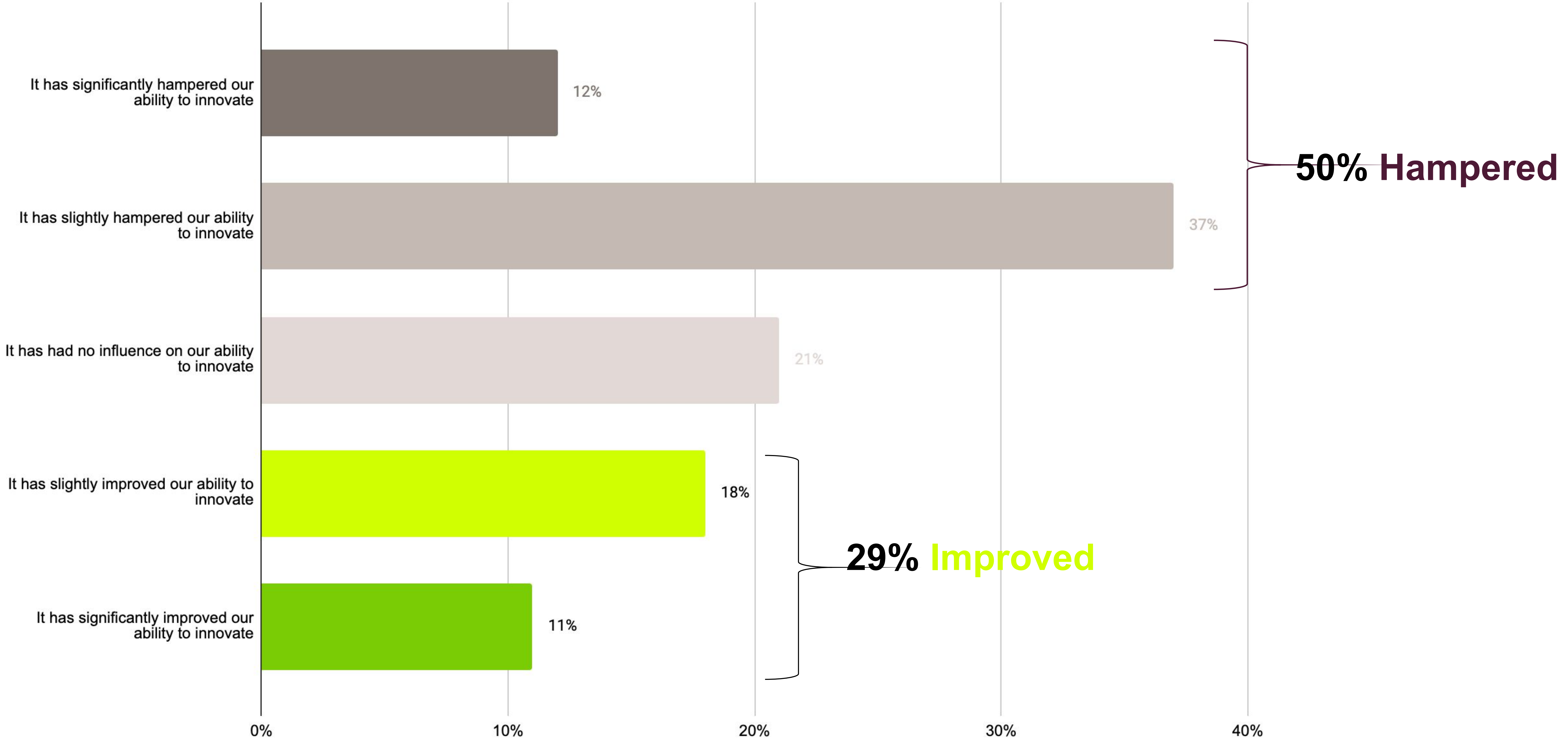
Making cyber security more accessible (41%), defining approaches to new threats (38%), and improving cyber security skills through training and talent acquisition (33%) are the main security priorities over the next year



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

Base: 211

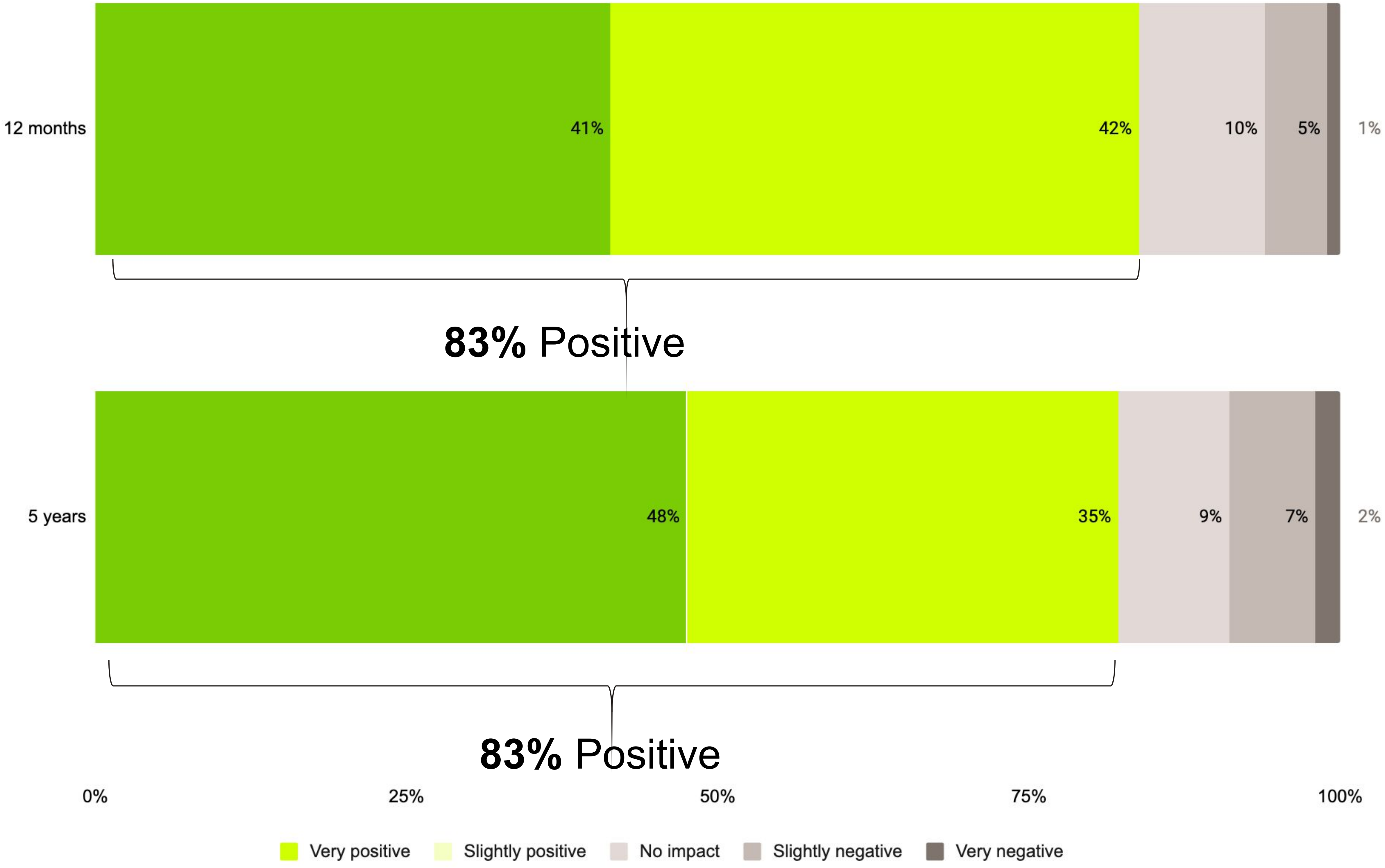
50% say that their organisations cybersecurity strategy has hampered business innovation
Only 29% say it has improved innovation



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

Base: 211

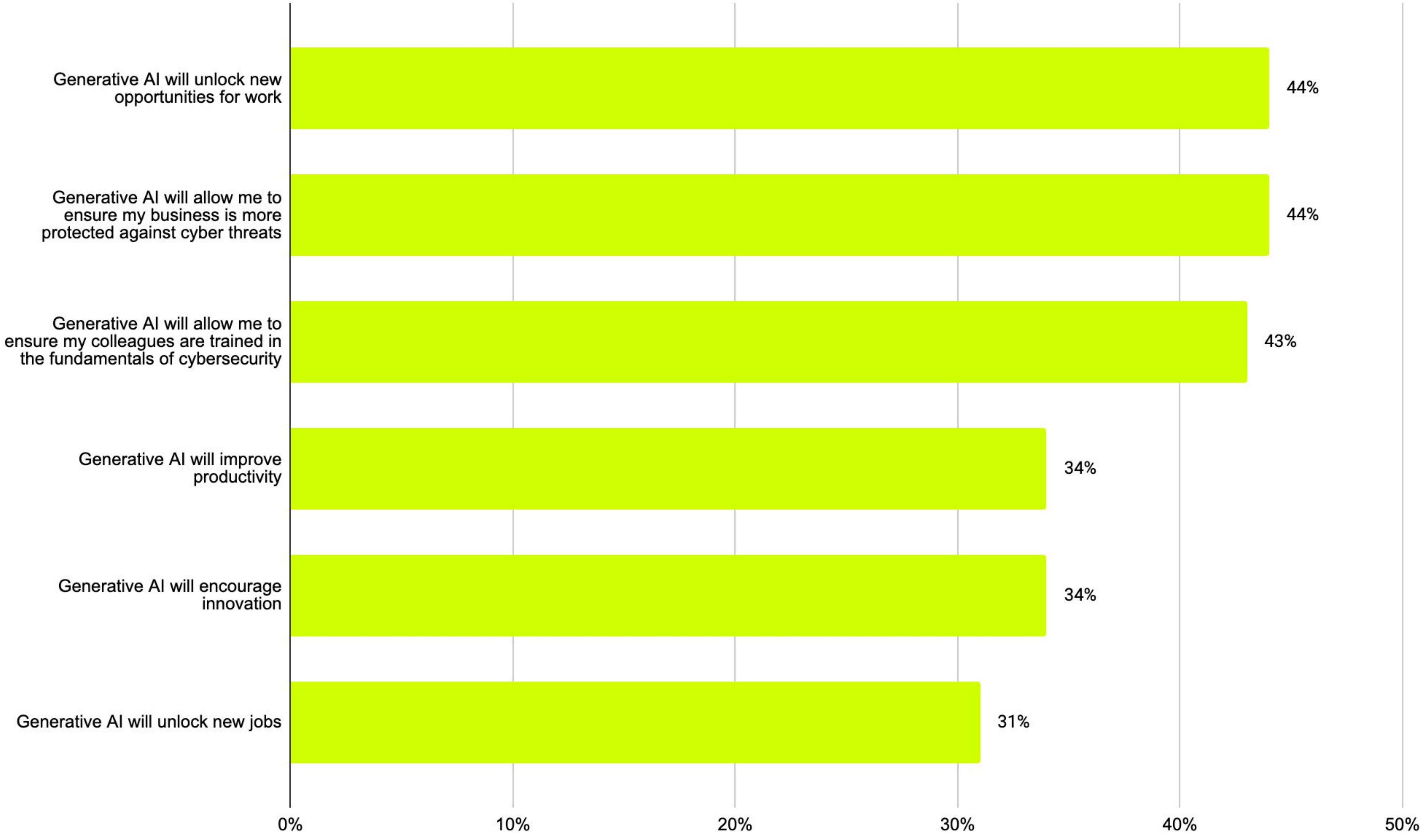
83% predict that Generative AI will have a positive impact on cybersecurity over the next 12 months
83% predict it will have a positive impact over the next 5 years



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

Base: 211

Unlocking opportunities and ensuring businesses are more protected against cyber threats (both 44%), followed by ensuring colleagues are trained in cybersecurity fundamentals (43%) are the forecasted positive impacts of generative AI

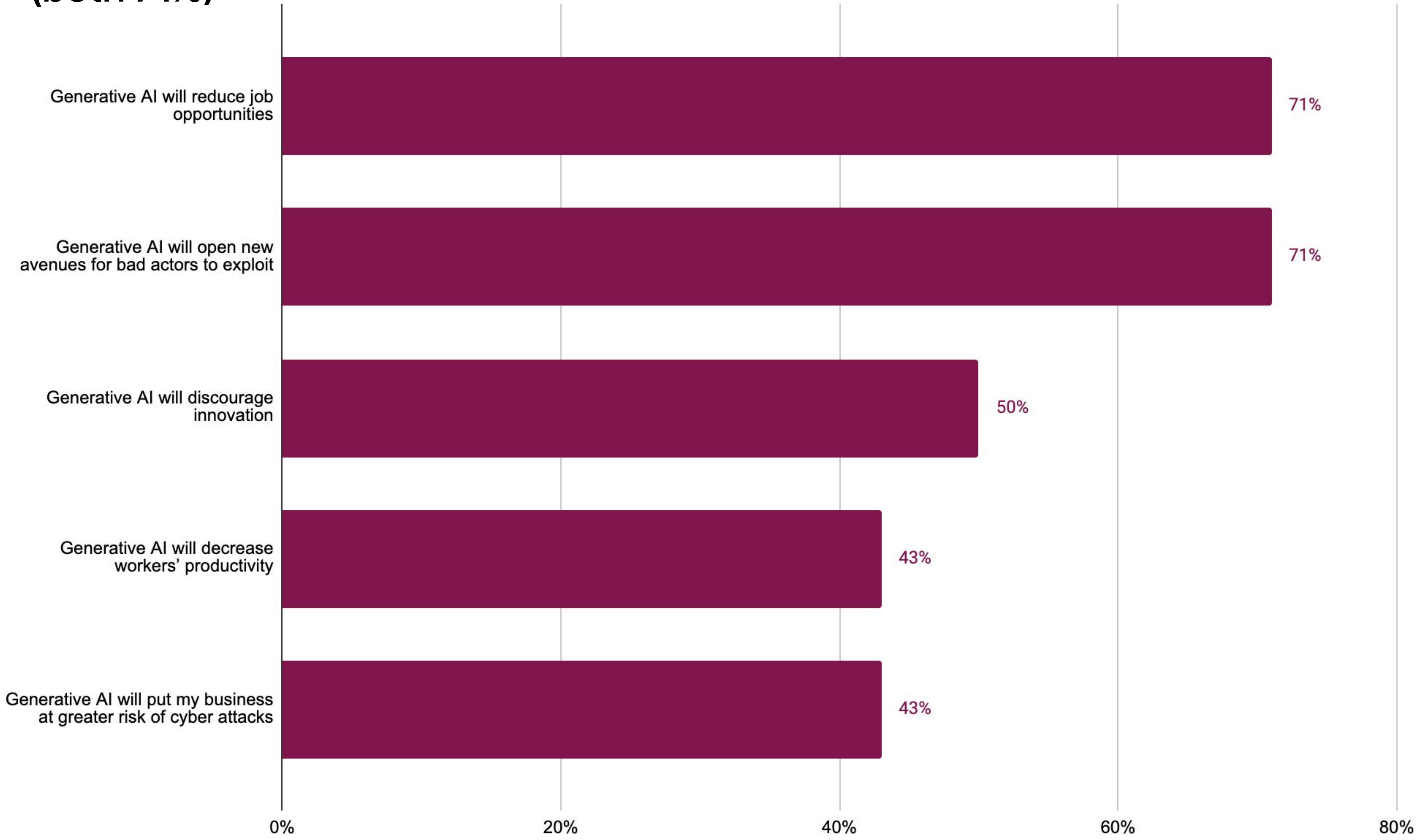


*only asked to those who said generative AI will have a positive impact in the next 12 months

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

Base : 176*

There are fears that Generative AI will reduce job opportunities and open new avenues for bad actors to exploit (both 71%)

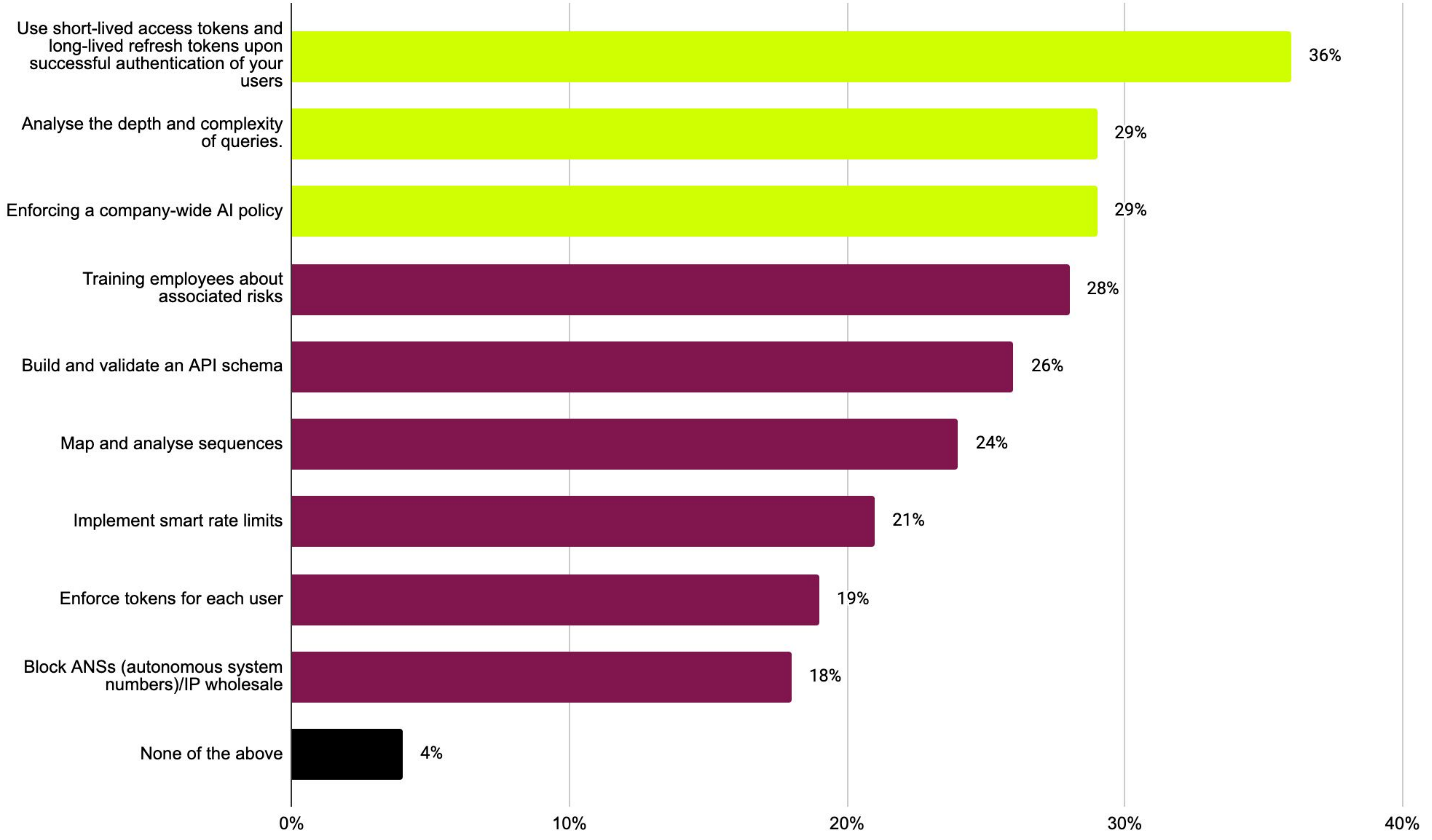


*only asked to those who said generative AI will have a negative impact in the next 12 months

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

Base: 14*

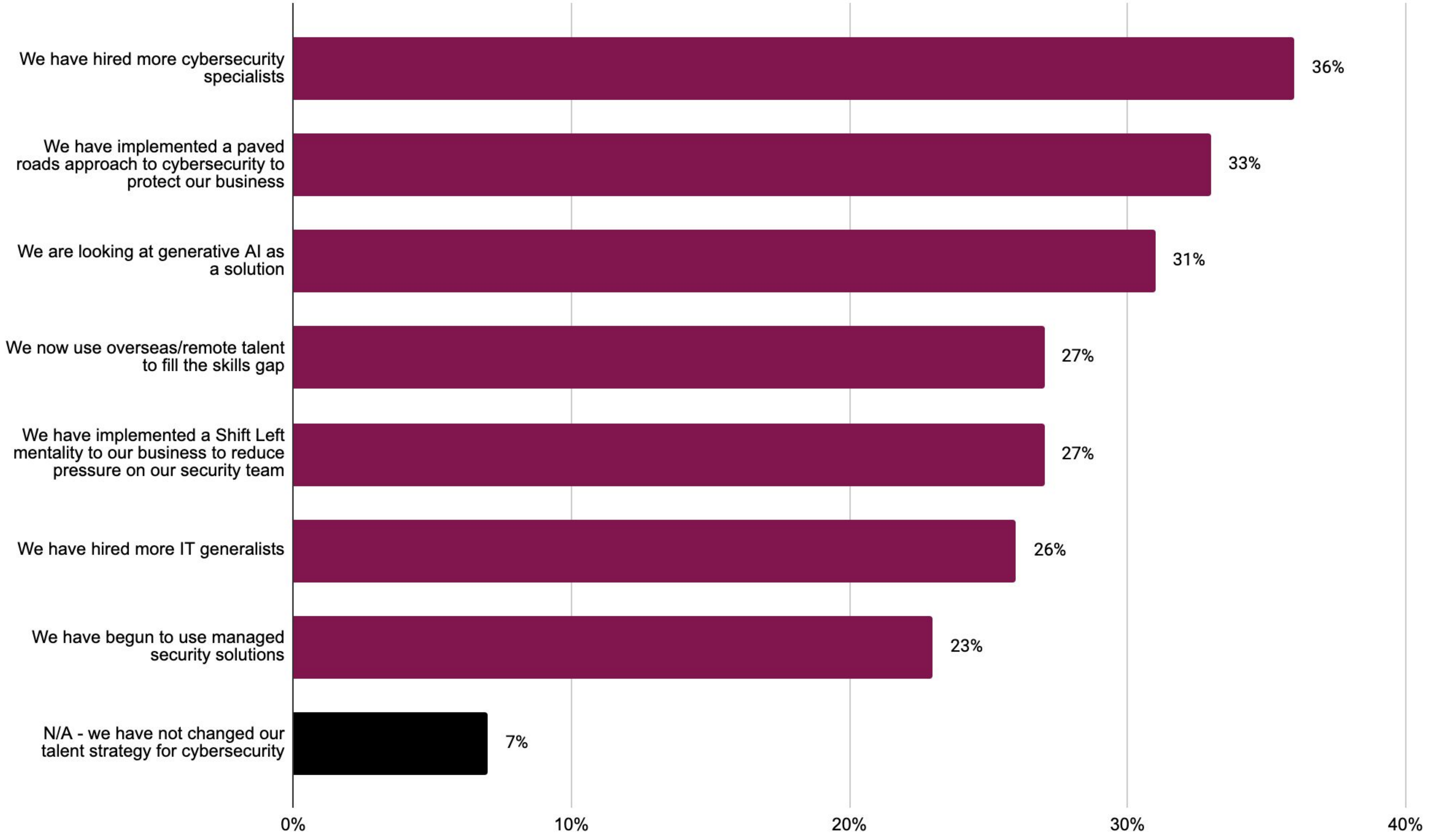
Using short-lived access tokens and long-lived refresh tokens (36%), analysing the depth and complexity of queries (29%) and enforcing a company-wide AI policy (29%) are the top three steps companies are taking to mitigate generative AI security threats



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

Base: 211

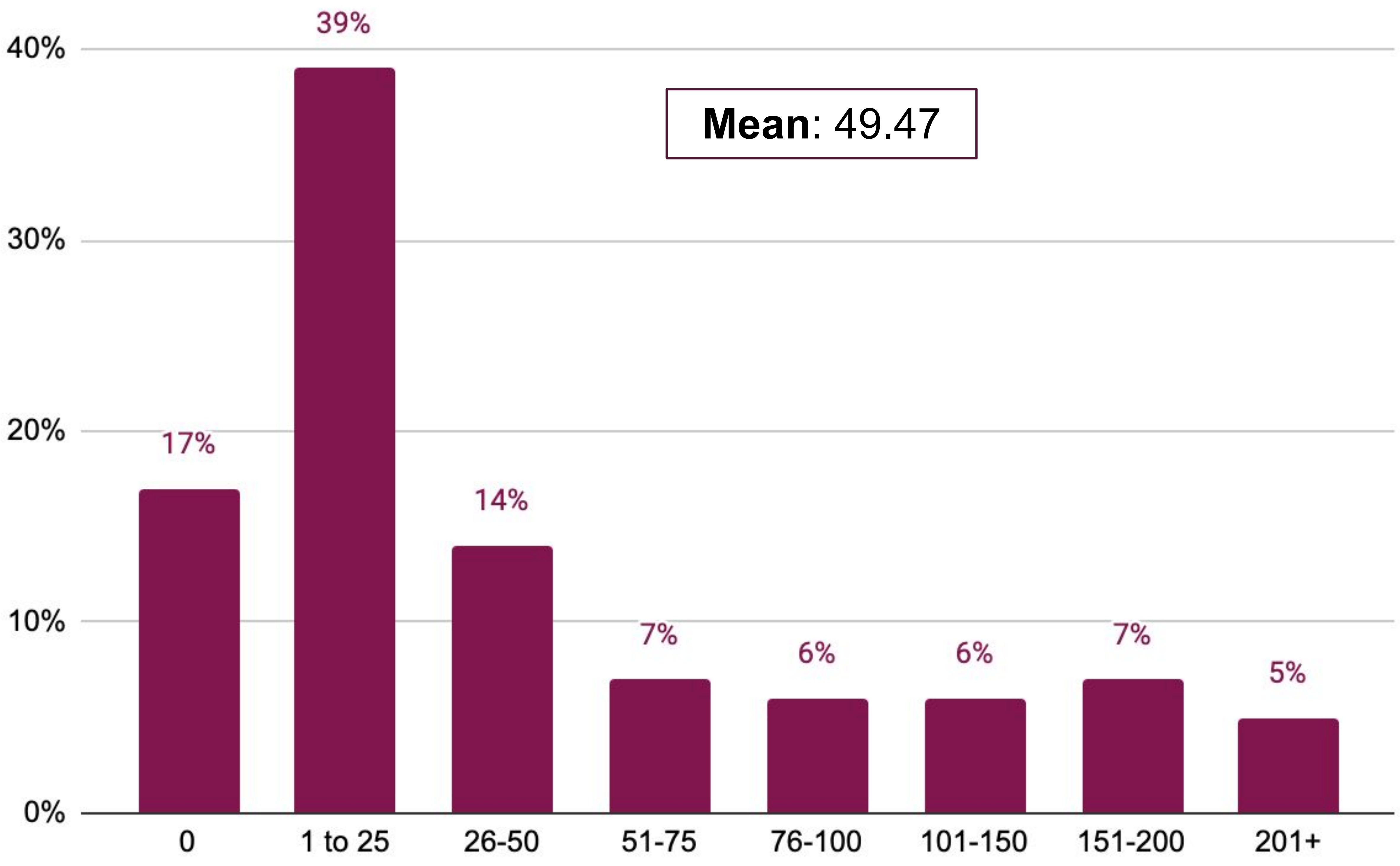
Companies have hired more cybersecurity specialists (36%) and implemented a paved roads approach (33%) over the last 12 months



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

Base: 211

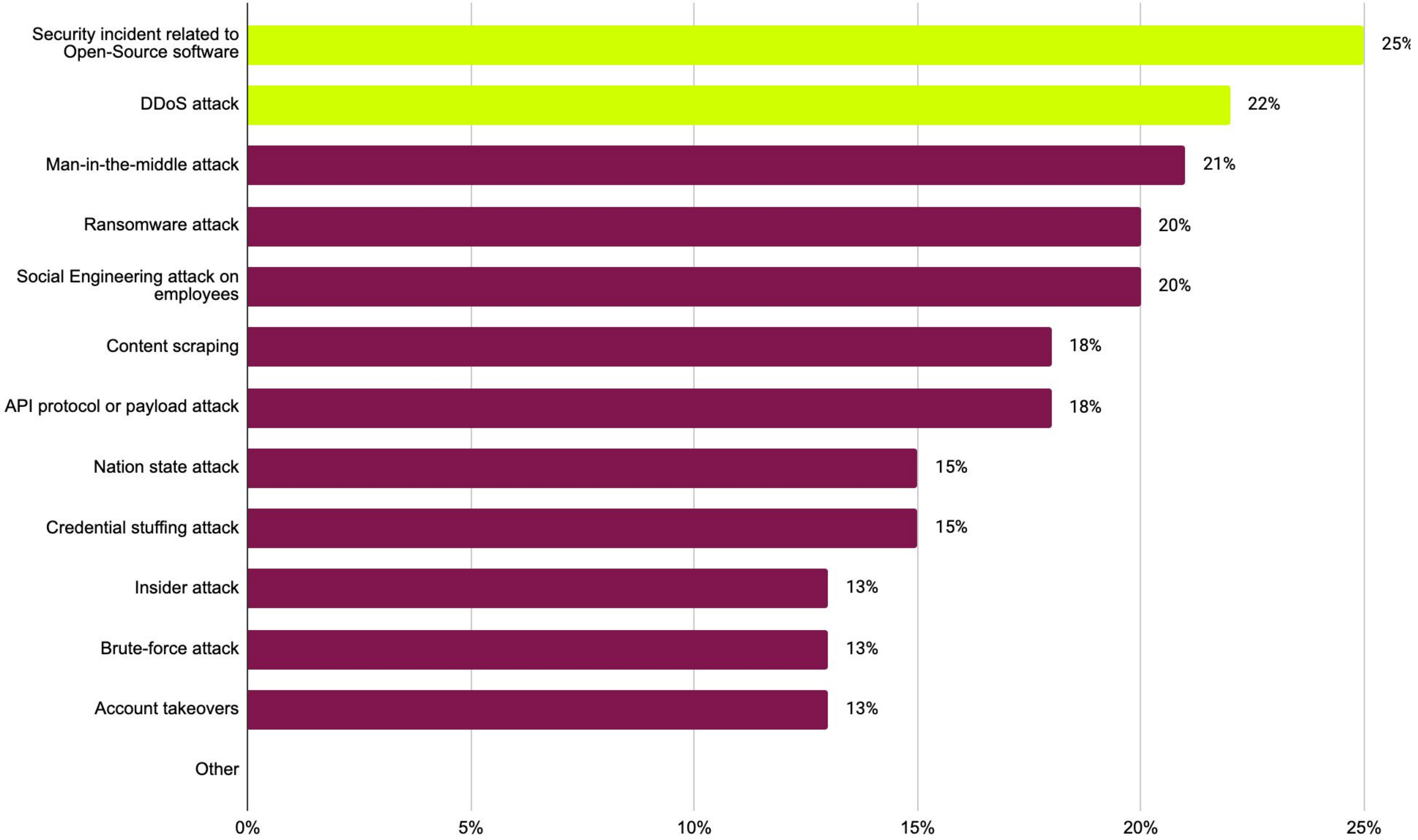
On average, businesses have suffered 49 cyberattacks in the past 12 months



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

Base: 211

The most common types of cyberattacks were security incidents related to Open-Source software (25%) and DDos attacks (22%)

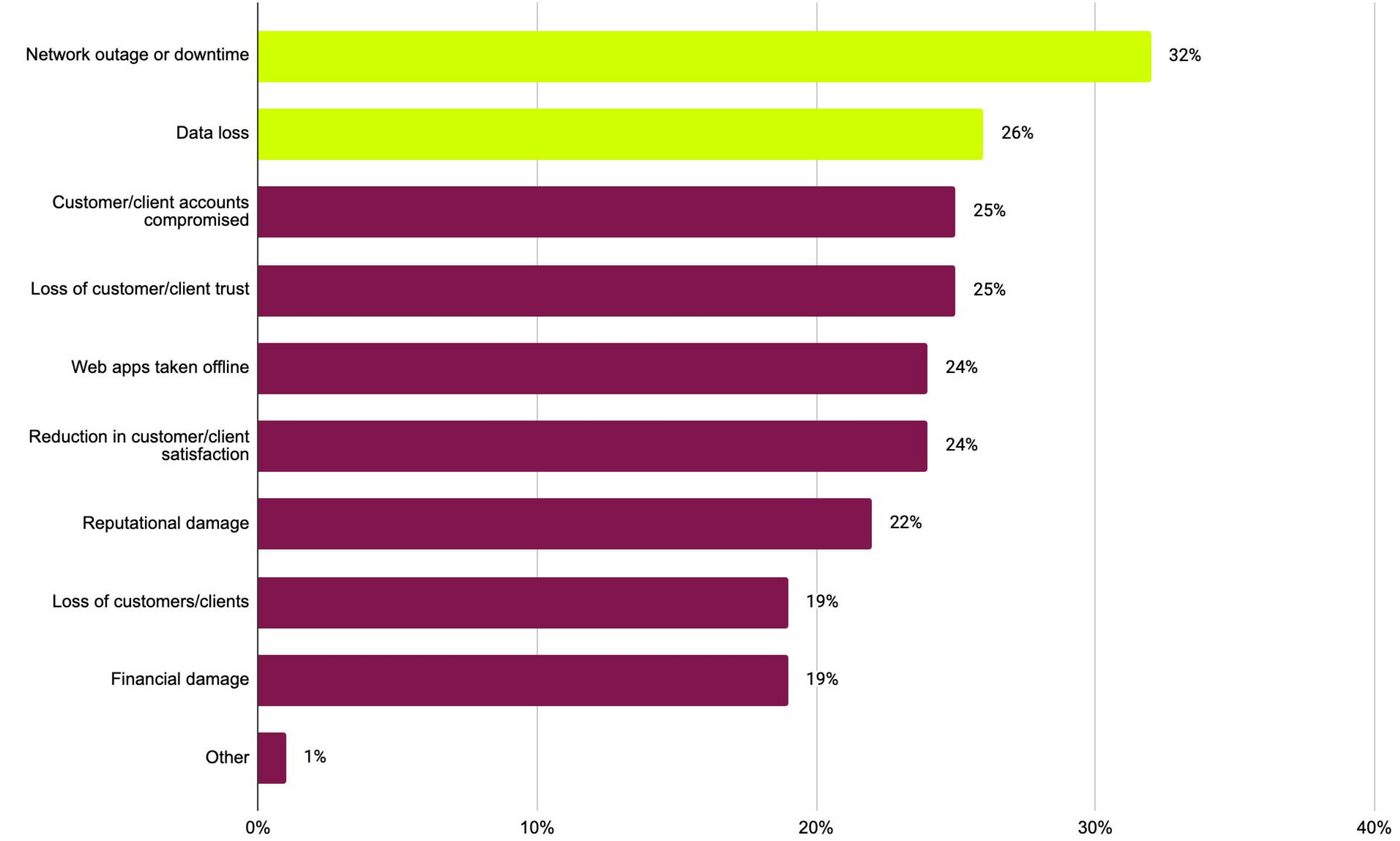


*only asked to those who have experienced a cyber attack

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

Base: 176*

Network outages or downtime (33%) and data loss (26%) were the main impacts of cyber attacks

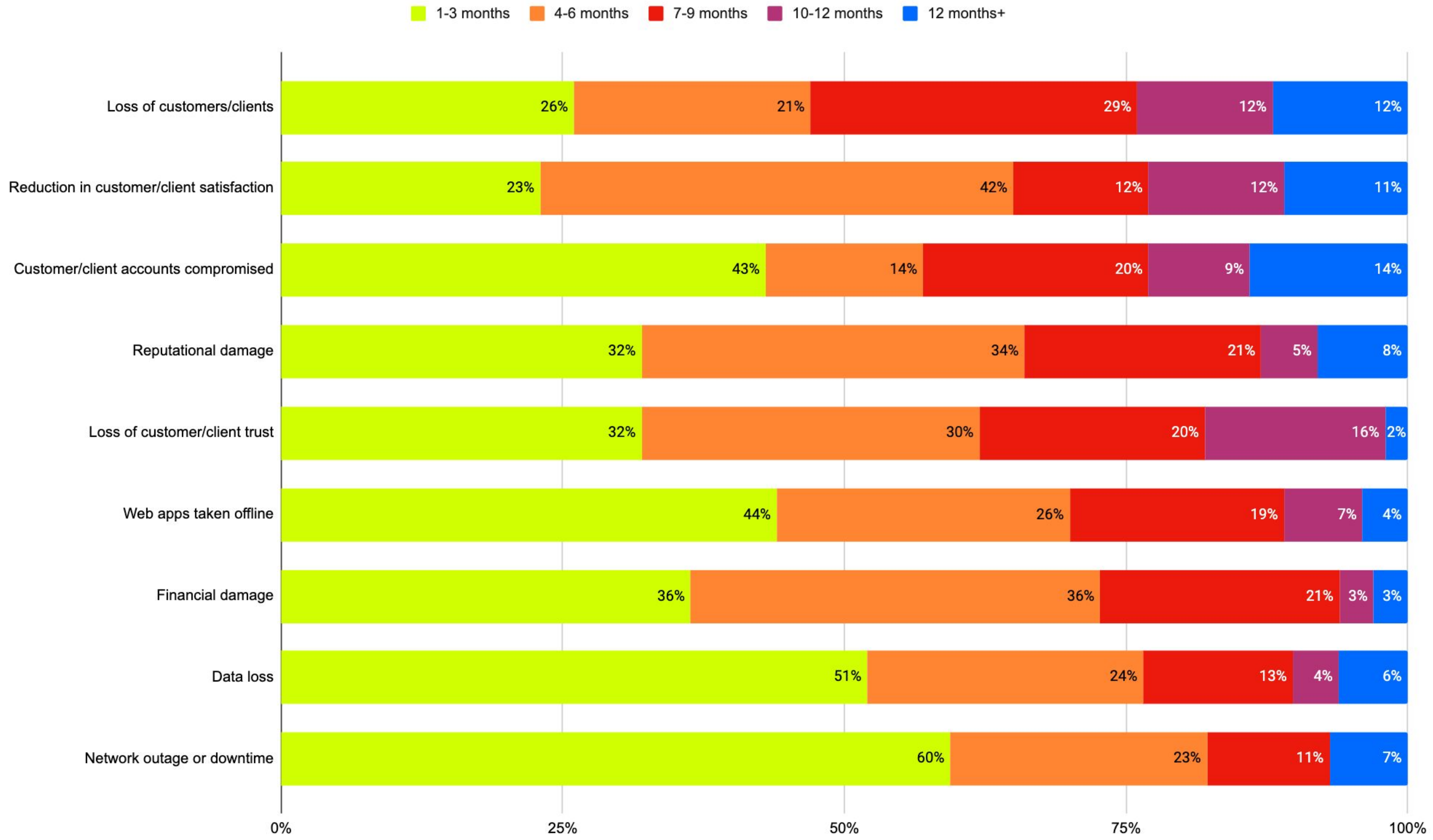


*only asked to those who have experienced a cyber attack

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

Base: 176*

On average, it will take businesses 7 months to recover from the loss of customers/ clients and the reduction of customer/client satisfaction as a result of a cyber attack



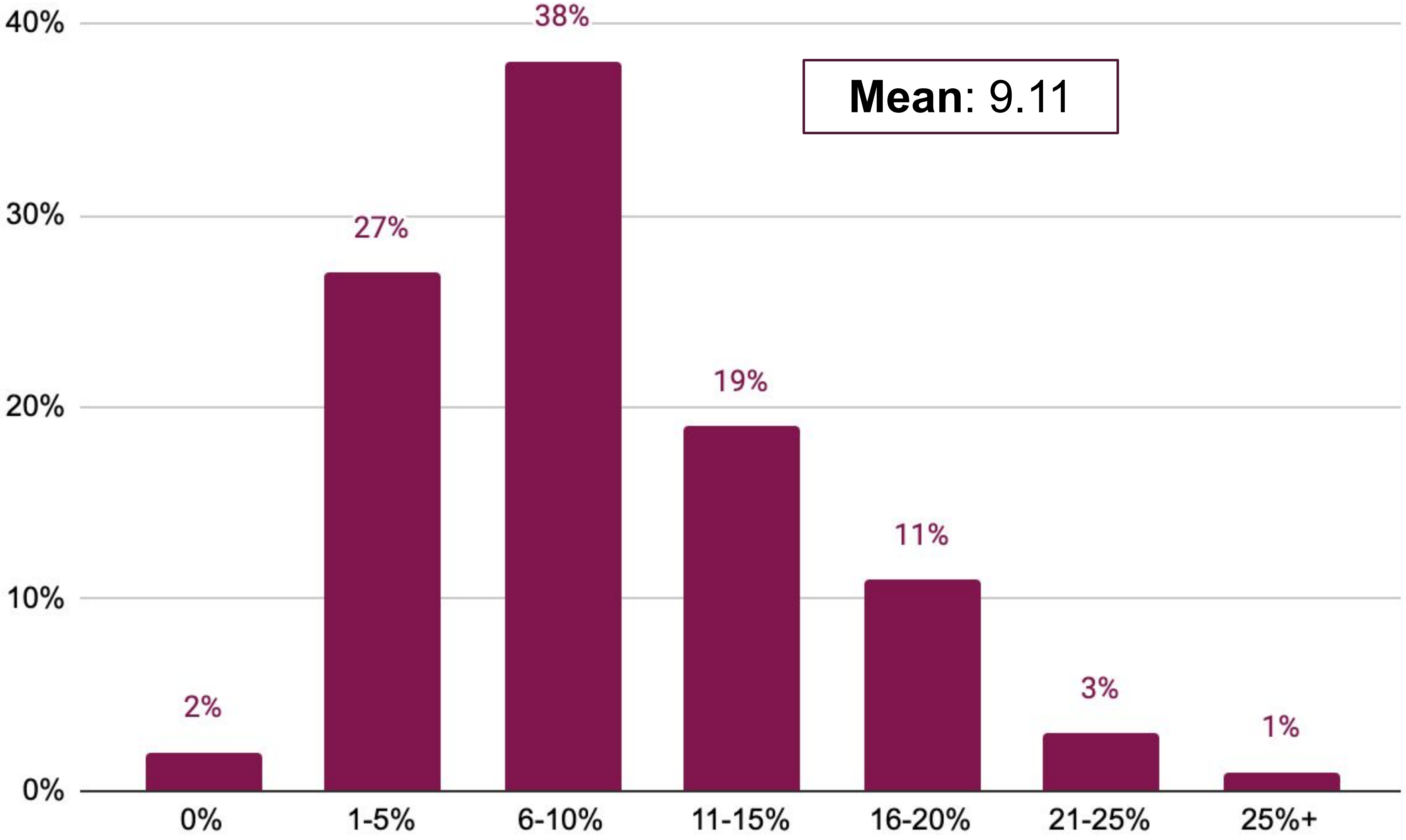
Average no. Months
7.22
6.64
6.3
6.11
5.89
5.31
5
4.9
4.32

*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 9% of their annual income as a result of cyber attacks



Mean: 9.11

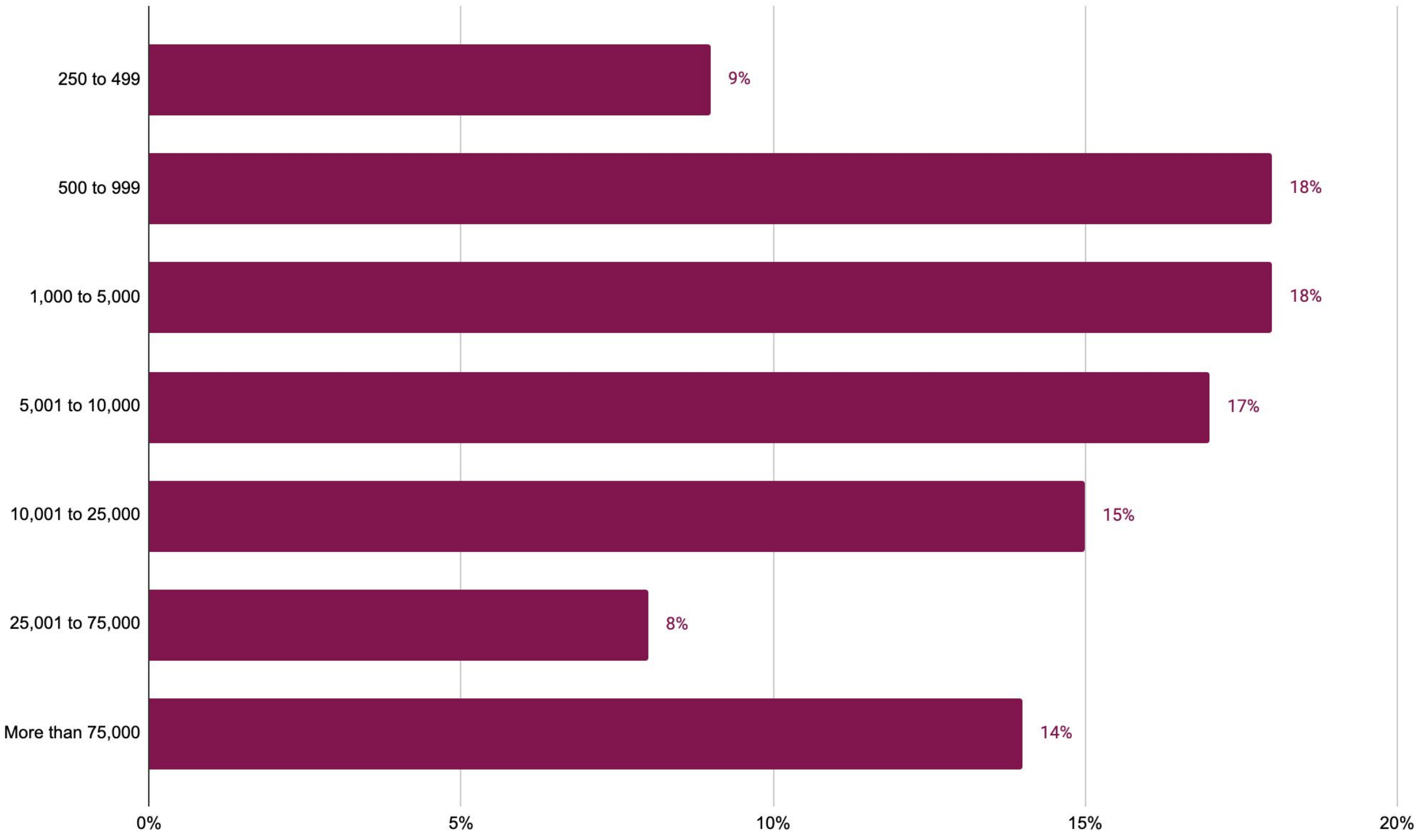
*only asked to those who had experienced each impact at Q22

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

Base: 176*

Demographics

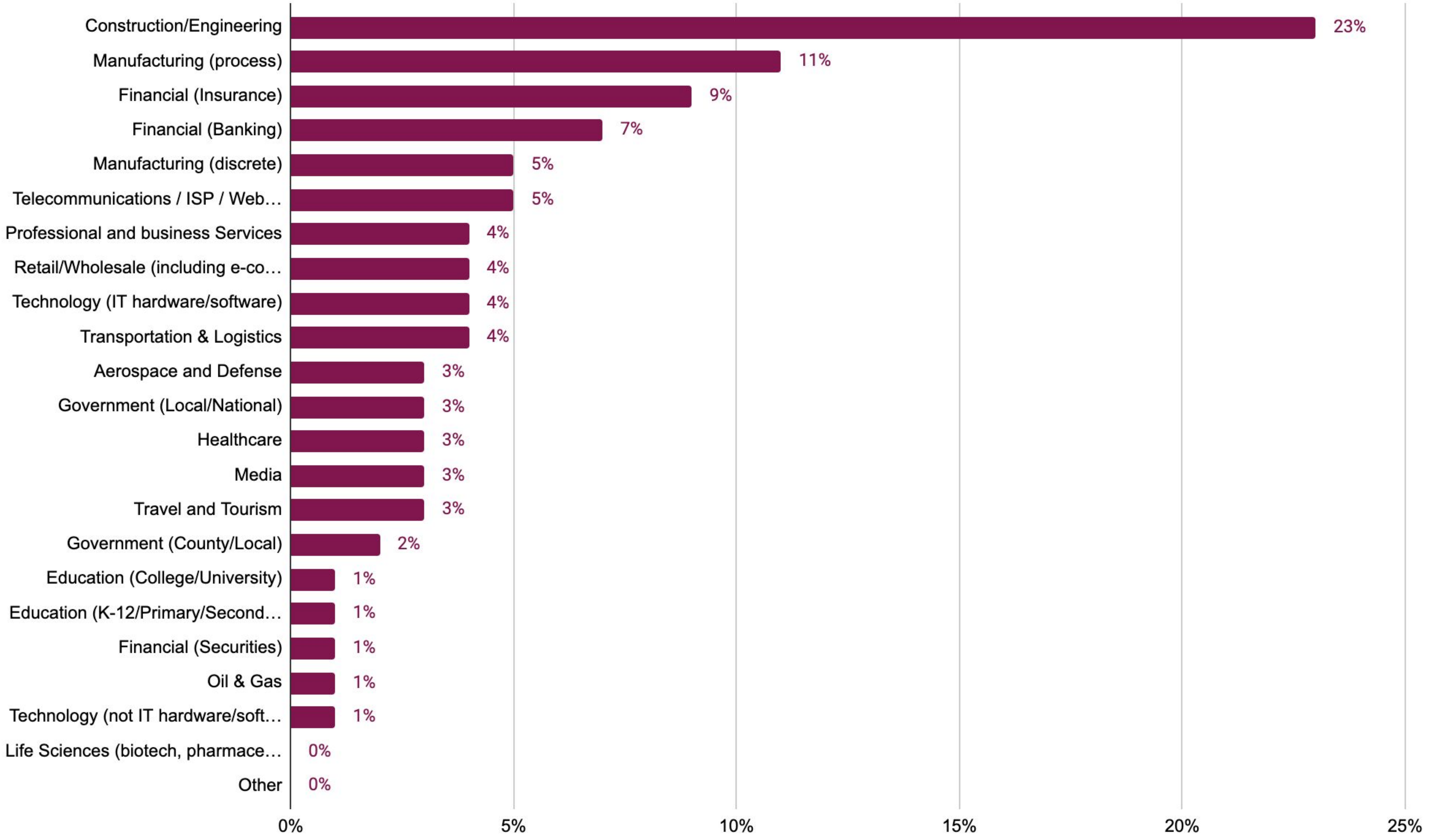
Size



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

Base: 211

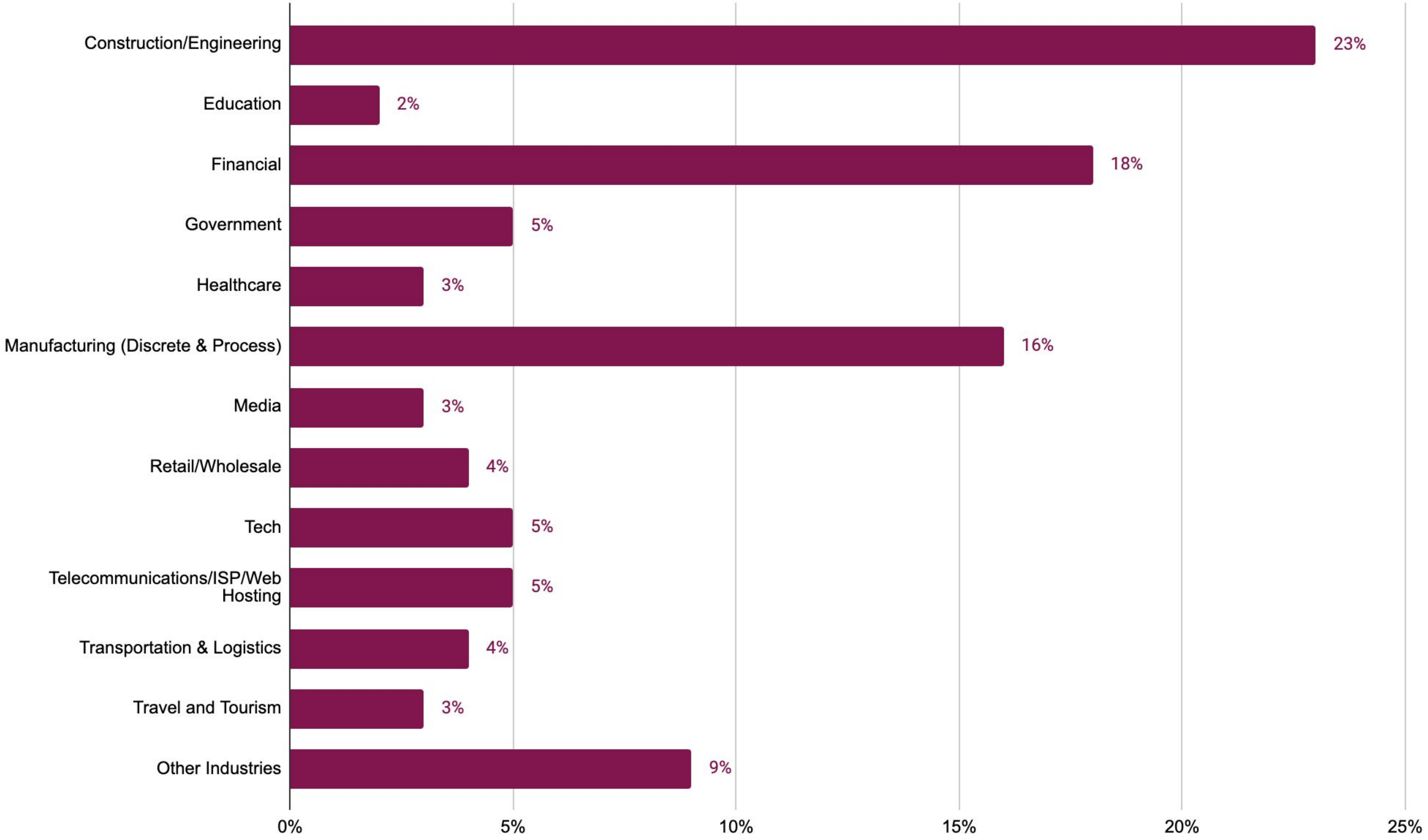
Industry



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

Base: 211

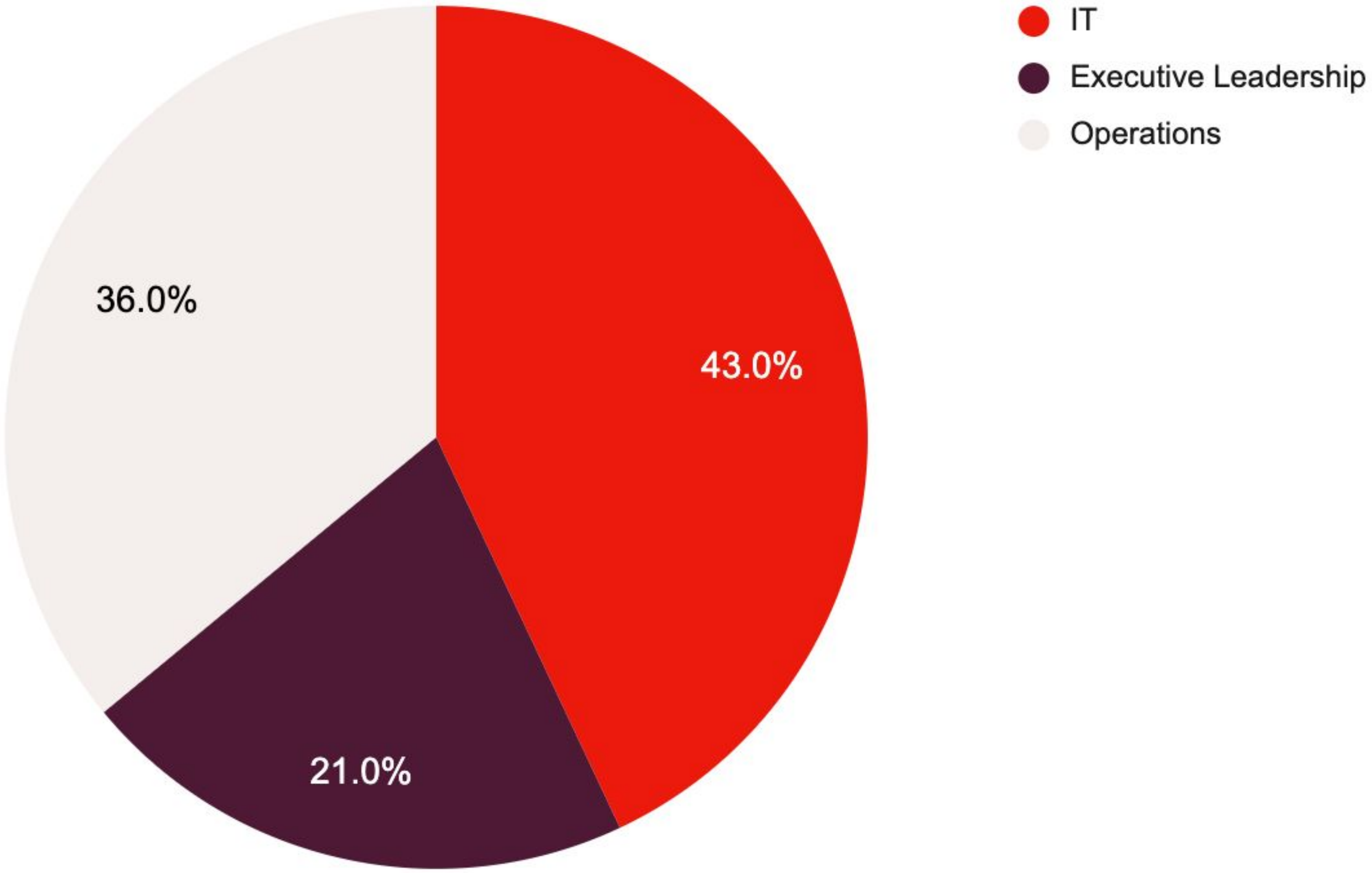
Industry - focus



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

Base: 211

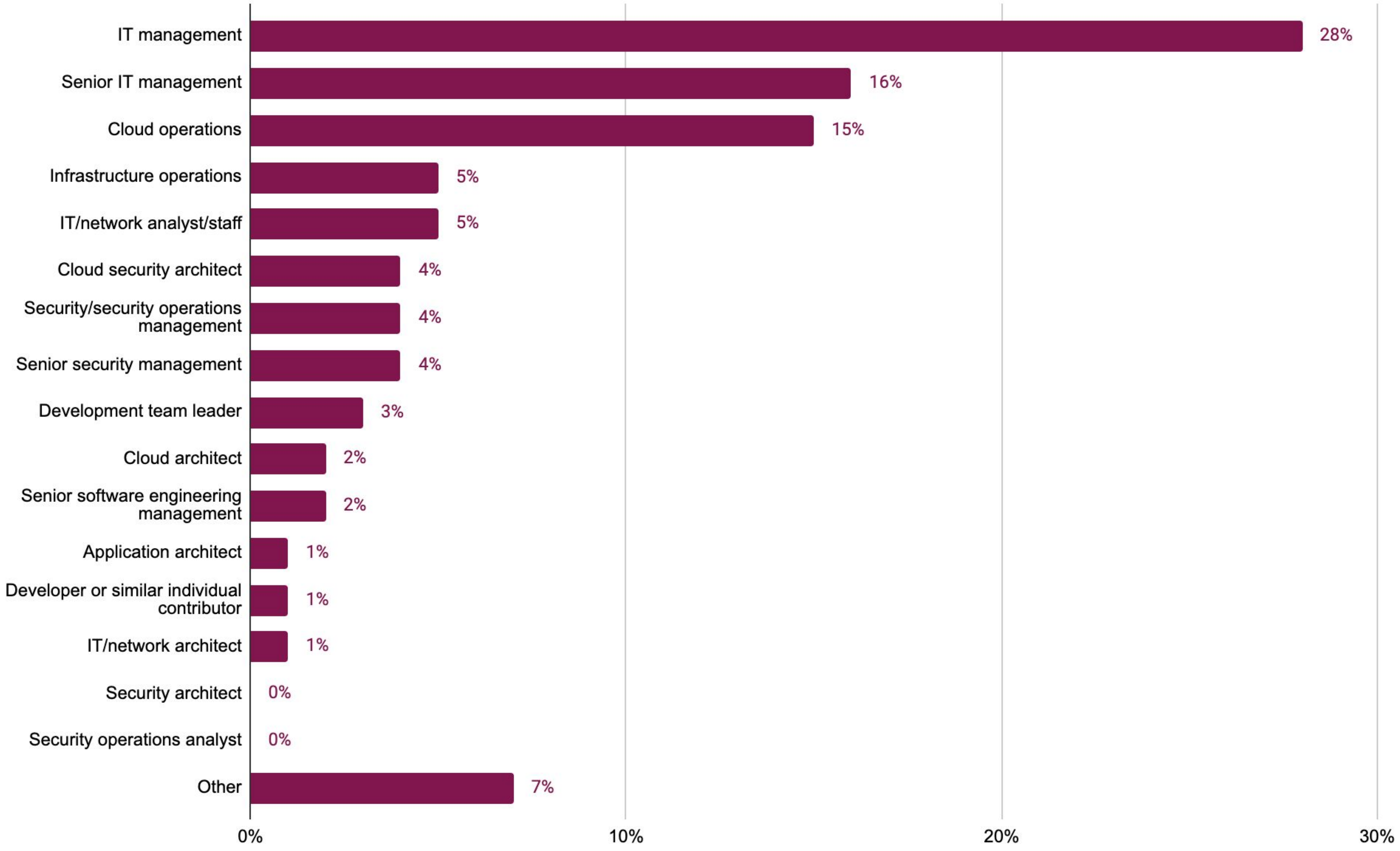
Department



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

Base: 211

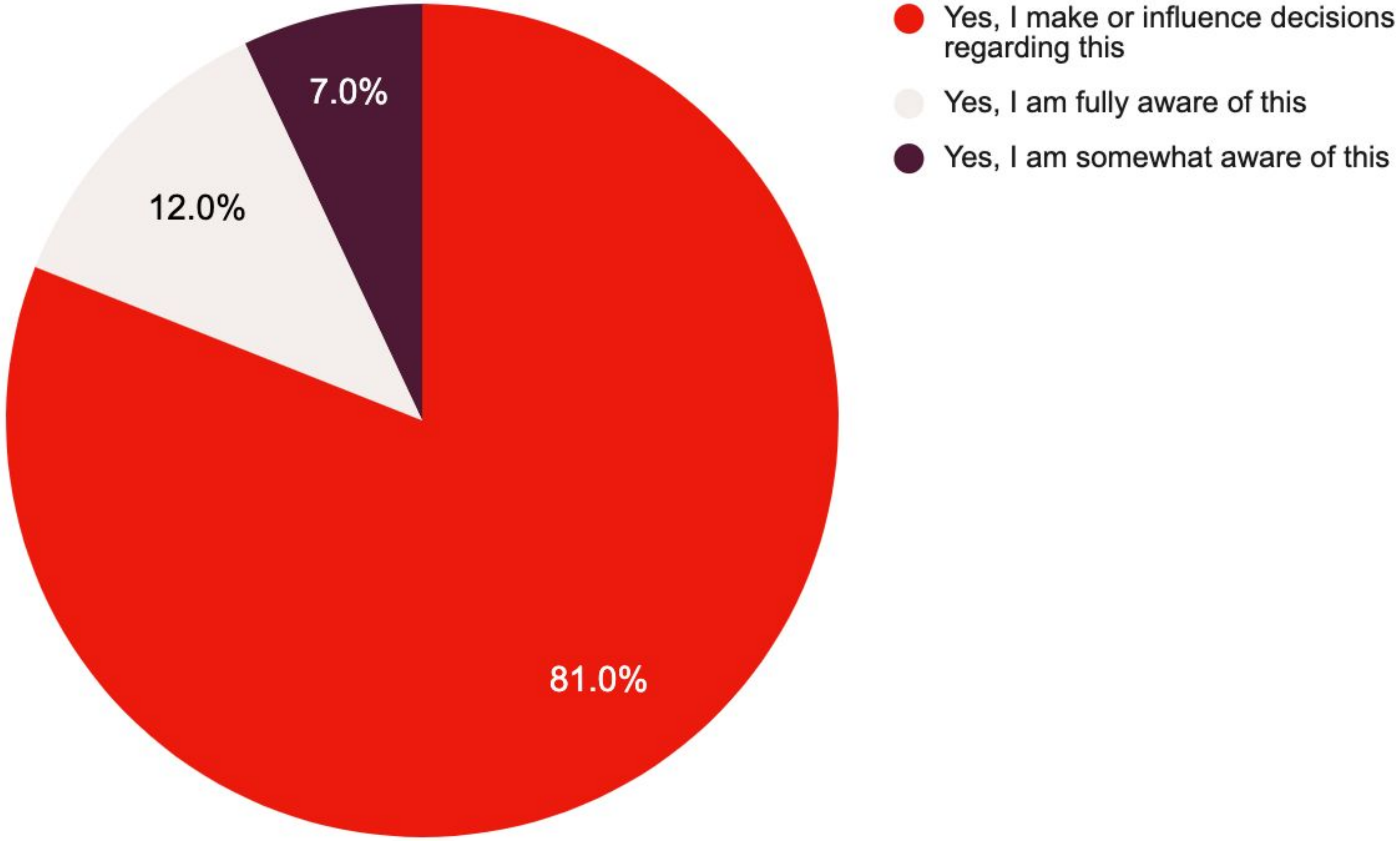
Current responsibility



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

Base: 211

Cyber security decision making



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: 211

Thank you!

fastly®