Fastly Global Security Research 2023

Spain 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+ employees in Spain. 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 ± **6.8%** 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

IT: 47%

Ops: 35%

Executive Leadership : 18%

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	-	27%	35%	17%	8%	6%	8%

Industry

Company sectors – top 3:

IT / Tech: 24%

Manufacturing: 12%

Government: 10%

Decision making (cyber security)

- 65% make or influence cybersecurity decisions
- 18% are fully aware of decisions regarding cybersecurity
- 18% are somewhat aware of cybersecurity decisions

Key stats

47% predict 'identity-based threats' as the biggest cybersecurity threat over the next 12 months

On average, businesses **lose 8% of their annual income** as a result of **cyber attacks**

43% of respondents feel there is gap among the current talent pool in experience with new and emerging technologies/ threats such as **generative AI**

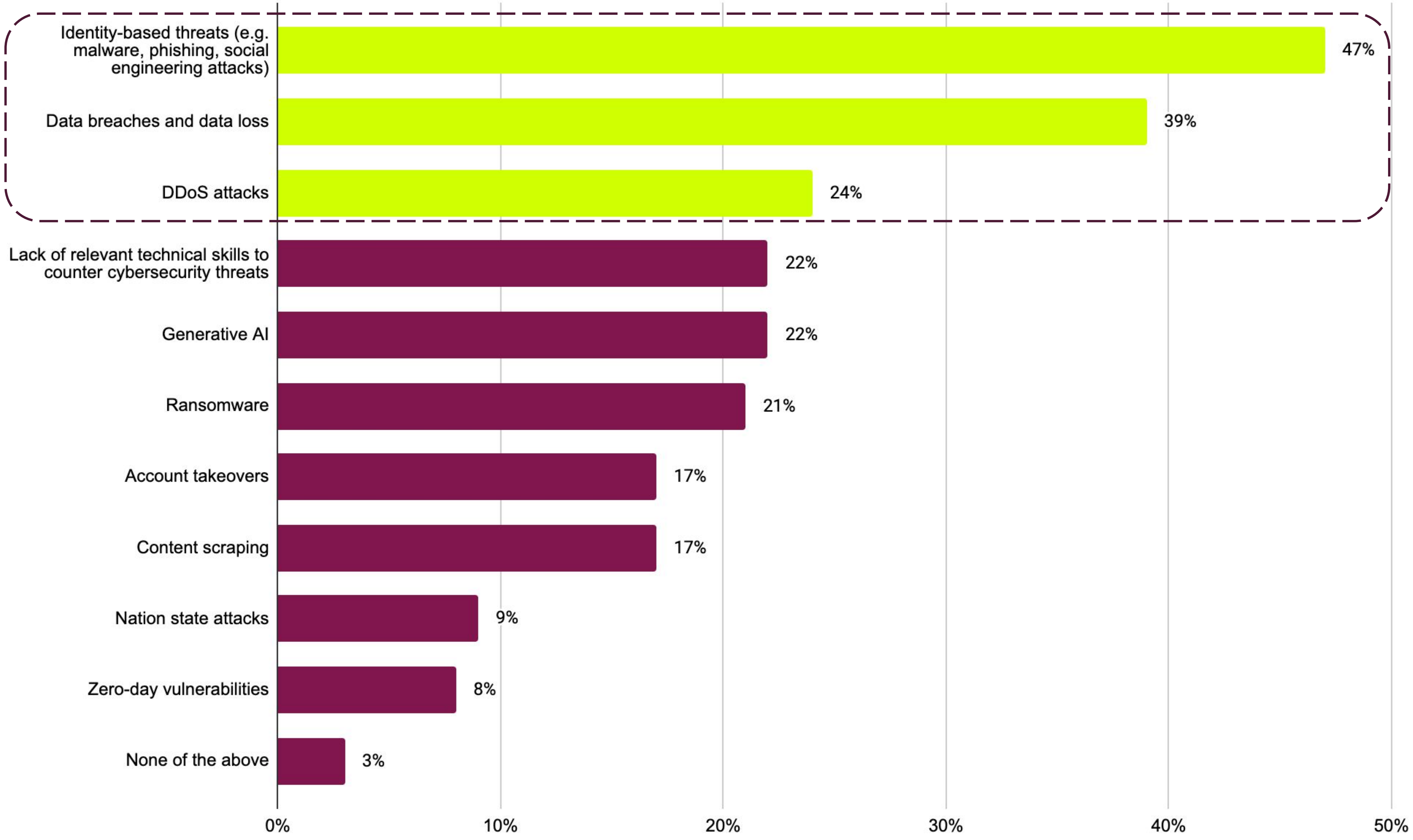
Defining approaches to new and emerging cybersecurity threats **(44%)** and improving cybersecurity skills through training and/or talent acquisition **(40%)** are the main security priorities over the next year

41% say that their organisations cybersecurity strategy has **hampered** business innovation

On average, 63% of cybersecurity tools are fully deployed / active

Main Findings

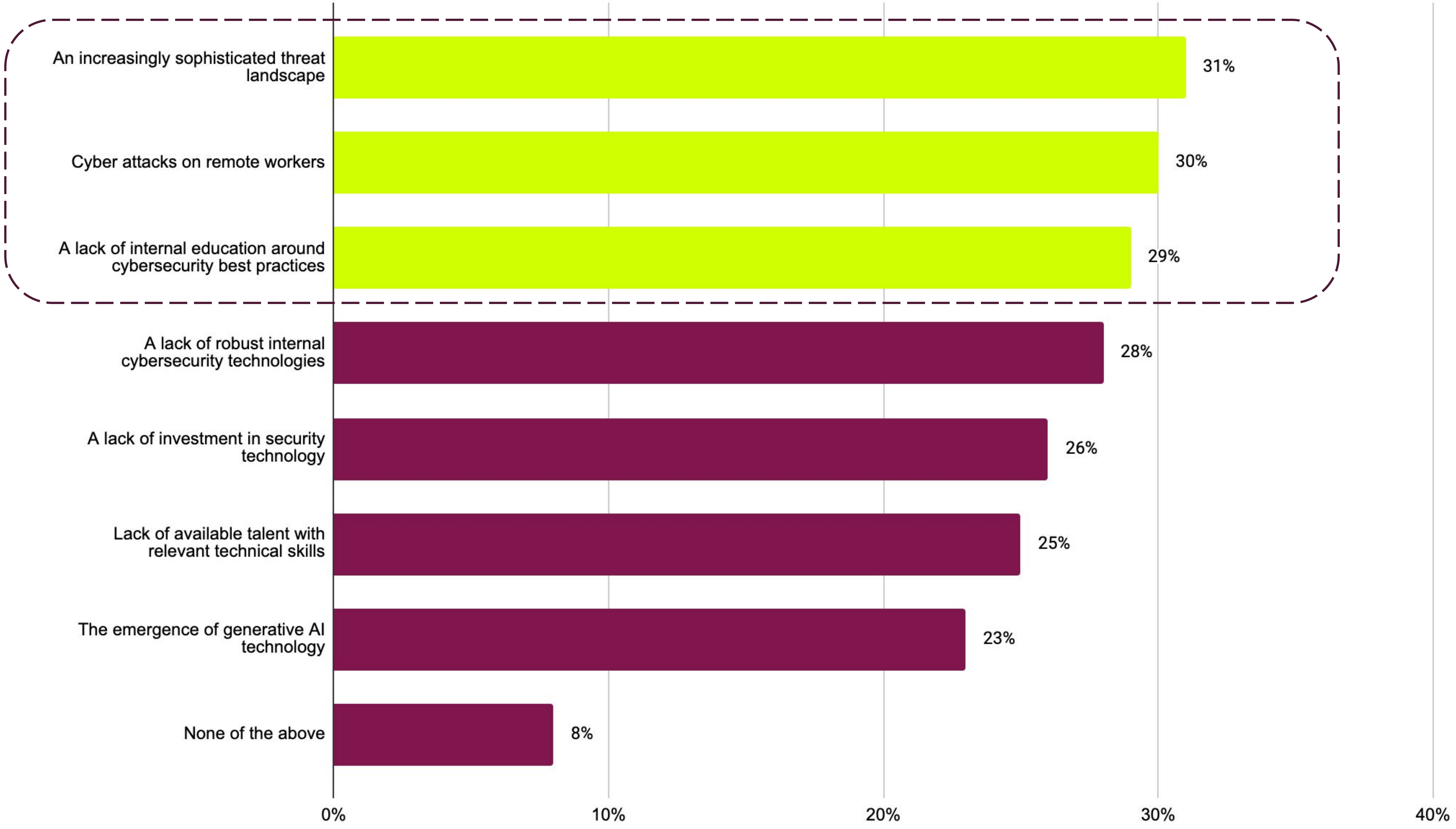
Identity-based threats (47%), data breaches and losses (39%), and DDoS attacks (24%), are viewed as the biggest cybersecurity threats to organisations over the next 12 months



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

Base: 209

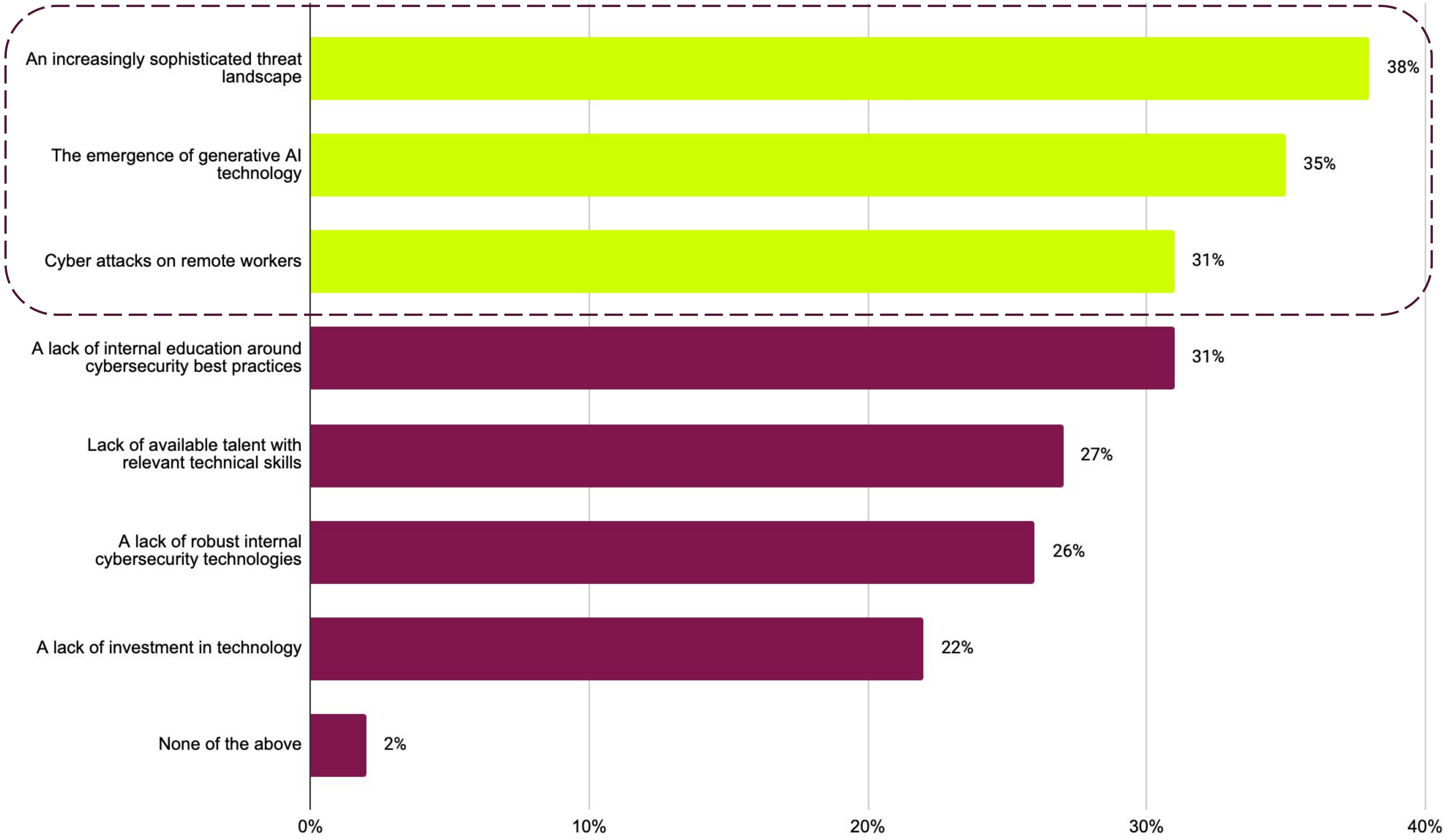
Over the last 12 months, an increasingly sophisticated threat landscape (31%), cyber attacks on remote workers (30%) and a lack of internal education around cybersecurity best practices (29%) were the main drivers of cybersecurity threats



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

Base: 209

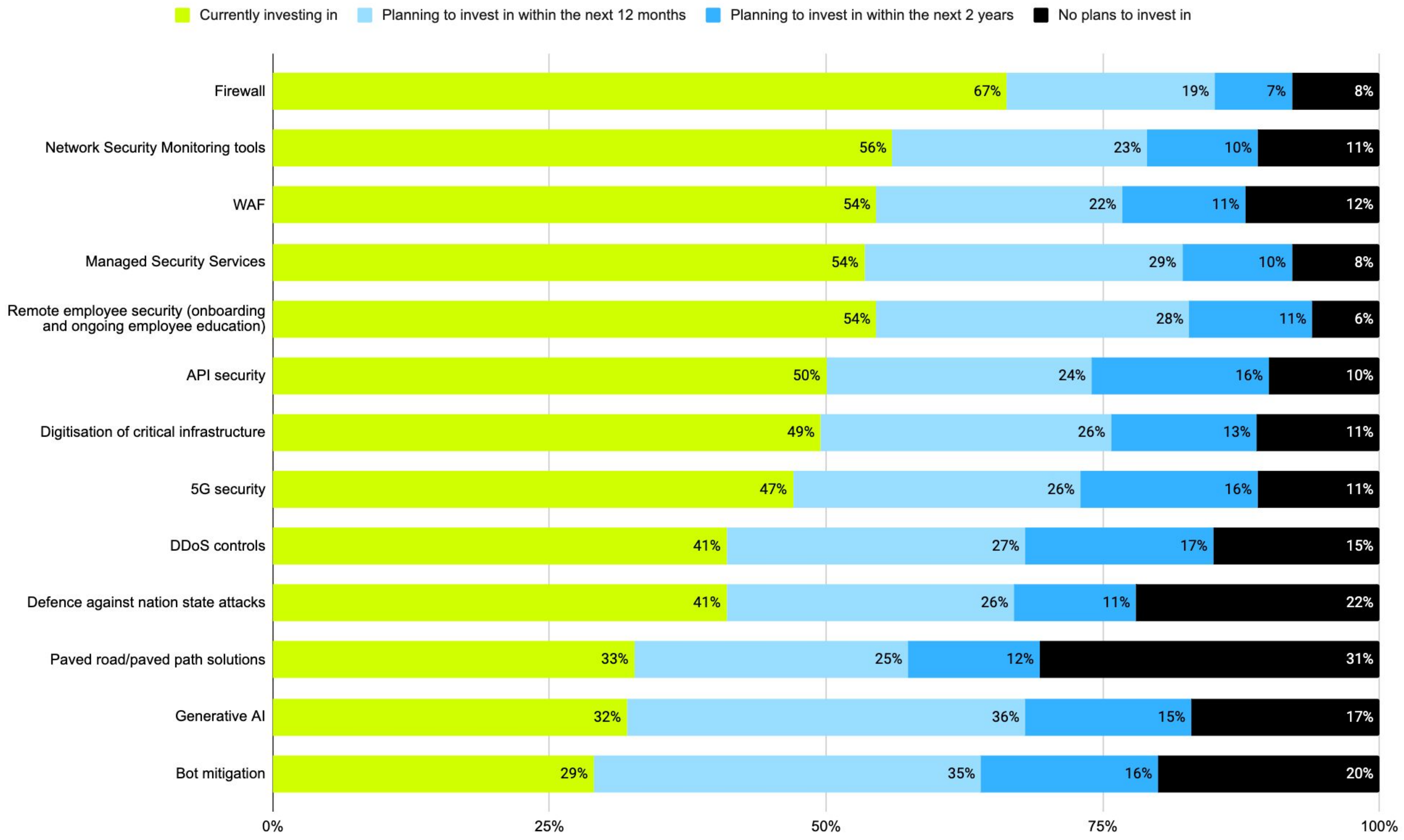
Over the next 12 months, an increasingly sophisticated threat landscape (38%), the emergence of generative AI (35%) and cyber attacks on remote workers (31%) are seen as the main drivers of cybersecurity threats



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

Base: 209

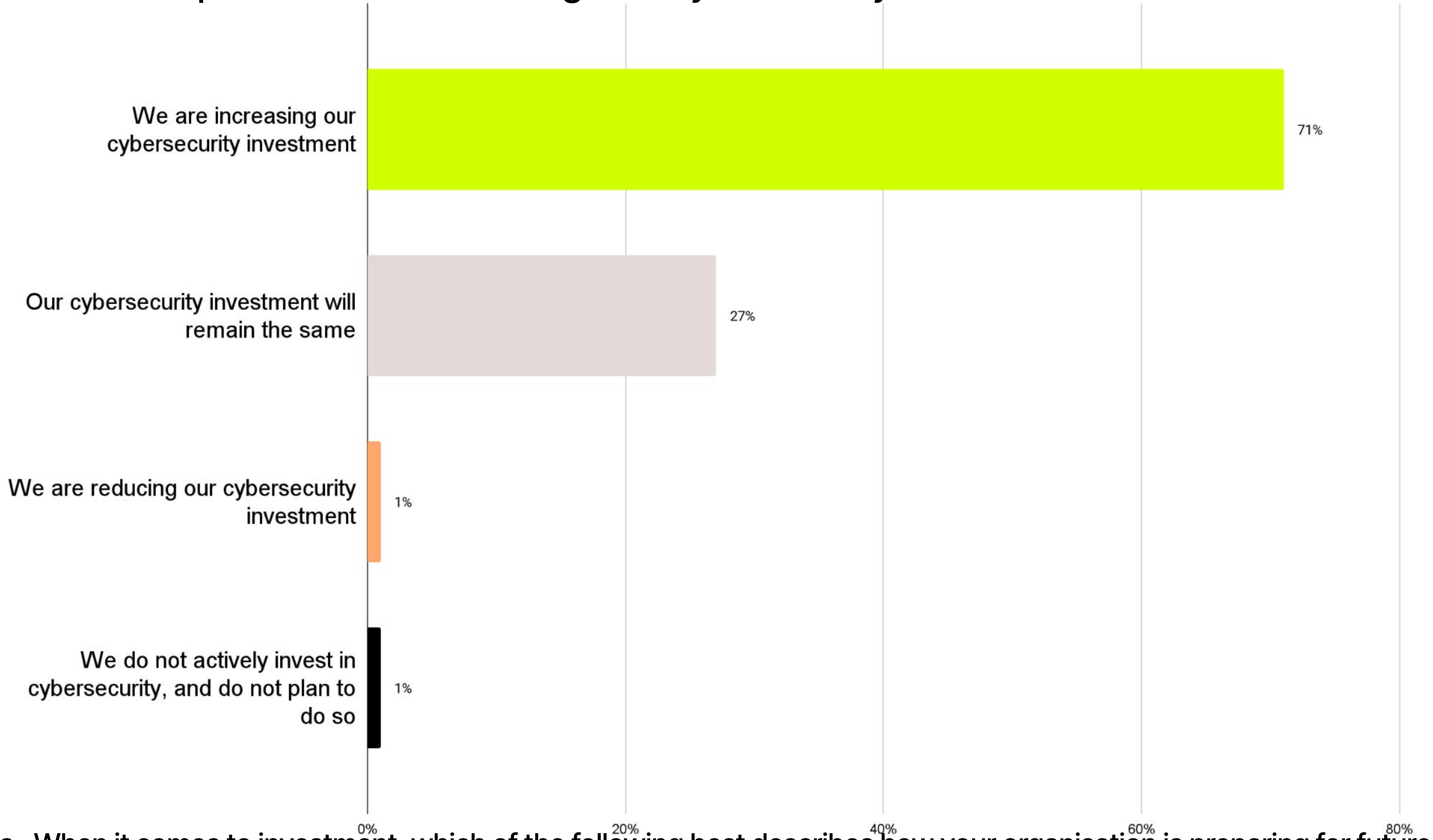
67% are currently investing in ‘Firewall’ technology, and over half are investing in ‘Network Security Monitoring tools’ (56%)
31% have no plans to invest in paved road/ paved path solutions



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

Base: 209

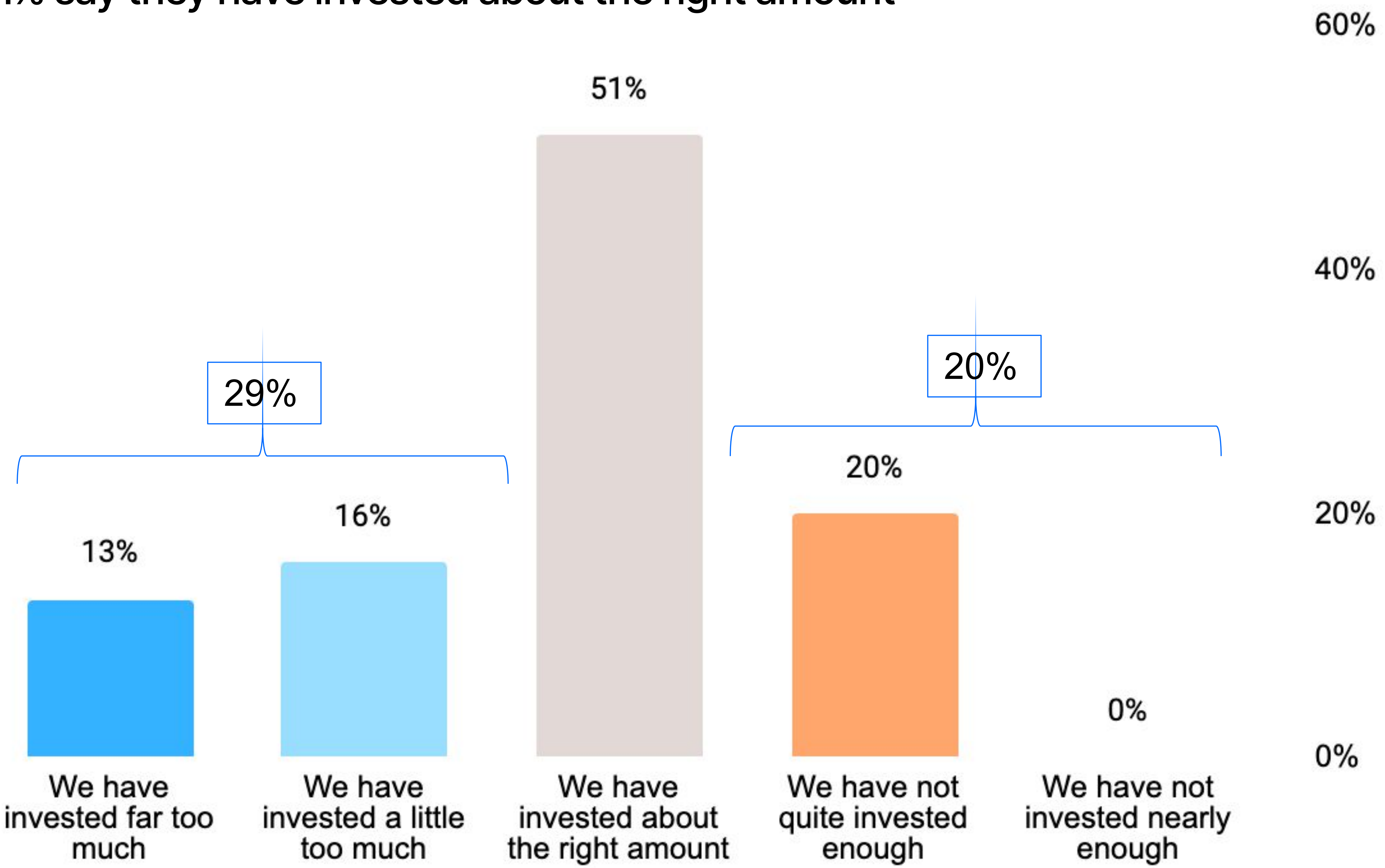
71% of respondents are increasing their cybersecurity investment



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

29% of respondents have invested too much into cybersecurity over the past 12 months 51% say they have invested about the right amount

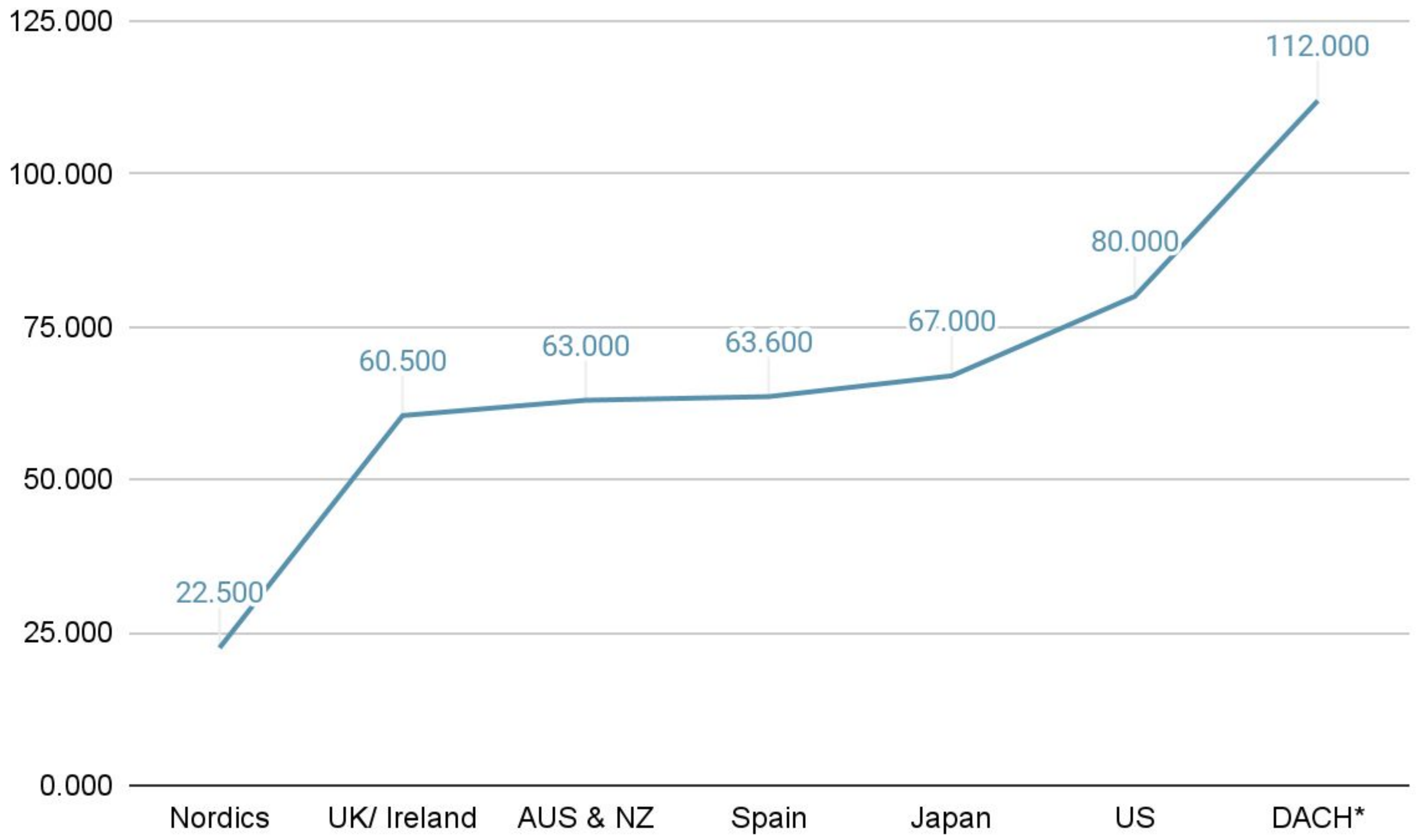


*only asked to those who invest in cybersecurity

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: 207*

On average (median), $63,600 USD are spent per year on web application and API security control/tools in Spain



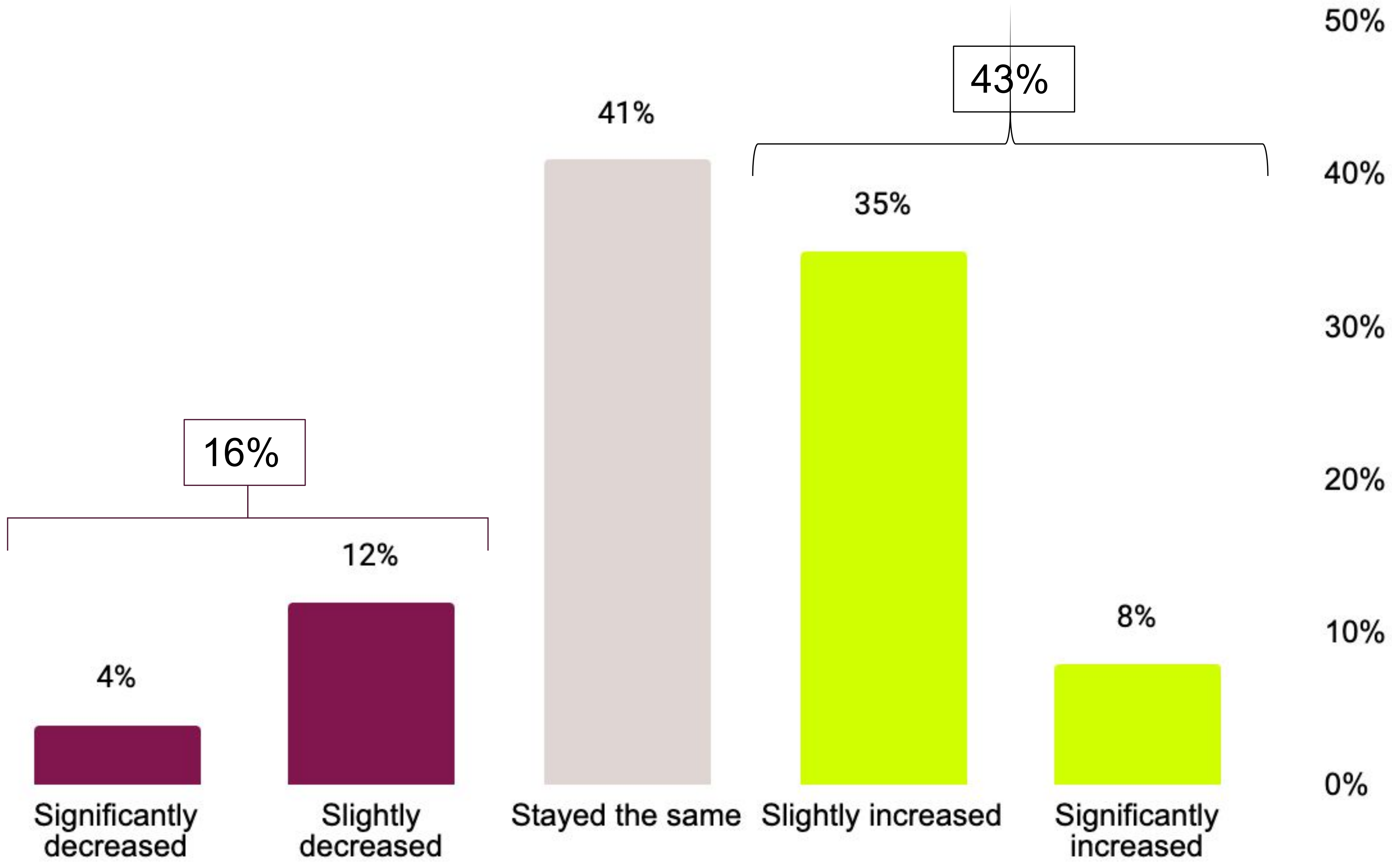
*The sample for DACH countries had a larger proportion of companies with more than 75,000+ employees

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

43% of respondents have increased talent spending, with only 16% having decreased talent spending

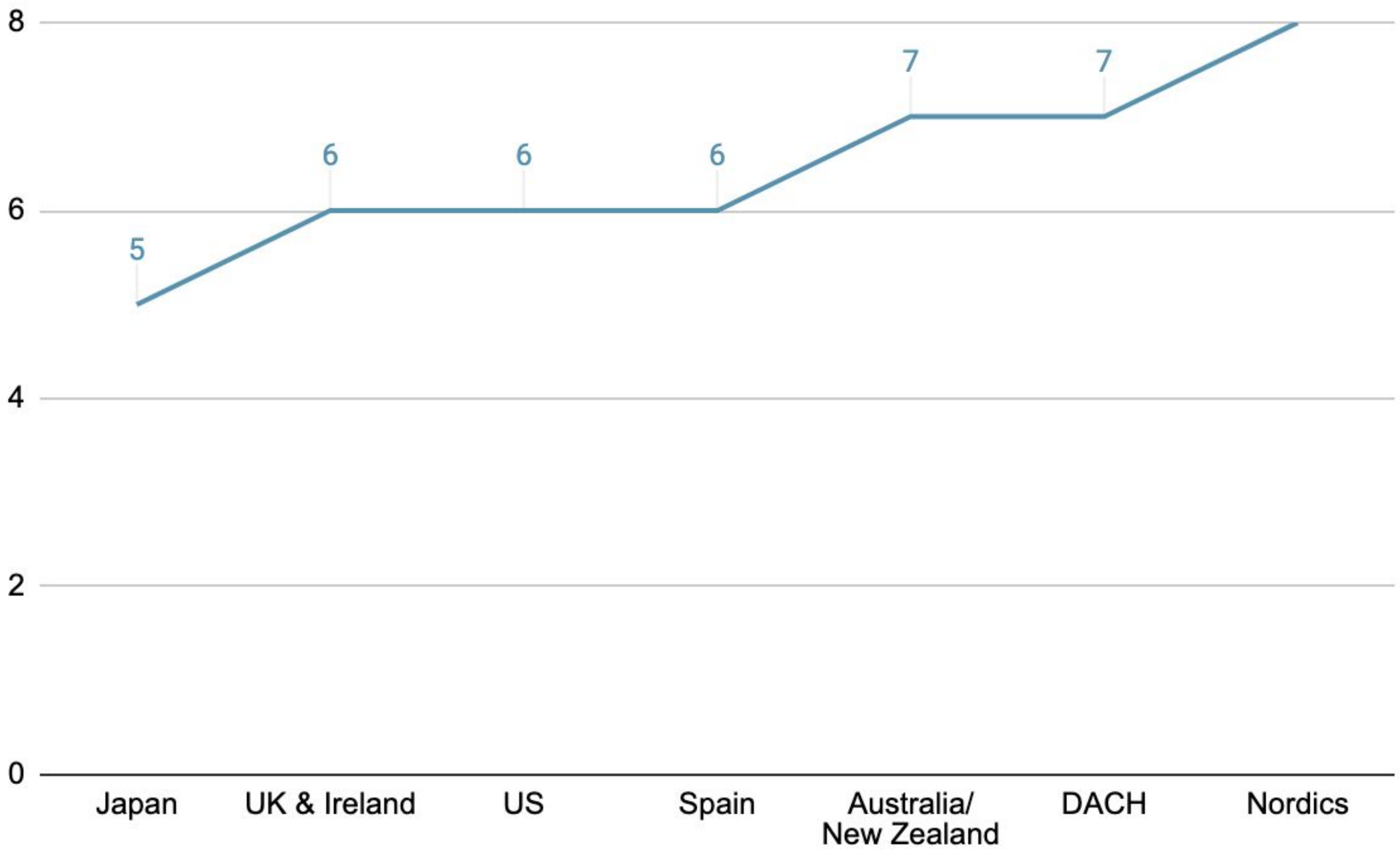


Q5b. How has your talent spending (e.g. new hires, wages) for cybersecurity changed, if at all? Select one

Base: 209

On average (median), organisations in Spain rely on 6 network and application cybersecurity solutions

Overall median: 6

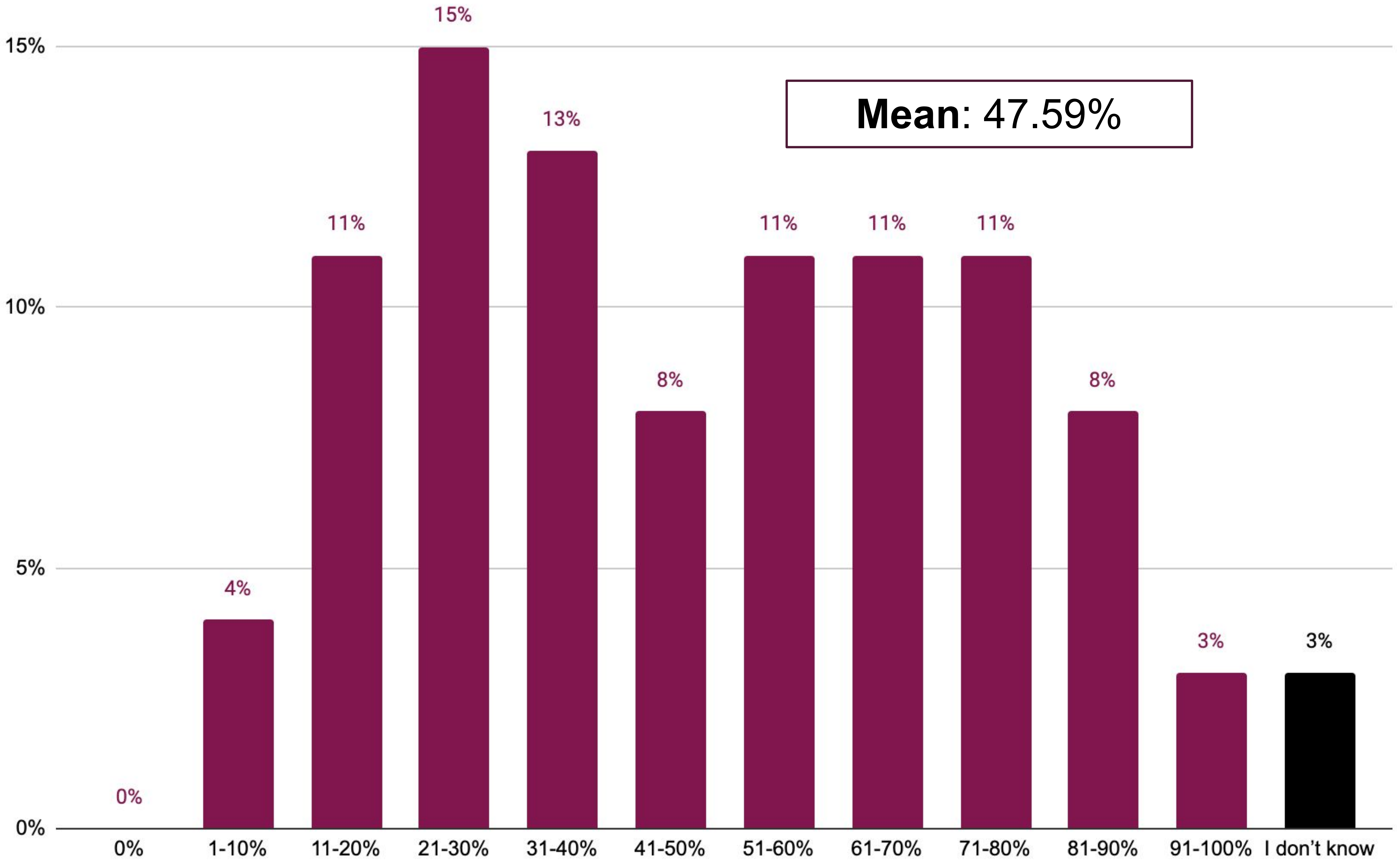


2022 Survey:
Japan **4**
Spain **5**
US **5**
UK & Ireland **6**
AUS & NZ **5**
DACH **5**
Nordics **7**

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

Base: 1484

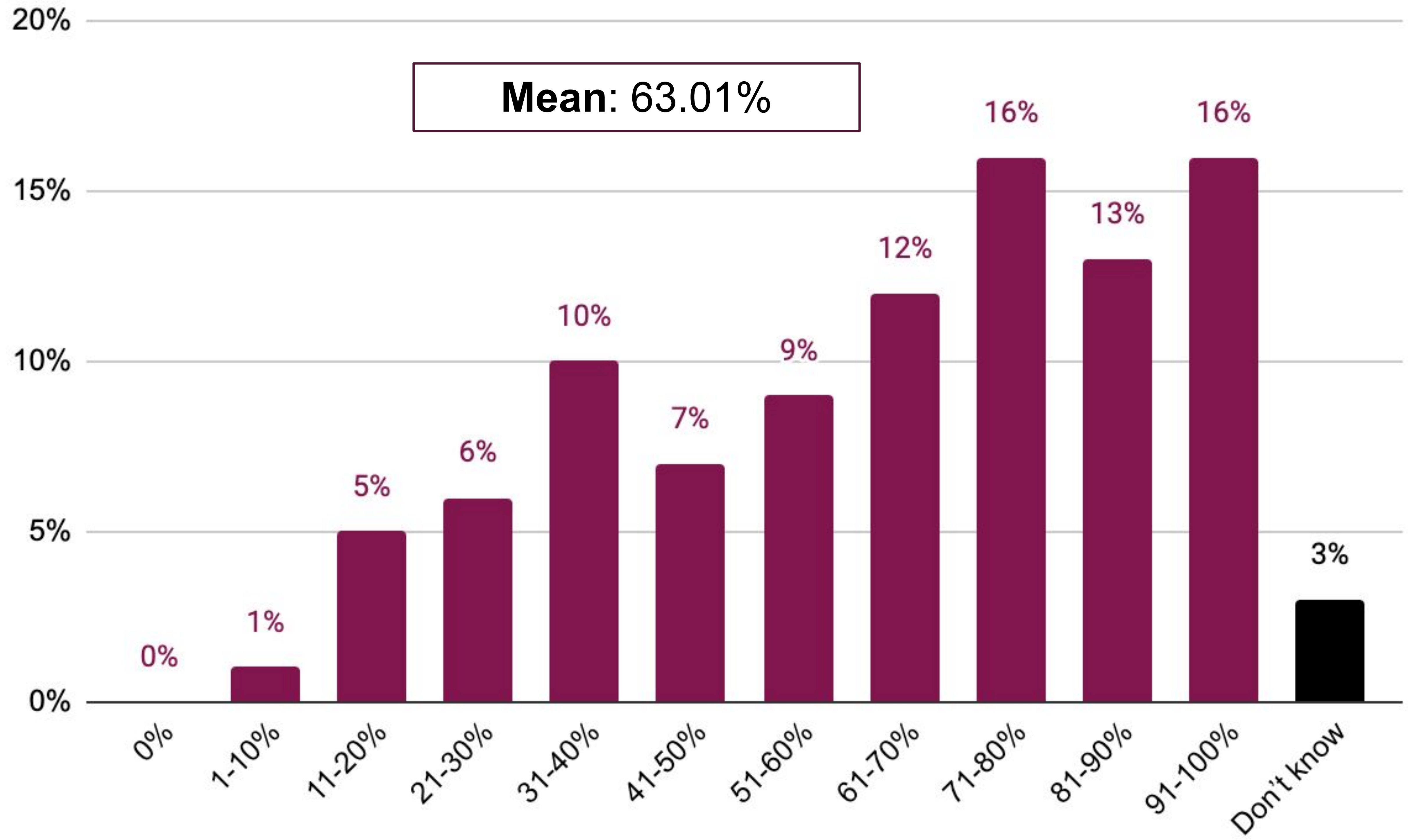
On average, 48% of network and application cybersecurity solutions overlap



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

Base: 209

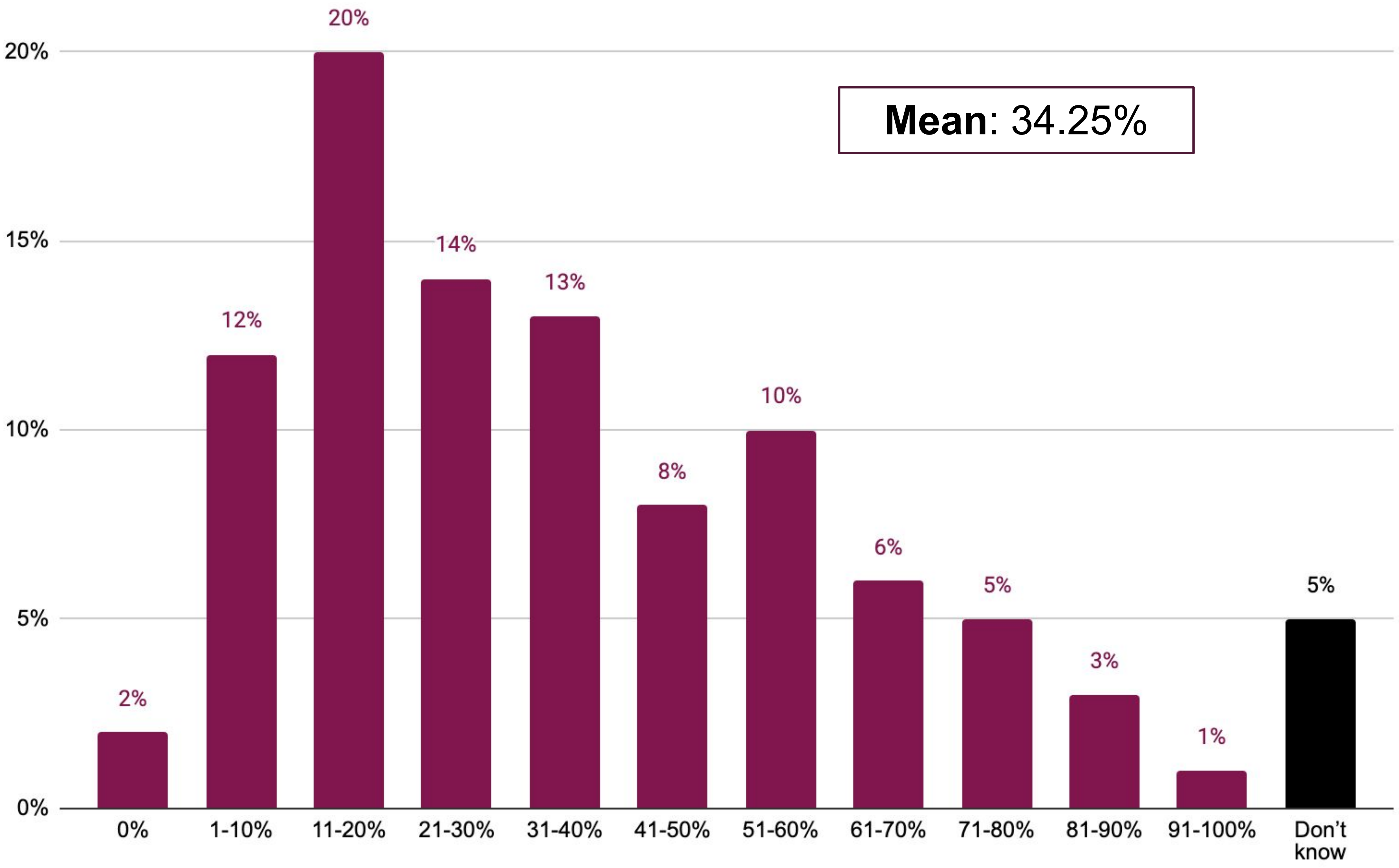
On average, only 63% of cybersecurity tools are fully active / deployed



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

Base: 209

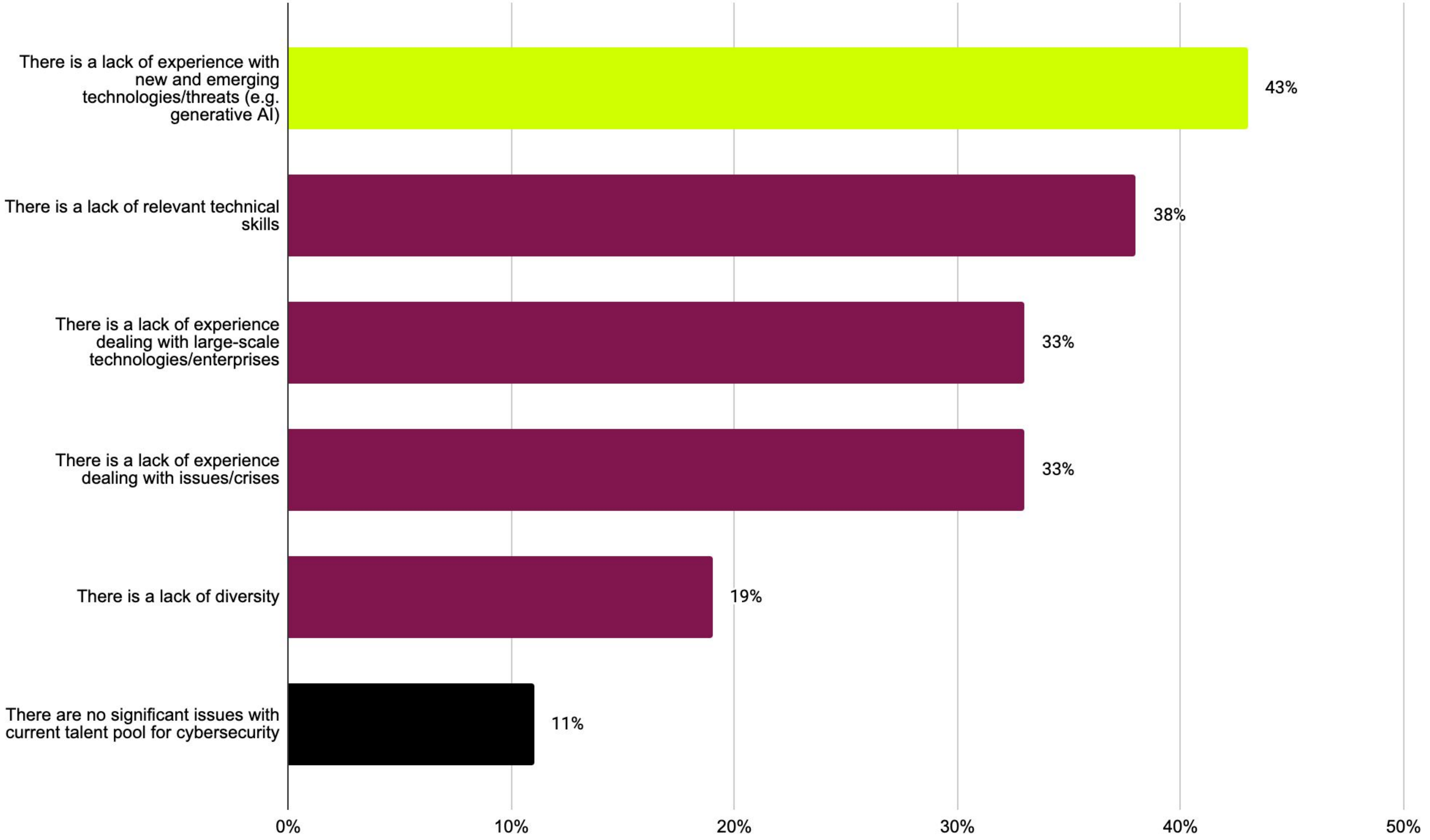
On average, 34% of security alerts detected by an organisations WAF are false alerts



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

Base: 209

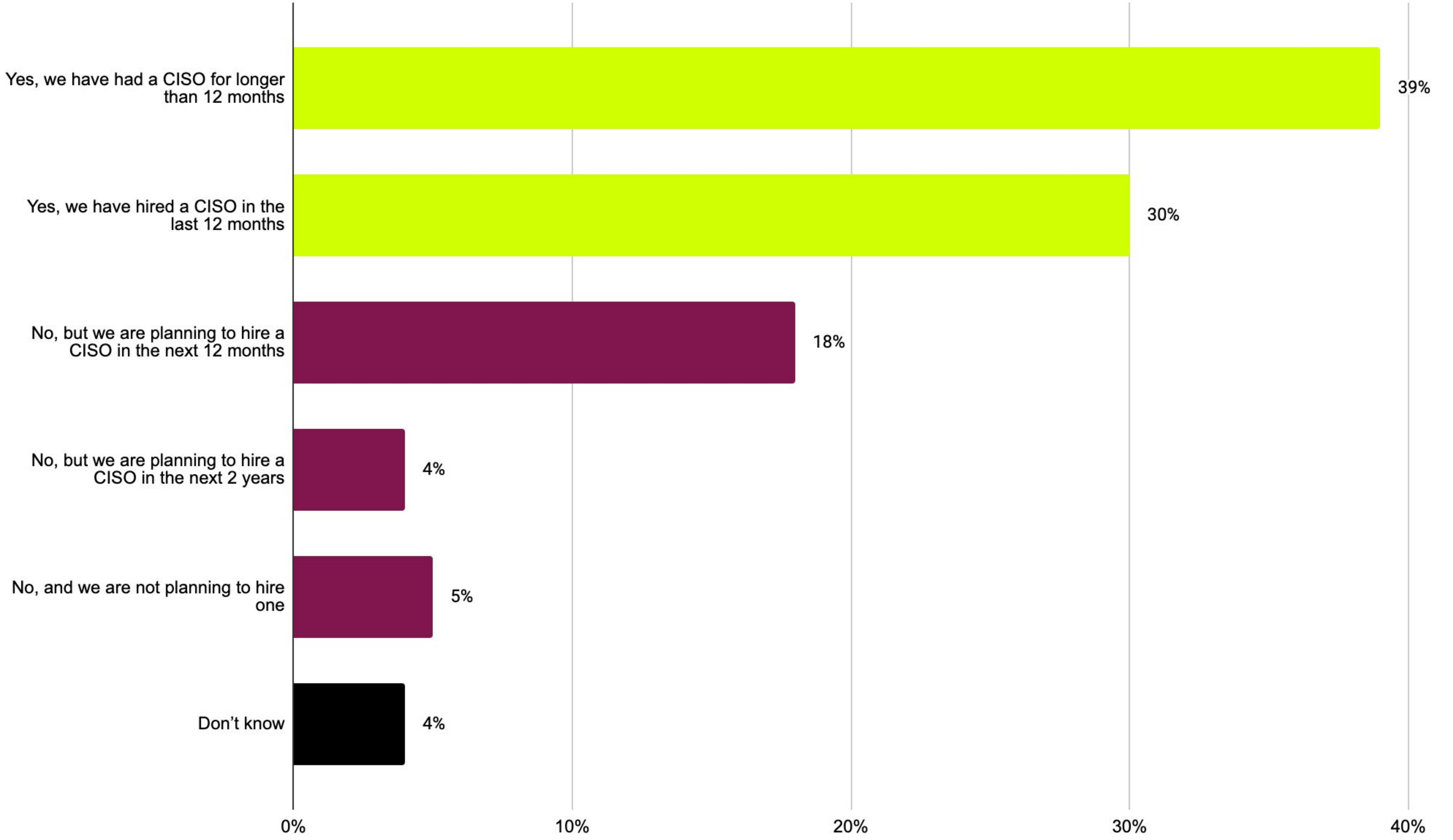
Respondents feel that the biggest gap among the current talent pool is experience with new and emerging technologies / threats such as generative AI (43%)



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

Base: 209

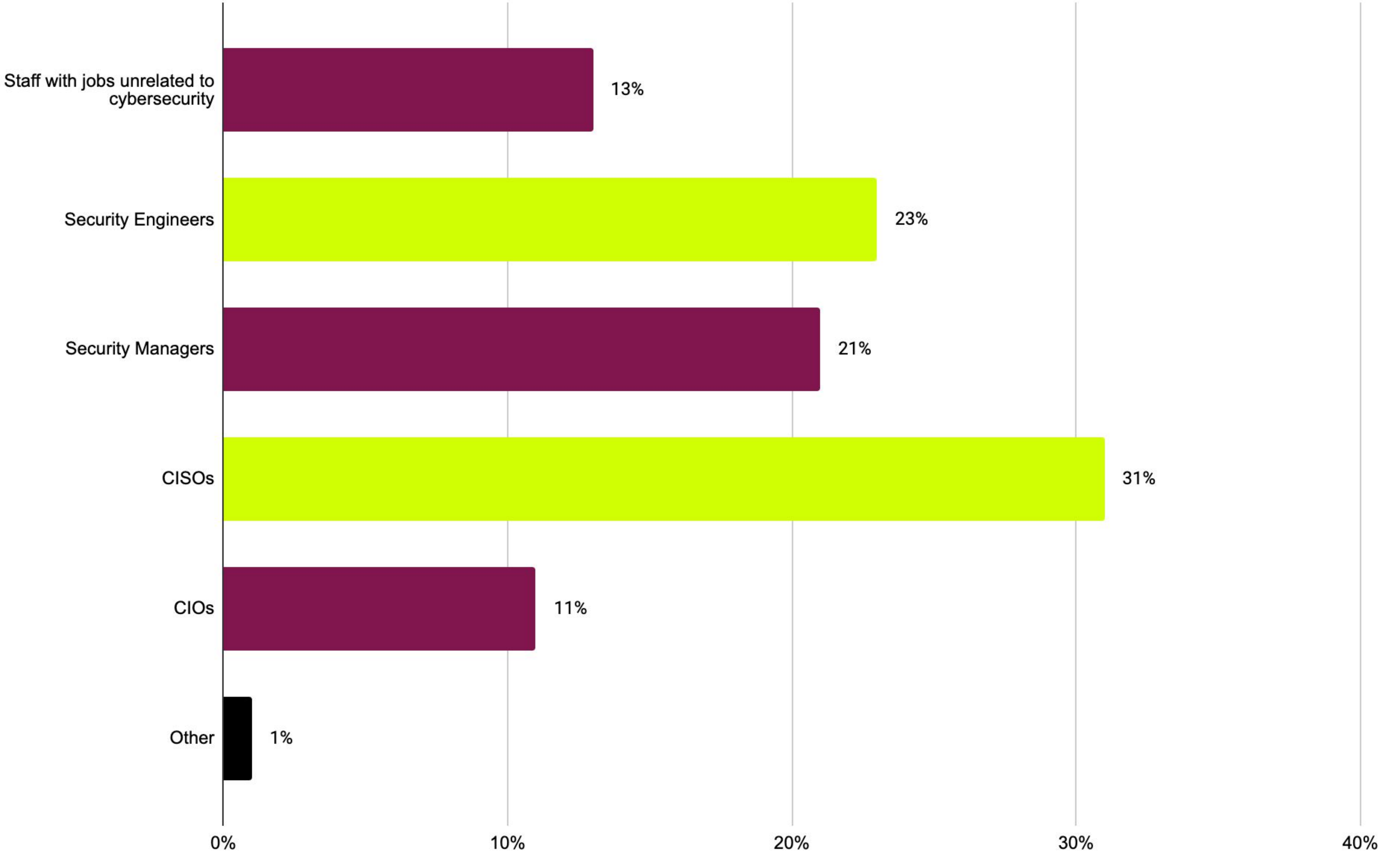
69% of respondents have hired a CISO, 30% of those within the last 12 months



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

Base: 209

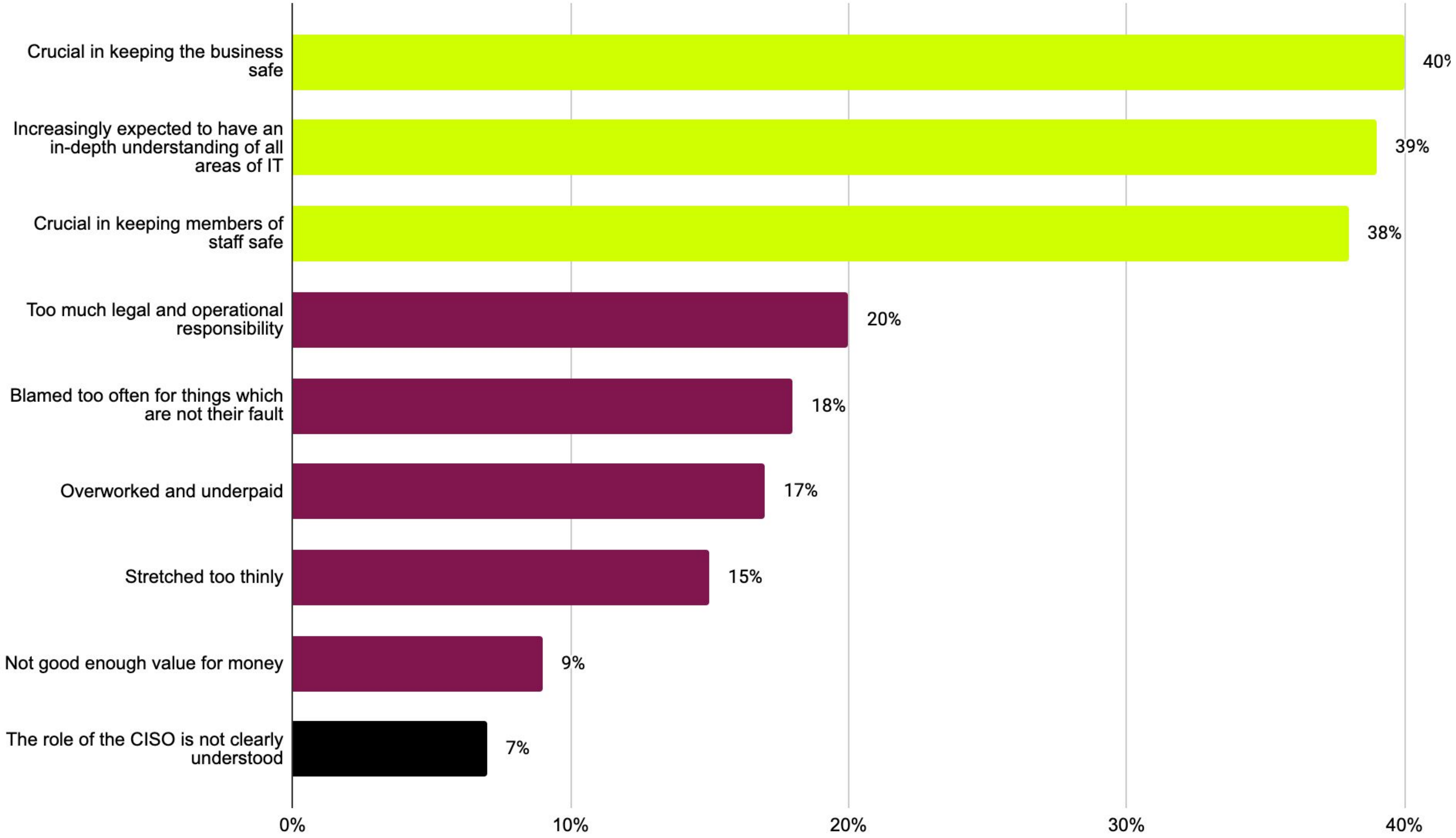
31% of respondents think CISOs are often held responsible for cybersecurity incidents, 23% think security engineers are often held responsible



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

Base: 209

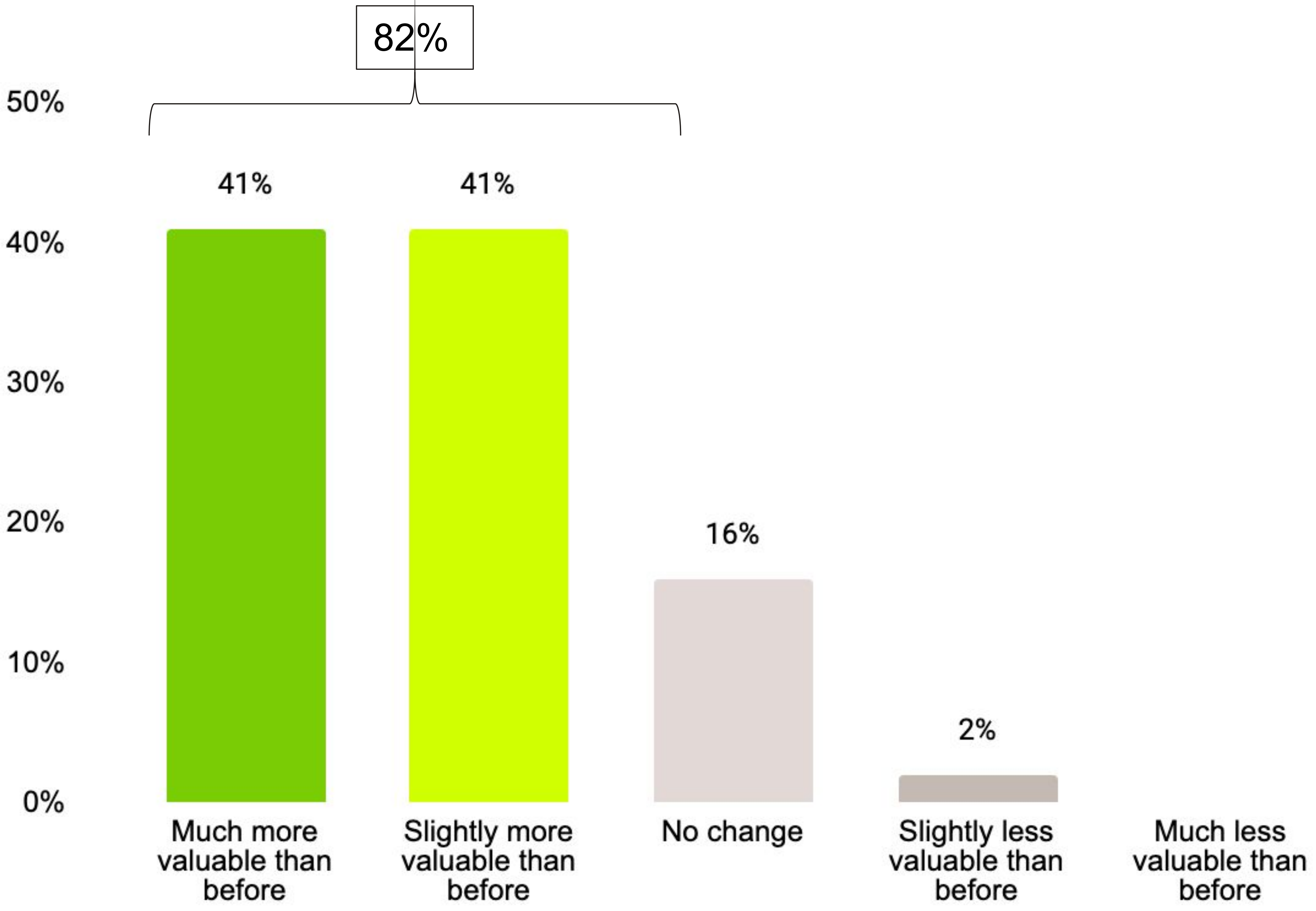
CISOs are viewed as crucial in keeping the business safe (40%), are increasinglyexpected to have an in-depth understanding of all areas of IT (39%), and crucial inkeeping members of staff safe (38%)



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

Base: 209

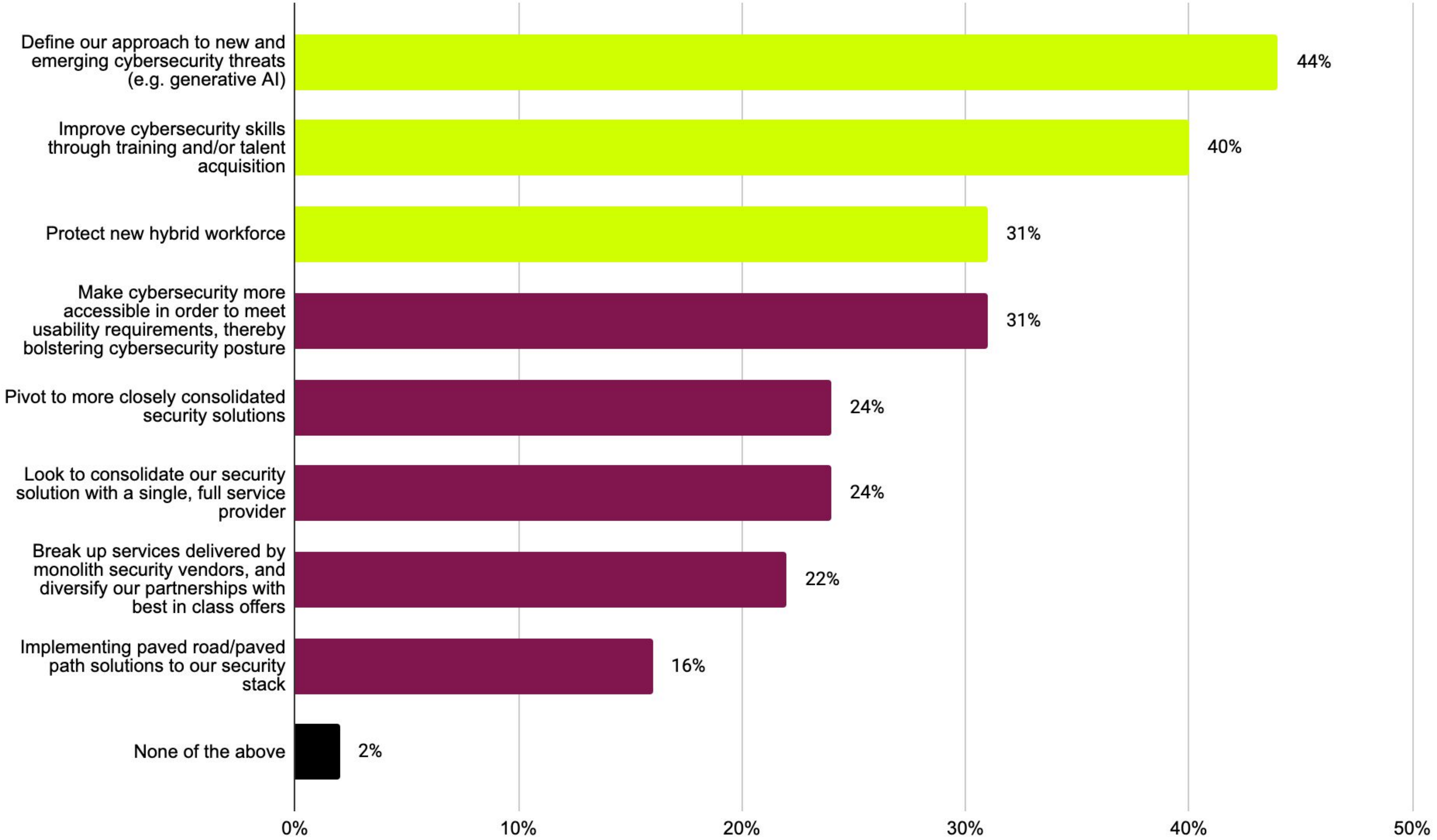
82% of respondents think their cybersecurity programme has become more valuable over the last 12 months



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

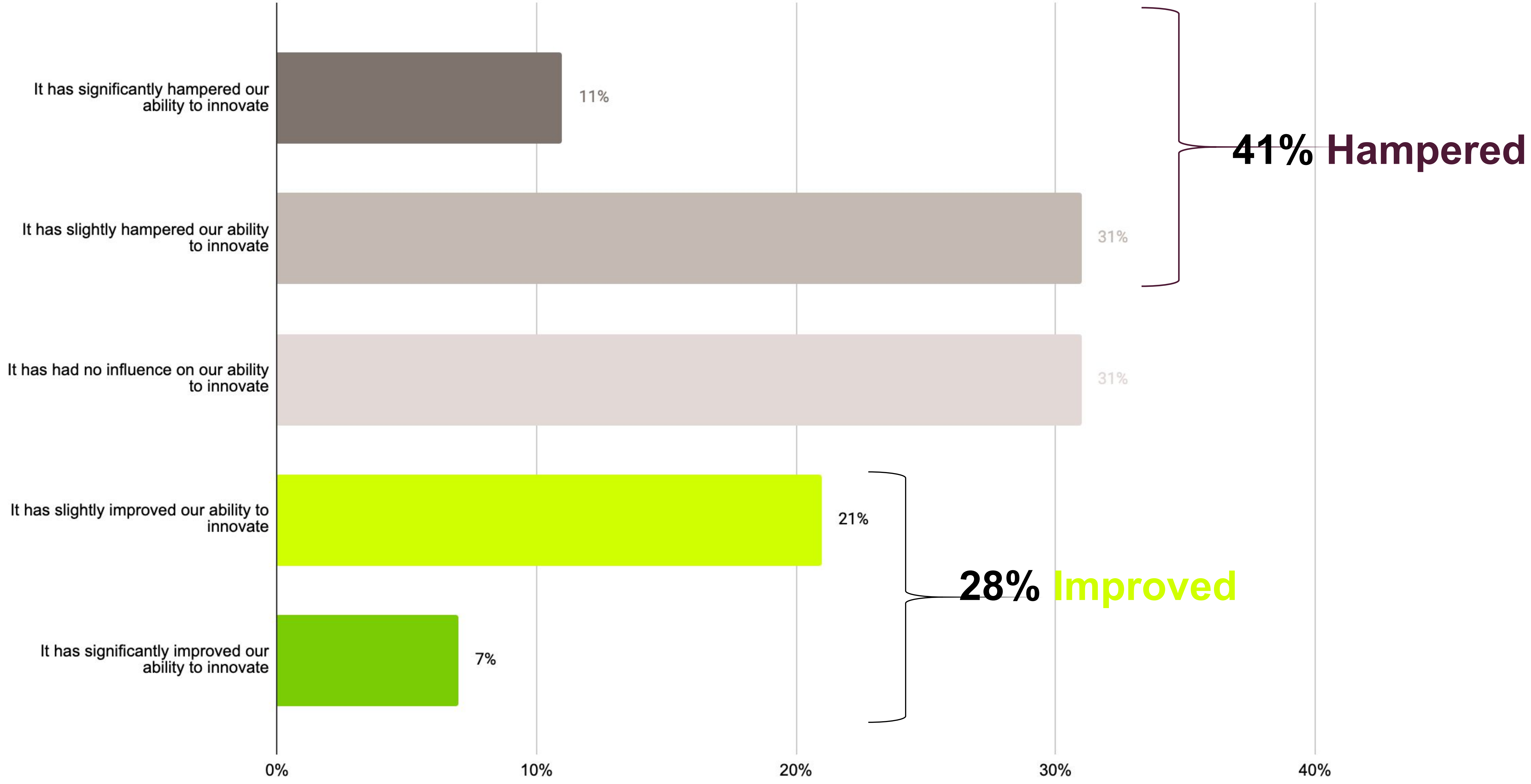
Defining approaches to new and emerging cybersecurity threats (44%) and improving cybersecurity skills through training and/or talent acquisition (40%) are the main security priorities over the next year



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

Base: 209

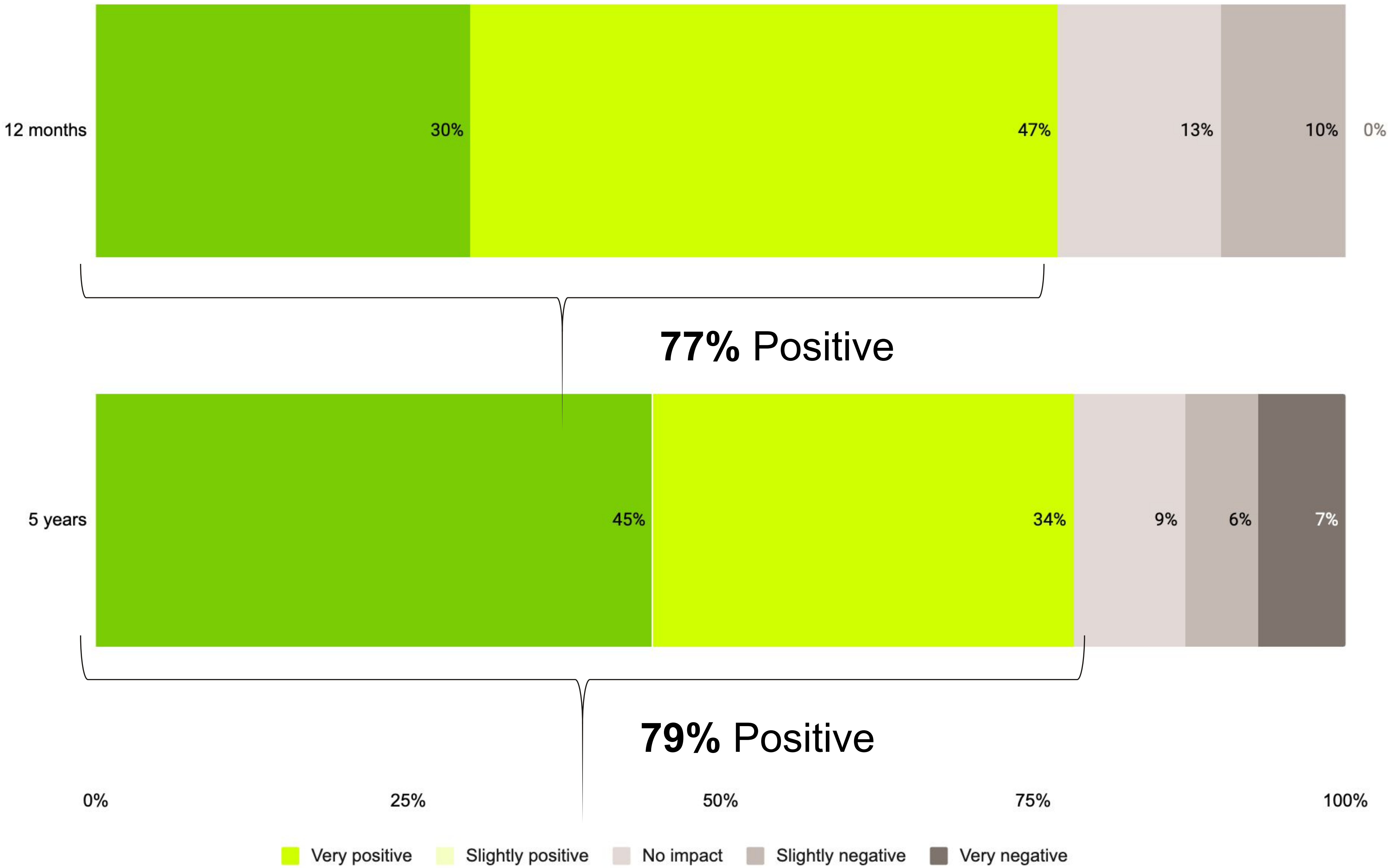
41% say that their organisations cybersecurity strategy has hampered business innovation
Less than a third say it has improved innovation (28%)



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

Base: 209

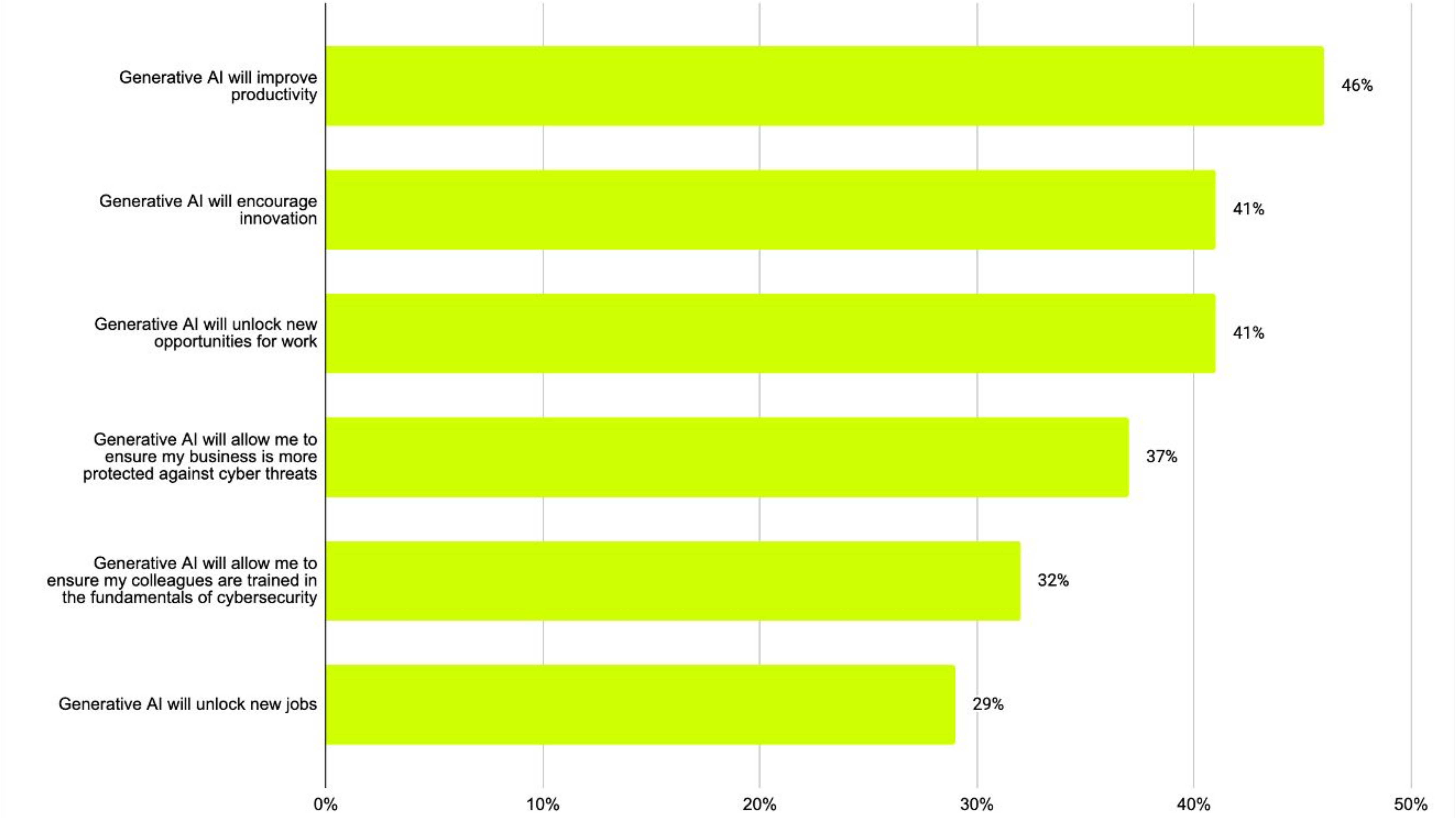
77% predict that Generative AI will have a positive impact on cybersecurity over the next 12 months 79% predict it will have a positive impact over the next 5 years



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

Base: 209

Improving productivity (46%), encouraging innovation (41%) and unlocking new opportunities for work (41%) are the main positive impacts of Generative AI

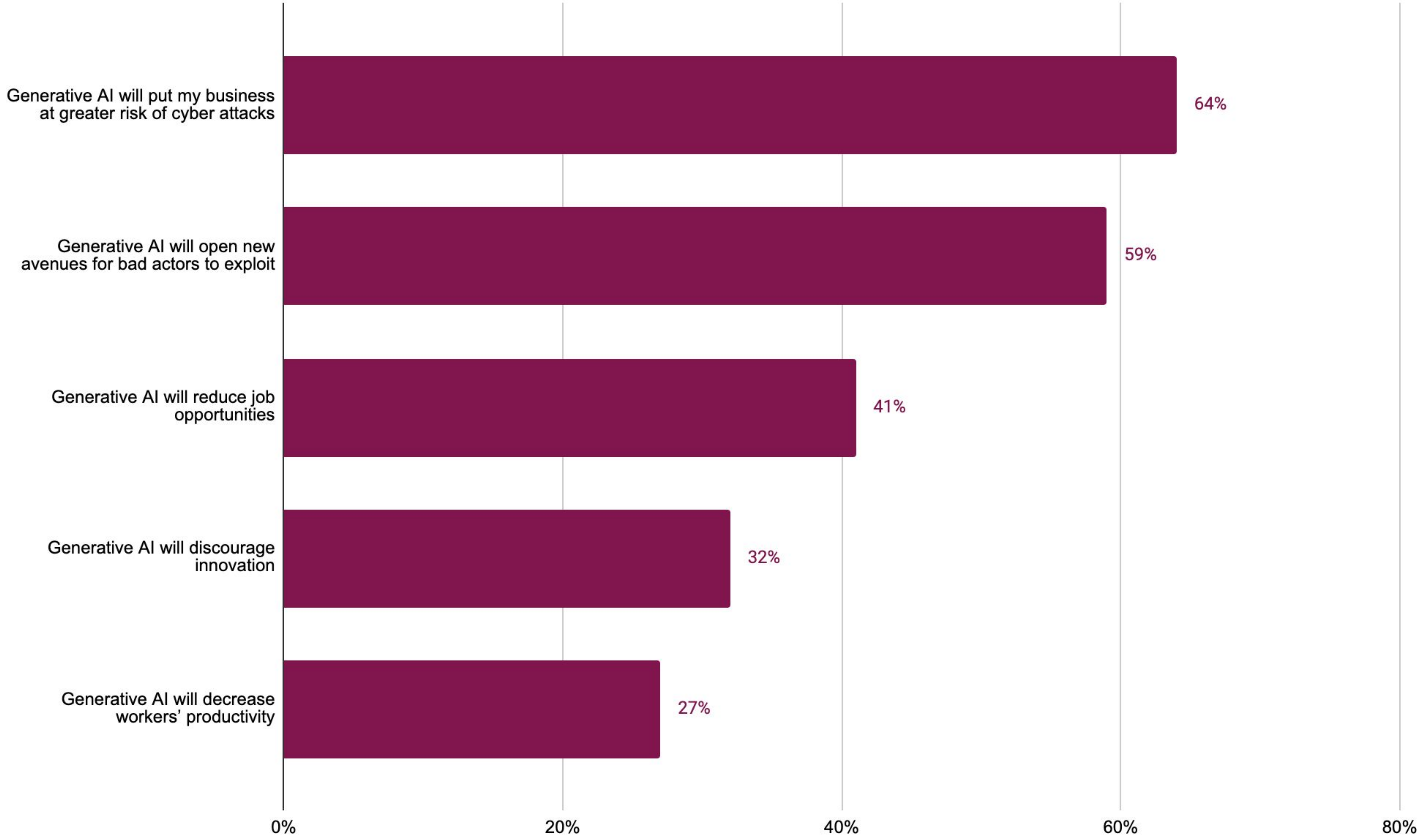


Q17a. You mentioned generative AI will have a positive impact over the next 12 months? Which of the following are the most likely reasons for this? Select all that apply

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

Base : 153*

There are fears that Generative AI will put businesses at greater risk of cyber attacks (64%), or that it will open new avenues for bad actors to exploit (59%)

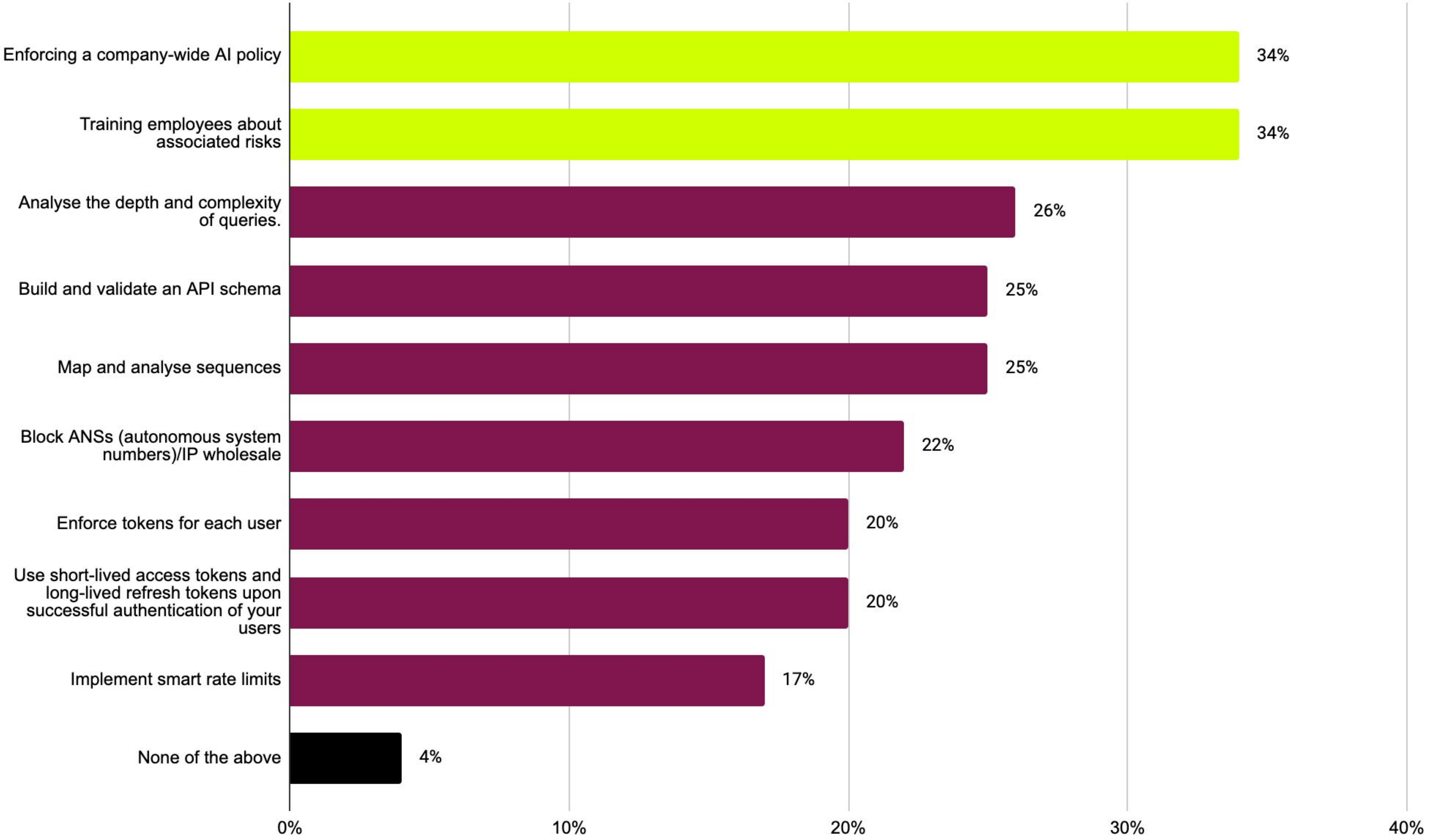


*only asked to those who said generative AI will have a negative impact in the next 12 months

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: 22*

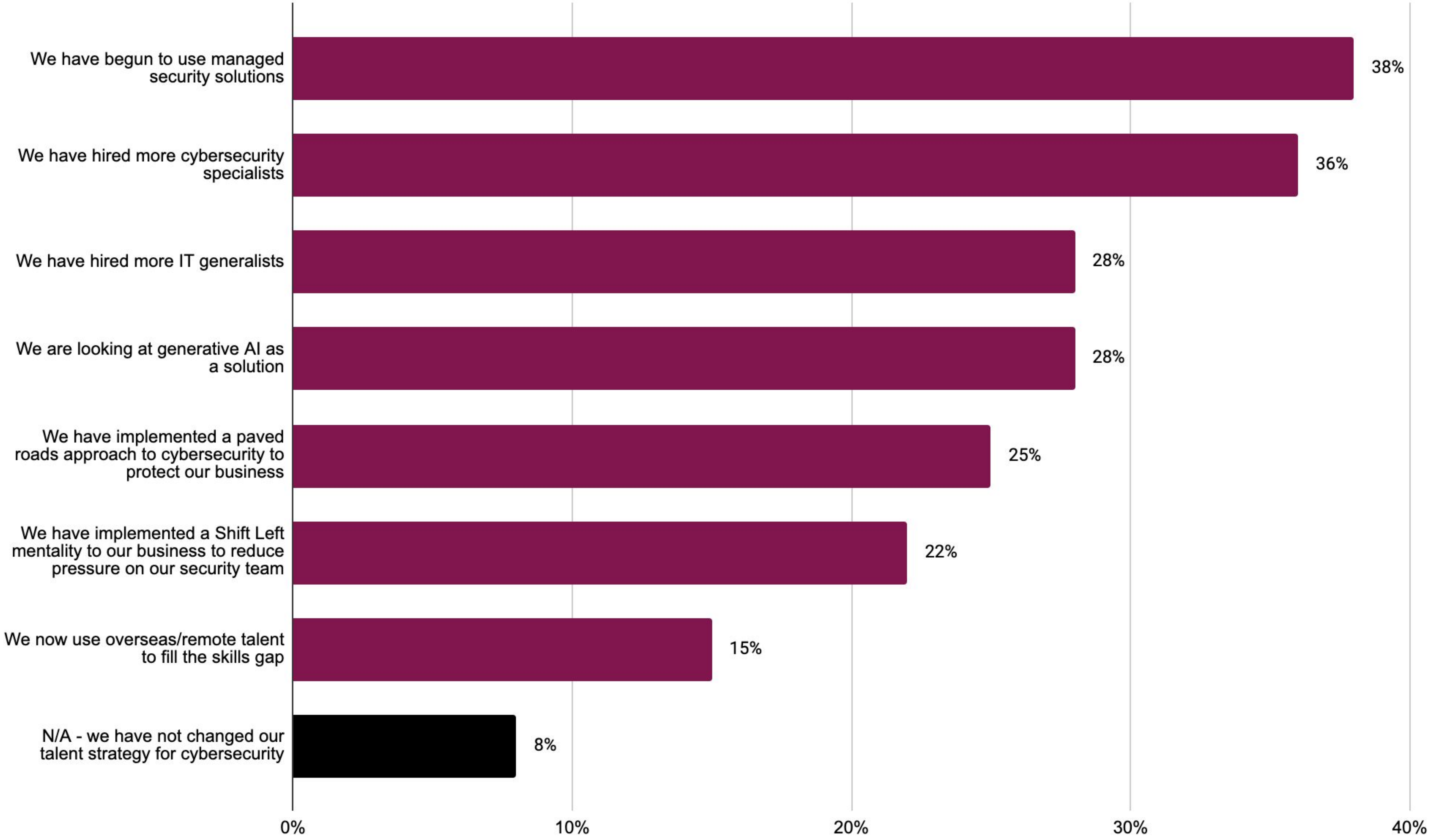
Enforcing a company-wide AI policy (34%) and training employees on the associated risks (34%) are the top two steps companies are taking to mitigate generative AI security threats



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

Base: 209

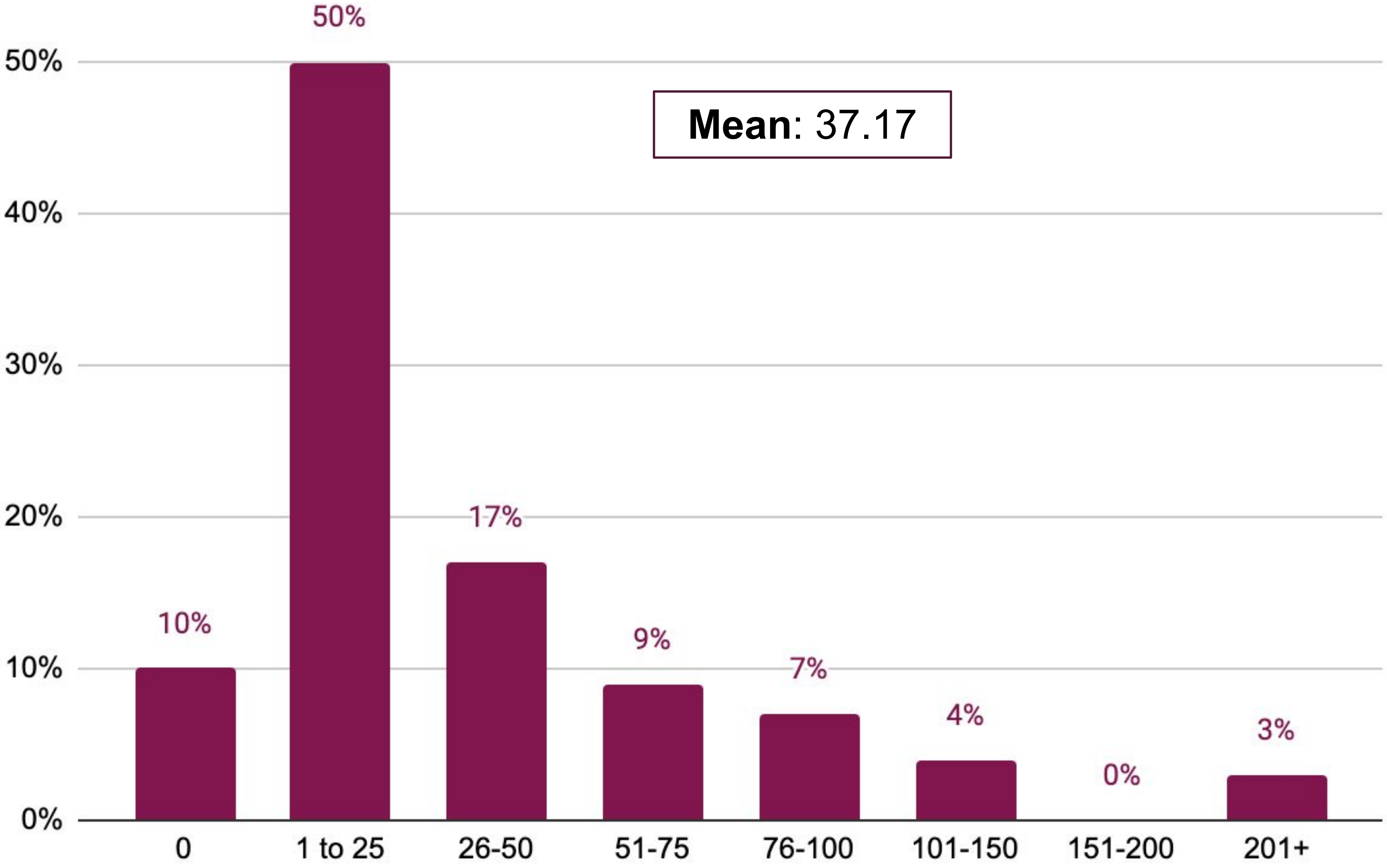
Companies have begun to use managed security solutions (38%) over the last 12 months



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

Base: 209

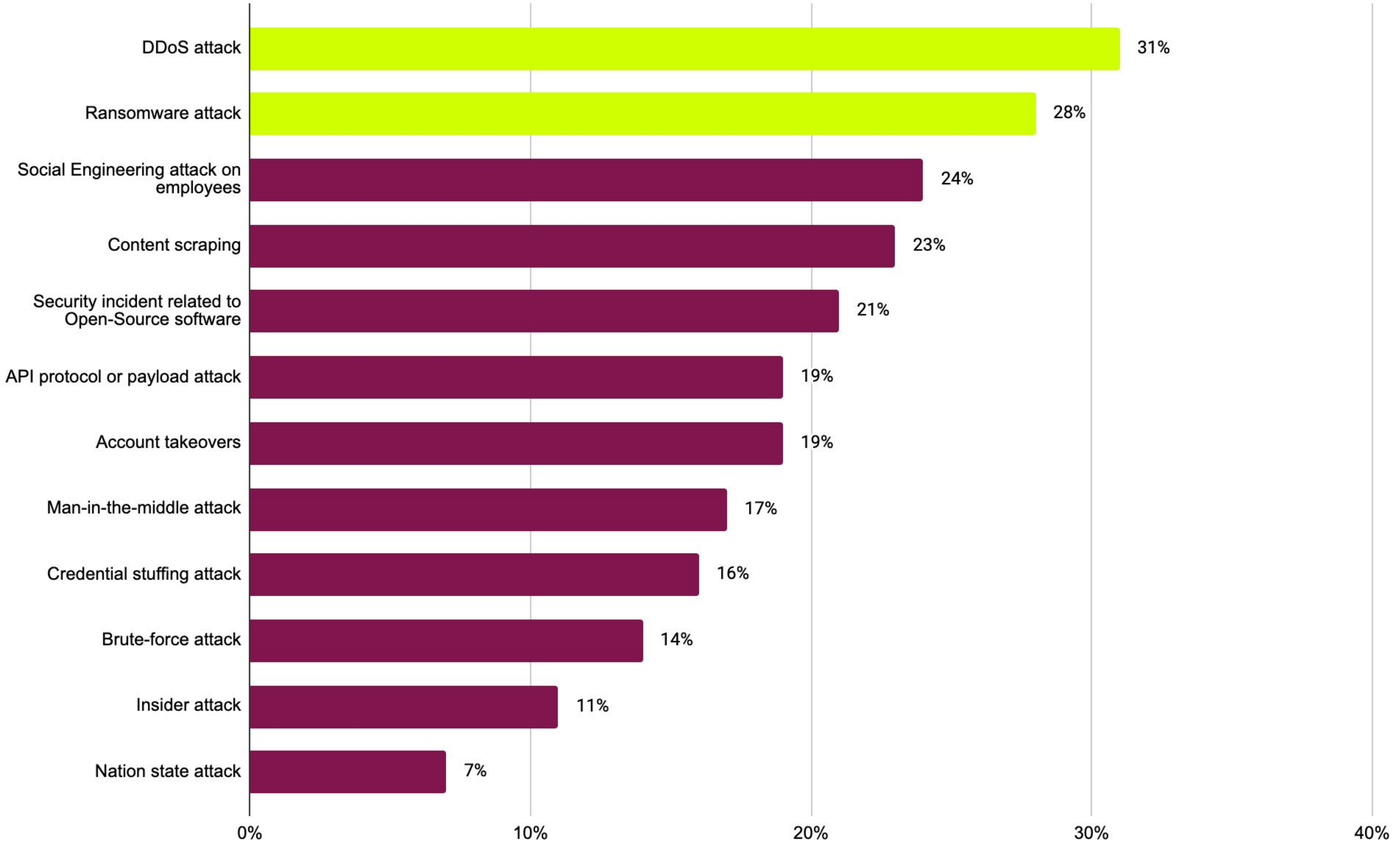
On average, businesses have suffered 37 cyberattacks in the past 12 months



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 (31%) and ransomware attacks (28%)

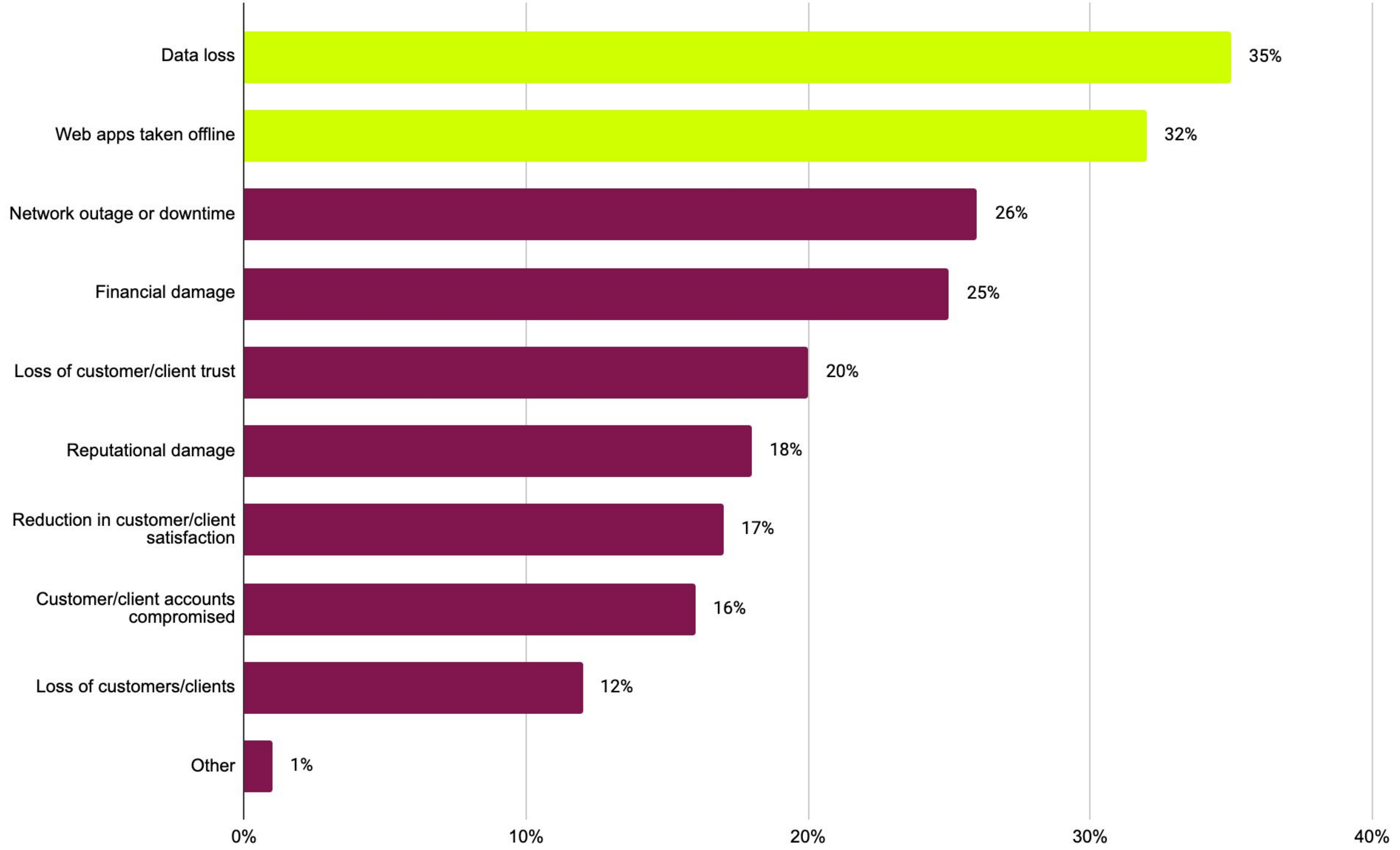


*only asked to those who have experienced a cyber attack

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

Base: 189*

Data loss (35%), web apps taken offline (32%), and network outage or downtime (26%) were the main impacts of cyber attacks

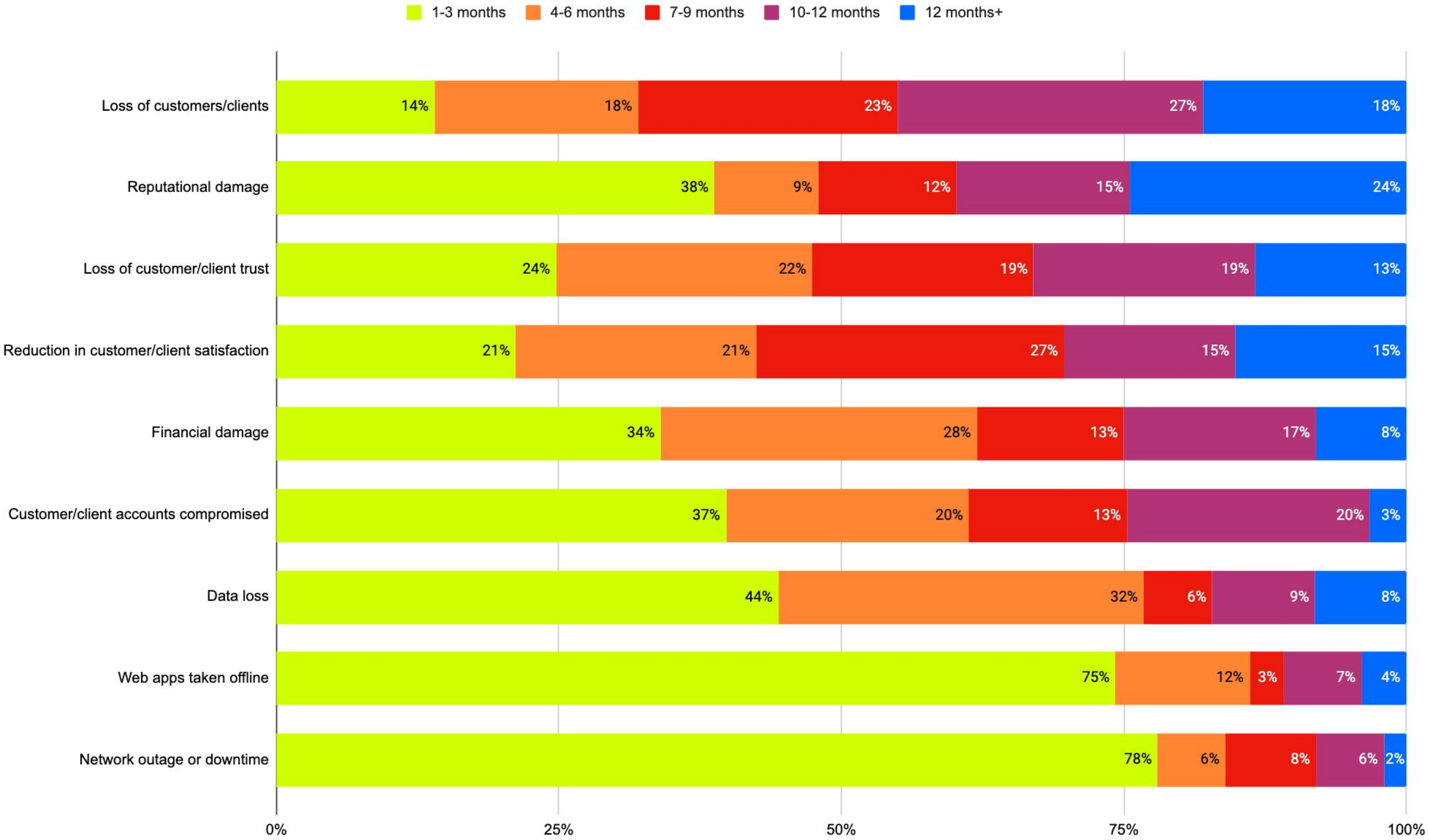


*only asked to those who have experienced a cyber attack

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

Base: 189*

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



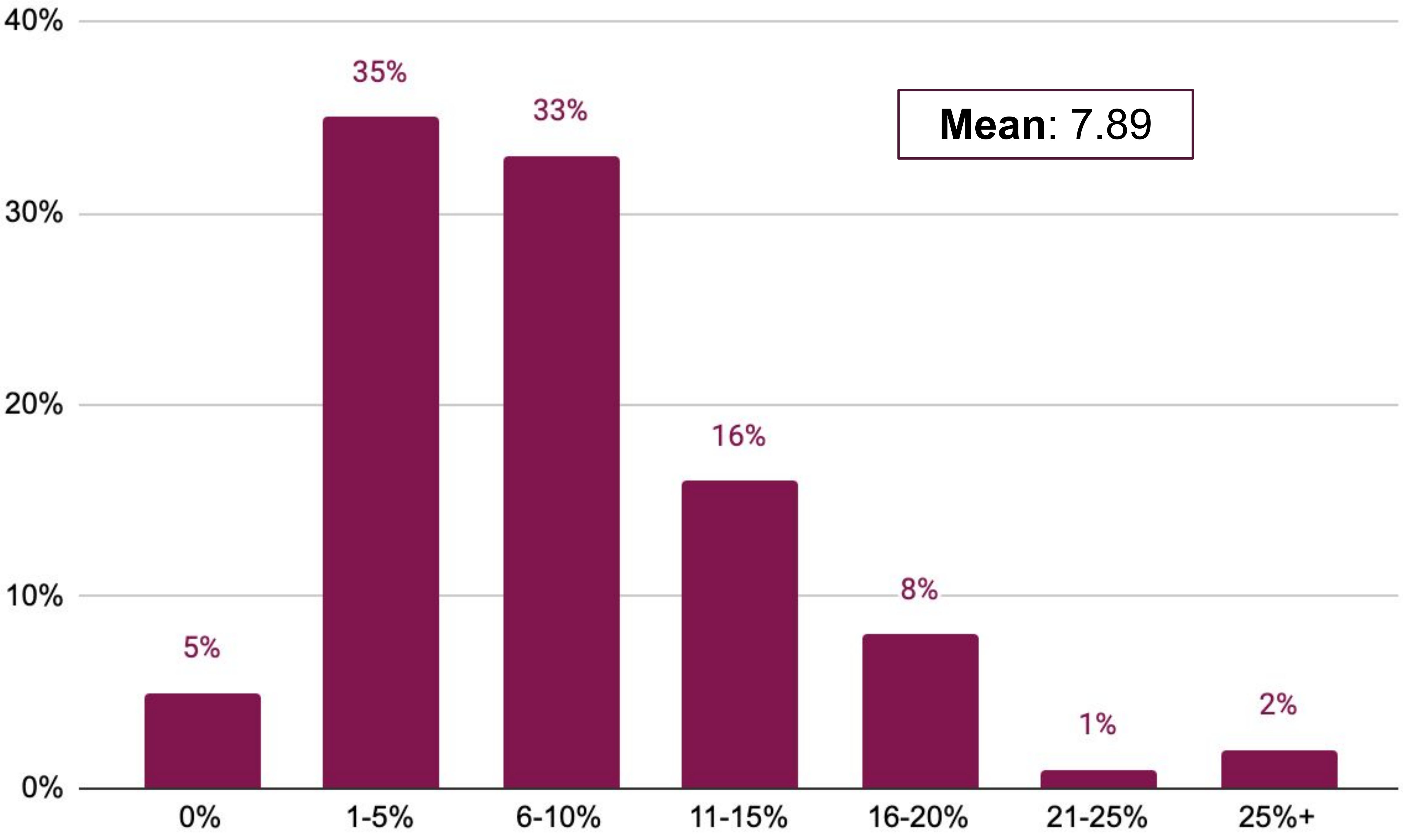
Average no. Months
8.82
7.95
7.75
7.73
6.21
5.96
5.59
3.6
3.44

*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 8% of their annual income as a result of cyber attacks



Mean: 7.89

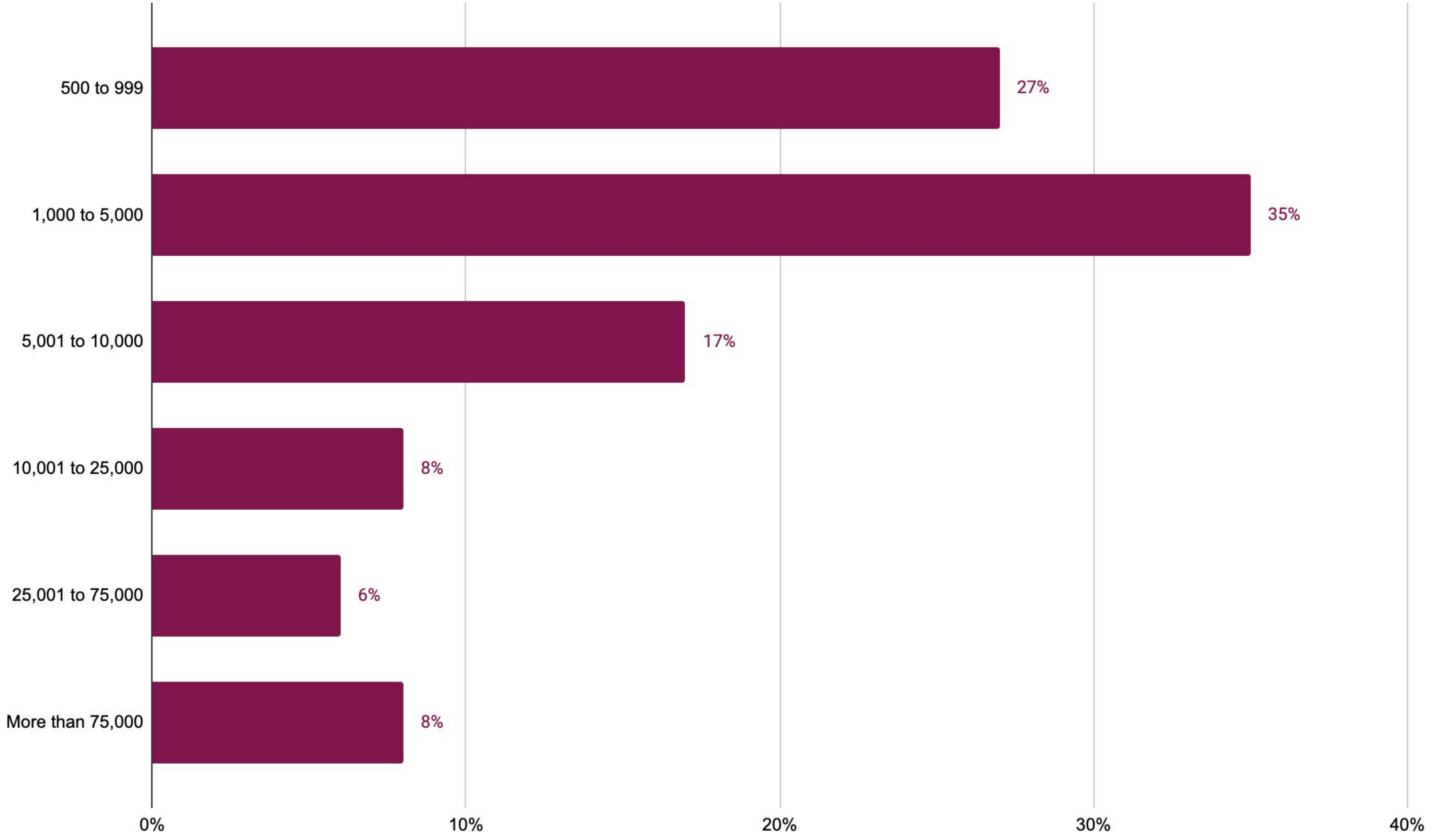
*only asked to those who had experienced each impact at Q22

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: 189*

Demographics

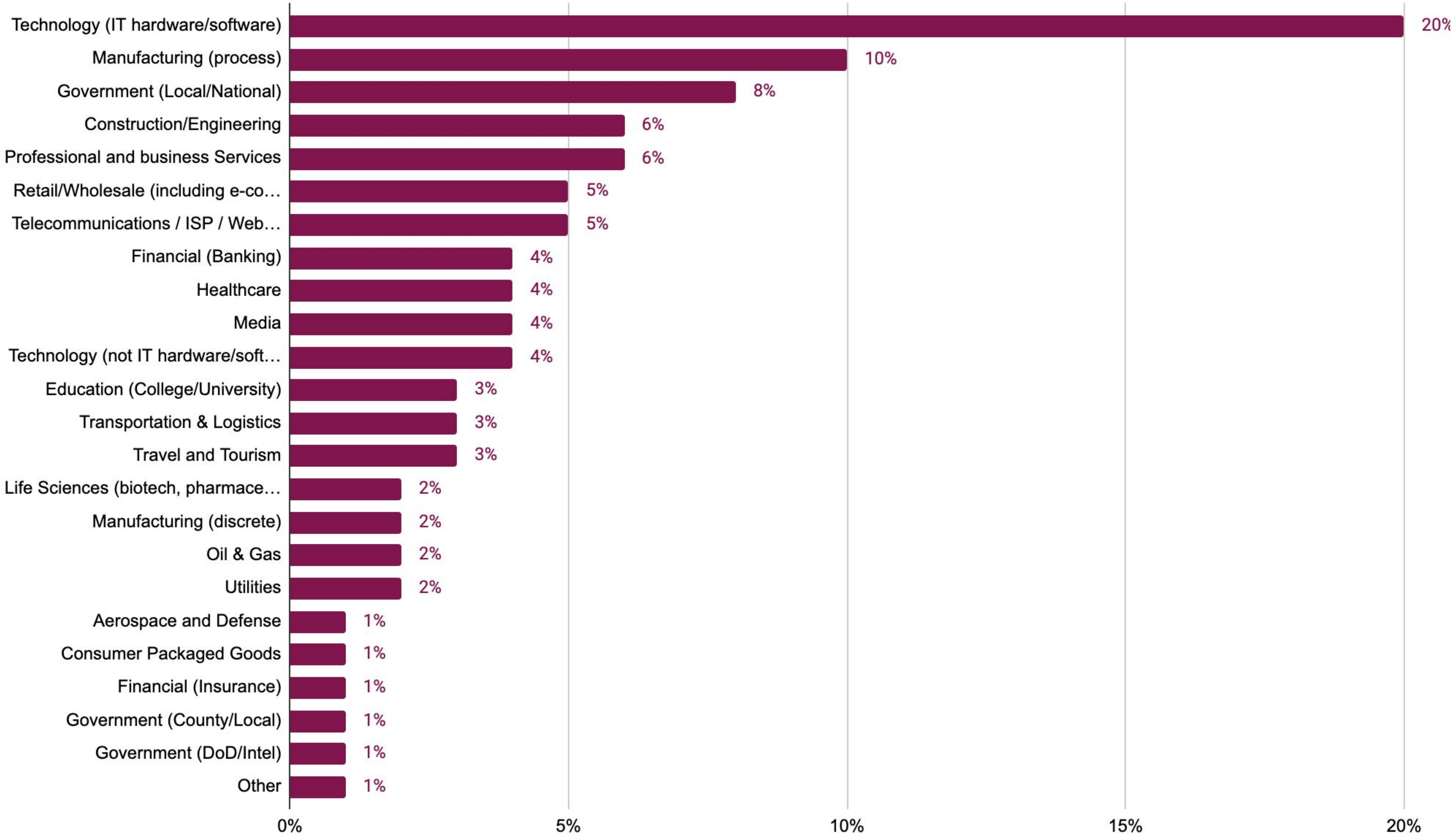
Size



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

Base: 209

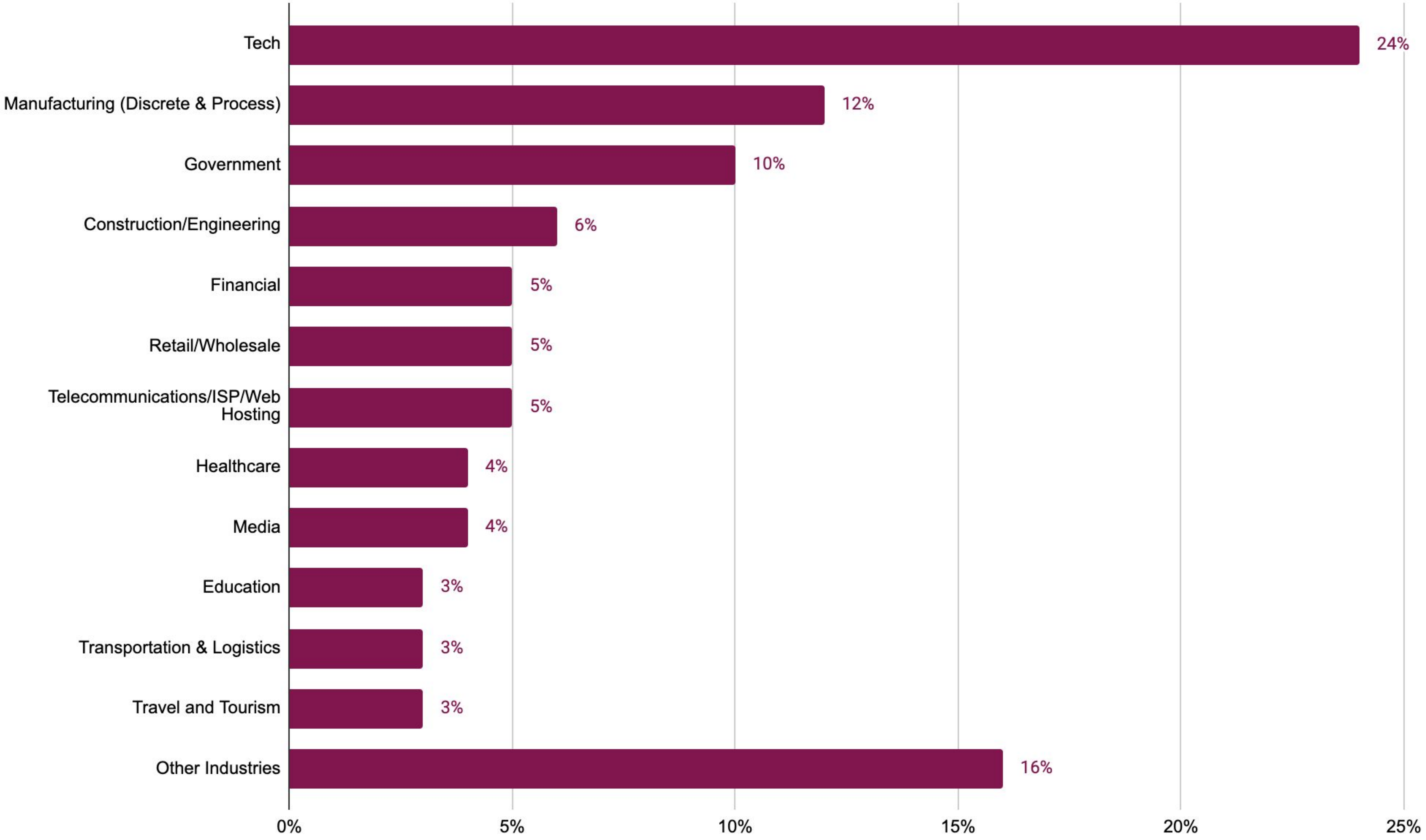
Industry



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

Base: 209

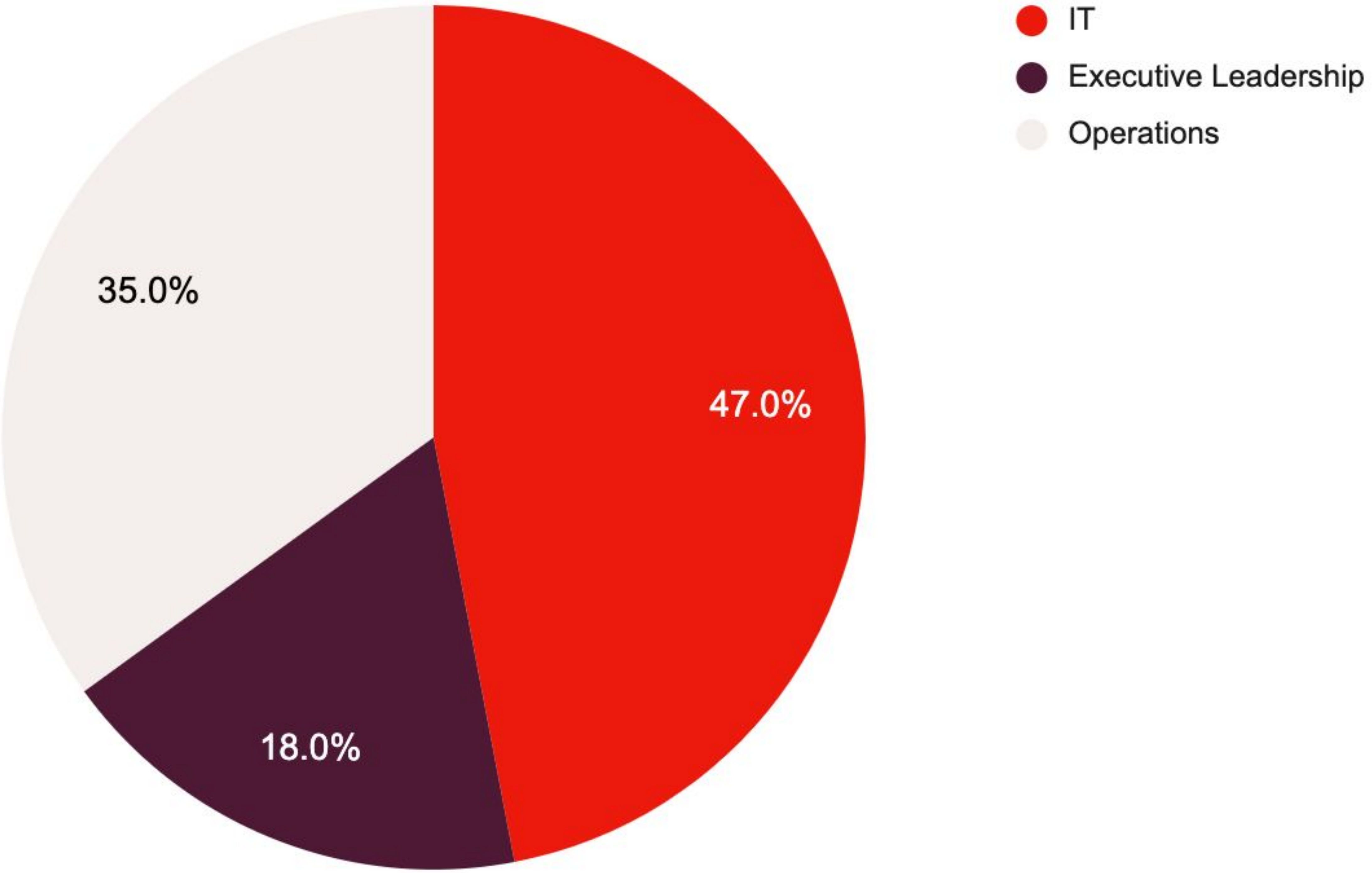
Industry - focus



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

Base: 209

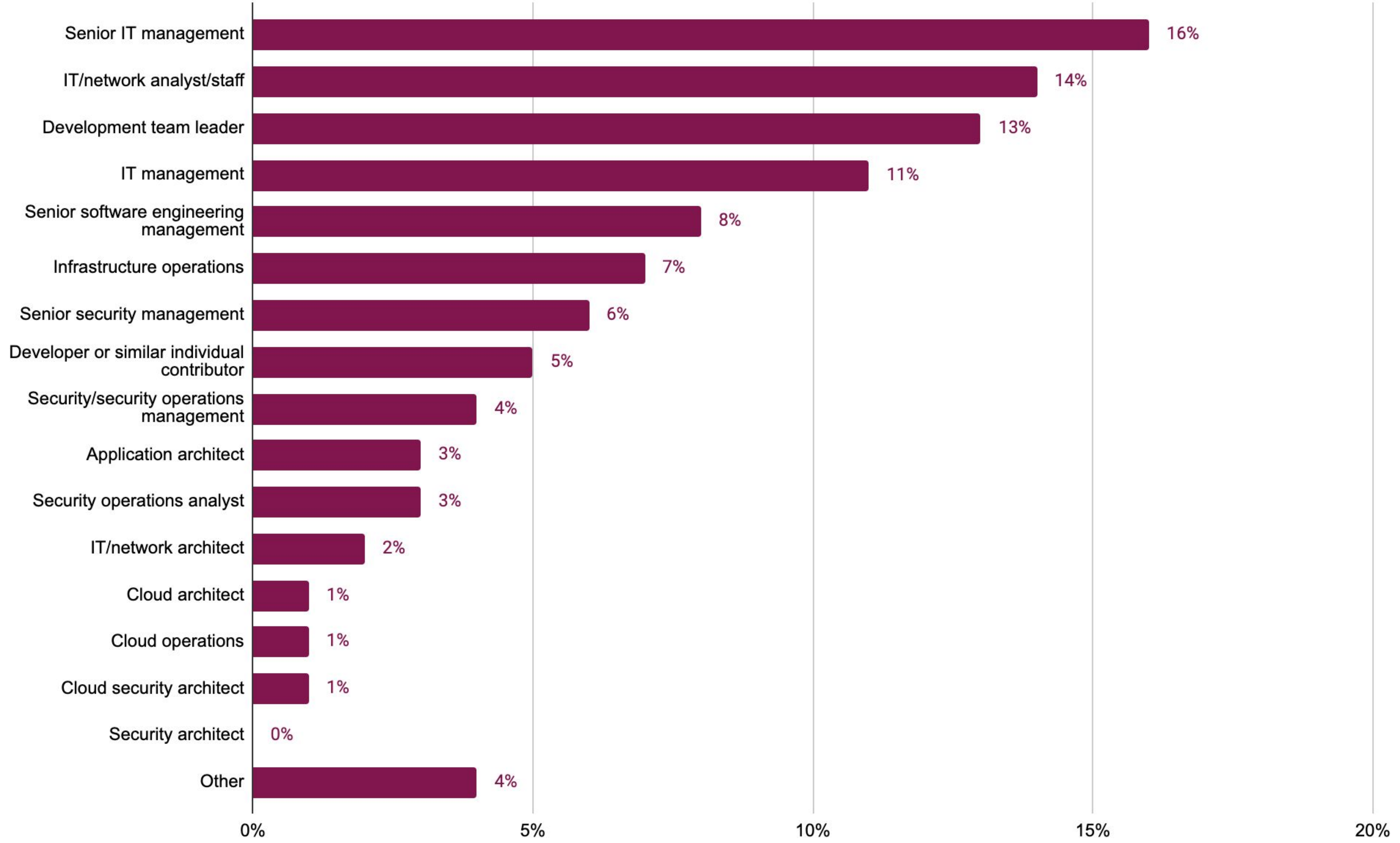
Department



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

Base: 209

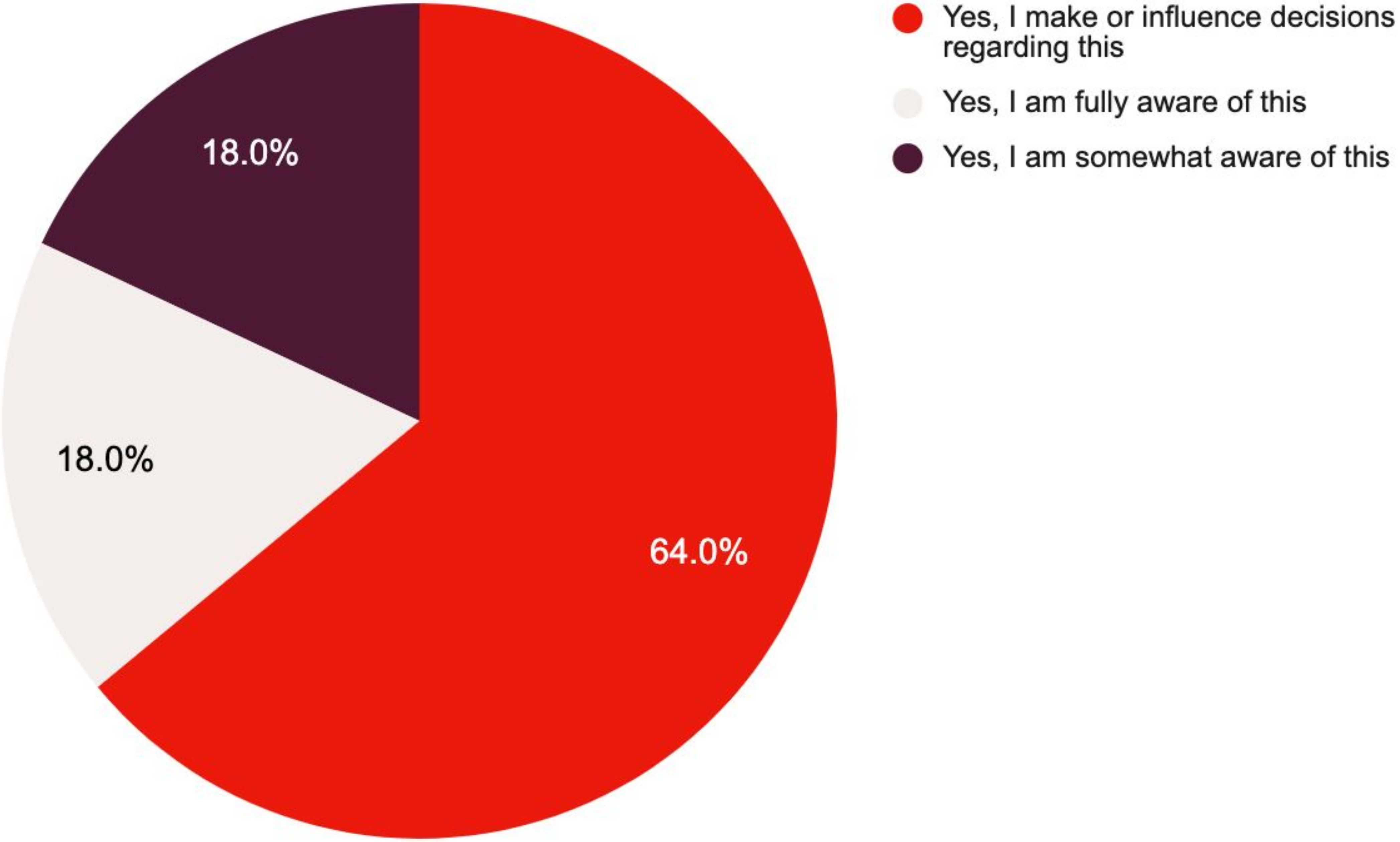
Current responsibility



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

Base: 209

Cyber security decision making



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®