



Fastly Global Security Research 2023

Japan Findings

November 2023

Research conducted by
SAPIO Research



Project overview and methodology

- The survey was conducted among **215** IT Decision Makers (more than 2/3 respondents are fully aware or directly make or influence cybersecurity decisions) in organisations with 500+ employees across Japan. 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 $\pm 6.7\%$ 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

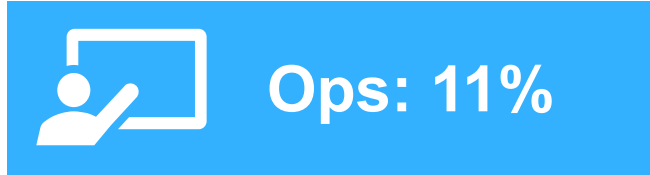
Demographics

Total respondents: 215

Country of residence



Department

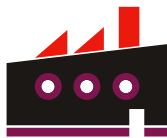


Size of company

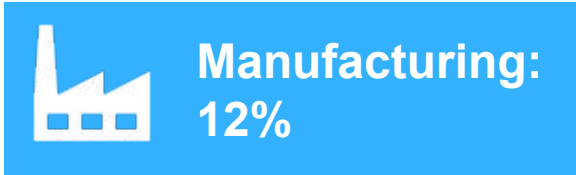


# of employees	250 - 499	500 to 999	1,000 to 5,000	5,001 to 10,000	10,001 to 25,000	25,000 to 75,000	75,000+
% of respondents	-	22%	40%	14%	12%	7%	6%

Industry



Company sectors – top 3:



Decision making (cyber security)



- 50% make or influence cybersecurity decisions
- 19% are fully aware of decisions regarding cybersecurity
- 32% are somewhat aware of cybersecurity decisions

Key stats

47% predict 'ransomware' as the biggest cybersecurity threat over the next 12 months

On average, businesses lose **7%** of their annual income as a result of **cyber attack**

46% of respondents feel there is gap among the current talent pool in experience with new and emerging technologies / threats such as **generative AI**

Improving cybersecurity skills through training and/or **talent acquisition**, defining approaches to new and **emerging cybersecurity threats**, and pivoting to more closely consolidated security solutions (all **34%**) are the main security priorities over the next year

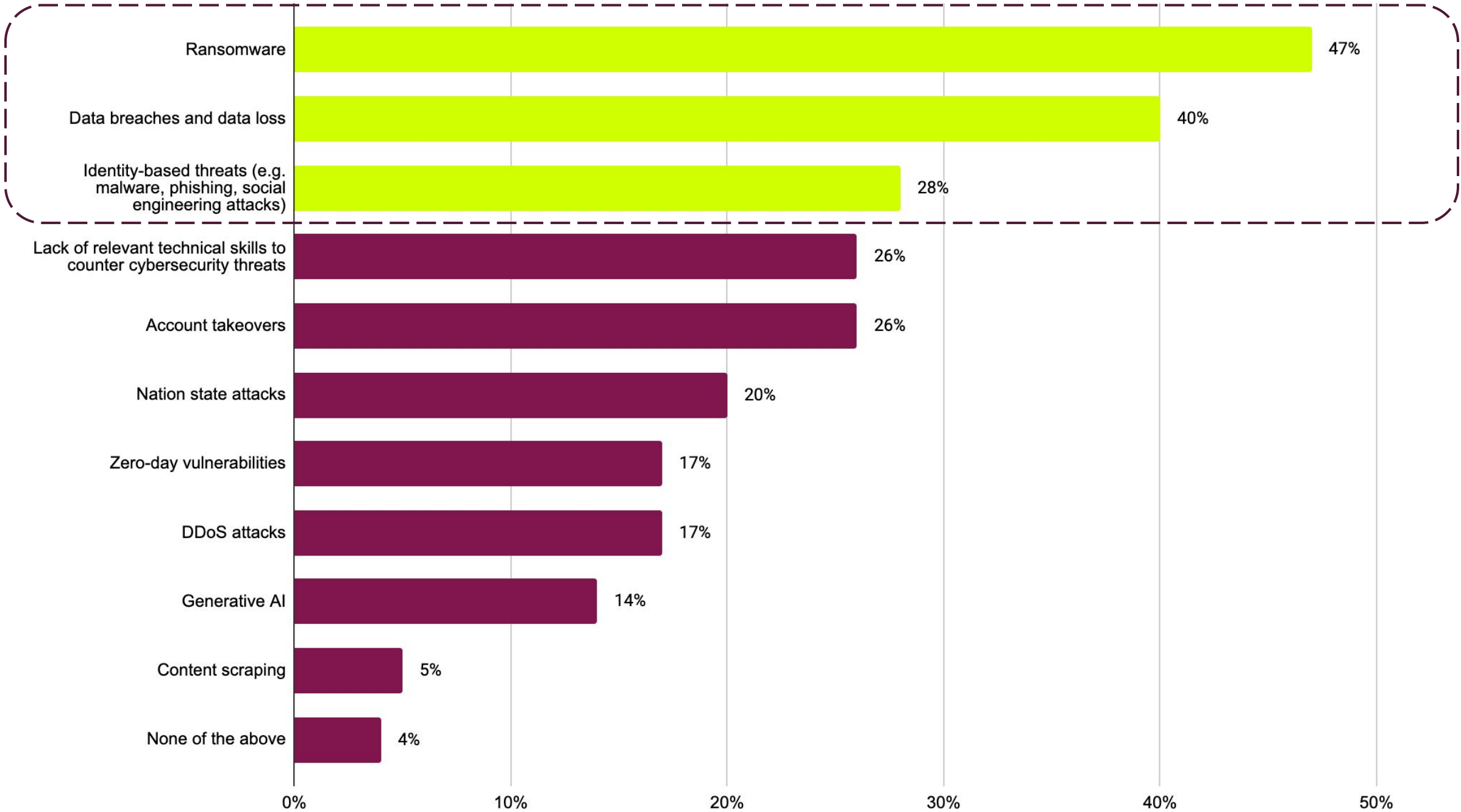
39% say that their organisations cybersecurity strategy has **hampered** business innovation

On average, **59%** of cybersecurity tools are **fully deployed/active**



Main Findings

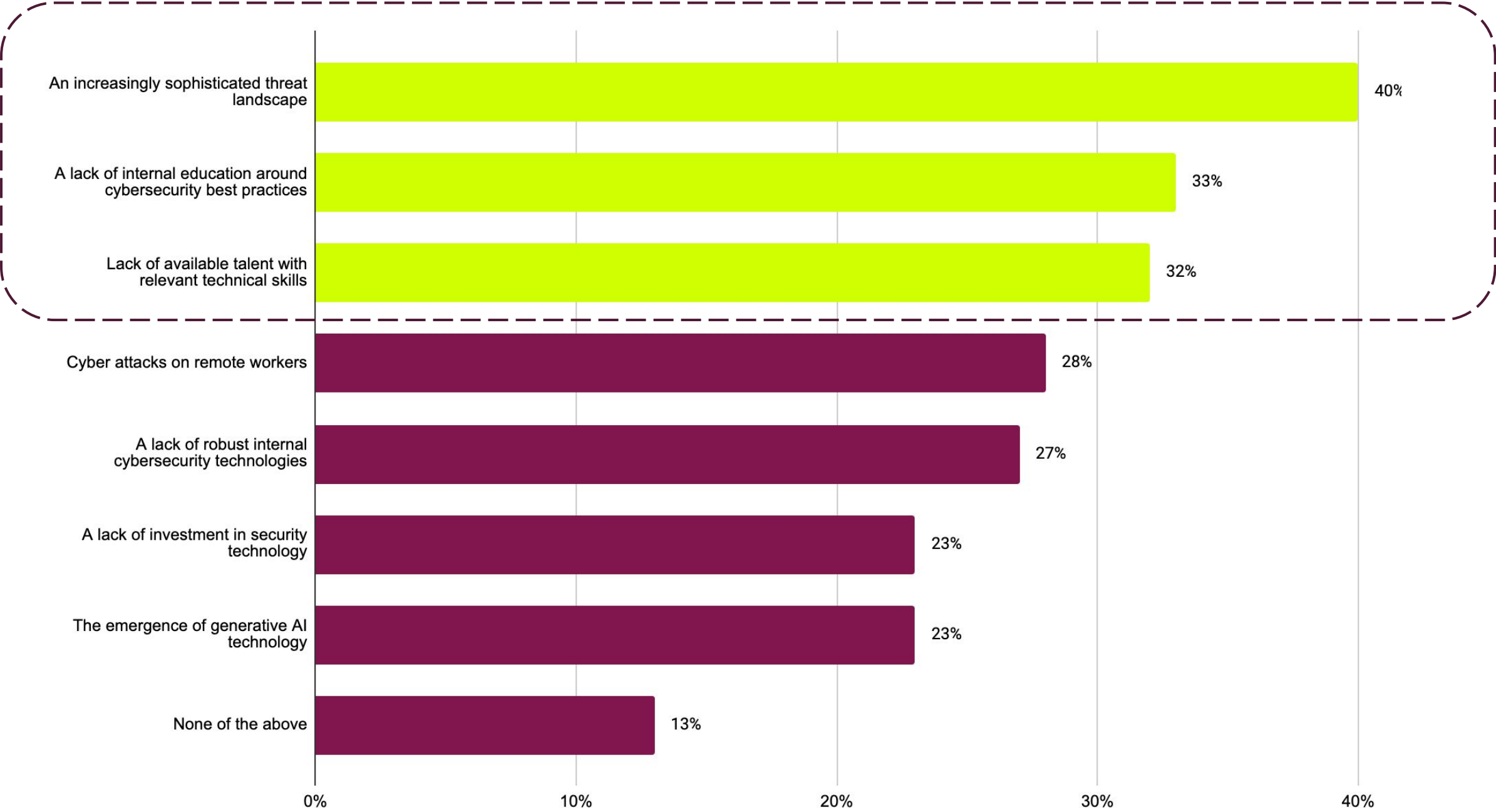
Ransomware (47%), data breaches and losses (40%), and identity-based threats (28%), are viewed as the biggest cybersecurity threats to organisations over the next 12 months



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

Base: 215

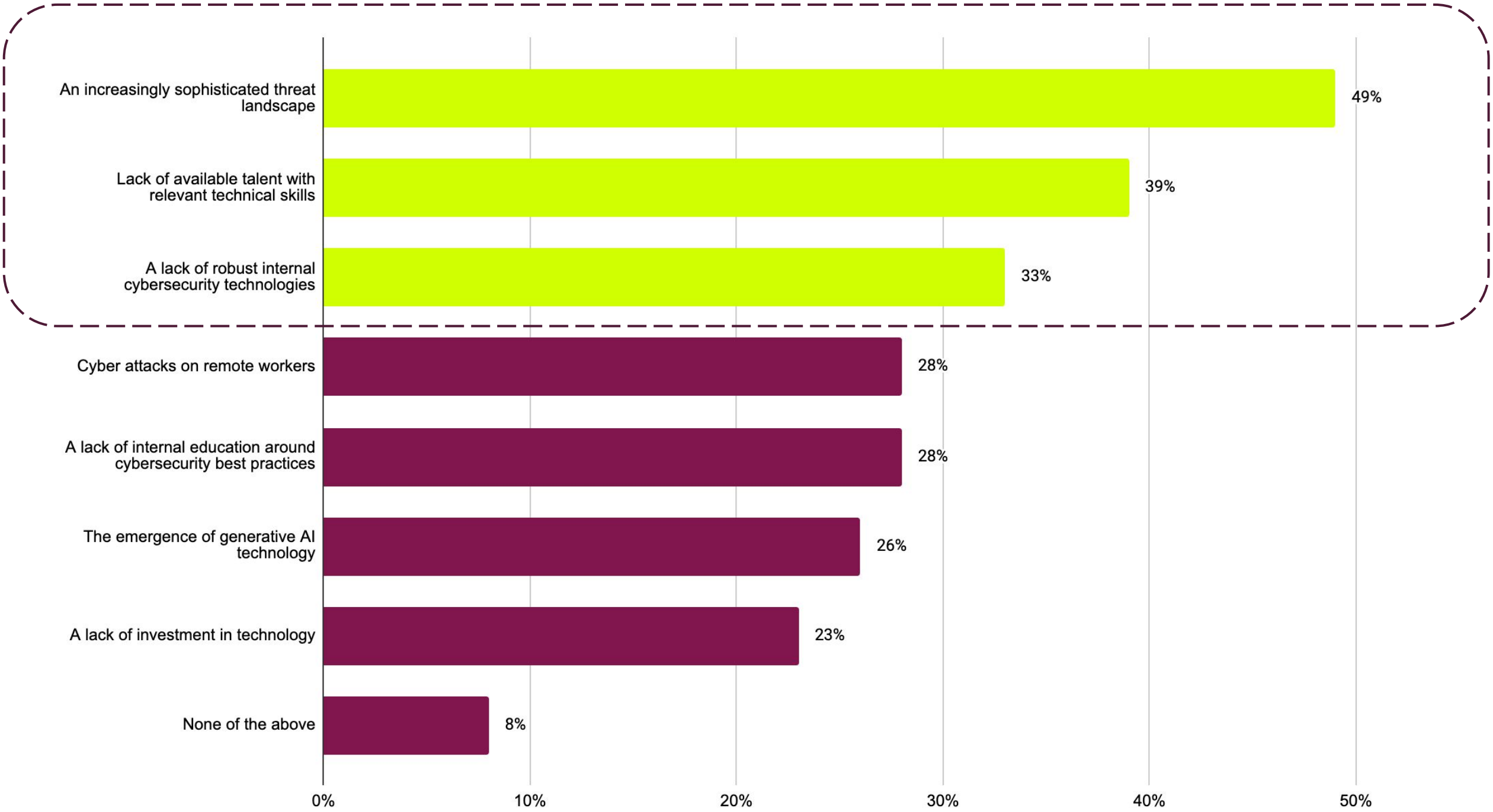
Over the last 12 months, an increasingly sophisticated threat landscape (40%), a lack of internal education (33%) and lack of available talent (32%) were the main drivers of cybersecurity threats'



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

Base: 215

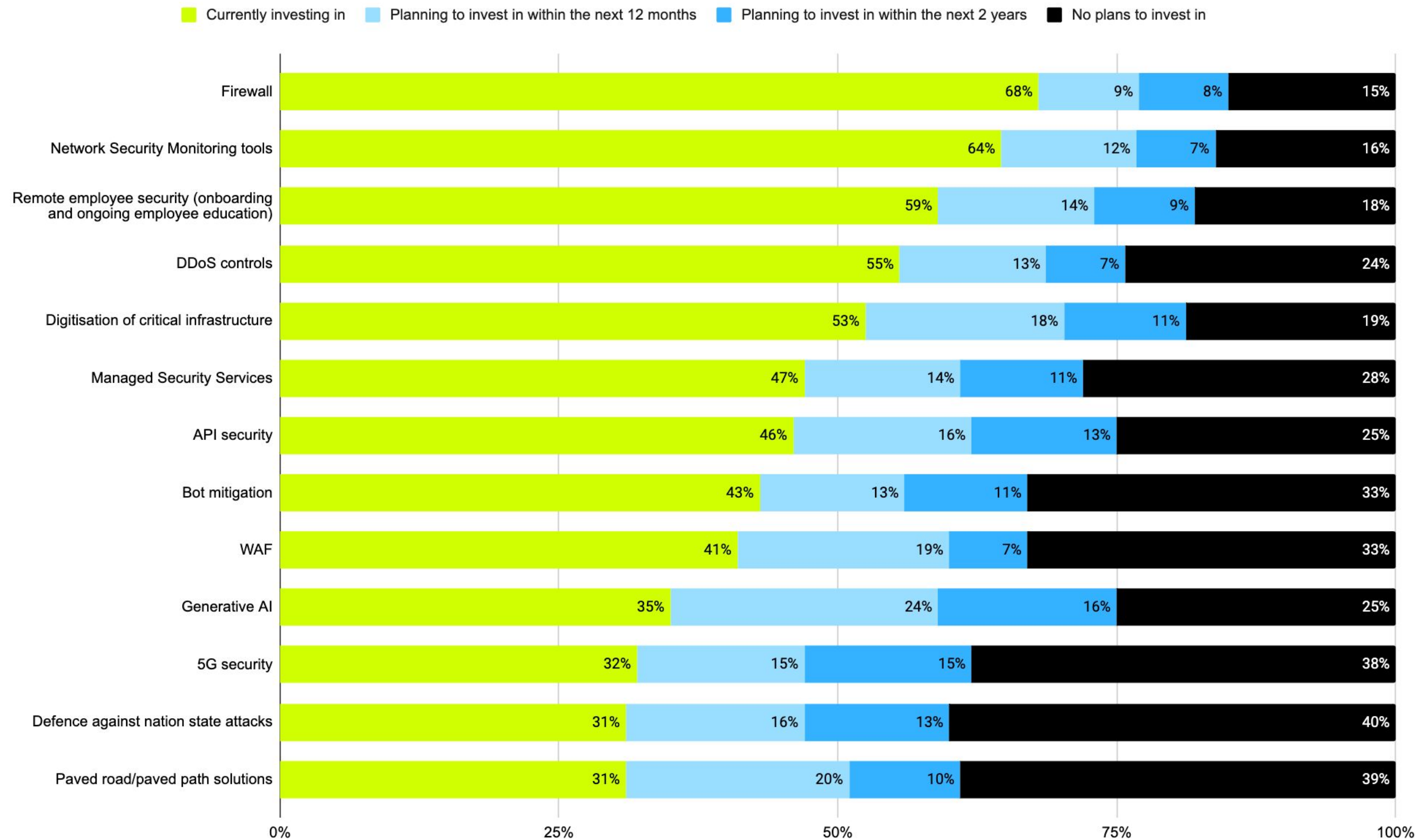
Over the next 12 months, an increasingly sophisticated threat landscape (49%) and a lack of available tech talent (39%) are seen as some of the main drivers of cybersecurity threats



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

Base: 215

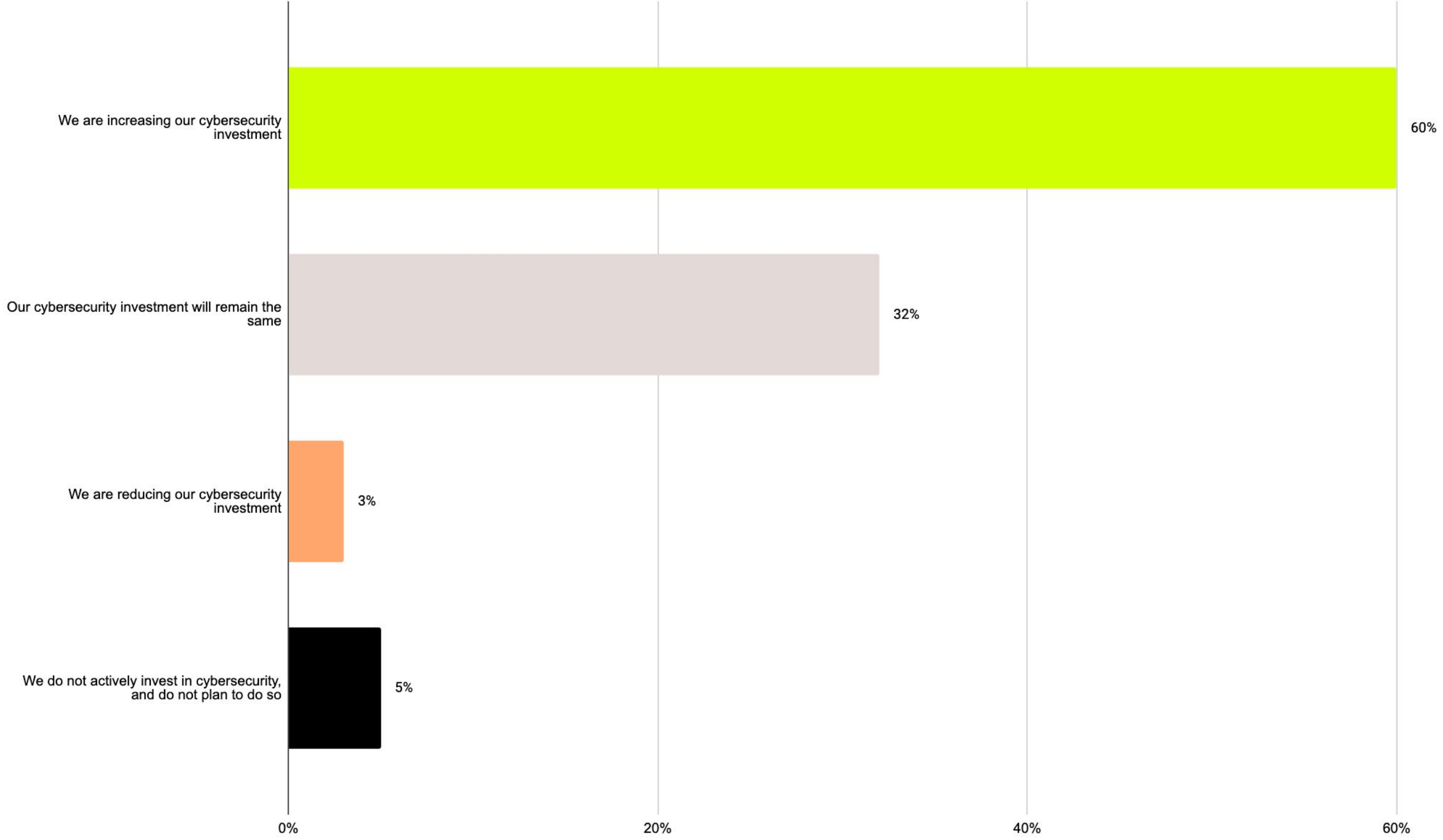
68% are currently investing in 'Firewall' technology, 64% are investing in 'Network Security Monitoring tools' 40% have no plans to invest in defence against nation state attacks



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

Base: 215

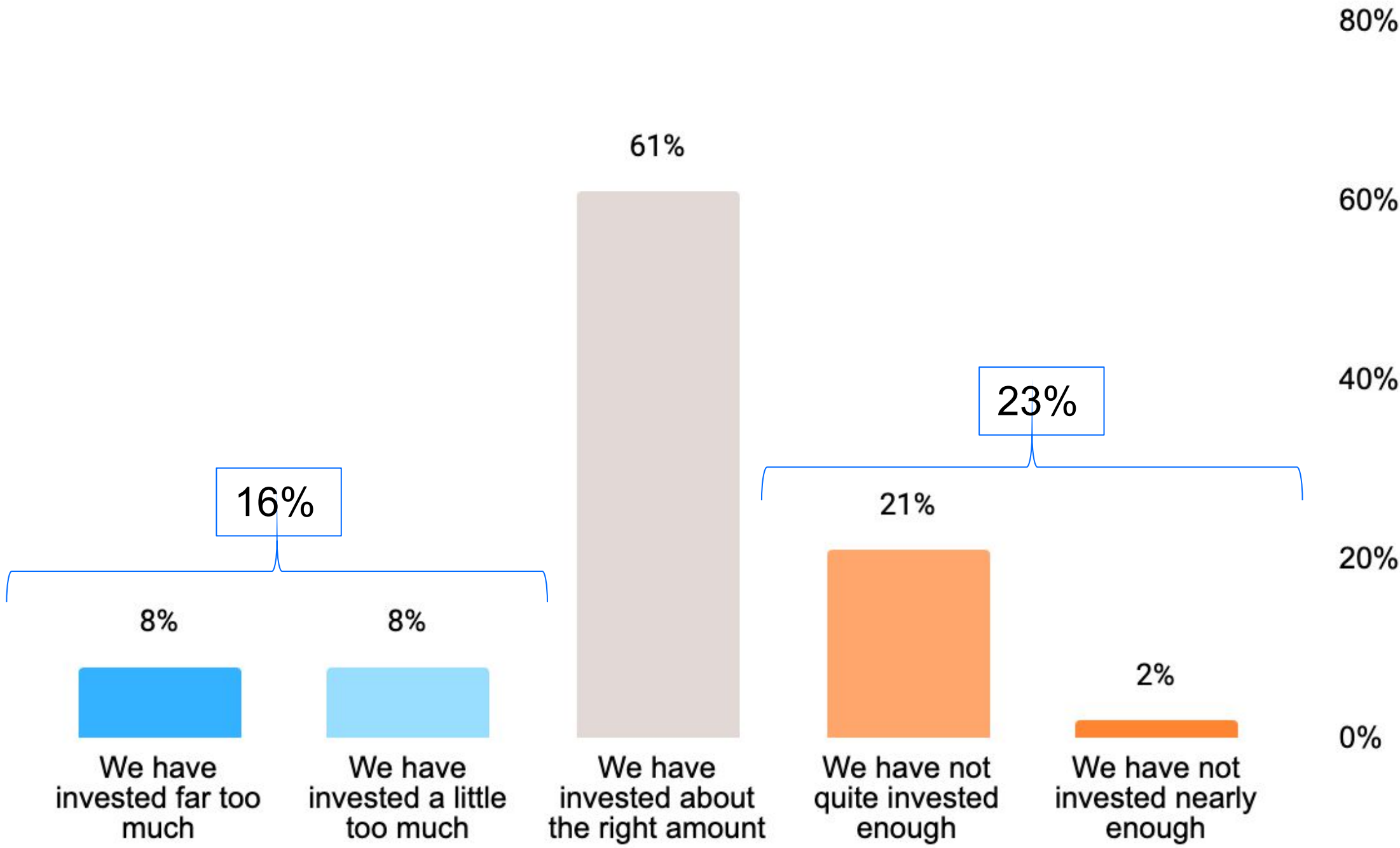
60% of respondents are increasing their cybersecurity investment



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: 215

16% of respondents have invested too much into cybersecurity over the past 12 months
61% say they have invested about the right amount

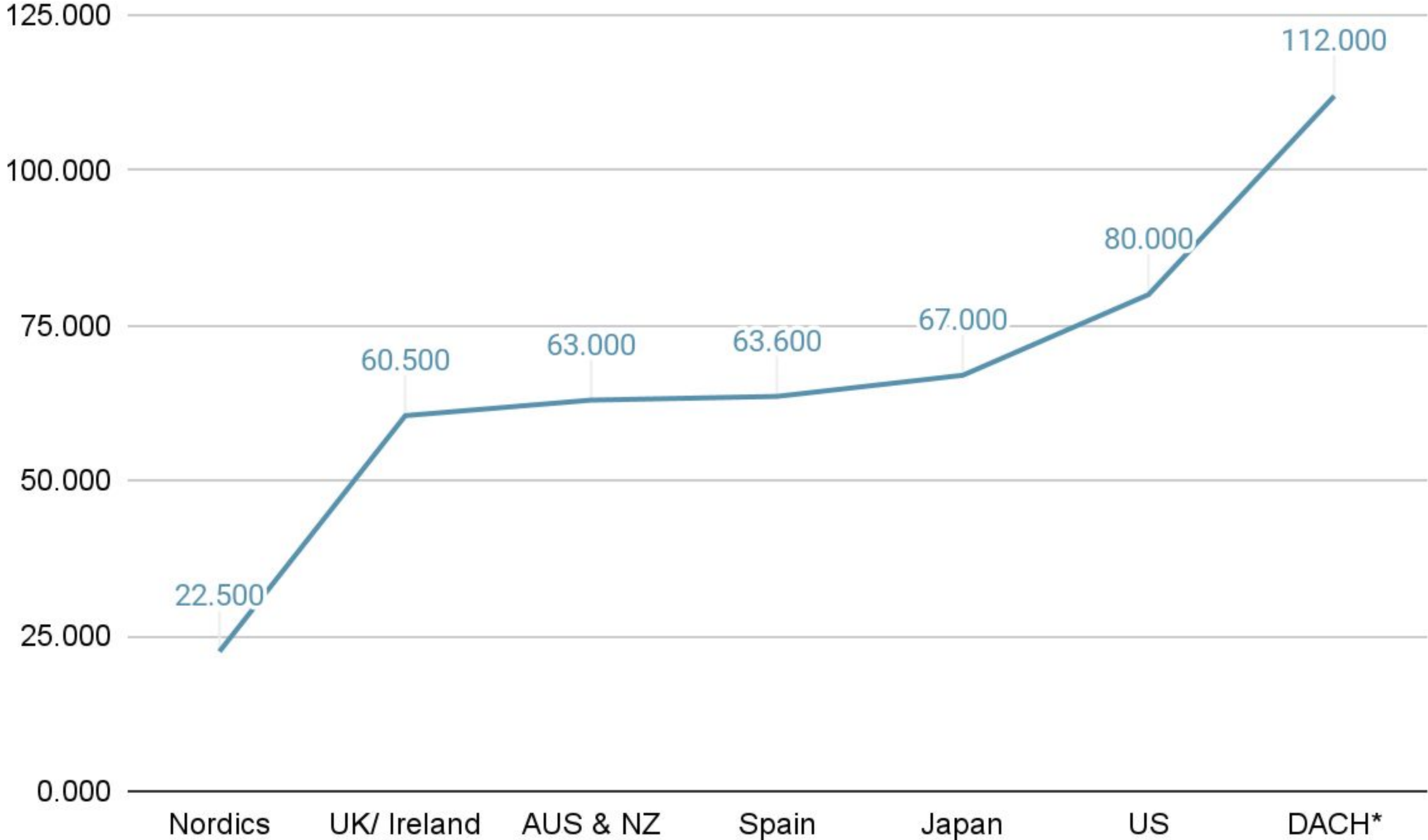


*only asked to those who invest in cybersecurity

Base: 189*

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

On average (median), \$67,000 USD are spent per year on web application and API security control/tools in Japan



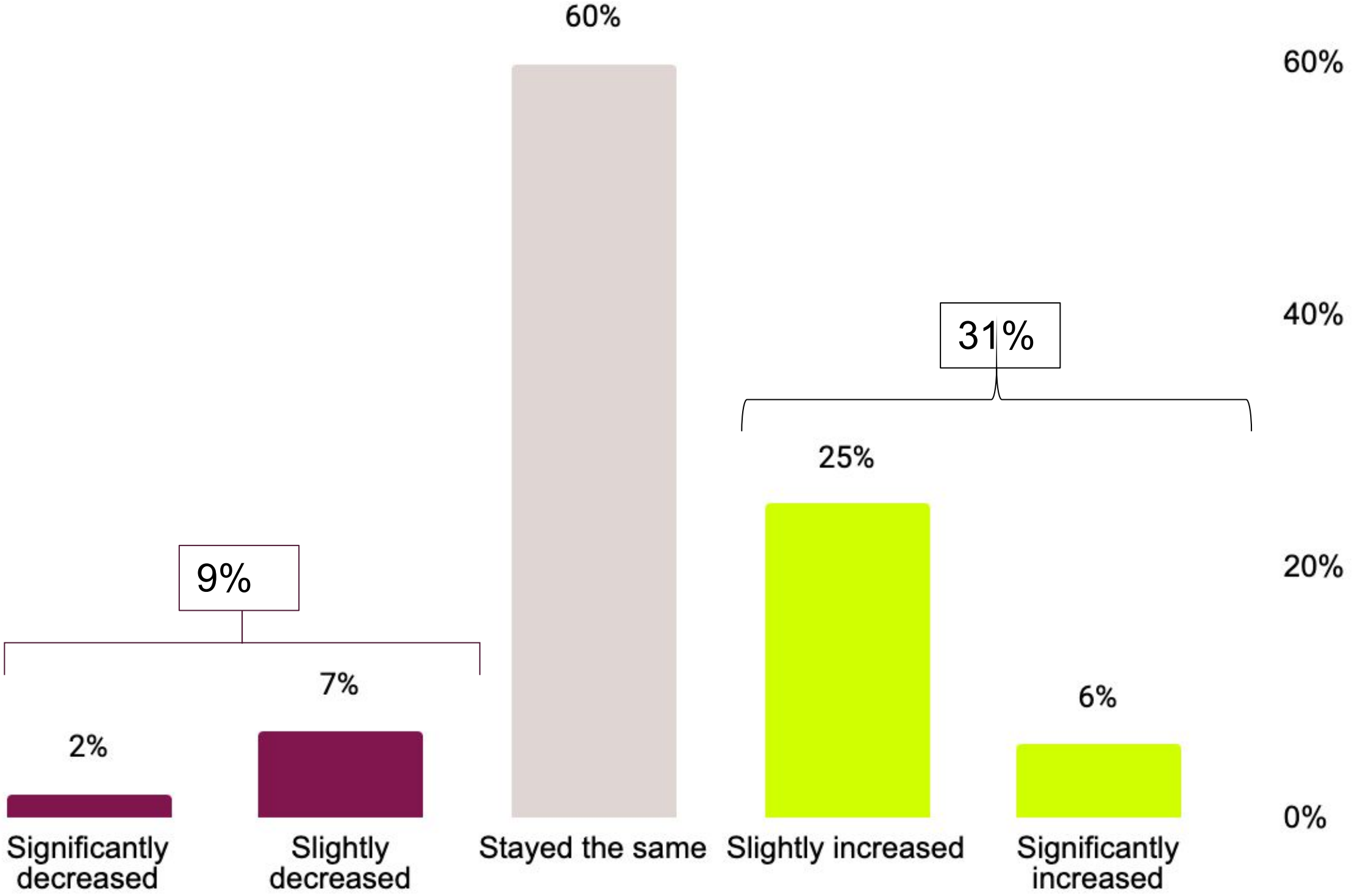
*The sample for DACH countries had a larger proportion of companies with more than 75,000+ employees

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

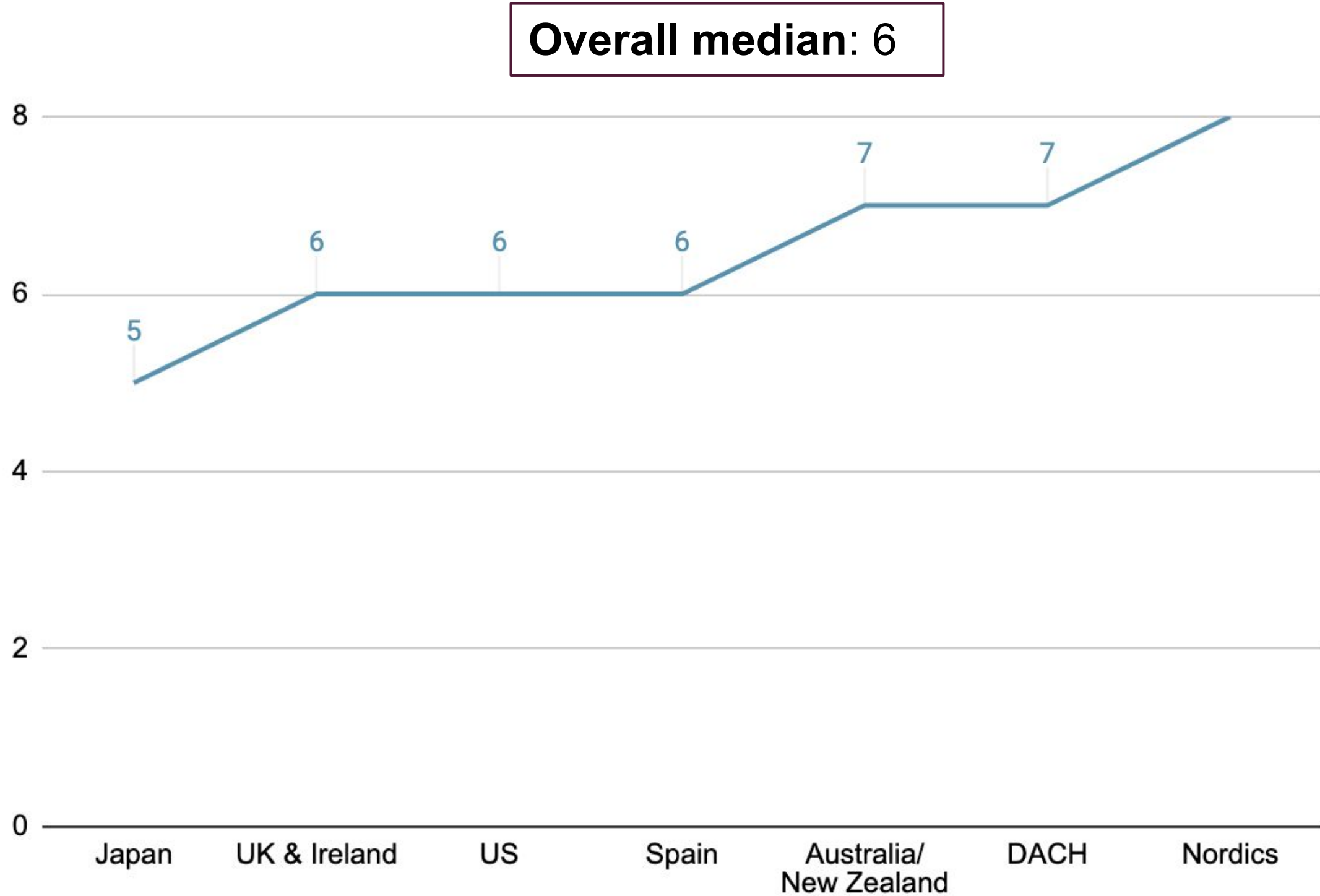
31% of respondents have increased talent spending, with only 9% having decreased talent spending



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

Base: 215

On average (median), organisations in Japan rely on 5 network and application cybersecurity solutions

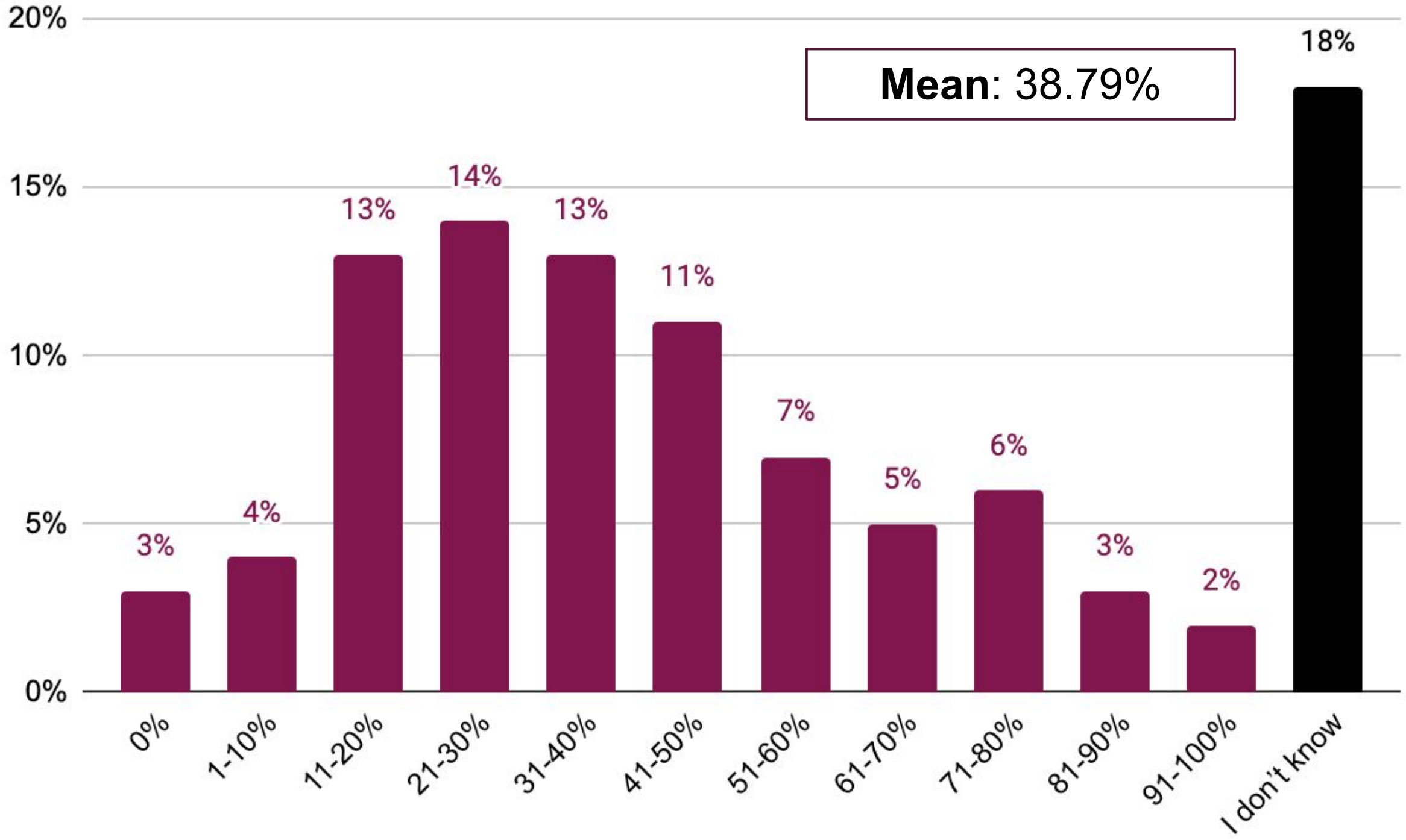


2022 Survey:
Japan **4**
Spain **5**
US **5**
UK & Ireland **6**
AUS & NZ **5**
DACH **5**
Nordics **7**

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

Base: 1484

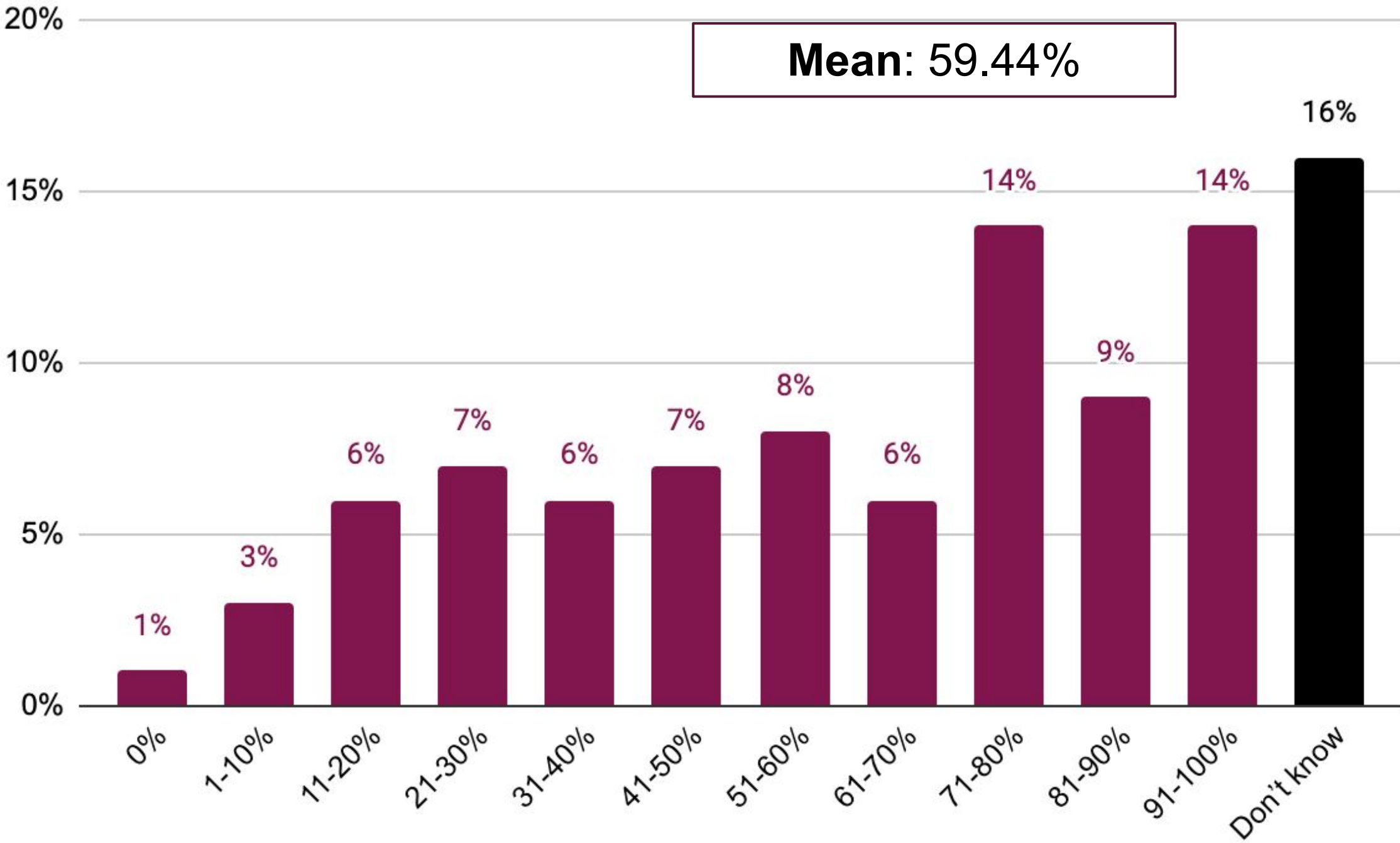
On average, 39% of network and application cybersecurity solutions overlap



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

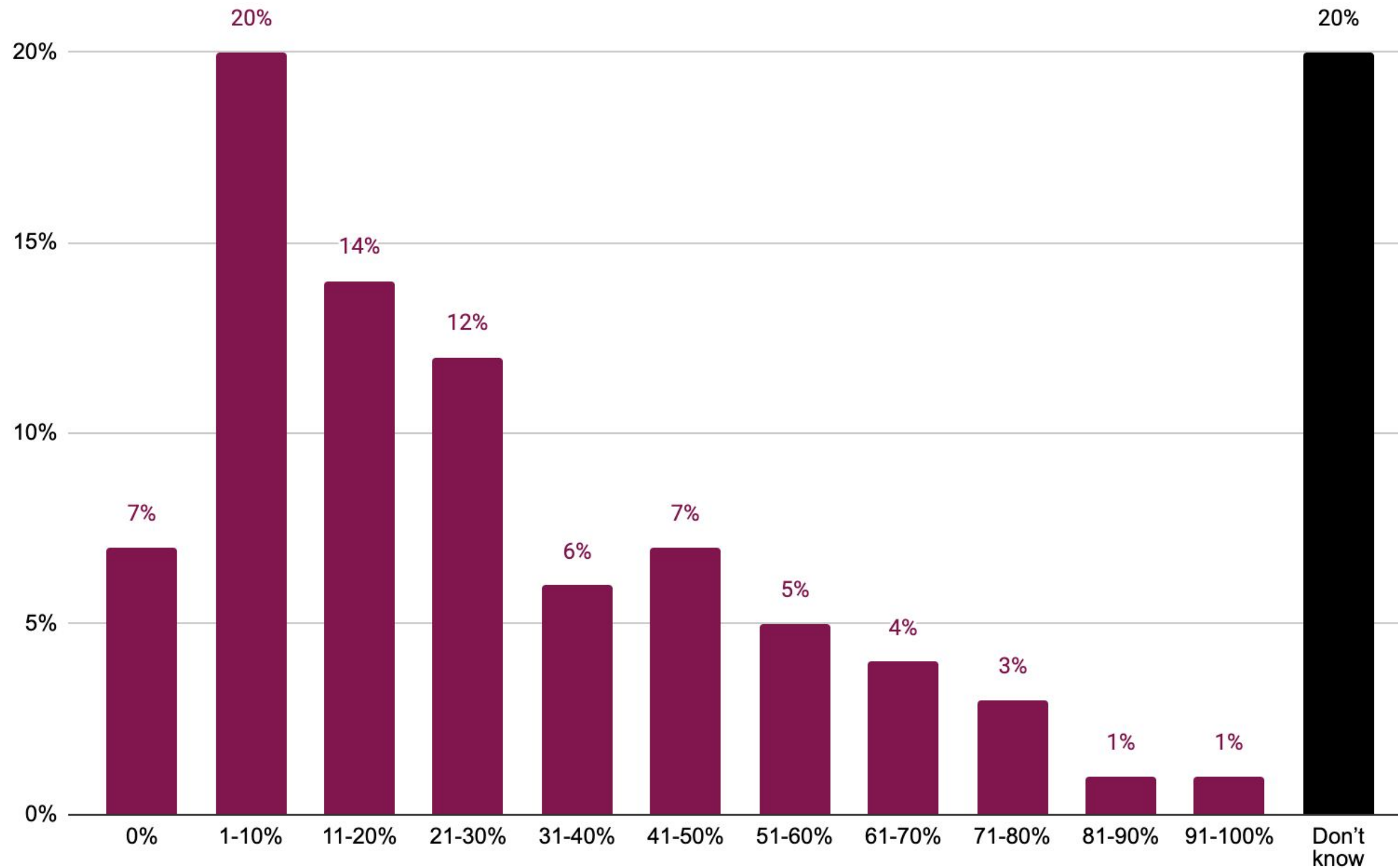
Base: 215

On average, 59% of cybersecurity tools are fully active/ deployed



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

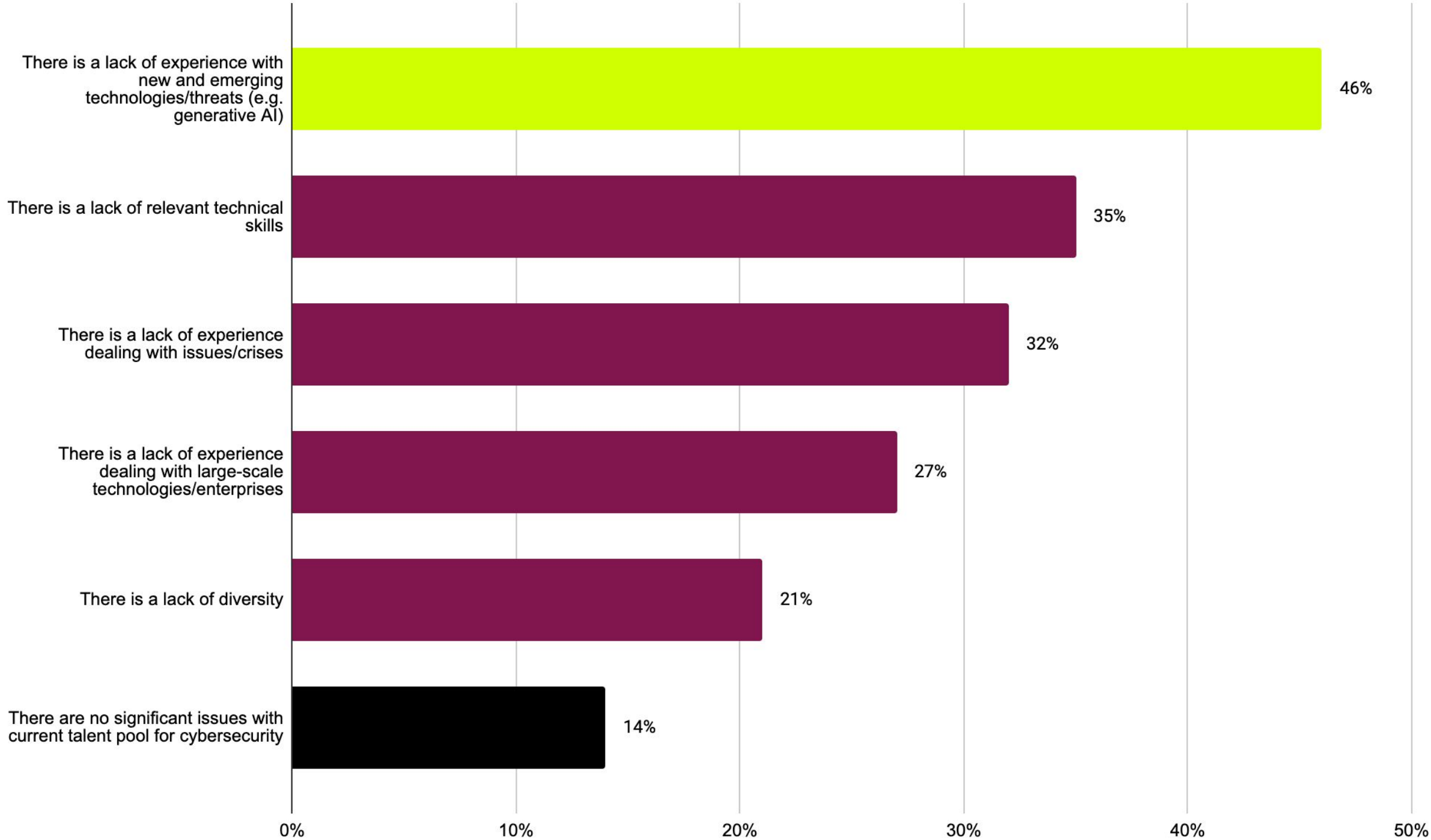
On average, 26% of security alerts detected by an organisations WAF are false alerts



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

Base: 215

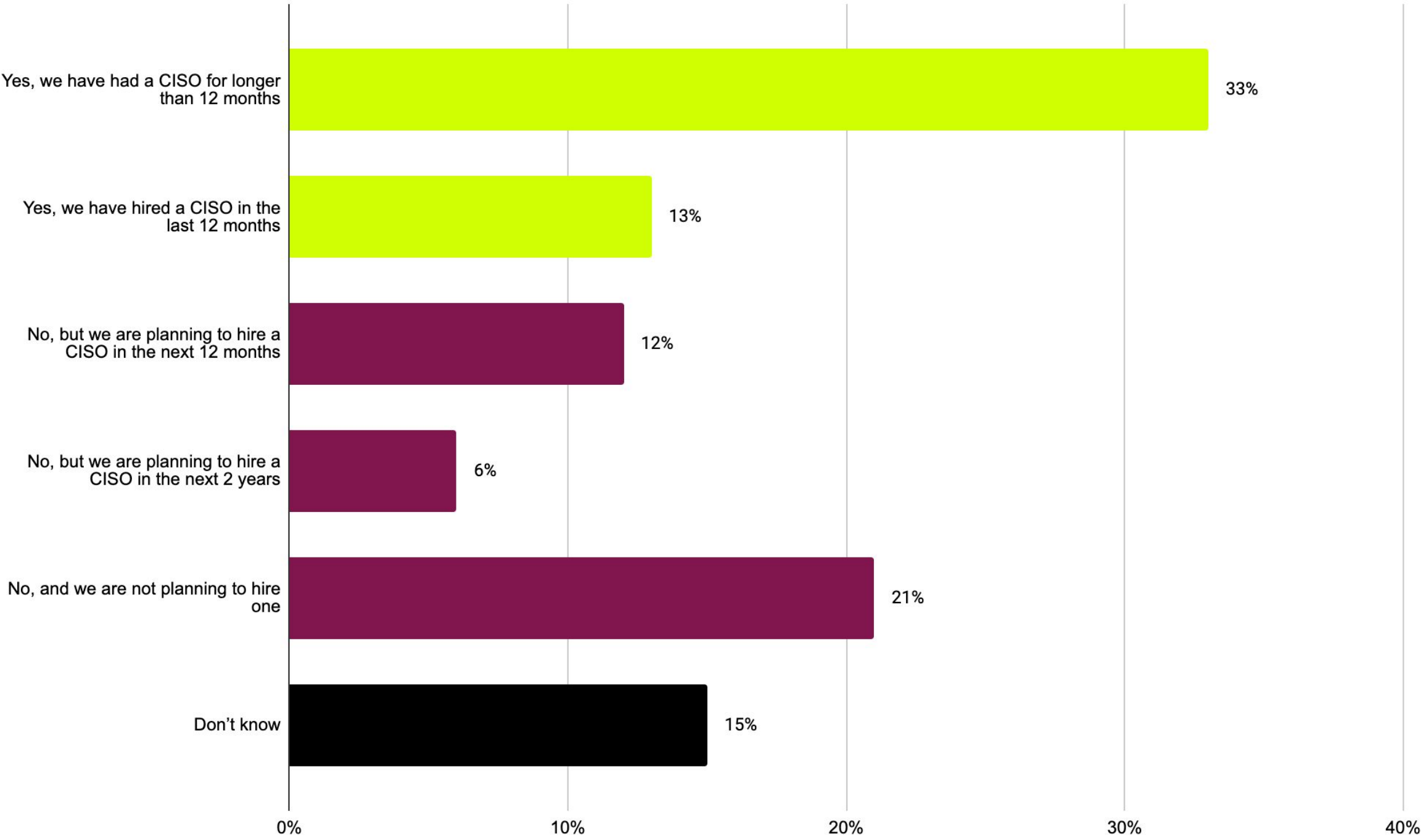
Respondents feel that the biggest gap among the current talent pool is experience with new and emerging technologies/ threats such as generative AI (46%)



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

Base: 215

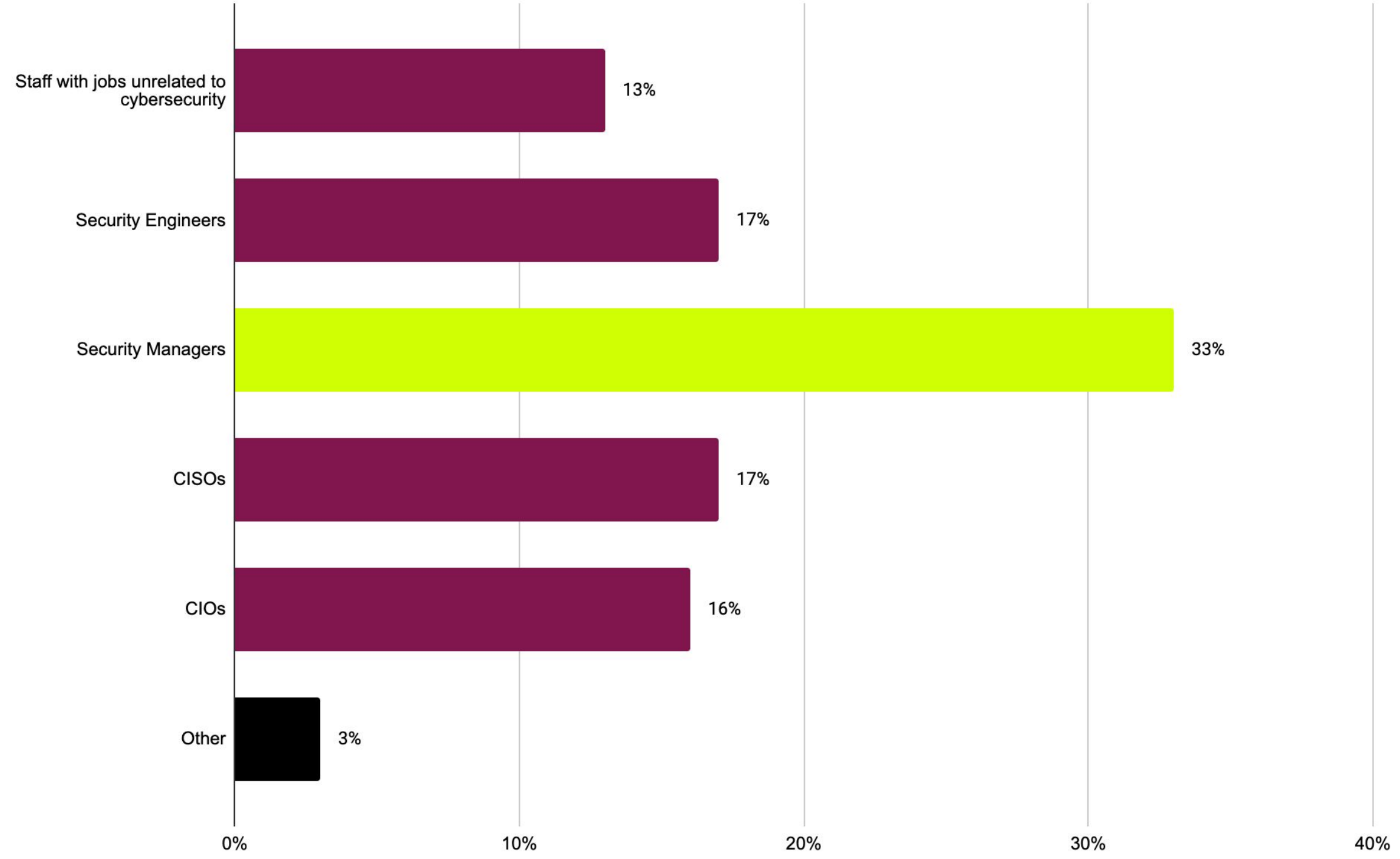
46% of respondents have hired a CISO, 13% of those within the last 12 months 21% do not plan to hire a CISO



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

Base: 215

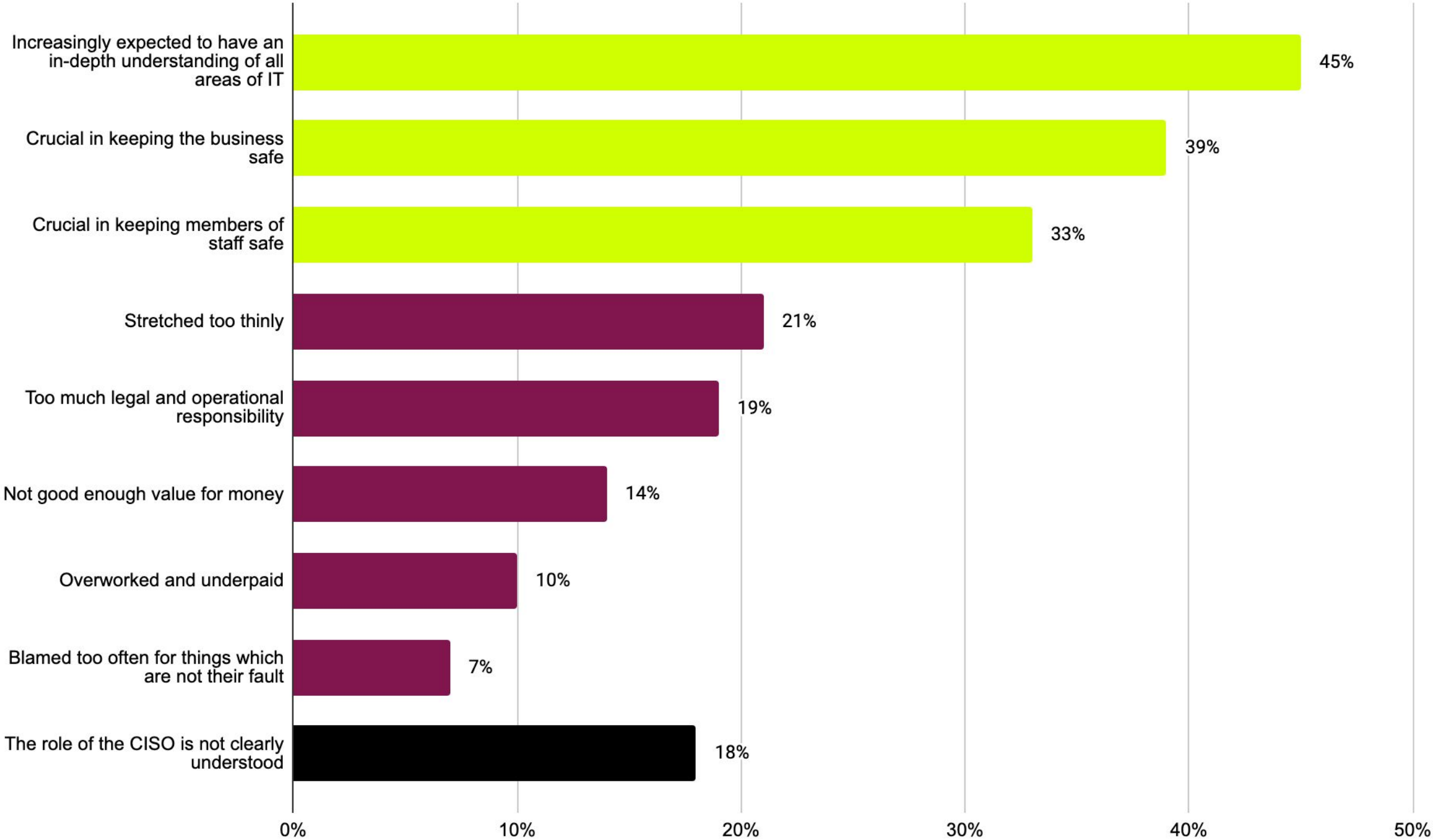
33% think security managers are often held responsible, while only 17% of respondents think CISOs are often held responsible for cybersecurity incidents



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

Base: 215

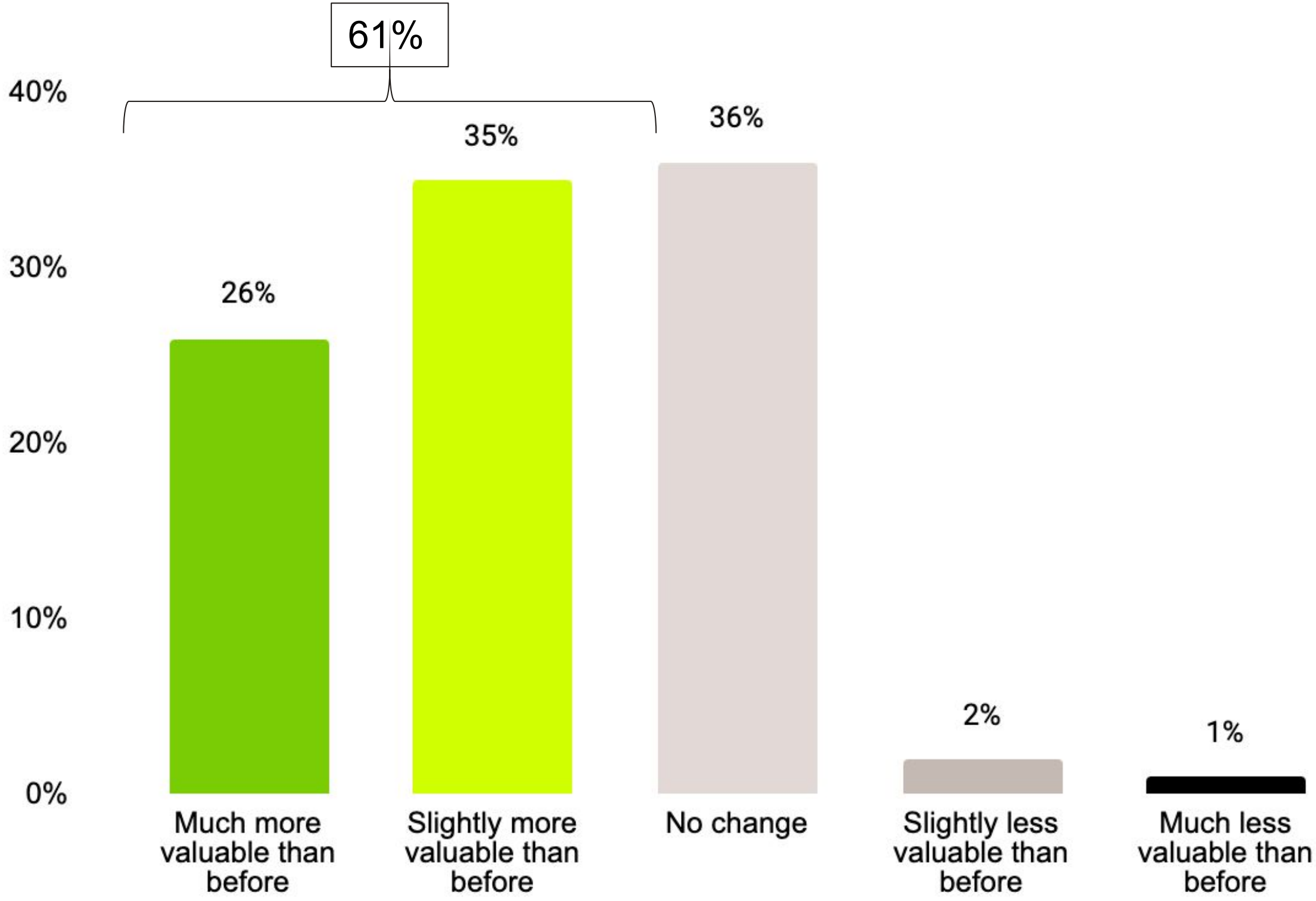
CISOs are viewed as having an in-depth understanding of all areas of IT (45%), crucial in keeping the business safe (39%), and crucial in keeping members of staff safe (33%)



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

Base: 215

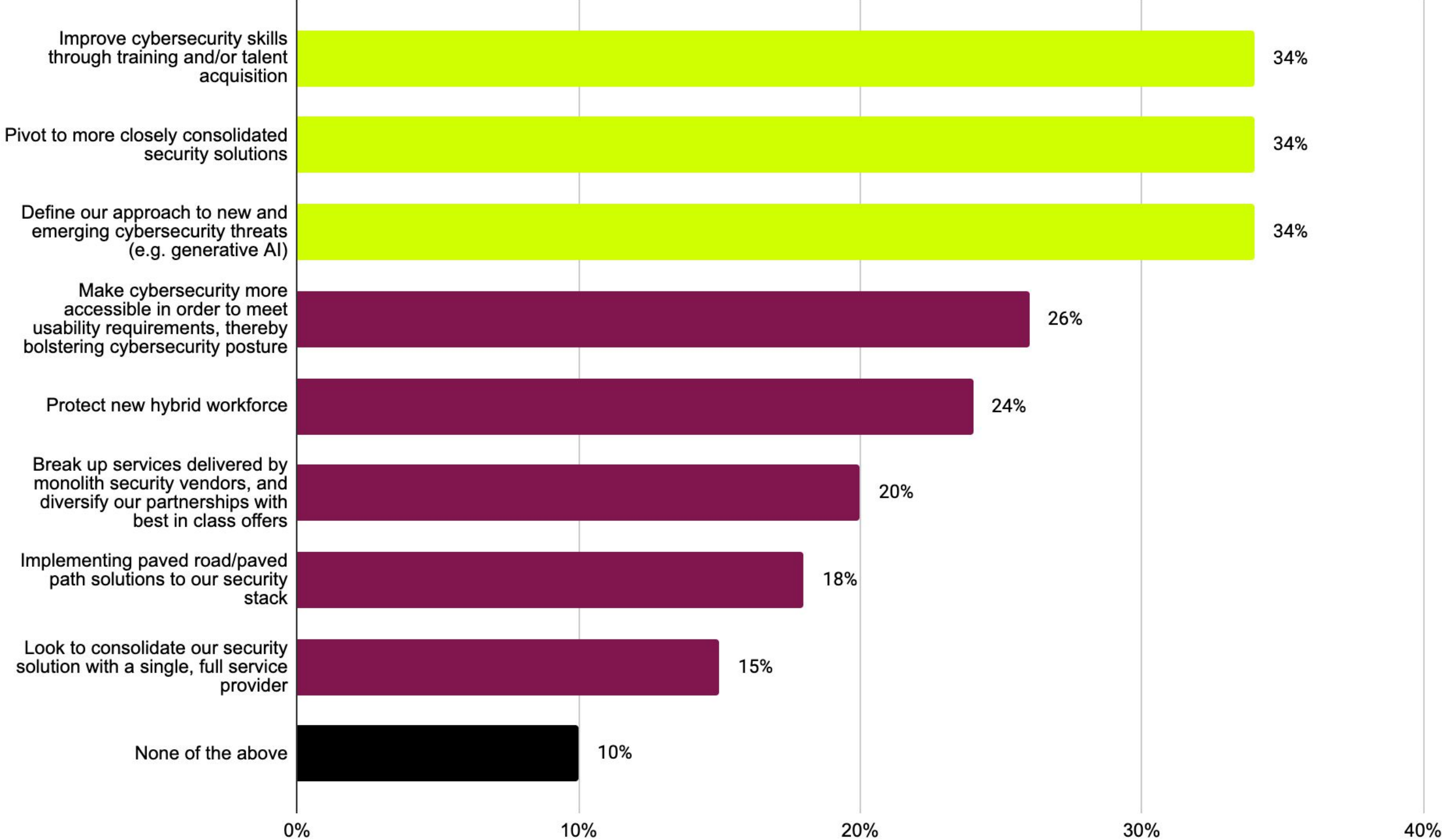
61% of respondents think their cybersecurity programme has become more valuable over the last 12 months



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: 215

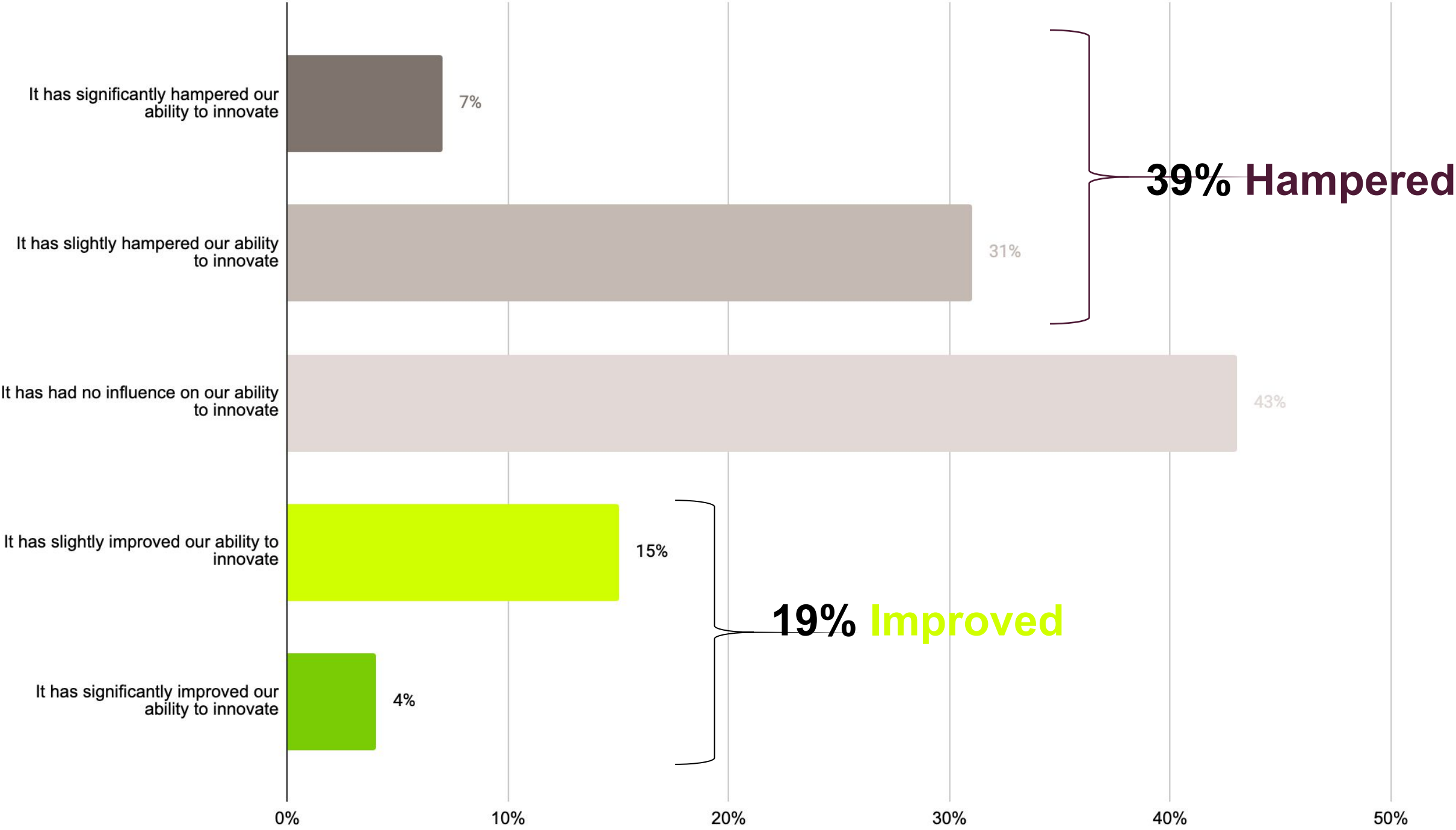
Improving cybersecurity skills through training and/or talent acquisition, defining approaches to new and emerging cybersecurity threats, and pivoting to more closely consolidated security solutions (all 34%) are the main security priorities over the next year



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

Base: 215

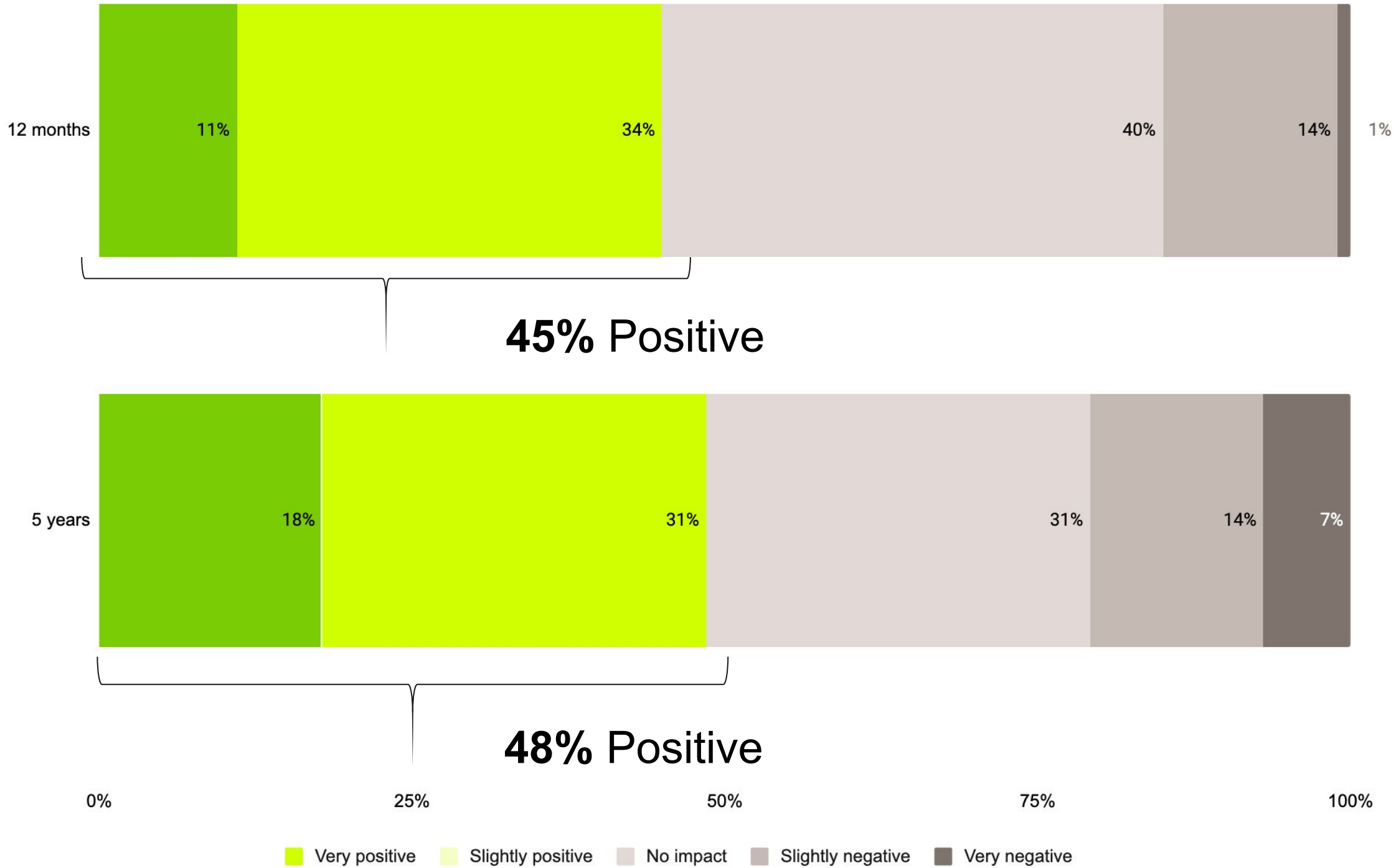
39% say that their organisations cybersecurity strategy has hampered business innovation
Only 19% say it has improved innovation



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

Base: 215

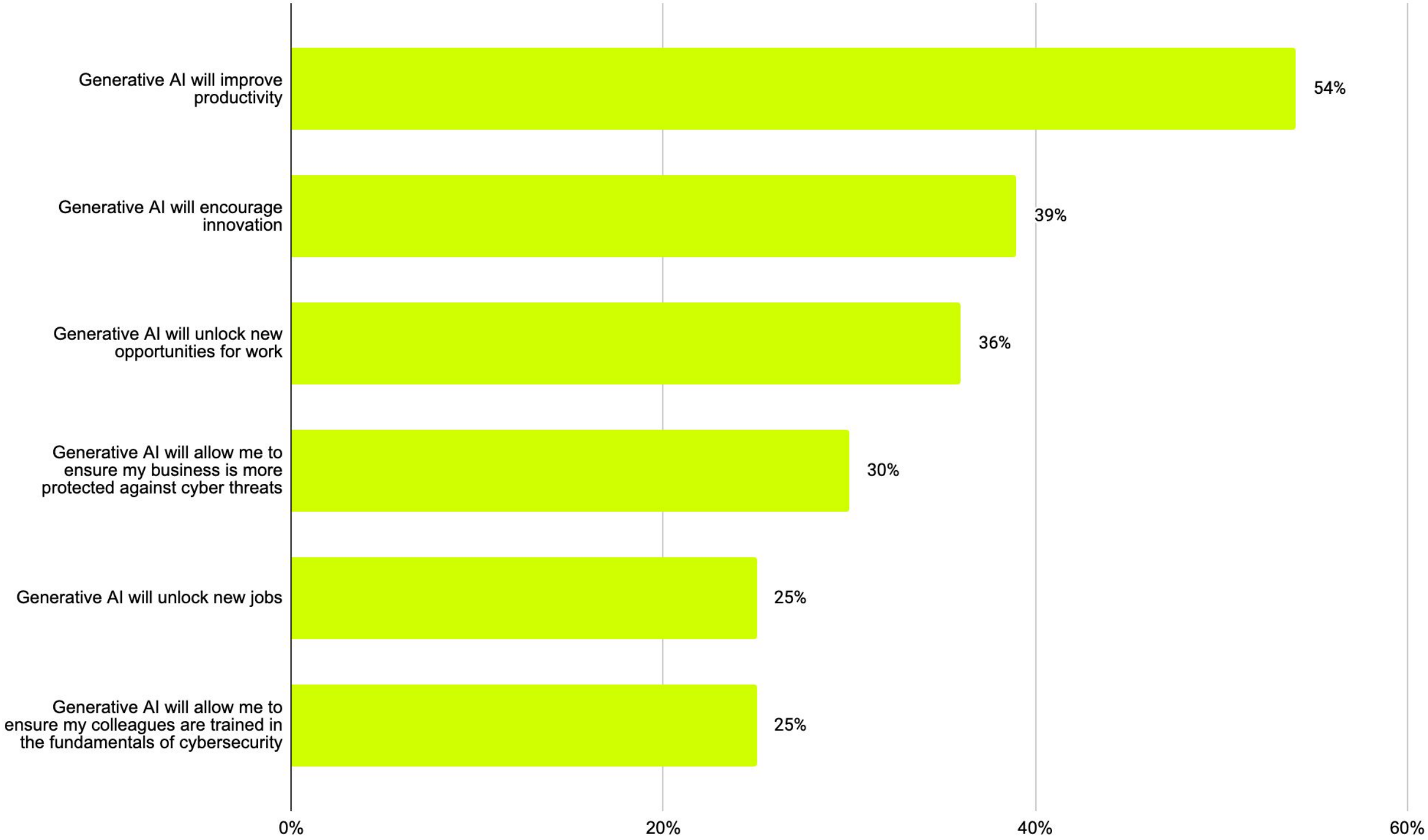
45% predict that Generative AI will have a positive impact on cybersecurity over the next 12 months
48% predict it will have a positive impact over the next 5 years



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

Base: 215

Improving productivity (54%) and encouraging innovation (39%) are the main positive impacts of Generative AI

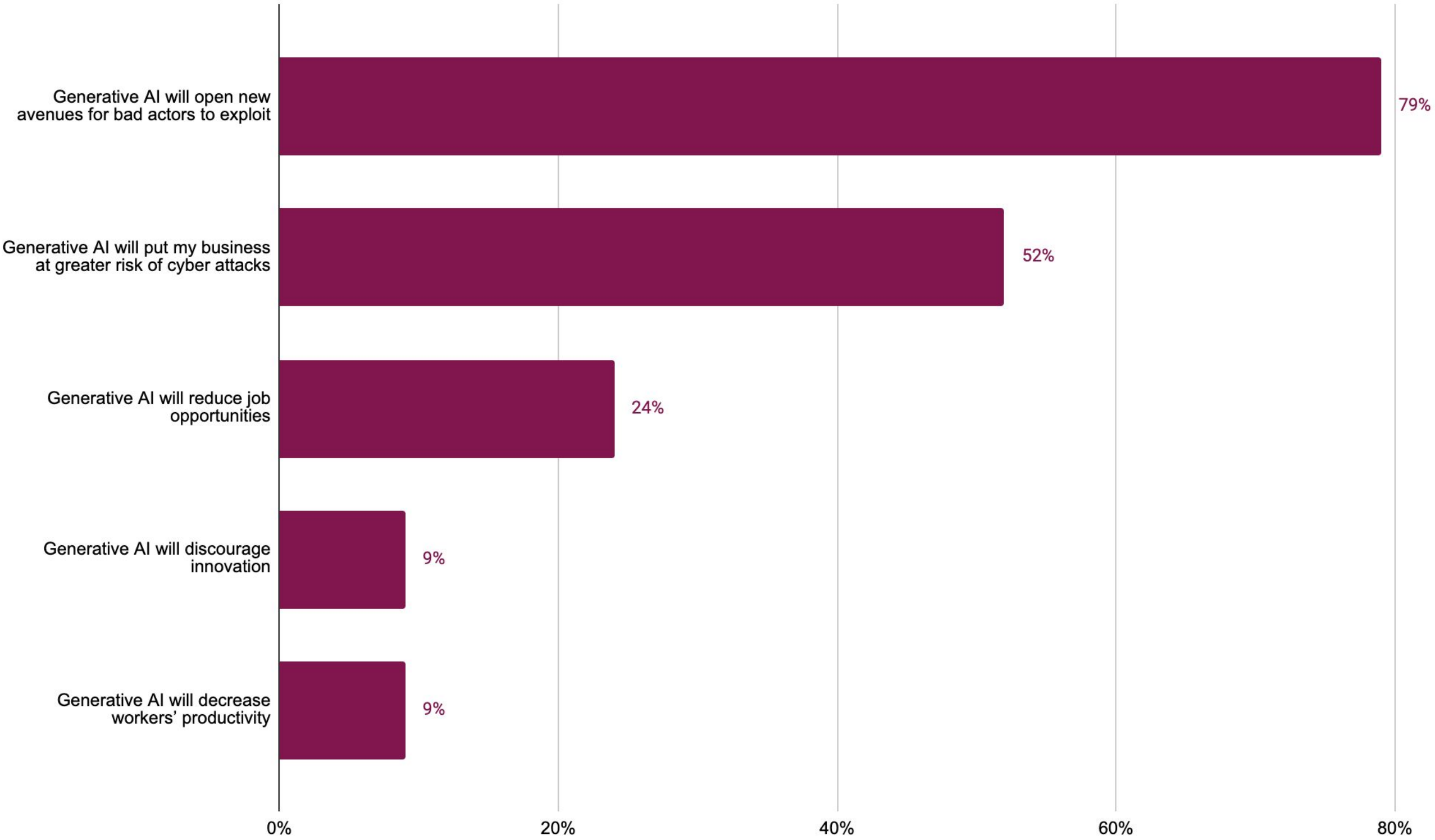


*only asked to those who said generative AI will have a positive impact in the next 12 months

Base : 97*

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 open new avenues for bad actors to exploit (79%), or that it will put businesses at greater risk of cyber attacks (52%)

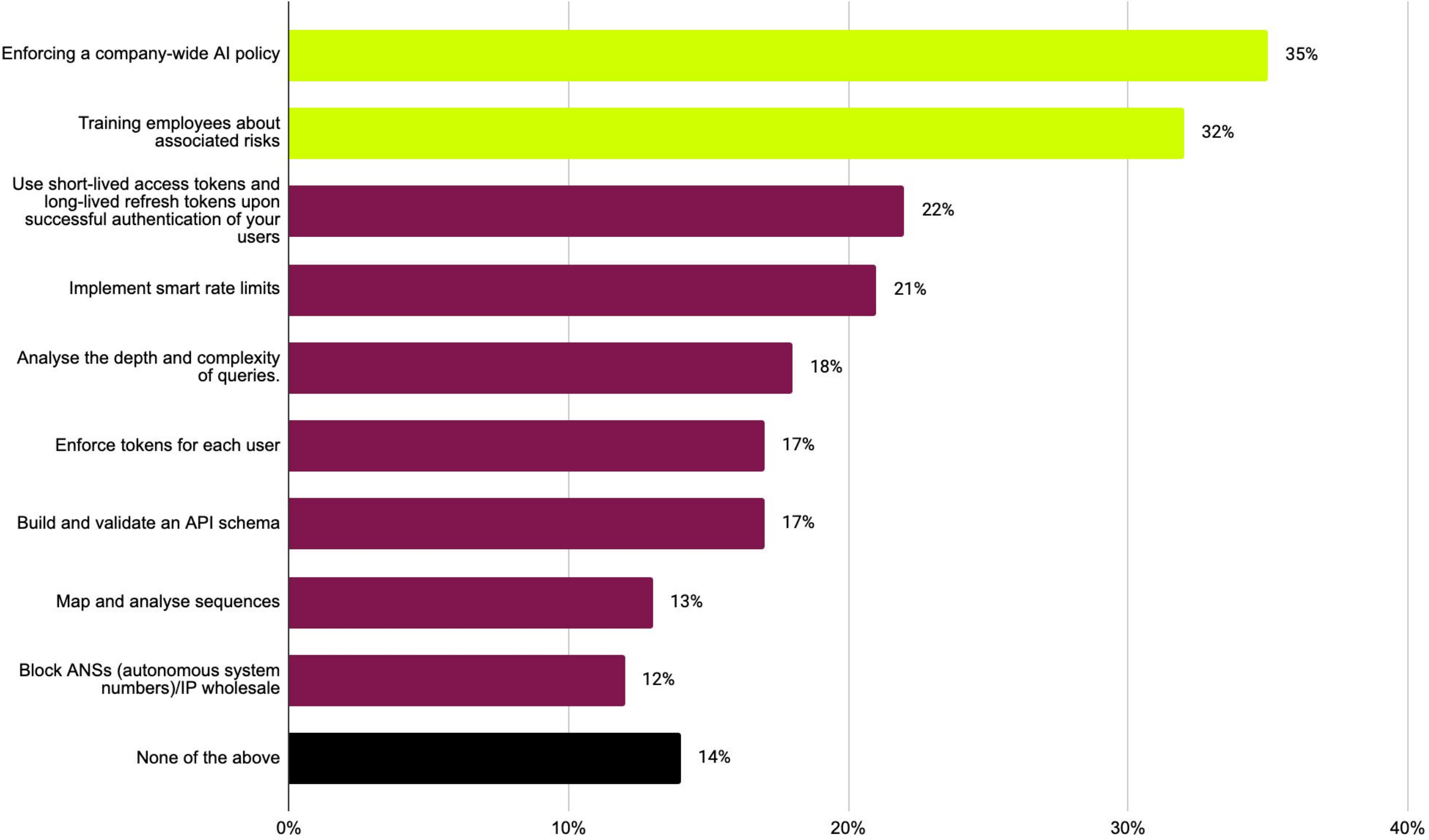


*only asked to those who said generative AI will have a negative impact in the next 12 months

Base: 33*

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

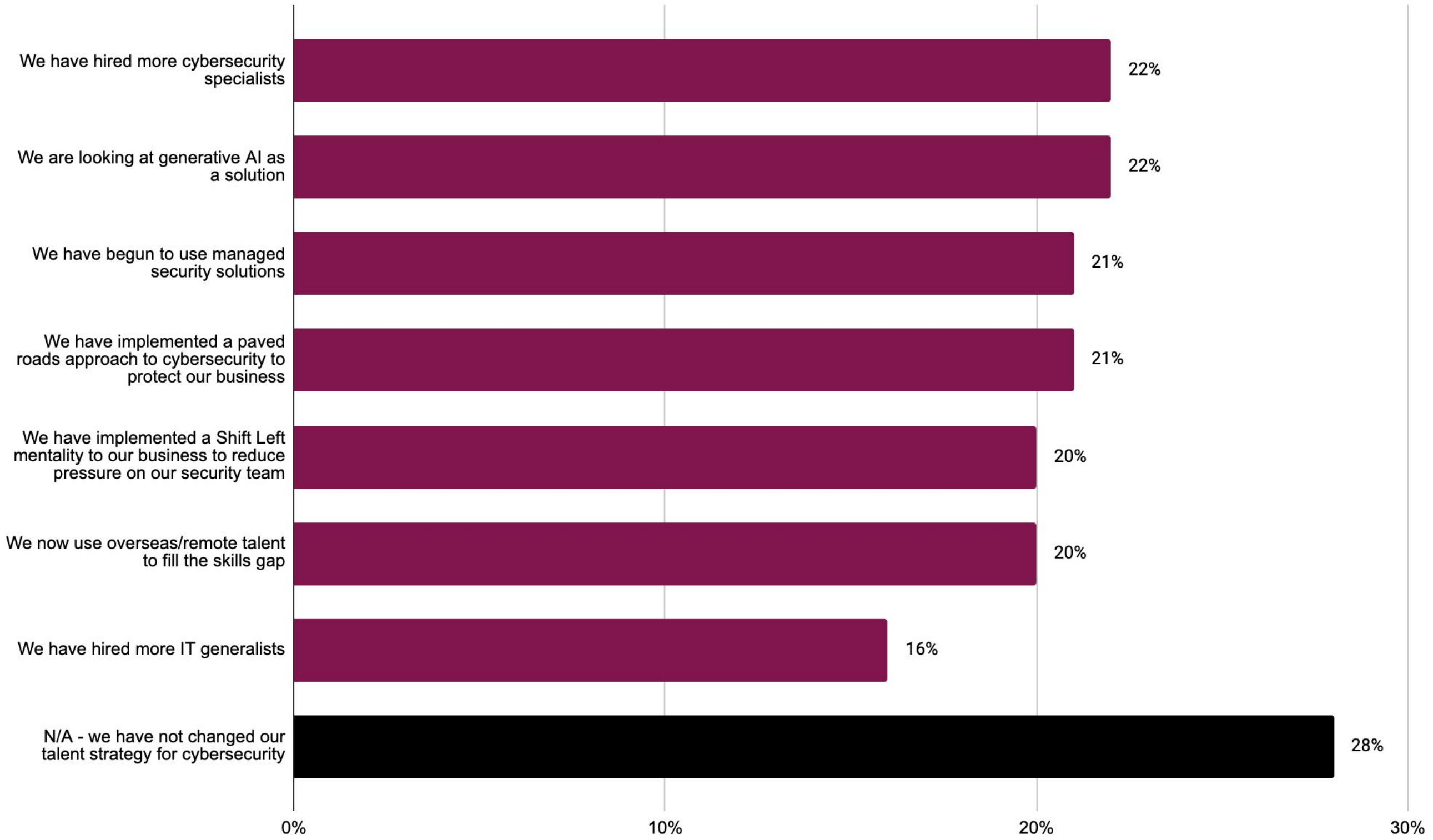
Enforcing a company-wide AI policy (35%) and training employees on the associated risks (32%) are the top two steps companies are taking to mitigate generative AI security threats



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

Base: 215

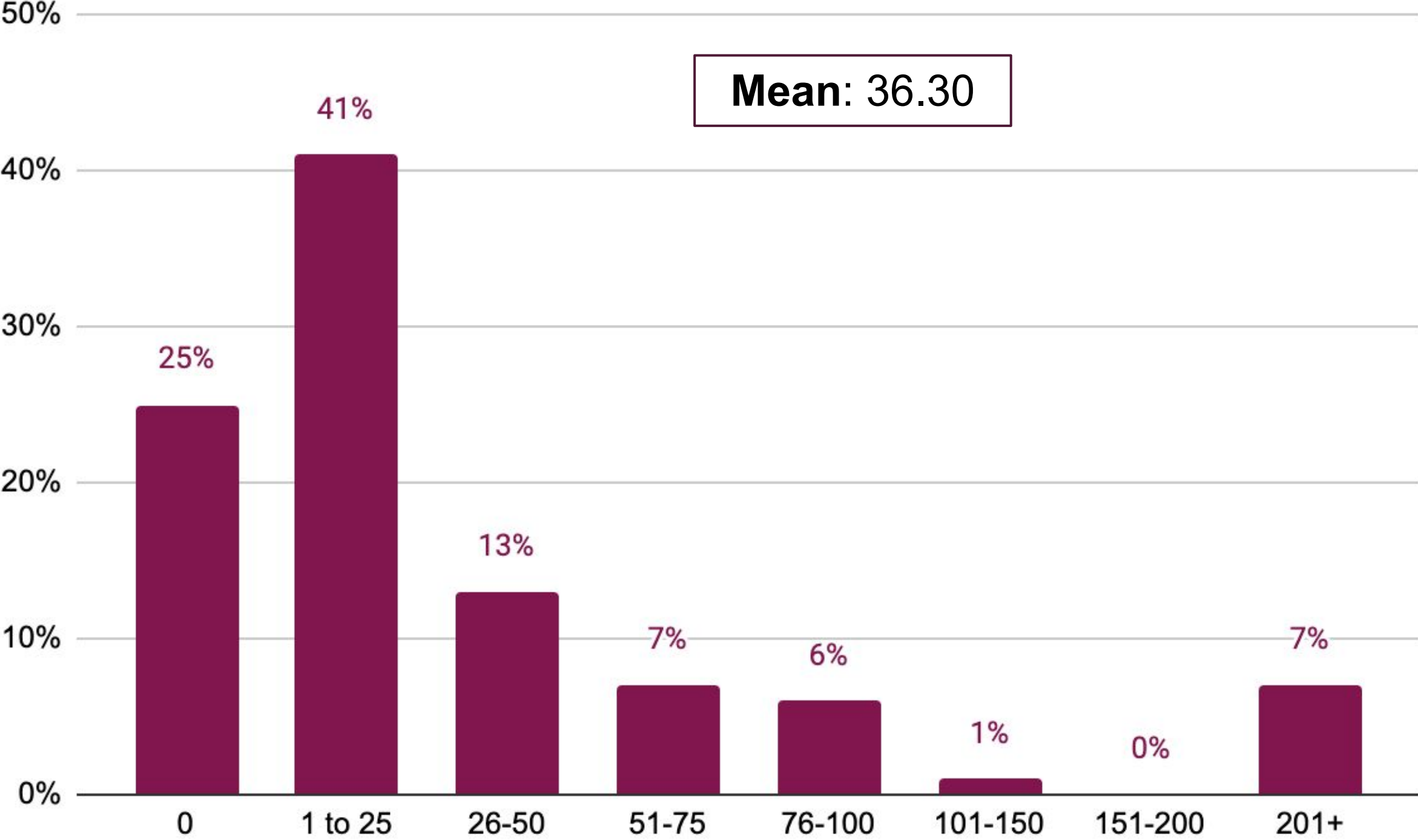
Companies have hired more cybersecurity specialists and begun looking at generative AI as a solution (both 22%) over the last 12 months



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

Base: 215

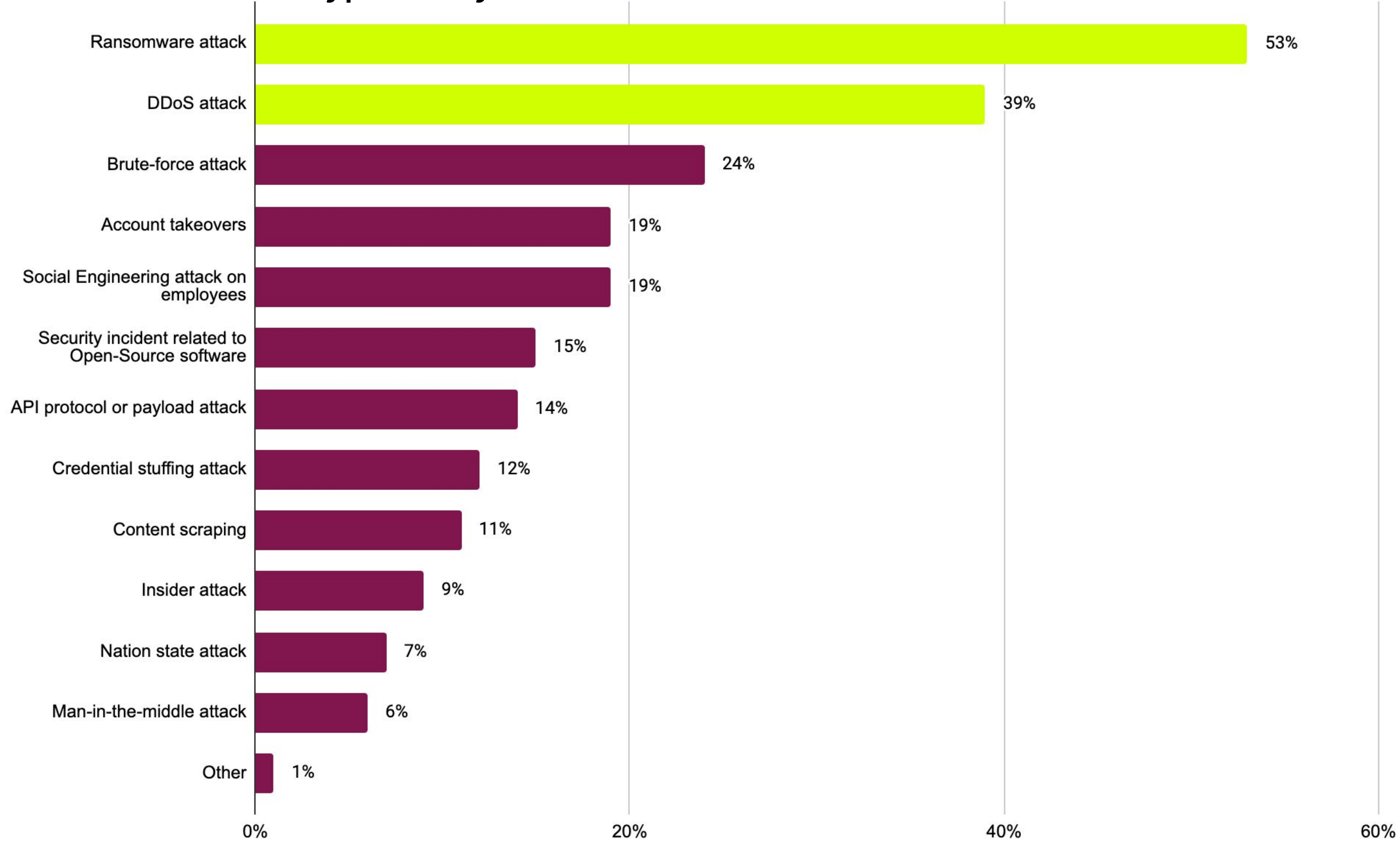
On average, businesses have suffered 36 cyberattacks in the past 12 months



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

Base: 215

The most common types of cyberattacks were ransomware attacks (53%) and DDoS attacks (39%)

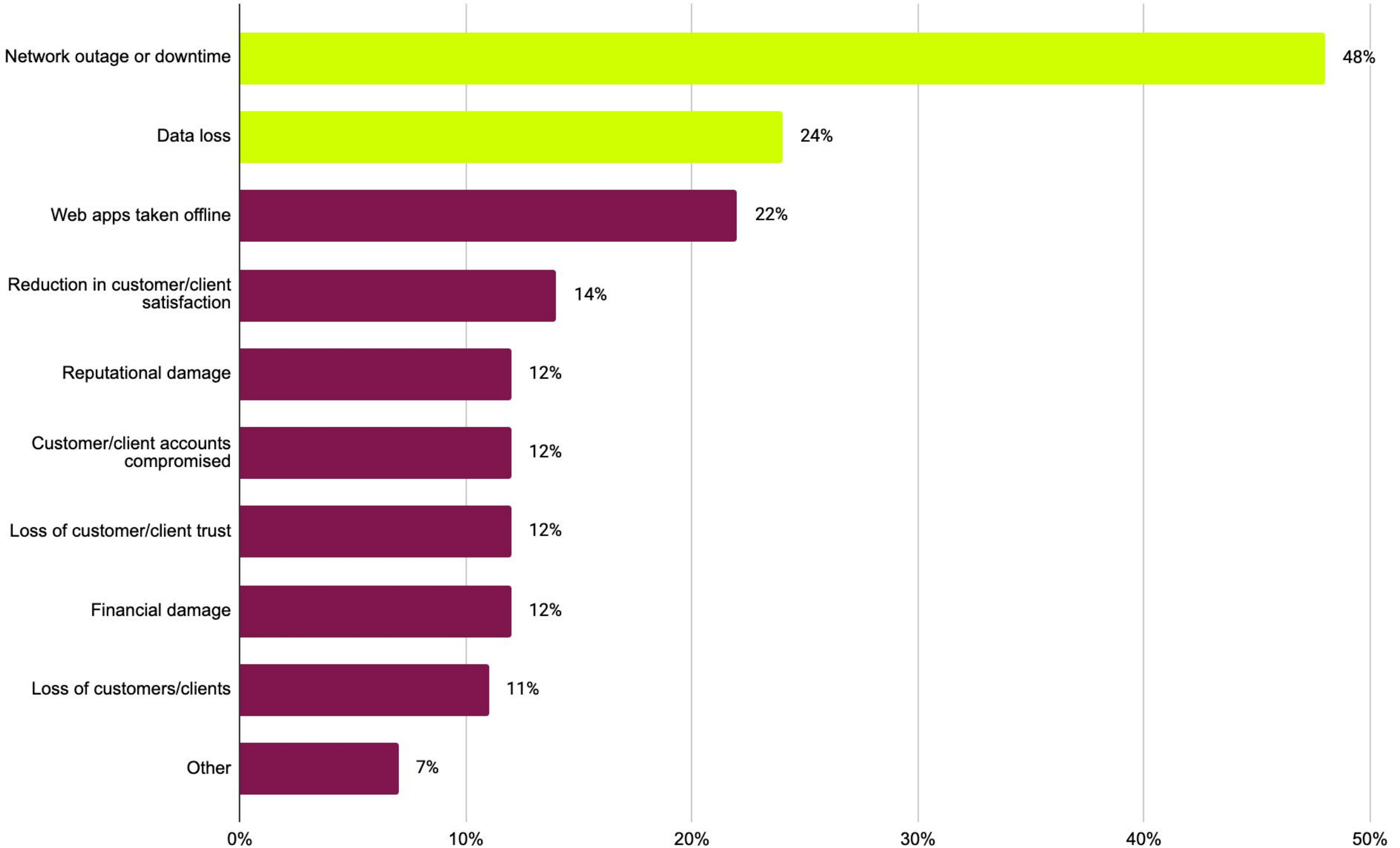


*only asked to those who have experienced a cyber attack

Base: 161*

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

Network outages or downtime (48%), data loss (24%), and web apps being taken offline (22%) were the main impacts of cyber attacks

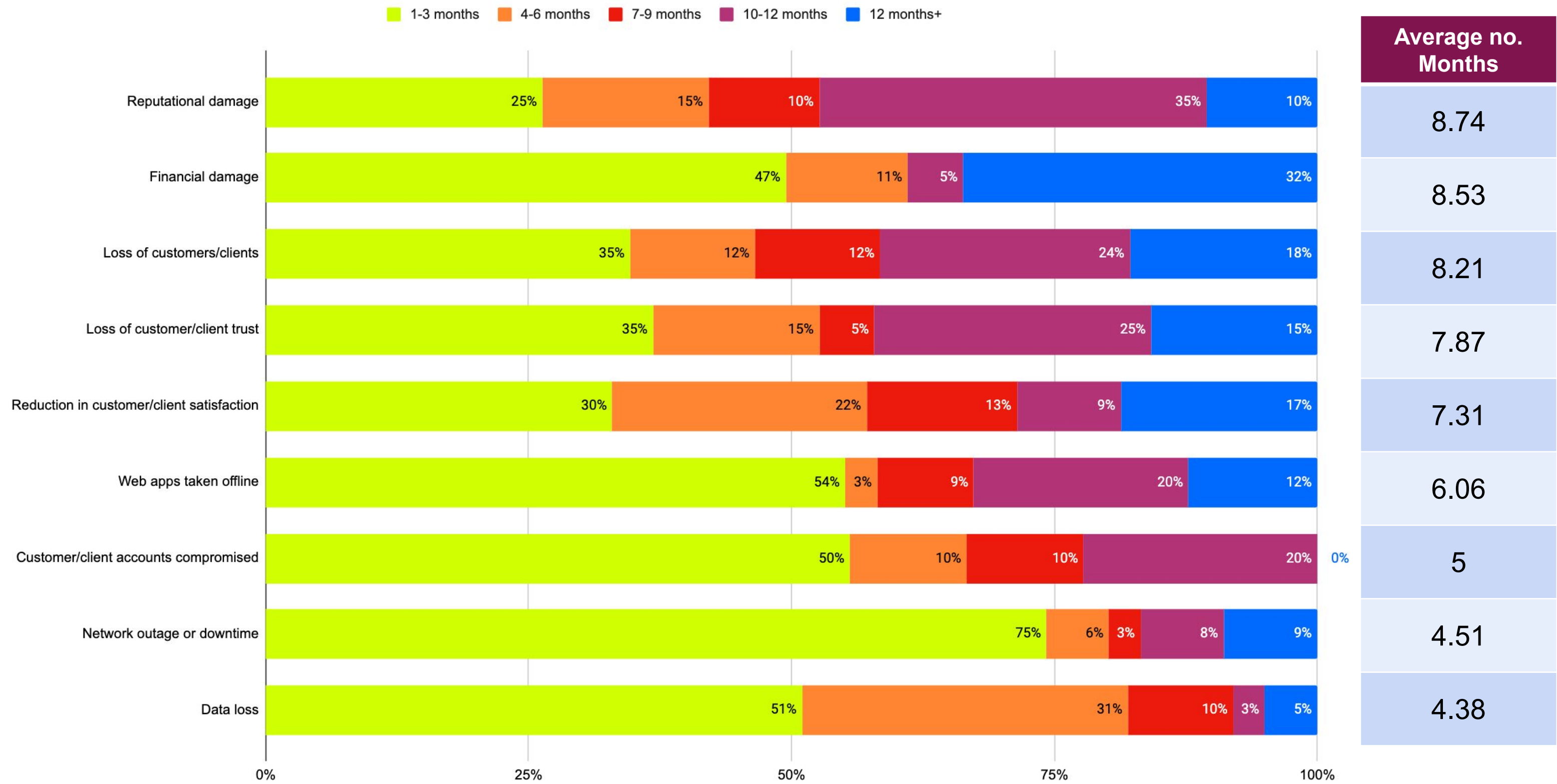


*only asked to those who have experienced a cyber attack

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

Base: 161*

On average, it will take businesses 9 months to recover from reputational or financial damage caused by a cyber attack

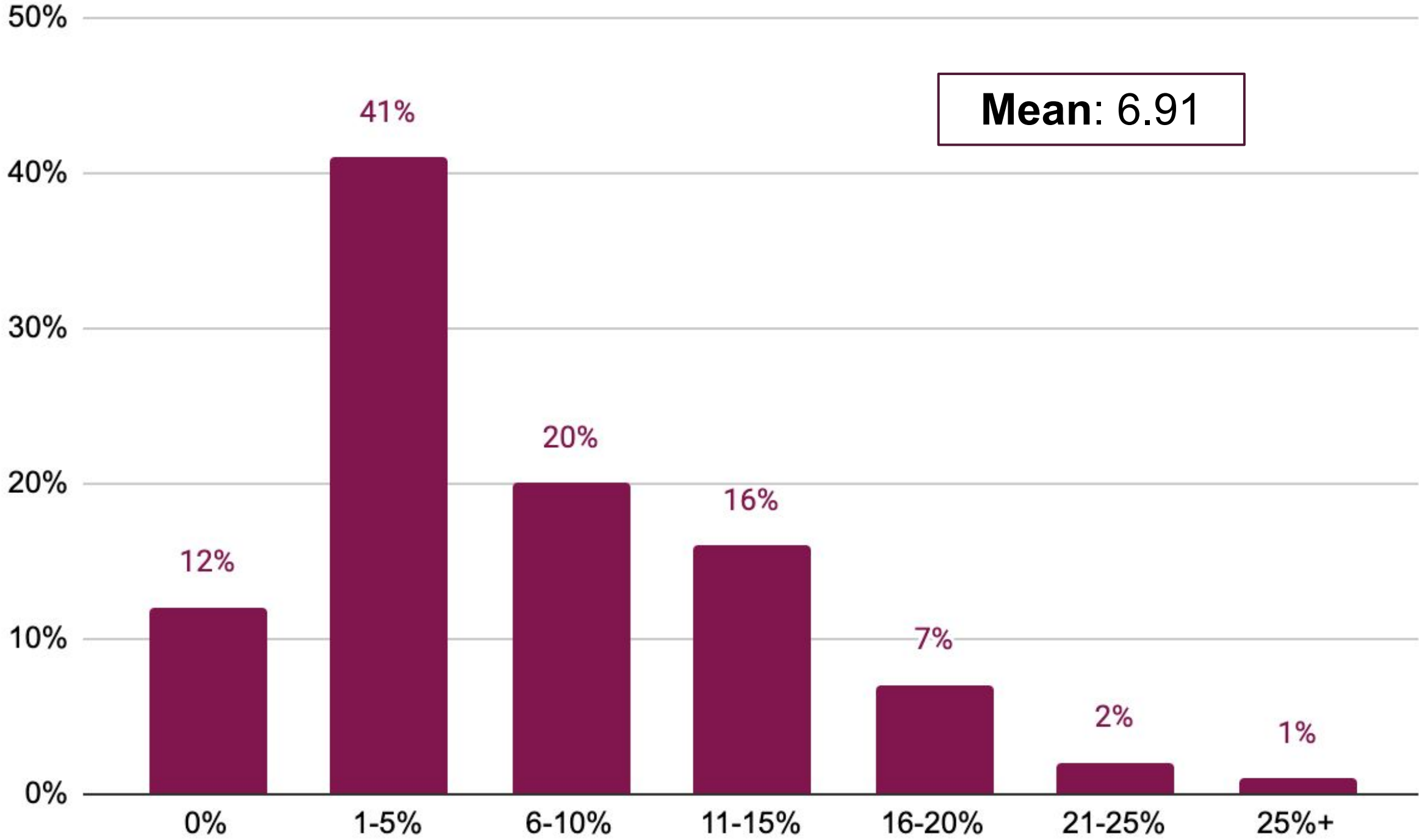


*only asked to those who had experienced each impact at Q22

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 7% of their annual income as a result of cyber attacks



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

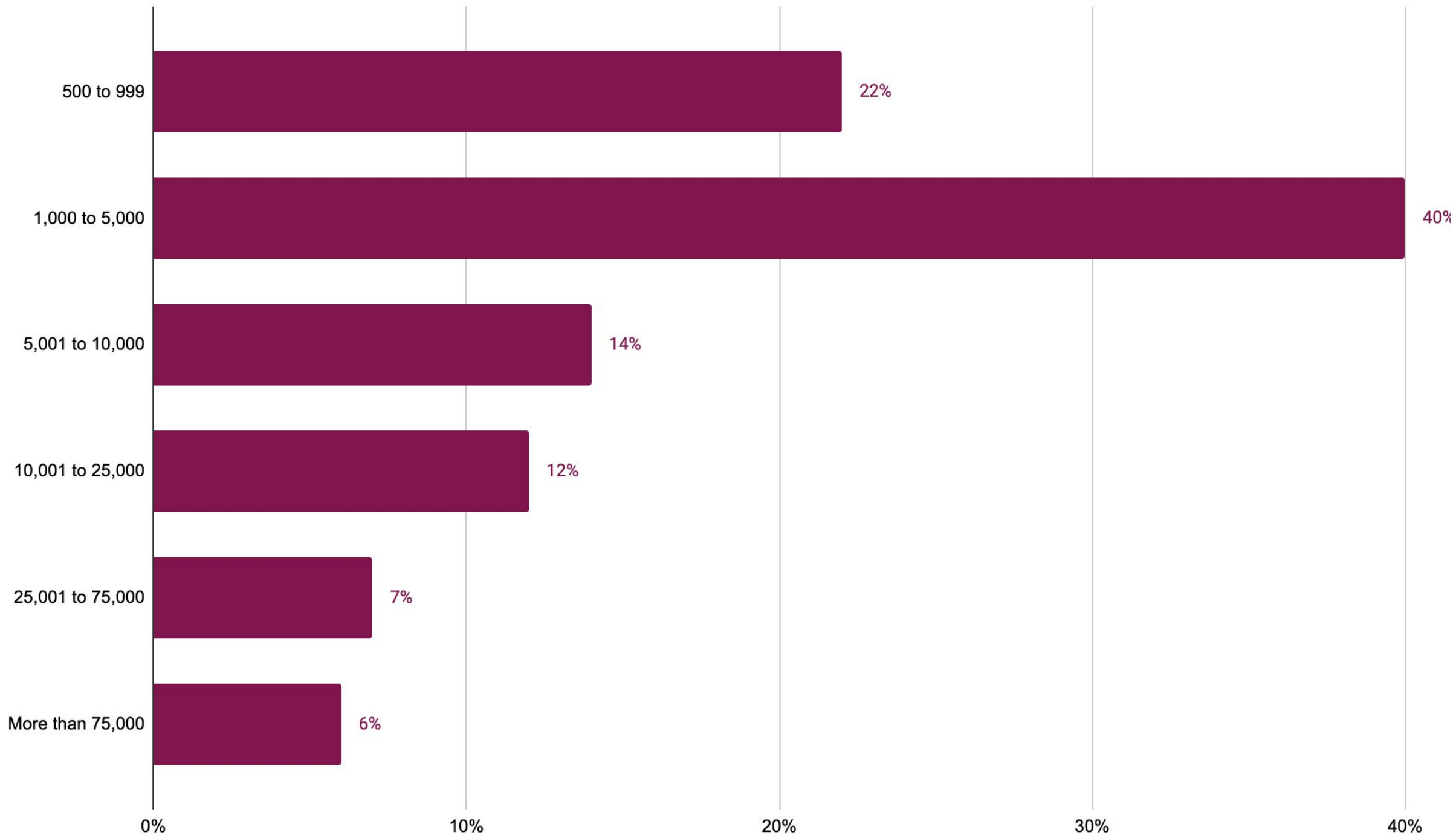
Base: 161*

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

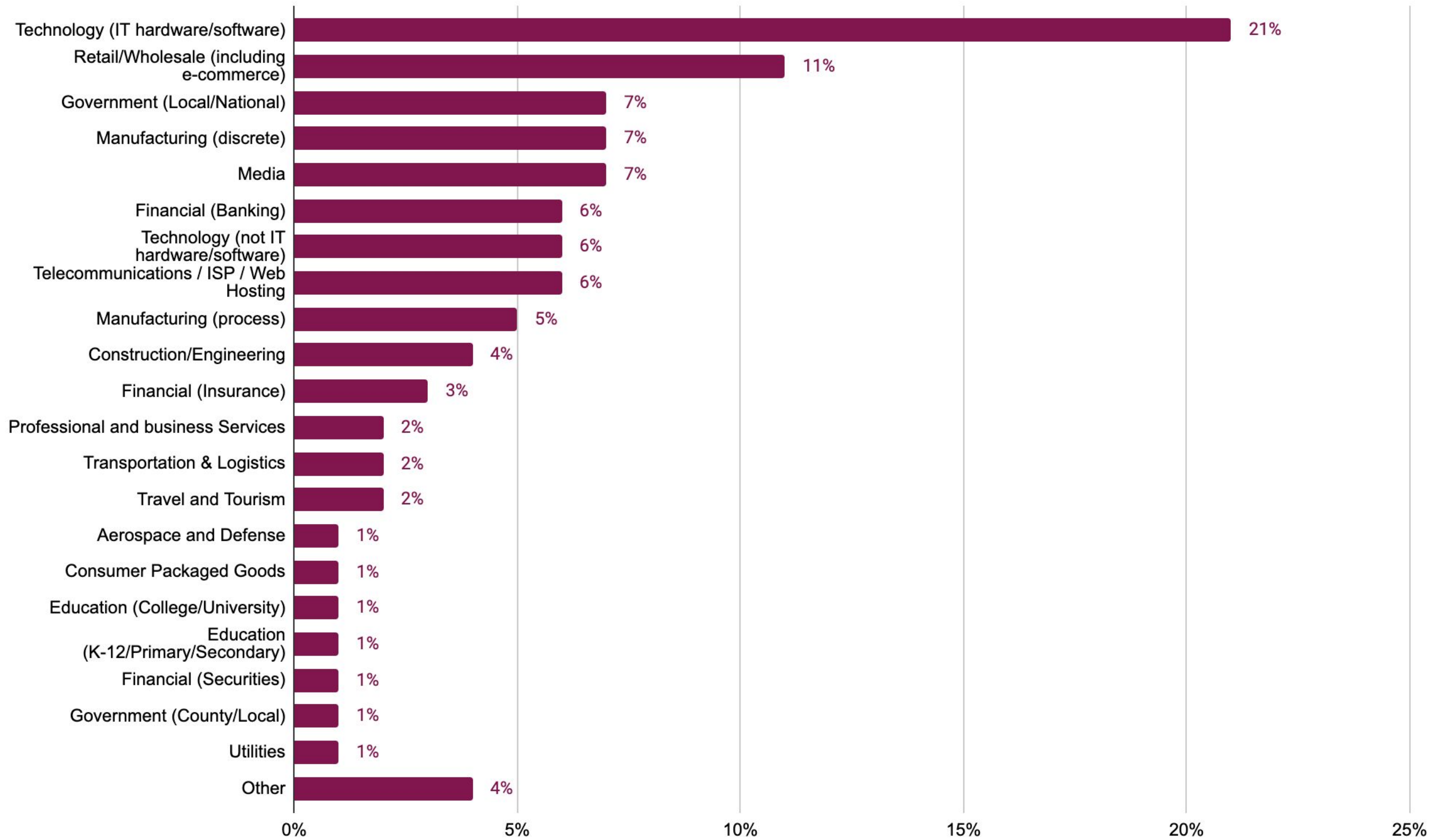
Size



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

Base: 215

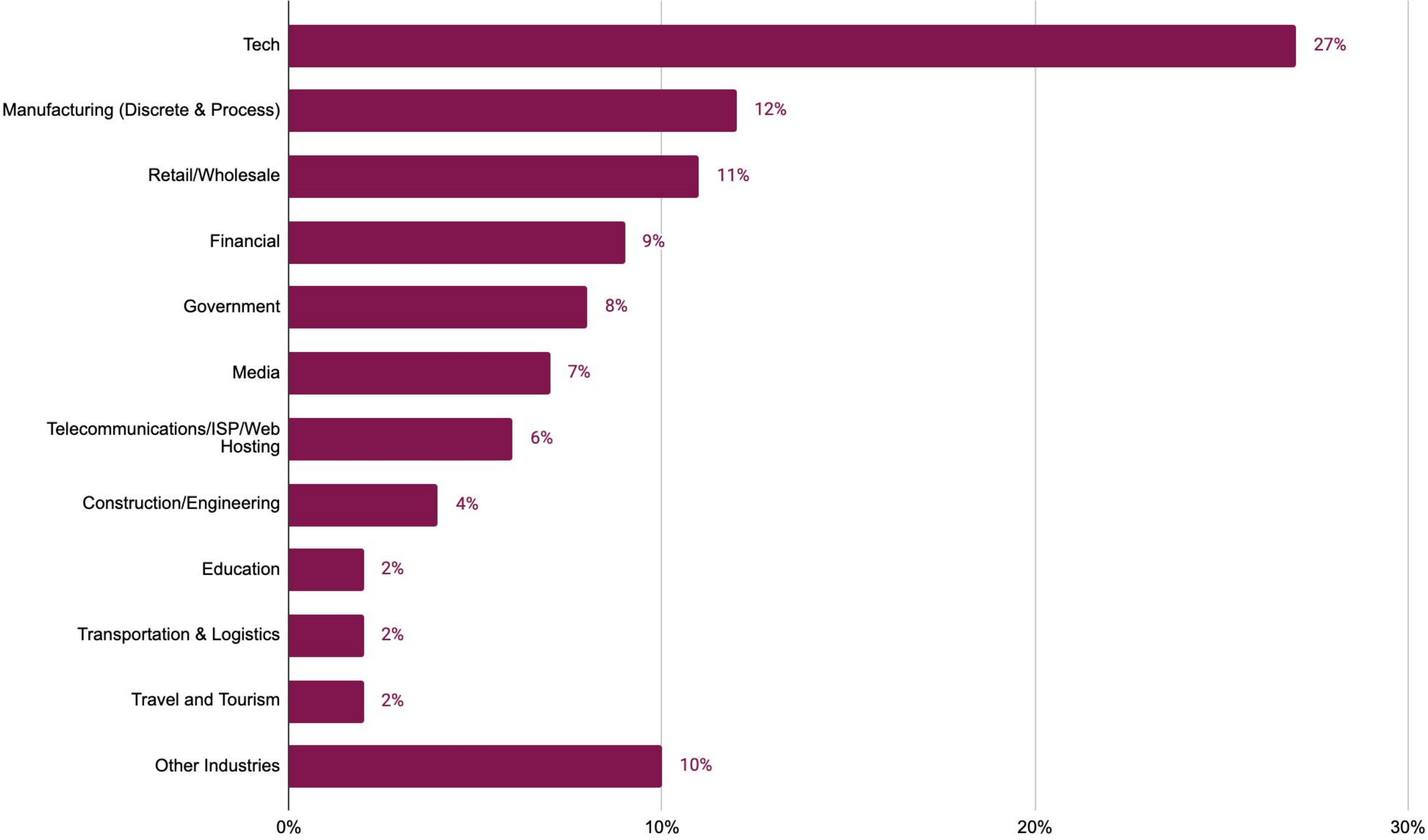
Industry



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

Base: 215

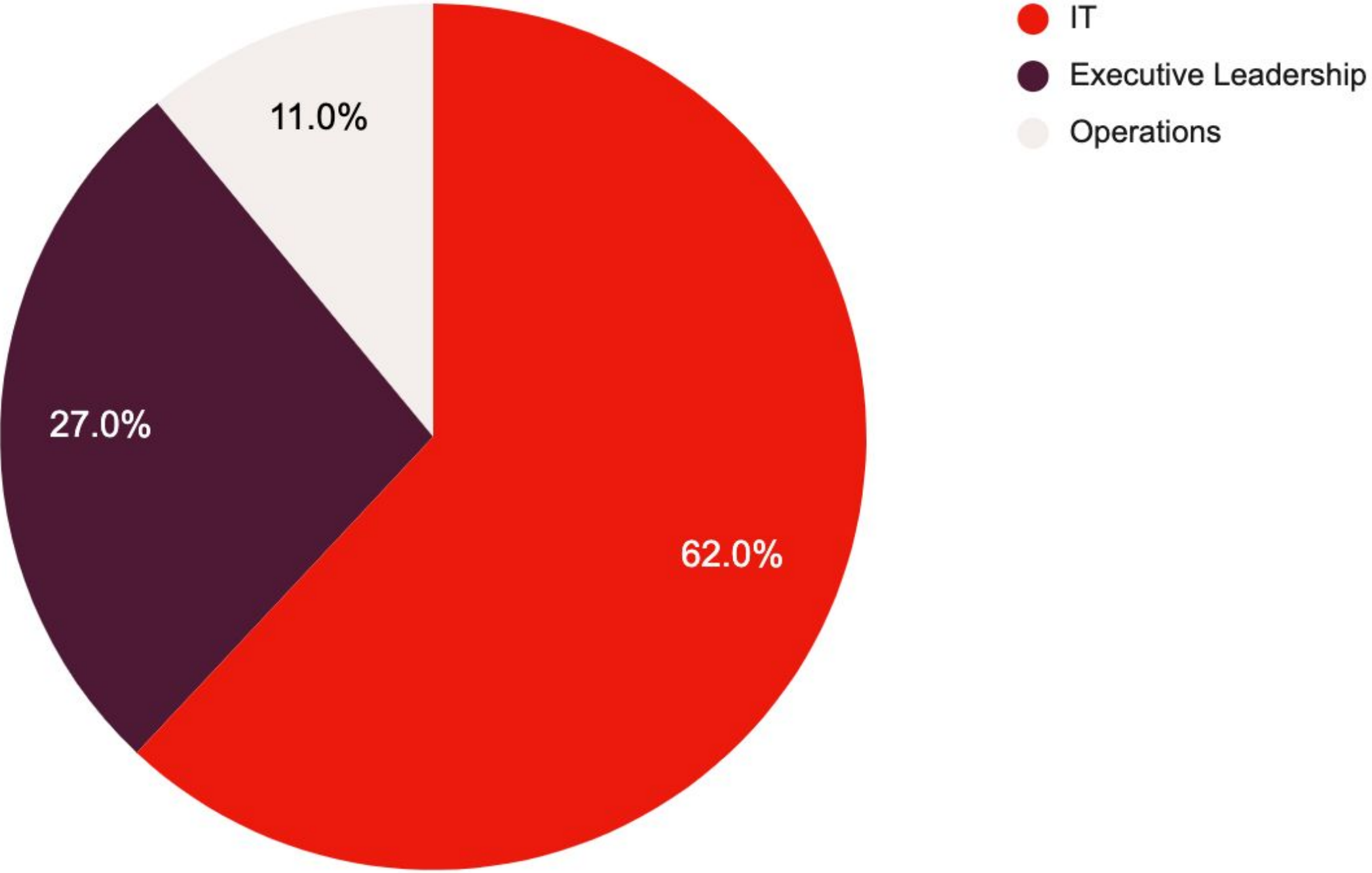
Industry - focus



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

Base: 215

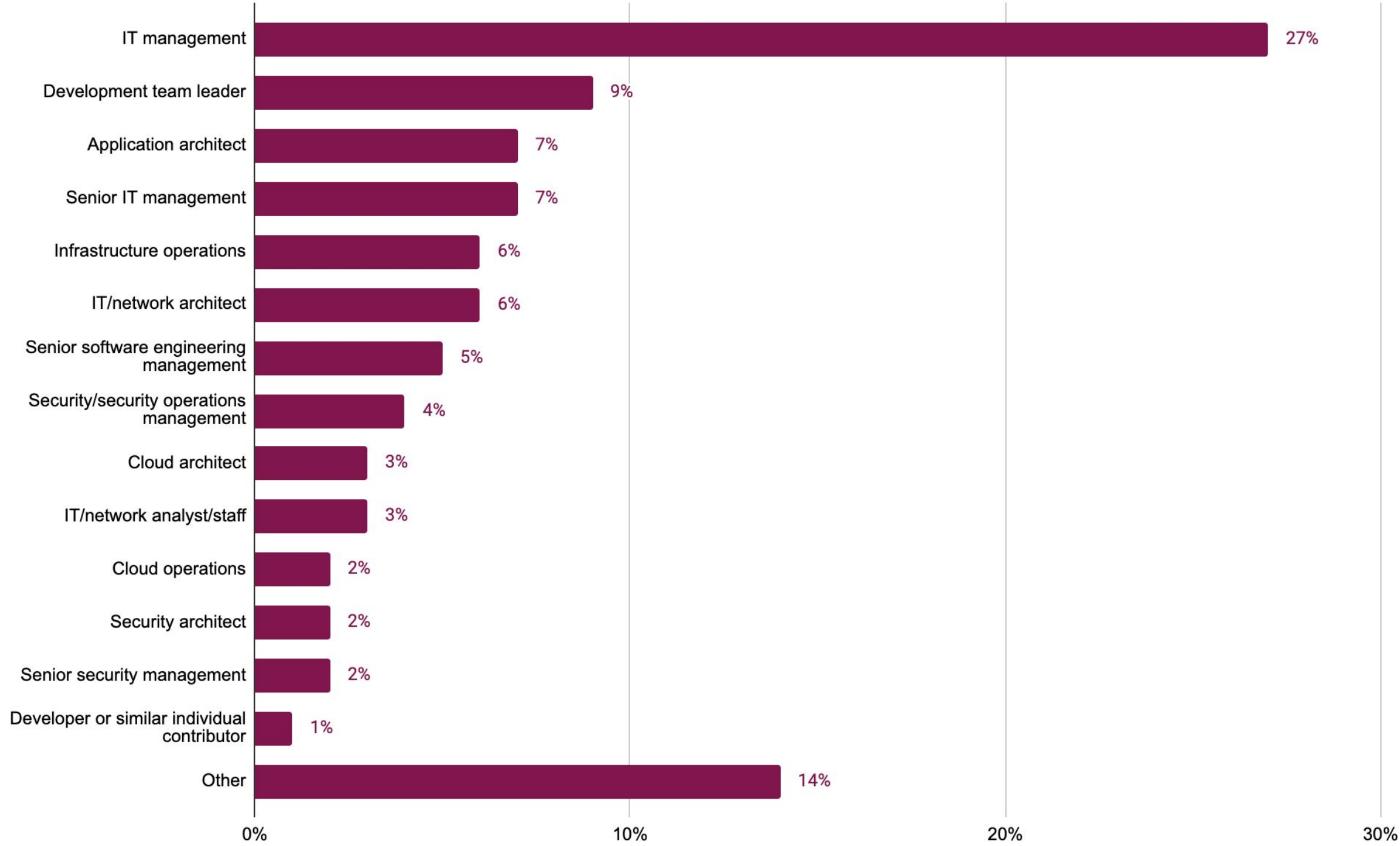
Department



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

Base: 215

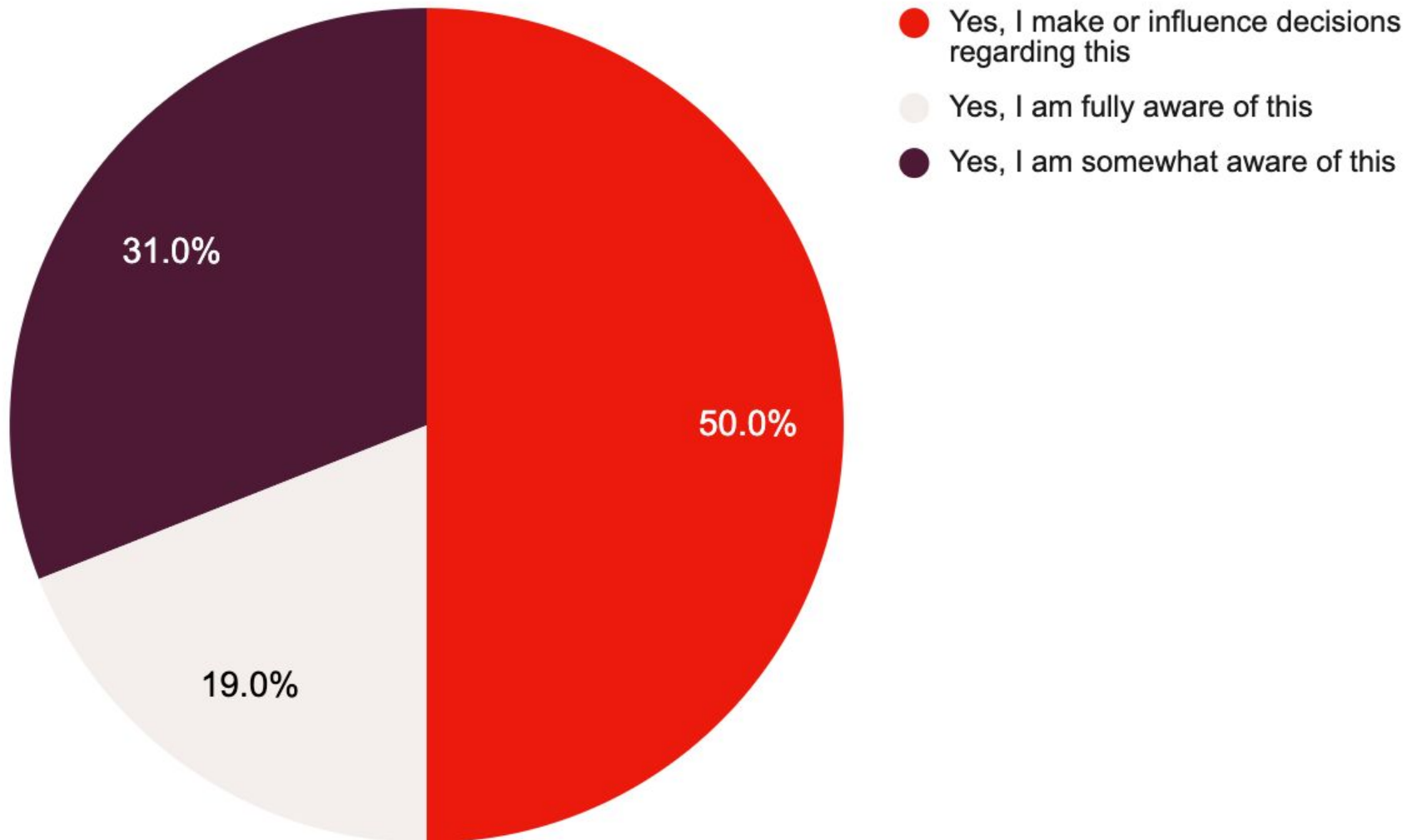
Current responsibility



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

Base: 215

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: 205

Thank you!

fastly[®]