# Fastly Global Security Research 2023

## DACH Findings

November 2023

Research conducted by
SAPIO Research

# Project overview and methodology

- The survey was conducted among **205** IT Decision Makers (more than 2/3 respondents directly make or influence cybersecurity decisions) in Germany, Austria and Switzerland (DACH). 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 ± **6.9%** 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: 205

**Country of residence**

**Department**

IT: 43%

Ops: 34%

Executive Leadership : 23%

**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% | 31% | 16% | 9% | 7% | 22% |

**Industry**

Company sectors – top 3:

Construction / Engineering: 26%

Tech: 17%

Financial: 14%

**Decision making (cyber security)**

- 72% make or influence cybersecurity decisions
- 16% are fully aware of decisions regarding cybersecurity
- 12% 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**

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

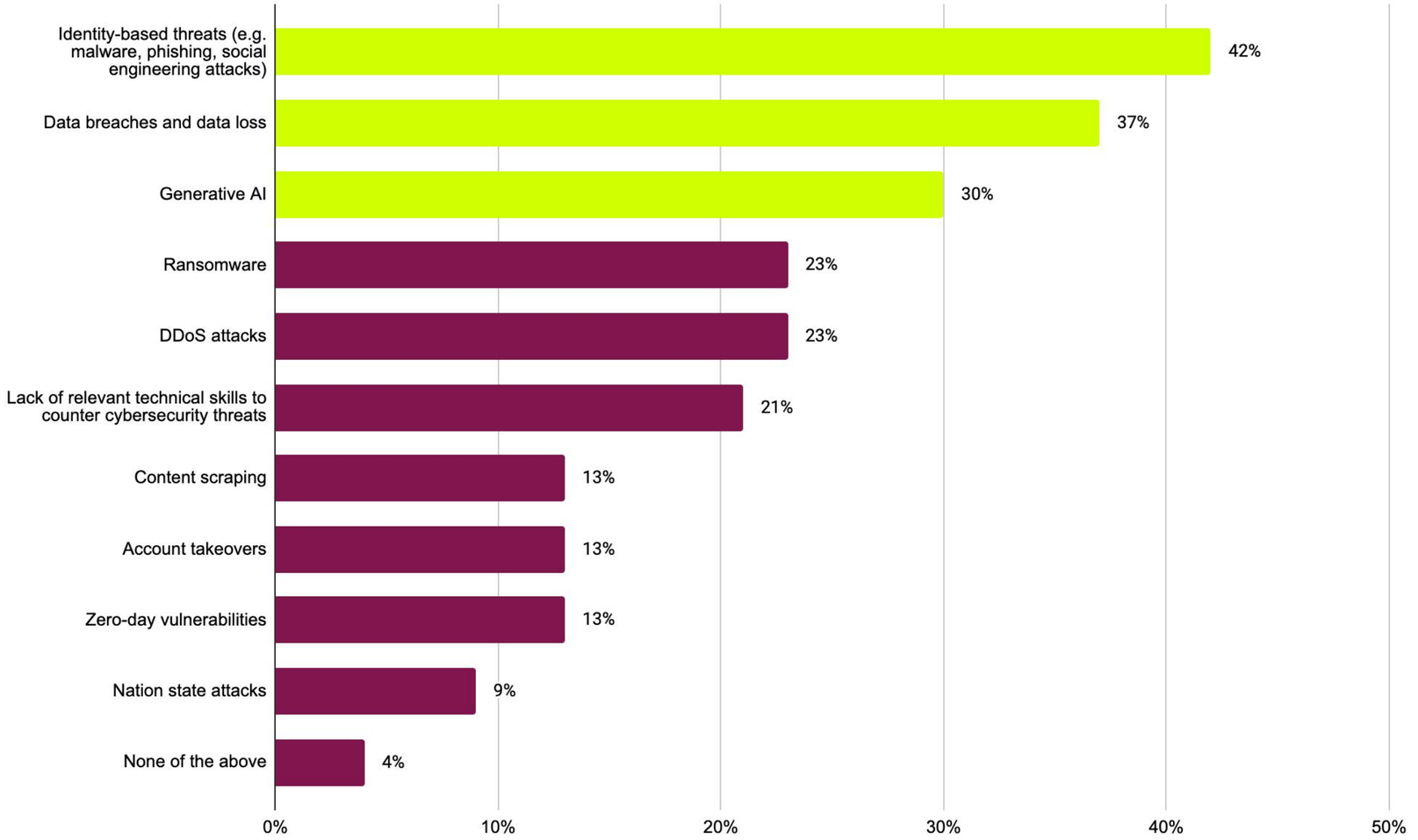
Defining approaches to new and emerging cybersecurity threats (38%), making cybersecurity more accessible (35%) and improving cybersecurity skills through training and/or talent acquisition (35%) are the main security priorities over the next year

**55%** say that their organisations cybersecurity strategy has **hampered business innovation**

On average, **52%** of cybersecurity tools are fully deployed/active

# Main Findings

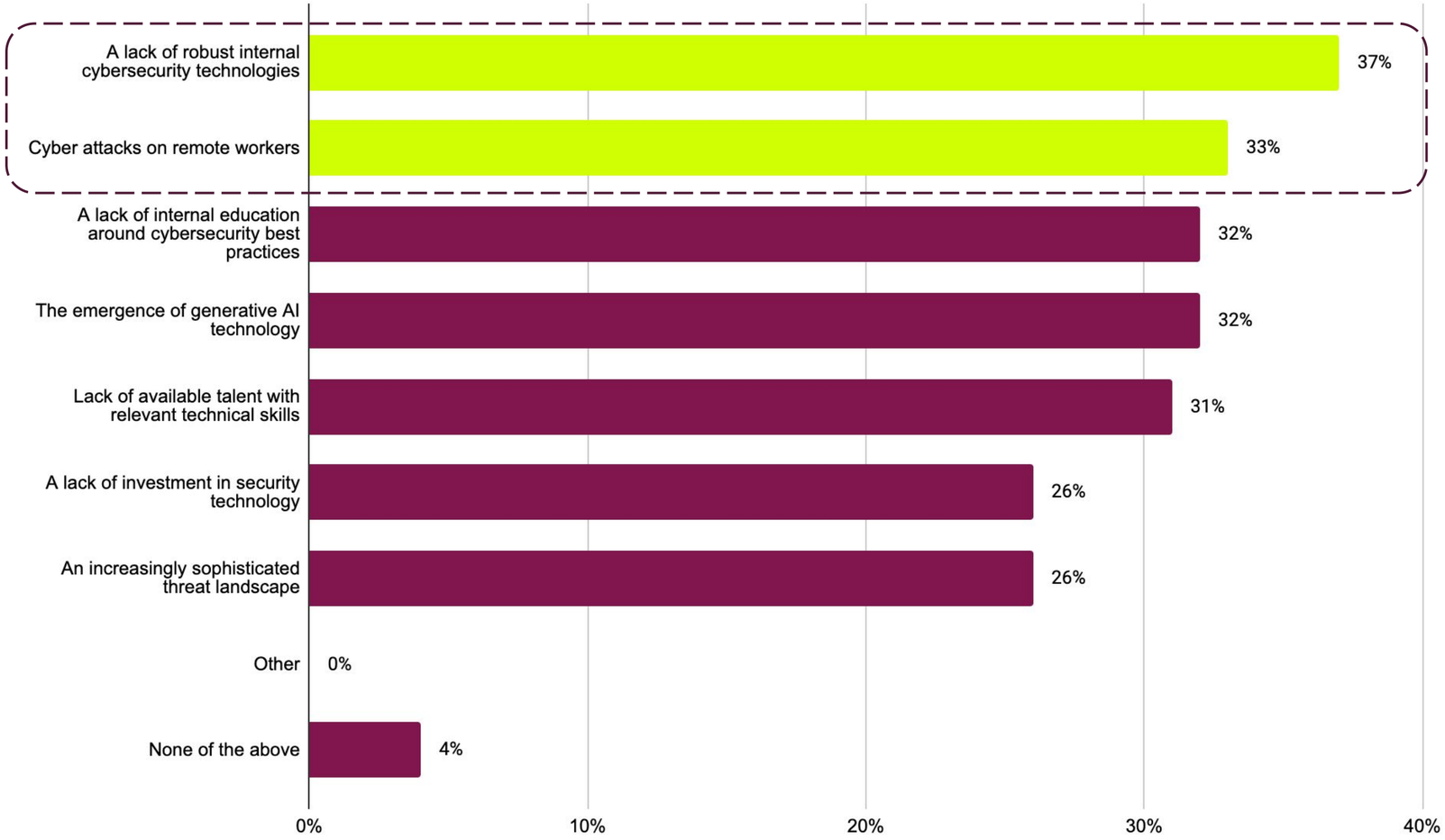
# Identity-based threats (42%), data breaches and data loss (37%), and Generative AI (30%), are viewed as the biggest cybersecurity threats to organisations over the next 12 months




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

Base: 205

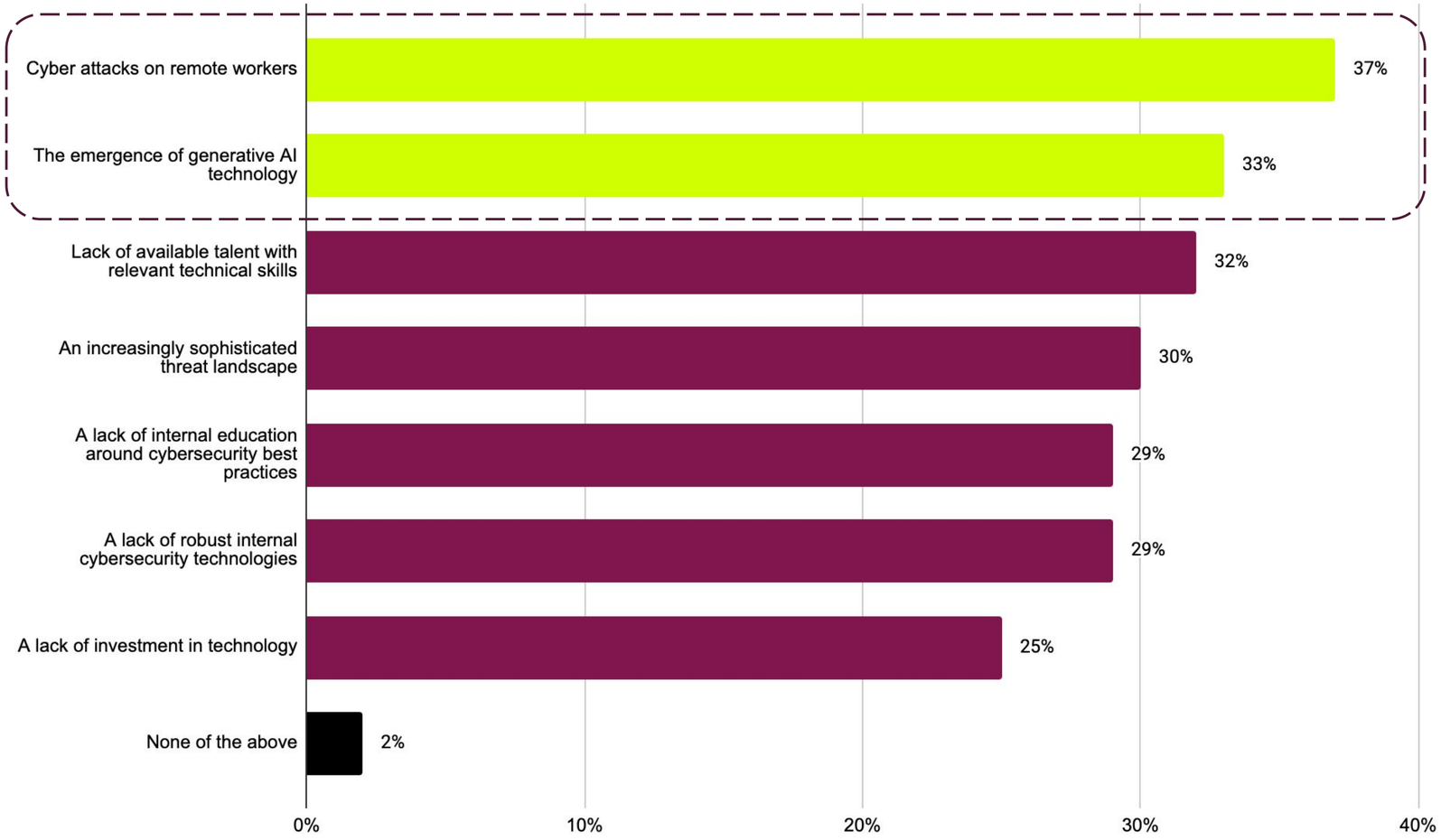
# Over the last 12 months, a lack of robust internal cybersecurity technologies (37%), cyber attacks on remote workers (33%) were the main drivers of cybersecurity threats




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

Base: 205

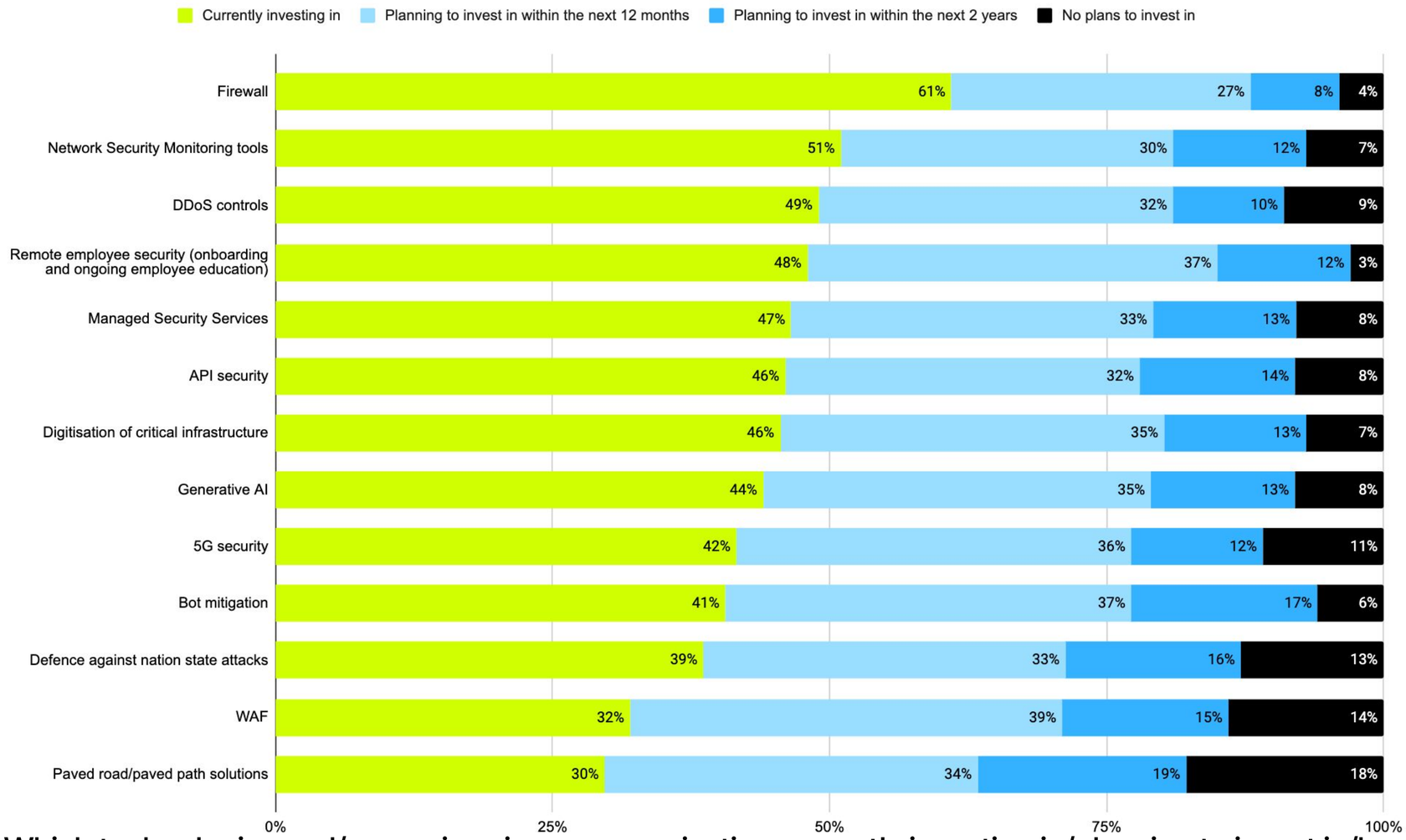
# Over the next 12 months, cyber attacks on remote workers (37%) and the emergence of generative AI (33%) are seen as the biggest drivers of cybersecurity threats




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

Base: 205

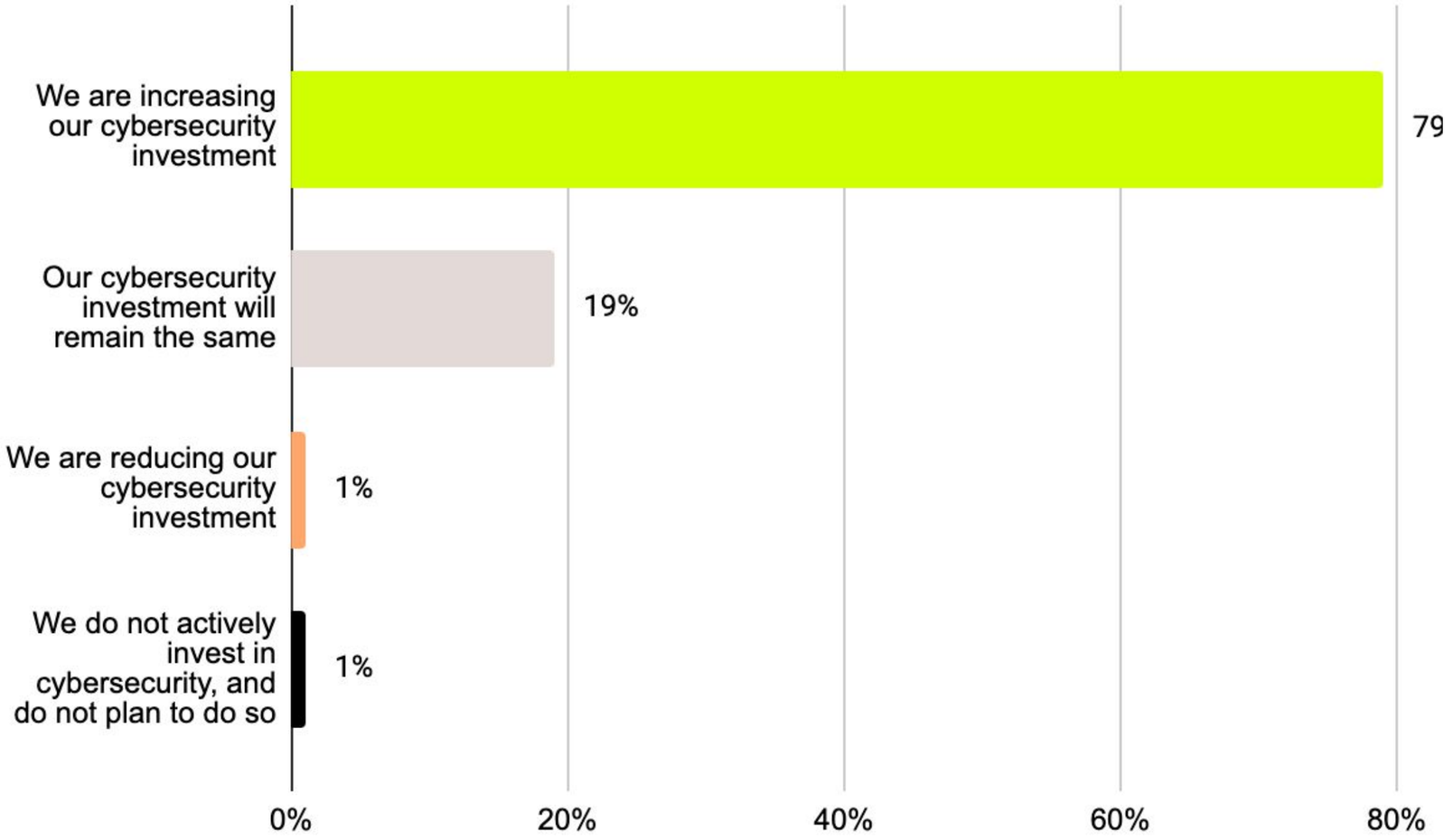
# 61% are currently investing in ‘Firewall’ technology, and around half are investing in ‘Network Security Monitoring tools’ (51%)
# 18% have no plans to invest in paved road/ paved path solutions




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

Base: 205

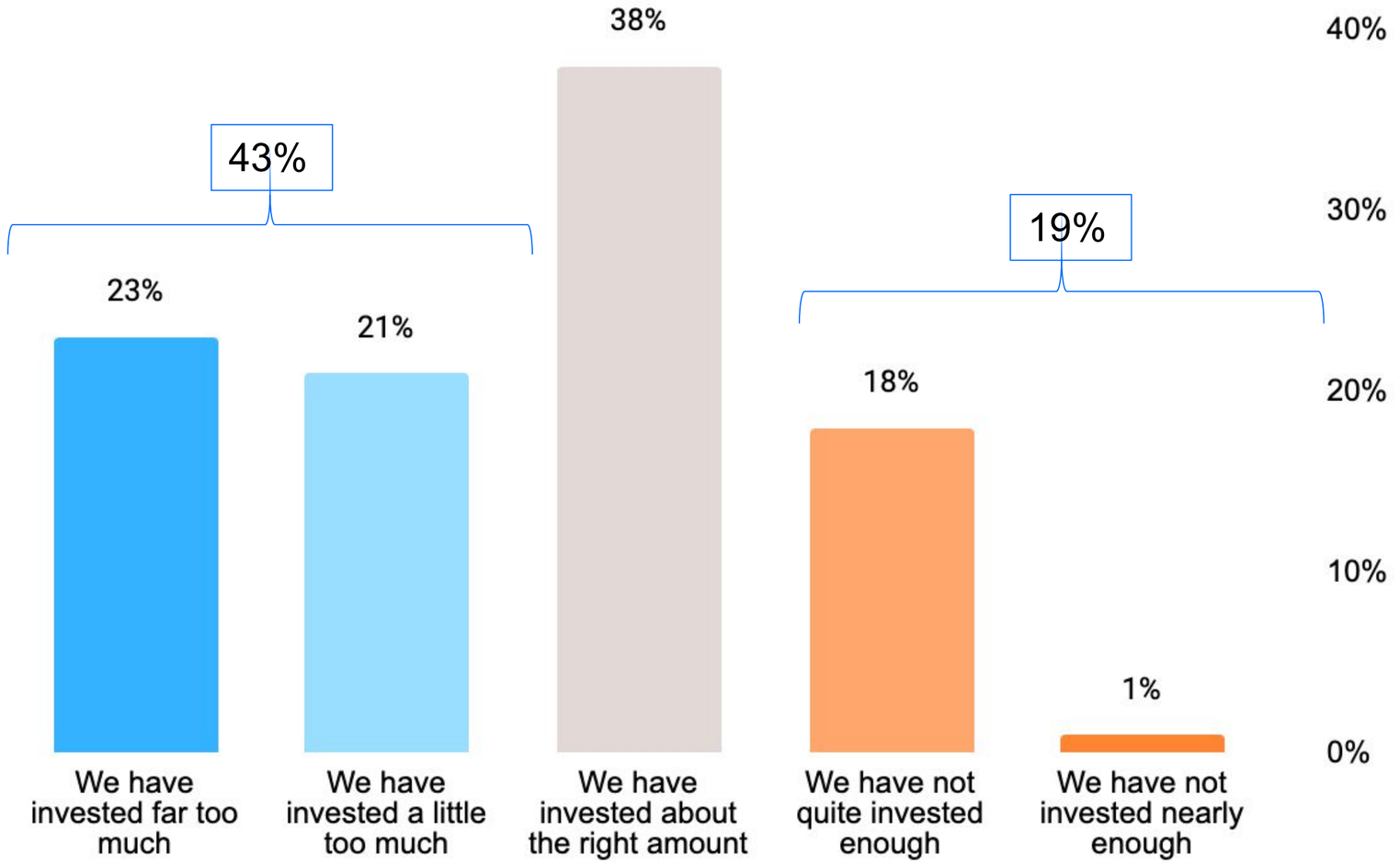
# 79% of respondents are increasing their cybersecurity investment




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: 205

# 43% of respondents have invested too much into cybersecurity over the past 12 months
*19% say they have not invested enough*

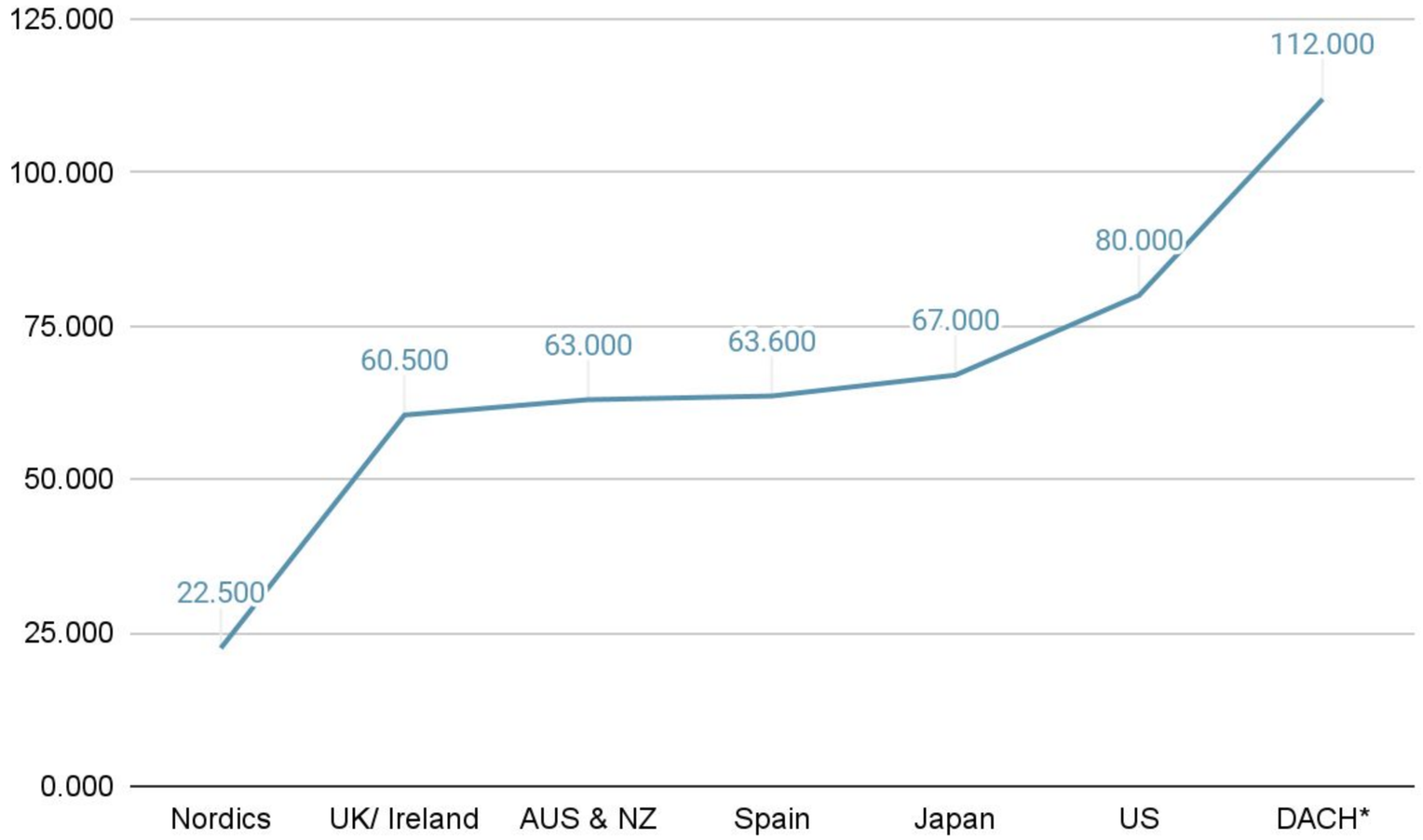



*only asked to those who invest in cybersecurity

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: 203*

# On average (median), $112,000 USD are spent per year on web application and API security control/tools in DACH



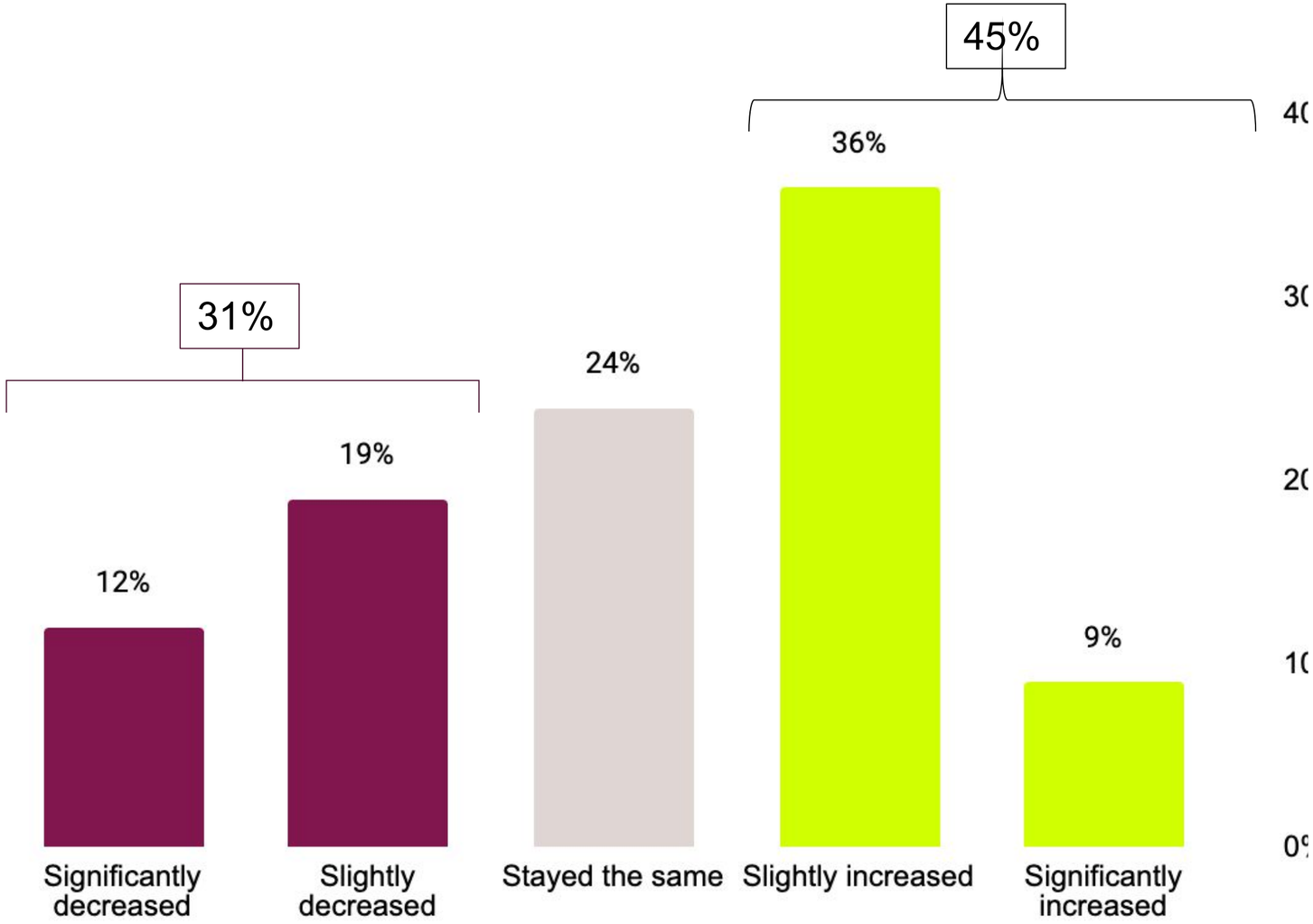

*The sample for DACH countries had a larger proportion of companies with more than 75,000+ employees

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: 205

# 45% of respondents have increased talent spending, with 31% having decreased talent spending

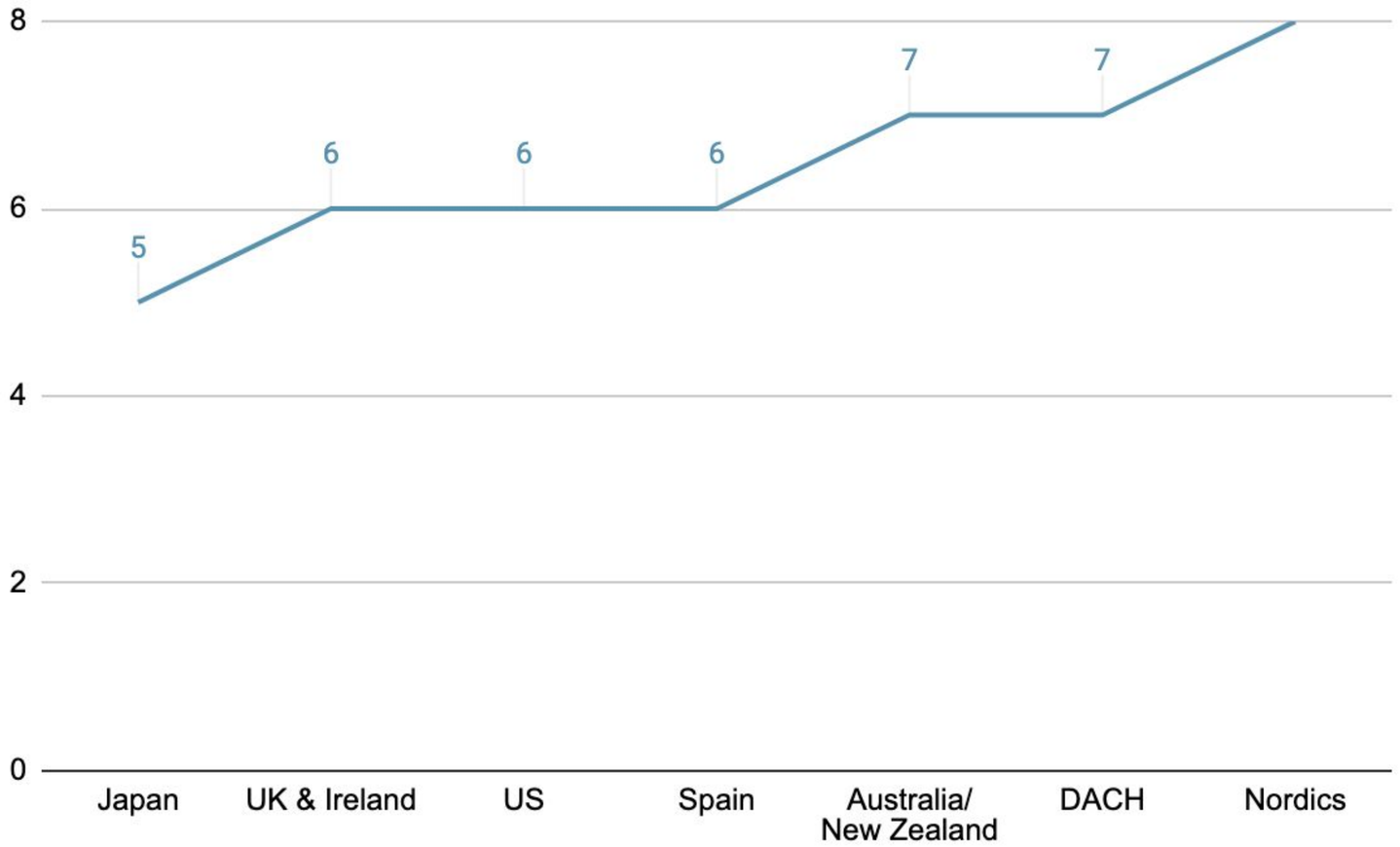



Q5b. How has your talent spending (e.g. new hires, wages) for cybersecurity changed, if at all? Select one

Base: 205

# On average (median), organisations in DACH rely on 7 network and application cybersecurity solutions

**Overall median**: 6

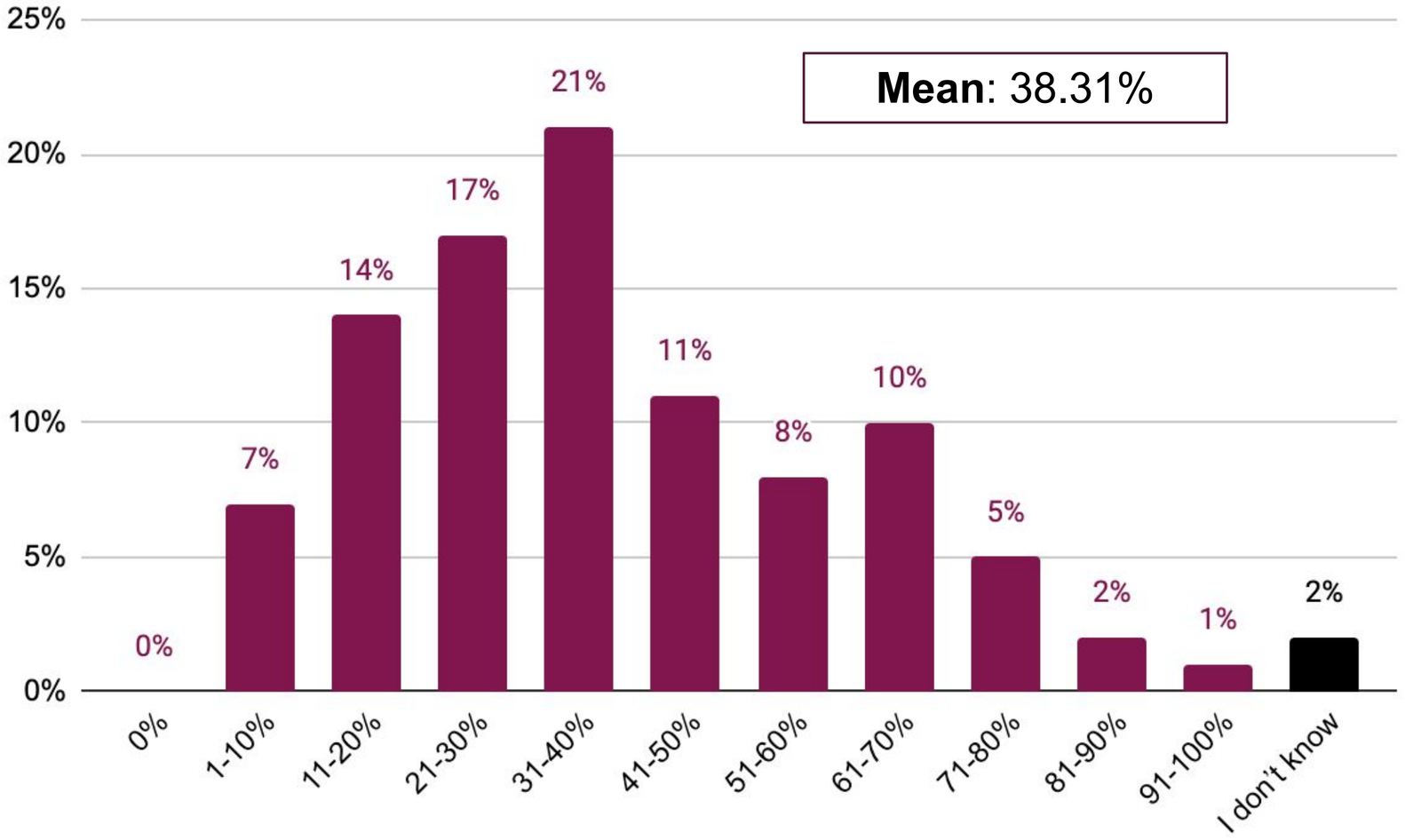



2022 Survey:
Japan **4**
Spain **5**
US **5**
UK & Ireland **6**
AUS & NZ **5**
DACH **5**
Nordics **7**

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

Base: 205

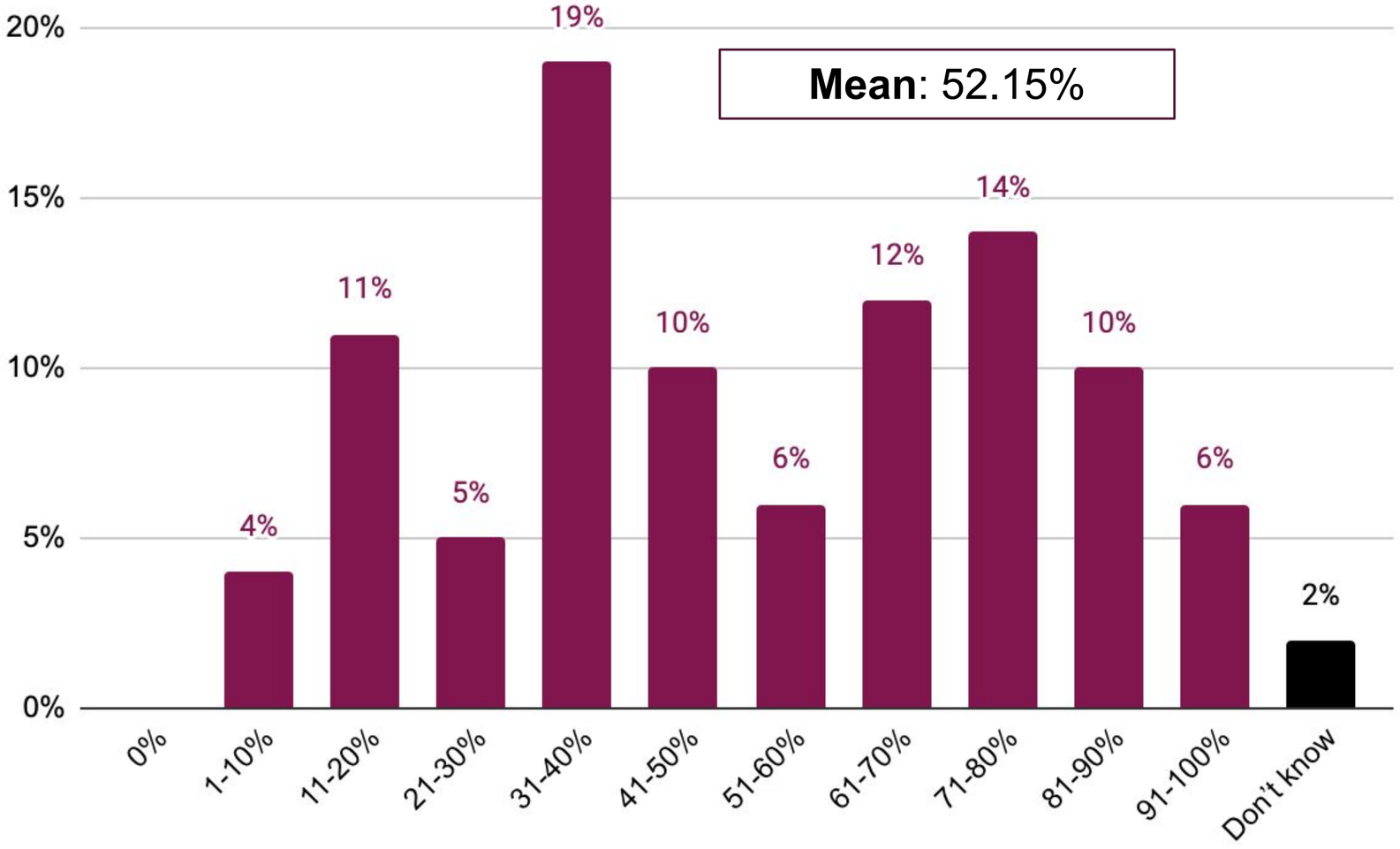
# On average, 38% of network and application cybersecurity solutions overlap




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

Base: 205

# On average, only 52% of cybersecurity tools are fully active/ deployed



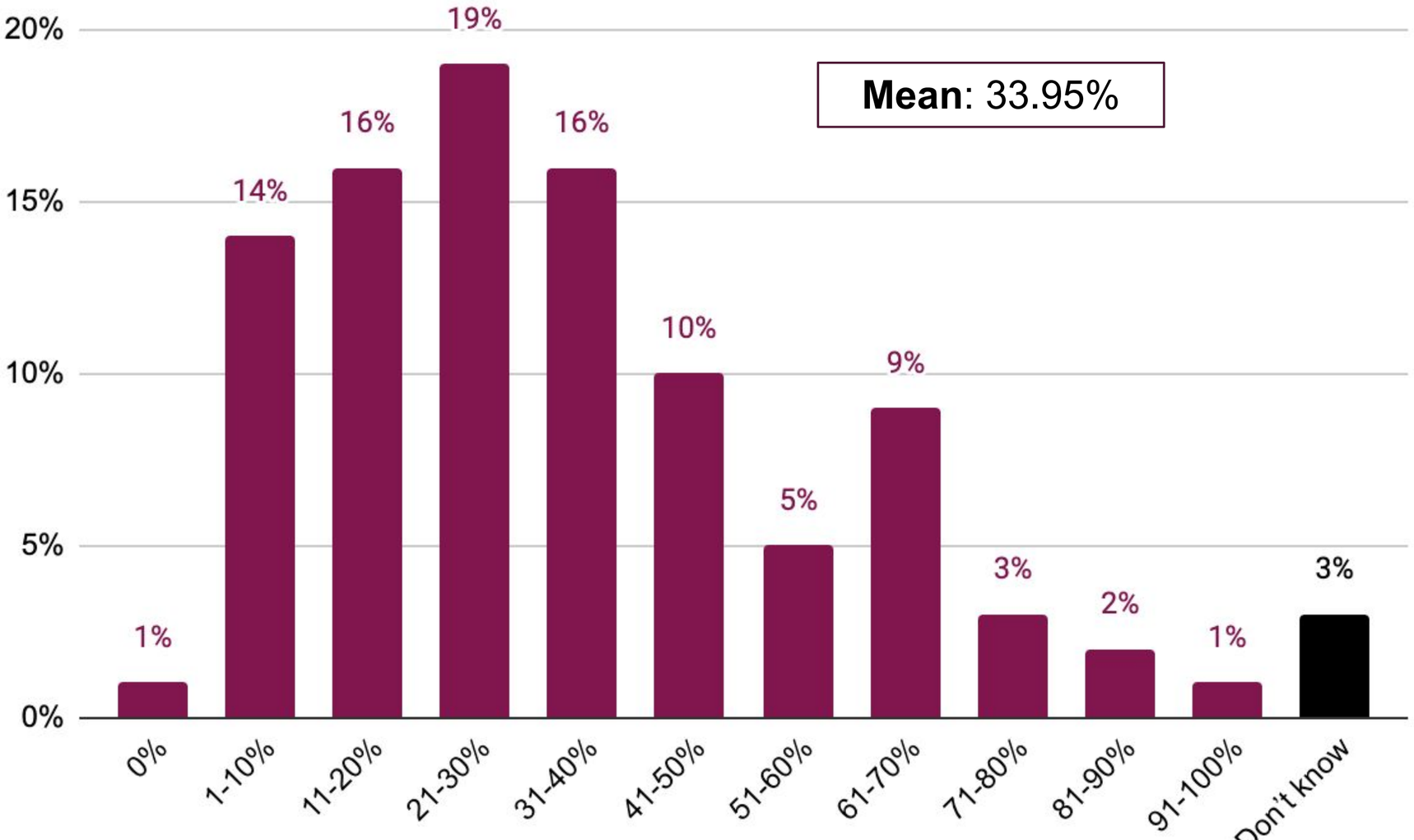

Q7. What percentage of your cybersecurity tools are fully active/deployed? Select one





Base: 205

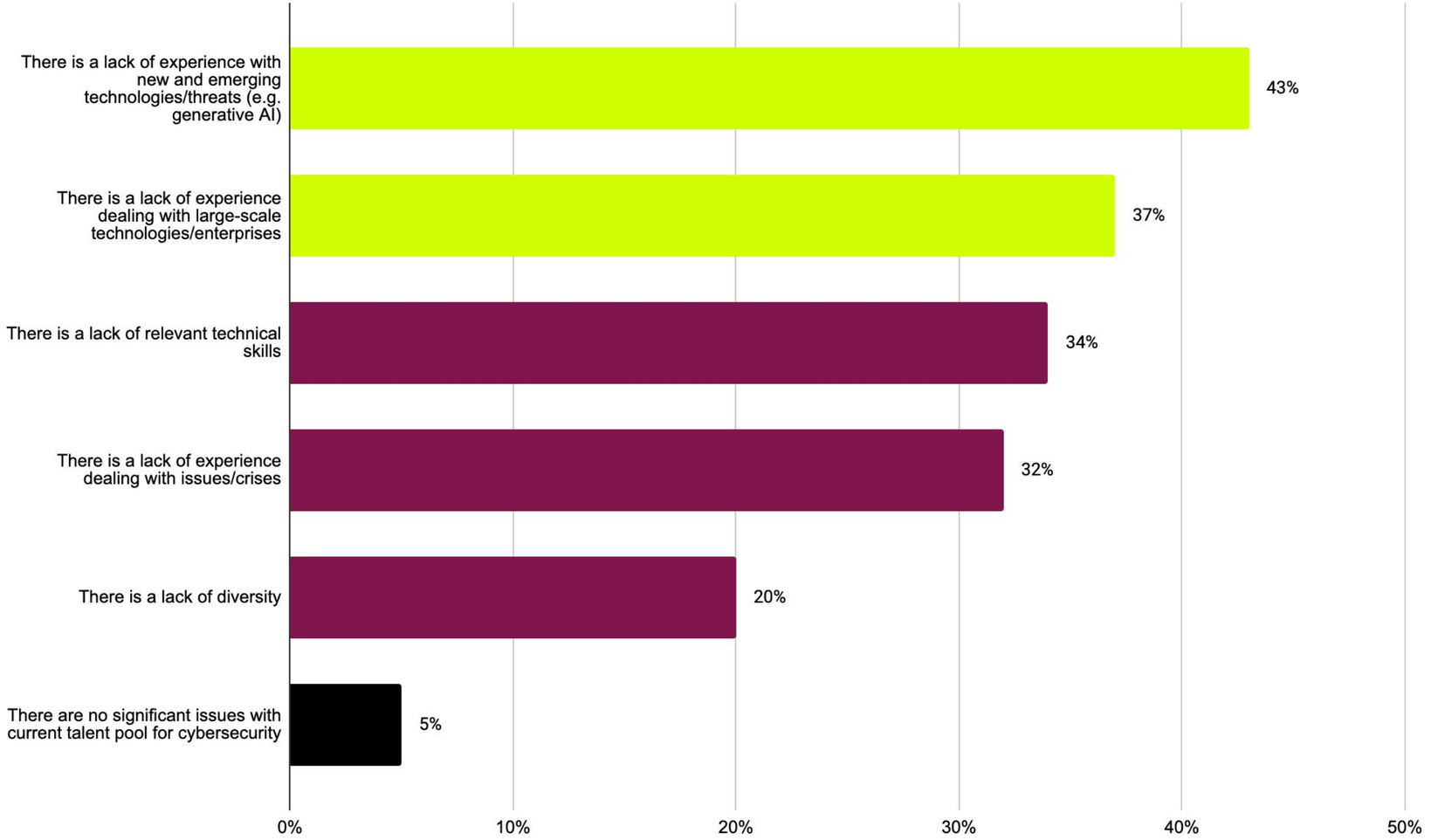
# On average, 34% of security alerts detected by an organisations WAF are false alerts




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

Base: 205

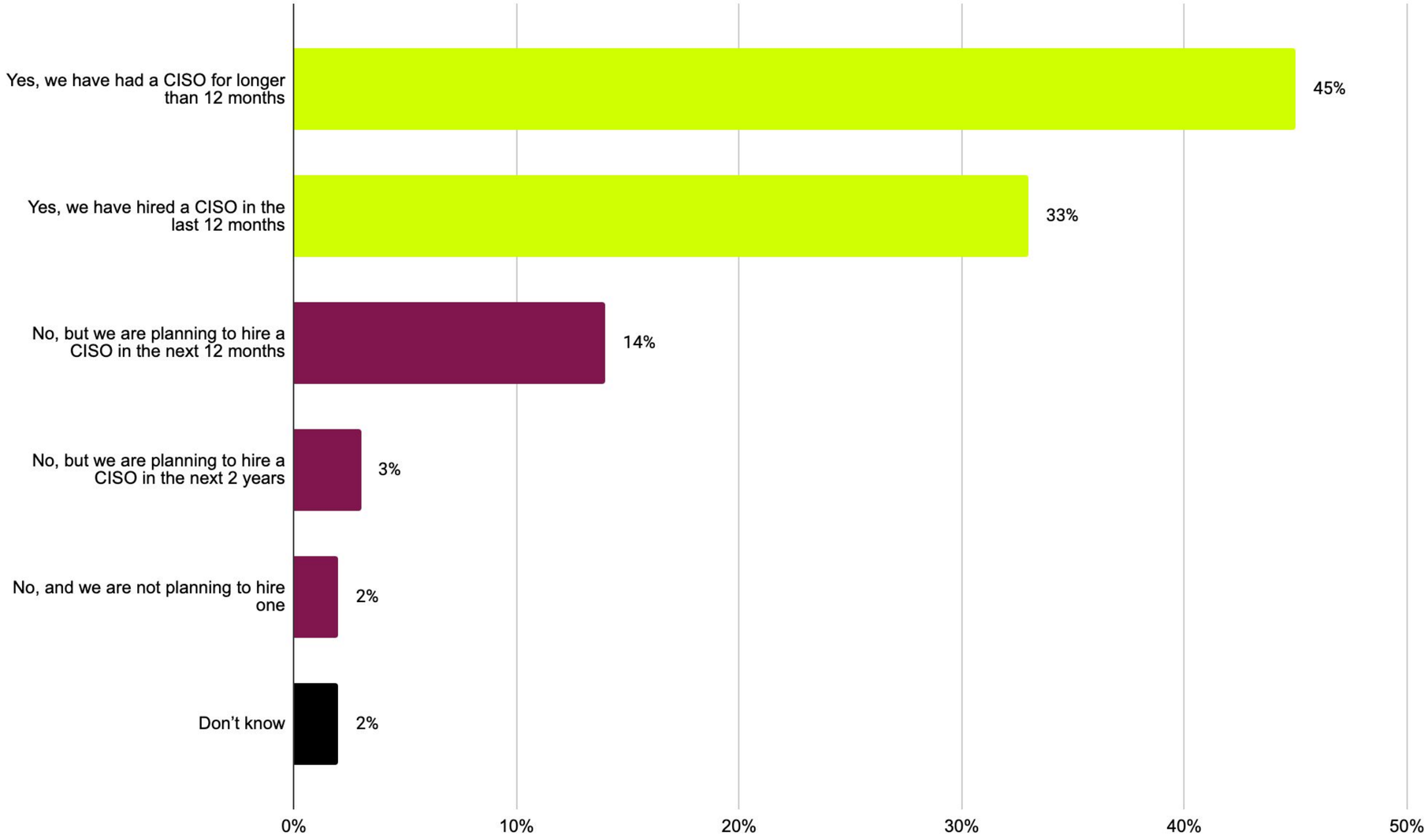
# Respondents feel that the biggest gap among the current talent pool is experience with new and emerging technologies/ threats such as generative AI (43%)




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

Base: 205

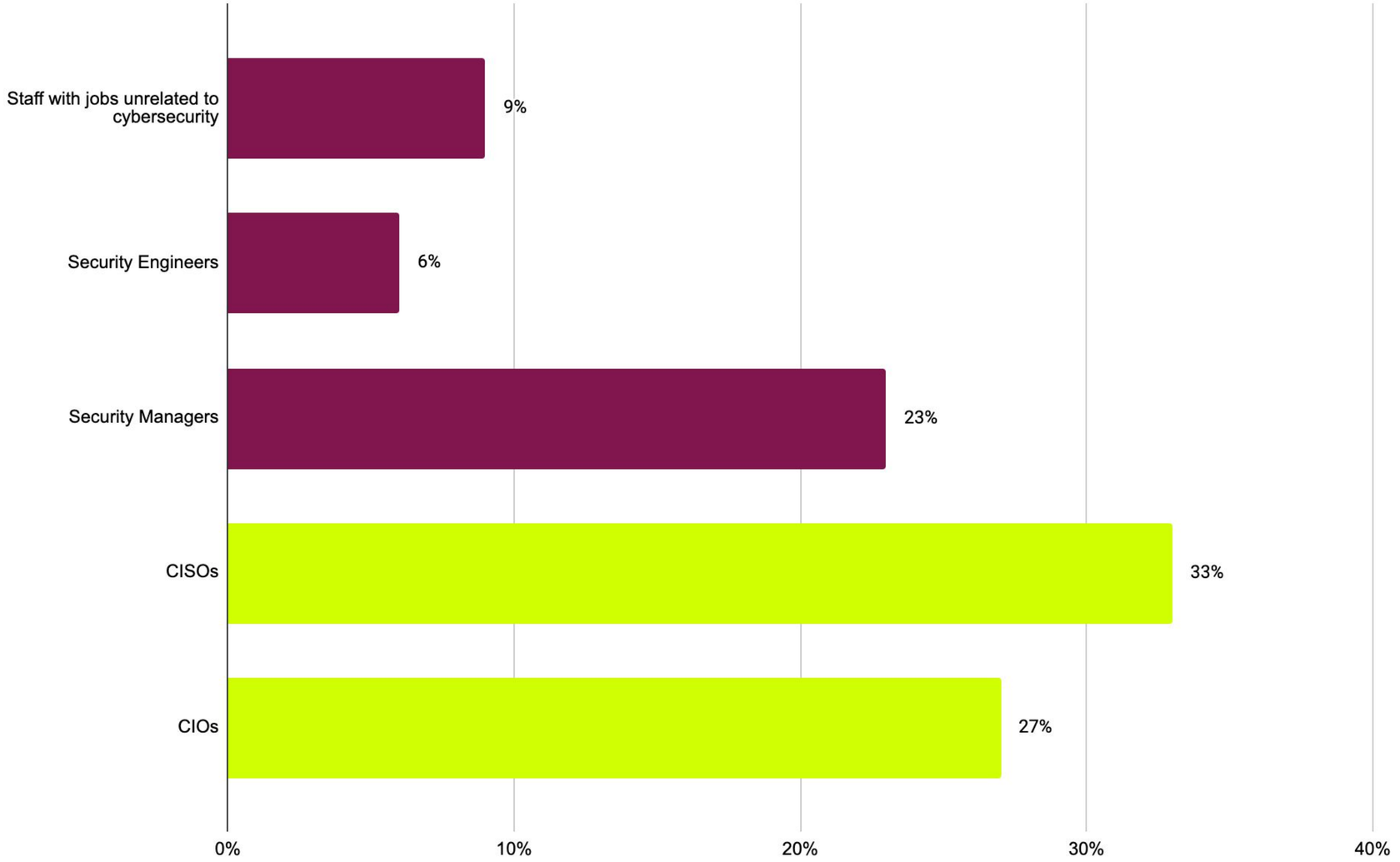
# 78% of respondents have hired a CISO, 33% of those within the last 12 months




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

Base: 205

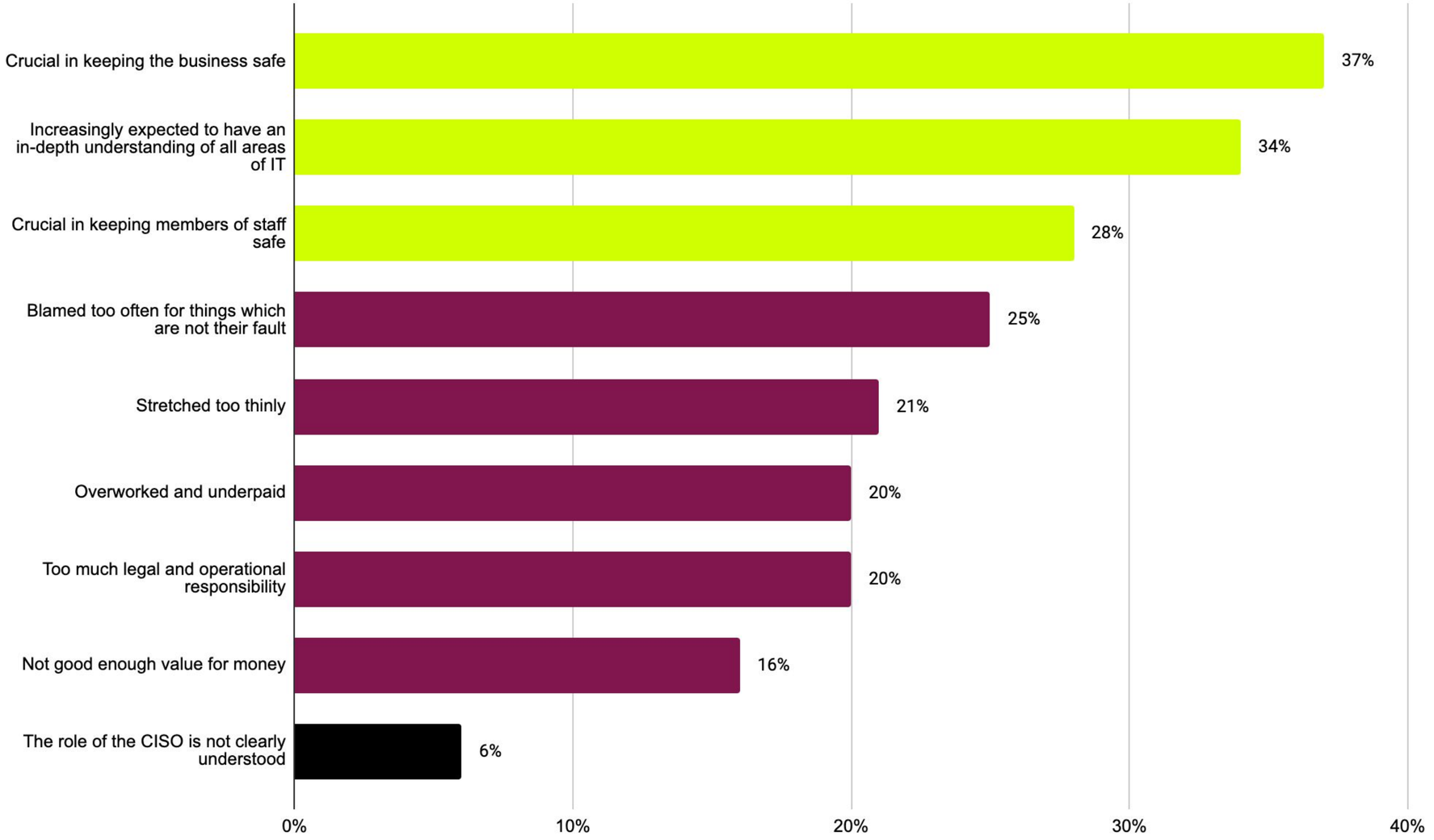
# 33% of respondents think CISOs are often held responsible for cybersecurity incidents, 27% think CIOs are often held responsible




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

Base: 205

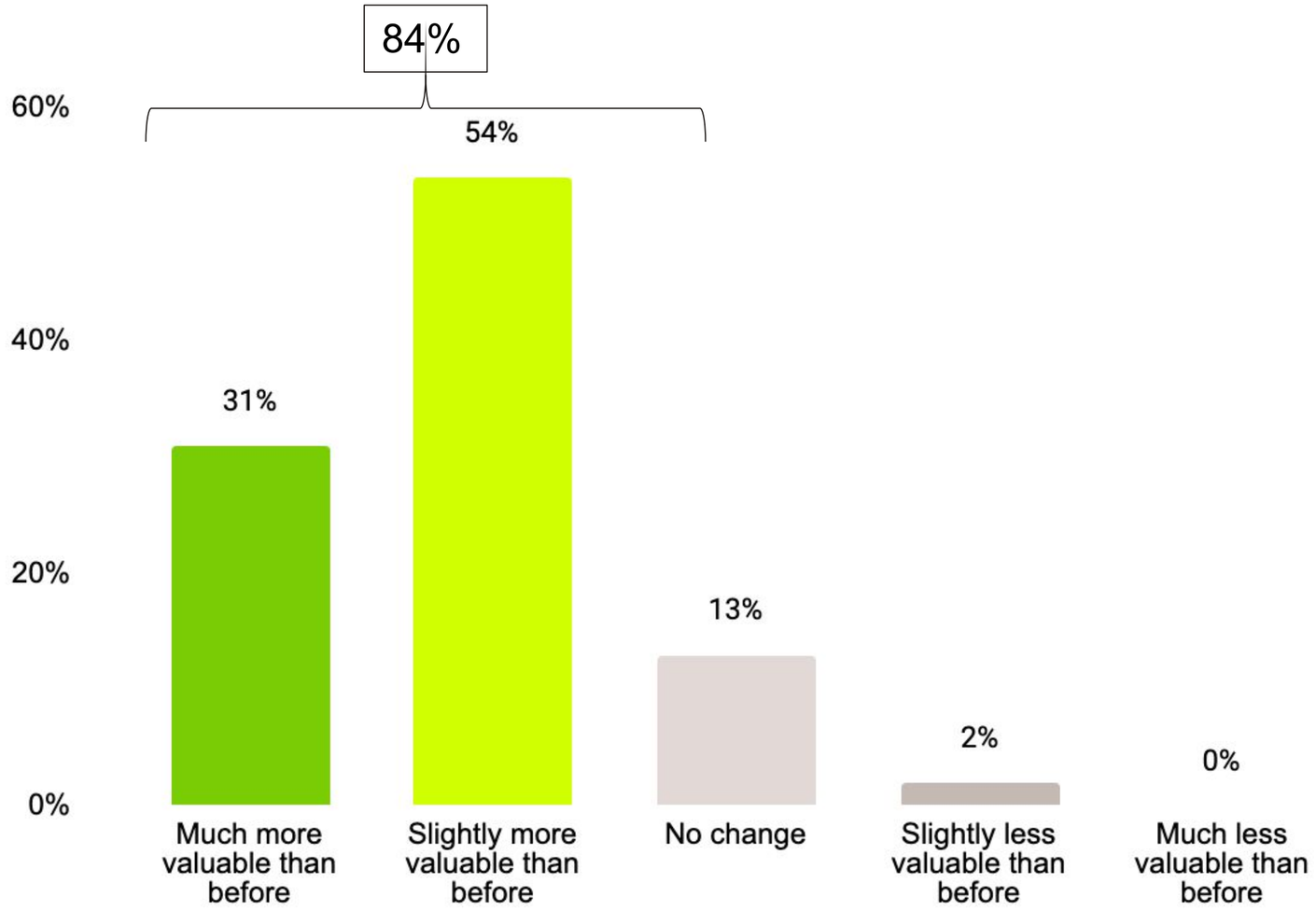
# CISOs are viewed as crucial in keeping the business safe (37%), increasingly expected to have an in-depth understanding of all areas of IT (34%), and crucial in keeping members of staff safe (28%)




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

Base: 205

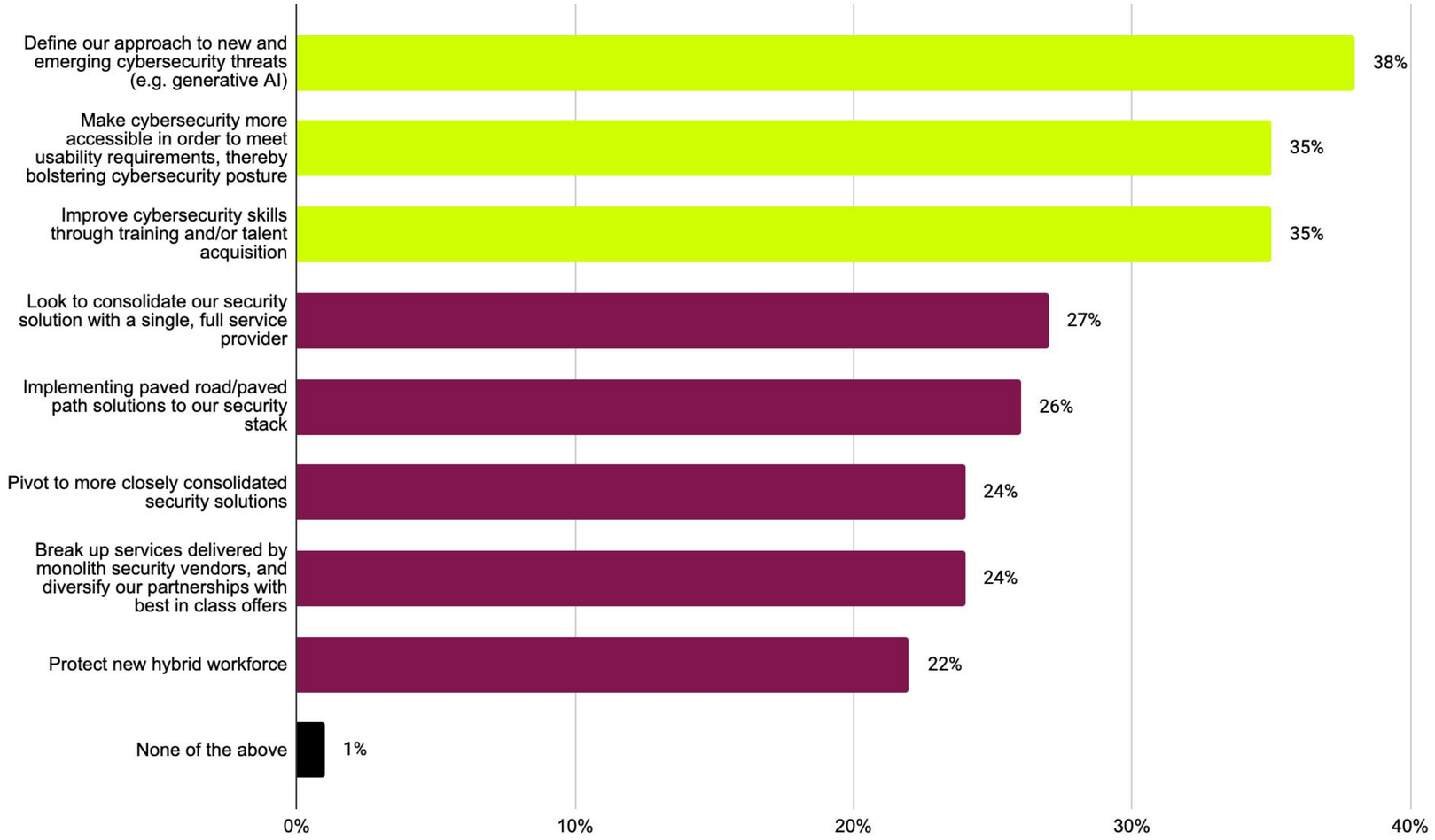
# 84% of respondents think their cybersecurity programme has become more valuable over the last 12 months




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: 205

# Defining approaches to new and emerging cybersecurity threats (38%), making cybersecurity more accessible (35%) and improving cybersecurity skills through training and/or talent acquisition (35%) are the main security priorities over the next year

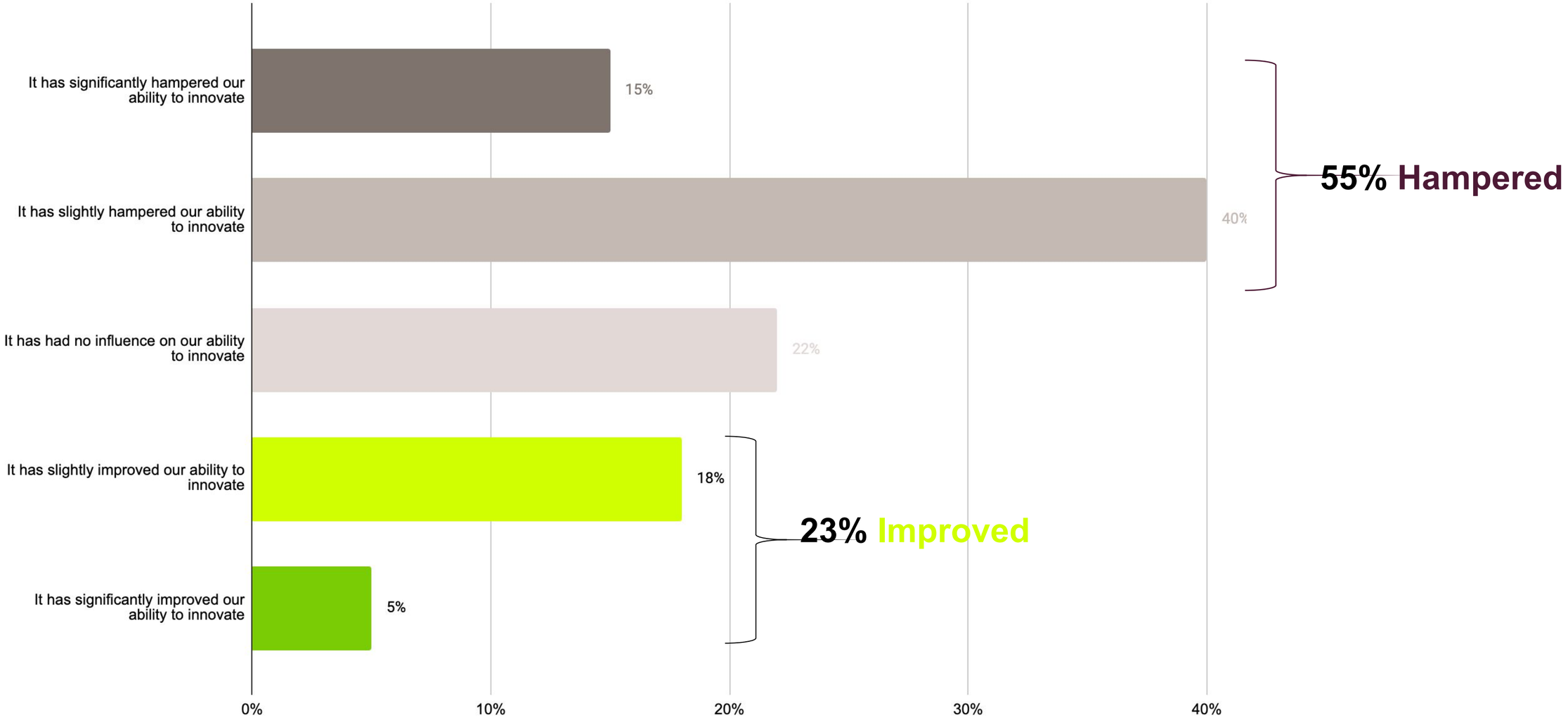



Q13. What are your organisation's security priorities over the next year? Select top three

Base: 205

# 55% say that their organisations cybersecurity strategy has hampered business innovation

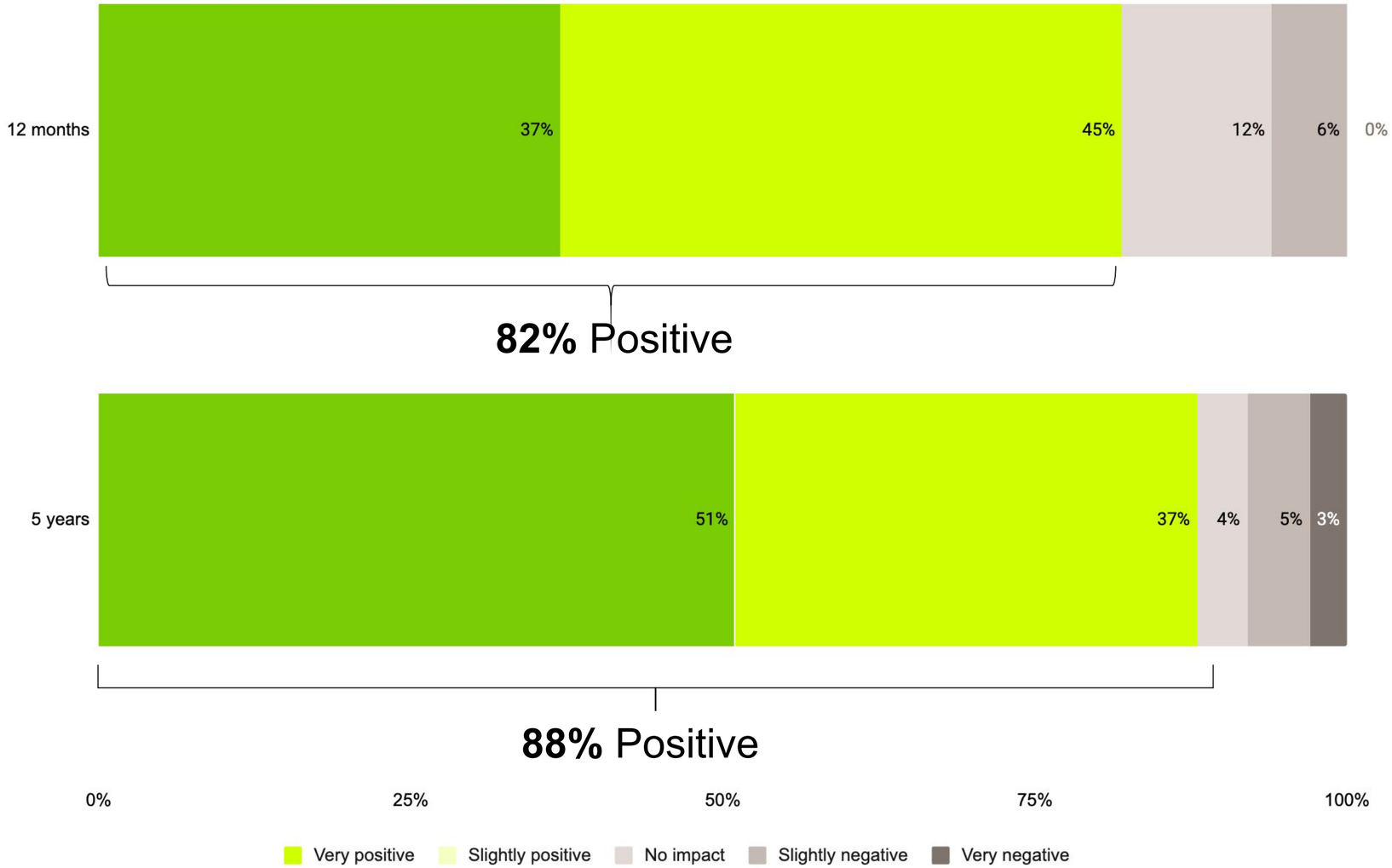
*Only one in five say it has improved innovation (23%)*




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

Base: 205

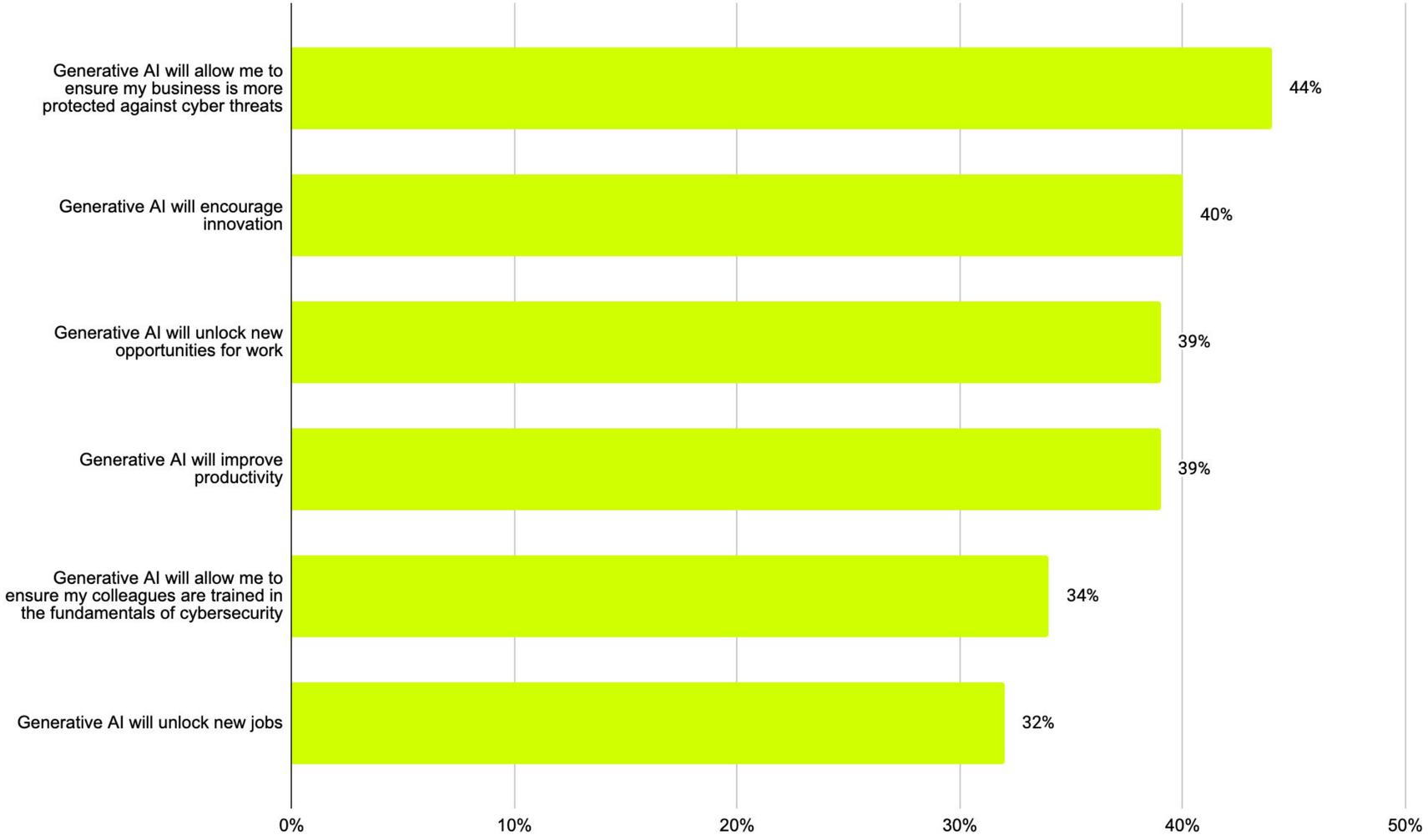
# 82% predict that Generative AI will have a positive impact on cybersecurity over the next 12 months
# 88% predict it will have a positive impact over the next 5 years




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

Base: 205

# Ensuring the business is more protected against cyber threats (44%) and encouraging innovation (40%) are the main positive impacts of Generative AI

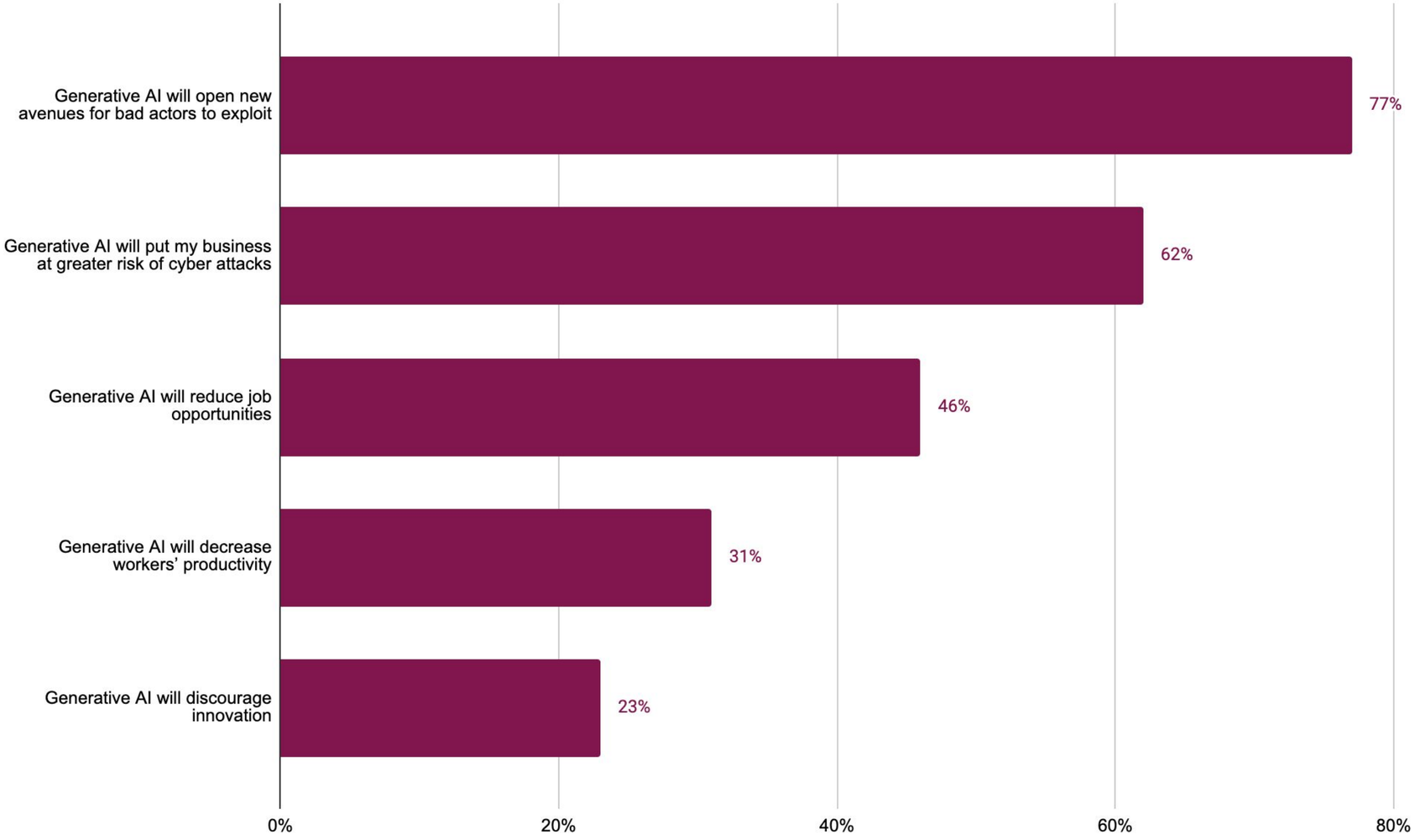



*only asked to those who said generative AI will have a positive impact in the next 12 months

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 : 168*

# There are fears that Generative AI will open new avenues for bad actors to exploit (77%), or that it will put businesses at greater risk of cyber attacks (62%)

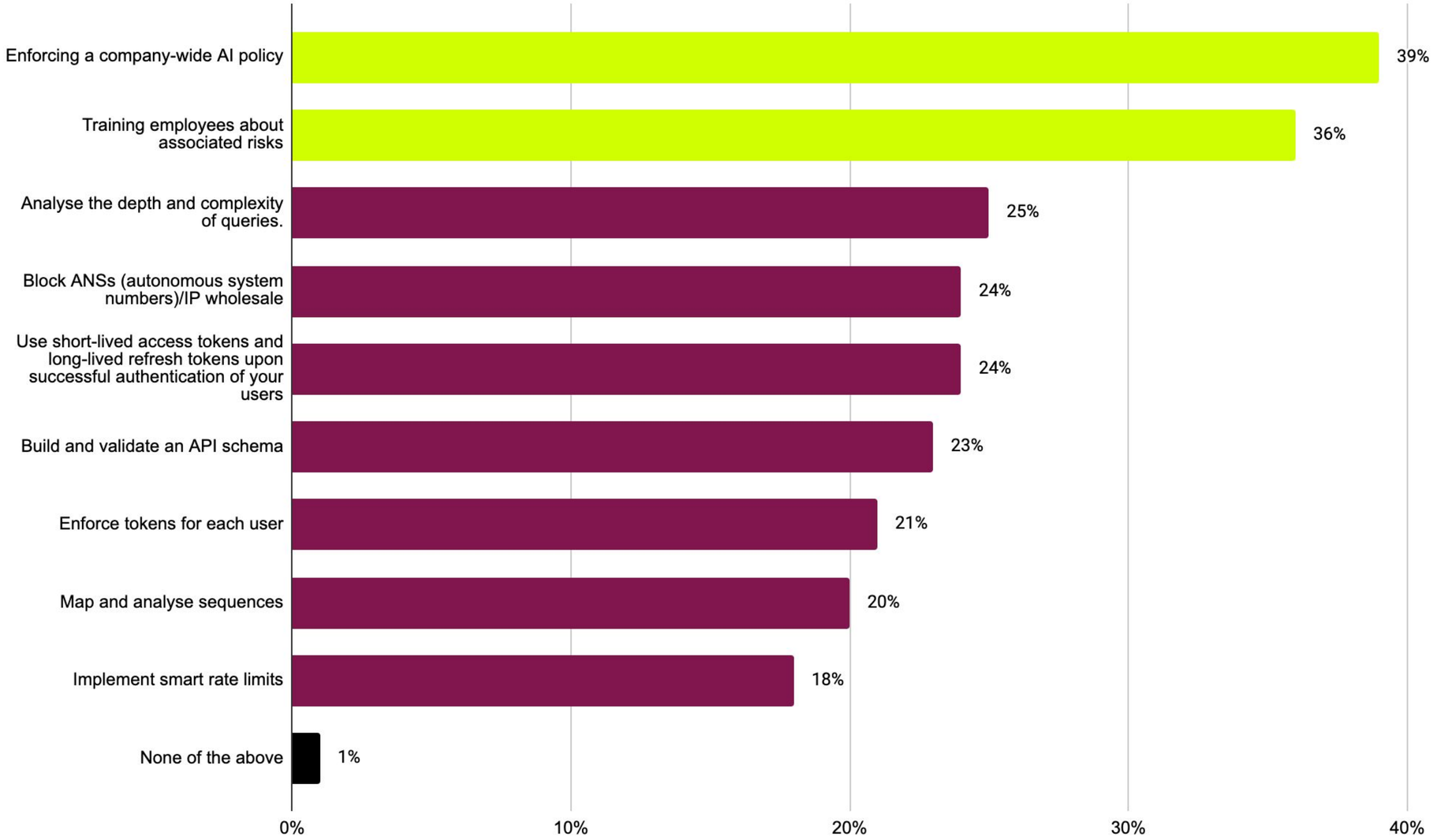



*only asked to those who said generative AI will have a negative impact in the next 12 months

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: 13*

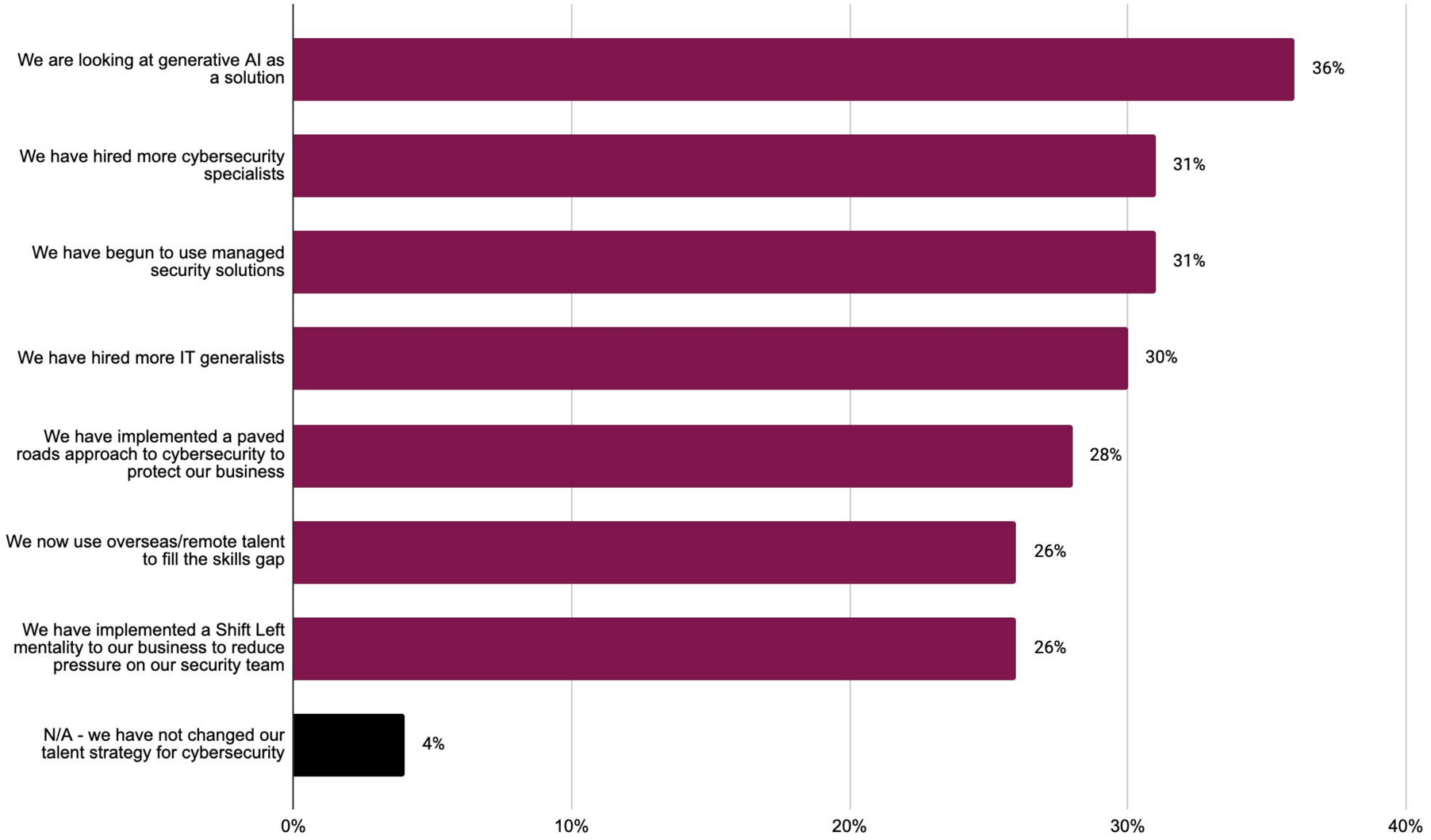
# Enforcing a company-wide AI policy (39%) and training employees on the associated risks (36%) are the top two steps companies are taking to mitigate generative AI security threats




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

Base: 205

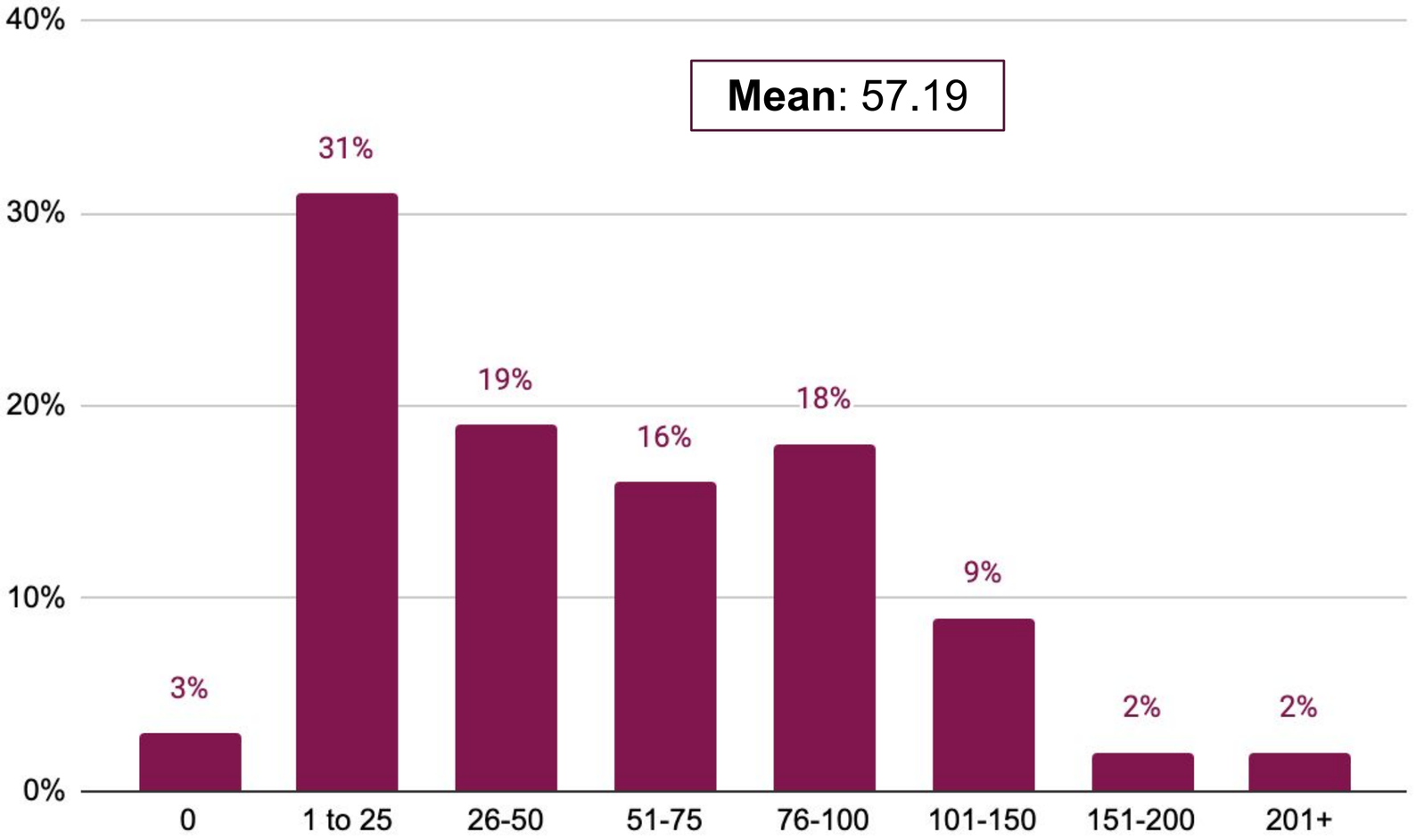
# Companies have been looking at generative AI as a solution (36%) over the last 12 months




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

Base: 205

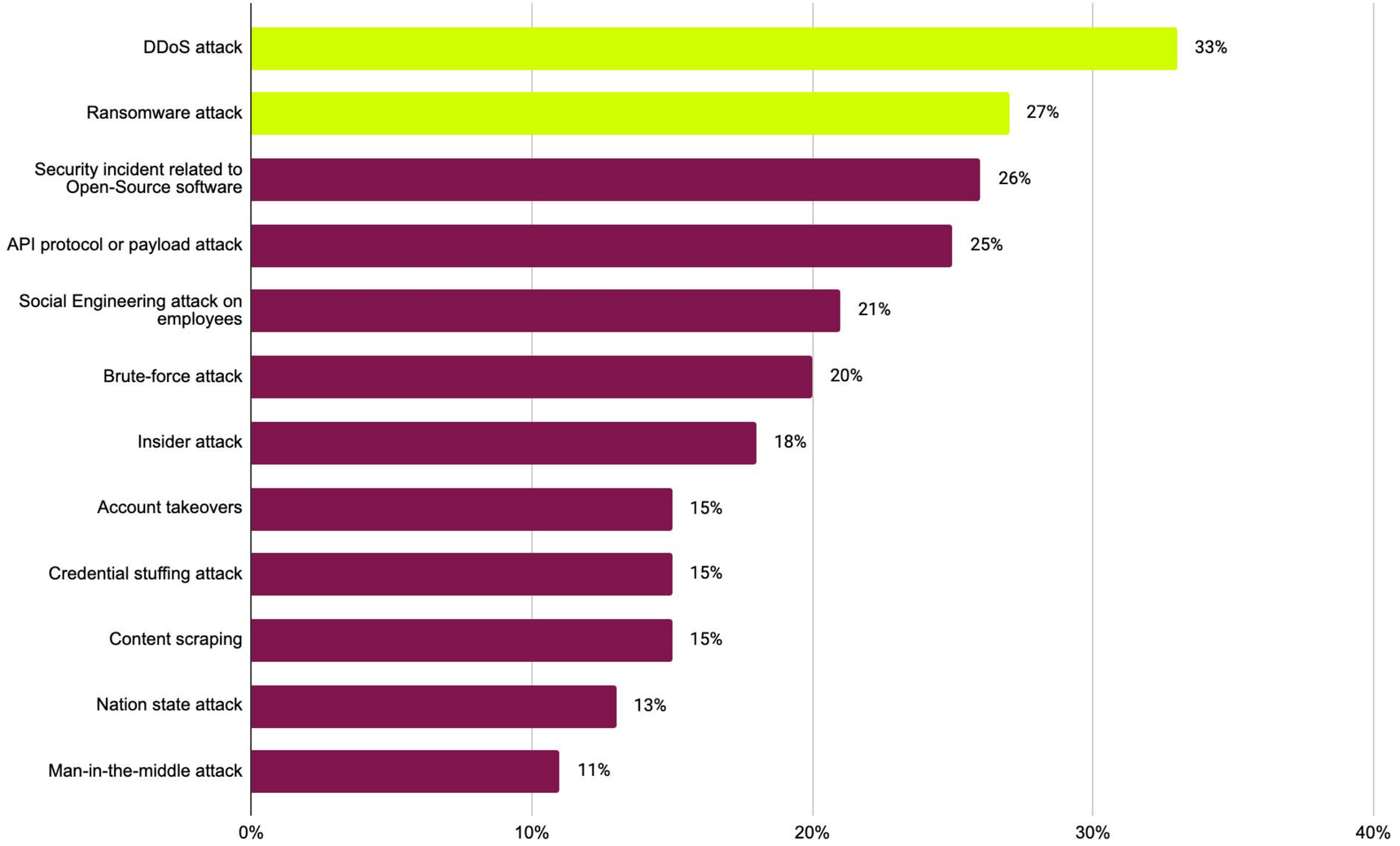
# On average, businesses have suffered 57 cyberattacks in the past 12 months




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

Base: 205

# The most common types of cyberattacks were DDoS attacks (33%) and ransomware attacks (27%)

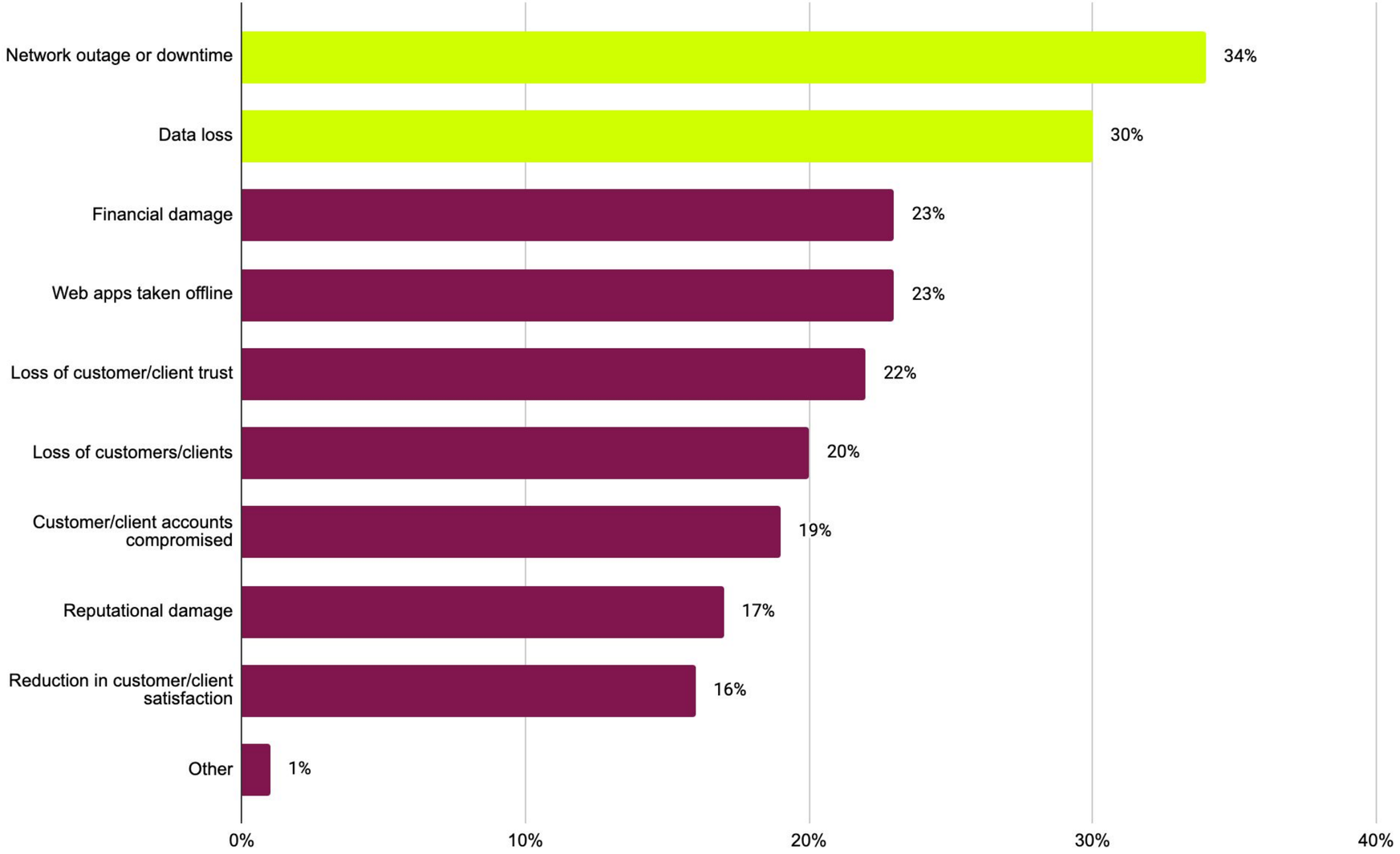



*only asked to those who have experienced a cyber attack

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

Base: 198*

# Network outages or downtime (34%) and data loss (30%) were the main impacts of cyber attacks

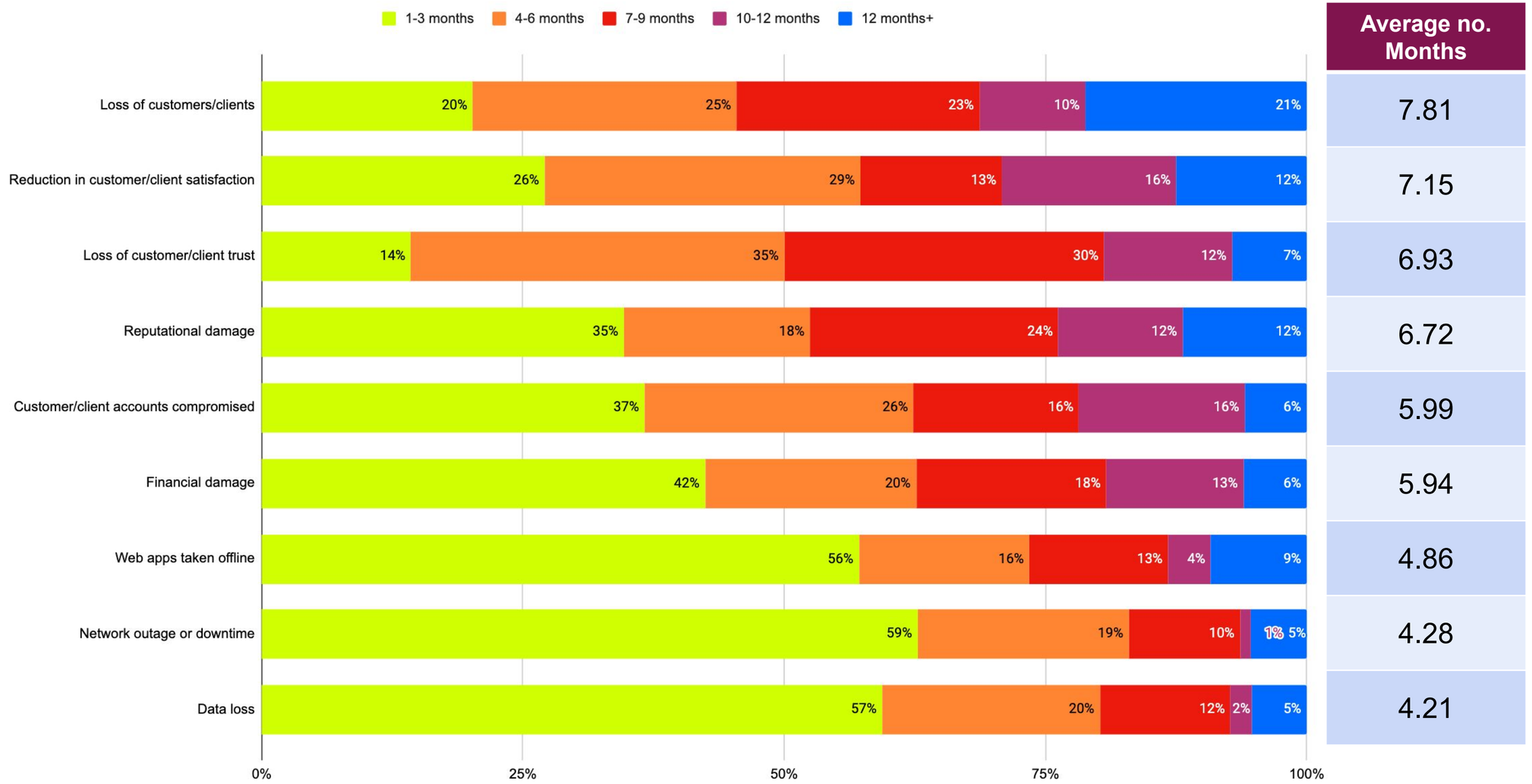



*only asked to those who have experienced a cyber attack

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

Base: 198*

# On average, it will take businesses 8 months to recover from the loss of customers/ clients and reputational damage as a result of cyber attacks



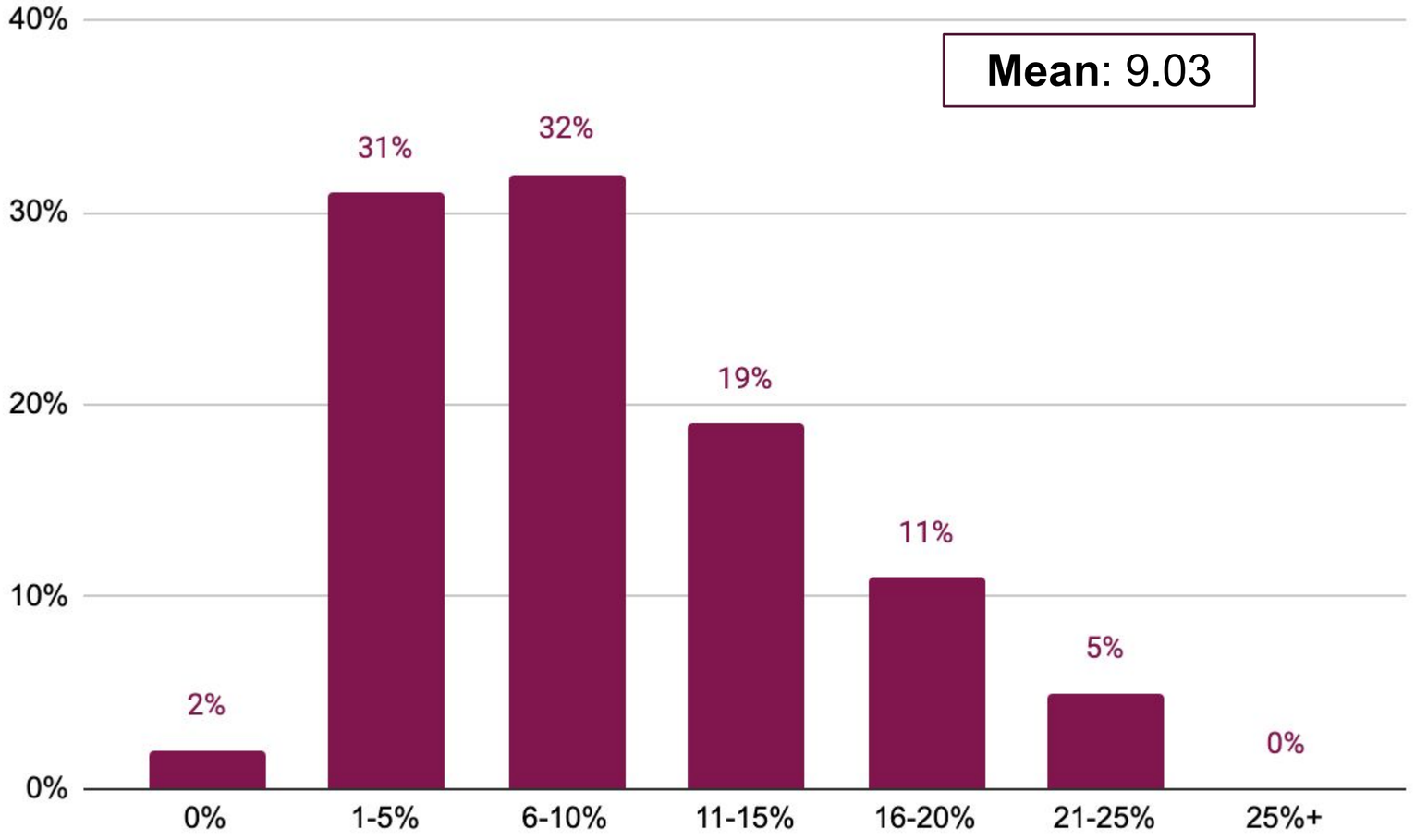

| Average no. Months |
|---|
| 7.81 |
| 7.15 |
| 6.93 |
| 6.72 |
| 5.99 |
| 5.94 |
| 4.86 |
| 4.28 |
| 4.21 |

*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



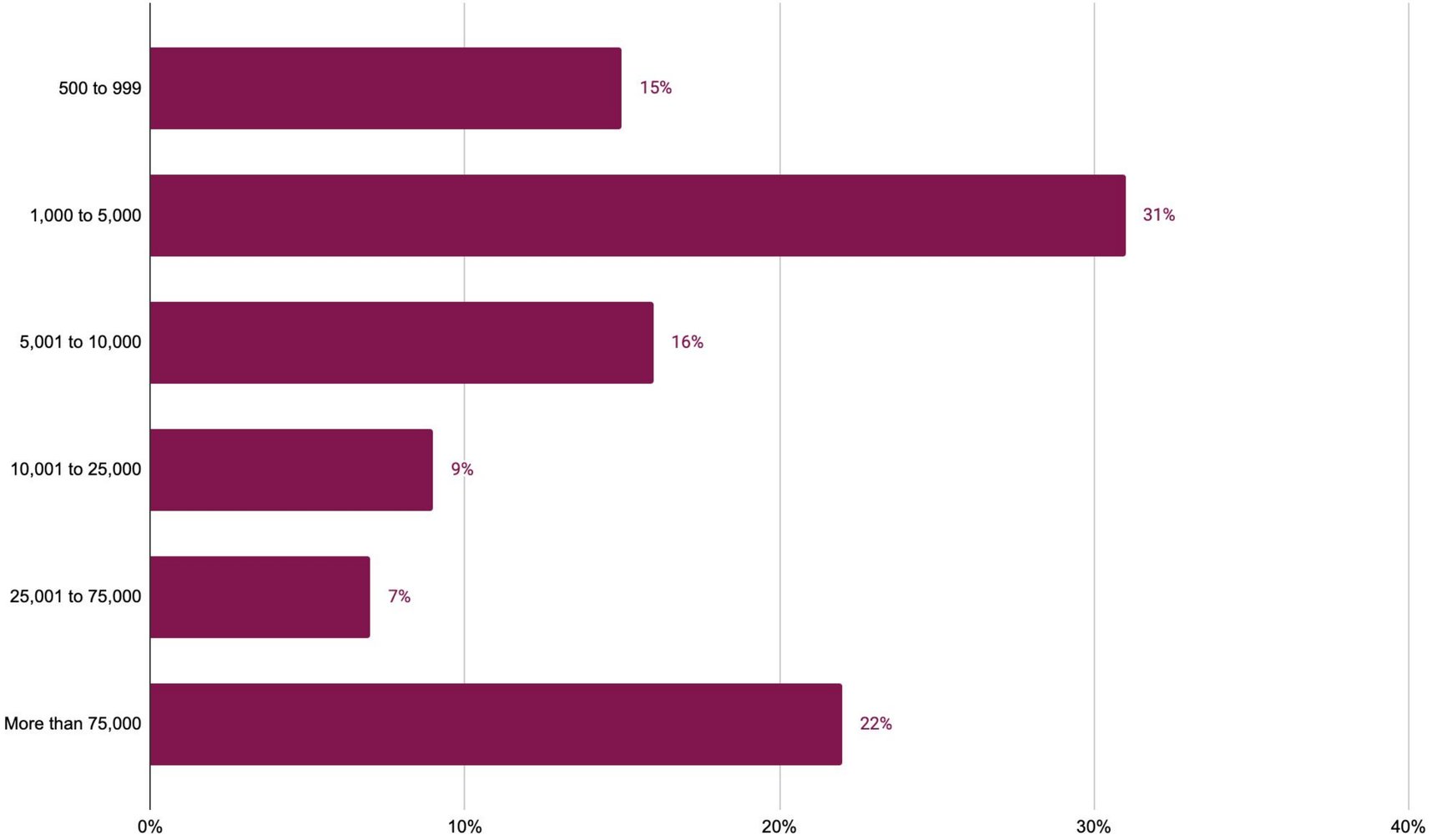

*only asked to those who had experienced each impact at Q22

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: 198*

# Demographics

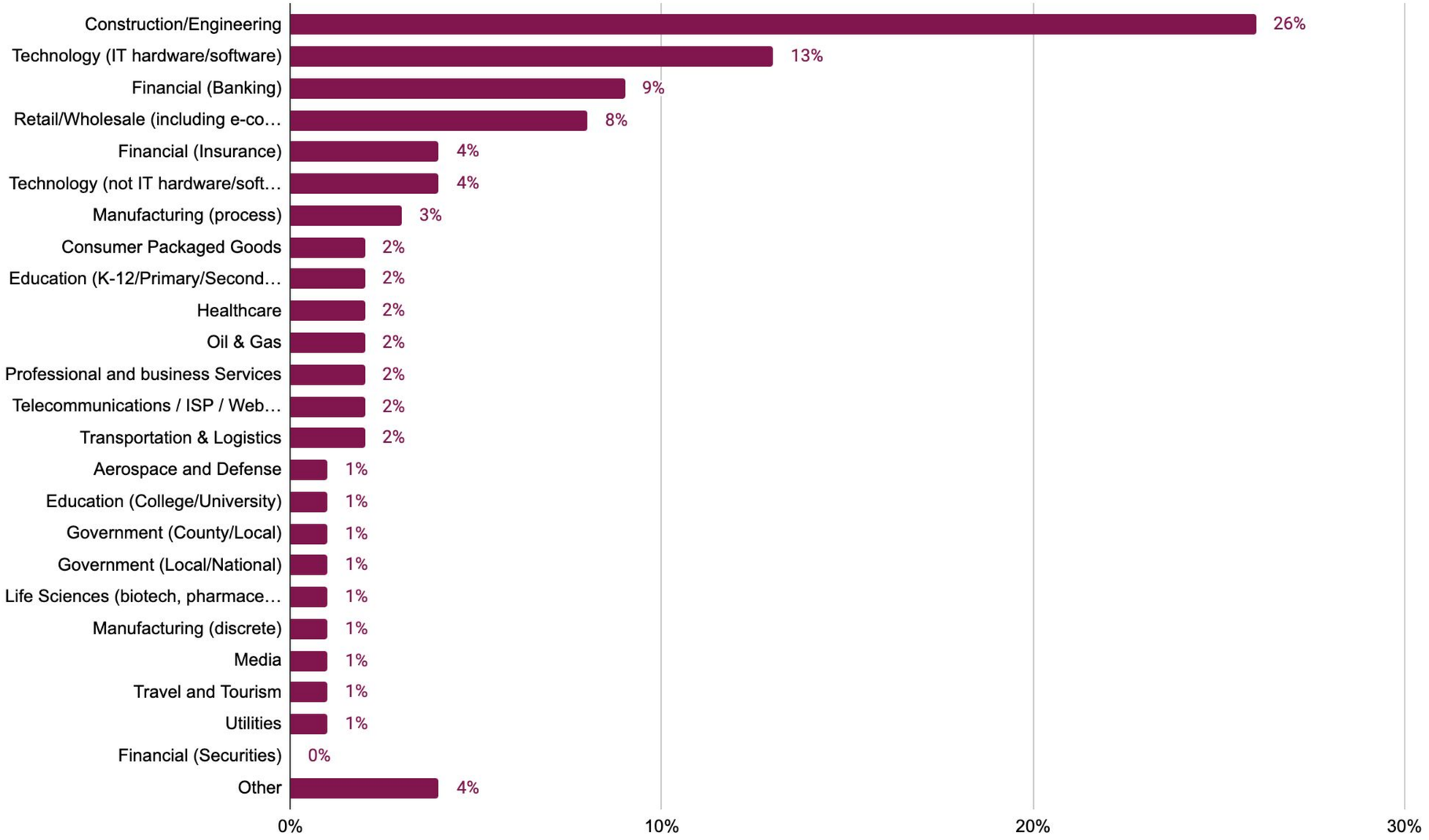
# Size




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

Base: 205

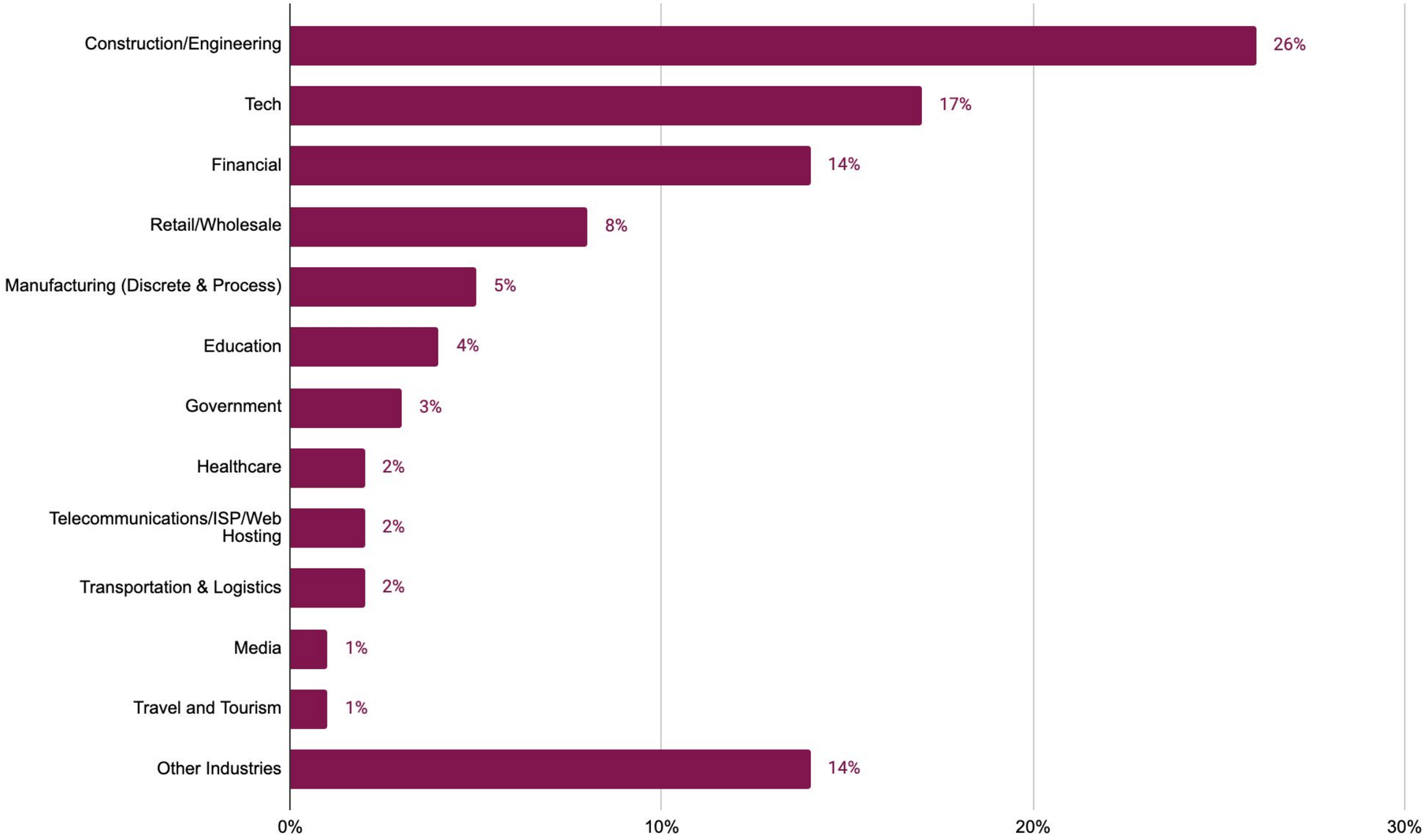
# Industry




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

Base: 205

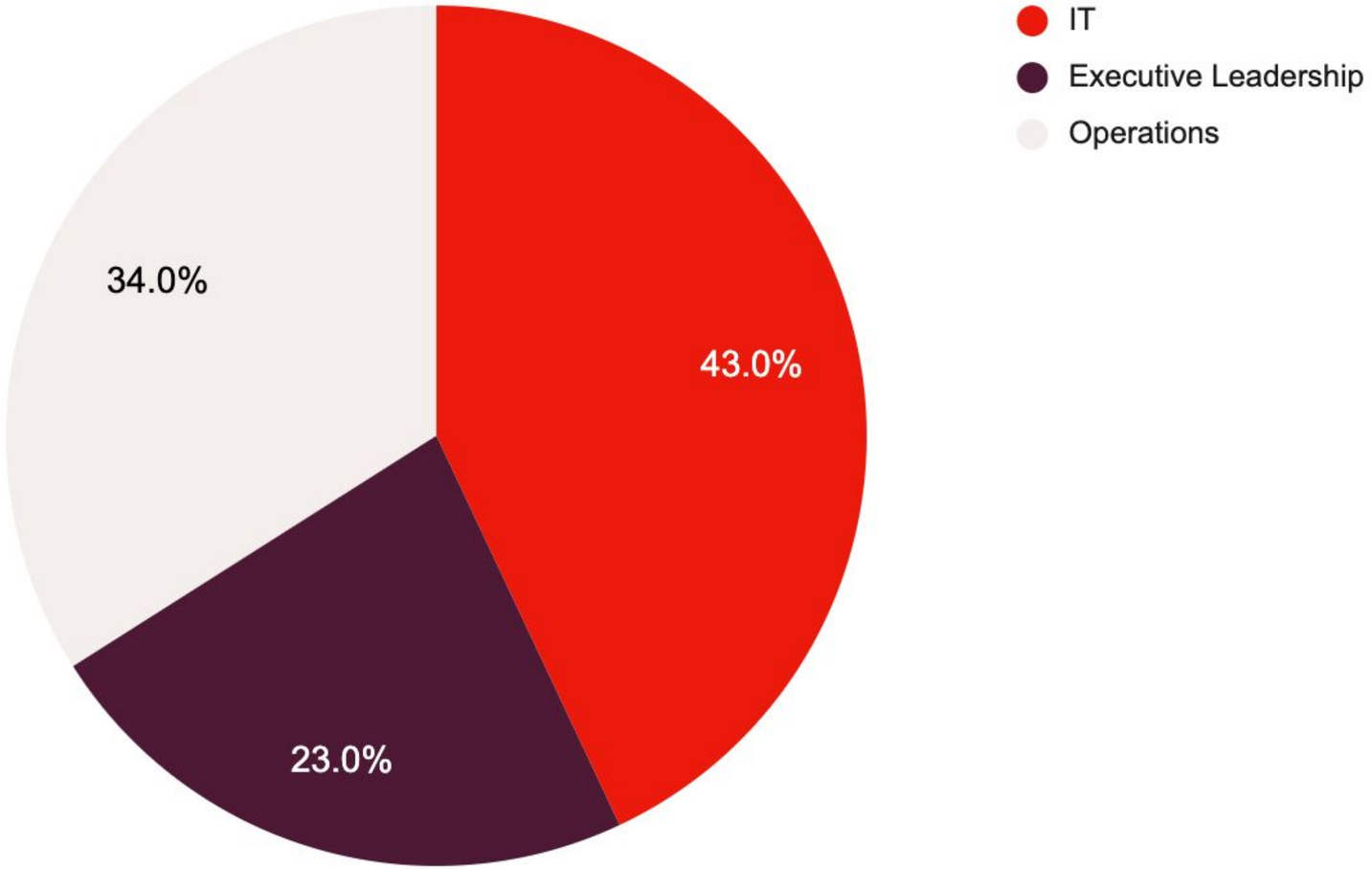
# Industry - focus




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

Base: 205

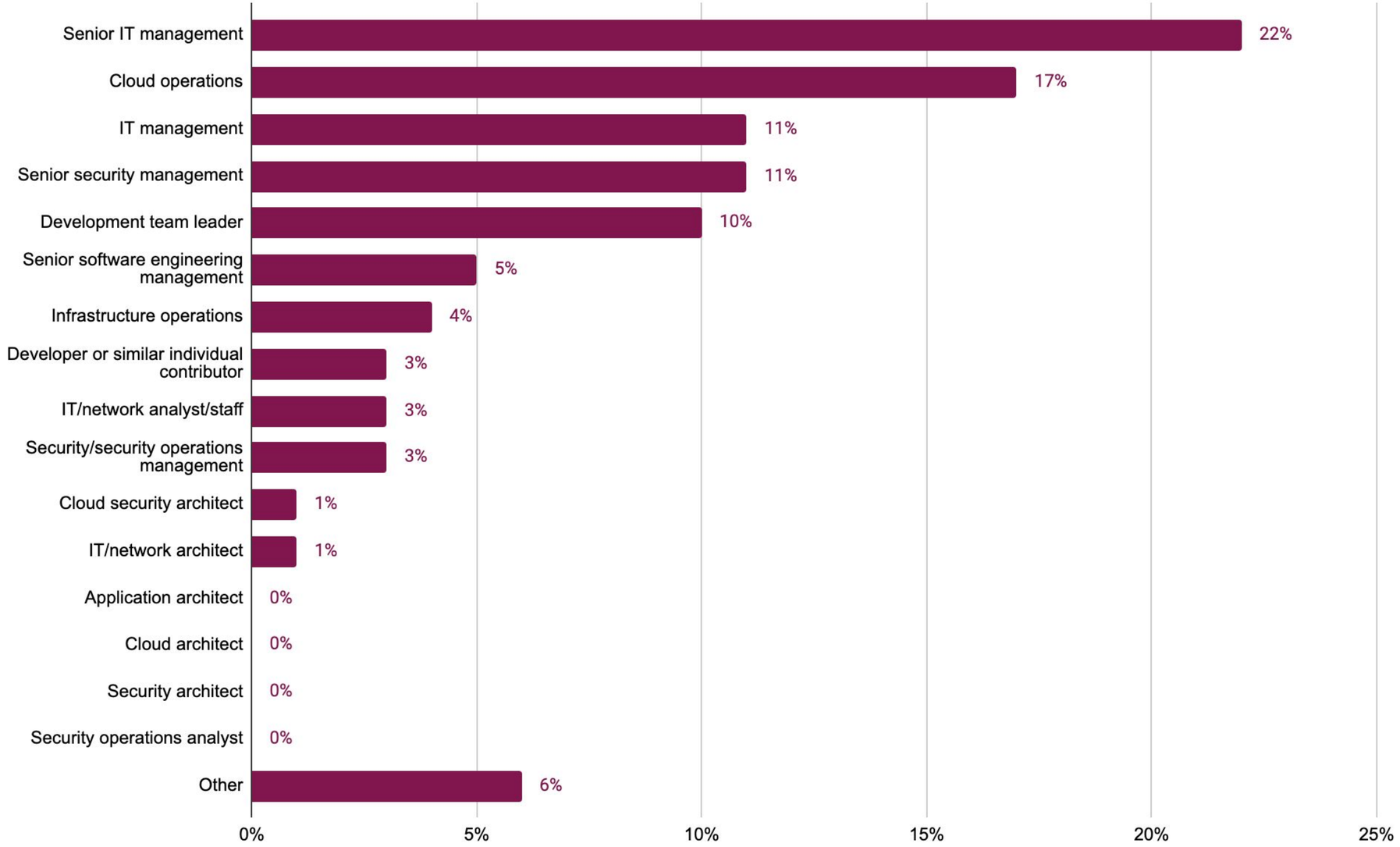
# Department




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

Base: 205

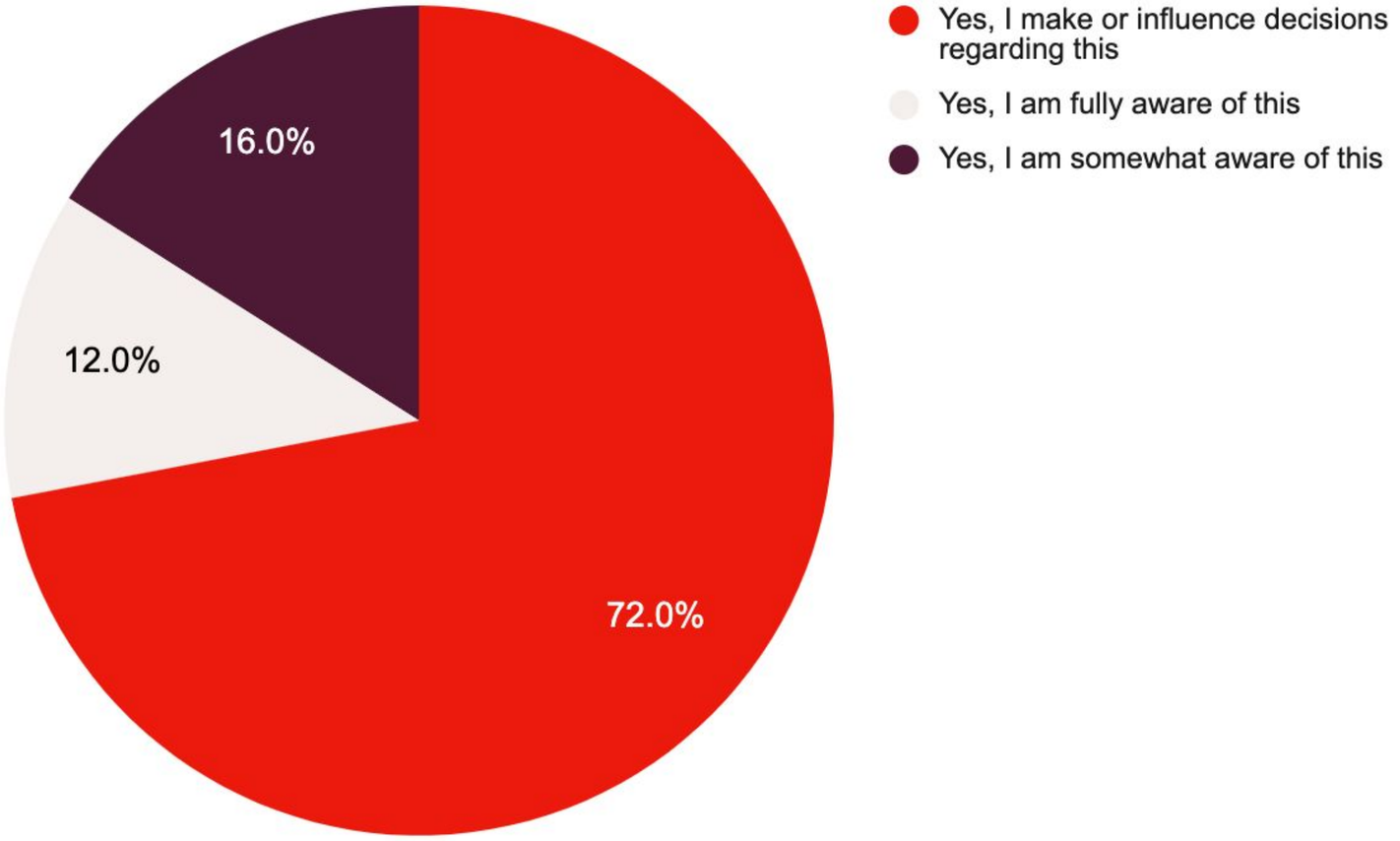
# Current responsibility




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

Base: 205

# 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!