fastly

Fastly Global Security Research 2023

Global Findings

November 2023

Research conducted by
SAPIO Research

Project overview and methodology

- The survey was conducted among **1,484** IT Decision Makers (more than 2/3 respondents directly make or influence cybersecurity decisions) in organisations with 500+ employees (250+ for AUS/NZ) across Japan, US, DACH, UK & Ireland, Spain, AUS & NZ, and 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 **± 2.5%** at 95% confidence limits assuming a result of 50%.

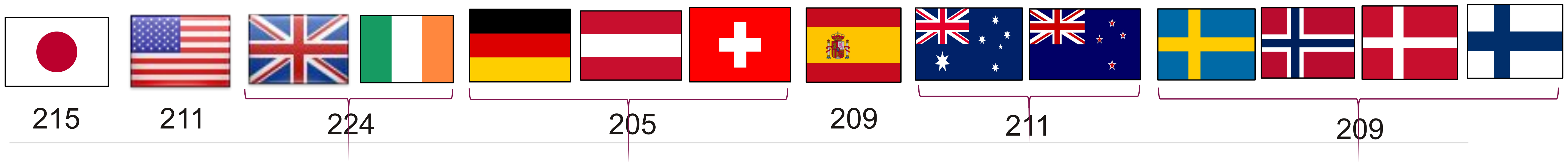
- The interviews were conducted online by Sapio Research in **August, September & October 2023** using an email invitation and an online survey.

Respondent demographics summary

Demographics

Total respondents: 1484

Country of residence



Department

IT: 50%

Ops: 28%

Executive Leadership : 22%

Responsibility within organisation

- 23% IT Management positions (e.g., Director of IT, etc.)
- 16% Senior IT management positions
- 8% Development team leader positions
- 8% Other Responsibility

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	1%	21%	34%	18%	10%	6%	11%

Industry

Company sectors – top 3:

IT / Tech : 18%

Financial (banking): 13%

Construction / Engineering: 12%

Decision making (cyber security)

- 69% make or influence cybersecurity decisions
- 17% are fully aware of decisions regarding cybersecurity
- 14% are somewhat aware of cybersecurity decisions

Key stats

40% predict **'data breaches and data loss'** as the biggest **cybersecurity threat** over the next **12 months**

On average, businesses **lose 9.17%** of their annual income as a result of **cyber attacks**

46% 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 **(37%)**, improving cybersecurity skills through training and/or talent acquisition **(37%)**, and making cybersecurity more accessible **(35%)** are the main security priorities over the next year

46% say that their organisations cybersecurity strategy has **hampered** business innovation

On average, **54.9%** of **cybersecurity tools** are **fully deployed/active**

Summary and Overview

1 **Cybersecurity threats – 40% predict ‘data breaches and data loss’ as the biggest cybersecurity threat to their organisation over the next 12 months, followed by ‘Identity based threats’ (38%) and ‘Generative AI’ (29%). Moreover, 35% predict that ‘an increasingly sophisticated threat landscape’ will drive cybersecurity threats over the next 12 months.**

2 **Preparing for cybersecurity threats – 76% are increasing cybersecurity investment to prepare for future cybersecurity risks, particularly in the UK & Ireland (84%) and the construction/ engineering industry (83%). Organisations are currently prioritising investing in ‘firewall’ technology (61%).**

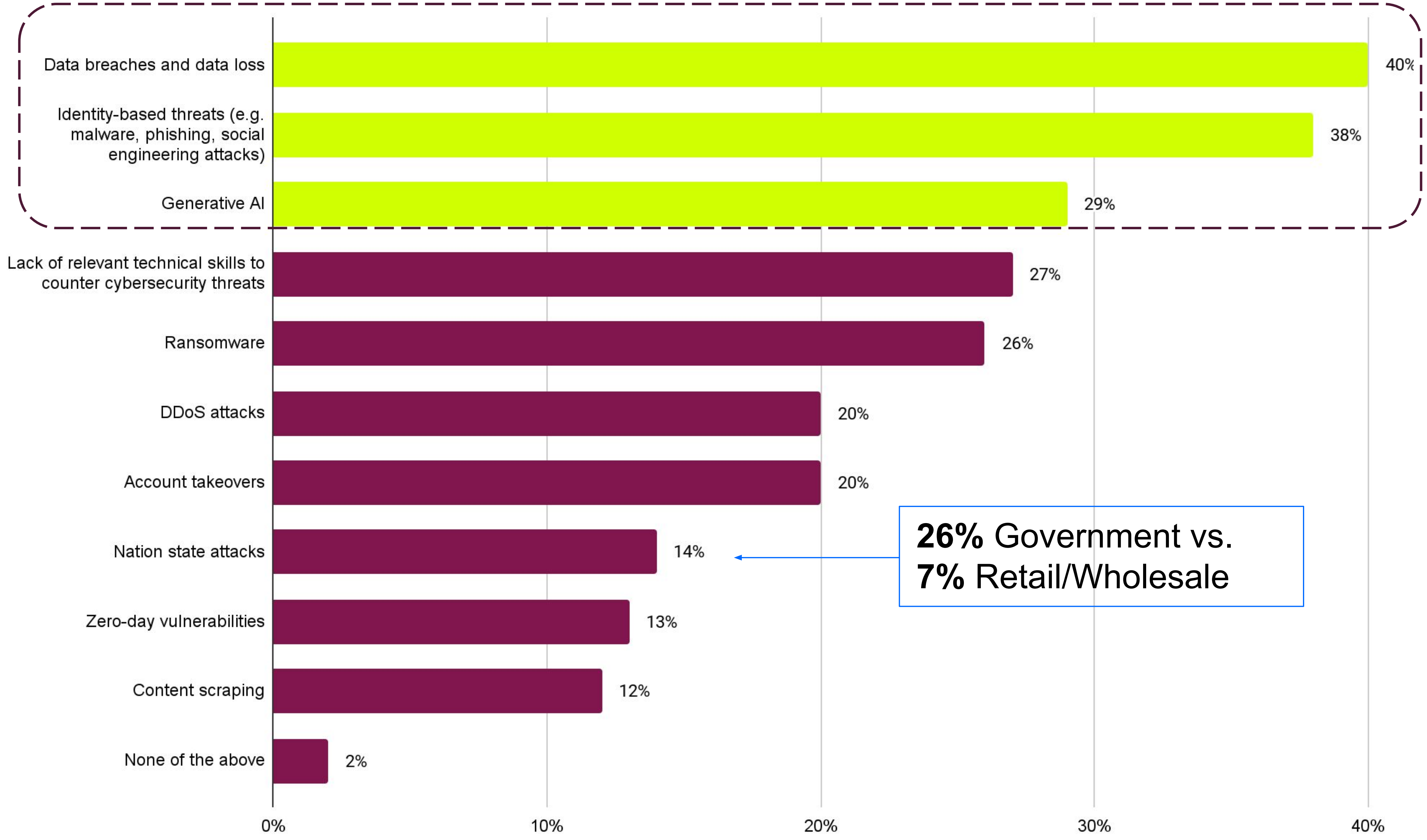
3 **Response to Generative AI – 29% see Generative AI as one of the biggest cybersecurity threats to their business over the next 12 months. This is reflected in 46% of respondents who feel that there is a gap in the talent pool in experience with emerging threats such as Generative AI. However, 43% believe Generative AI will increase productivity.**

4 **Cybersecurity priorities – 37% of respondents say ‘defining our approach to new and emerging cybersecurity threats (e.g. generative AI)’ is a security priority over the next year, along with ‘improving cybersecurity skills through training and/ or talent acquisition (also 37%).**

5 **Role of a CISO – 70% have had a CISO for at least the last 12 months and 17% are planning to hire a CISO in the next 1-2 years. Along with security managers (26%), CISOs (27%) are held the most accountable for cybersecurity incidents. 41% of respondents feel that CISOs are increasingly expected to have an in depth understanding of all areas of IT.**

Main Findings

Data breaches and data loss (40%), Identity-based threats (38%), and Generative AI (29%), are viewed as the biggest cybersecurity threats to organisations over the next 12 months



59% Healthcare vs.
28% Education

47% Spain vs.
28% Japan

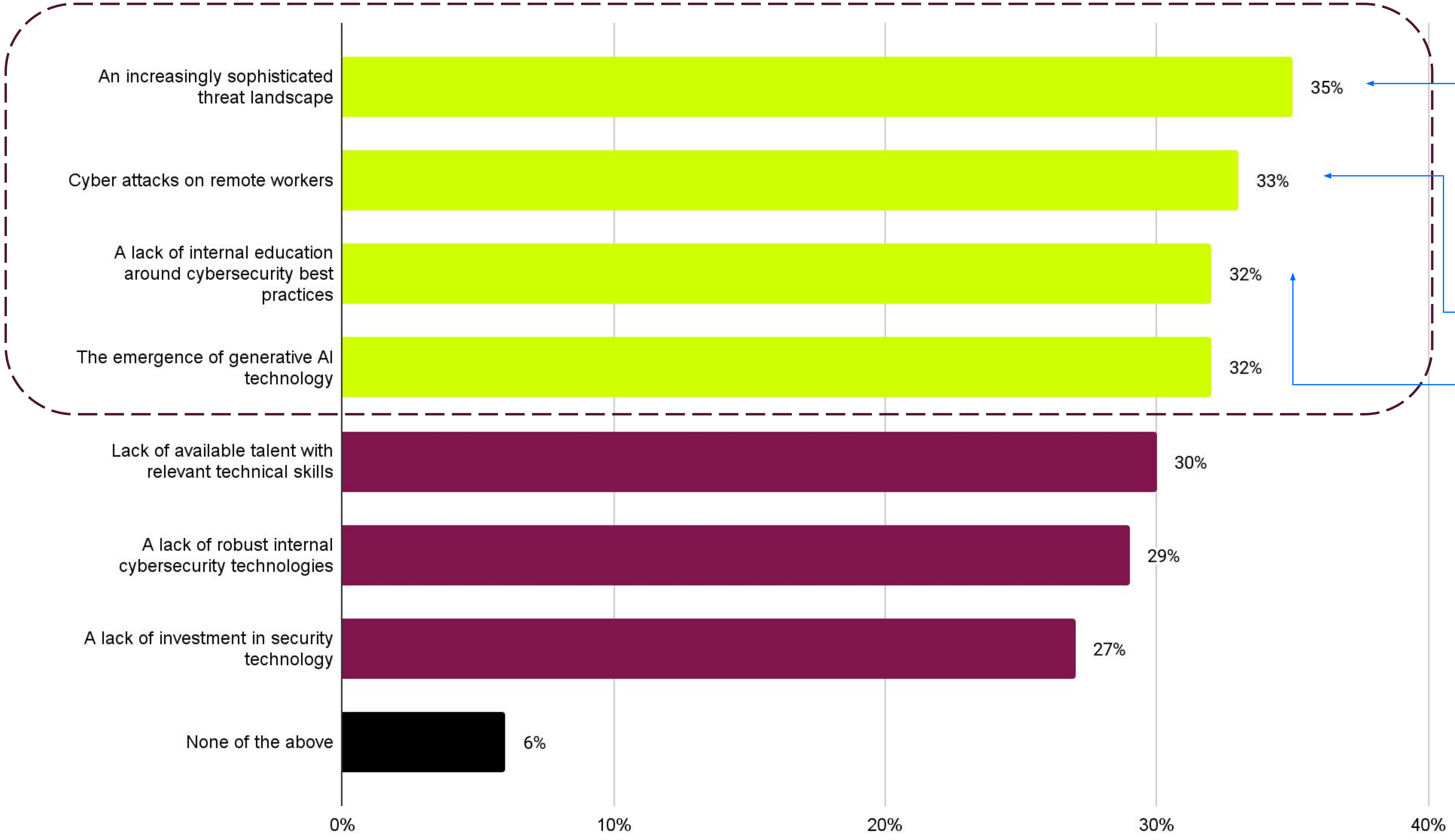
46% 500 to 999 employees vs.
32% 75,000+ employees

26% Government vs.
7% Retail/Wholesale

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

Base: 1484

Over the last 12 months, an increasingly sophisticated threat landscape (35%), cyber attacks on remote workers (33%), a lack of internal education around cybersecurity (32%) and the emergence of generative AI (32%) were the main drivers of cybersecurity threats



41% AUS & NZ vs.
26% DACH

40% Government vs.
22% Education

39% US vs.
28% Japan

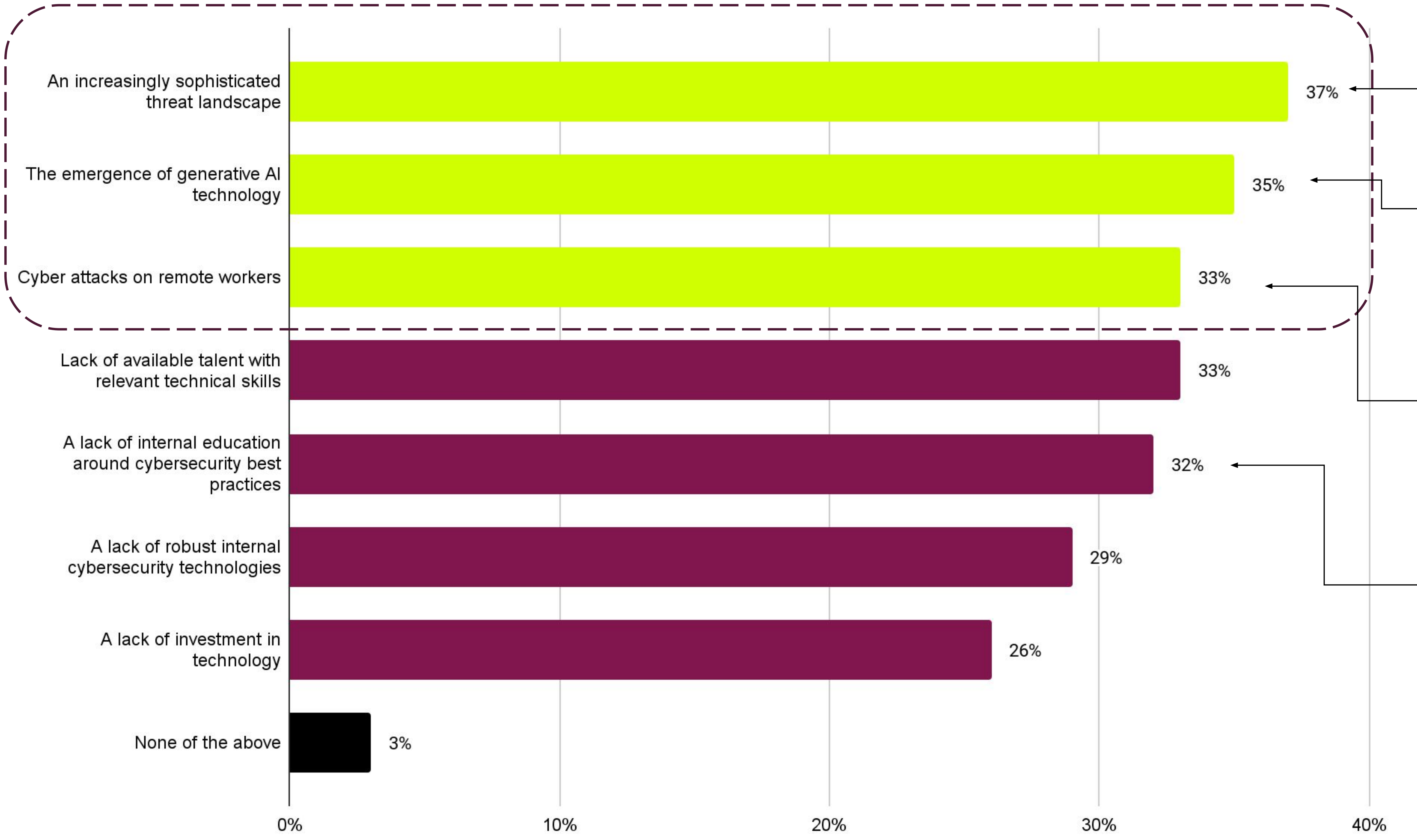
53% Transportation & Logistics vs.
20% Telecommunications

41% 500 to 999 employees vs.
24% 25,000+ employees

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

Base: 1484

Over the next 12 months, an increasingly sophisticated threat landscape (37%) and cyber attacks on remote workers (33%) are still seen as some of the main drivers of cybersecurity threats, but there is an increased focus the emergence of generative AI technology (35%)



49% Japan vs.
30% DACH

41% Financial vs.
30% Construction/ Engineering

40% Transportation & Logistics vs.
19% Government

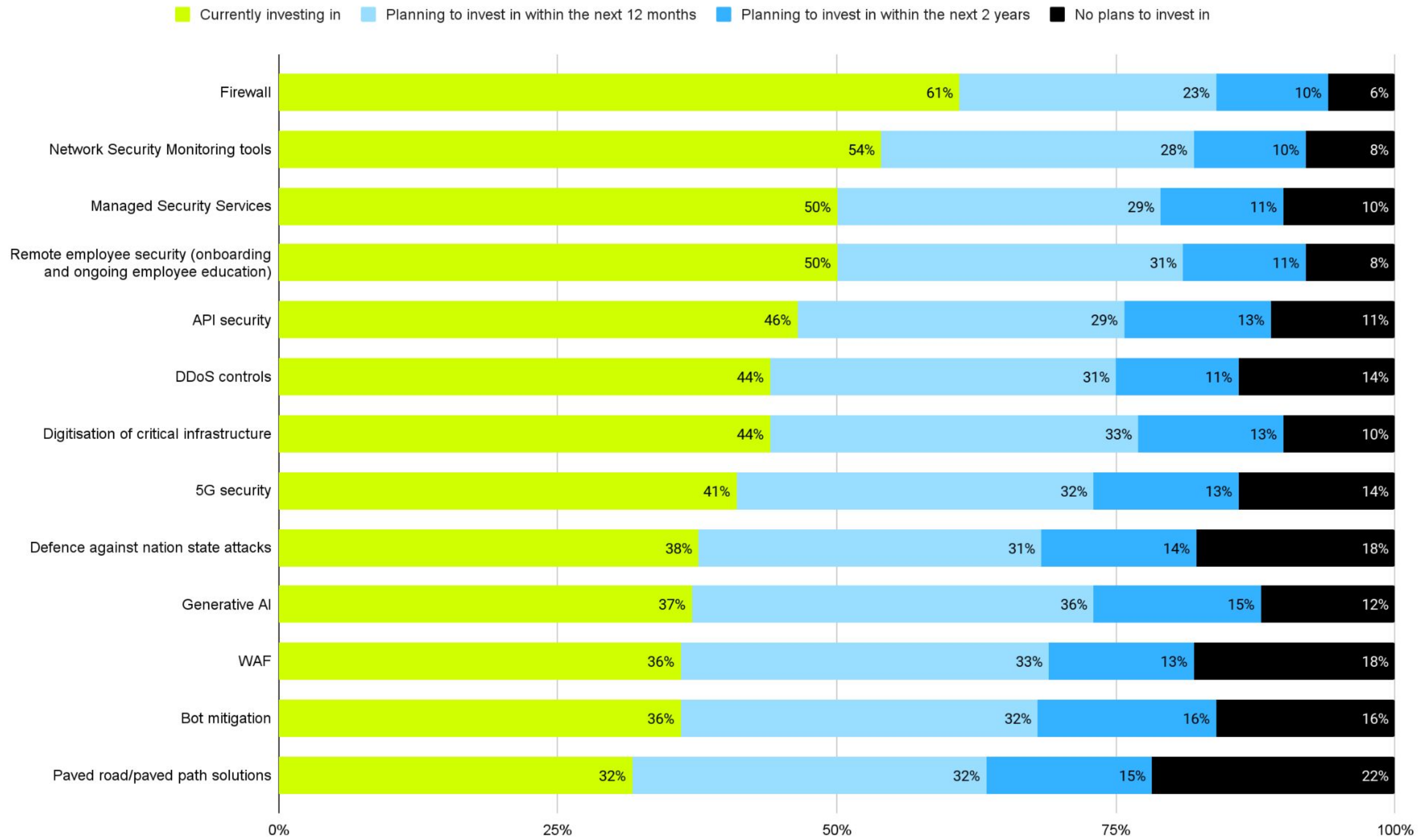
41% UK / Ireland vs.
27% AUS / NZ

39% 5,001 to 10,000 employees vs.
21% 75,000+ employees

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

Base: 1484

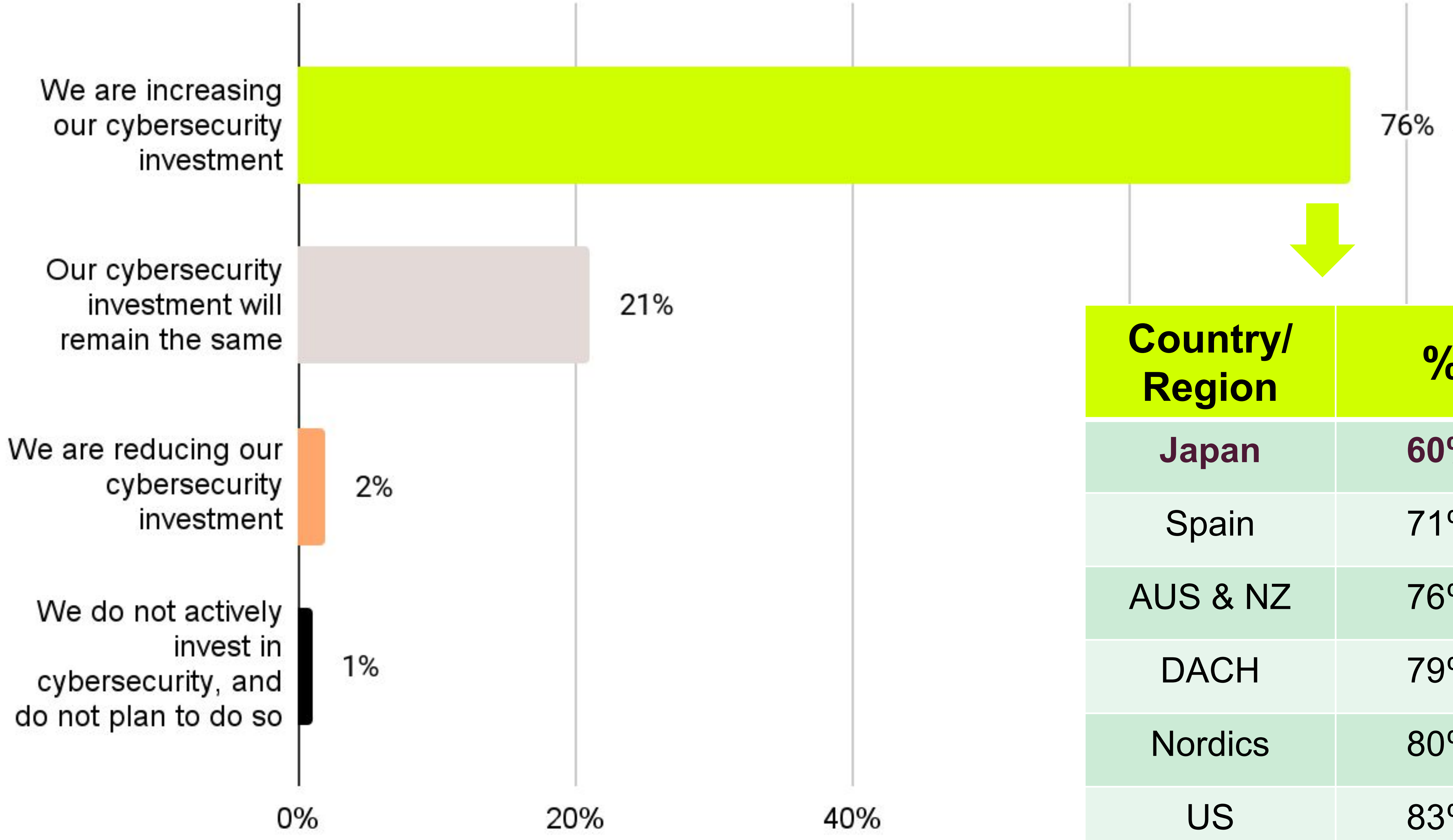
61% are currently investing in ‘Firewall’ technology, and over half are investing in ‘Network Security Monitoring tools’ (54%)
22% have no plans to invest in paved road/ paved path solutions



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

Base: 1484

76% of respondents are increasing their cybersecurity investment
This increases to 84% for those in the UK & Ireland



83% Construction/ Engineering vs. **63%** Government

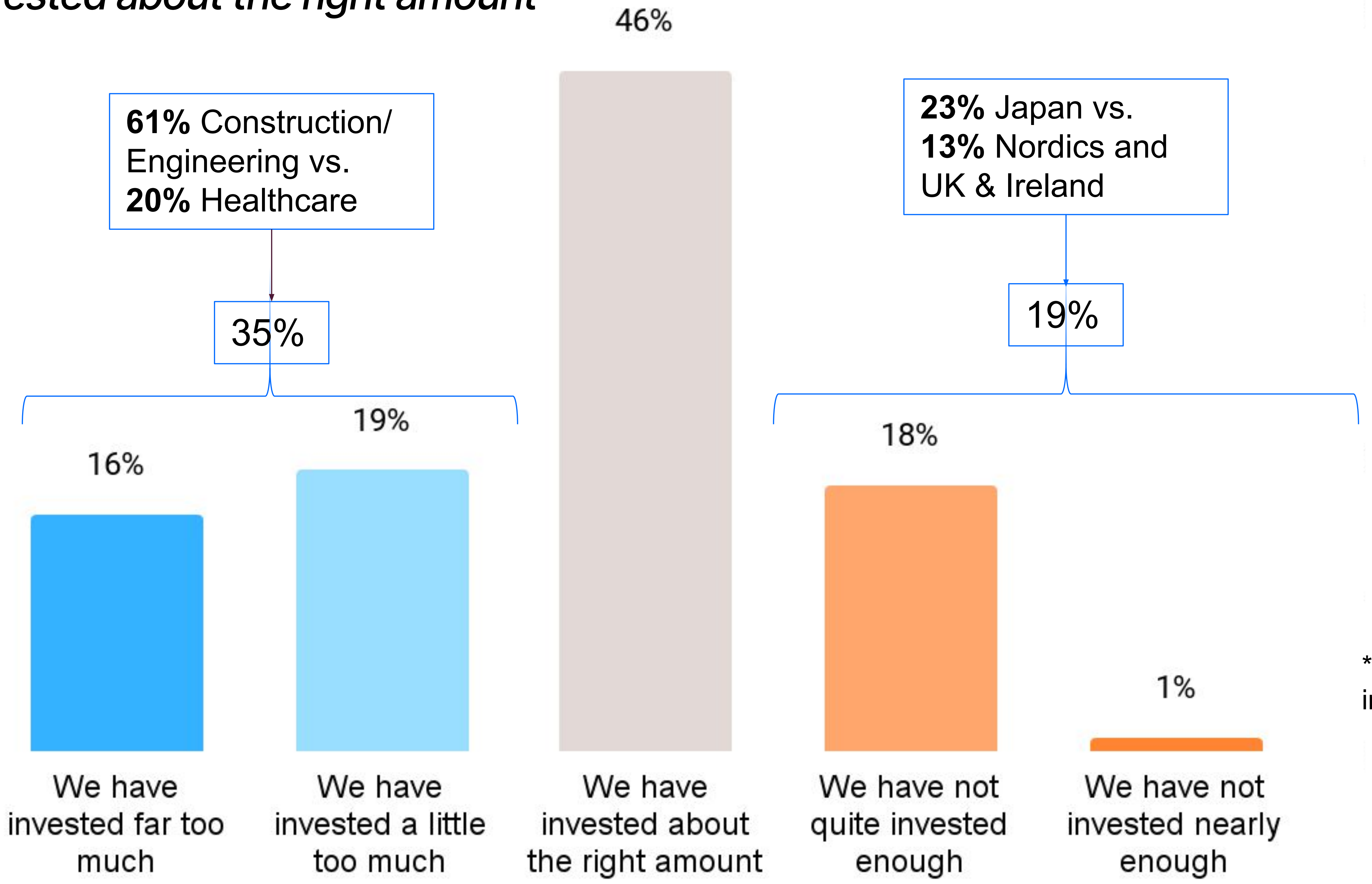
Country/ Region	%
Japan	**60%**
Spain	71%
AUS & NZ	76%
DACH	79%
Nordics	80%
US	83%
UK & Ireland	**84%**

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: 1484

35% of respondents have invested too much into cybersecurity over the past 12 months, this increases to 61% for those in the construction/ engineering sectors

46% say they have invested about the right amount

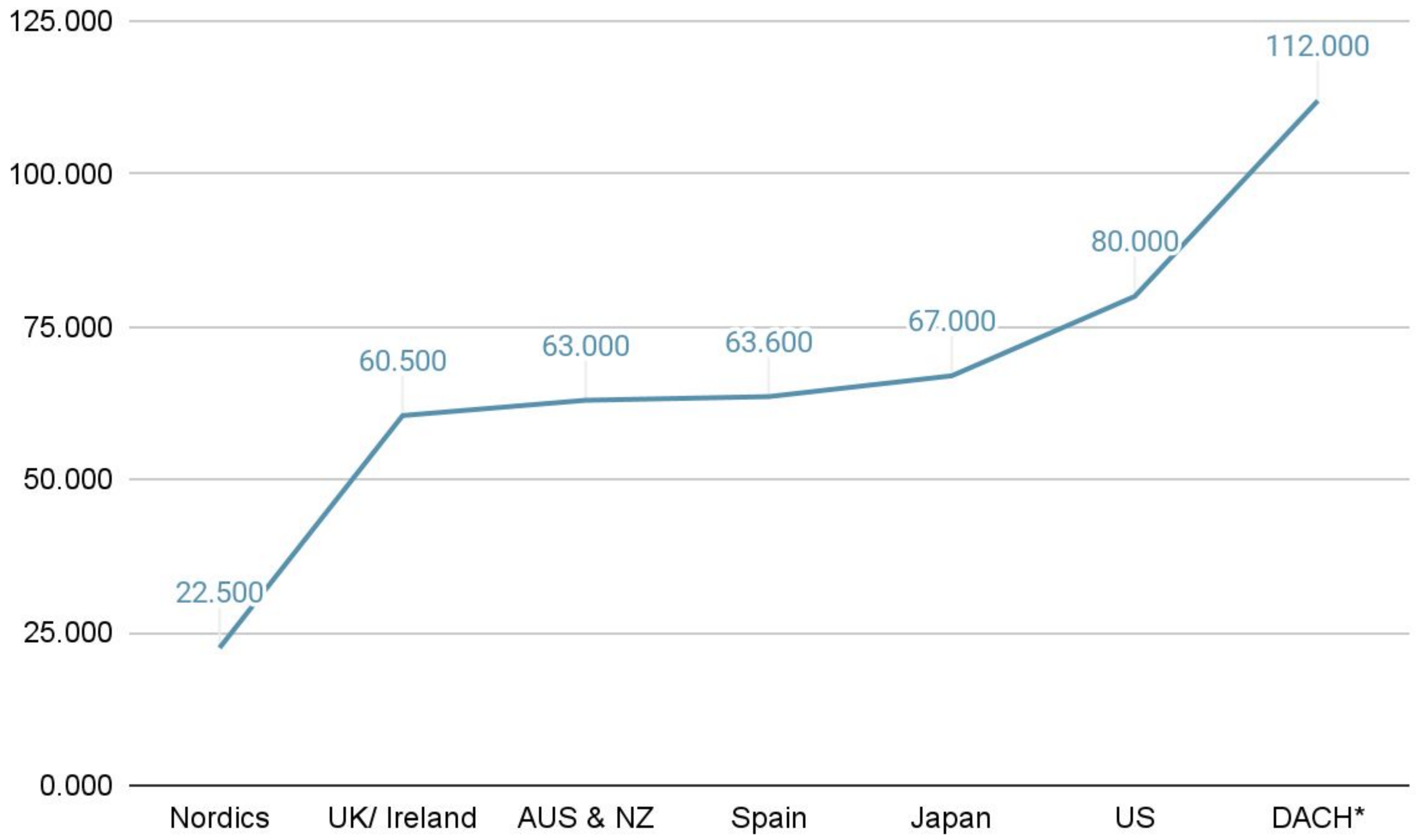


*only asked to those who invest in cybersecurity

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: 1465*

On average (median), $80,000 USD are spent per year on web application and API security control/tools in the US, compared with $22,500 USD (median) in the Nordics



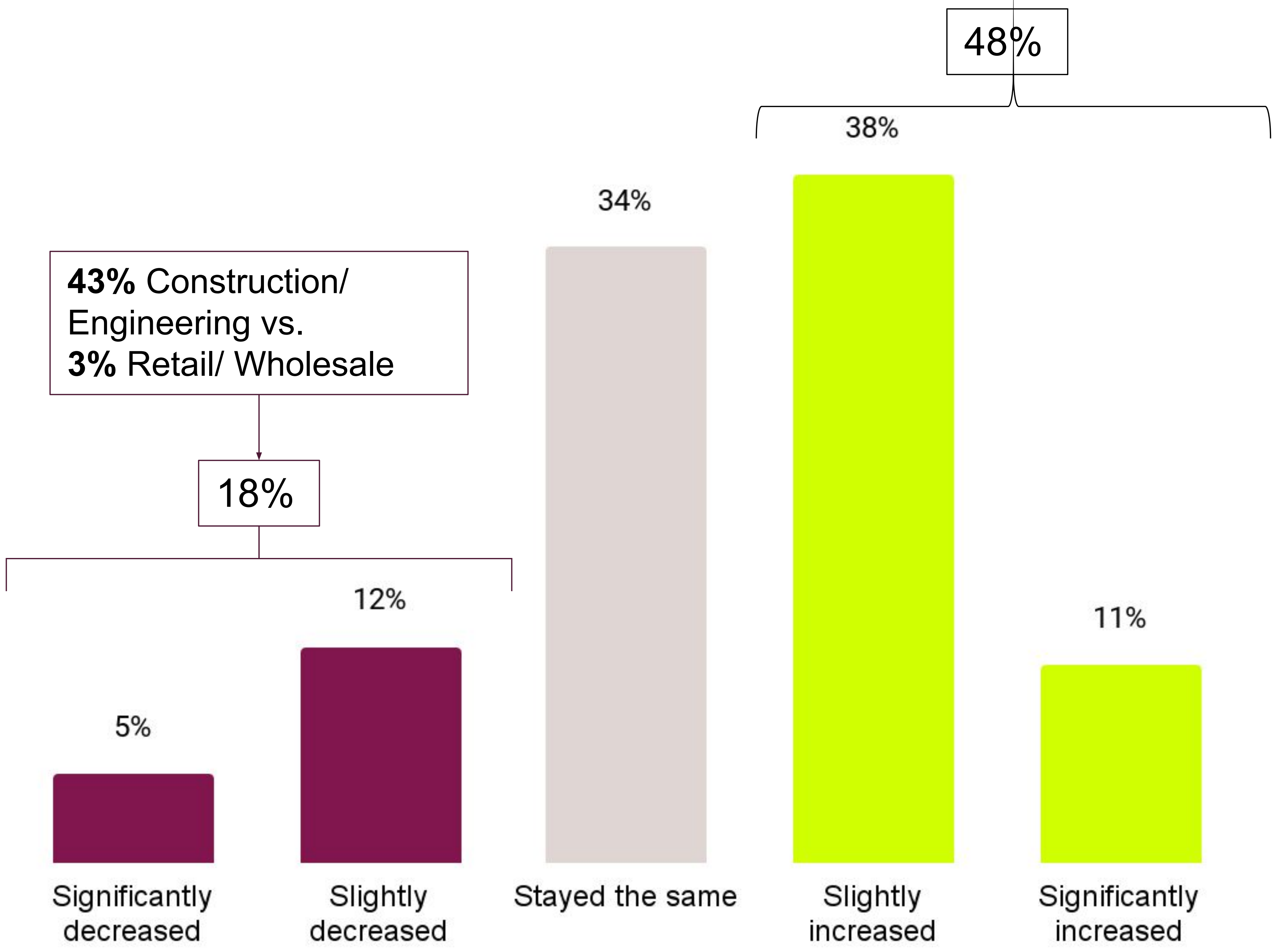
*The sample for DACH countries had a larger proportion of companies with more than 75,000+ employees

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

48% of respondents have increased talent spending, with only 18% having decreased talent spending



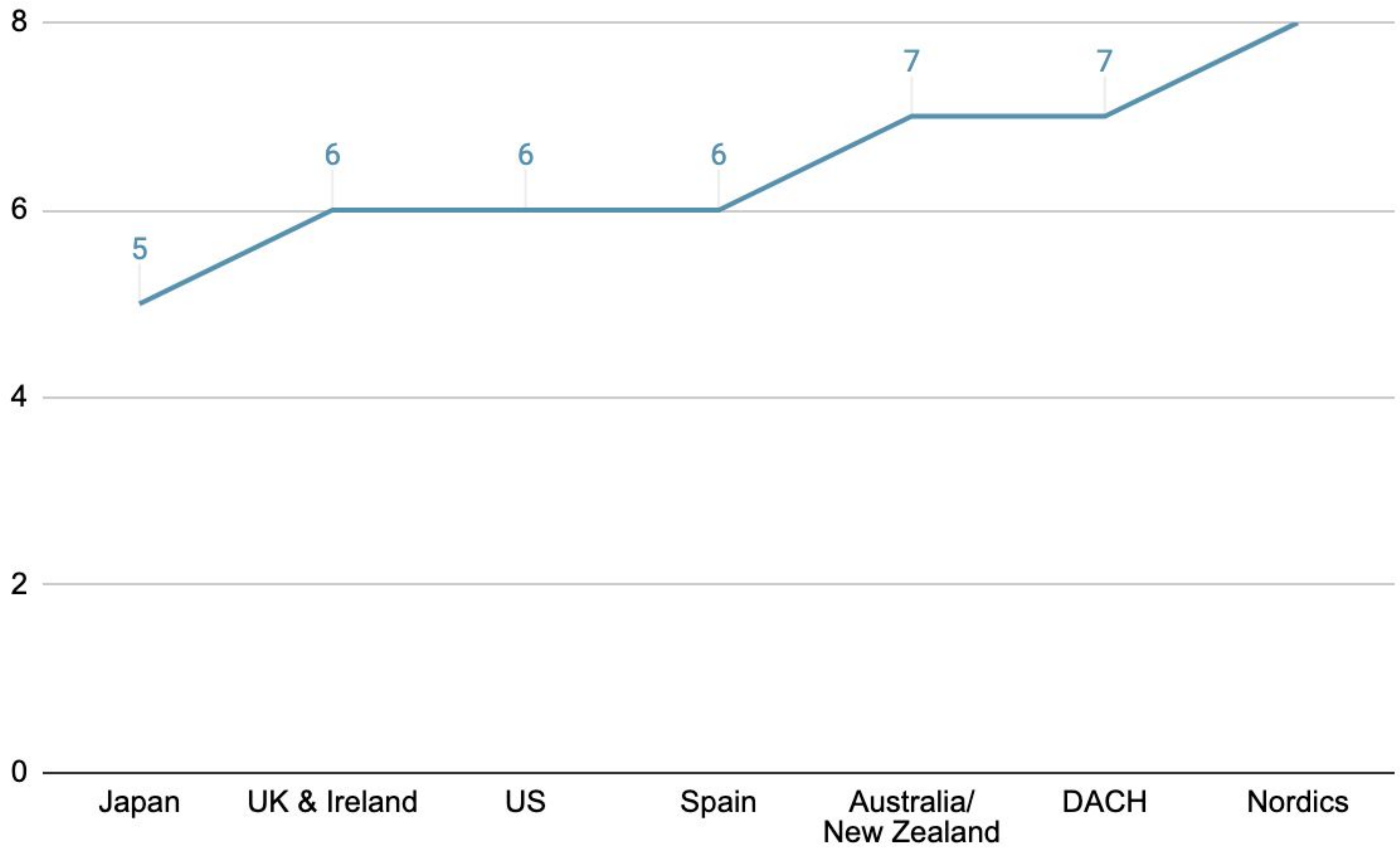
Q5b. How has your talent spending (e.g. new hires, wages) for cybersecurity changed, if at all? Select one

Base: 1484

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

This increases to 8 for the Nordics

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

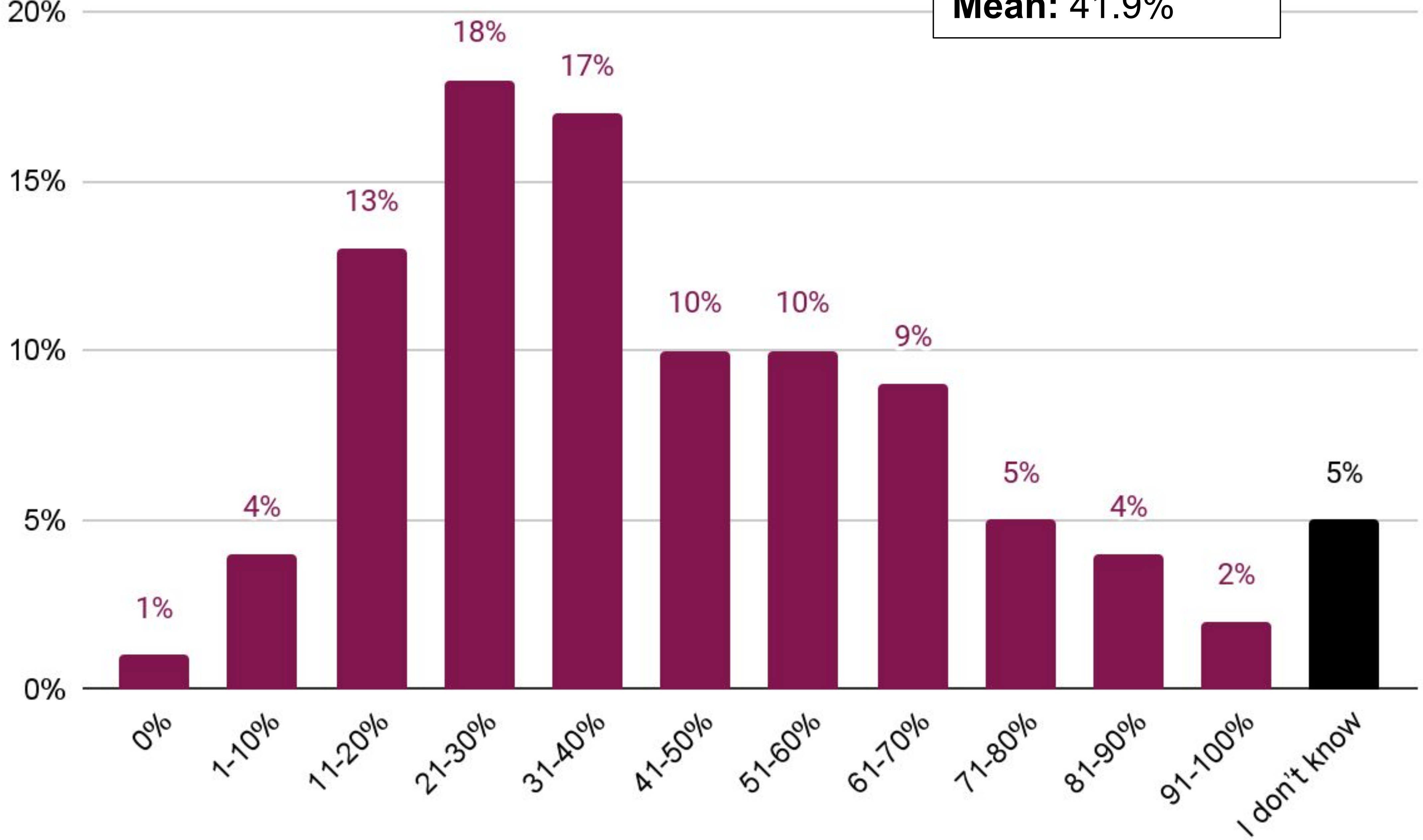
Base: 1484

On average, 40.7% of network and application cybersecurity solutions overlap
This decreases to 31.2% for Australia & New Zealand

47.2% Telecommunications vs. **33.5%** Construction / Engineering

Mean: 40.7%

2022 Survey:
Mean: 41.9%



Country/ Region	Mean (%)
AUS & NZ	**31.2**
Nordics	36.5
DACH	38.3
Japan	38.8
UK & Ireland	44.9
US	46.7
Spain	**47.6**

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

Base: 1484

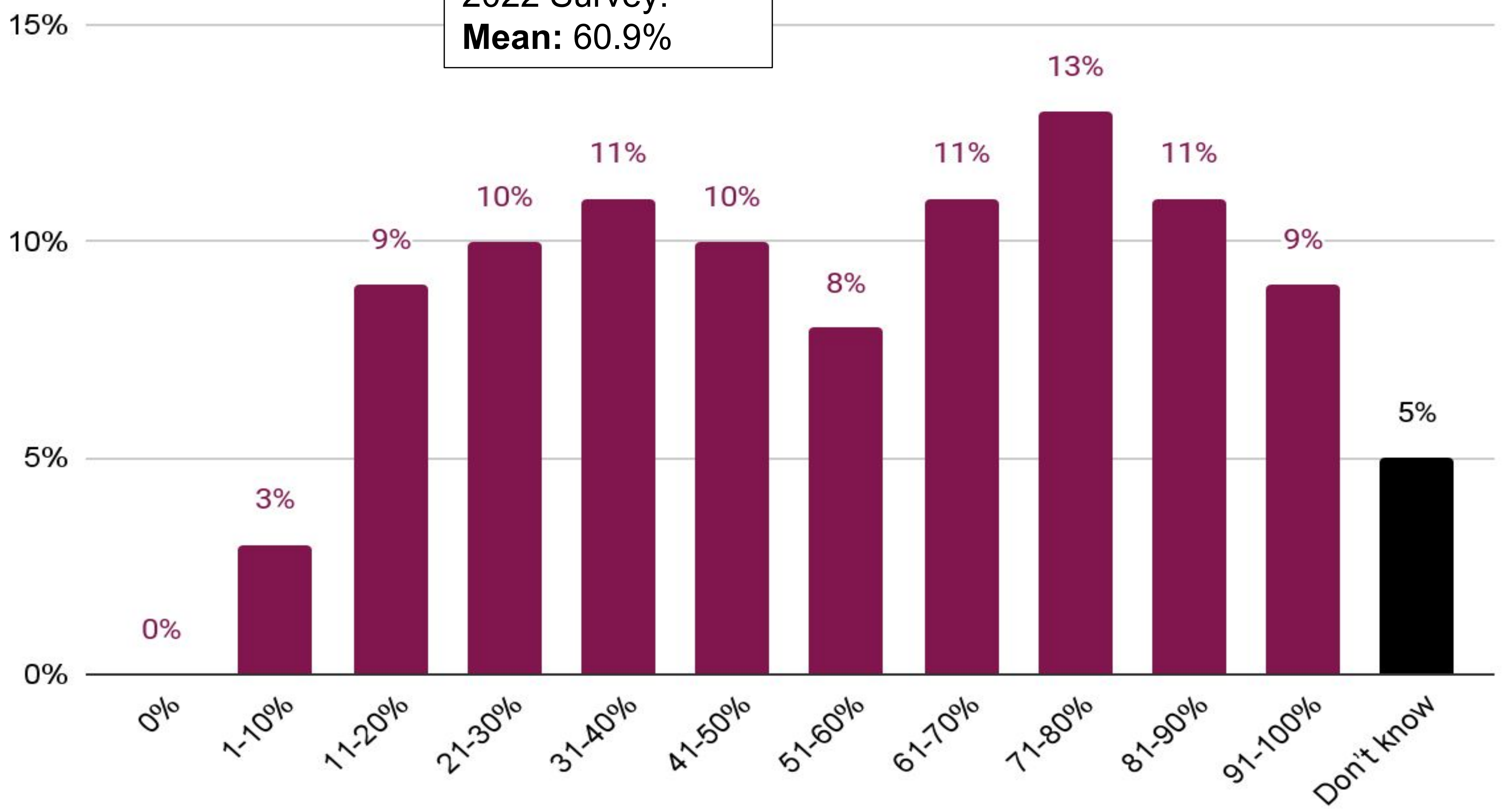
On average, only 54.9% of cybersecurity tools are fully active/ deployed
This increases to 63.0% in Spain

Country/ Region	Mean
Nordics	**45.6**
AUS & NZ	46.9
DACH	52.2
UK & Ireland	56.8
Japan	59.4
US	60.9
Spain	**63.0**

Mean: 54.9%

2022 Survey:
Mean: 60.9%

63.0% Government vs.
40.3% Construction/ Engineering



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

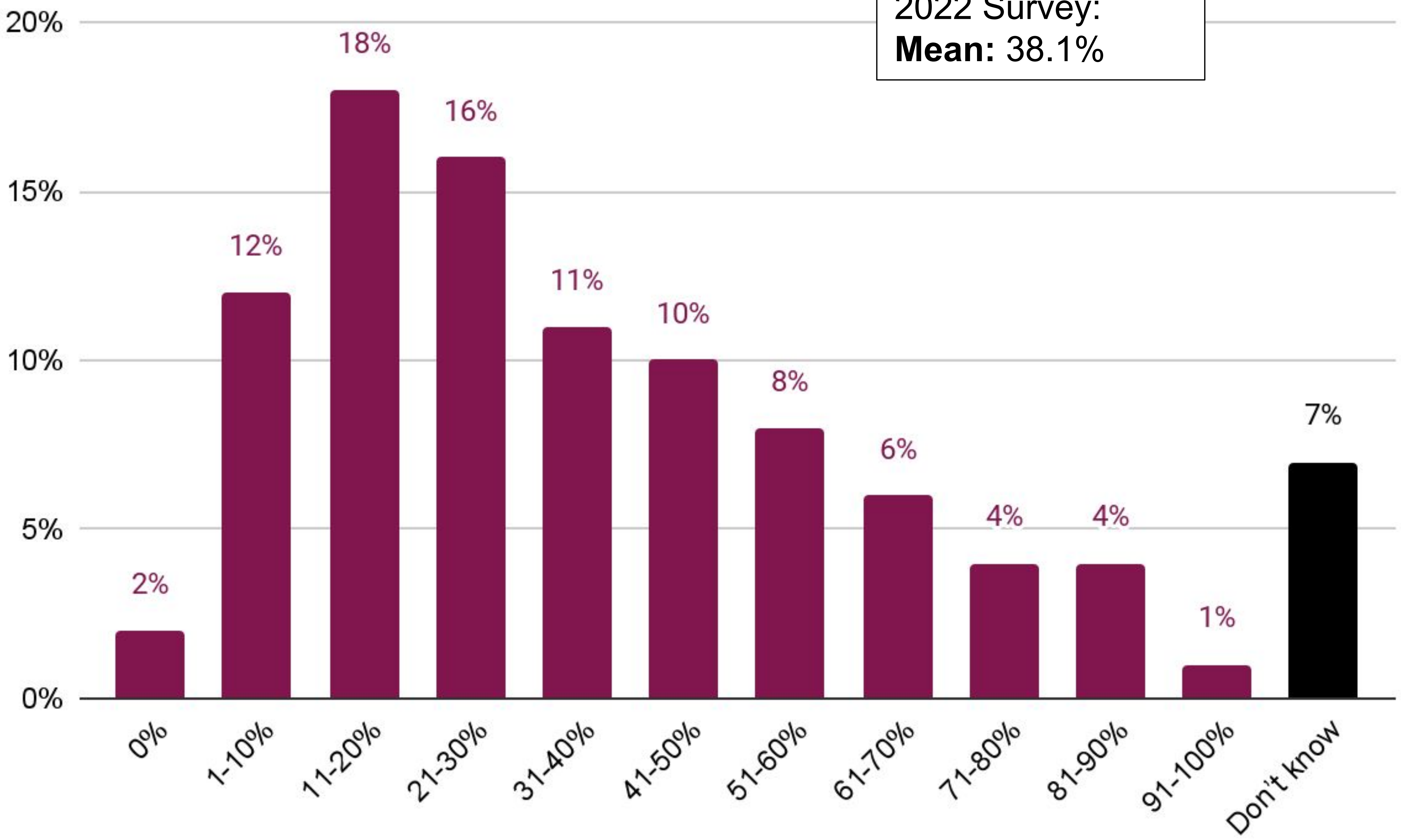
Base: 1484

On average, 34.2% of security alerts detected by an organisations WAF are false alerts
This increases to 40.6% for the UK/ Ireland

42.3% Education vs.
30.1% Transportation & Logistics

Mean: 34.2%

2022 Survey:
Mean: 38.1%

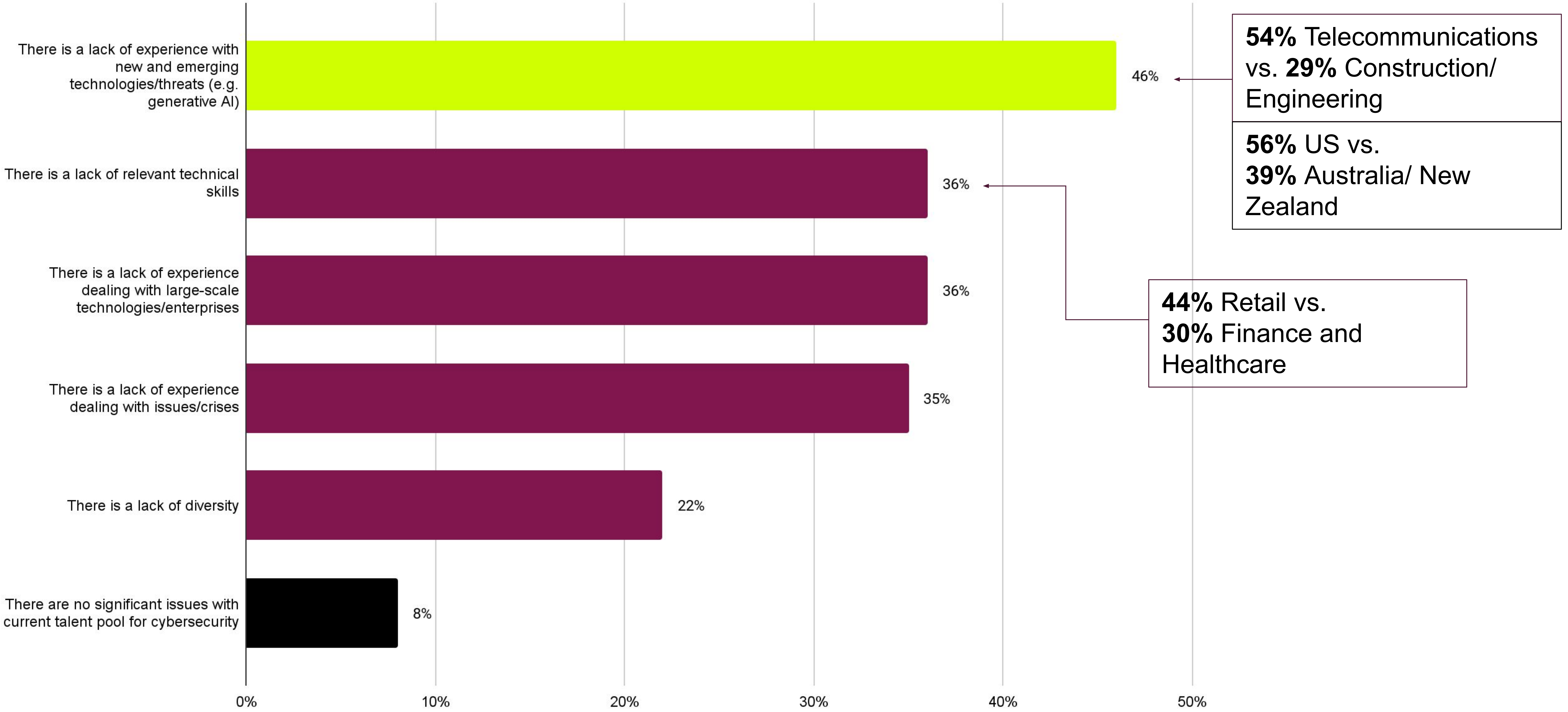


Country/ Region	Mean
Japan	**26.3**
AUS & NZ	28.9
DACH	34.0
Spain	34.3
US	35.4
Nordics	38.7
UK & Ireland	**40.6**

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

Base: 1484

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



54% Telecommunications vs. **29%** Construction/ Engineering

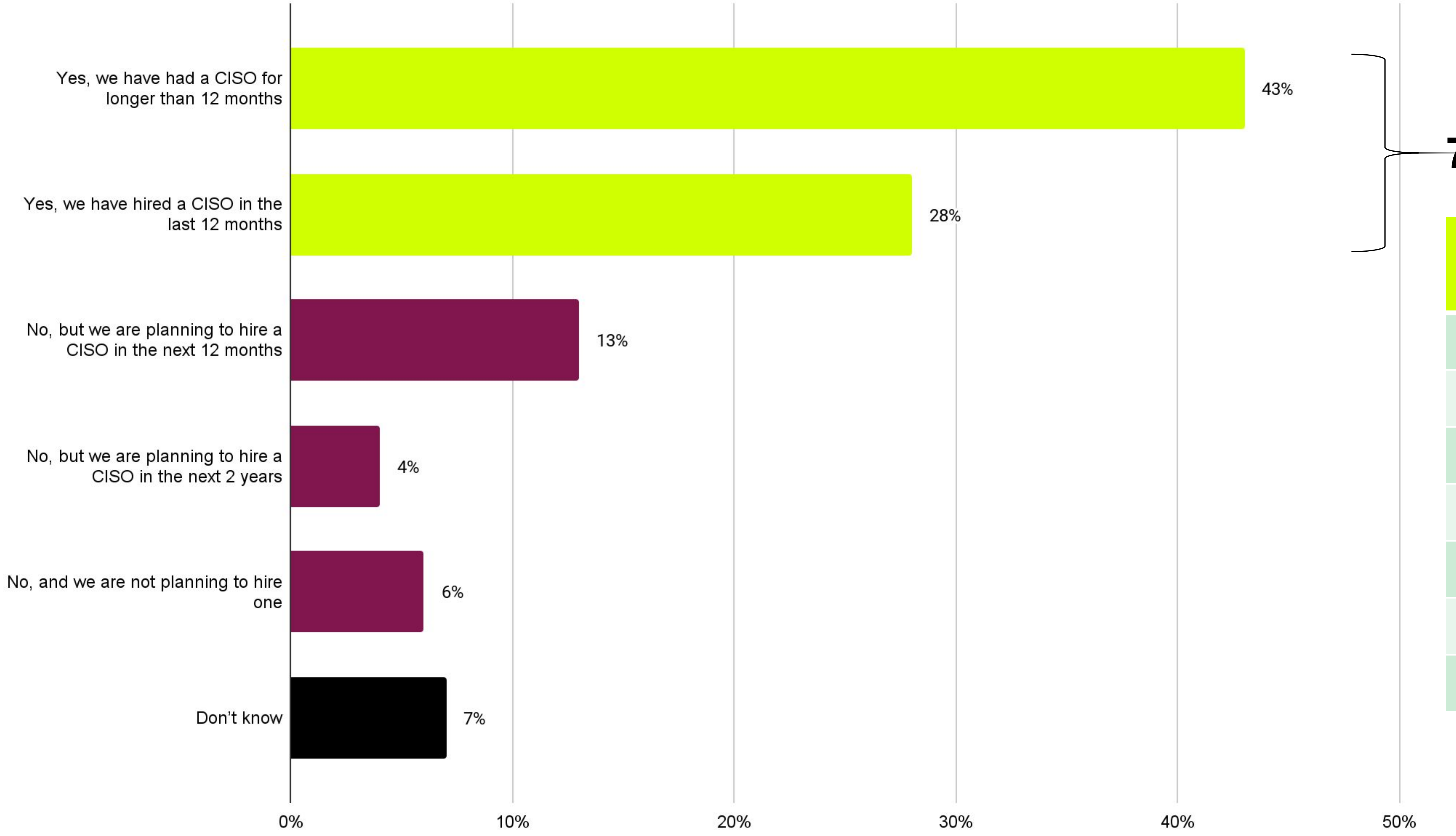
56% US vs. **39%** Australia/ New Zealand

44% Retail vs. **30%** Finance and Healthcare

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

Base: 1484

70% of respondents have hired a CISO, 28% of those within the last 12 months
Only 46% of those in Japan have hired a CISO, compared to 81% in Australia and New Zealand



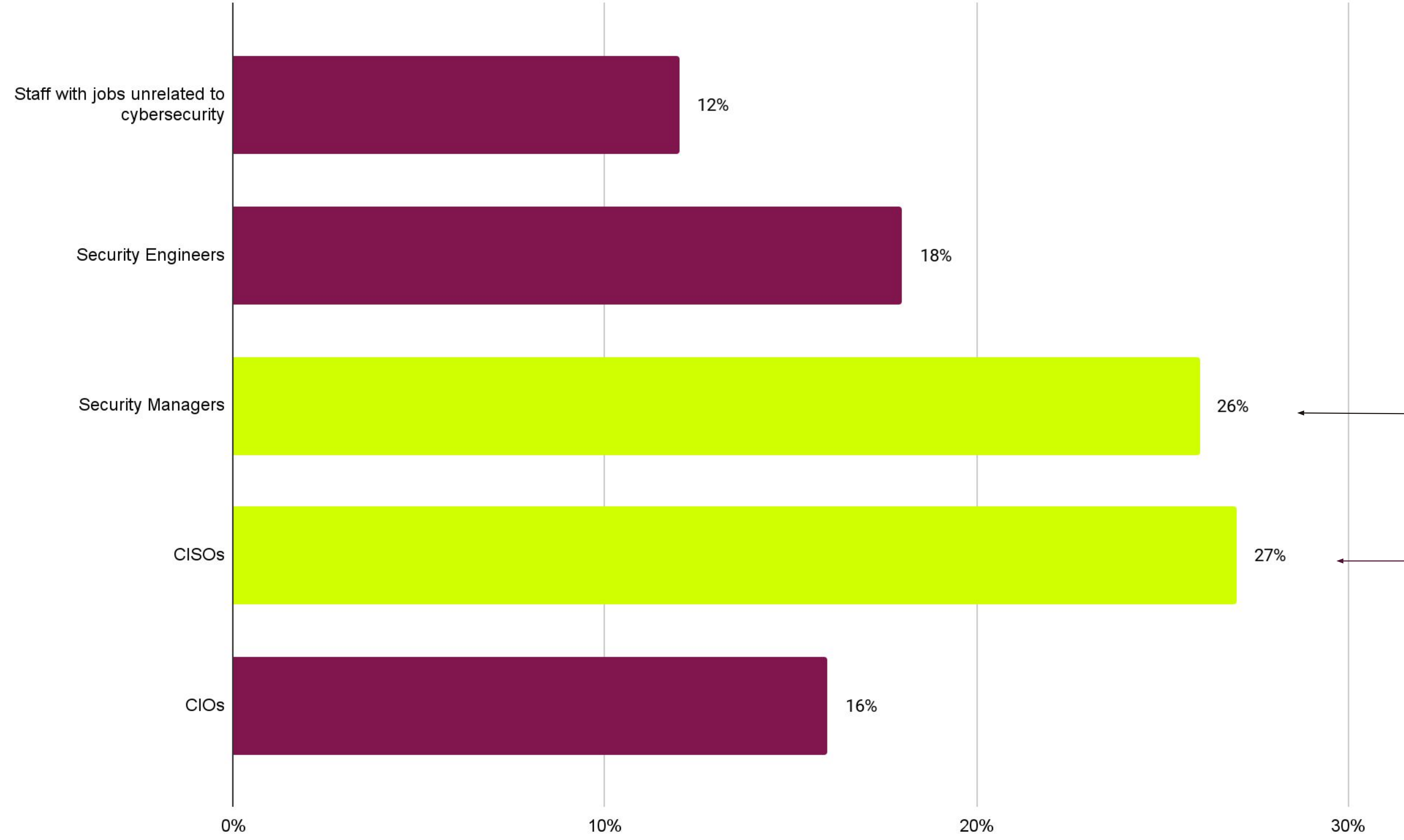
2022 Survey:
57% Yes

Country/ Region	% Yes
Japan	**46%**
Spain	69%
US	70%
UK & Ireland	73%
Nordics	77%
DACH	78%
AUS & NZ	**81%**

Q10. Does your organisation have a CISO? Select one

Base: 1484

27% of respondents think CISOs are often held responsible for cybersecurity incidents, 26% think security managers are often held responsible



2022 Survey:
Security managers: **29**%
Security engineers: **21%**
CISOs: **19%**

33% Japan vs.
21% Spain

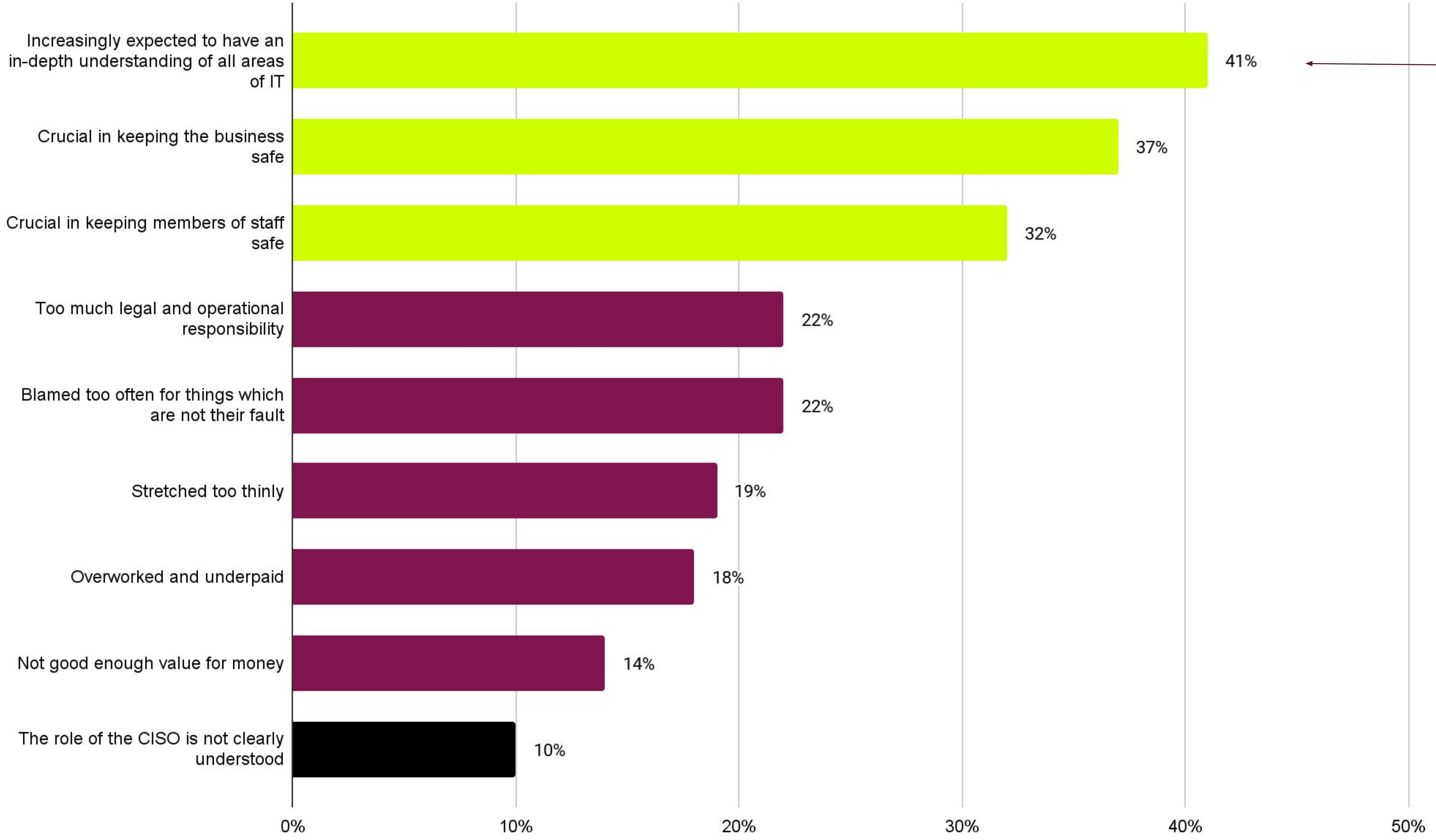
36% Financial vs.
19% Government

34% UK & Ireland vs.
17% Japan

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

Base: 1484

CISOs are viewed as having an in-depth understanding of all areas of IT (41%), crucial in keeping the business safe (37%), and crucial in keeping members of staff safe (32%)



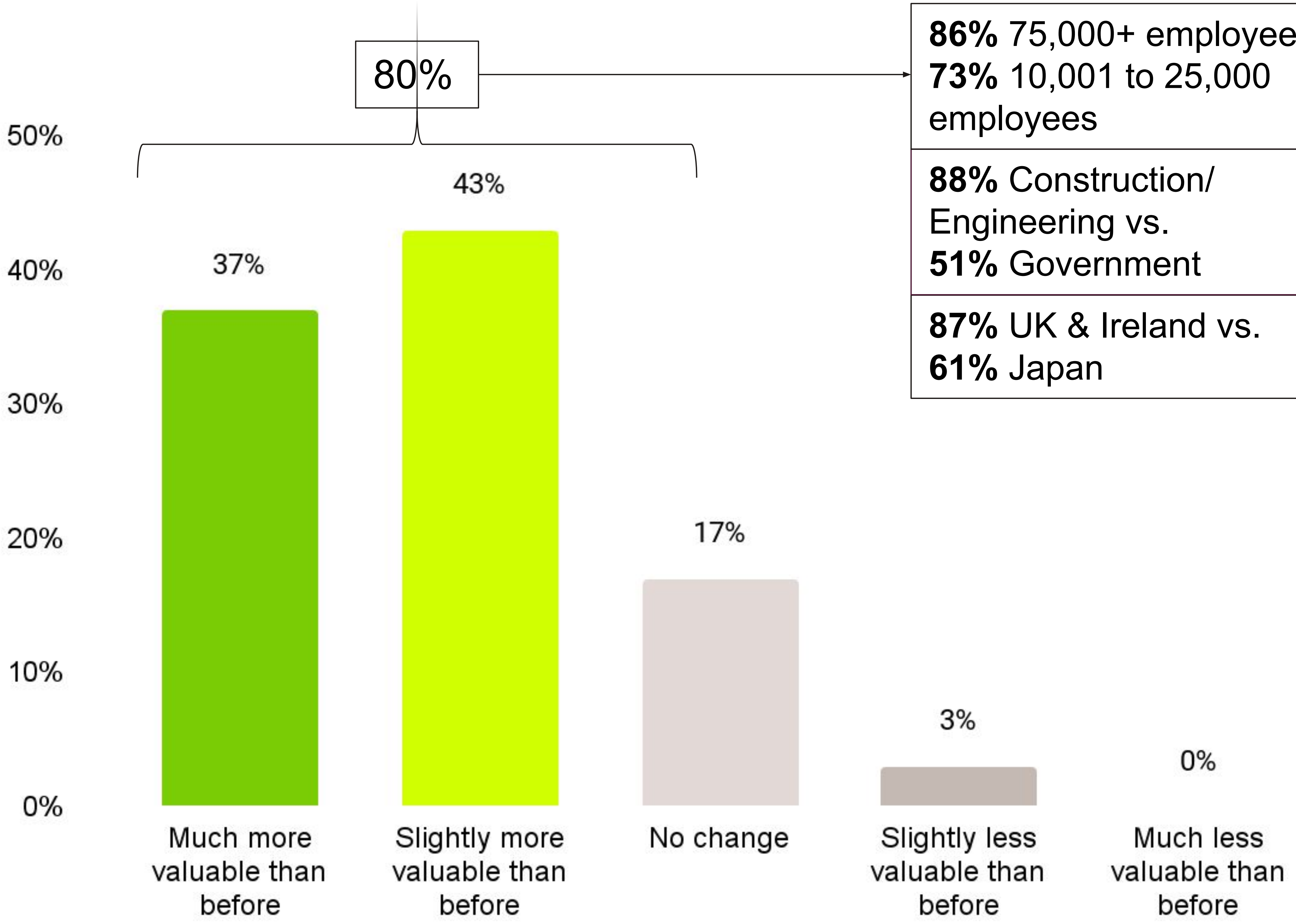
51% Manufacturing vs.
28% Government

51% US vs.
33% Nordics

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

Base: 1484

80% of respondents think their cybersecurity programme has become more valuable over the last 12 months



86% 75,000+ employees vs. **73%** 10,001 to 25,000 employees

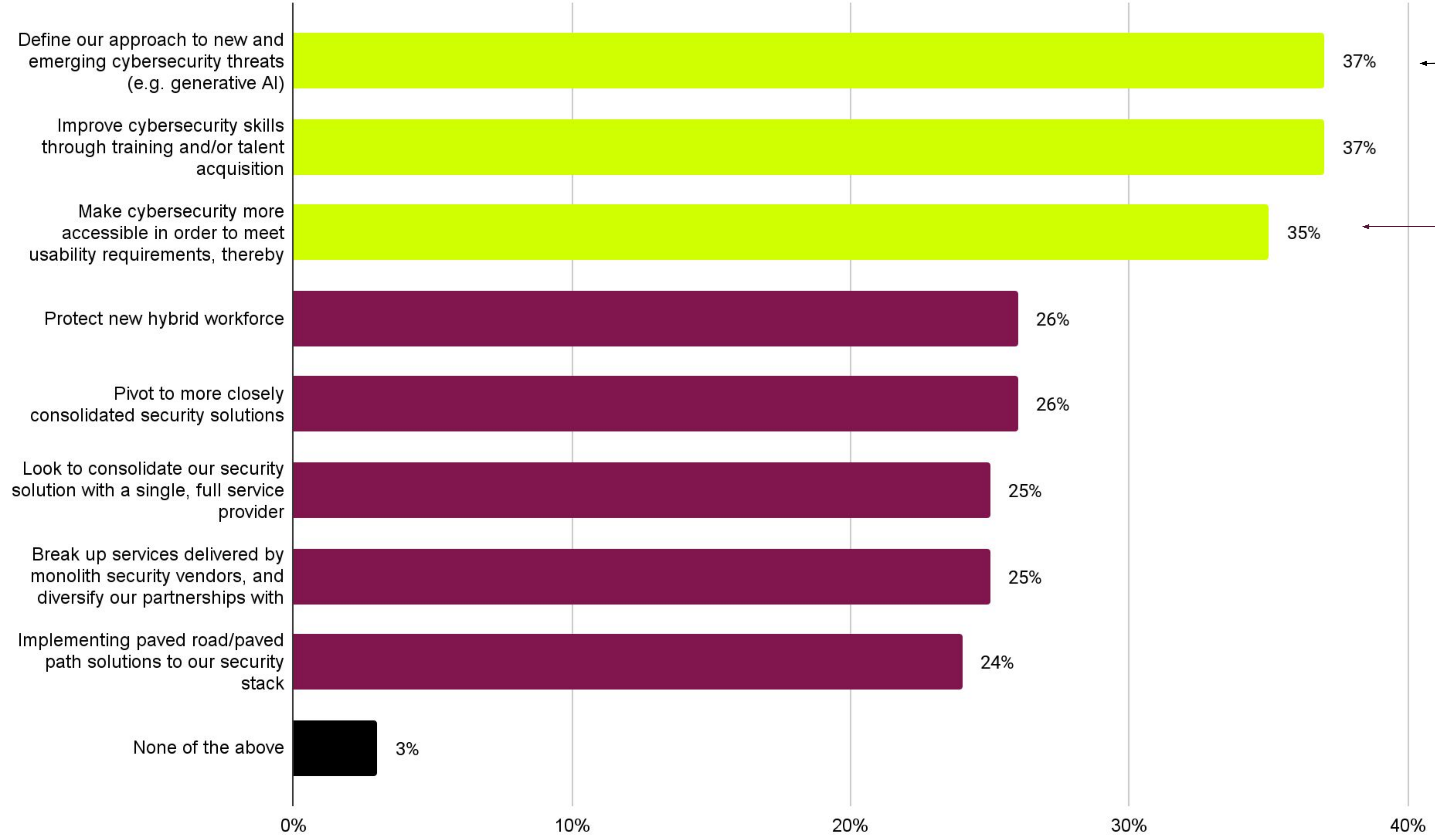
88% Construction/ Engineering vs. **51%** Government

87% UK & Ireland vs. **61%** Japan

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: 1484

Defining approaches to new and emerging cybersecurity threats (37%), improving cybersecurity skills through training and/or talent acquisition (37%), and making cybersecurity more accessible (35%) are the main security priorities over the next year



44% Spain vs.
27% Nordics

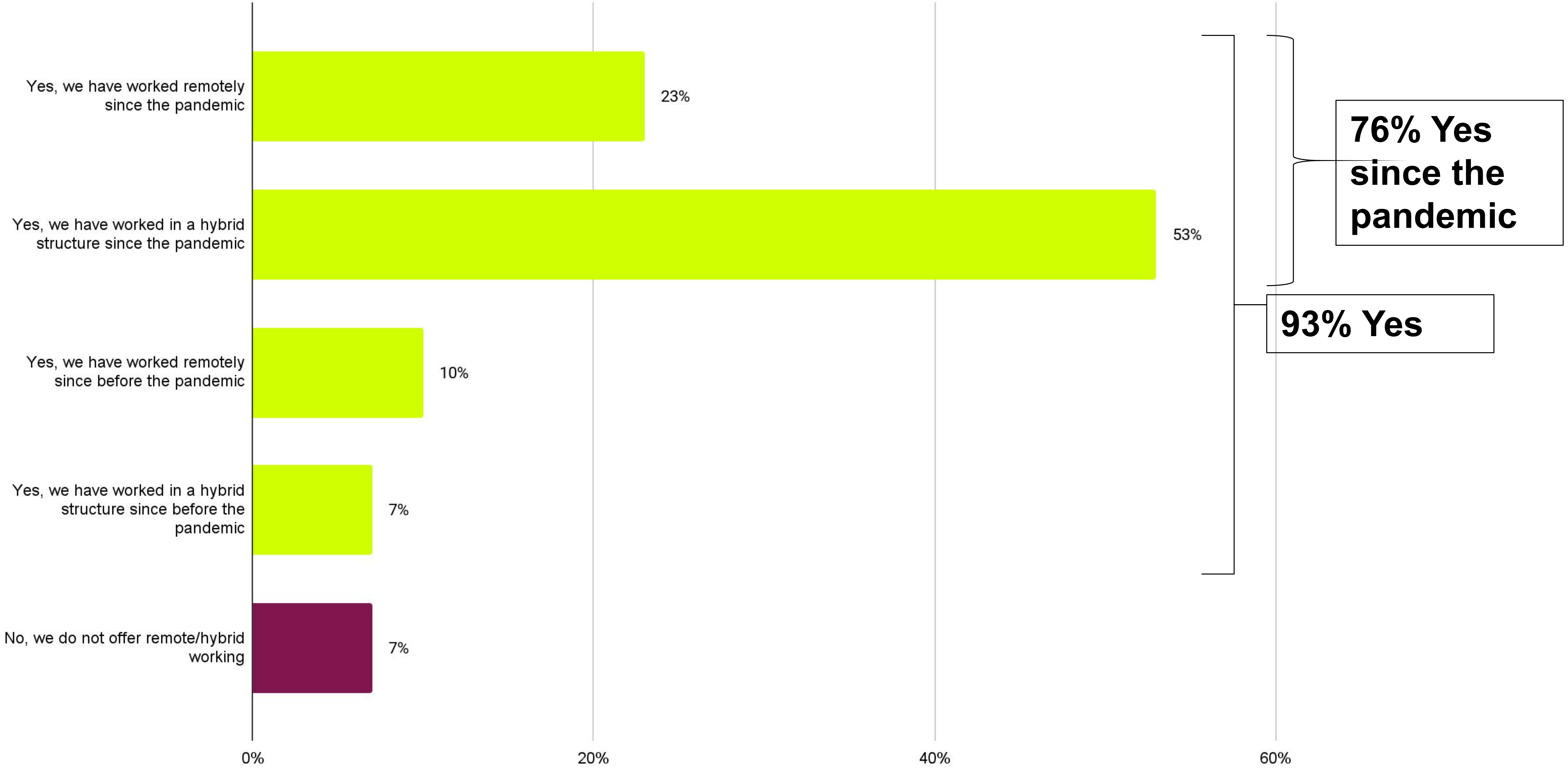
50% Telecommunications vs.
24% Construction/ Engineering

46% Telecommunications vs.
25% Government

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

Base: 1484

93% of businesses have adopted a hybrid/remote working culture
76% have adopted this culture since the pandemic



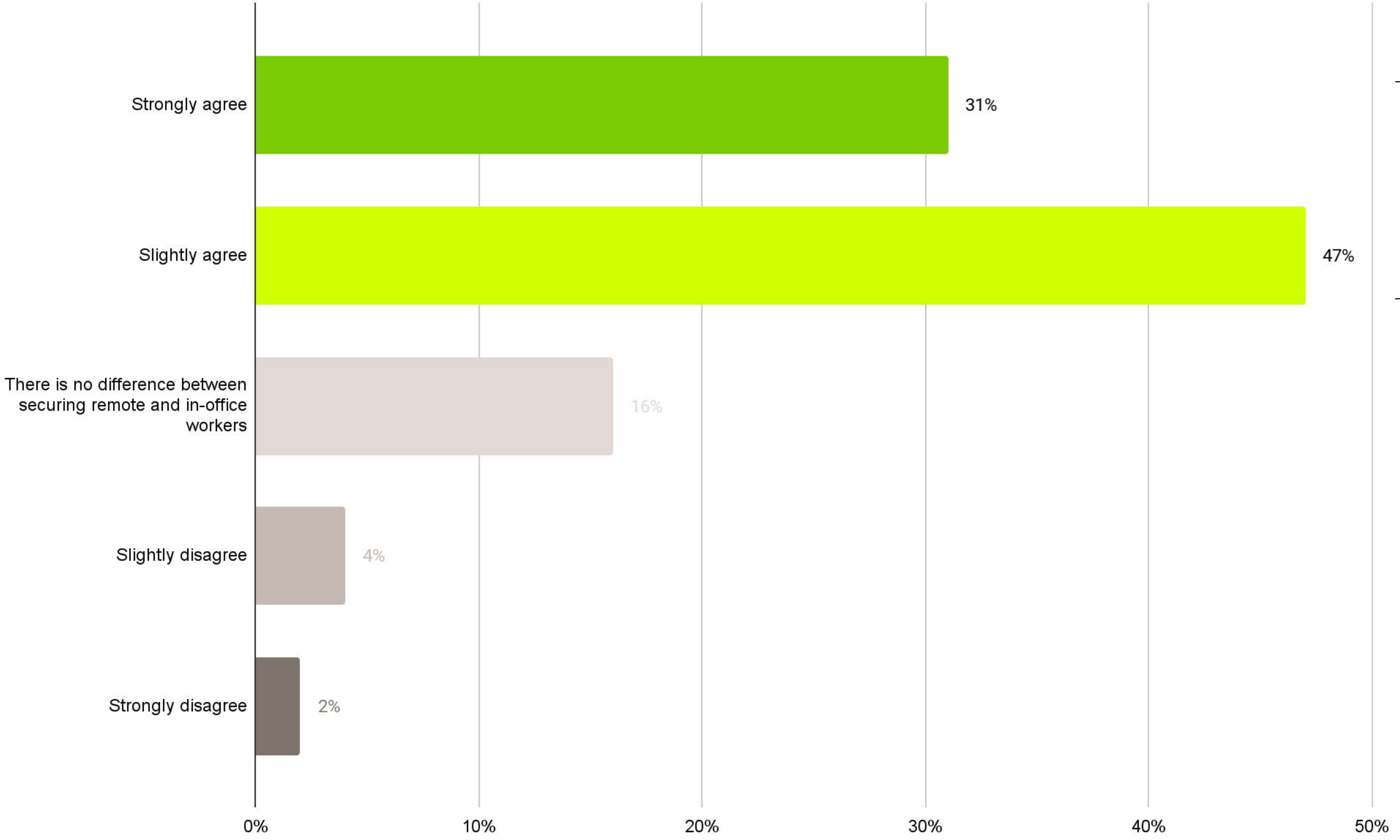
76% Yes since the pandemic

93% Yes

Q14a. Has your organisation adopted a remote/hybrid working culture? Select one

Base: 1484

78% agree that remote workers are more difficult to secure than in-office workers
This is more of an issue for those in the construction industry



78% Agree

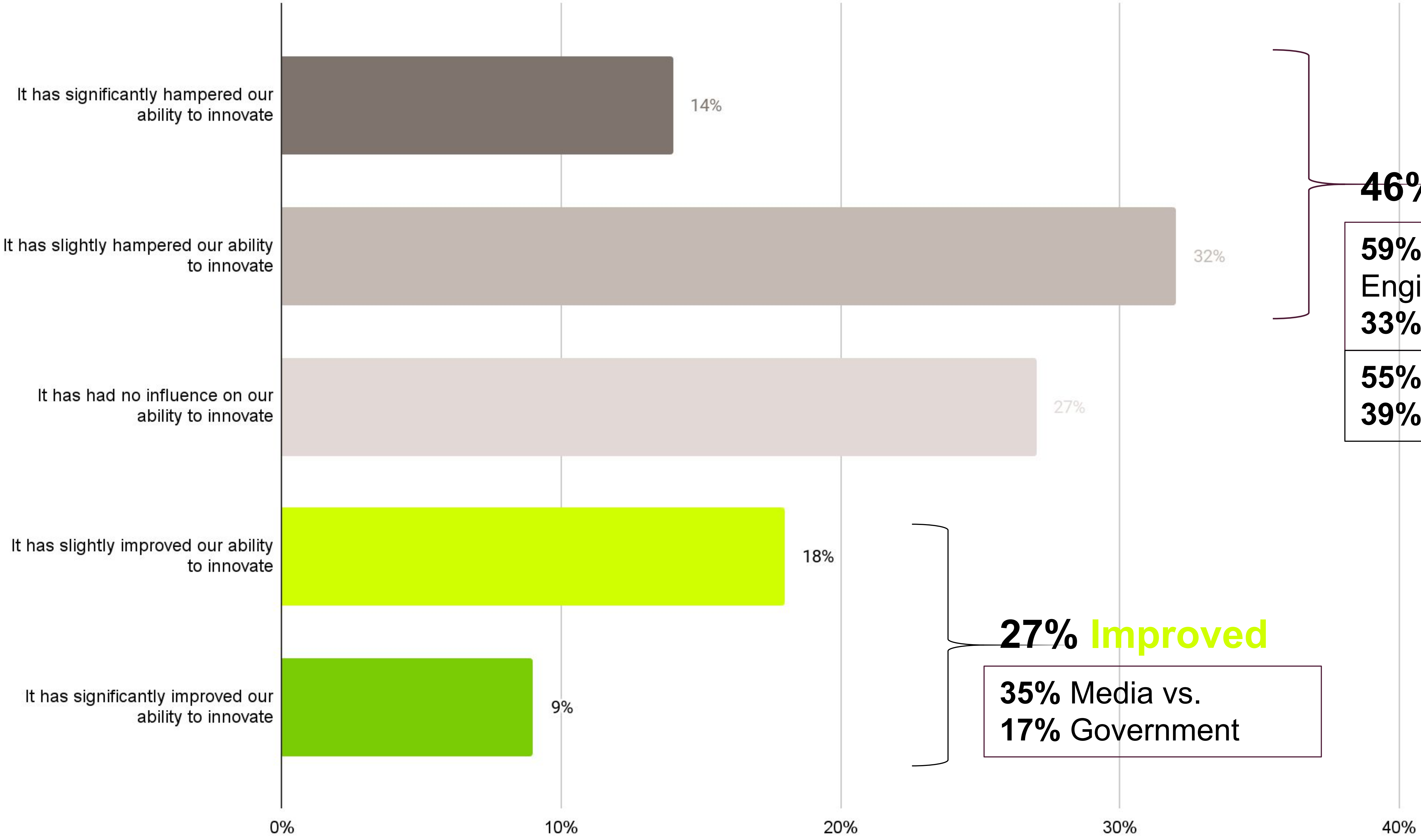
90% Construction/ Engineering vs. **69%** Media and Government

*asked to all asked to those who have adopted a remote / hybrid working culture

Q14b. To what extent do you feel remote workers are more difficult to secure than in-office workers? Select one

Base: 1386*

46% say that their organisations cybersecurity strategy has hampered business innovation
Only a quarter say it has improved innovation (27%)



46% Hampered

59% Construction/ Engineering vs. **33%** Retail

55% DACH vs. **39%** Japan

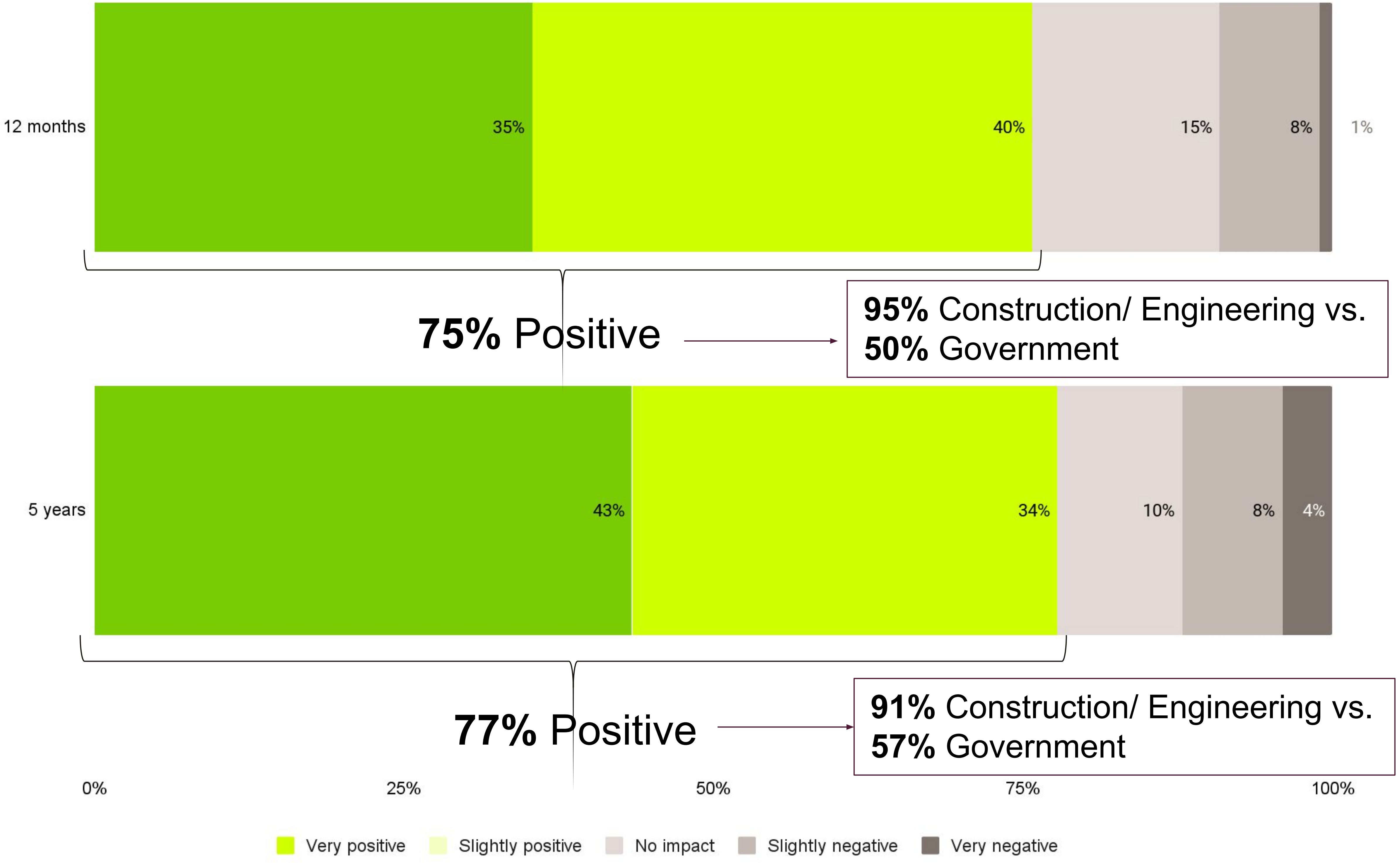
27% Improved

35% Media vs. **17%** Government

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

Base: 1484

75% predict that Generative AI will have a positive impact on cybersecurity over the next 12 months
77% predict it will have a positive impact over the next 5 years



75% Positive

95% Construction/ Engineering vs.
50% Government

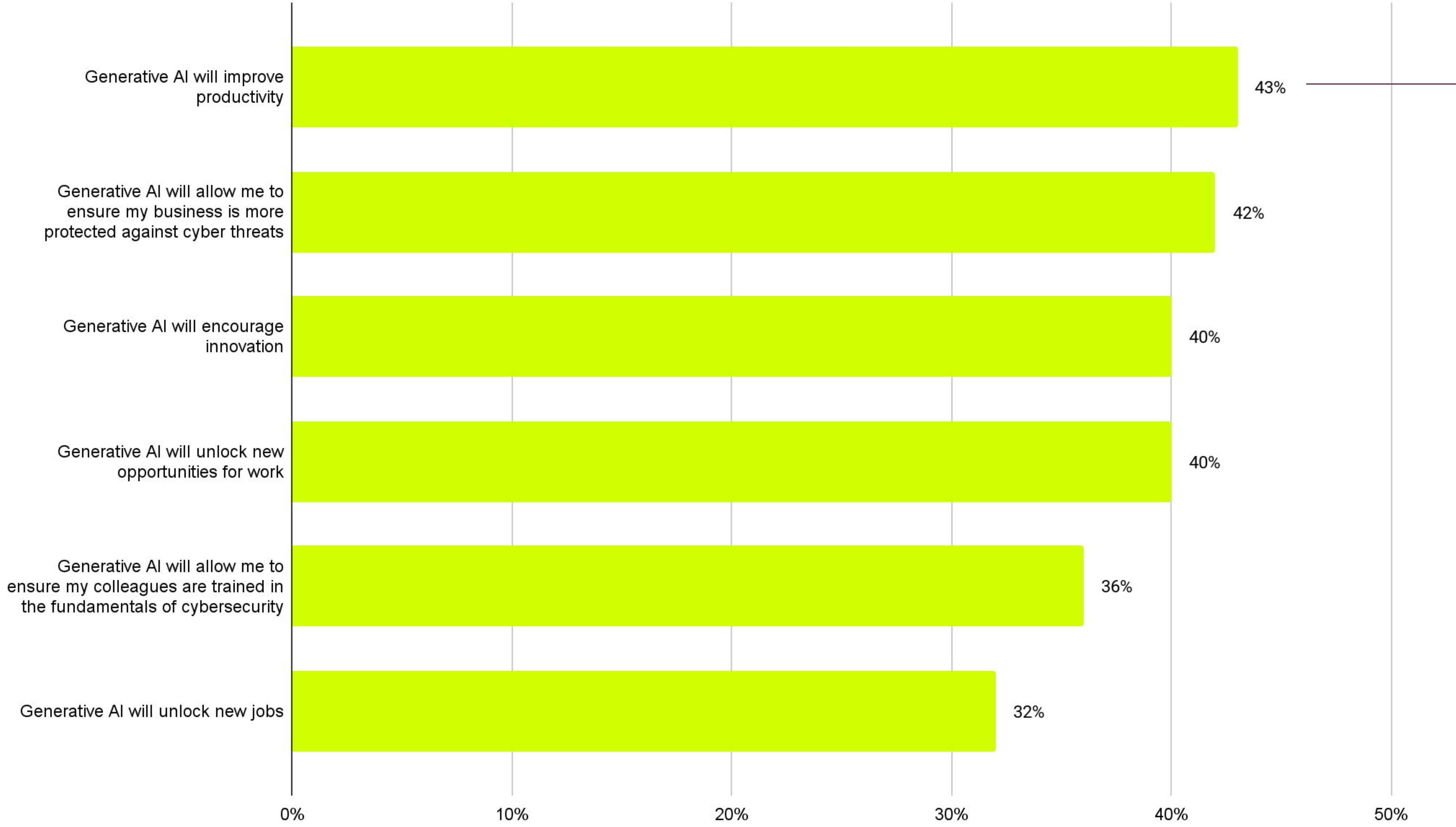
77% Positive

91% Construction/ Engineering vs.
57% Government

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

Base: 1484

Improving productivity (43%) and ensuring the business is more protected against cyber threats (42%) are the main positive impacts of Generative AI



52% Retail/ Wholesale vs. **33%** Financial

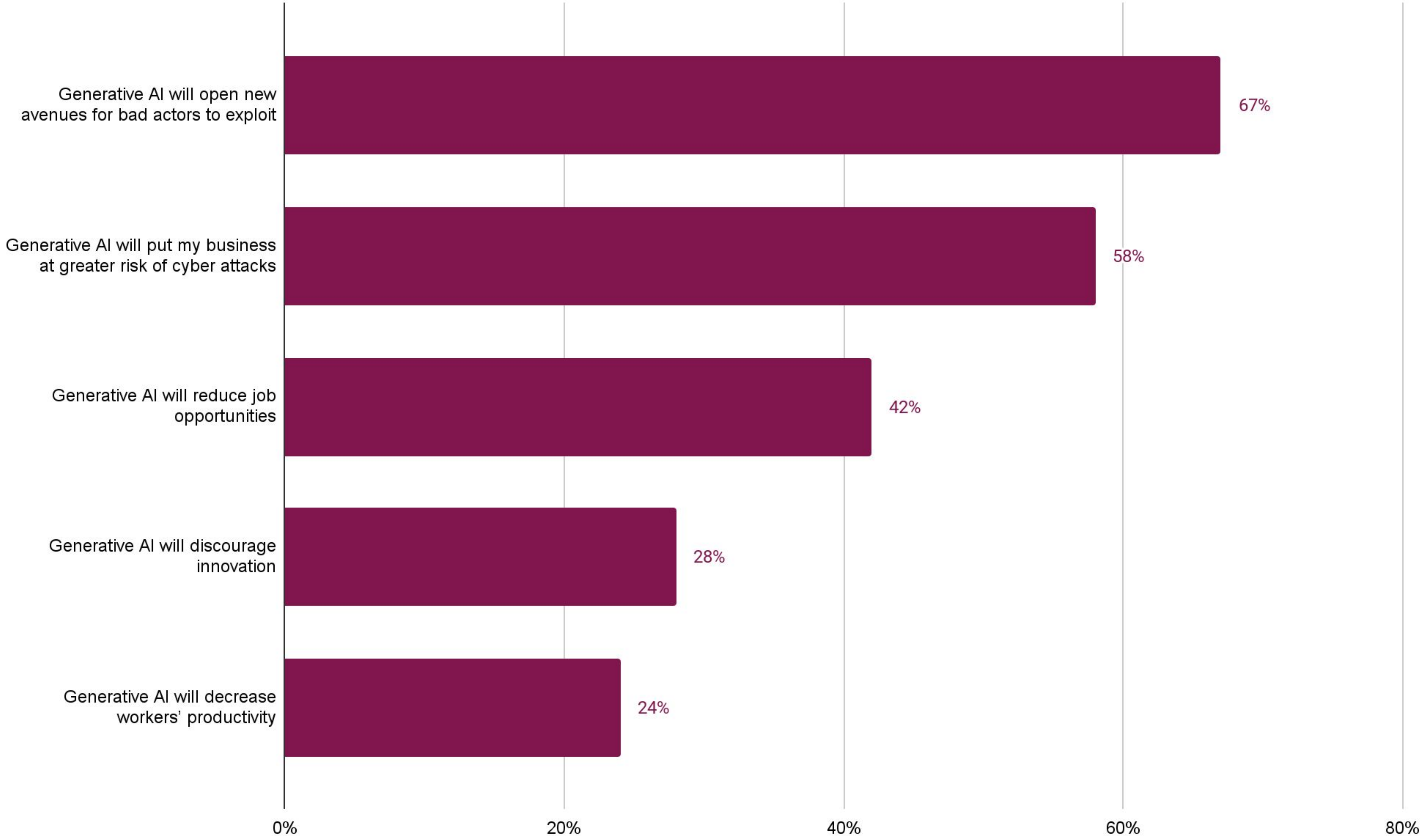
Country/ Region	**%**
AUS & NZ	**34**
DACH	39
UK & Ireland	39
Nordics	42
Spain	46
Japan	**54**
US	**54**

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

Base : 1118*

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 (67%), or that it will put businesses at greater risk of cyber attacks (58%)

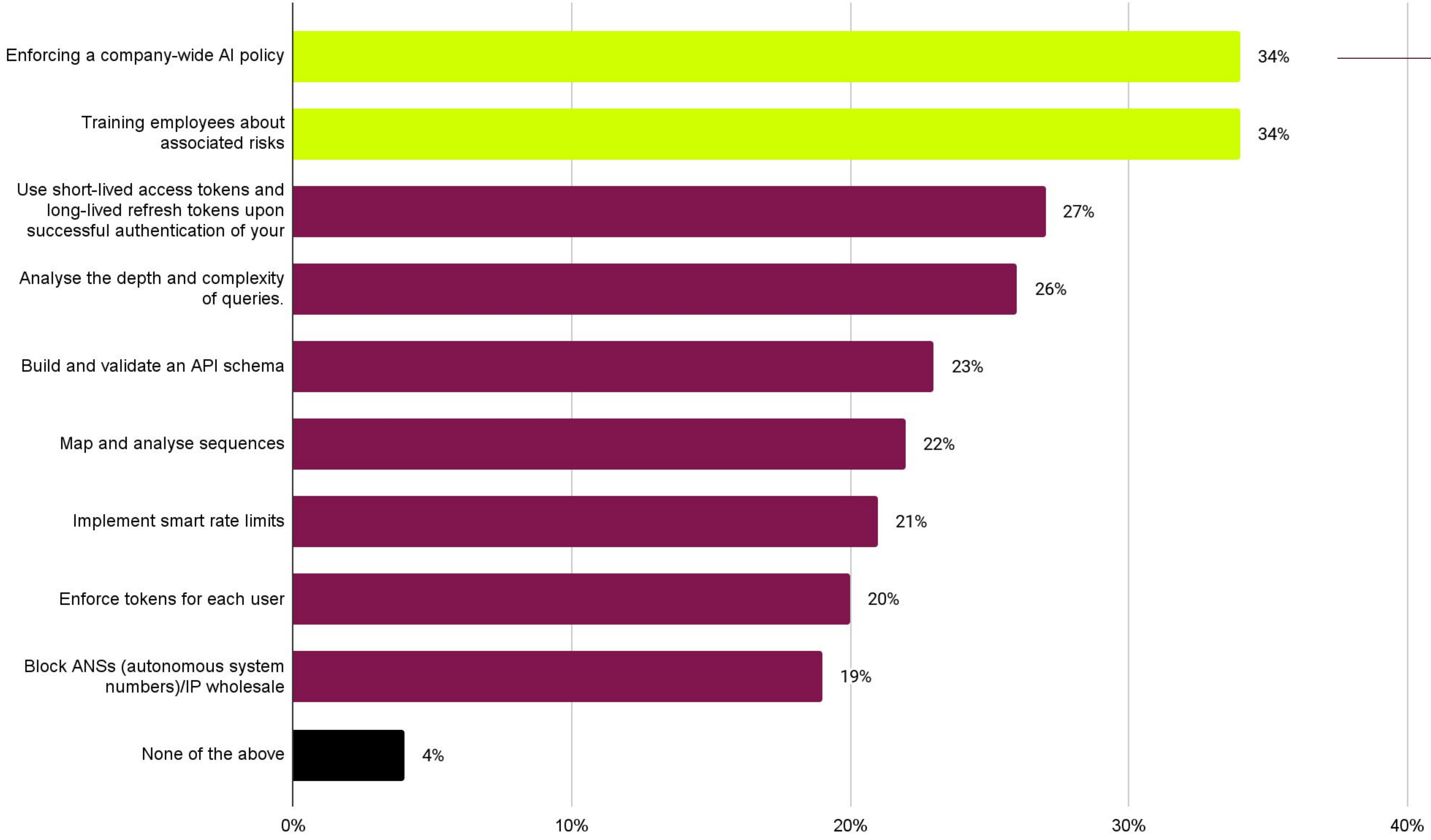


*only asked to those who said generative AI will have a negative impact in the next 12 months

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: 144*

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

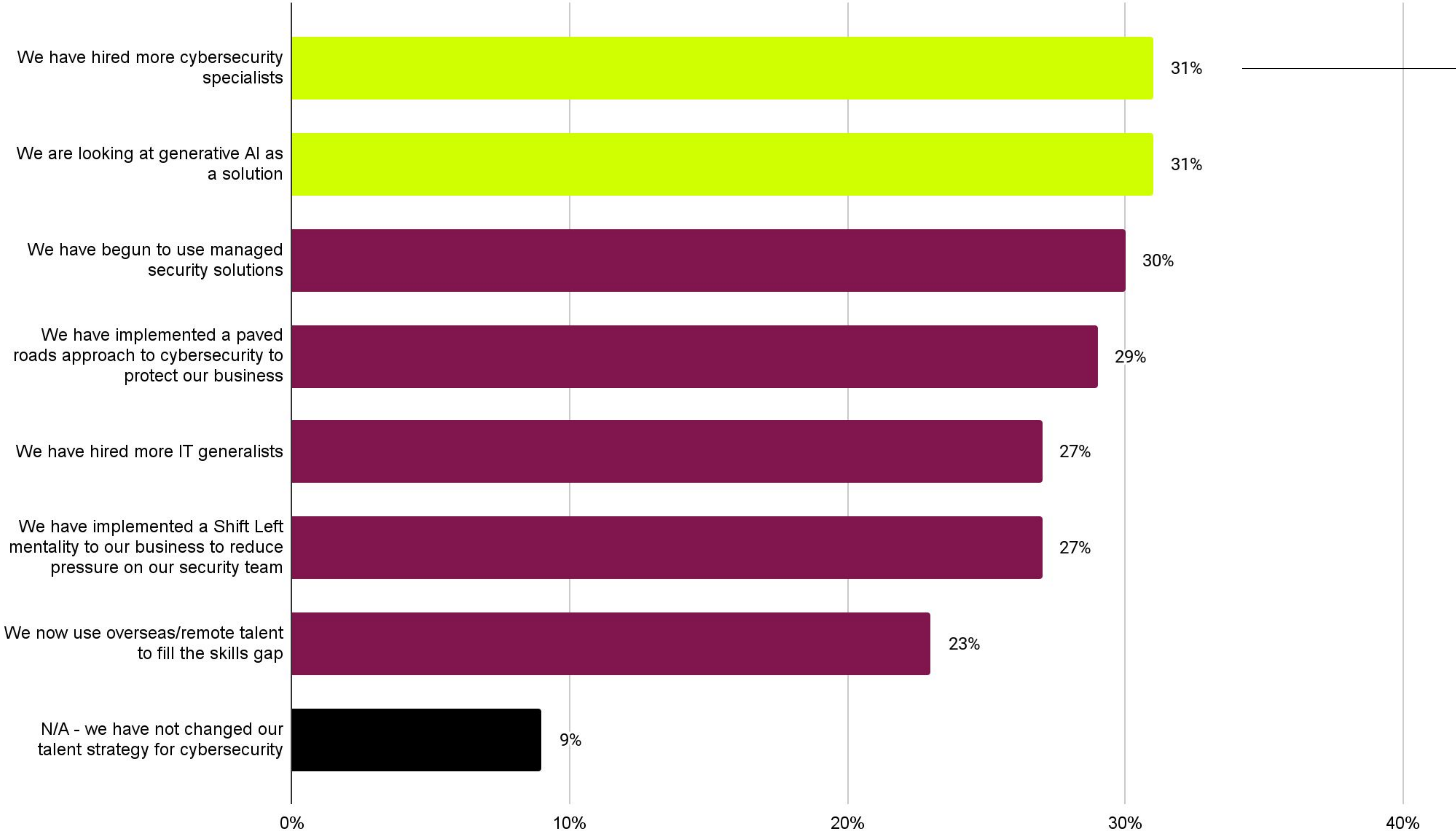


42%Telecommunications vs. **27%** Construction/ Engineering

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

Base: 1484

Companies have hired more cybersecurity specialists and look at generative AI as a solution (both 31%) over the last 12 months



43% 25,001 to 75,000 employees vs. **27%** 75,000+

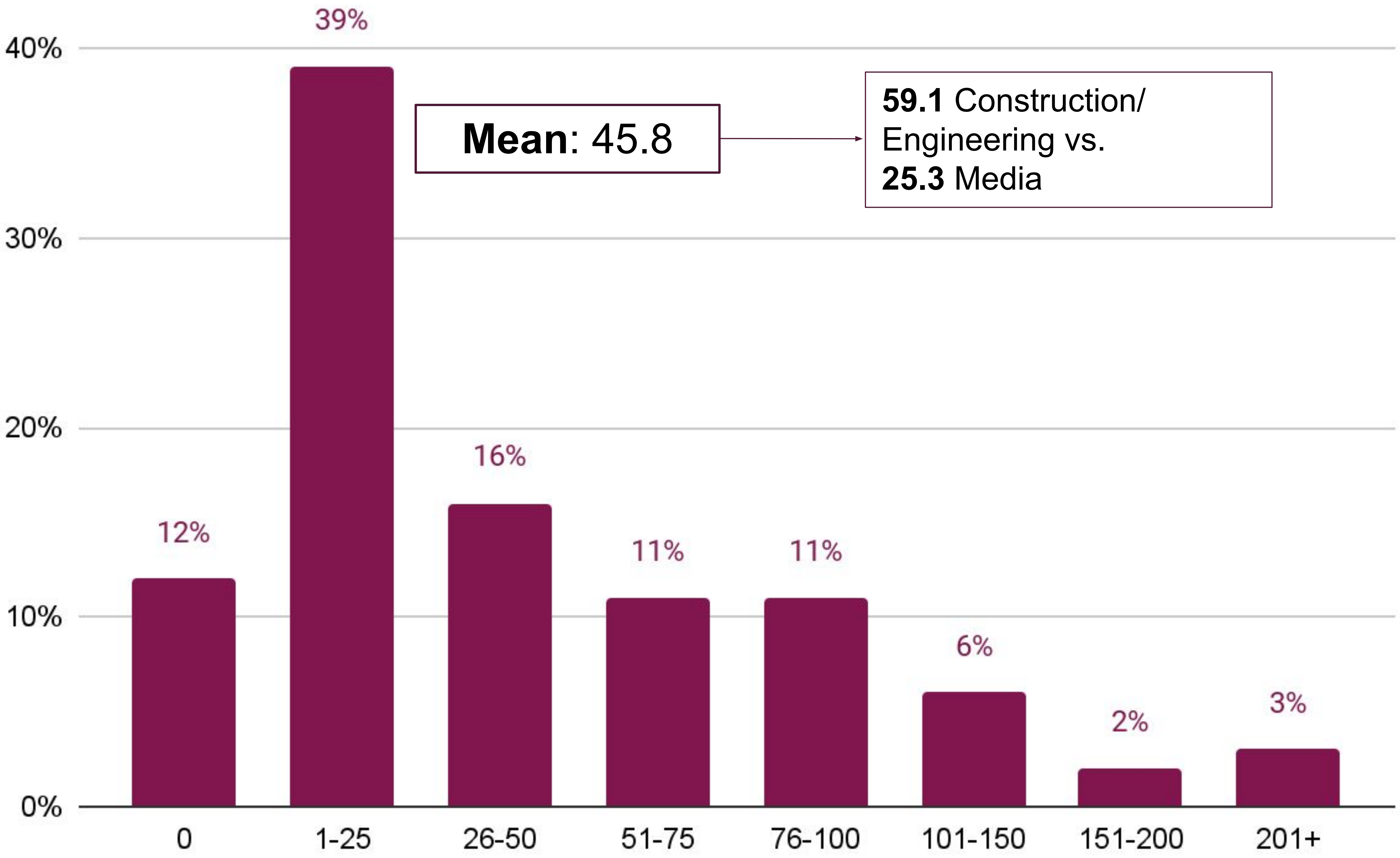
40% Telecommunications vs. **21%** Construction/ Engineering

36% US and Aus / NZ vs. **22%** Japan

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

Base: 1484

On average, businesses have suffered 46 cyberattacks in the past 12 months
With those in DACH experiencing 57



Mean: 45.8

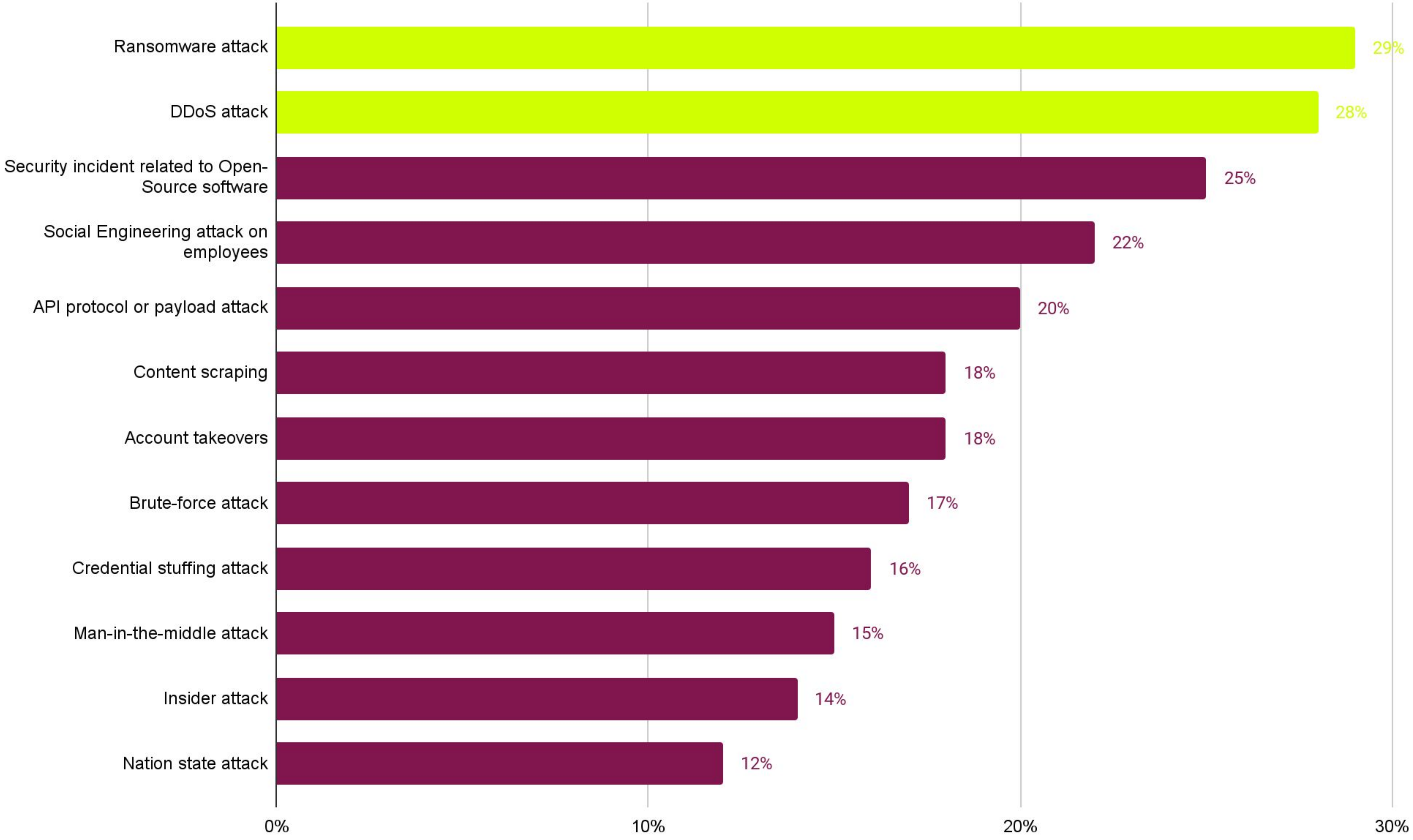
59.1 Construction/ Engineering vs. **25.3** Media

Country/ Region	Mean
Japan	**36.3**
Spain	37.2
UK & Ireland	43.3
US	46.6
AUS & NZ	49.5
Nordics	51.2
DACH	**57.2**

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

Base: 1484

The most common types of cyberattacks were ransomware attacks (29%) and DDoS attacks (28%)



46% Government vs.
18% Construction/ Engineering

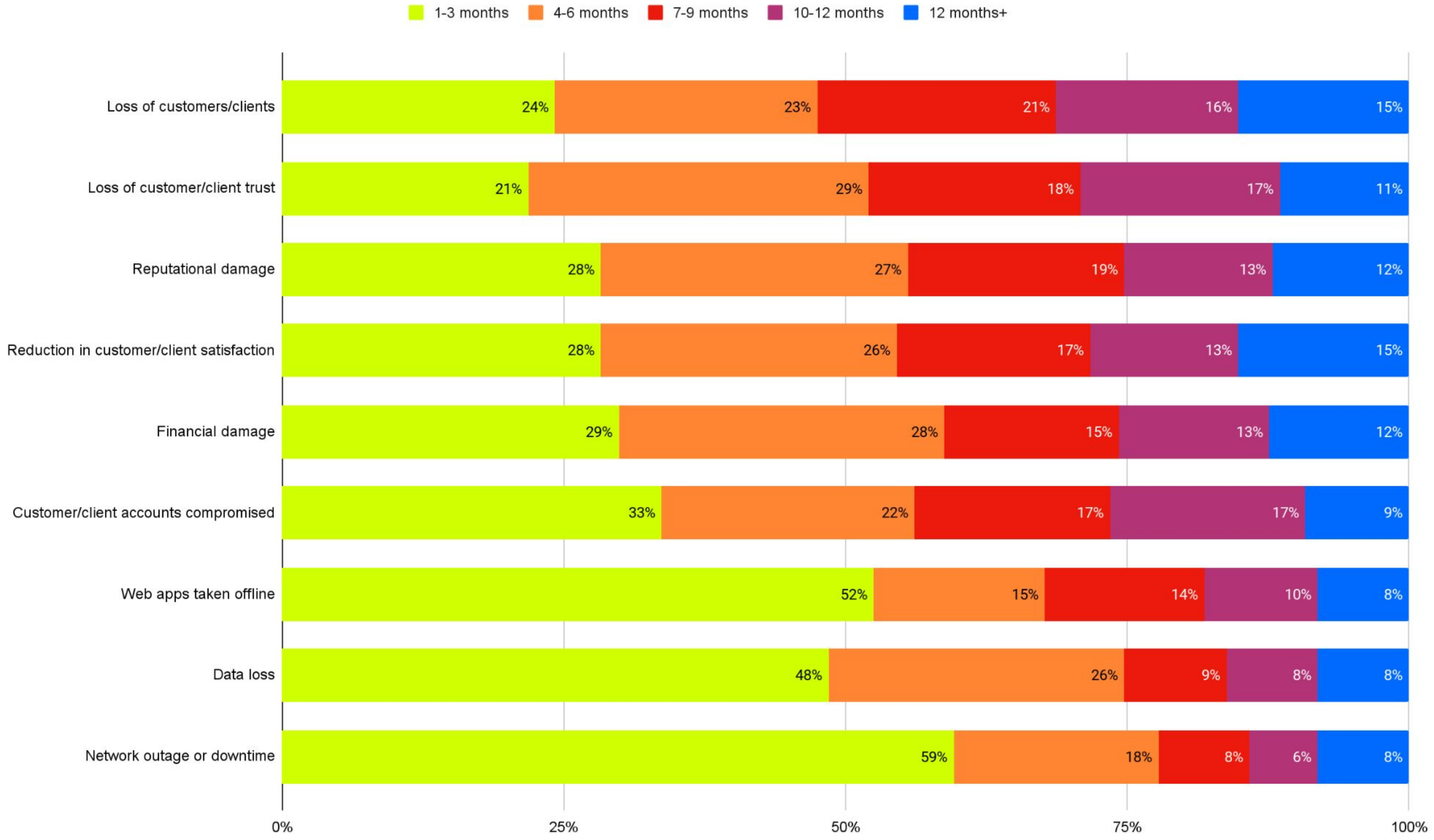
53% Japan vs.
15% Nordics

*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: 1309*

On average, it will take businesses 7.67 months to recover from the loss of customers/ clients as a result of a cyber attack



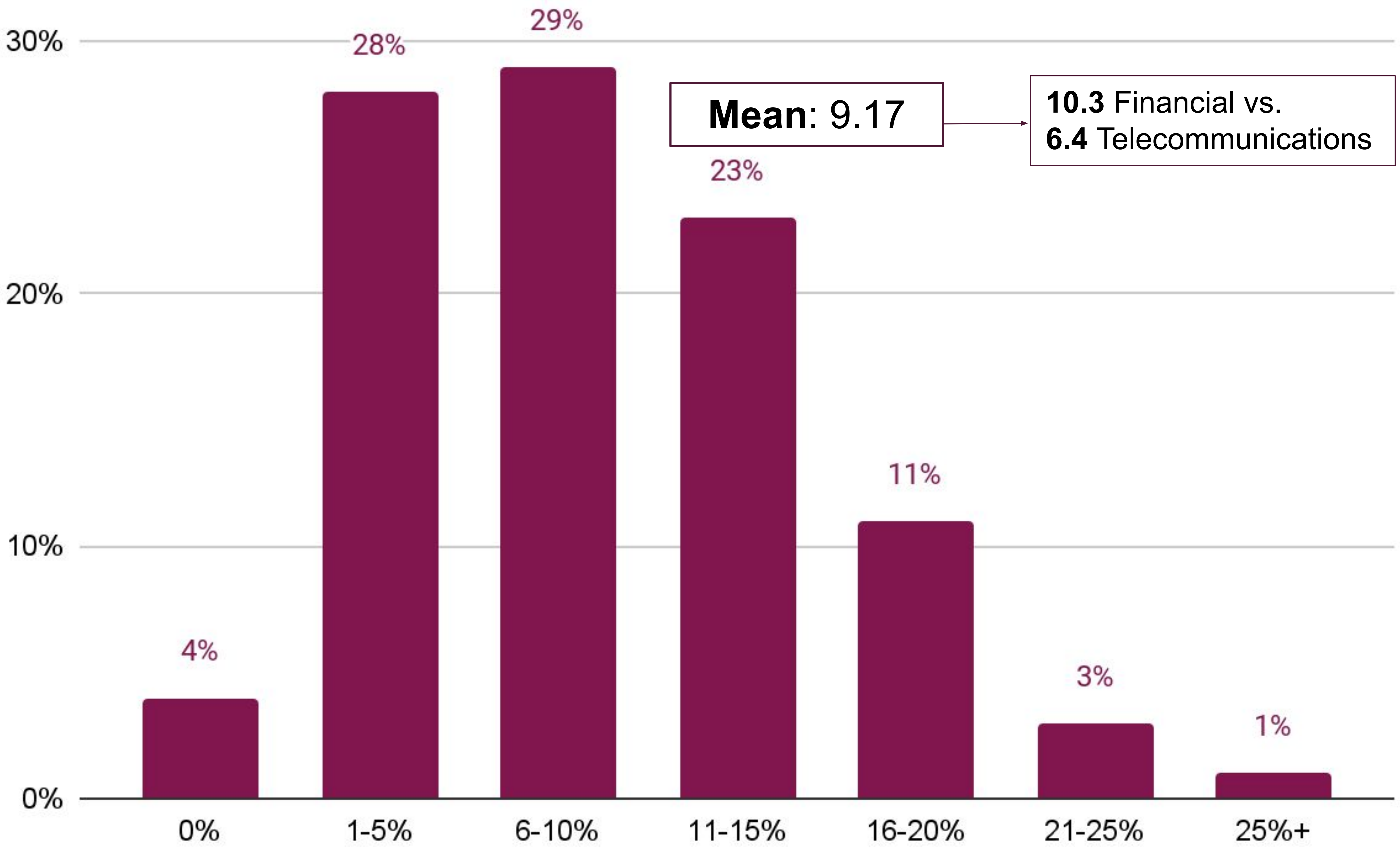
Average no. Months
7.67
7.45
7.15
7.13
6.96
6.57
5.29
5.11
4.68

*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 9.17% of their annual income as a result of cyber attacks



Mean: 9.17

10.3 Financial vs.
6.4 Telecommunications

Country/ Region	Mean
Japan	**6.9**
Spain	7.9
DACH	9.0
AUS & NZ	9.1
Nordics	9.9
US	10.3
UK & Ireland	**10.6**

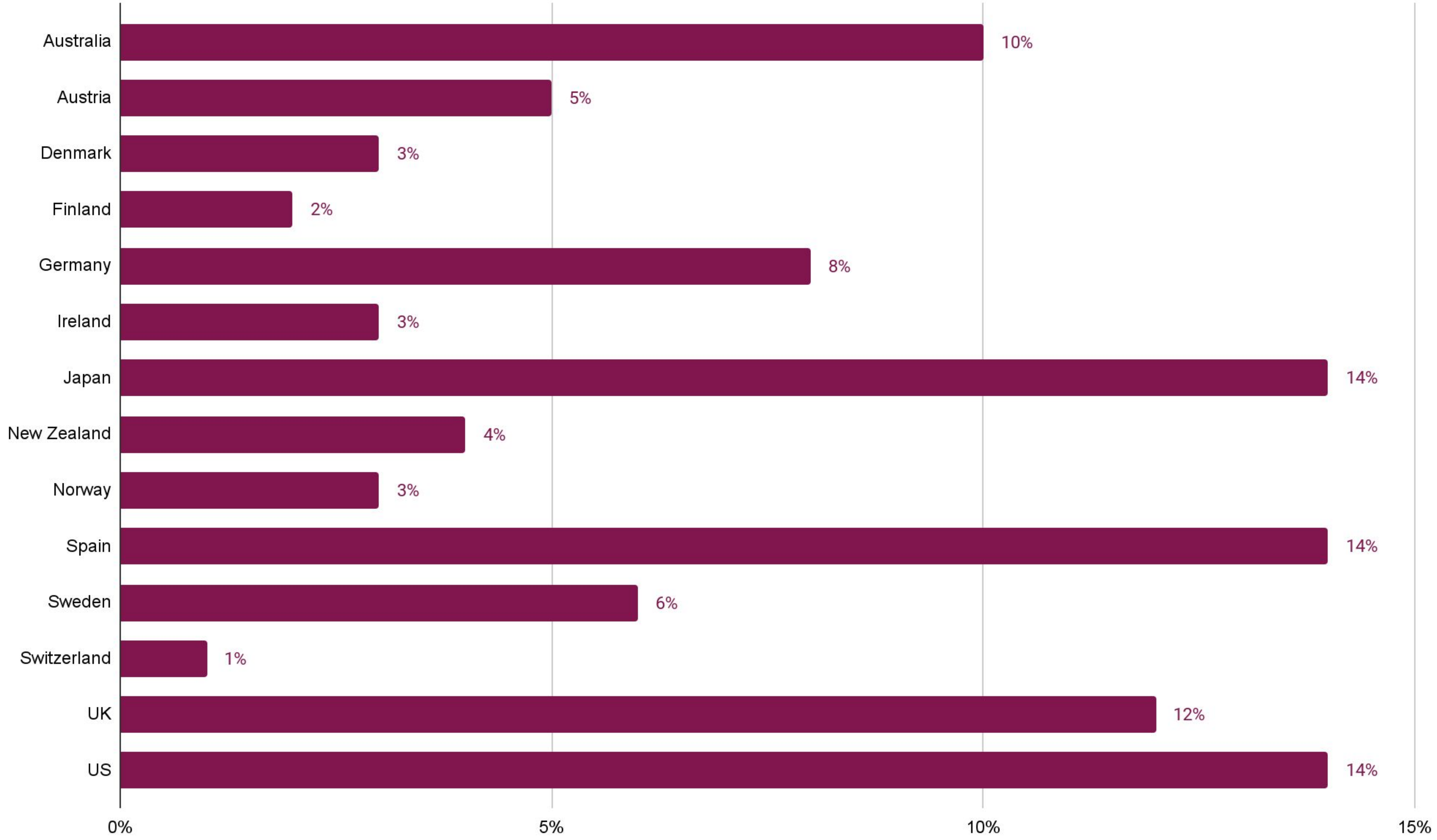
Q24. As a percentage of your business's overall revenue, what would you estimate to be the financial impact of these attacks in the past 12 months? Select one

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

Base: 1309*

Demographics

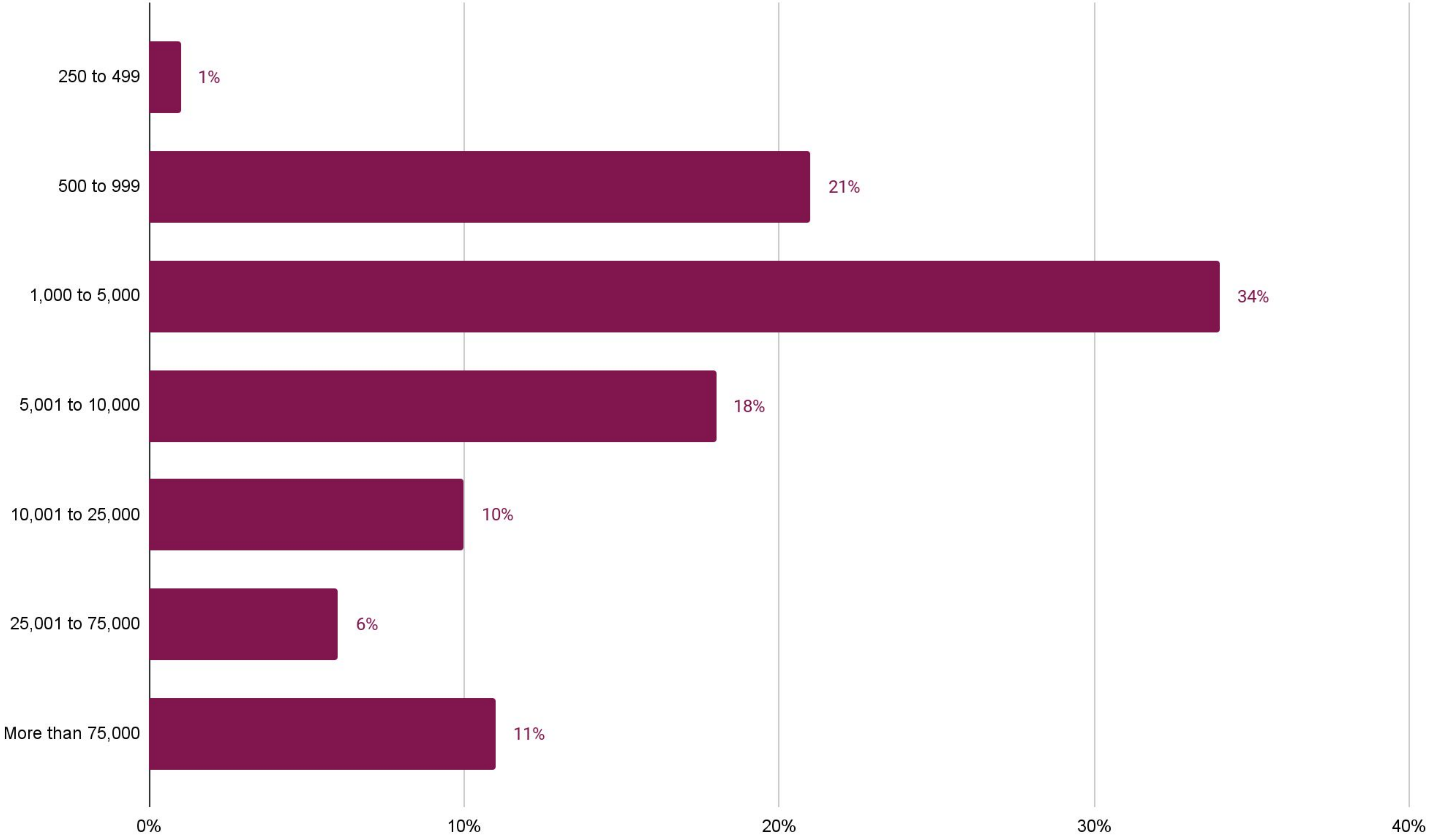
Country



S0. Which country do you live in? Select one

Base: 1484

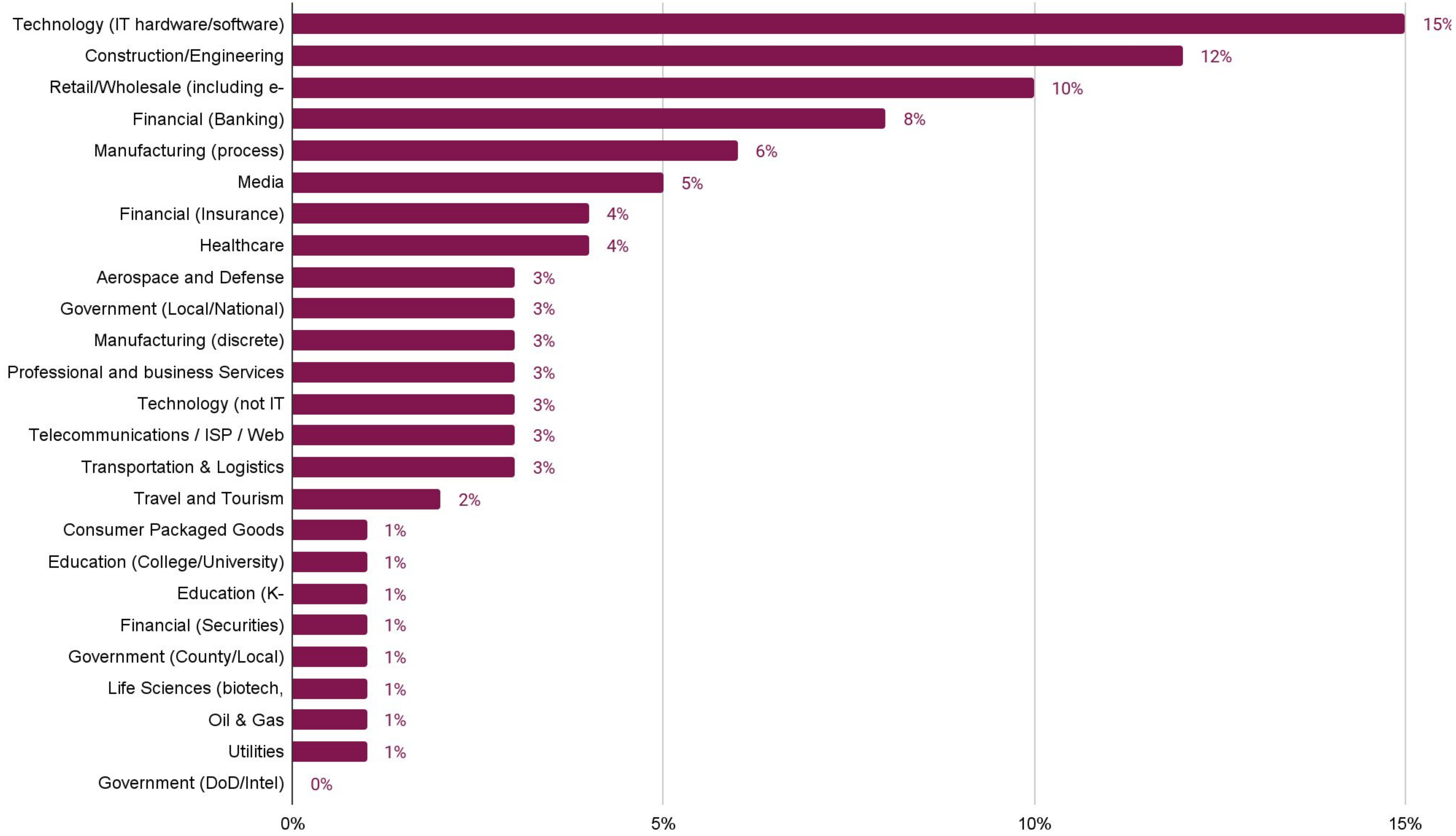
Size



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

Base: 1484

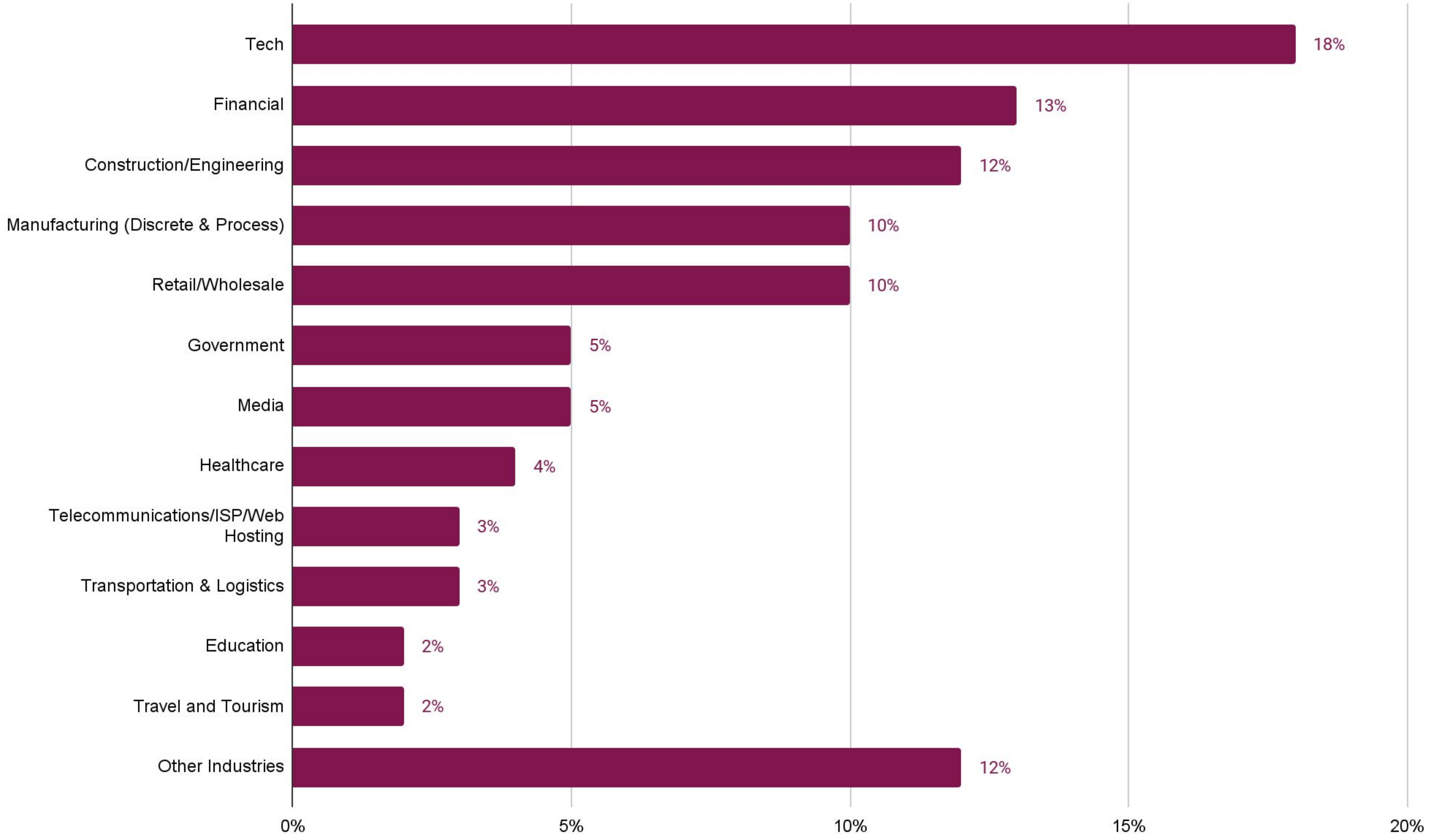
Industry



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

Base: 1484

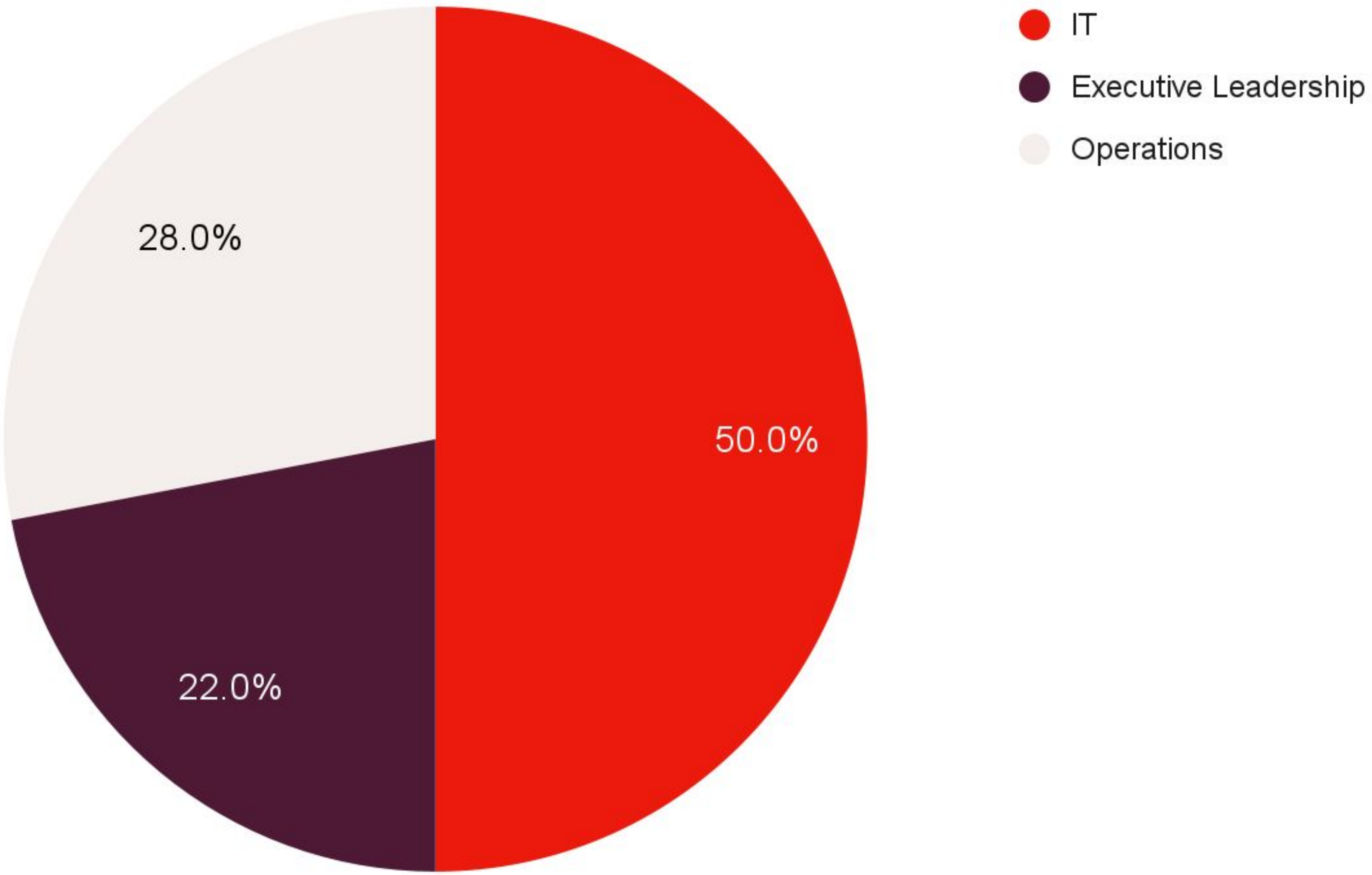
Industry - focus



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

Base: 1484

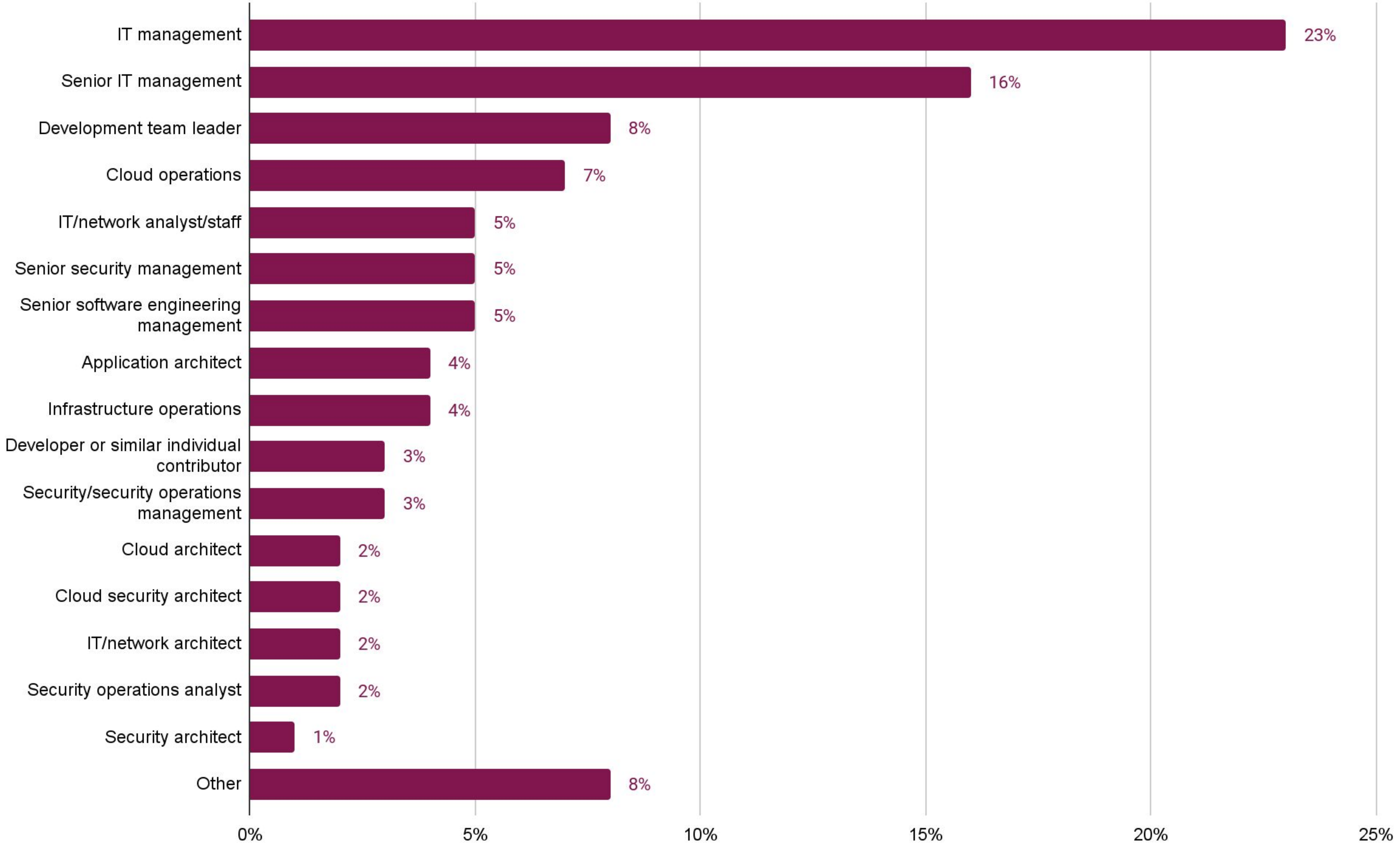
Department



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

Base: 1484

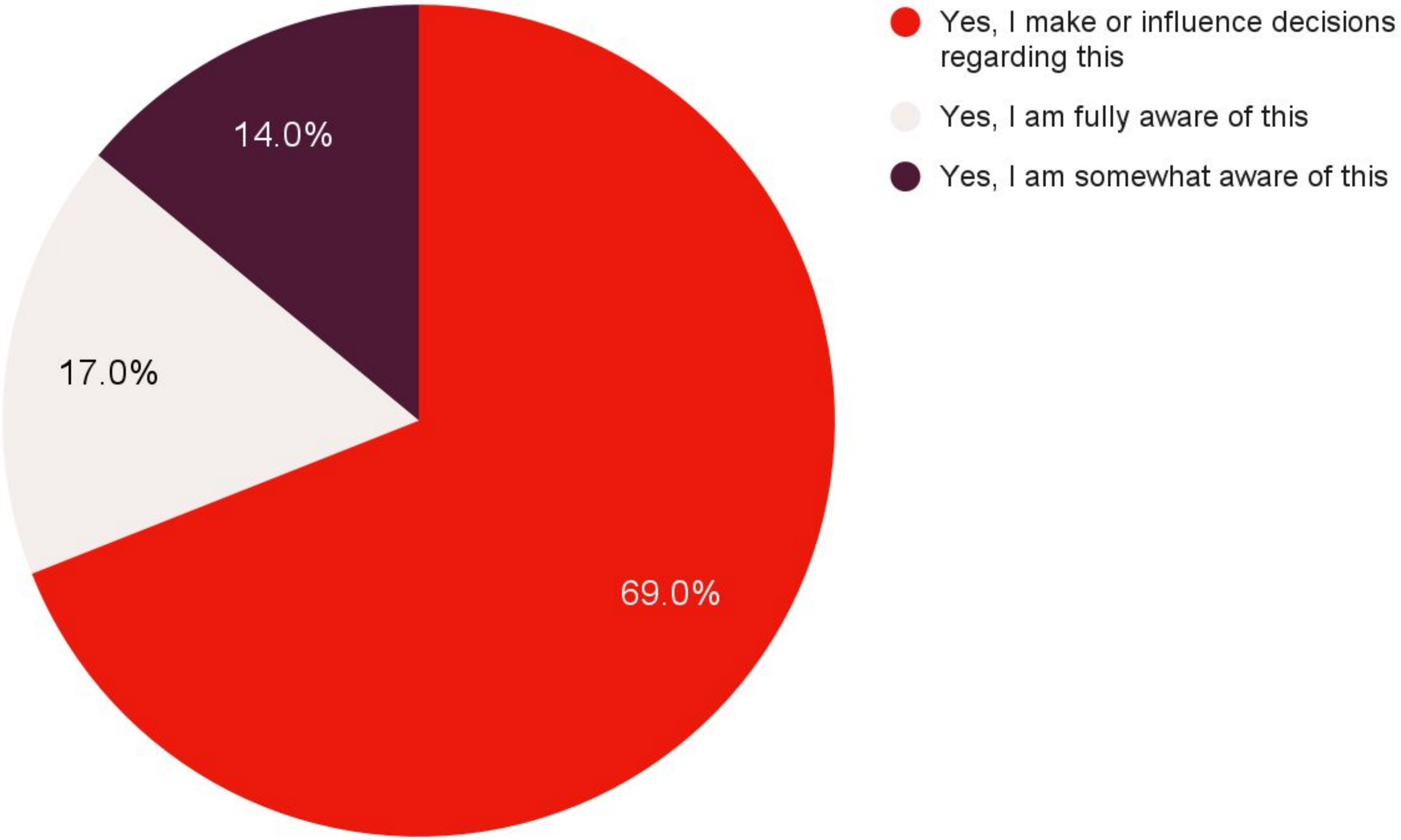
Current responsibility



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

Base: 1484

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: 1484

Thank you!

fastly