

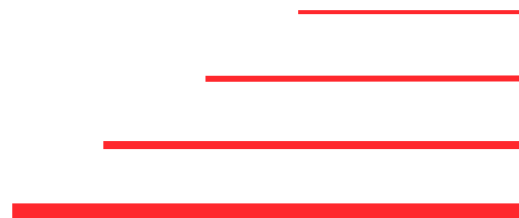


Fastly Global Security Research 2024

USA Findings

November 2024

Research conducted by
SAPIO Research



Overview & methodology

The survey was conducted among **200 cybersecurity decision makers** (with **2/3 respondents directly making or influencing cybersecurity decisions**) in businesses **with 500 or more employees in the US**. Participants came from a range of roles across the IT, Operations and Executive Leadership functions.

At an overall level results are accurate to $\pm 6.9\%$ at 95% confidence limits assuming a result of 50%.

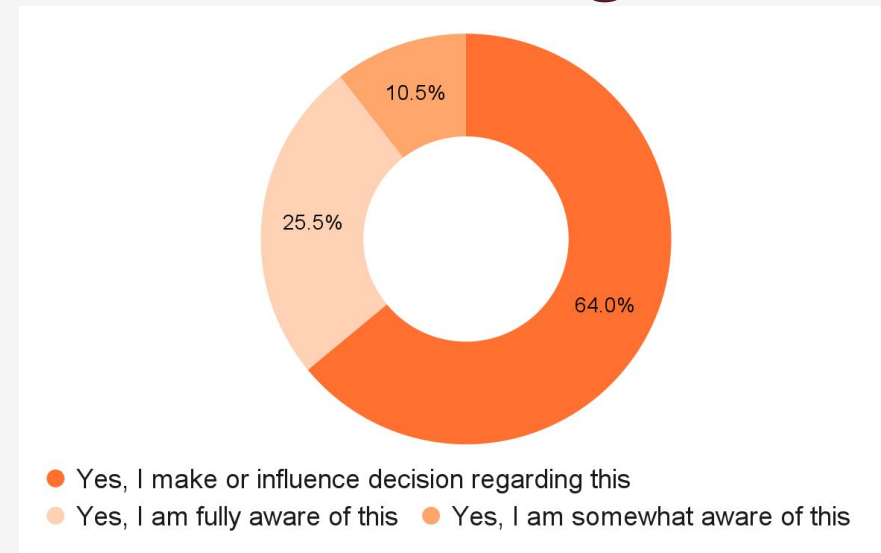
The interviews were conducted online by Sapio Research in September 2024 using an email invitation and an online survey.

Respondent demographics summary – Cybersecurity Decision Makers

Seniority

Department	% of respondents
IT	44%
Operations	34%
Executive leadership	22%

Decision-making



Company size

No of employees	% of respondents
500-999	23%
1,000-4,999	27%
5,000-24,999	31%
25,000+	20%

Primary sectors of Business

1. Healthcare / Life Sciences - 36%
2. Government / Public Sector - 13%
3. Technology - 10%
4. Construction / Engineering - 7%
5. Finance / Accounting - 7%
6. Media/Entertainment / Travel & Tourism - 7%

Country of residence

US





Key takeaways

Key stats

Companies expect it to take **6.34 months** to recover from security incidents

Businesses have experienced **~52** security incidents in the past year, with the top factors present being **external attackers** (31%) and **software bugs** (29%)

Businesses report being reliant upon an average of **7 cybersecurity solutions**, with **40%** of these cybersecurity solutions overlapping in their primary function

Organisations predict that **social engineering attacks (34%)** and **lack of technical skills (29%)** will be their biggest cybersecurity threats in the next 12 months

24% of businesses reported revenue loss as a top impact of security incidents, with those reporting this suffering an average **3.1% loss** following a security incident

81% say that consolidation of security solutions is more appealing due to tighter budgets



Main findings

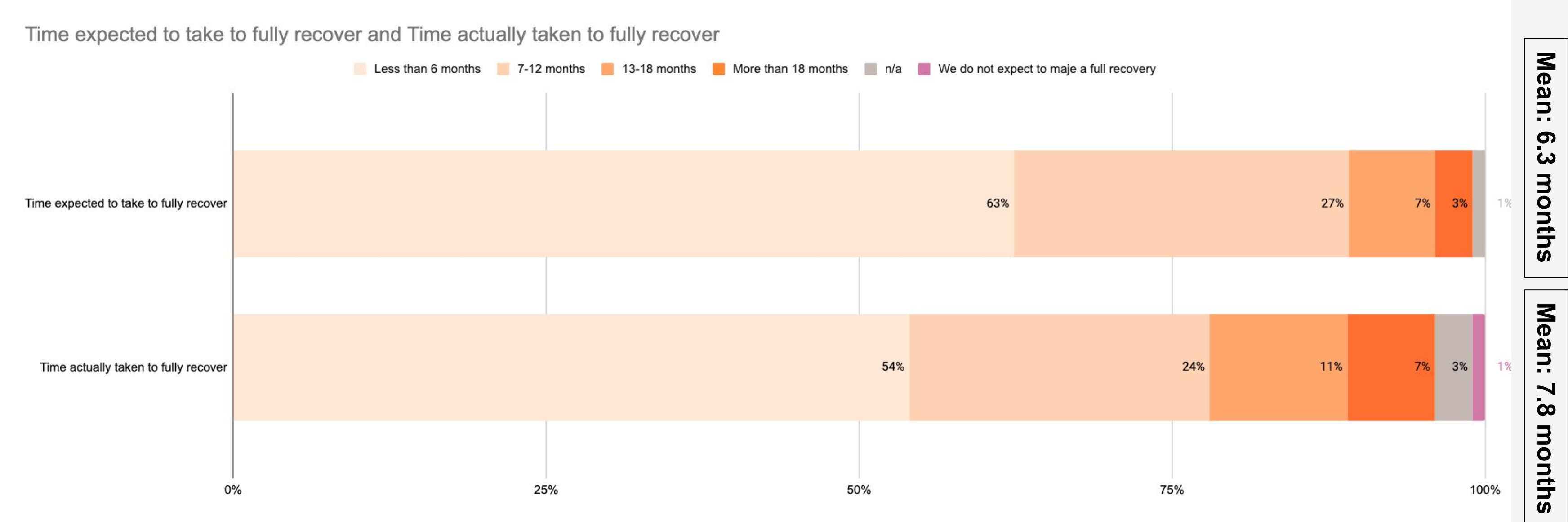


Main Findings

Incident response time and recovery

Expected vs. Actual Recovery Time Following a Security Incident

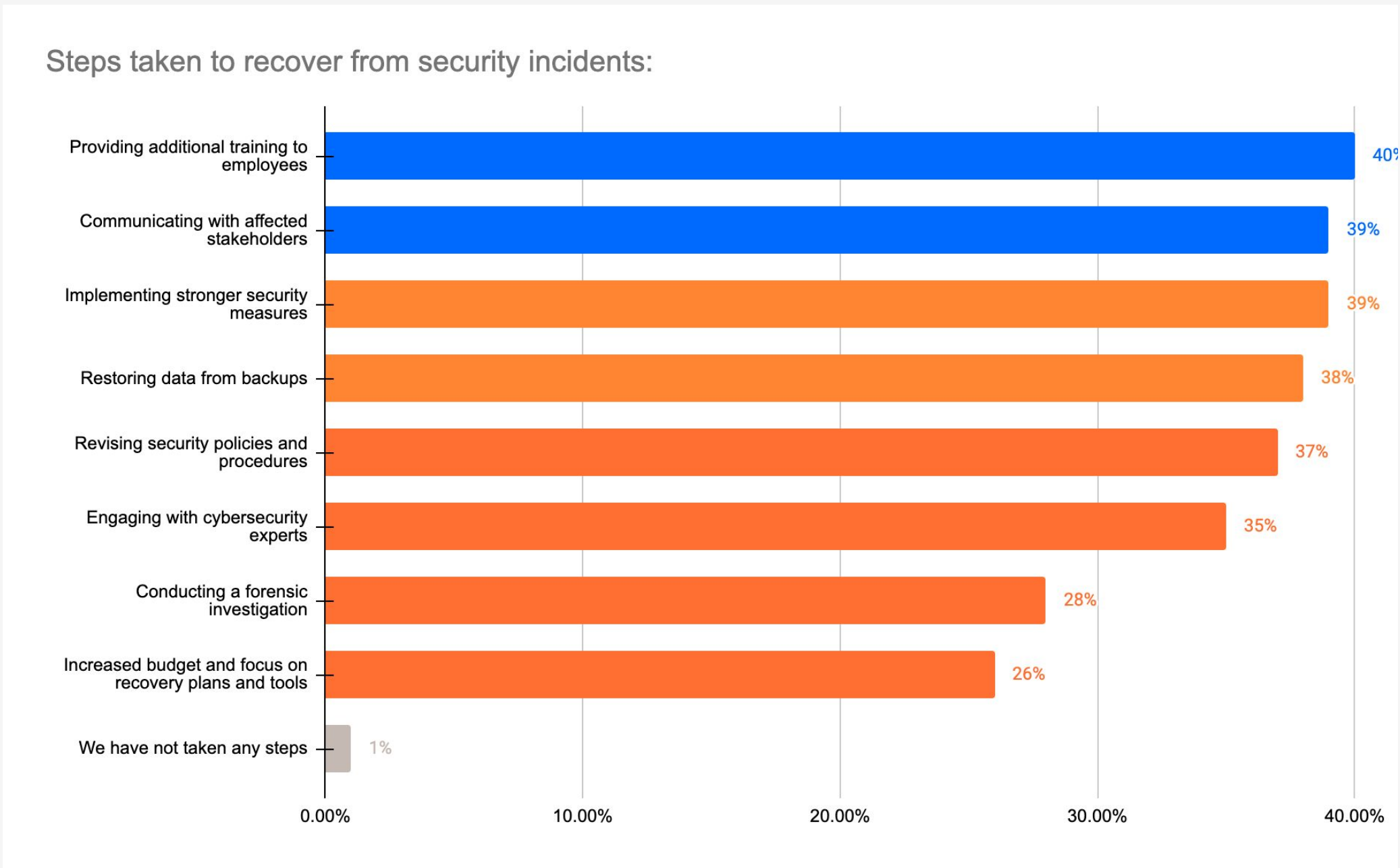
The average time taken for organisations to recover from a security incident is 7 months, 1 month longer than the average business anticipates



Q17e. How long do you expect it to take, and how long has it taken, to fully recover from each of these impacts? | Base: 192 *Only asked to those who have experienced a security incident in the last 12 months

Steps Taken Toward Security Incident Recovery

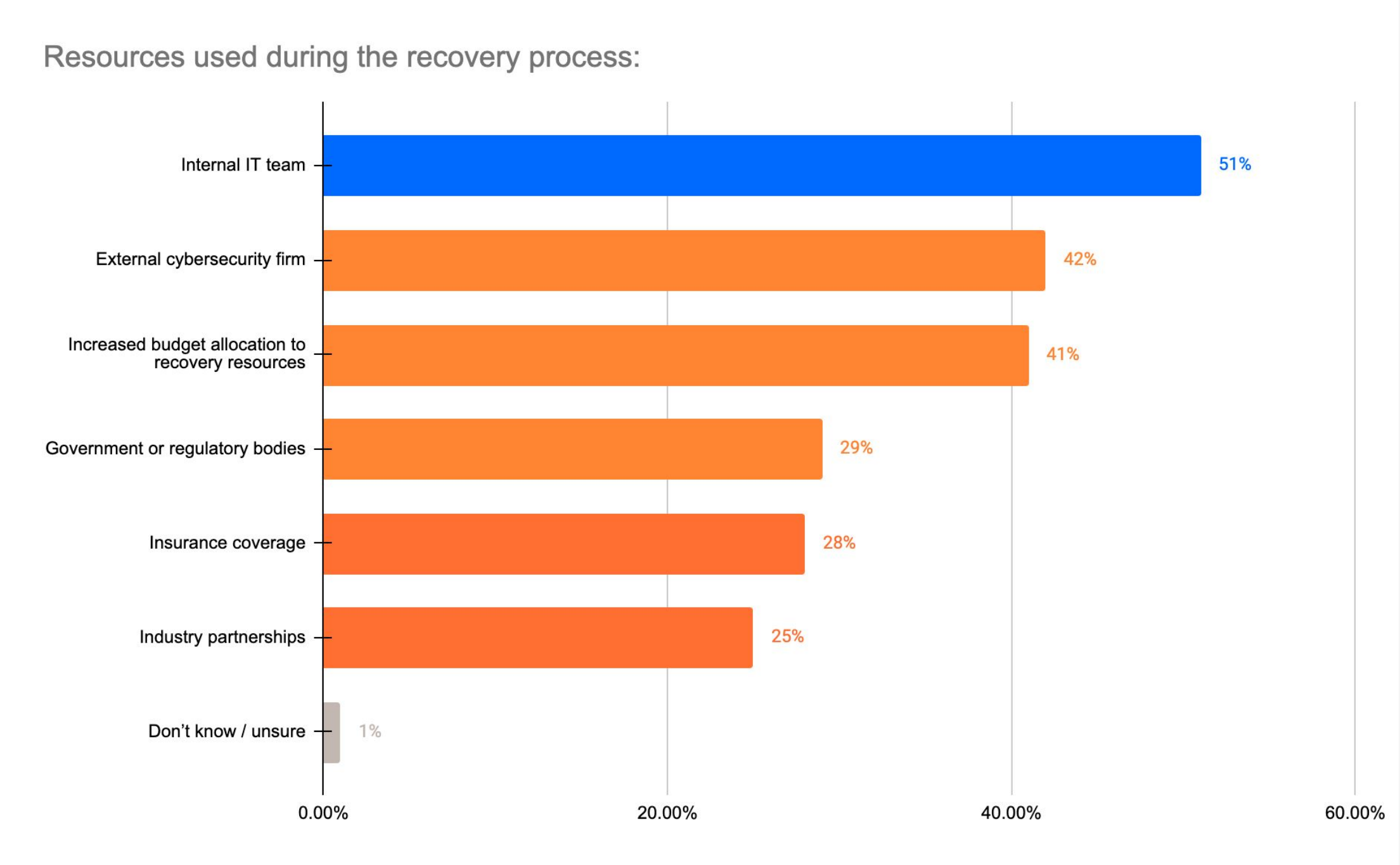
The most common steps businesses are taking to recover from security incidents are providing additional training to employees (40%) and implementing stronger security measures (39%)



Q18. What steps has your business taken to recover from the security incident? Select all that apply | Base: 192 *Only asked to those who have experienced a security incident in the last 12 months

Resources Used for Security Incident Recovery

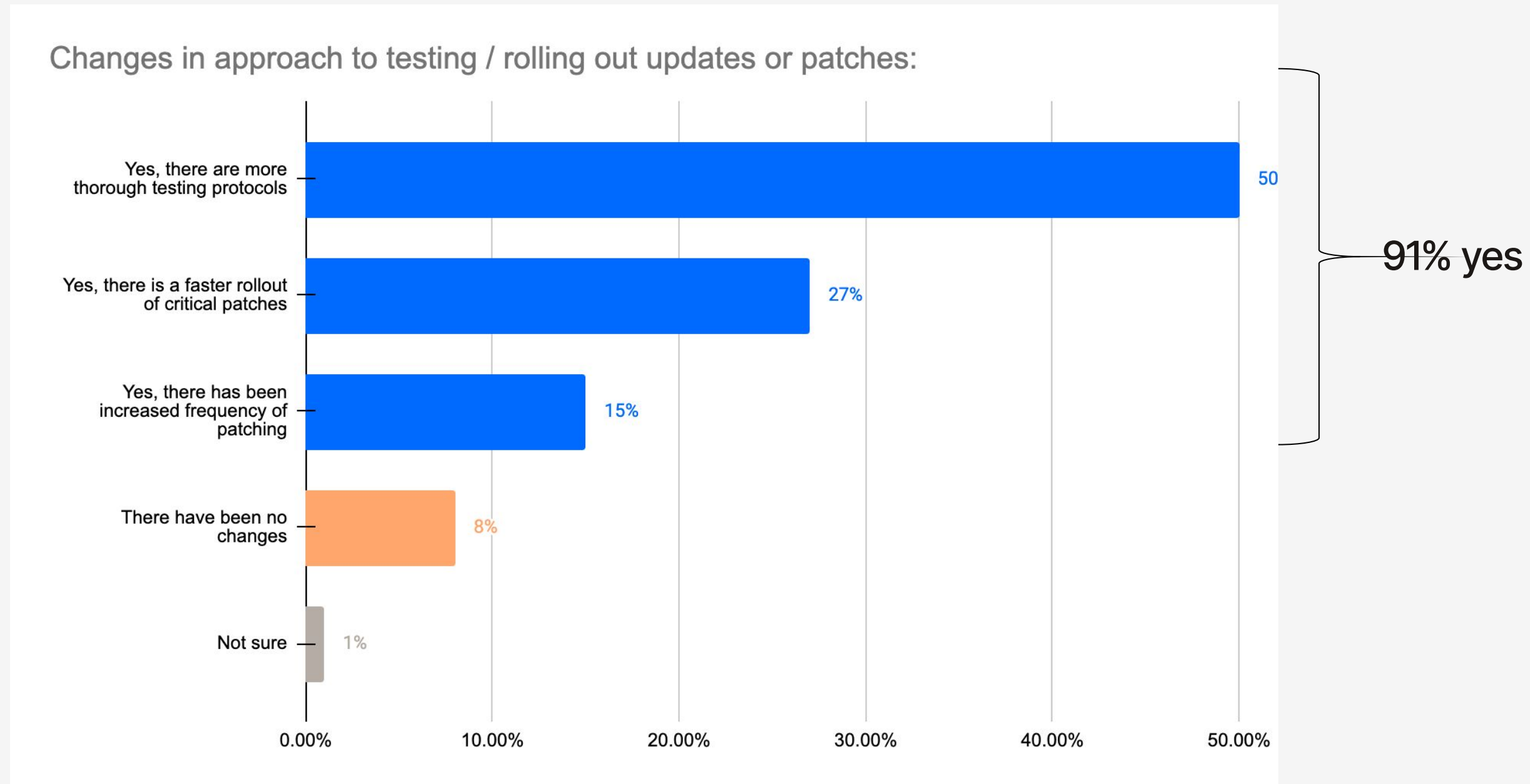
Most businesses are opting to use their internal IT team (51%) for recovery following a security incident



Q19. What resources did your business use for recovery? Select all that apply | Base: 191 (only asked to those who have taken step towards business recovery)

Changes in Approach to Updates and Patch Testing

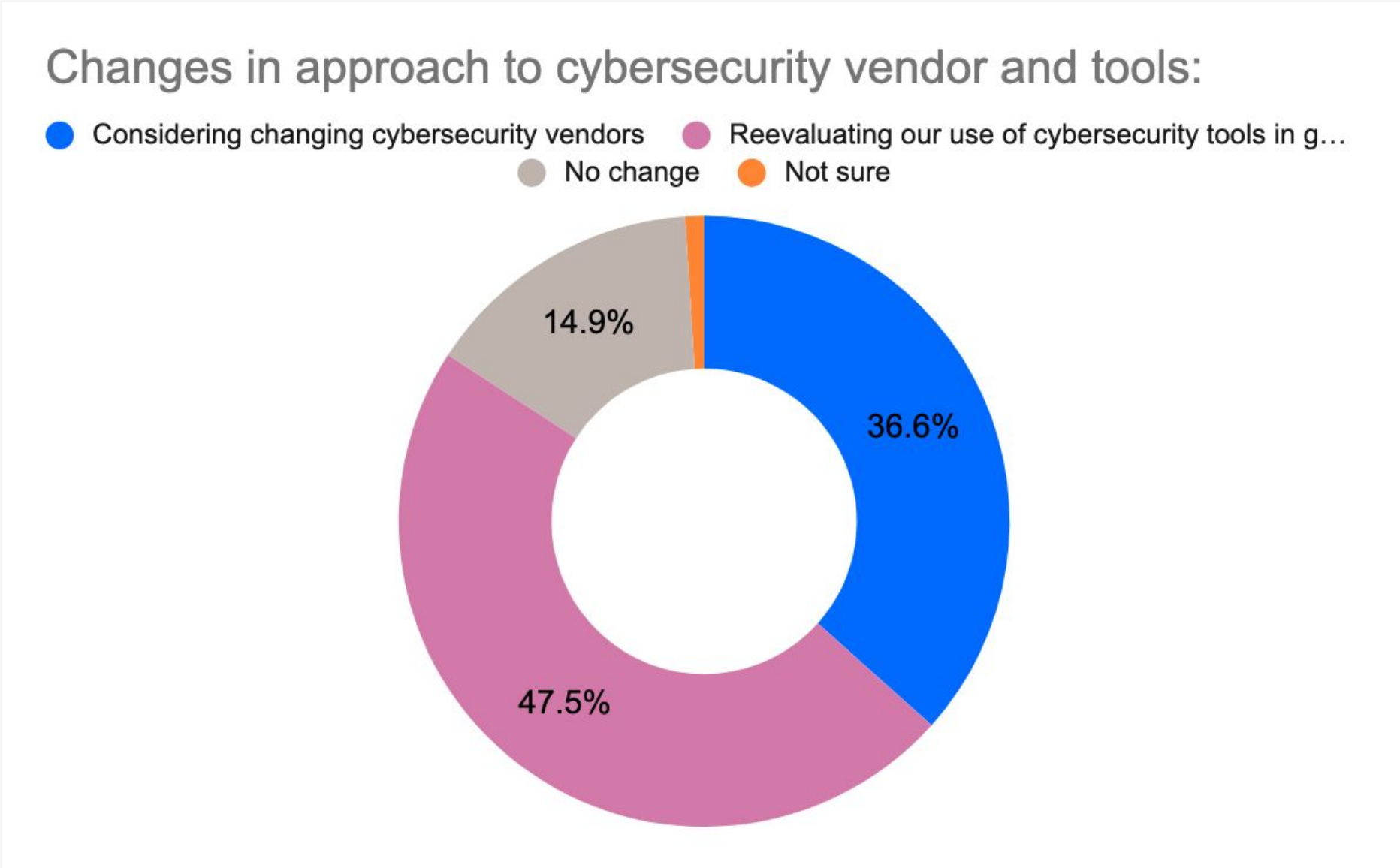
91% report that recent reliability incidents have encouraged their business to change their approach to testing or rolling out updates or patches



Q20. In response to recent reliability incidents like the CrowdStrike outage, has your business changed its approach to testing or rolling out updates or patches? Select one | Base: 200

Approach to Cybersecurity Vendors and Tools

48% are re-evaluating their use of cybersecurity tools in general, following the recent CrowdStrike outage, with a further 37% considering changing cybersecurity vendors

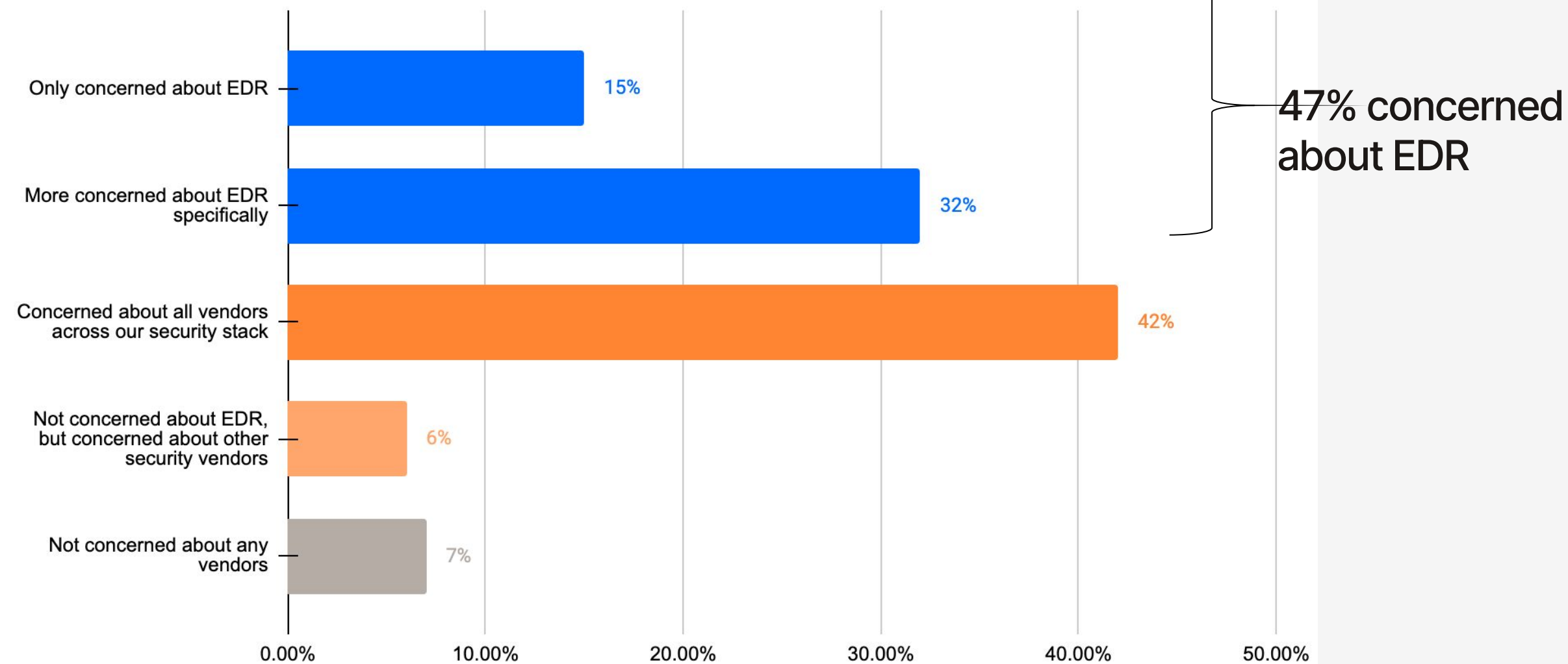


Q21. In response to recent reliability incidents like the CrowdStrike outage, has your business changed its approach to cybersecurity vendors and tools?
Select one | Base: 200

Concerns About Reliability in EDR Vendors

88% are concerned about the reliability and quality of their vendors, with a split between those concerned about all vendors in their security stack (42%) and those more concerned about EDR (47%)

Concern towards reliability and quality issues in EDR vendors compared to all cybersecurity vendors:



Q22a. In response to the CrowdStrike outage, to what extent are you concerned about reliability and software quality issues in EDR vendors vs all cybersecurity vendors? Select one | Base: 200

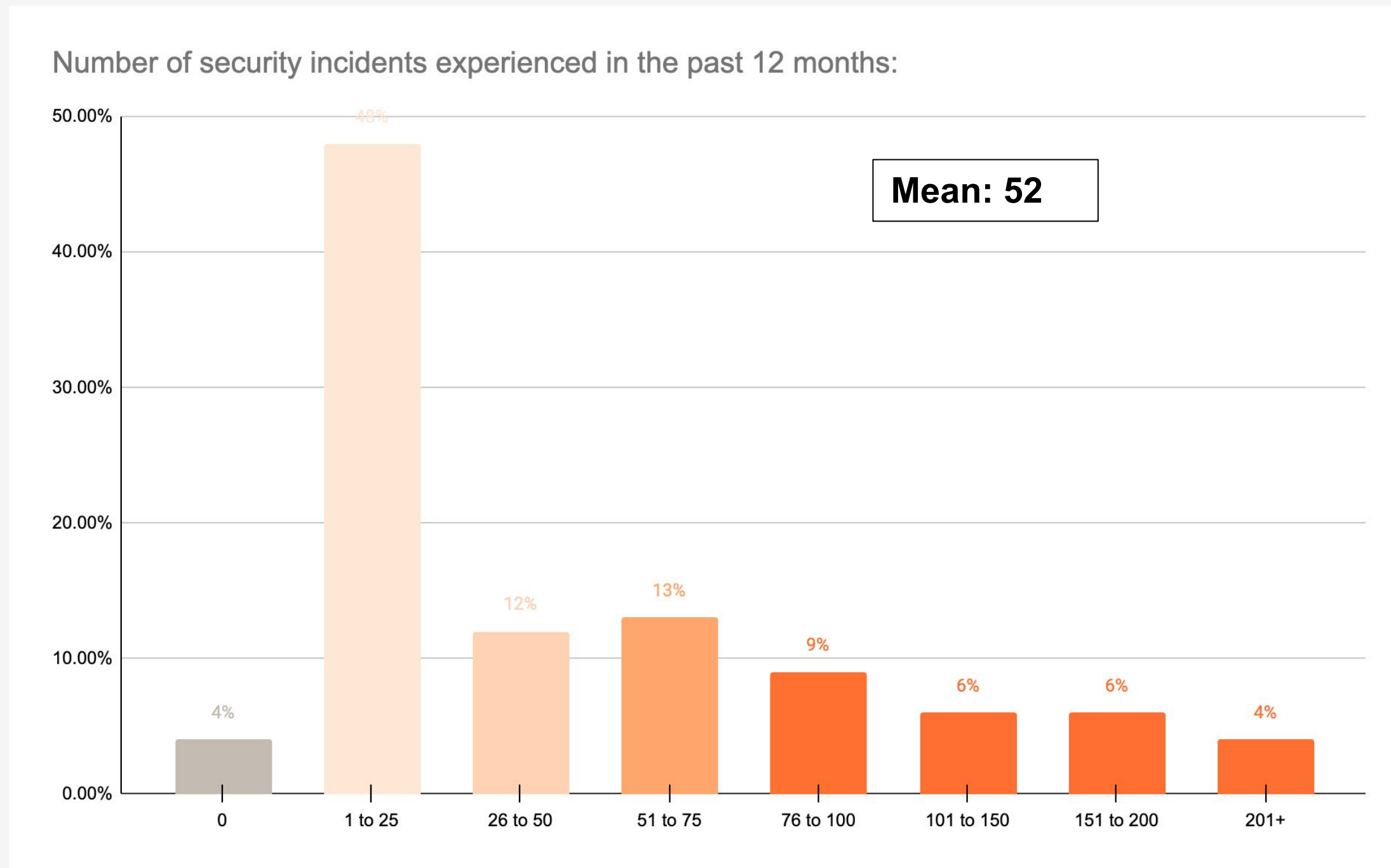


Main Findings

The attack landscape

Number of Security Incidents in the Past Year

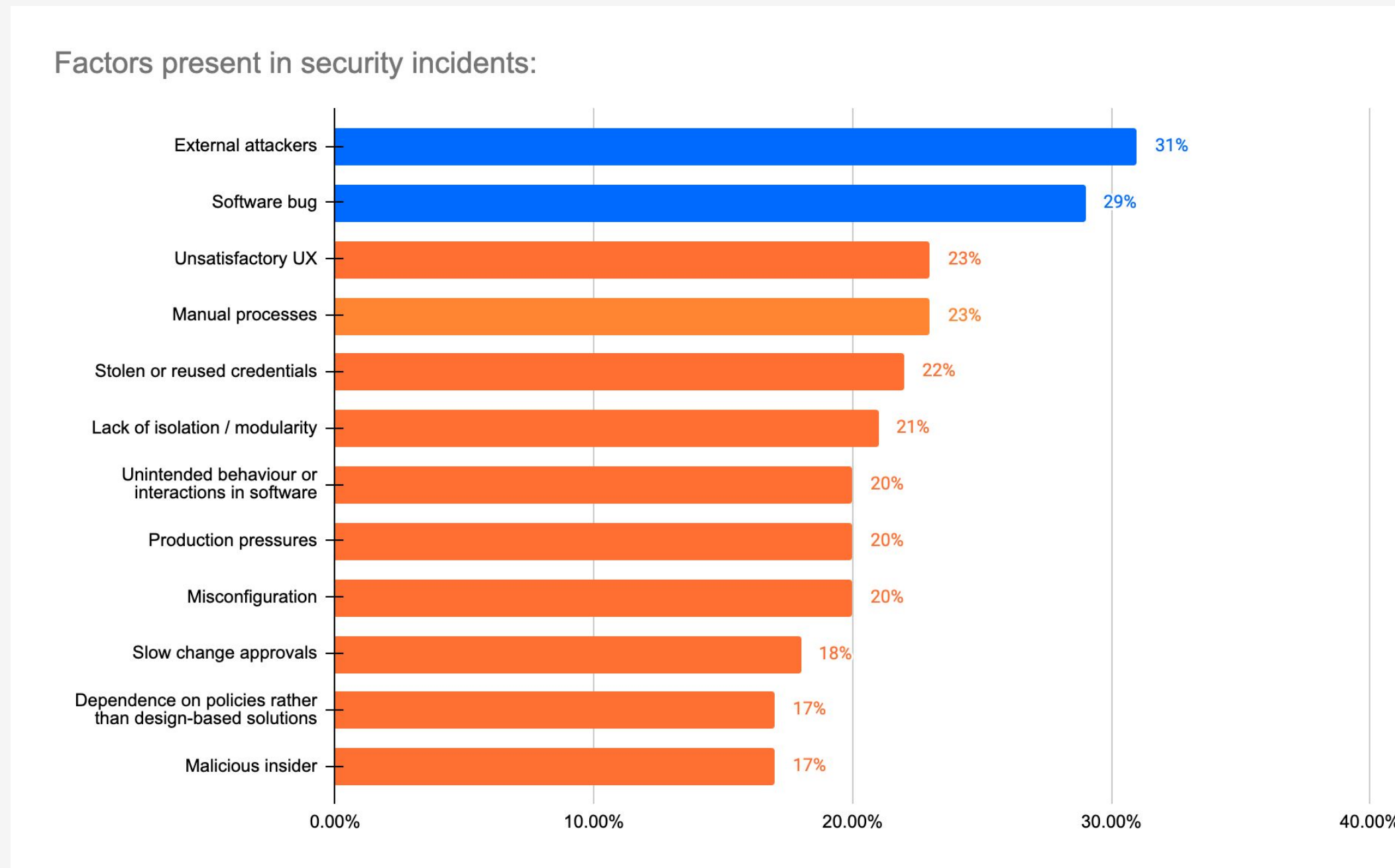
On average, businesses have experienced 52 security incidents in the past 12 months



Q15. How many security incidents, including those caused by human error, has your business experienced in the past 12 months? Select one | Base: 200

Factors Present in Security Incidents

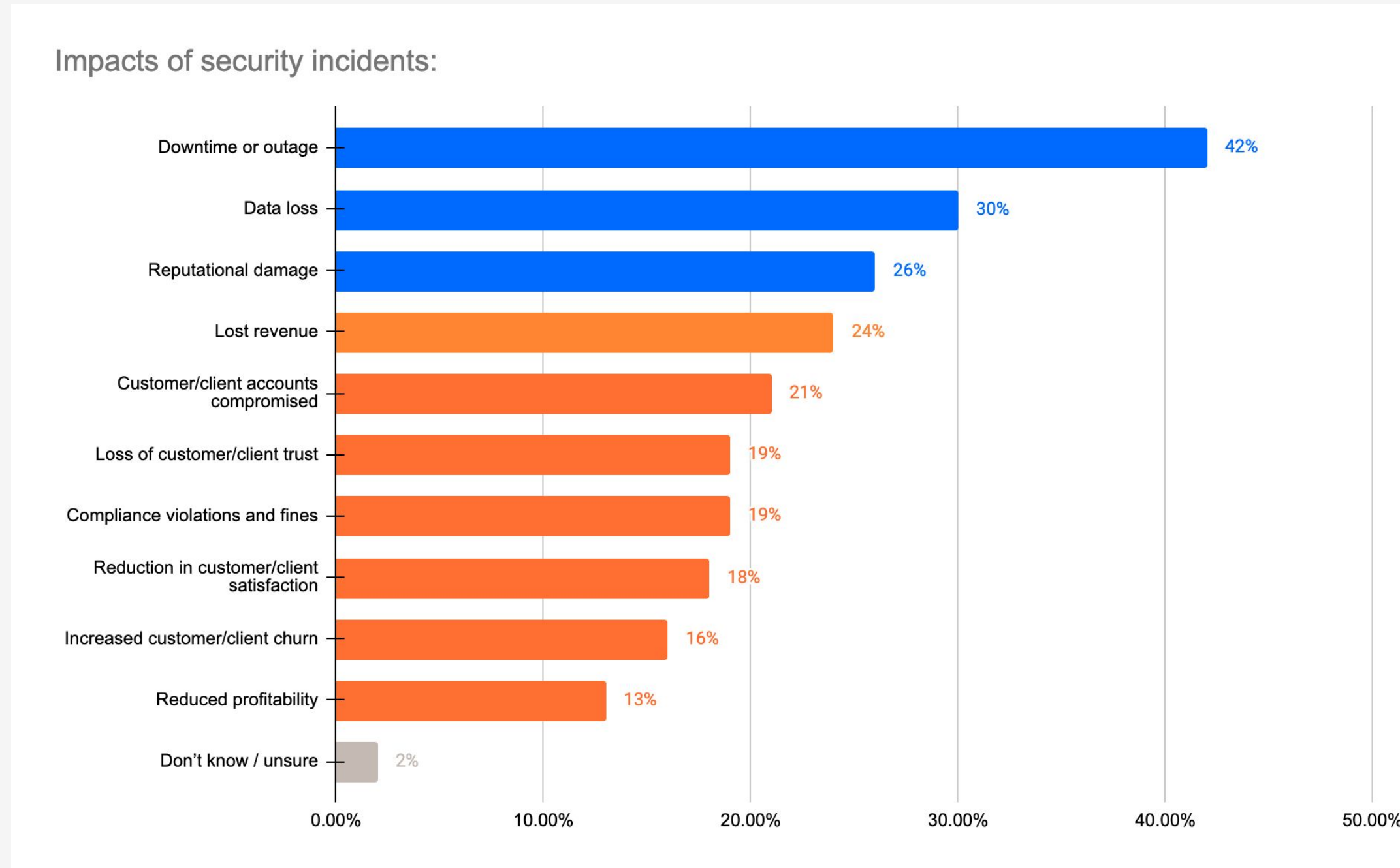
The top factors present in security incidents were external attackers (31%) and software bugs (29%)



Q16. Which of the following factors were present in the security incident? Select all that apply | Base: 192 *Only asked to those who have experienced a security incident in the last 12 months

Main Impacts of Security Incidents

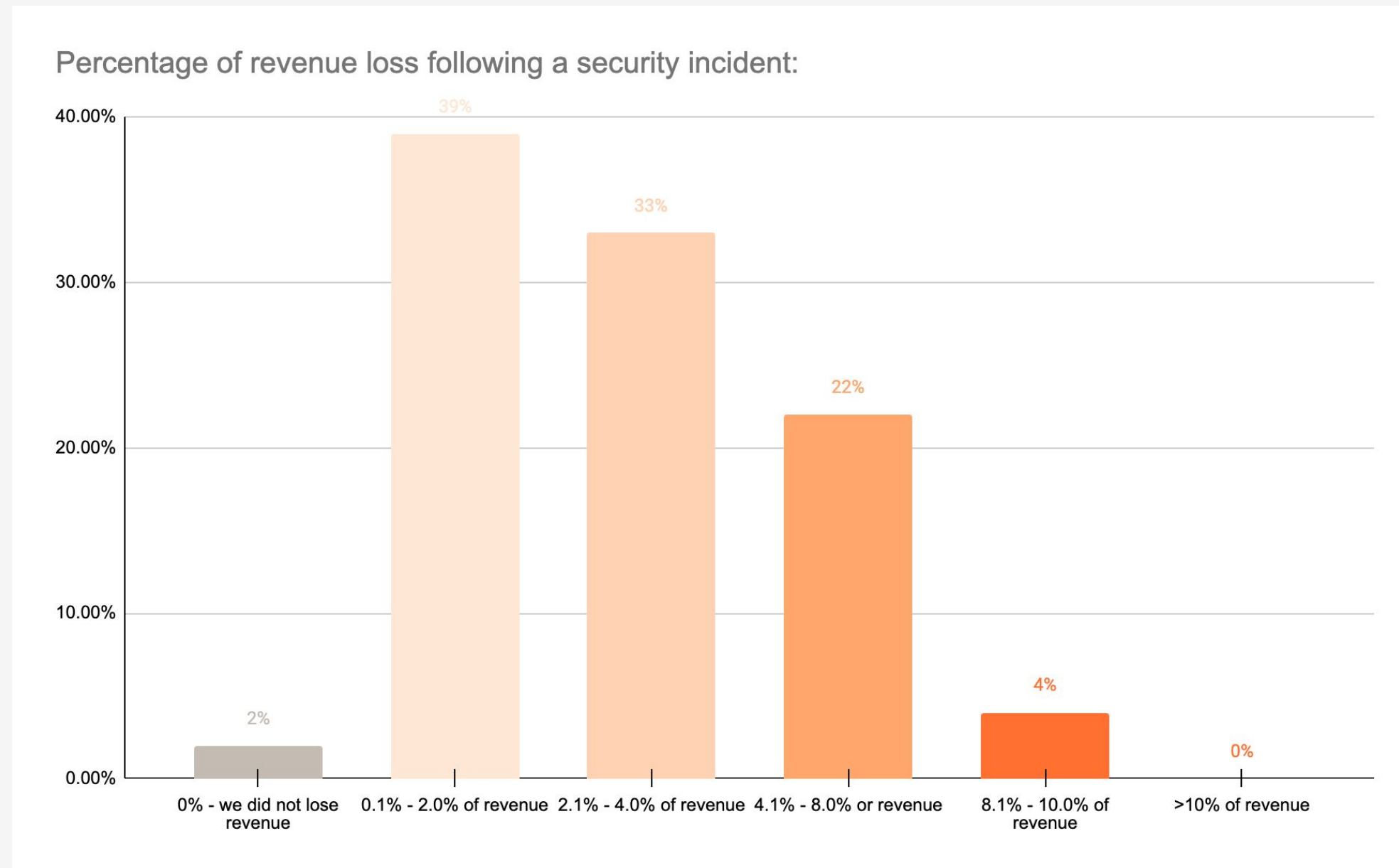
The top impacts of security incidents are downtime or outage (42%), data loss (30%) and reputational damage (26%)



Q17a. What were the main impacts of the security incident? Select top three | Base: 192 *Only asked to those who have experienced a security incident in the last 12 months

Revenue Loss from Security Incidents

Amongst those who report revenue loss as a top impact of security incidents, businesses report losing an average of 3.1% of their revenue

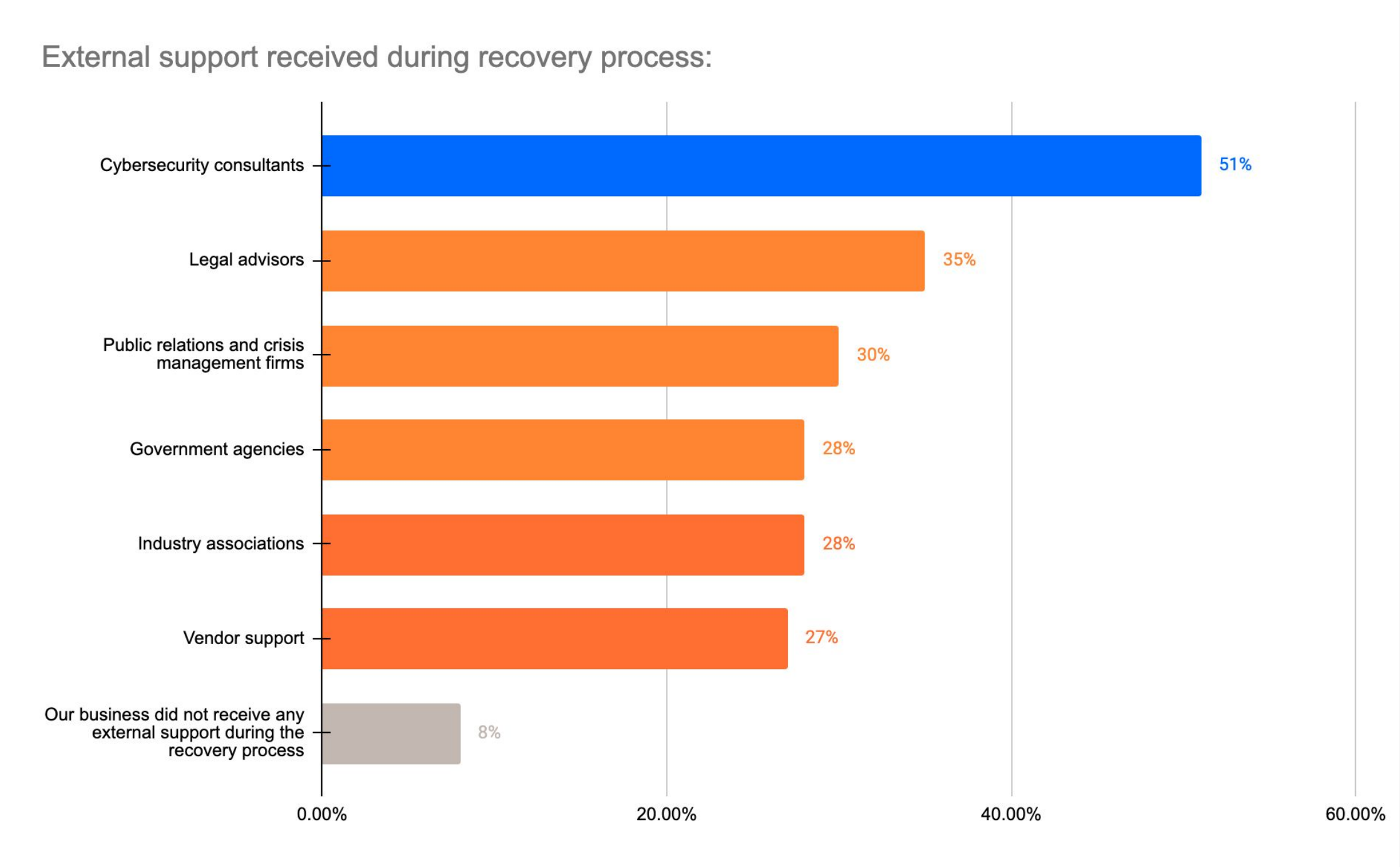


Mean: 3.1%

Q17b. Approximately what percentage of your revenue did you lose as a result of a security incident? Select one | Base: 46 *Only asked to those who lost revenue as a result of security incidents

External Support During Recovery

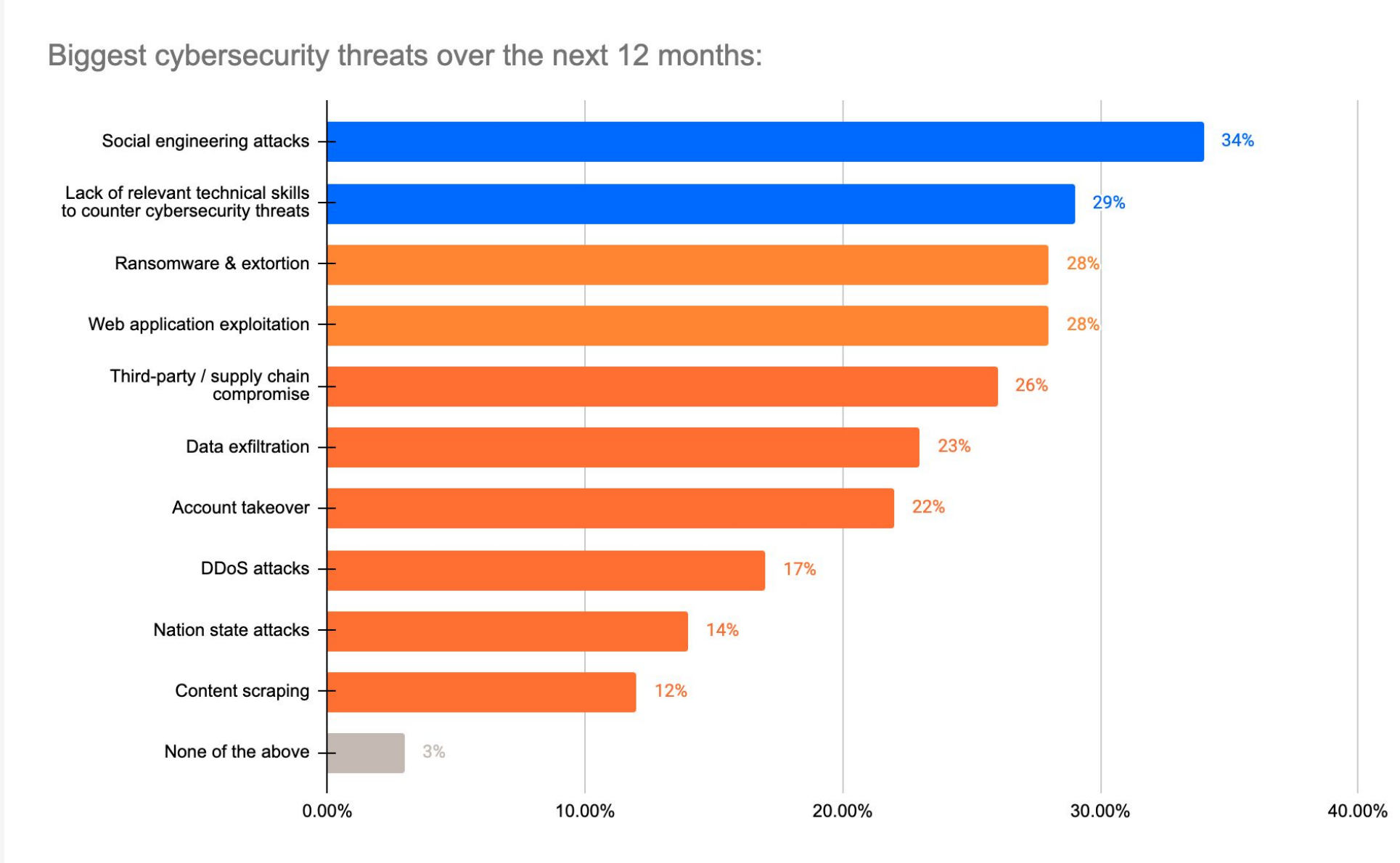
51% say their business utilised cybersecurity consultants during the recovery process



Q22b. What external support or assistance, if any, did your business receive during the recovery process? Select all that apply | Base: 200

Predicted Biggest Cybersecurity Threats

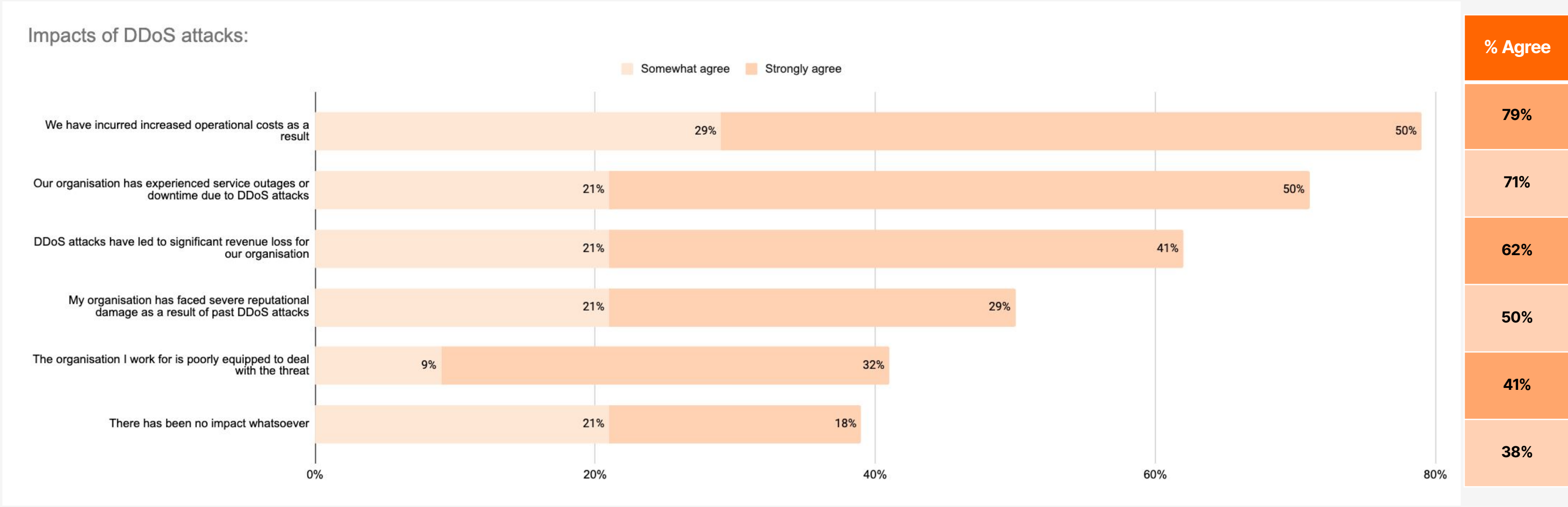
Organisations predict that social engineering attacks (34%) will be their biggest cybersecurity threat in the next 12 months, followed by a lack of relevant technical skills (29%)



Q1a. What do you predict will be the biggest cybersecurity threat to your organisation over the next 12 months? Select top three | Base: 200

Impacts of DDoS Attacks

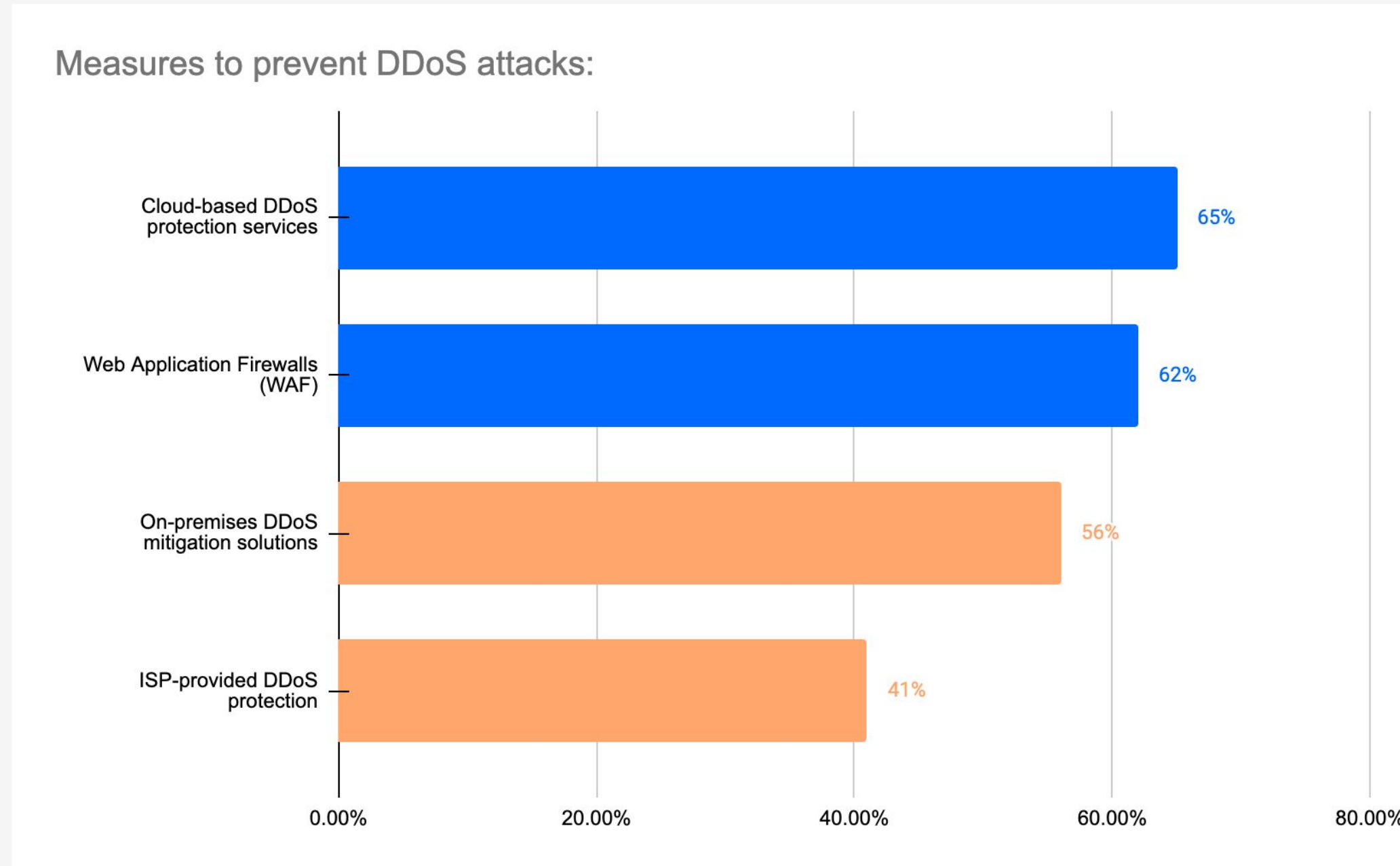
Decision makers who think DDoS attacks will be one of the biggest threats over the next 12 months are likely driven by the significant negative impacts of DDoS attacks, with 79% saying they result in increased operational cost



Q1b. To what extent do you agree or disagree with the following statements? | Base: 34 *Only asked to those who believe DDoS attacks are a threat

DDoS Protection Measures

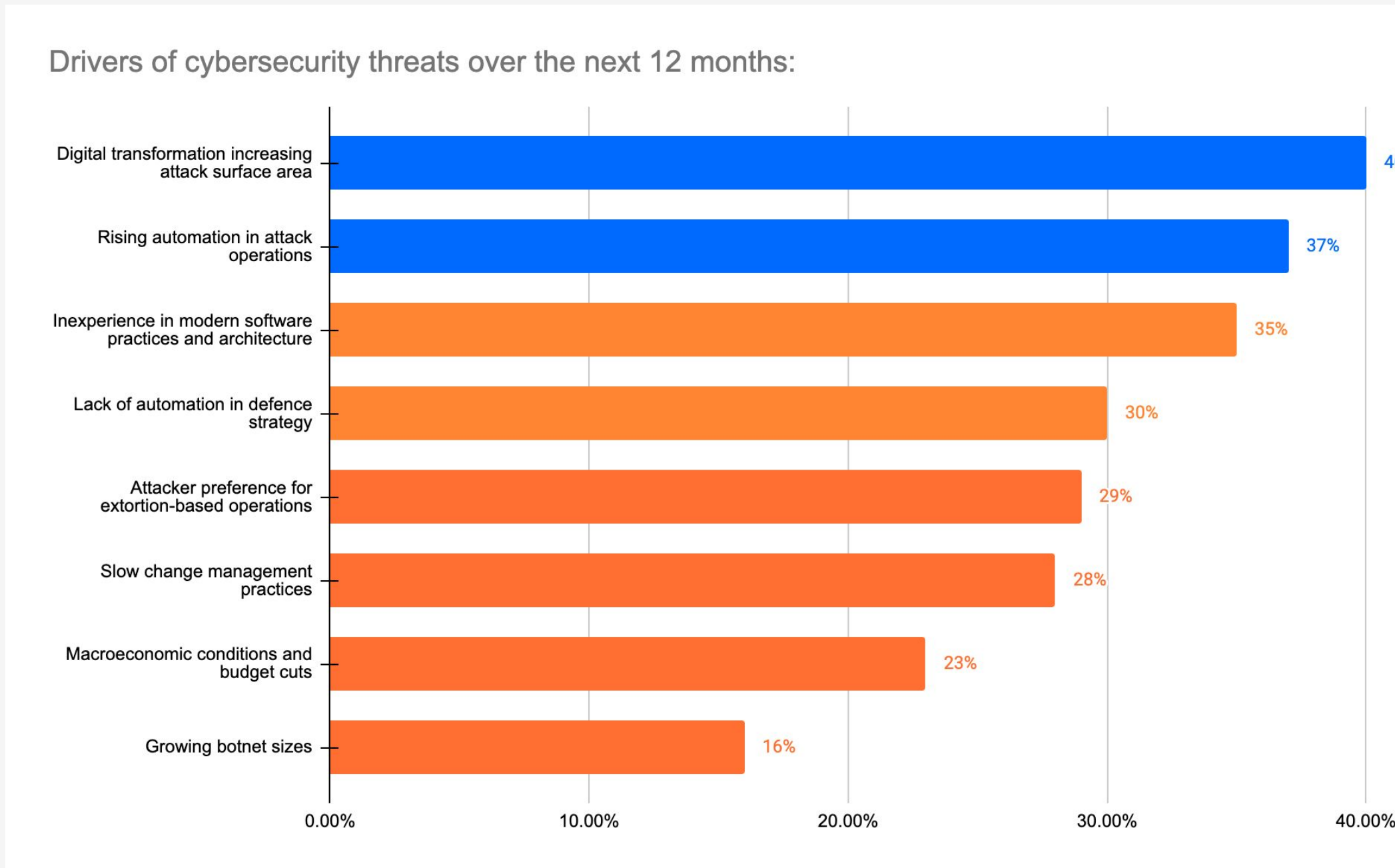
Organisations are most commonly using cloud-based DDoS protection services (65%) and WAF (62%) to combat DDoS attacks



Q1c. What measures does your organisation currently use for DDoS protection? Select all that apply | Base: 34 *Only asked to those who believe DDoS attacks are a threat

Drivers of Future Cybersecurity Threats

Looking ahead, decision makers believe that digital transformation increasing the attack surface area (40%) and rising automation in attack operations (37%) will be the biggest drivers of cybersecurity threats

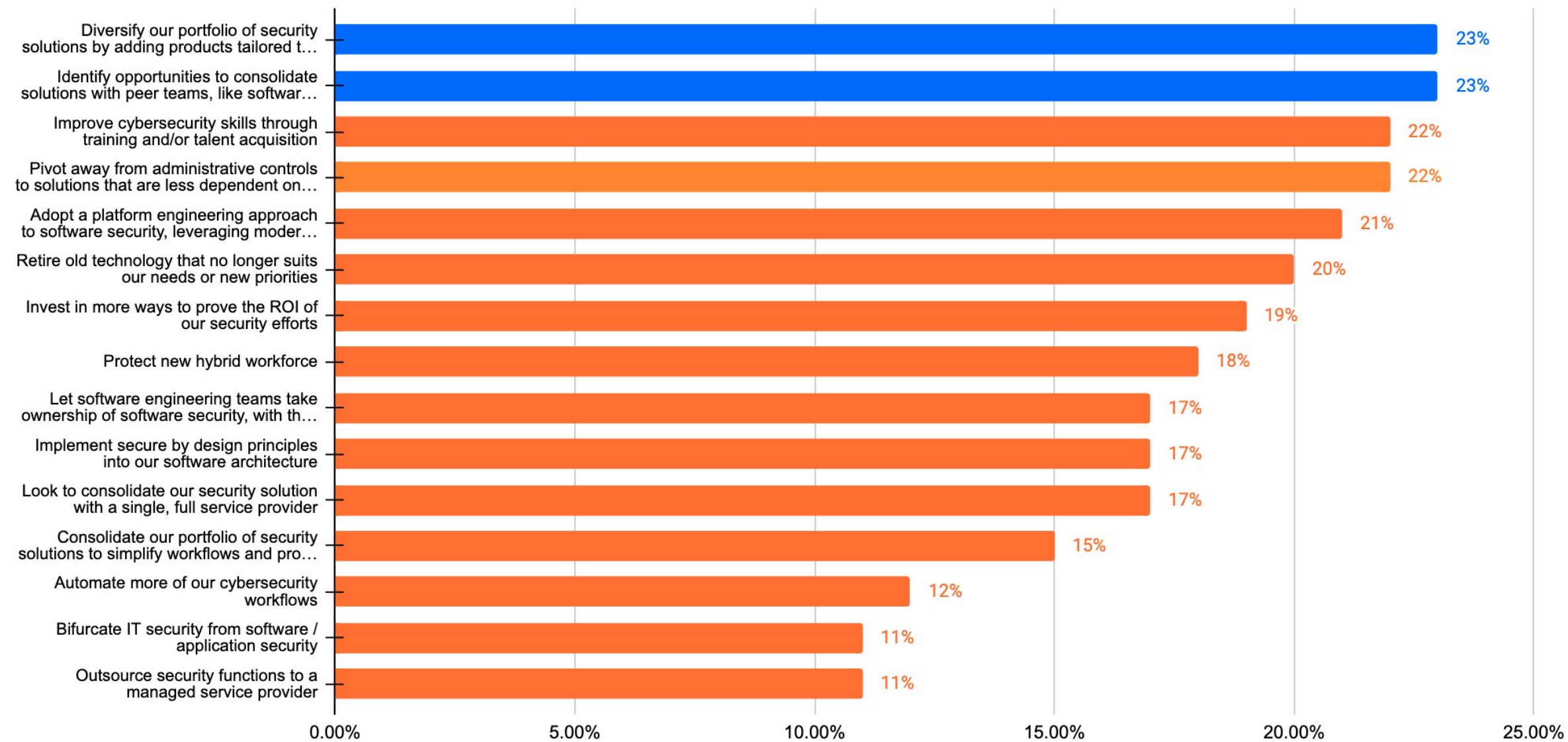


Q3. Which of the following do you predict will drive cybersecurity threats to your business over the next 12 months? Select top three | Base: 34

Security Priorities for the Next Year

Organisations' top security priorities for the next year revolve around diversifying security solutions (23%) and identifying opportunities to consolidate solutions with peer teams (23%)

Top security priorities over the next year:



Q14. What are your organisation's security priorities over the next year? Select top three | Base: 200

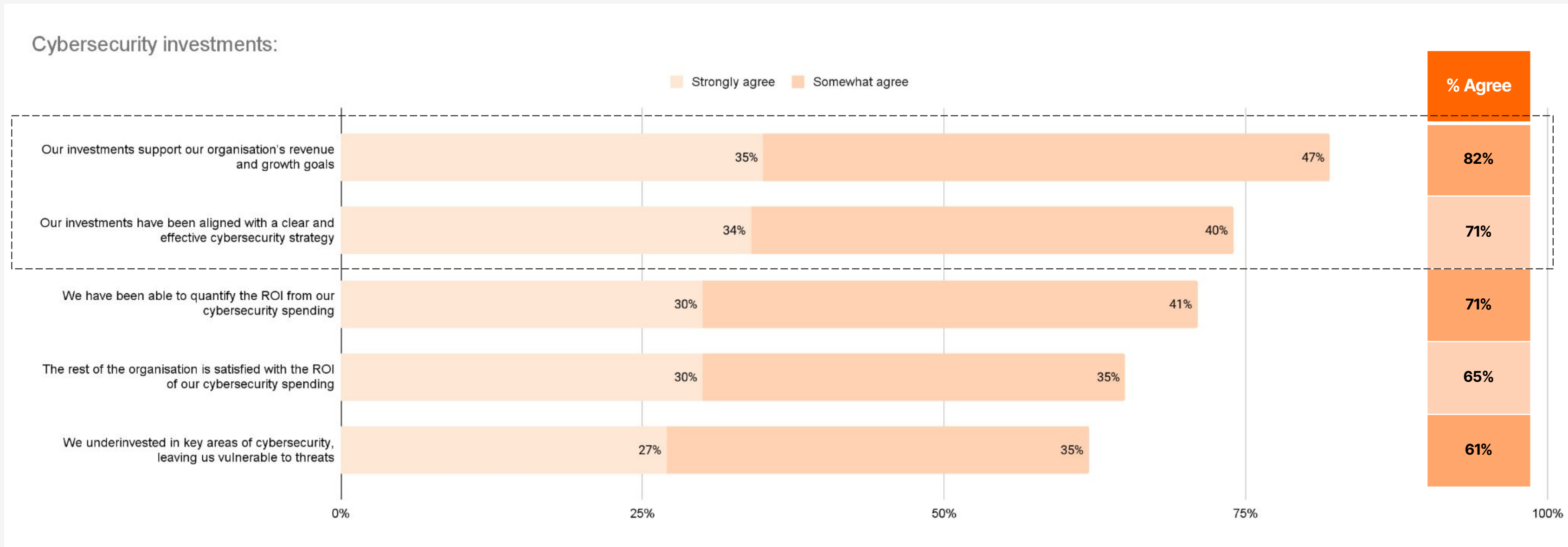


Main Findings

Is cybersecurity spending
falling behind?

Investment in Cybersecurity

82% agree that their investments in cybersecurity support their organisation's revenue and growth goals, with a further 74% agreeing that these investments are aligned with a clear and effective cybersecurity strategy...

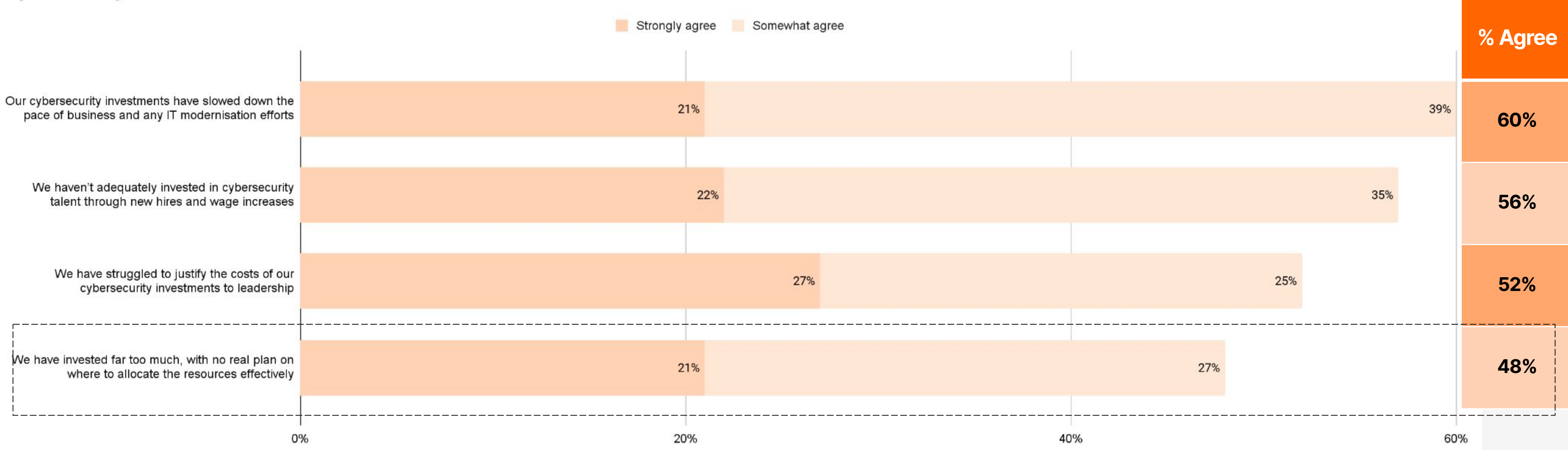


Q6j. Thinking about the investment you made to prepare for cybersecurity risk over the past 12 months, to what extent do you agree or disagree with the following statements? | Base: 200

Investment in Cybersecurity

...furthermore, just 48% agree that they have invested too much, with no real plan on where to allocate the resources effectively, demonstrating that organisations are actively preparing for future cybersecurity risks

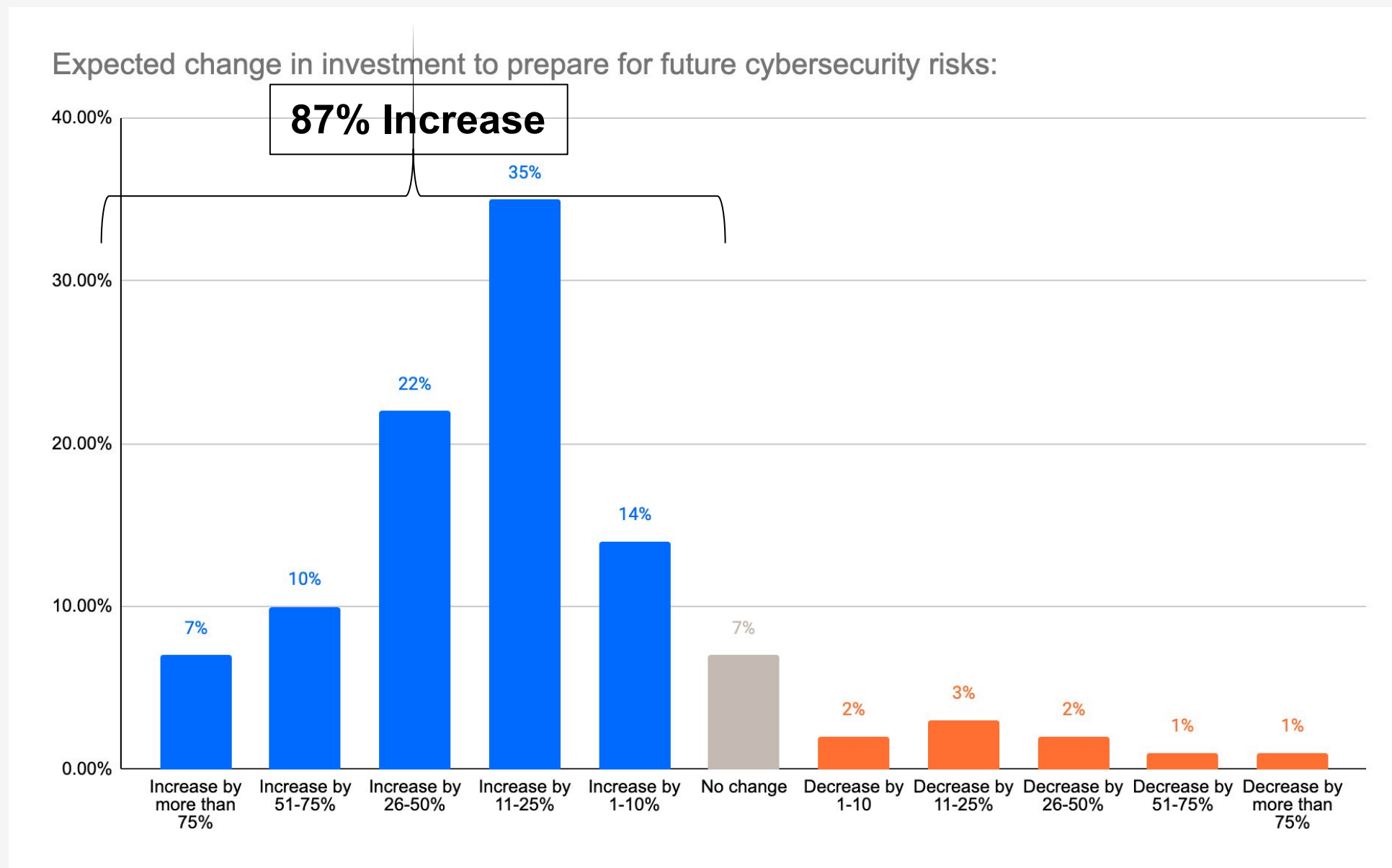
Cybersecurity investments:



Q6j. Thinking about the investment you made to prepare for cybersecurity risk over the past 12 months, to what extent do you agree or disagree with the following statements? | Base: 200

Future Cybersecurity Investment Changes

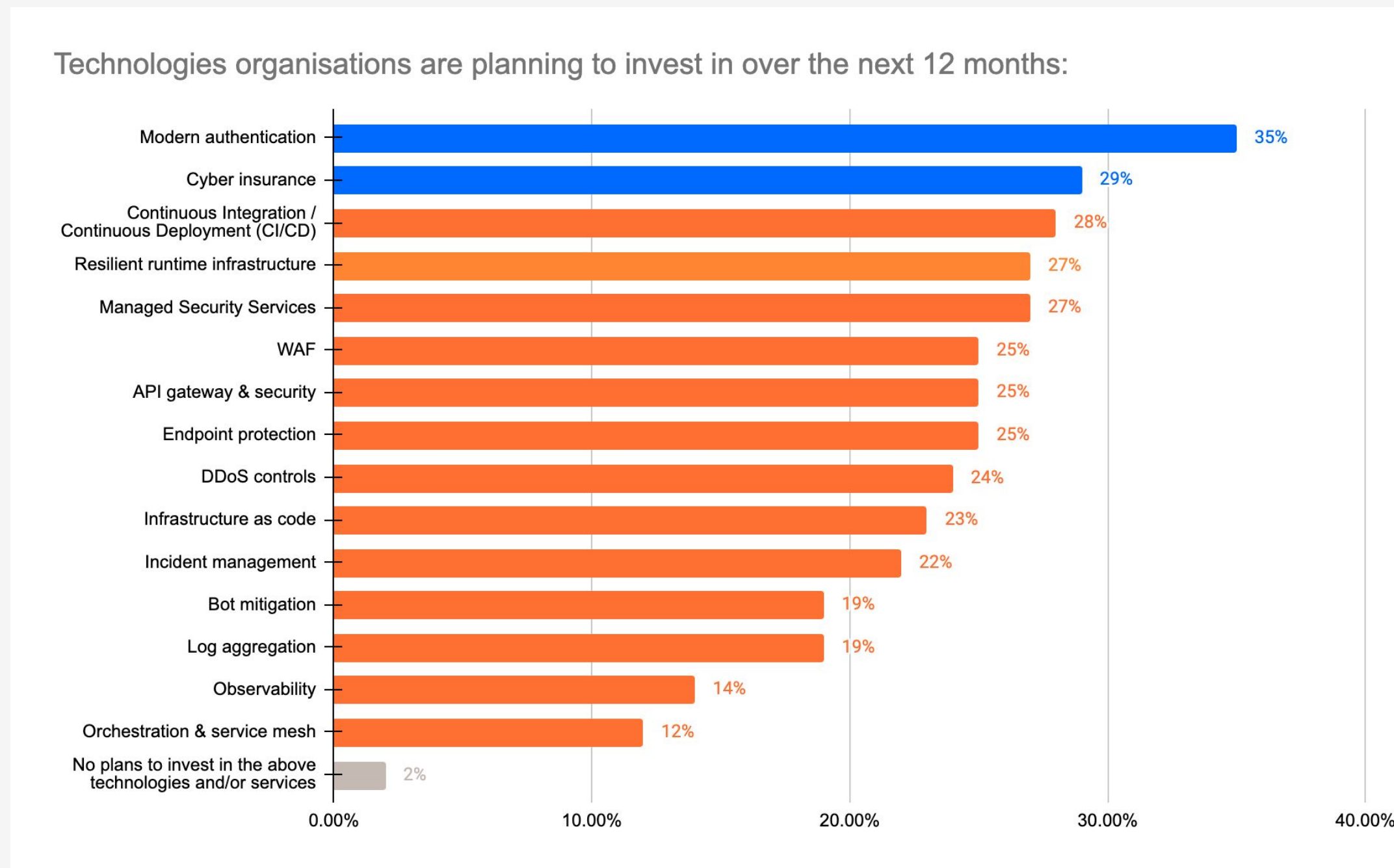
87% of decision makers are expecting their organisation's investment to **increase** to prepare for future cybersecurity risks over the coming 12 months



Q5. How do you expect your organisation's investment to prepare for future cybersecurity risks to change over the next 12 months? Select one | Base: 200

Planned Investments in Cybersecurity Technologies

Almost all organisations have plans to invest in technologies over the next 12 months, particularly modern authentication (35%) and cyber insurance (29%)



Q4. Which technologies and/or services does your organisation plan to invest in over the next 12 months? Select all that apply | Base: 200

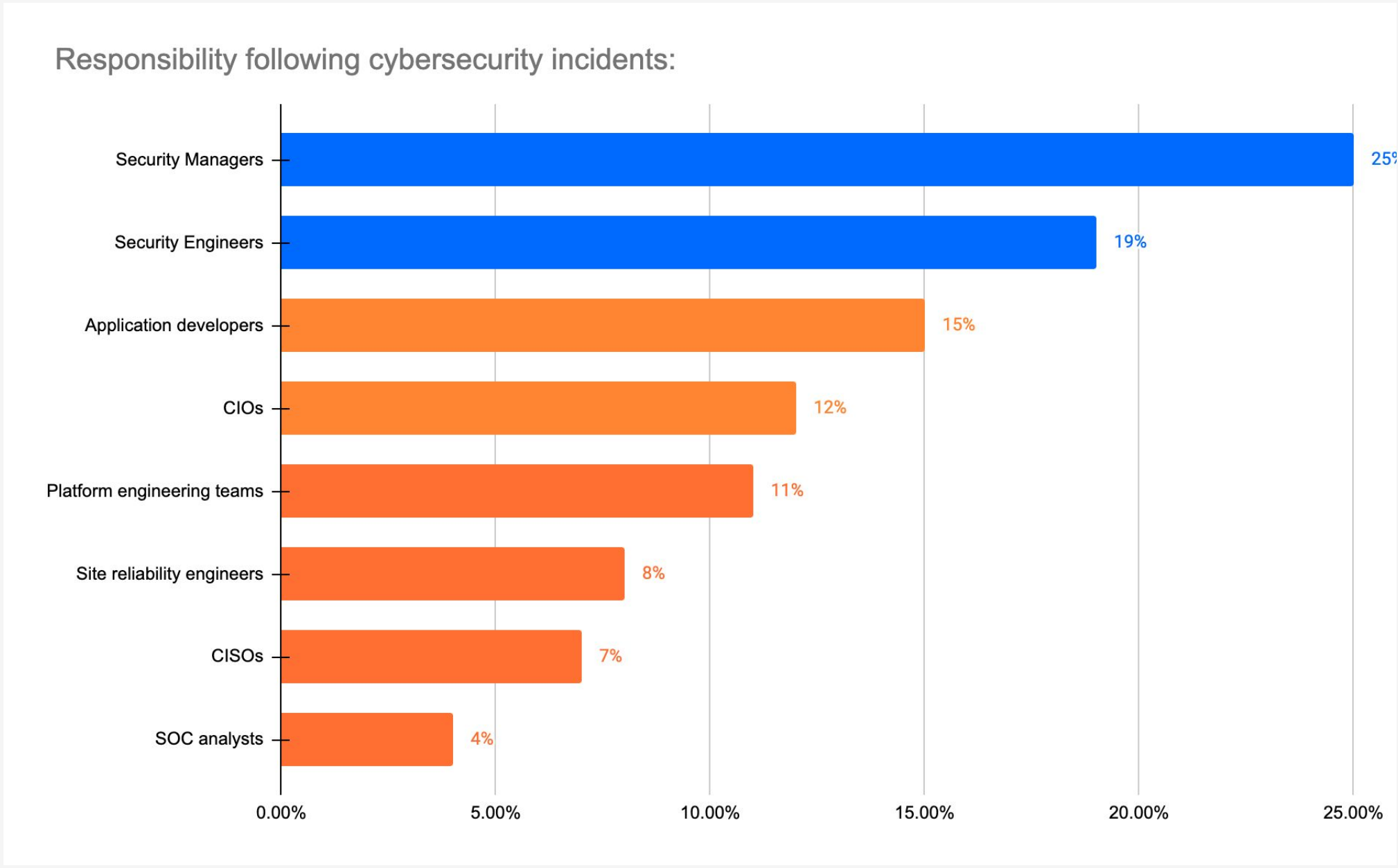


Main Findings

Shifting accountability

Responsibility During Cybersecurity Incidents

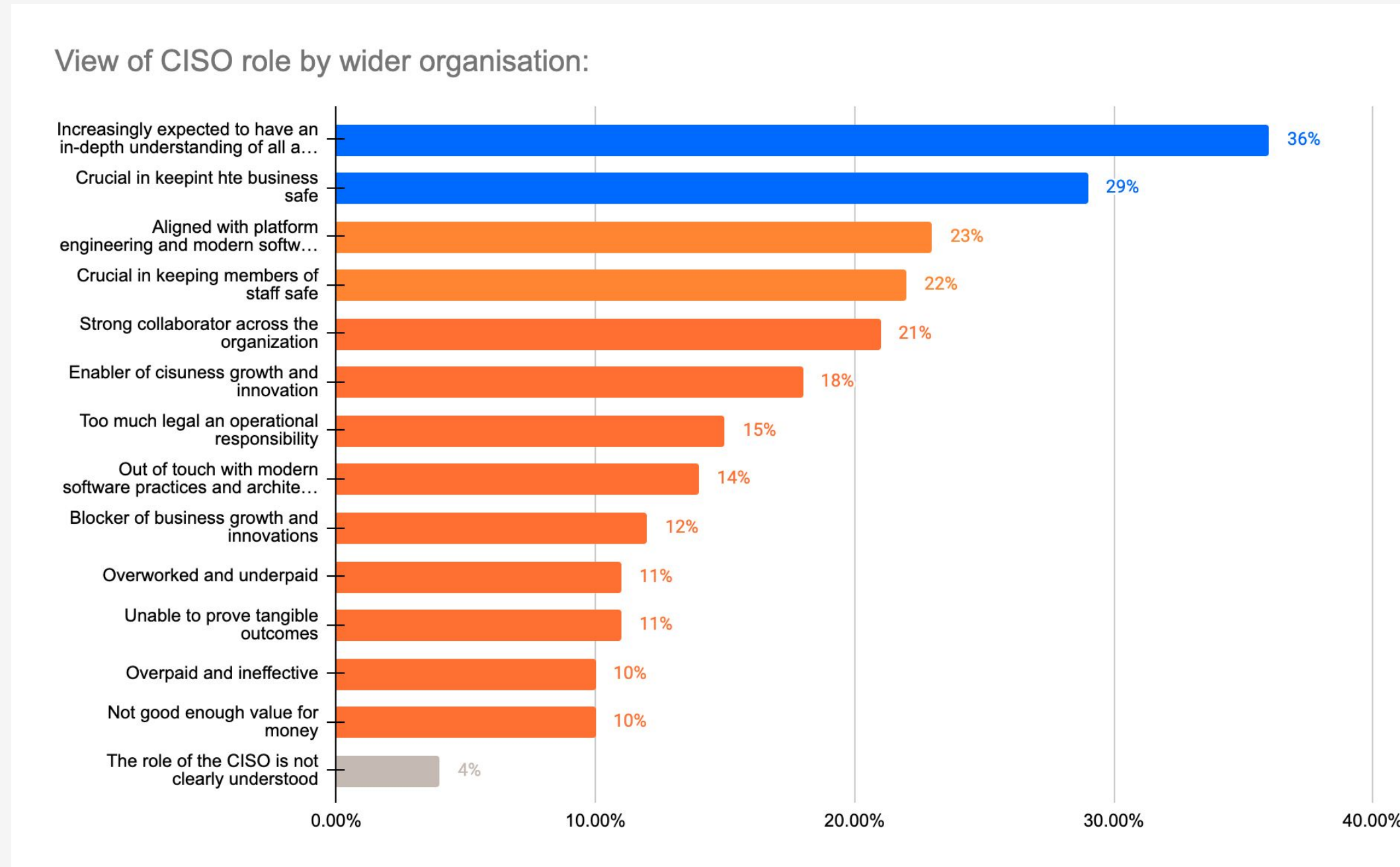
There is a wide spread of responsibility when it comes to security incidents, however, Security Managers (25%) and Engineers (19%) are most often held responsible for cybersecurity incidents



Q9. Who do you feel is most often held responsible for cybersecurity incidents in your organisation? Select one | Base: 200

Perception of CISO Role

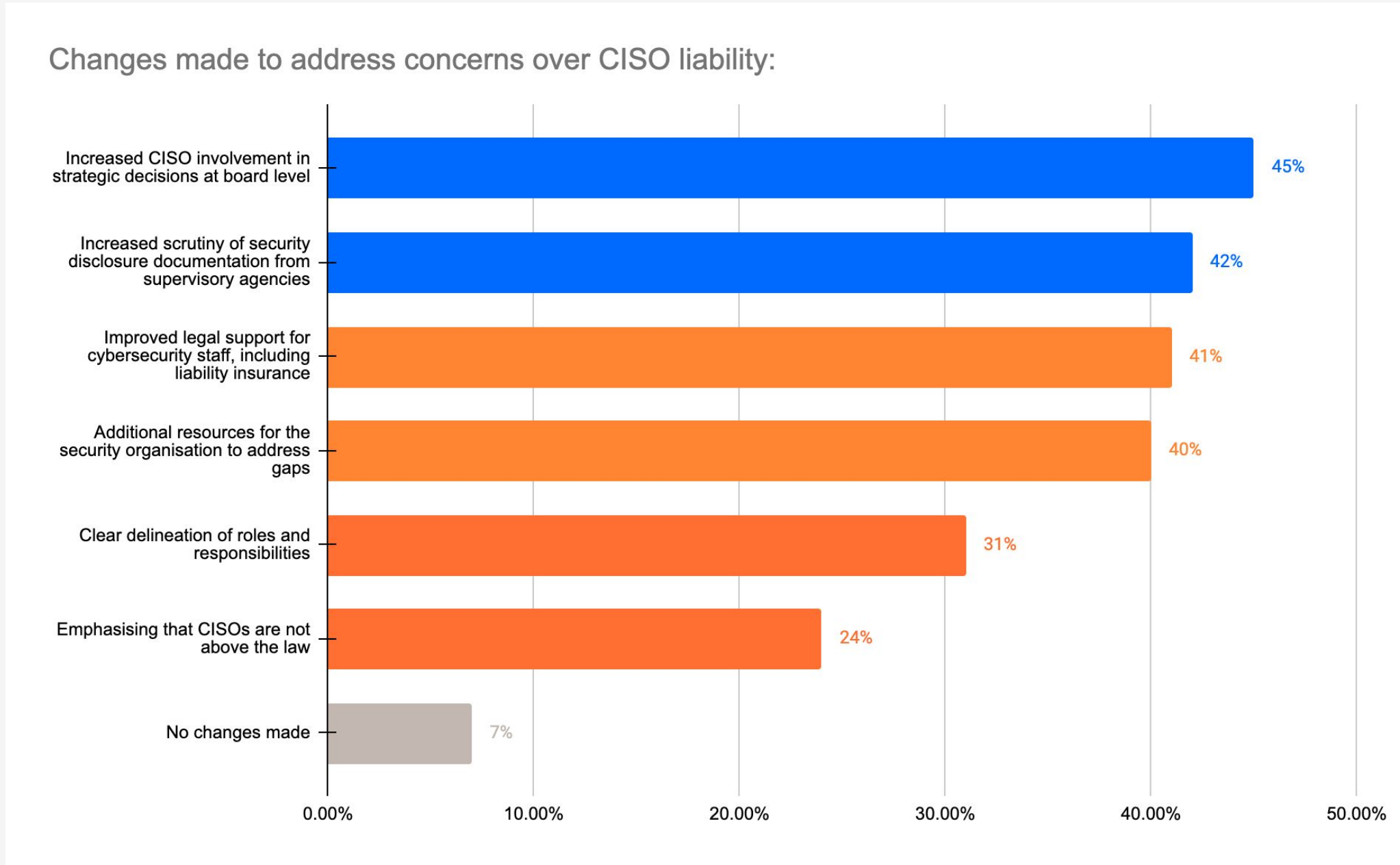
Decision makers feel that the role of CISO is increasingly expected to have an in-depth understanding of all areas of IT (36%) and are viewed as crucial in keeping the business safe (31%)



Q10. How do you think the role of the CISO is viewed by your wider organisation? Select top three | Base: 200

Changes to Address CISO Liability

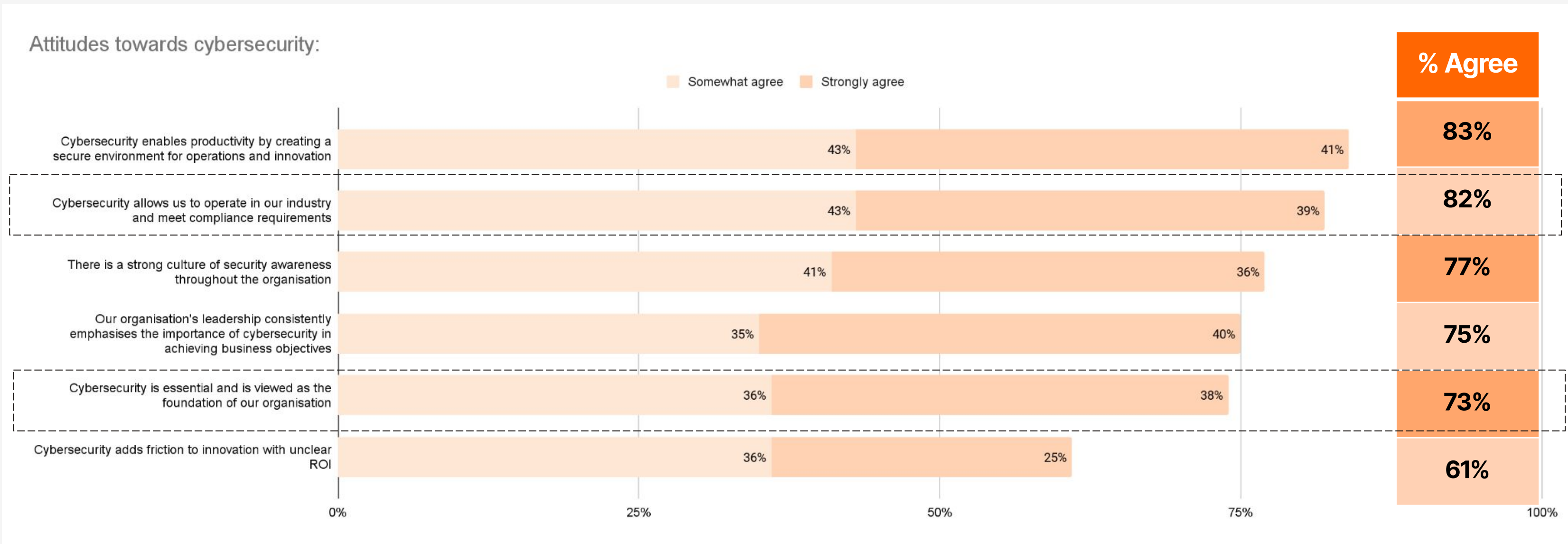
Businesses are actively addressing concerns regarding CISO liability, with 45% increasing CISO involvement in strategic decisions and a further 42% increasing the scrutiny of security disclosure documentation from supervisory agencies



Q12. What changes has your company made to address concerns regarding CISO liability? Select all that apply | Base: 200

Perception of Value of Cybersecurity

There is a strong consensus on the essential nature of cybersecurity (75%), particularly when it comes to meeting compliance requirements (82%)...

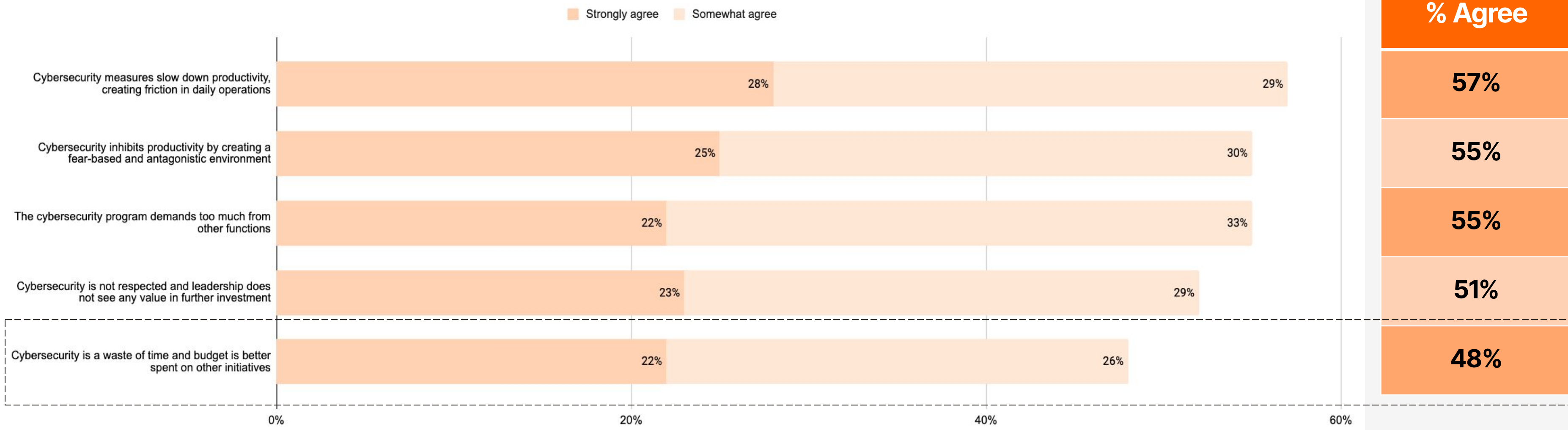


Q11. Thinking about the perception of the value of cybersecurity in your organisation, to what extent do you agree or disagree with the following statements?
 | Base: 200

Perception of Value of Cybersecurity

...this is further illustrated by only 48% agreeing that cybersecurity is a waste of time, and that budget would be better spent elsewhere

Attitudes towards cybersecurity:

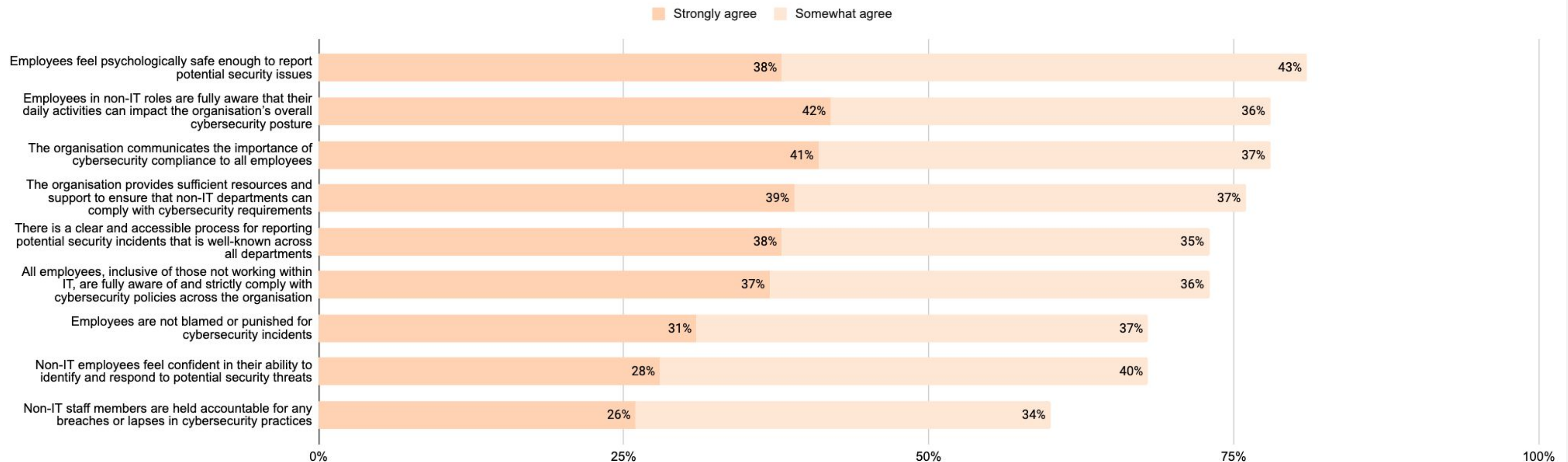


Q11. Thinking about the perception of the value of cybersecurity in your organisation, to what extent do you agree or disagree with the following statements?
| Base: 200

Cybersecurity Policies

73% of businesses have a strong culture of compliance with cybersecurity policies across all departments, facilitated by effective communication of the importance of security (78%)

Cybersecurity policies across the business:



Q13. Thinking about how well cybersecurity policies are followed by all employees, including those in non-IT departments, to what extent do you agree with the following statements? | Base: 200

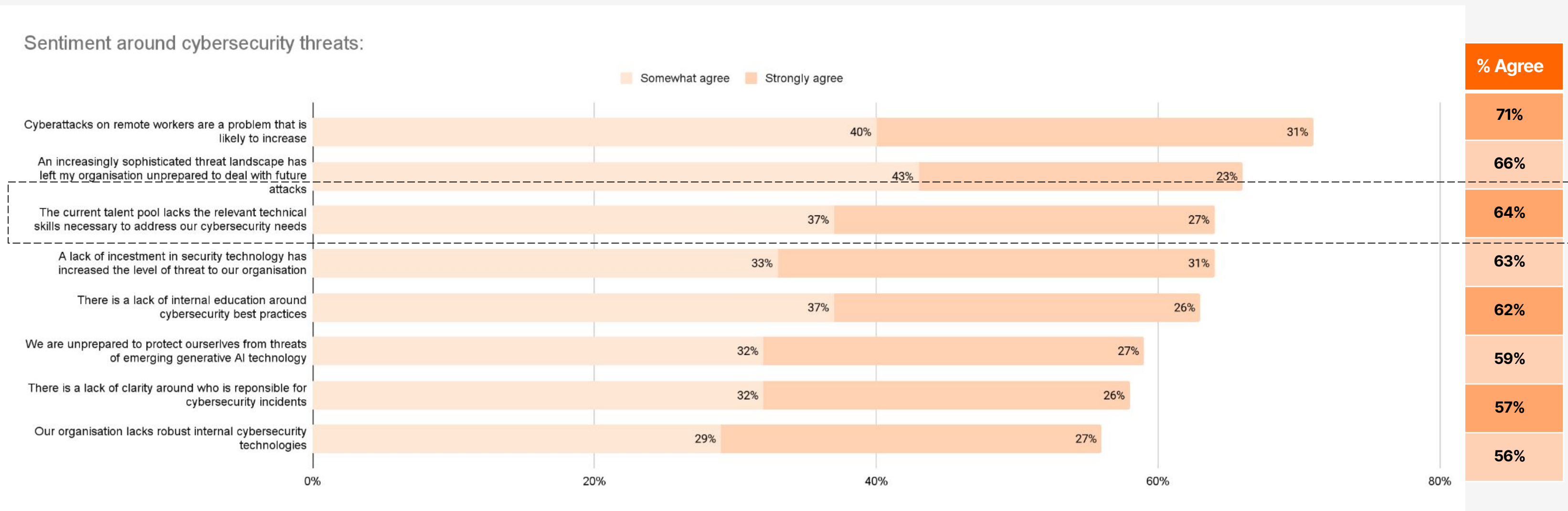


Main Findings

The cybersecurity talent pool

Cybersecurity Threats

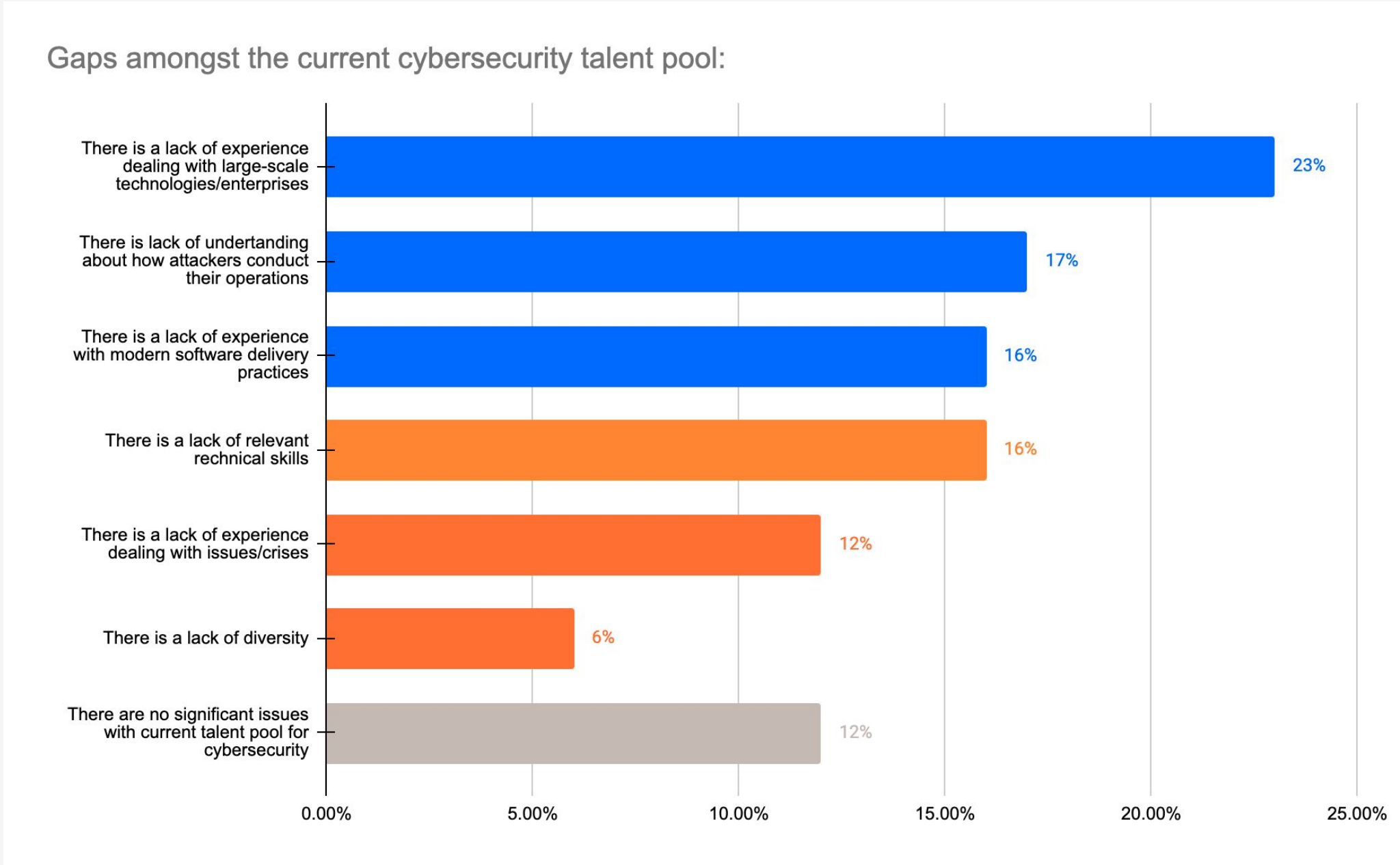
There are rising concerns over cyberattacks on remote workers (**71%**), an issue businesses may not be prepared for as **64%** of cybersecurity decision makers think that the **current talent pool lacks the relevant technical skills to address their needs**



Q2. Thinking about cybersecurity threats to your organisation, to what extent do you agree with the following statements? | Base: 200

Gaps in Cybersecurity Talent Pool

At an overall level, the gaps in the talent pool are multifaceted with there being no clear driver - however, the majority (88%) agree there are issues...



Q8. Where do you feel there are gaps amongst the current talent pool when it comes to cybersecurity? Select one | Base: 200



Main Findings

Annual Spending on Web Application / API Security

On average, businesses spend \$1,541,462 annually on web application and API security controls / tools, with businesses reporting reliance upon an average of 7 cybersecurity solutions



Average amount spent annually on web application and API security controls / tools

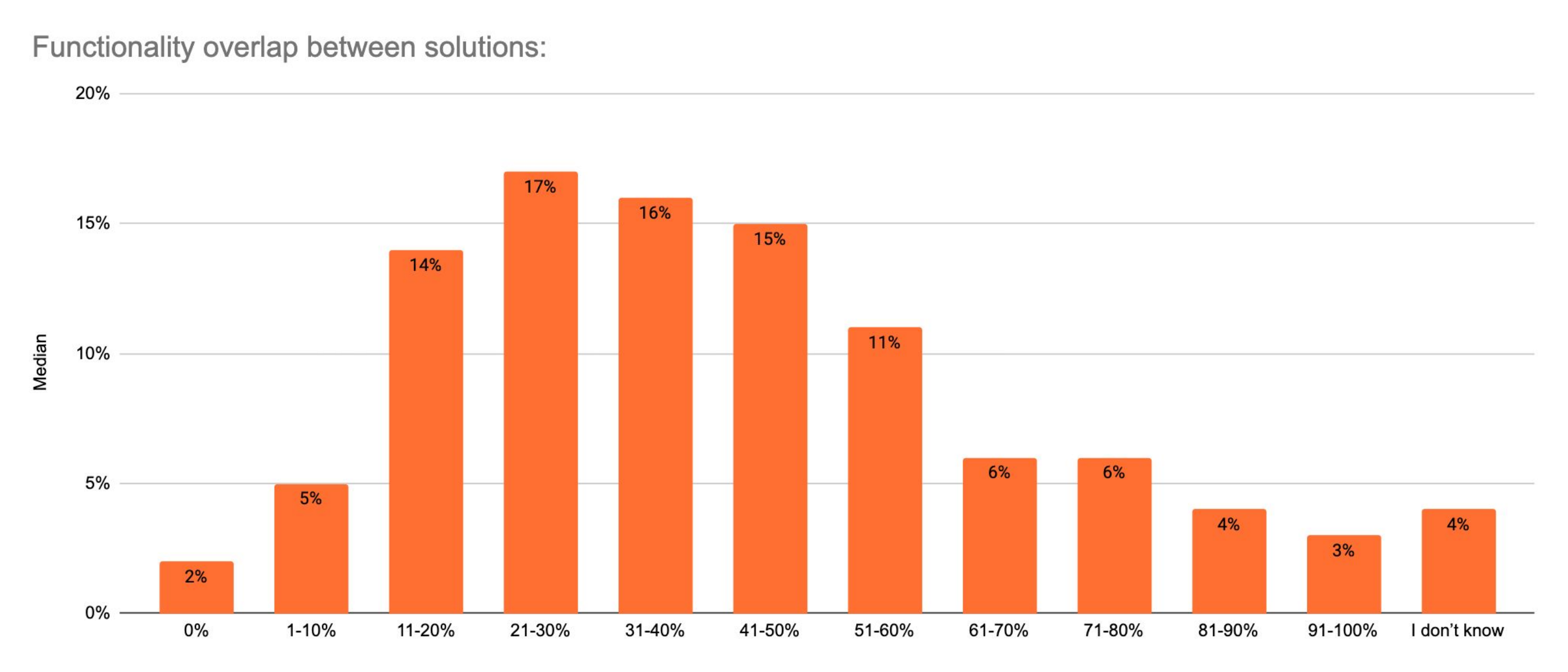


Average number of network and application cybersecurity solutions organisations rely on

Q7a. In USD (\$), approximately how much would you estimate your organisation spends per year on web application and API security controls/tools? | Base: 200

Overlap in Cybersecurity Solutions

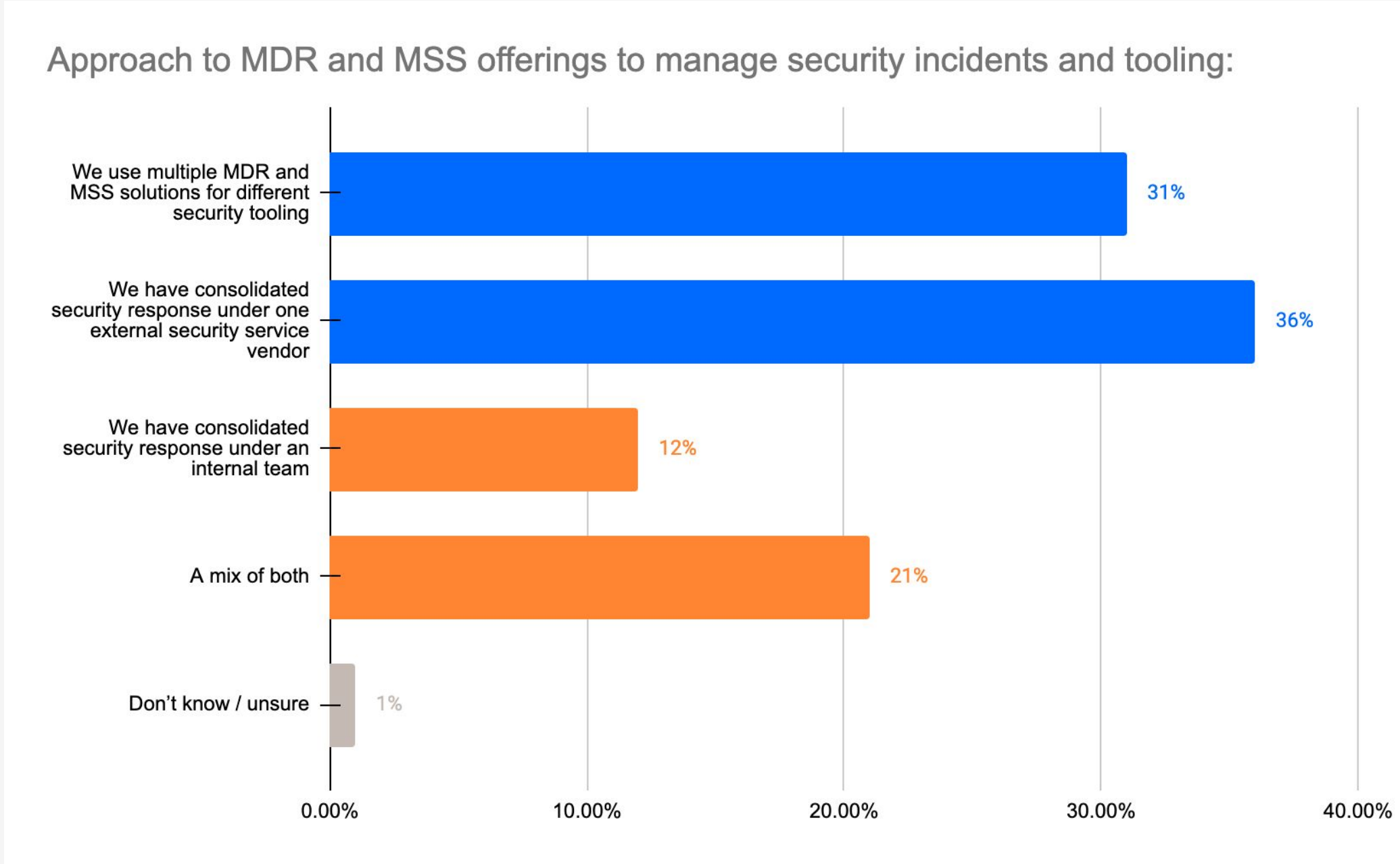
On average, **40%** of these cybersecurity solutions overlap in their primary function



Q7c. Roughly, how many of these solutions overlap in their primary function? Select one | Base: 200

Approach to MDR and MSS Offerings to Manage Security Incidents

36% have consolidated their security response under one external security service vendor, whilst 31% are using multiple MDR and MSS solutions for different security tooling



Q24a. What is your organisation's approach to Managed Detection & Response (MDR) and Managed Security Service (MSS) offerings to manage security incidents and security tooling? Select one | Base: 200

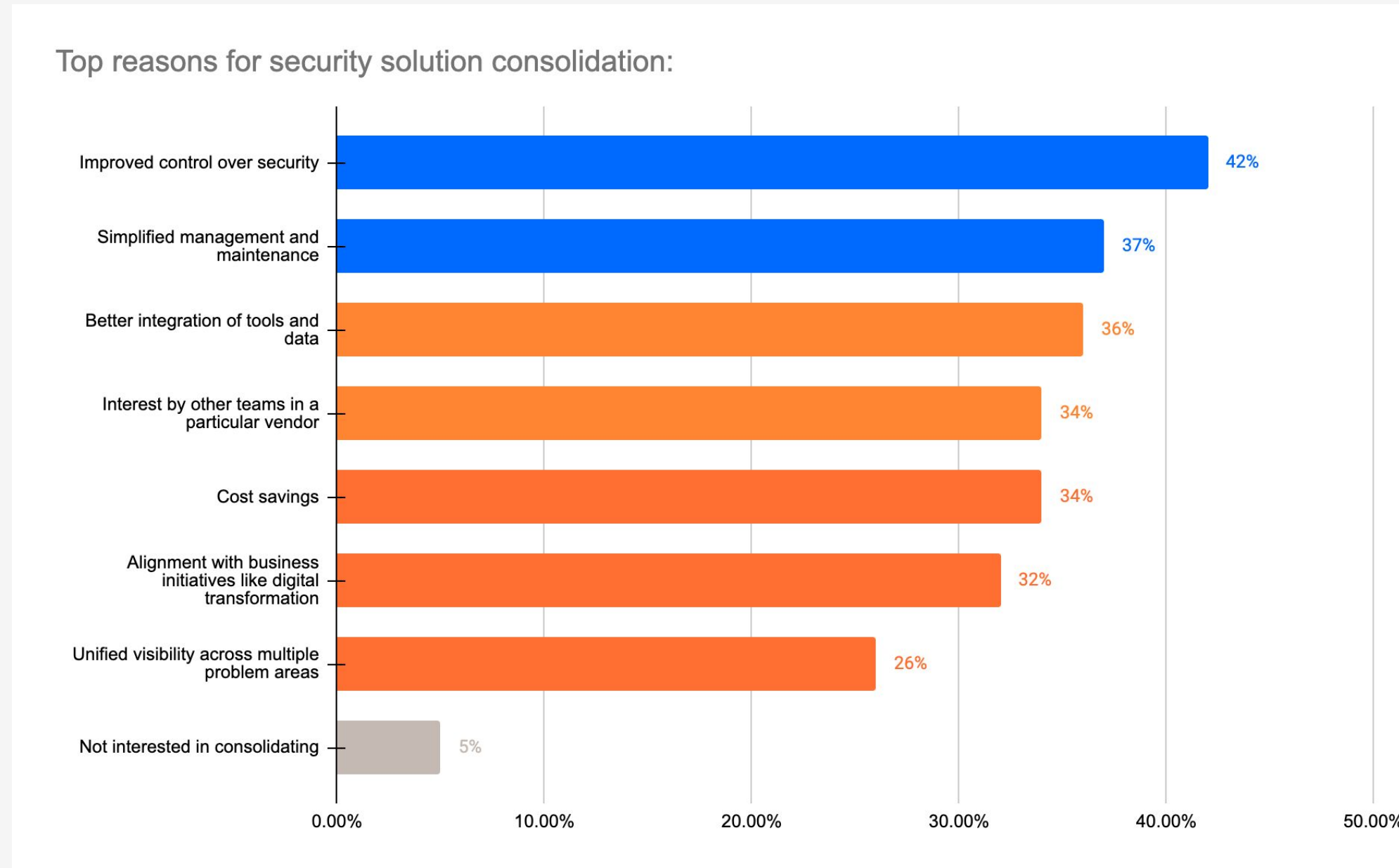


Main Findings

Consolidation and Integration of Security Solutions

Reasons for Security Solution Consolidation

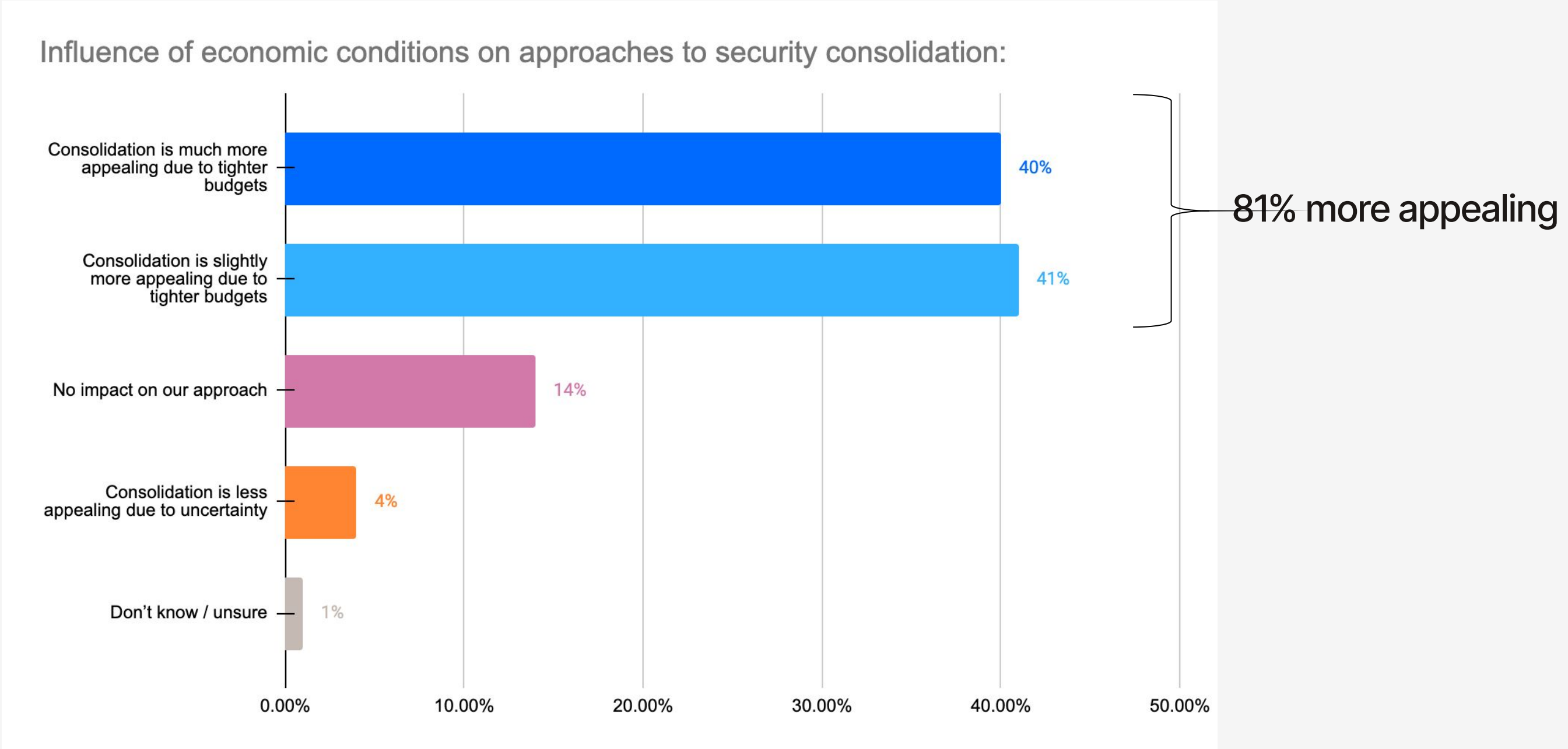
42% attribute their organisation's interest in consolidating security solutions to improving control over security, while a further 37% are looking to simplify management and maintenance



Q23a. If you are interested in consolidating security solutions, what are the primary reasons for your organisation's interest in doing so? Select all that apply | Base: 200

Economic Influence on Security Consolidation

81% say that consolidation is more appealing due to tighter budgets

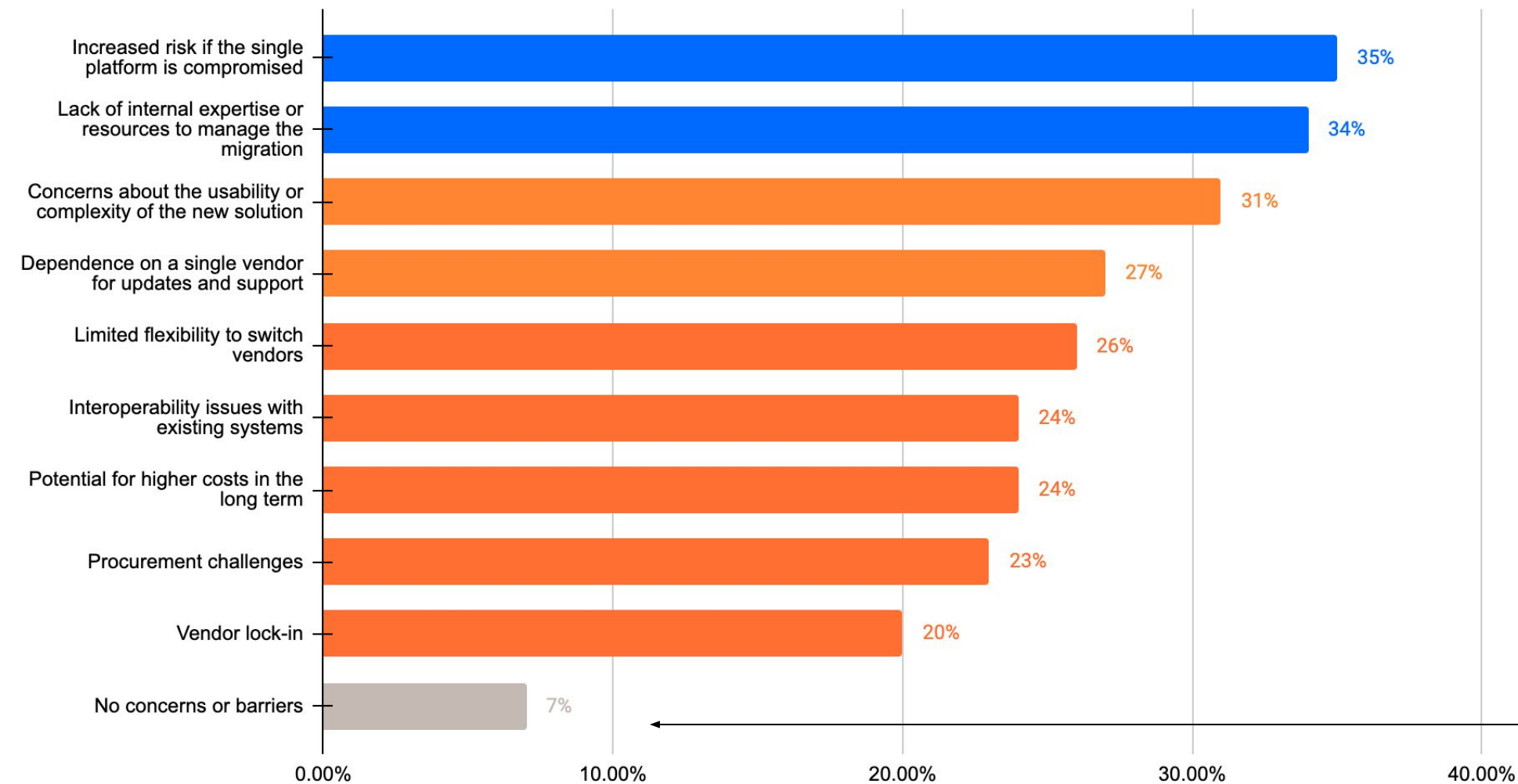


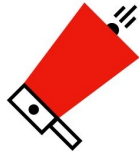
Q23b. How have economic conditions influenced your organisation's approach to security consolidation? Select one | Base: 190

Concerns with Security Tool Consolidation

35% are concerned about increased risk if the single platform is compromised when it comes to consolidating security tools, shortly followed by the lack of internal expertise or resources to manage the migration (34%)

Barriers to consolidating security tools into a single platform / vendor, or switching to a new security solution altogether:



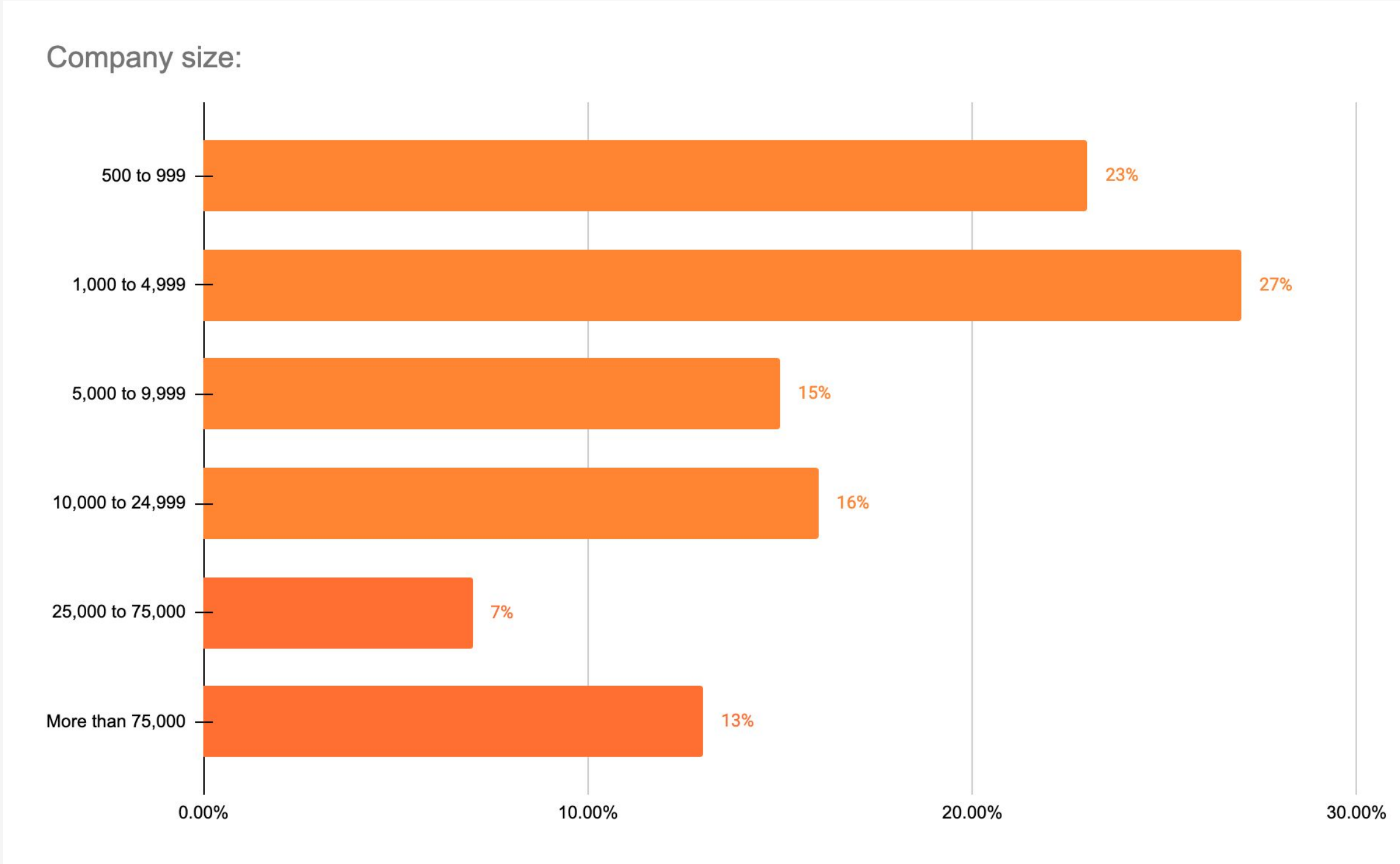
 **93%** of businesses have concerns or are facing barriers when it comes to security tool consolidation

Q24b. What are the concerns or barriers to consolidating your security tools onto a single platform/vendor, or switching to a new security solution? Select all that apply | Base: 200



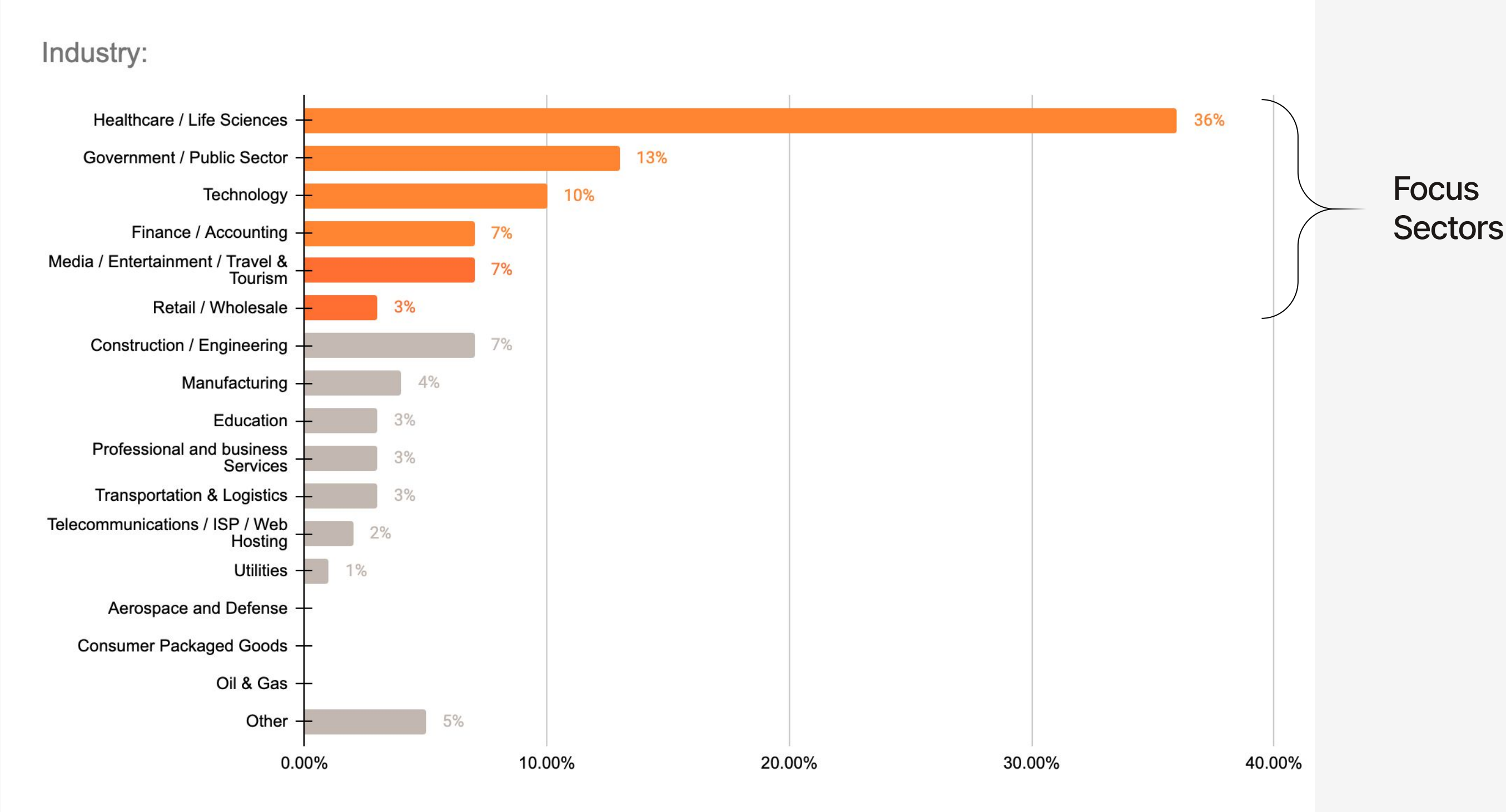
Demographics

Company size



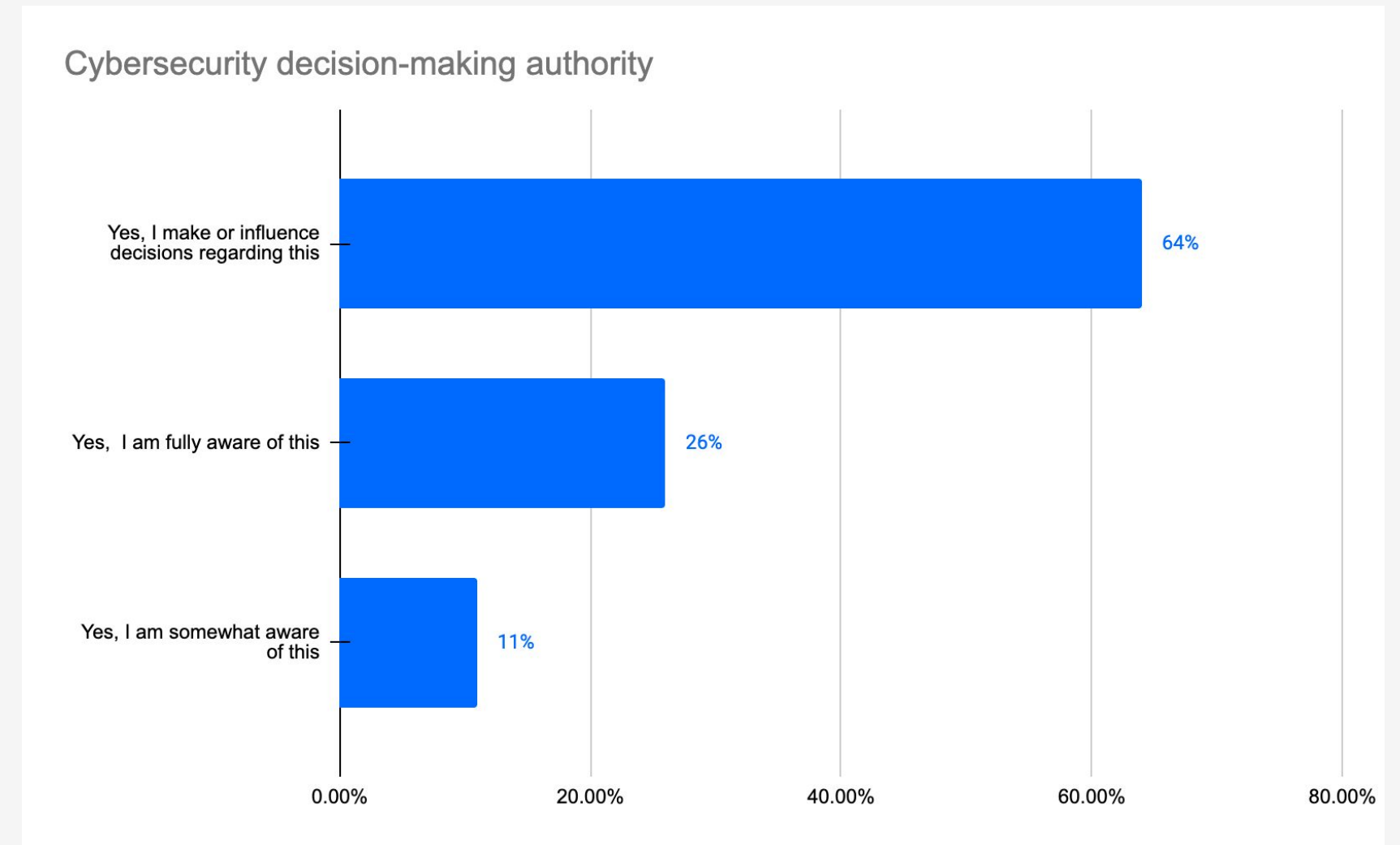
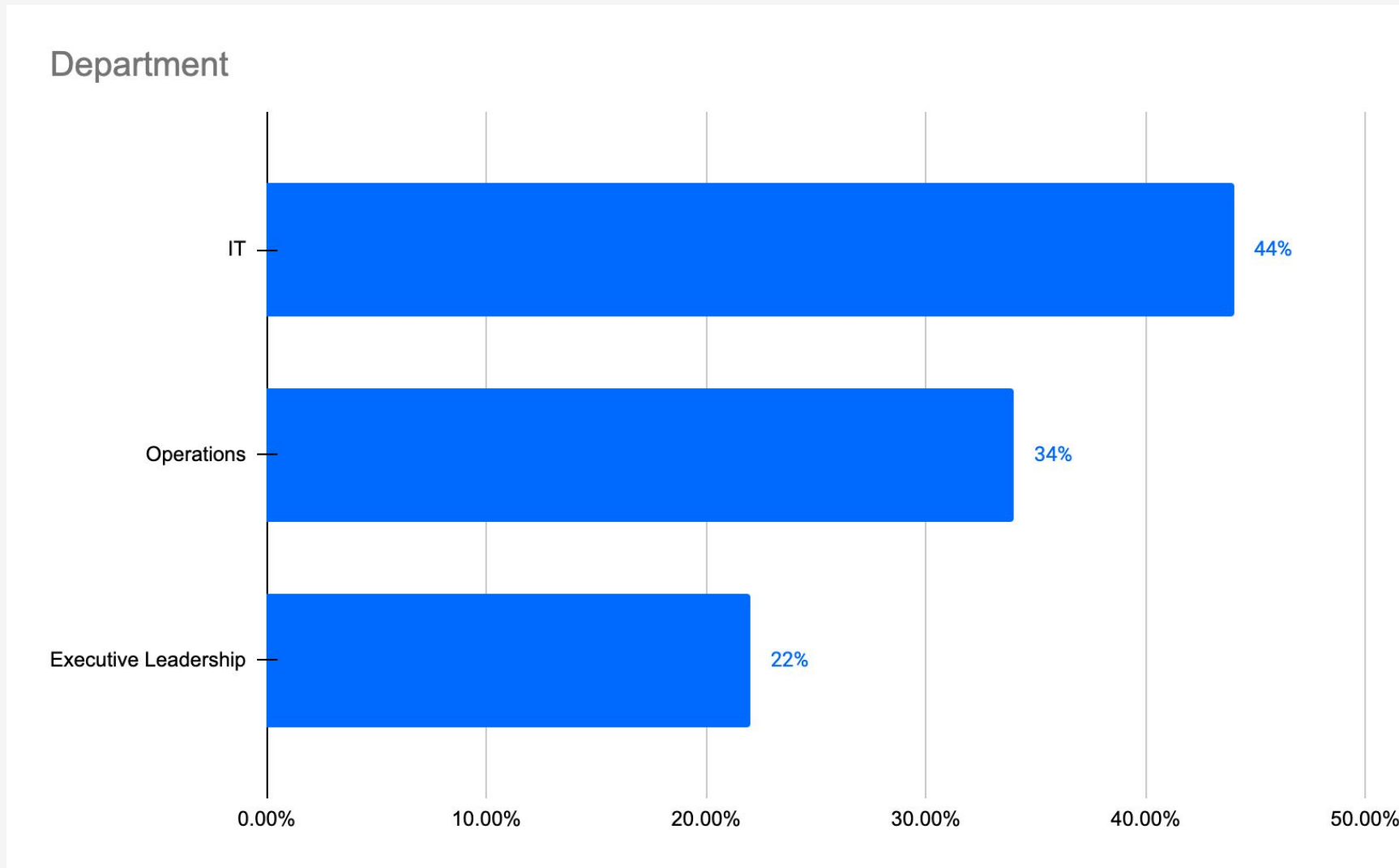
S2. How many people does your company employ? Select one

Industry



S3. Which of the following most closely describes the industry your organization is in? Select one | Base: 200

Department and Authority



S4. Which of the following best describes the department you sit within? Select one

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: 200

Thank you!

fastly[®]