

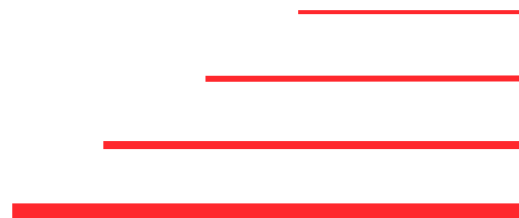


# Fastly Global Security Research 2024

Japan 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 more than 500 employees in Japan**. 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%.

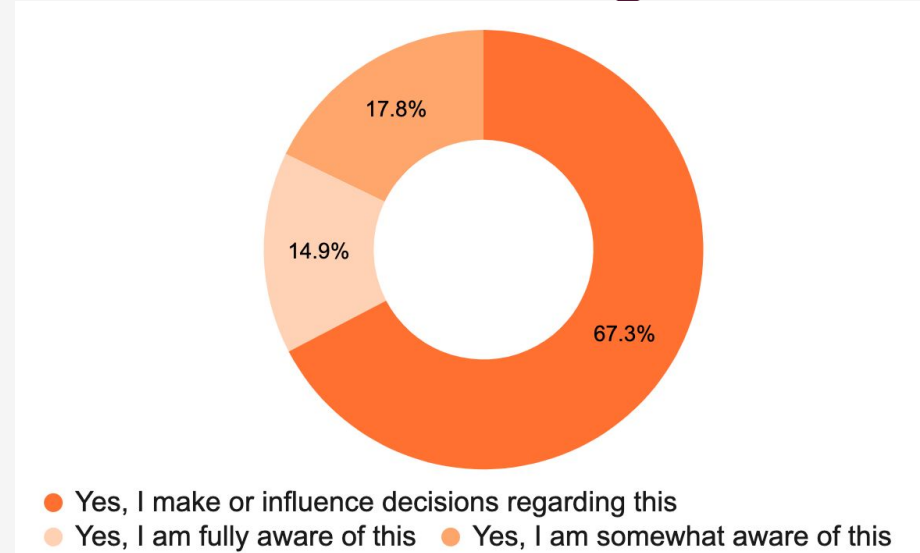
The interviews were conducted online by Sapio Research in September 2024 using an email invitation and an online survey.

# Respondent demographics summary – Cybersecurity Decision Makers

## Seniority

Department	% of respondents
IT	62%
Operations	18%
Executive leadership	20%

## Decision-making



## Seniority

No of employees	% of respondents
250-999	16%
1.000-4.999	43%
5.000-24.999	27%
25.000+	15%

## Primary sectors of Business

1. Manufacturing - 24%
2. Retail / Wholesale - 16%
3. Technology - 13%
4. Telecommunications / ISP / Web Hosting- 9%
5. Government & Public Sector - 5%
6. Finance / Accounting - 4%
- 7.

## Country of residence

Japan





# Key takeaways

# Key stats

Companies expect it to take **5.41 months** to recover from security incidents

Businesses have experienced an average of **38** security incidents in the past year, with the top factors present being **external attackers** (30%) and **Misconfiguration** (30%)

Businesses report being reliant upon an average of **7** cybersecurity solutions, with **36%** of these cybersecurity solutions overlapping in their primary function

Organisations predict that **social engineering attacks** (53%) and **ransomware and extortion** (35%) will be their biggest cybersecurity threats in the next 12 months

**Revenue loss** was one of the top impacts of security incidents (**26%**), with those reporting this suffering an average **2.8%** loss following a security incident

**7 in 10** (70%) say that consolidation of security solutions is more appealing due to tighter budgets



# Main findings

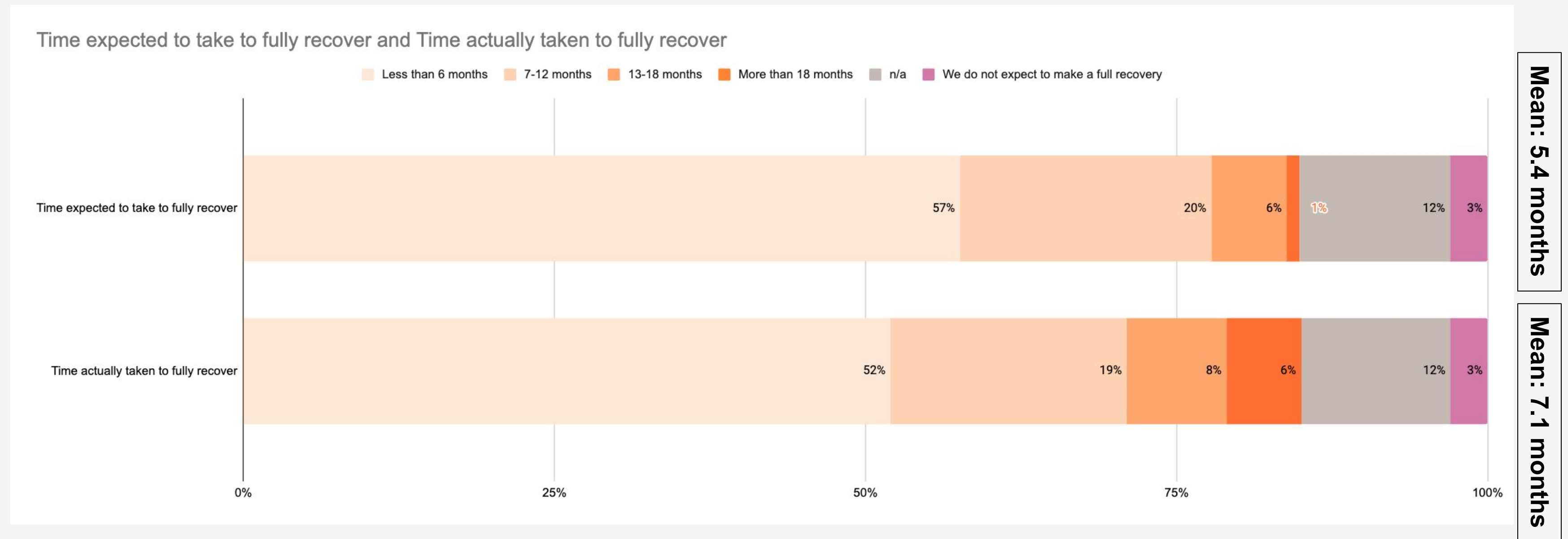


## Main Findings

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 7.1 months, 1.7 months longer than the average business anticipates

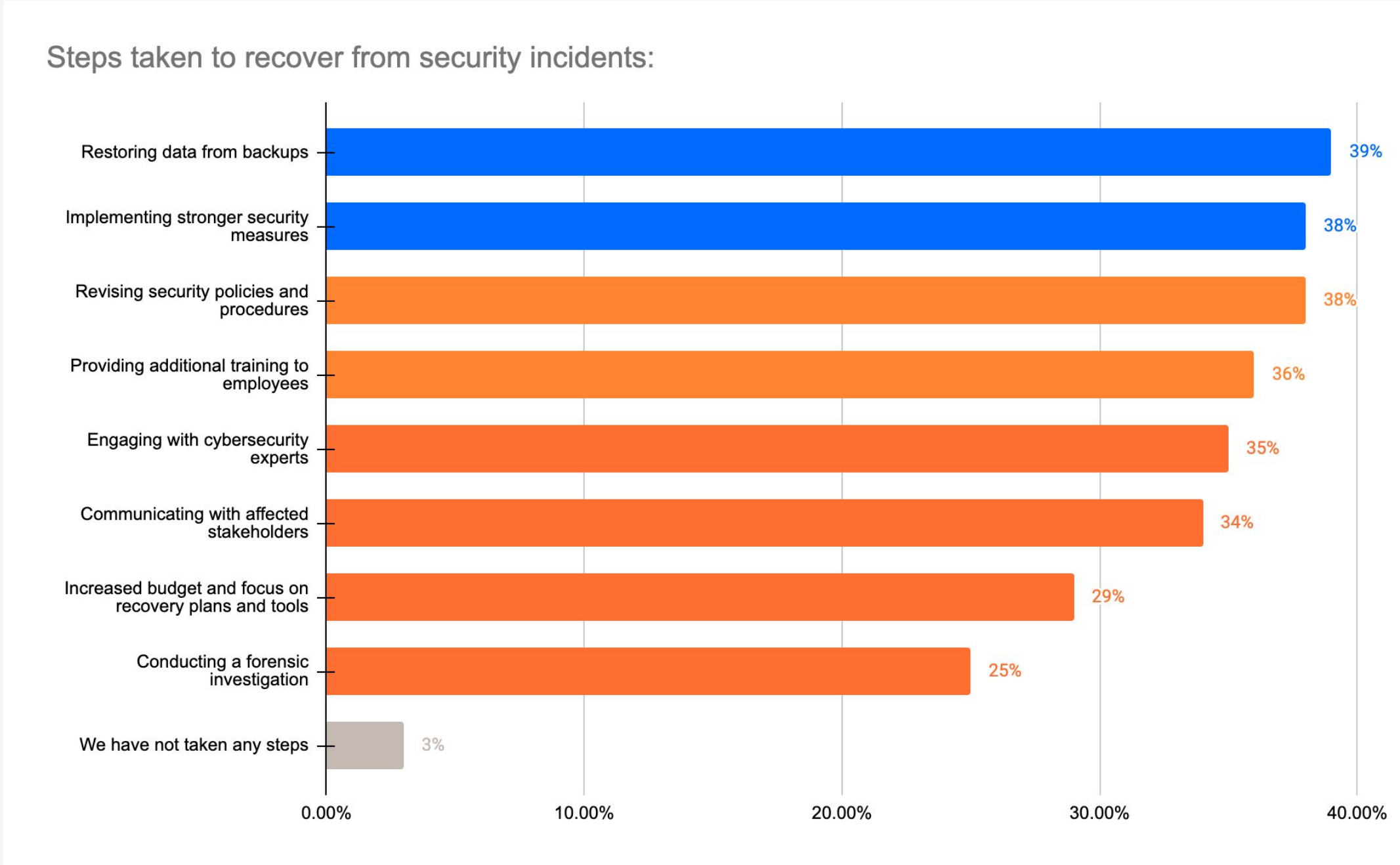


Q17e. How long do you expect it to take, and how long has it taken, to fully recover from each of these impacts? | Base: 172 \*Only asked to those who have experienced a security incident in the last 12 months



# Steps Taken Toward Security Incident Recovery

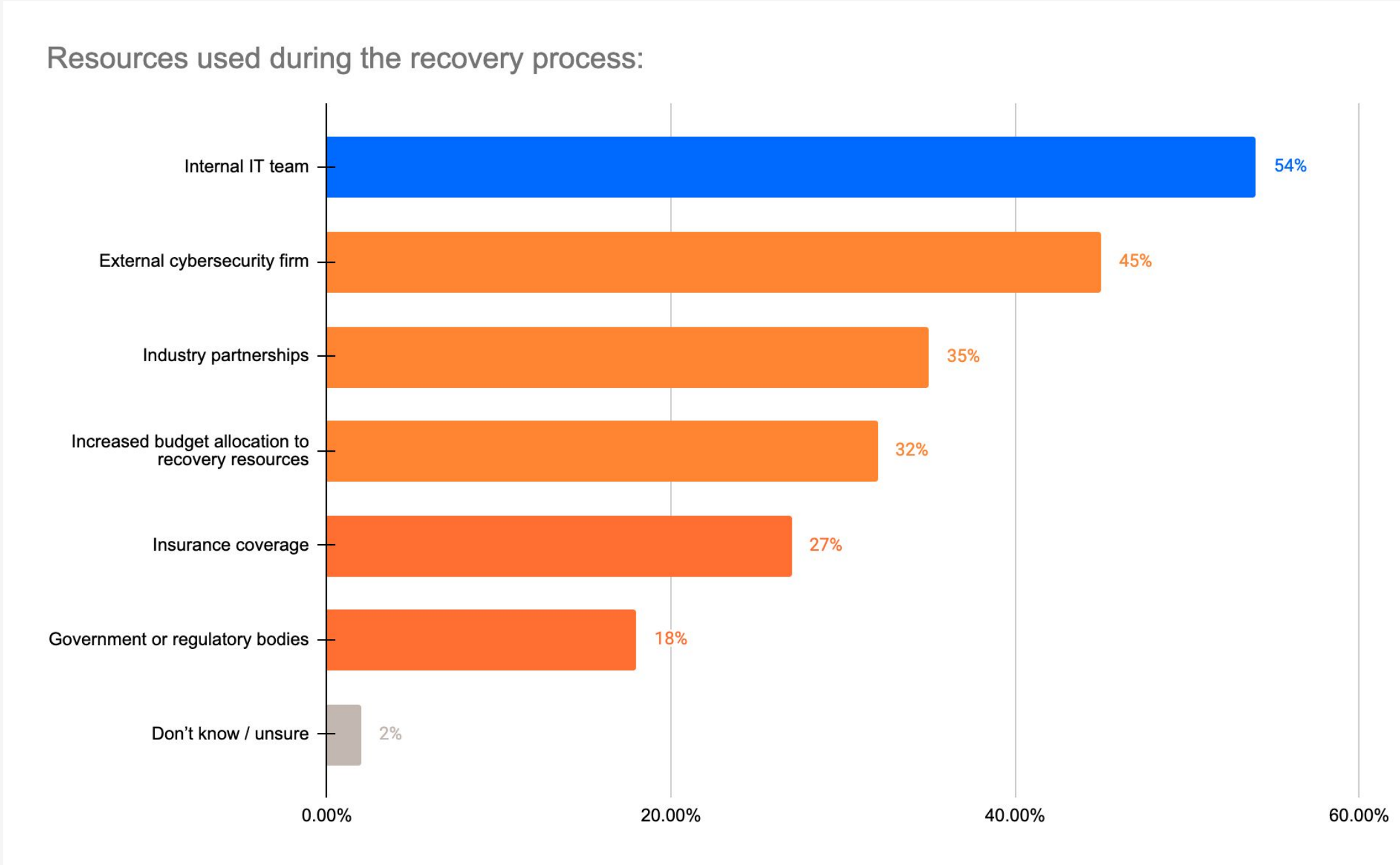
The most common steps businesses are taking to recover from security incidents are restoring data from backups (39%) and implementing stronger security measures (38%)



Q18. What steps has your business taken to recover from the security incident? Select all that apply | Base: 172 \*Only asked to those who have experienced a security incident in the last 12 months

# Resources Used for Security Incident Recovery

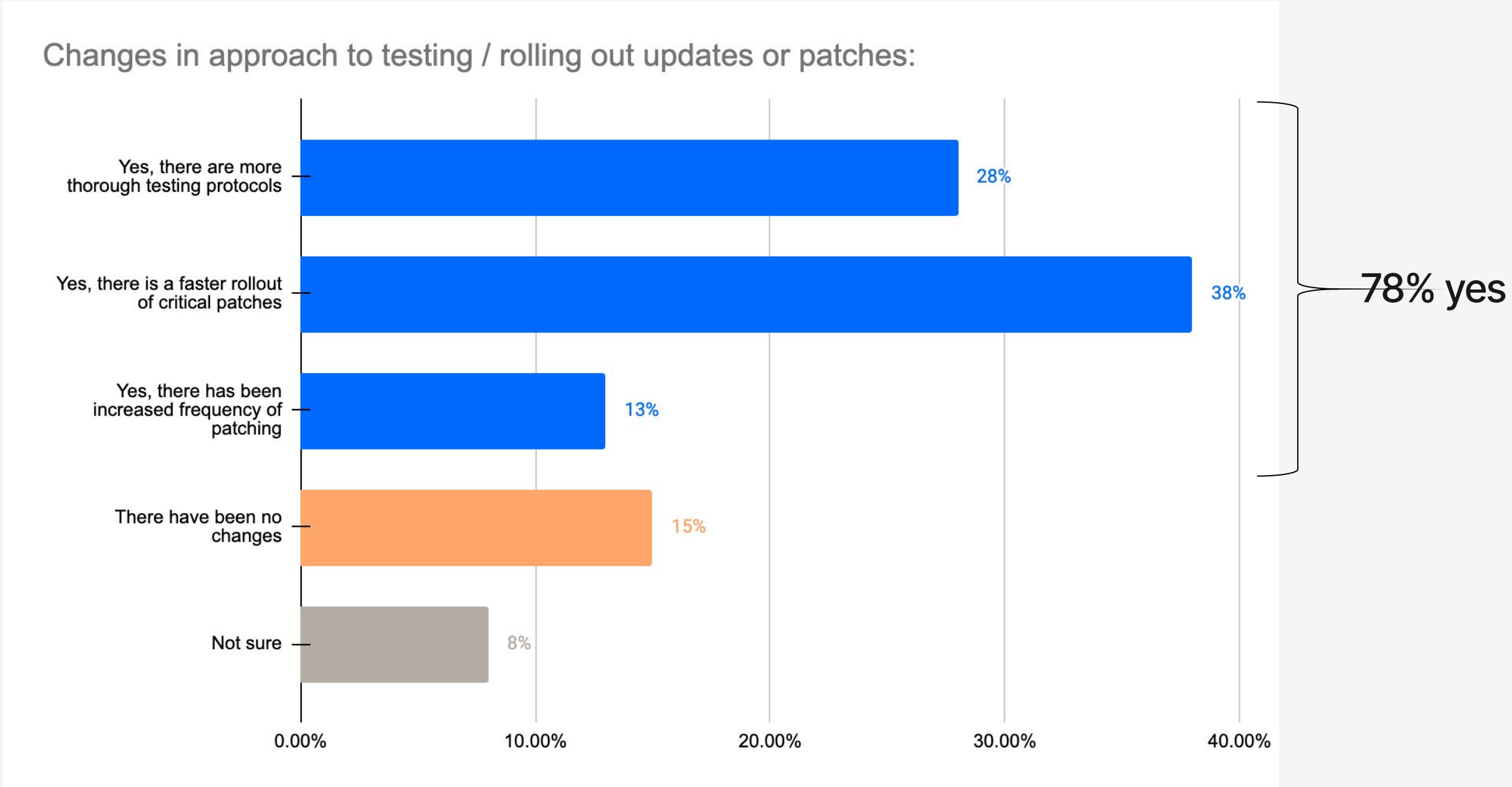
Most businesses are opting to use their internal IT team (54%) for recovery following a security incident



Q19. What resources did your business use for recovery? Select all that apply | Base: 166 (only asked to those who have taken step towards business recovery)

# Changes in Approach to Updates and Patch Testing

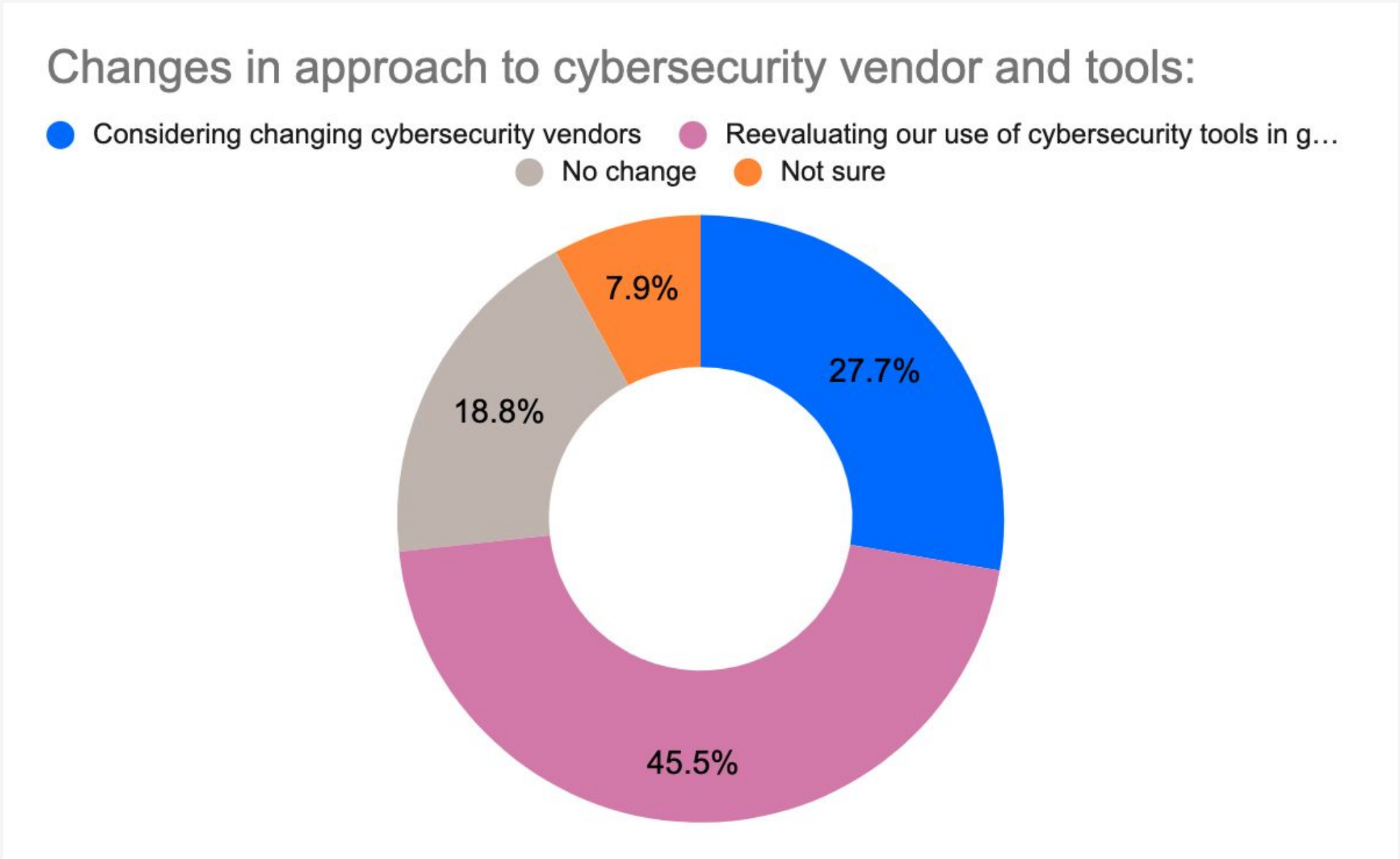
78% report that recent reliability incidents have encouraged their business to change their approach to testing or rolling out updates or patches



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

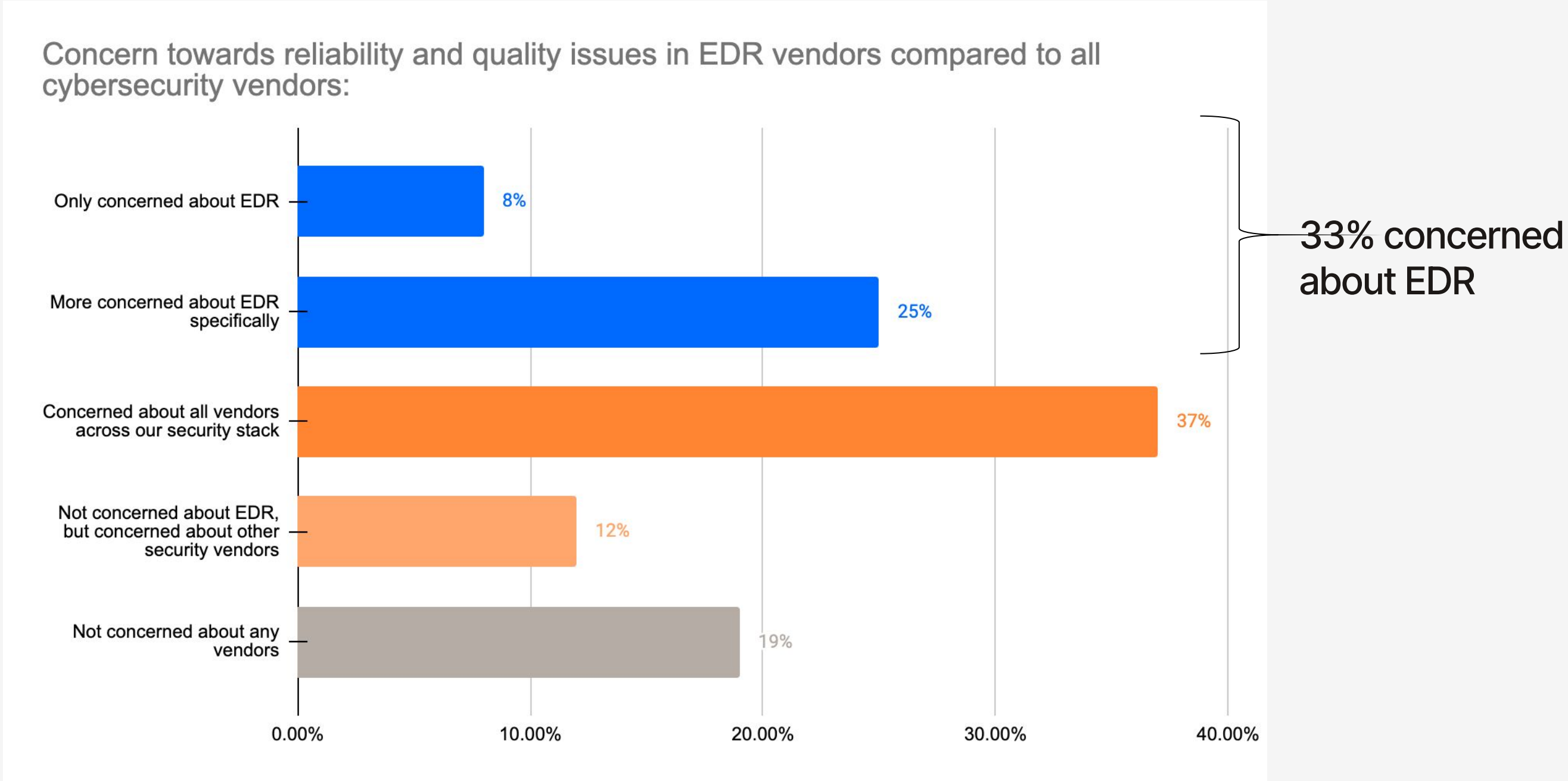
46% are re-evaluating their use of cybersecurity tools in general, following the recent CrowdStrike outage, with a further 28% considering changing cybersecurity vendors



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

69% are concerned about the reliability and quality of their vendors, with a split between those concerned about all vendors in their security stack (37%) and those more concerned about EDR (33%)



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

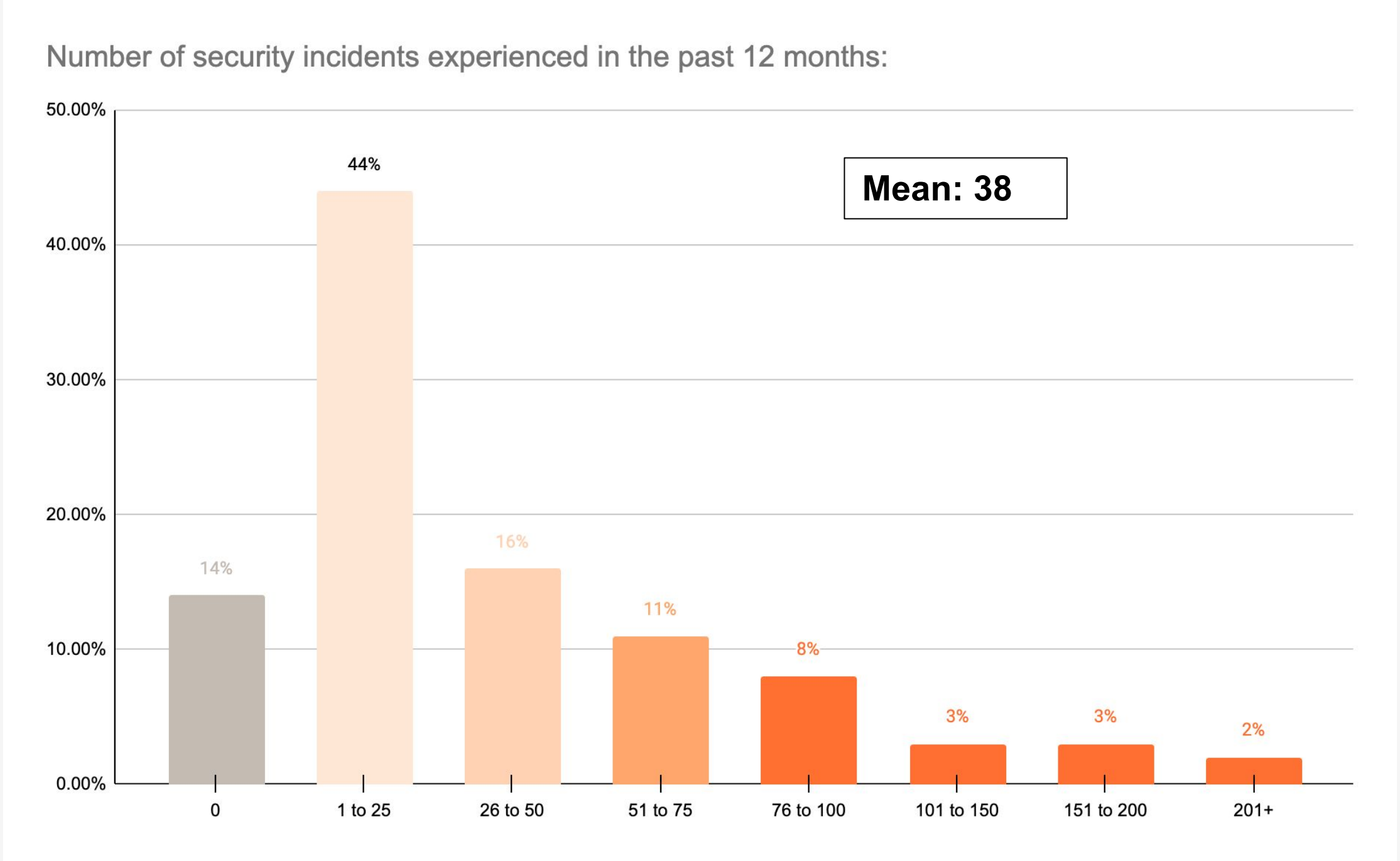


## Main Findings

## The attack landscape

# Number of Security Incidents in the Past Year

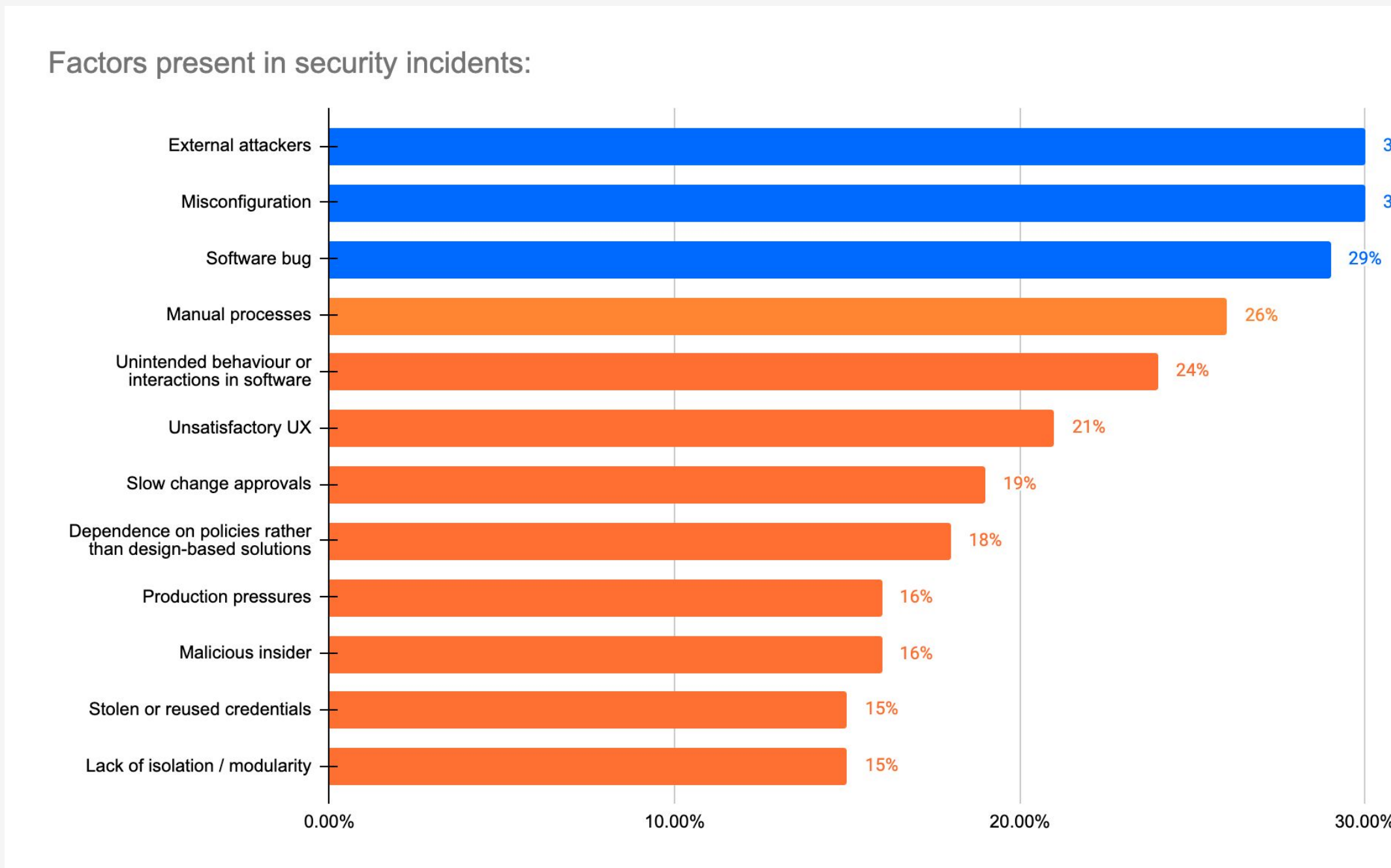
On average, businesses have experienced 38 security incidents in the past 12 months



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 (30%), misconfiguration (30%) and software bugs (29%)

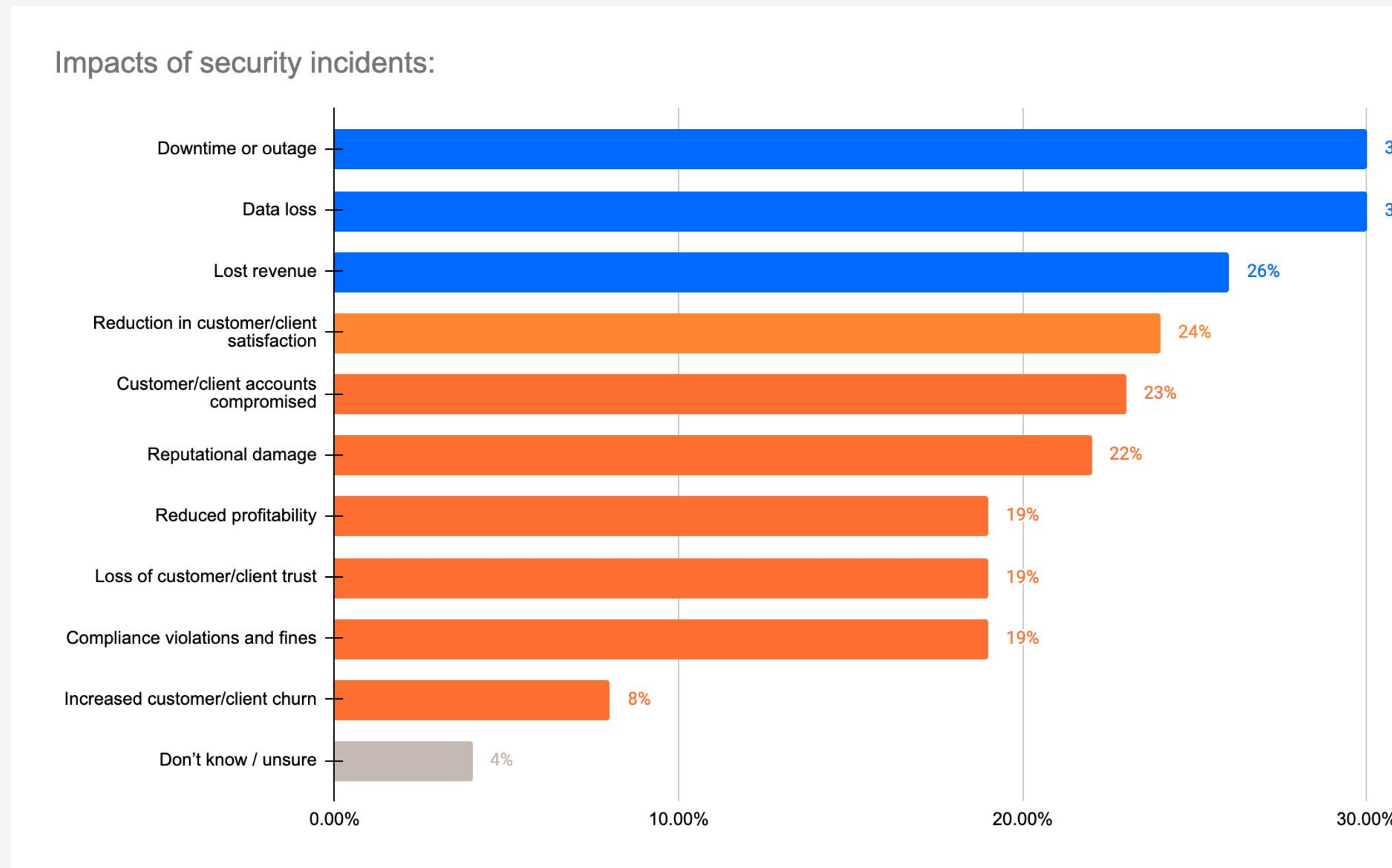


Q16. Which of the following factors were present in the security incident? Select all that apply | Base: 172 \*Only asked to those who have experienced a security incident in the last 12 months



# Main Impacts of Security Incidents

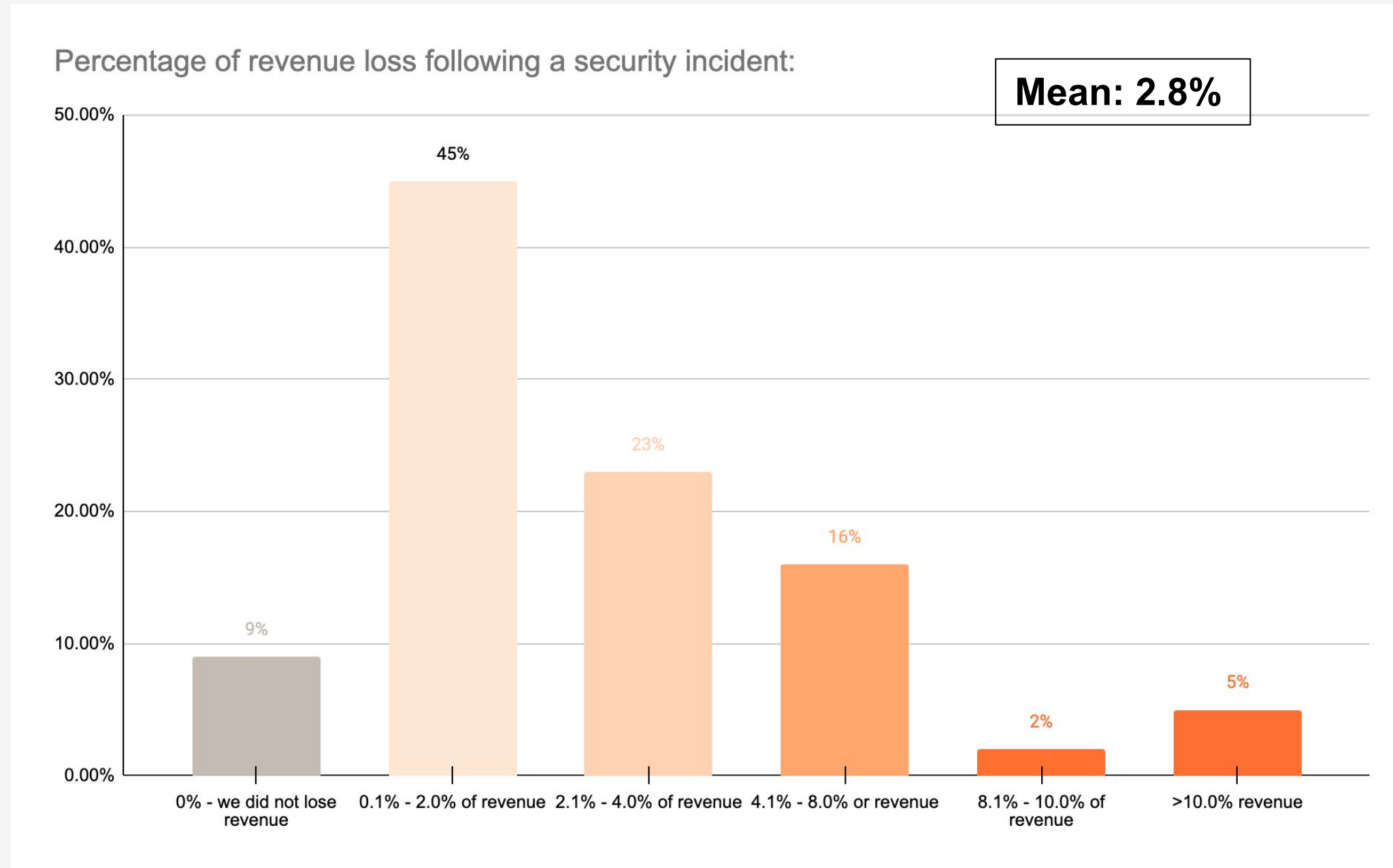
The top impacts of security incidents are downtime or outage (30%), data loss (30%) and lost revenue (26%)



Q17a. What were the main impacts of the security incident? Select top three | Base: 172 \*Only asked to those who have experienced a security incident in the last 12 months

# Revenue Loss from Security Incidents

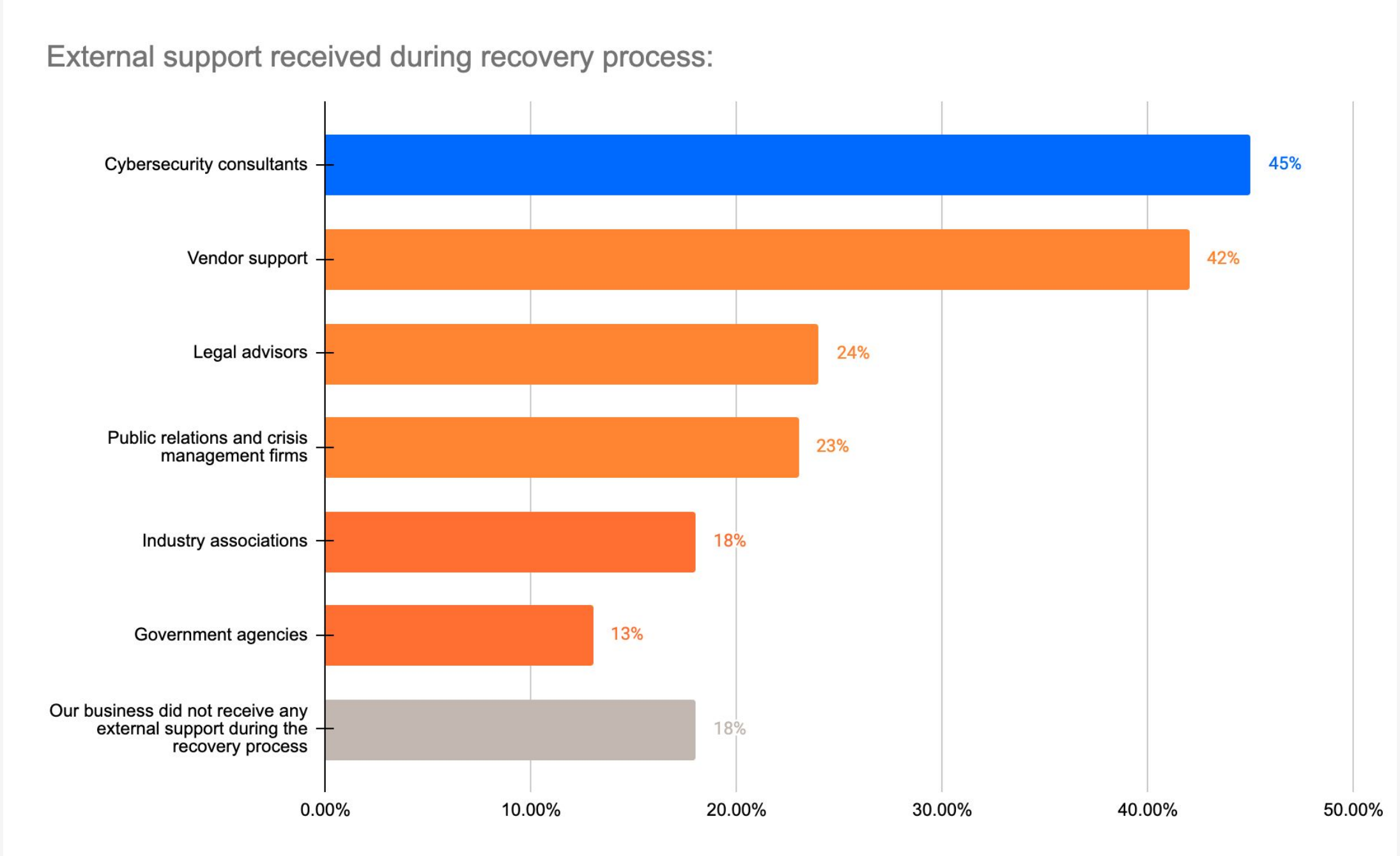
Amongst those who report revenue loss as a top impact of security incidents, businesses report losing an average of 2.8% of their revenue



Q17b. Approximately what percentage of your revenue did you lose as a result of a security incident? Select one | Base: 44 \*Only asked to those who lost revenue as a result of security incidents

# External Support During Recovery

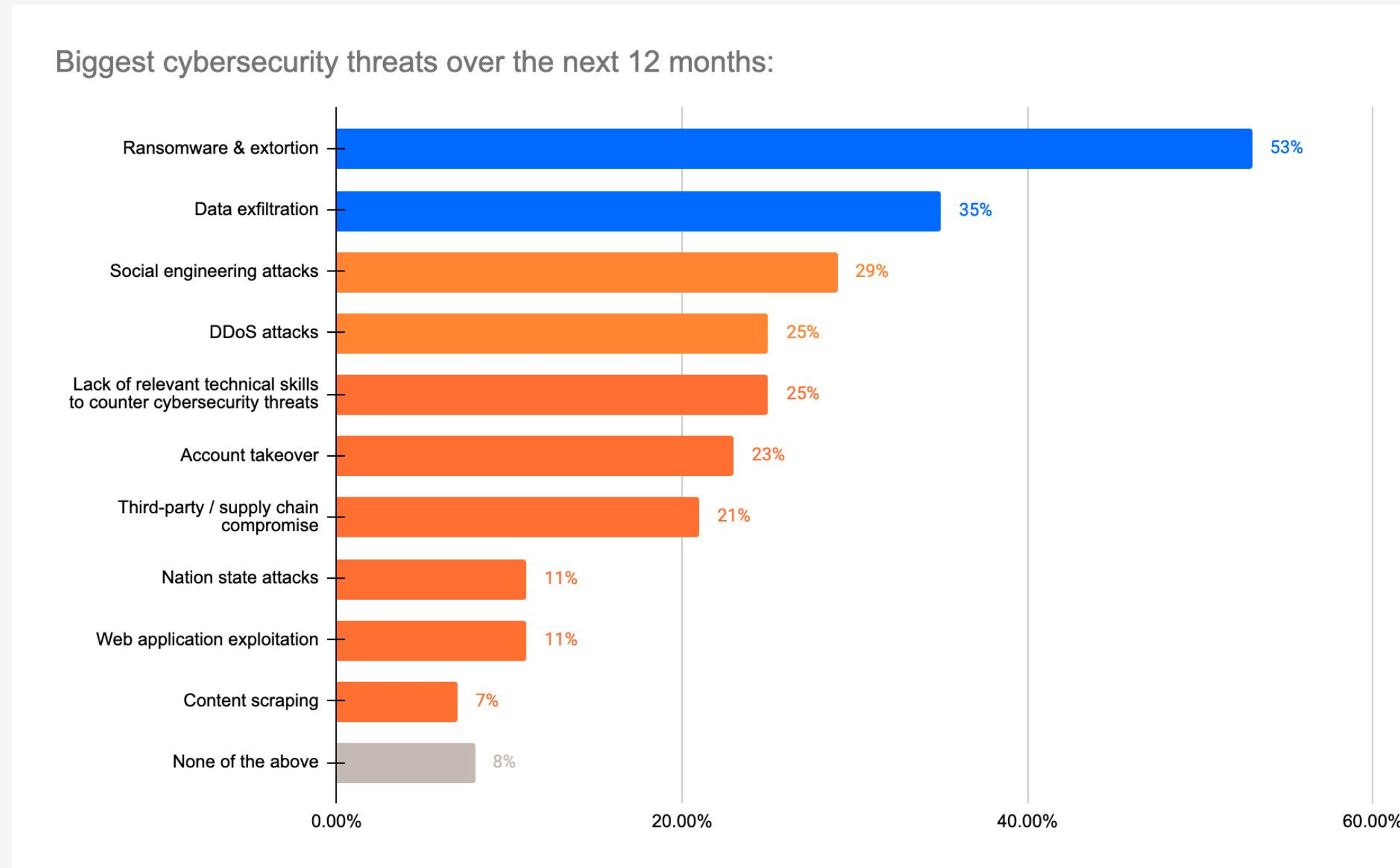
45% say their business utilised cybersecurity consultants during the recovery process



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

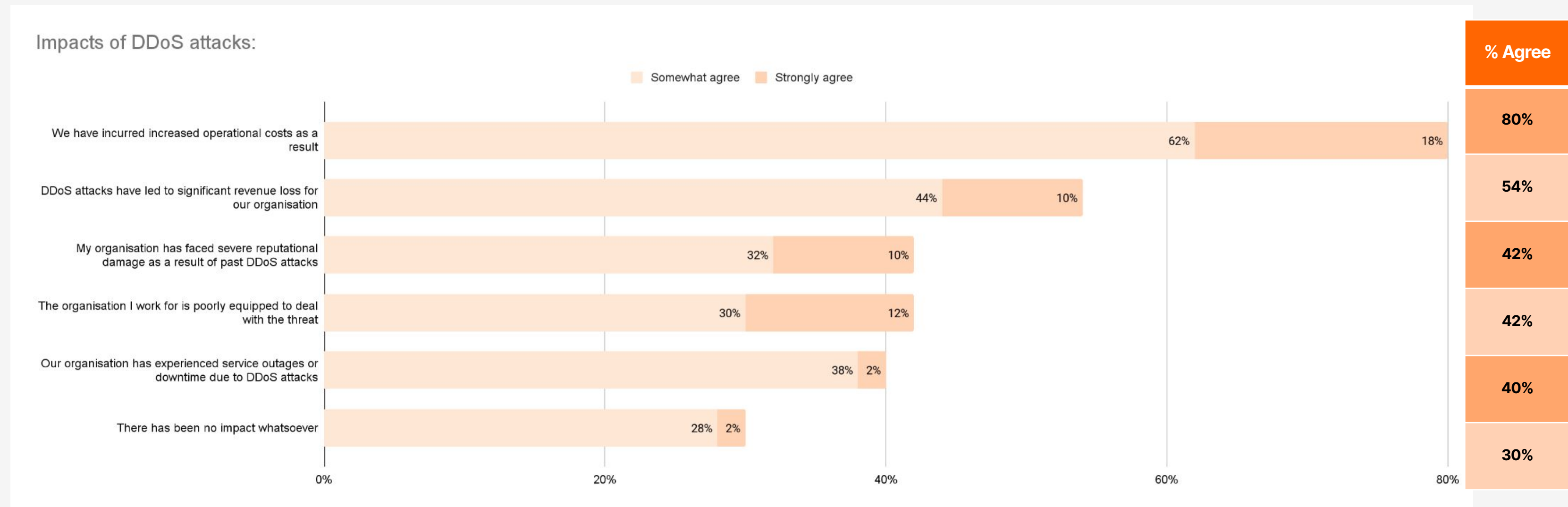
Organisations predict that ransomware and extortion (53%) and data exfiltration (35%) will be their biggest cybersecurity threats in the next 12 months



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

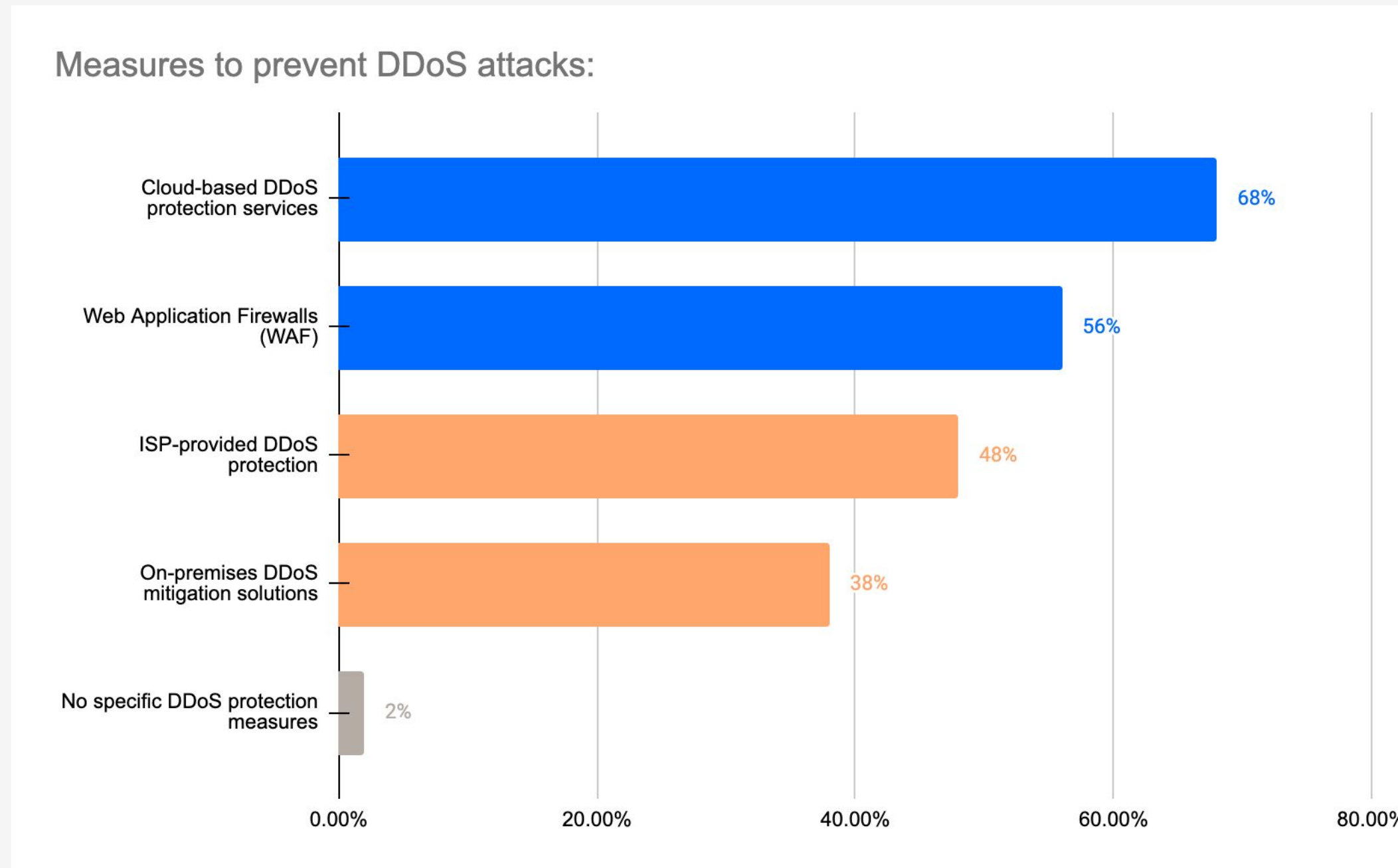
Decision makers who think DDoS attacks will be one of the biggest threats over the next 12 months are likely driven by the significant negative impacts of DDoS attacks, with the majority (80%) saying they result in increased operational cost



Q1b. To what extent do you agree or disagree with the following statements? | Base: 50 \*Only asked to those who believe DDoS attacks are a threat

# DDoS Protection Measures

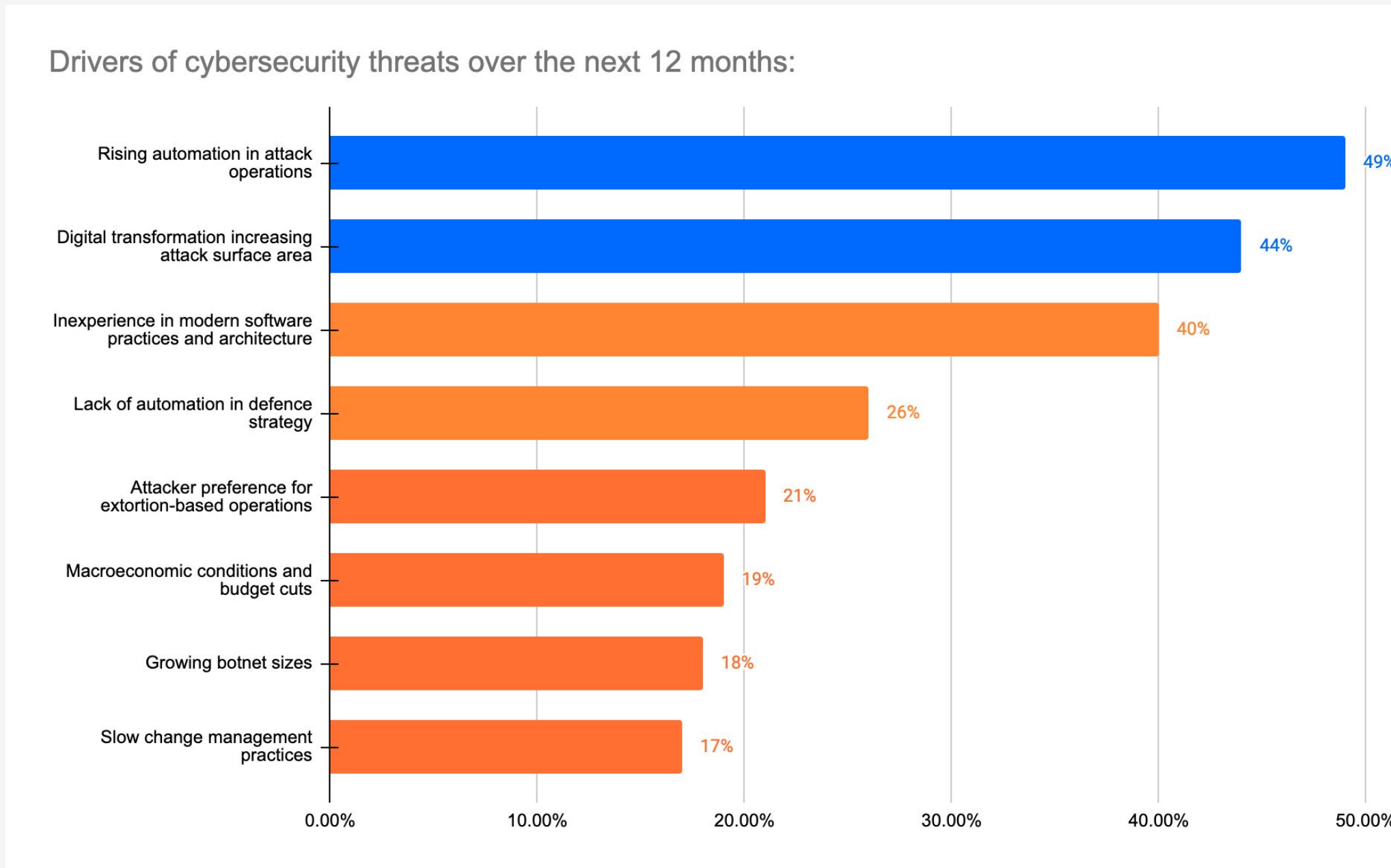
Organisations are most commonly using cloud-based DDoS protection services (68%) and Web Application Firewalls (WAF) (56%) to combat DDoS attacks



Q1c. What measures does your organisation currently use for DDoS protection? Select all that apply | Base: 50 \*Only asked to those who believe DDoS attacks are a threat

# Drivers of Future Cybersecurity Threats

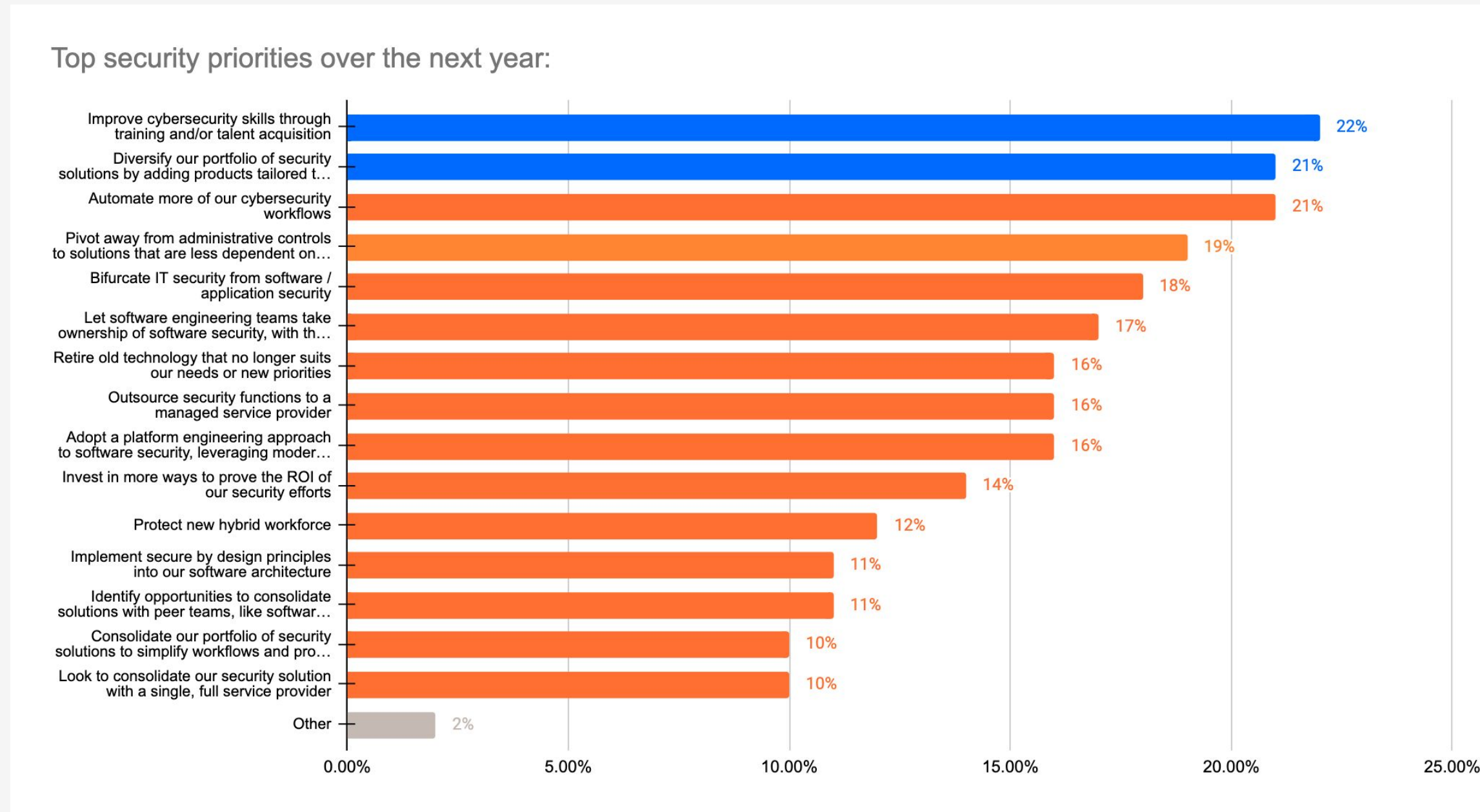
Looking ahead, decision makers believe that rising automation in attack operations (49%) and digital transformation increasing the attack surface area (44%) will be the biggest drivers of cybersecurity threats



Q3. Which of the following do you predict will drive cybersecurity threats to your business over the next 12 months? Select top three | Base: 200

# Security Priorities for the Next Year

Organisations' top security priorities for the next year revolve around improving cybersecurity skills (22%), diversifying their portfolio of security solutions by adding tailored products (21%), and automation of cybersecurity workflows (21%)



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



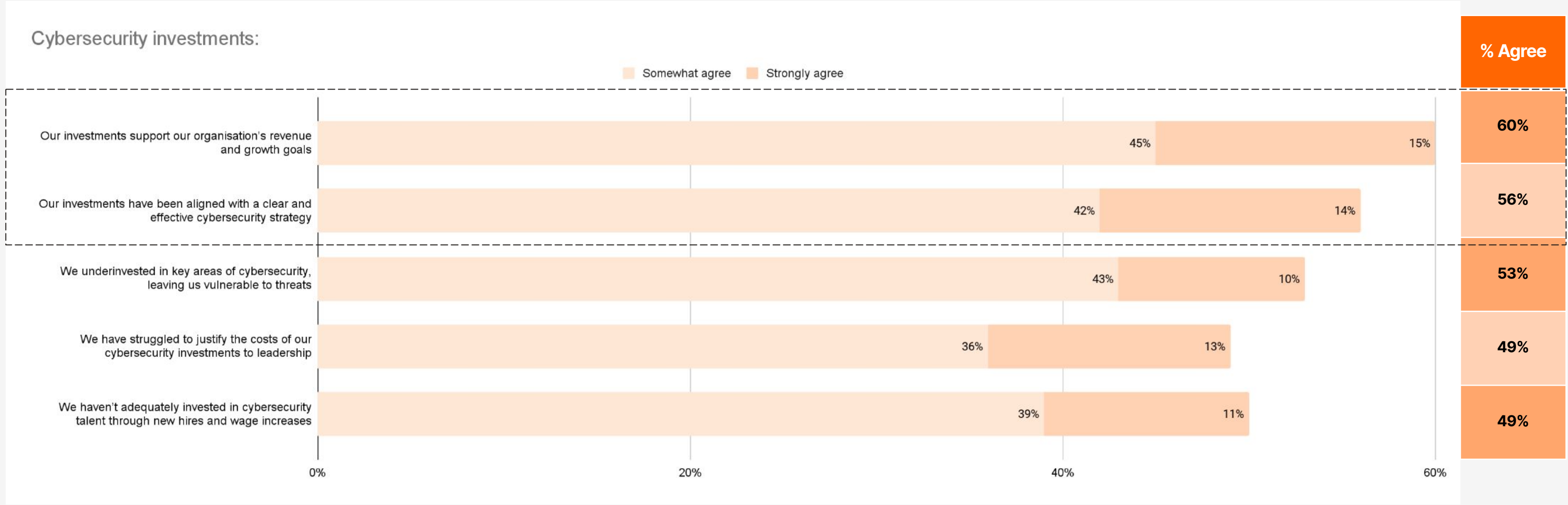


## Main Findings

Is cybersecurity spending  
falling behind?

# Investment in Cybersecurity

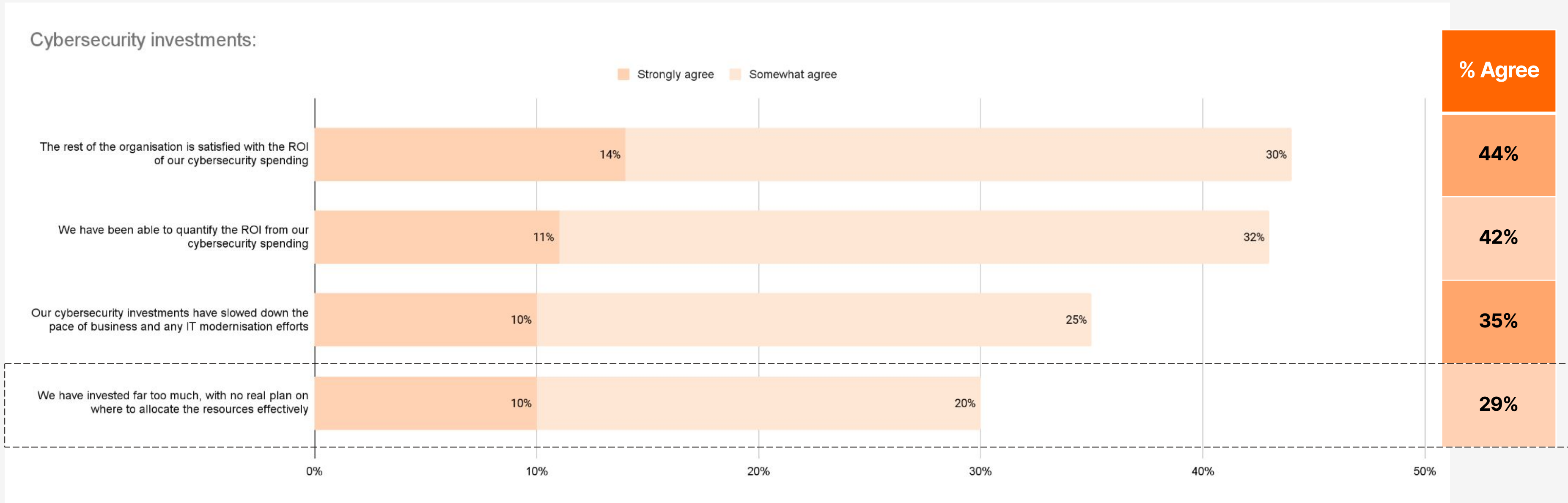
60% agree that their investments in cybersecurity support their organisation's revenue and growth goals, with a further 56% agreeing that these investments are aligned with a clear and effective cybersecurity strategy...



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

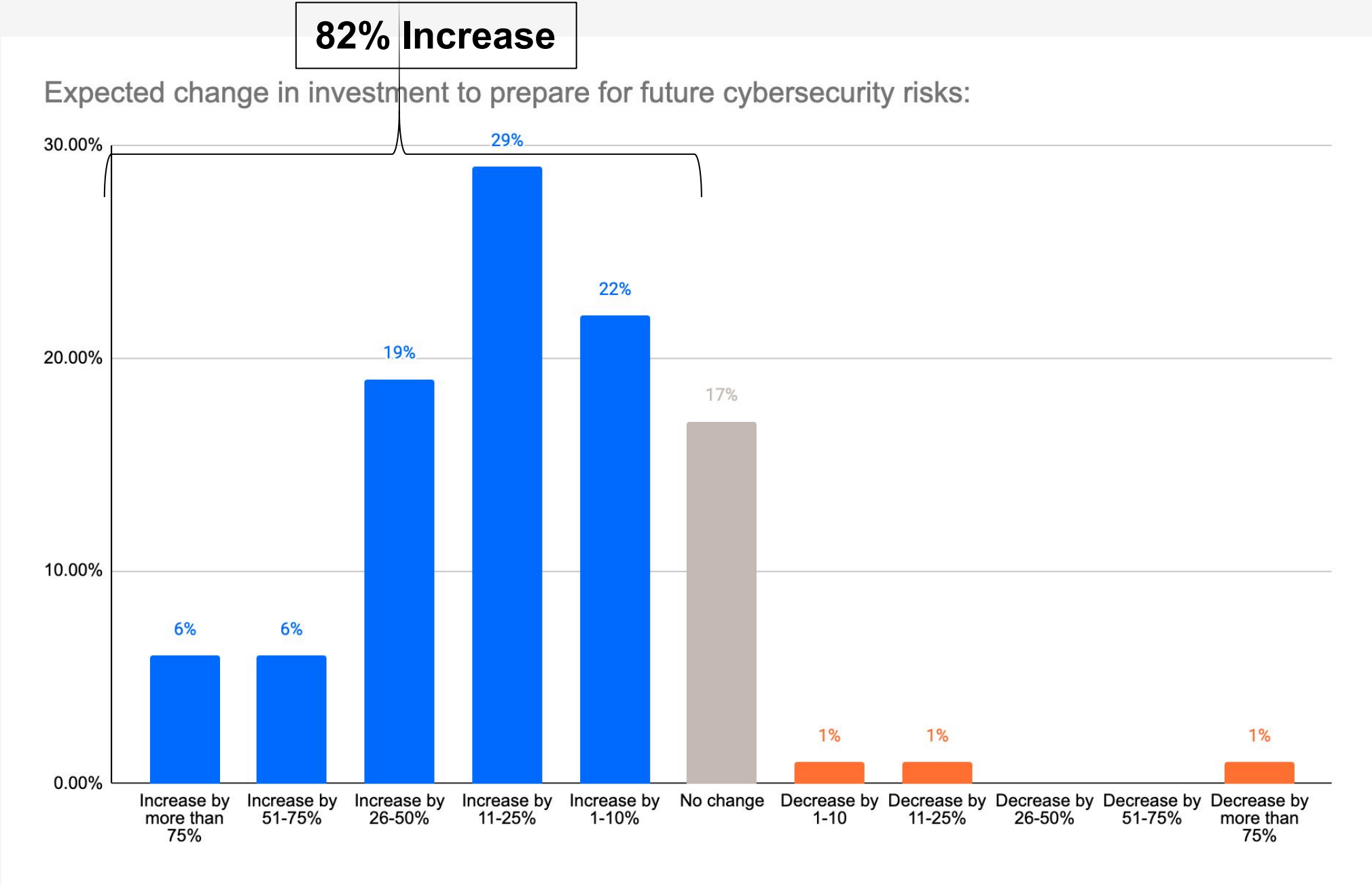
...furthermore, just 29% agree that they have invested too much, with no real plan on where to allocate the resources effectively, demonstrating that organisations are actively preparing for future cybersecurity risks



**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

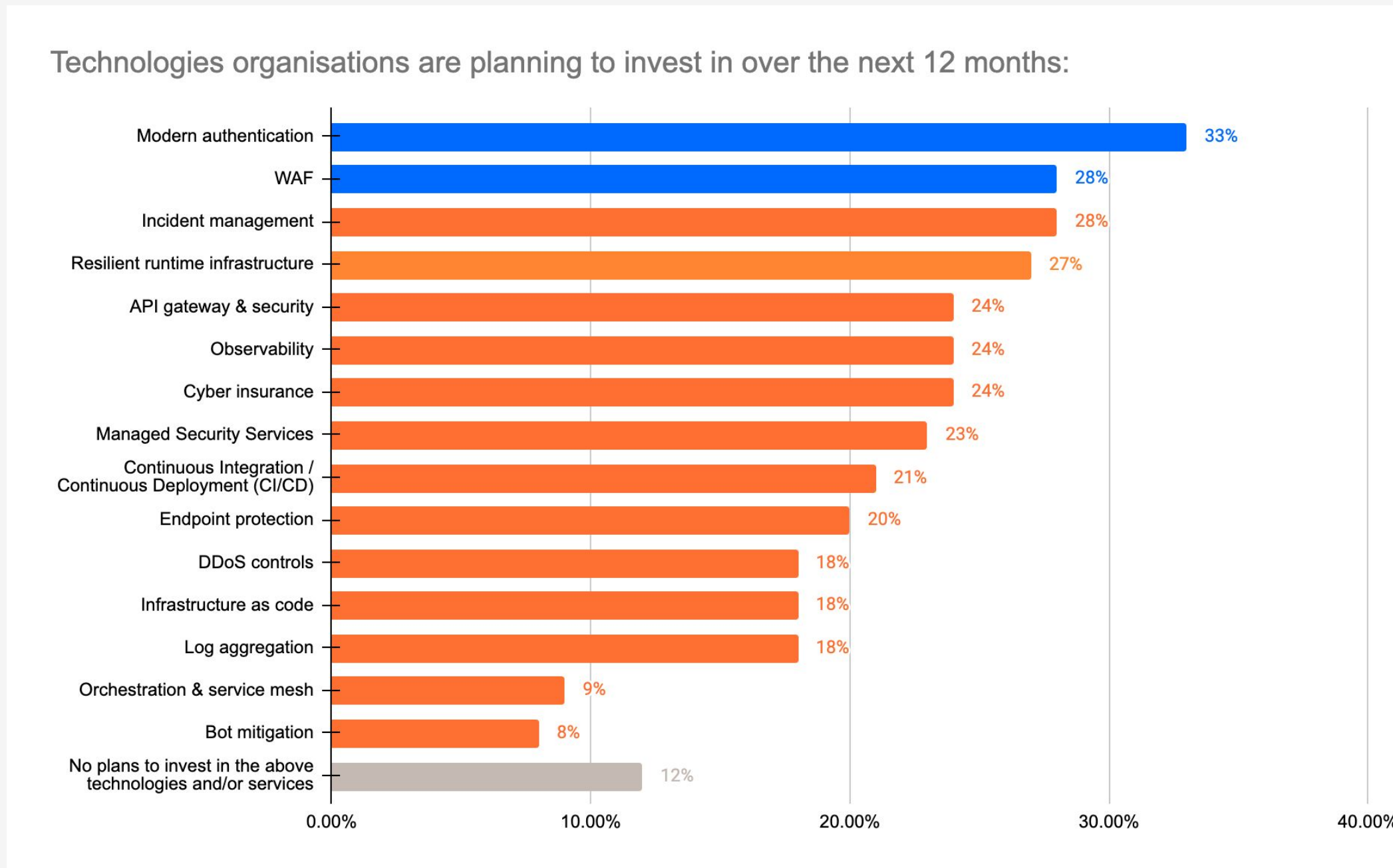
82% of decision makers are expecting their organisation's investment to increase to prepare for future cybersecurity risks over the coming 12 months



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 (33%) and web application firewalls (WAF) (28%)



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

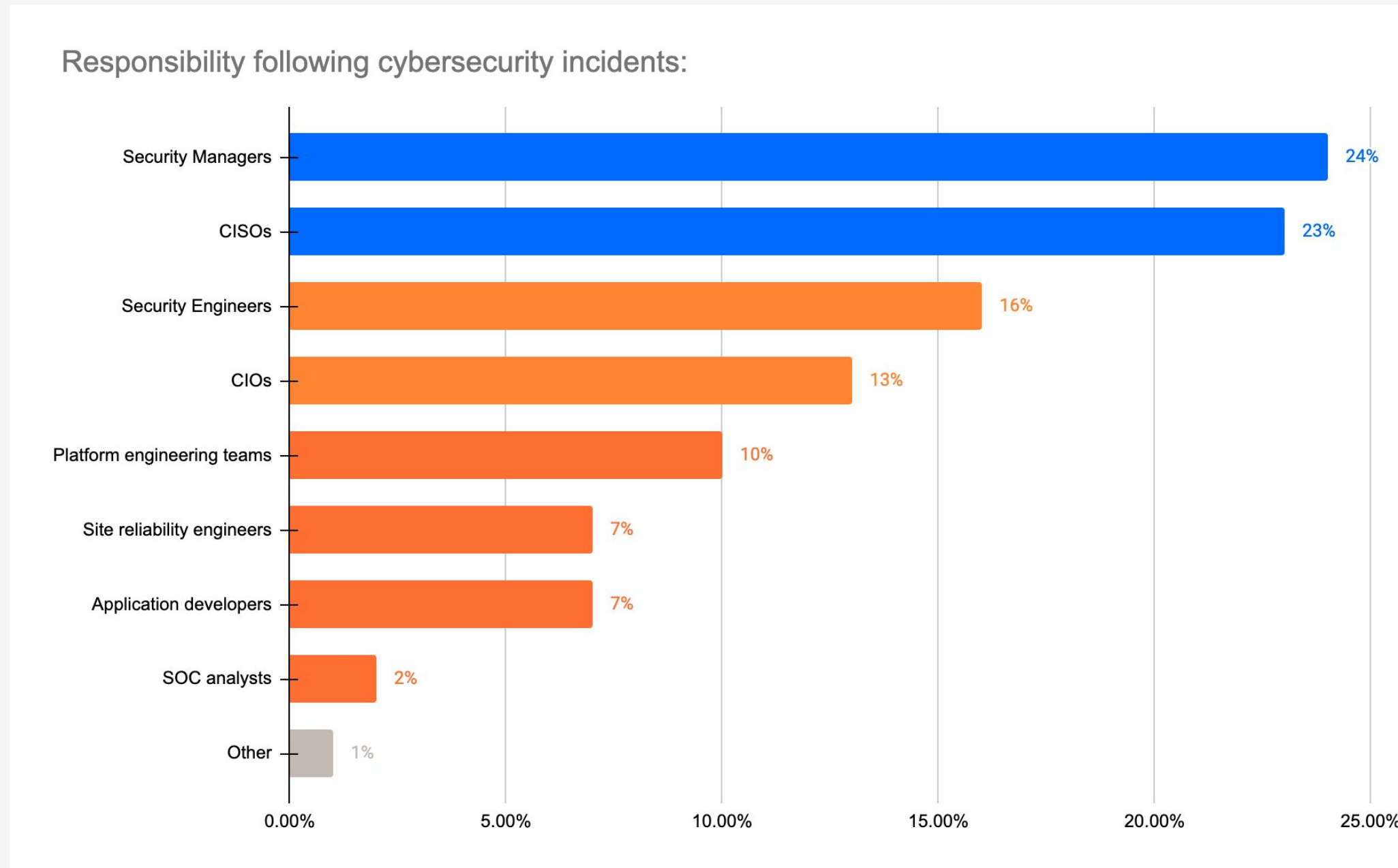


## Main Findings

## Shifting accountability

# Responsibility During Cybersecurity Incidents

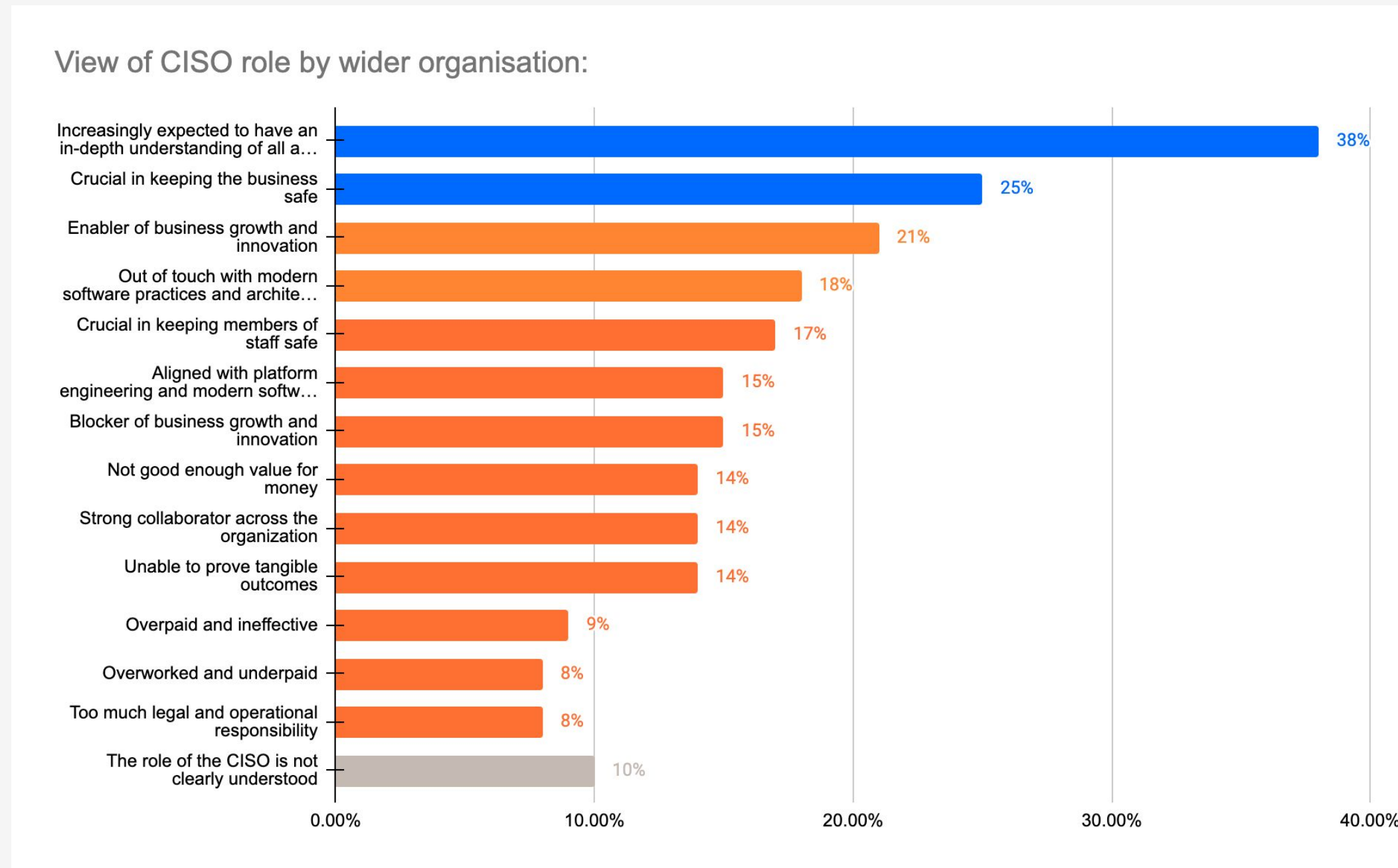
There is a wide spread of responsibility when it comes to security incidents, however, Security Managers (24%) and CISOs (23%) are most often held responsible for cybersecurity incidents



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 (38%) and are viewed as crucial in keeping the business safe (25%)

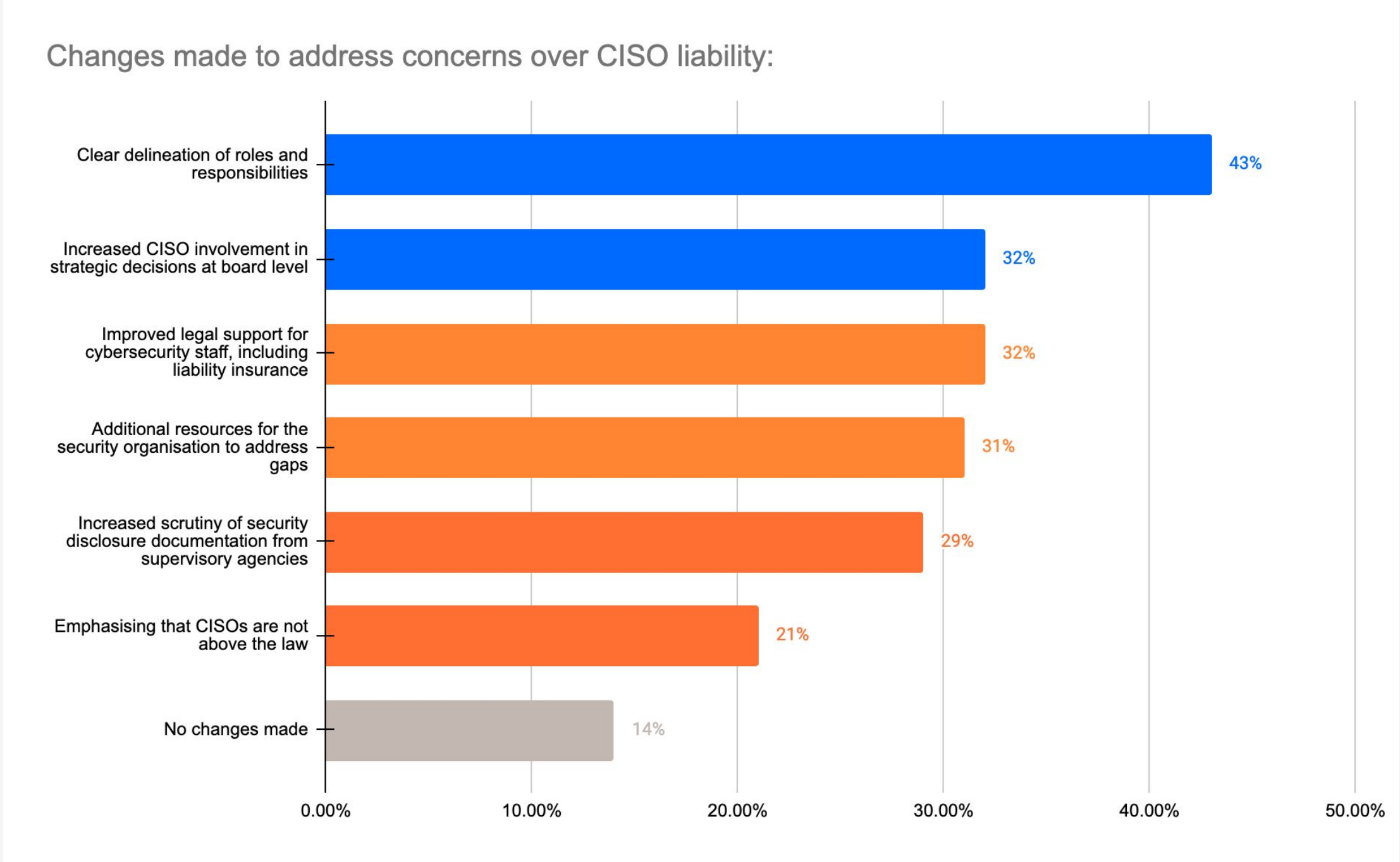


Q10. How do you think the role of the CISO is viewed by your wider organisation? Select top three | Base: 200



# Changes to Address CISO Liability

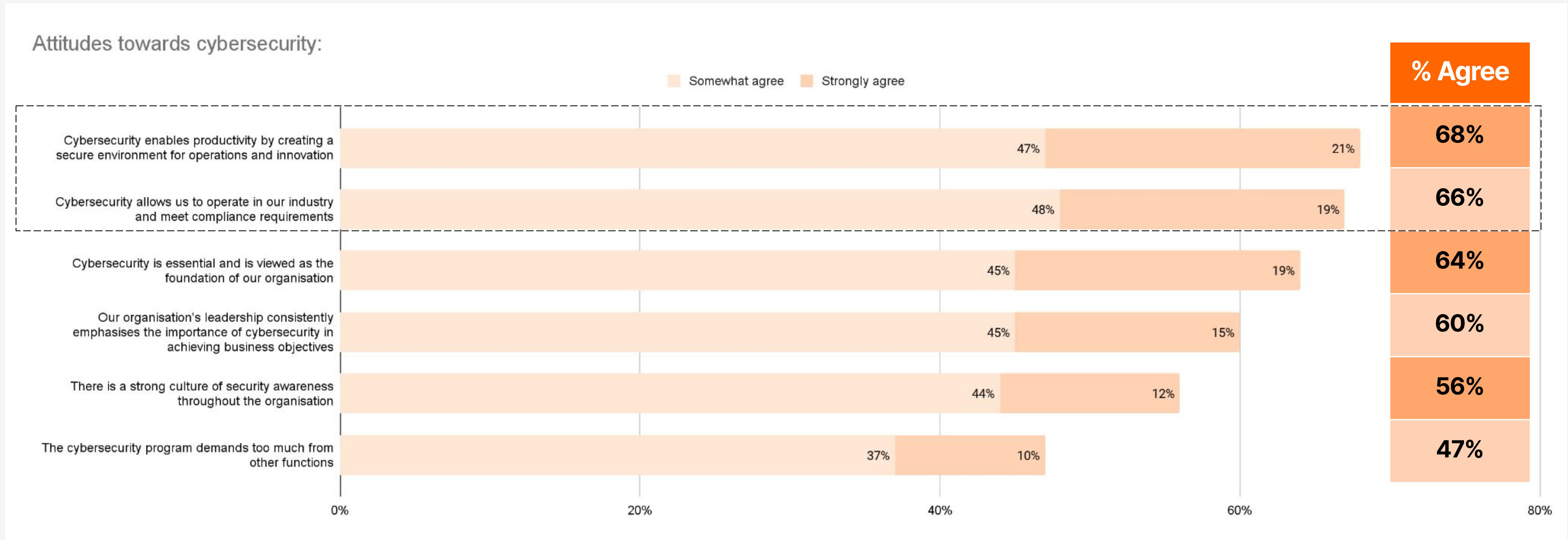
Businesses are actively addressing concerns regarding CISO liability, with 43% clearly delineating roles and responsibilities



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

# Perception of Value of Cybersecurity

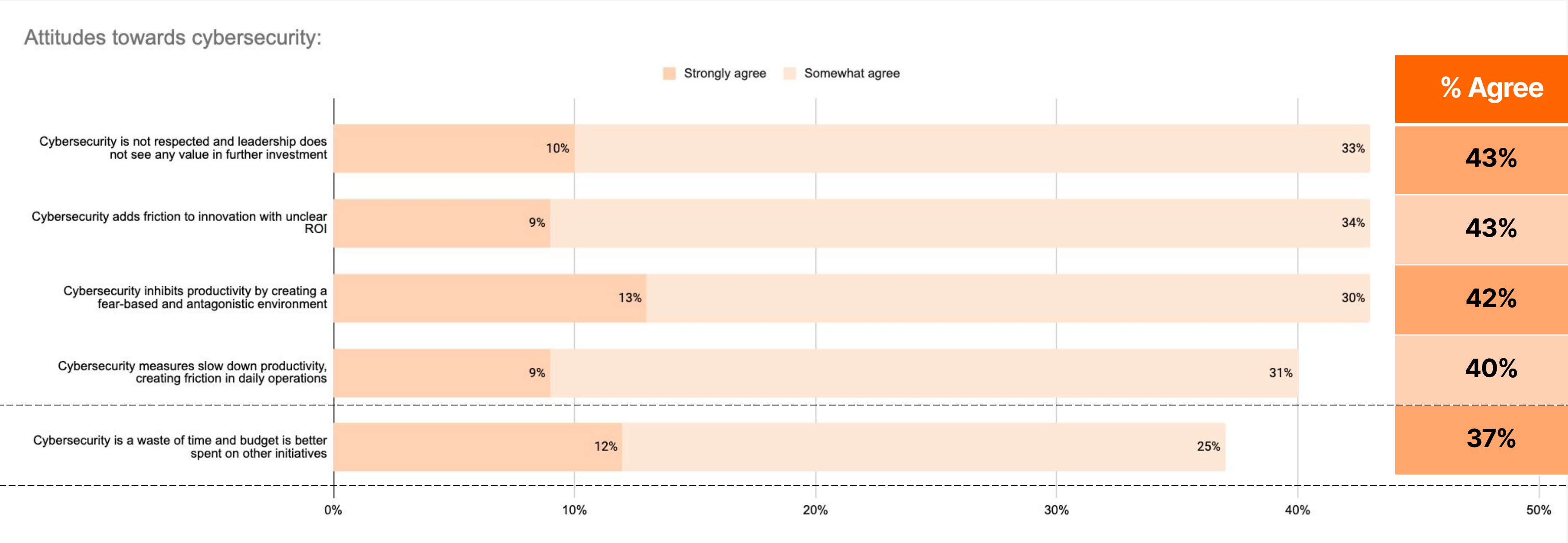
There is a strong consensus on the essential nature of cybersecurity (64%), particularly when it comes to meeting compliance requirements (66%)...



**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

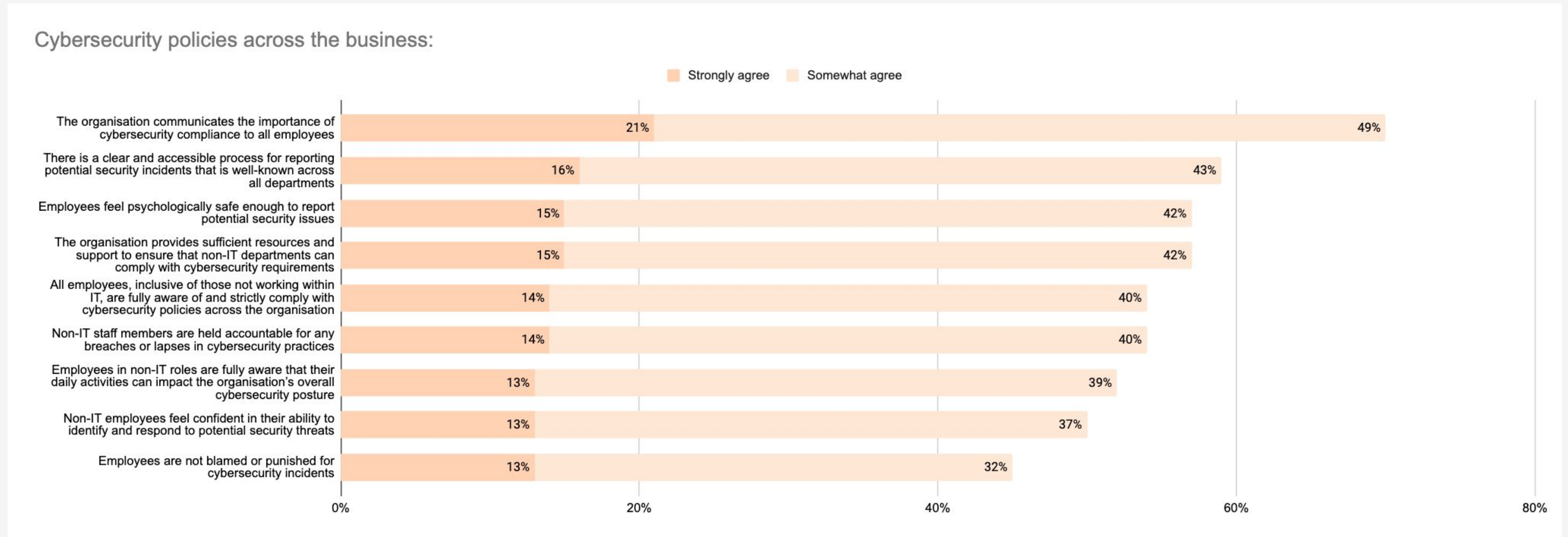
...this is further illustrated by only 37% agreeing that cybersecurity is a waste of time, and that budget would be better spent elsewhere



**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

54% of businesses have a strong culture of compliance with cybersecurity policies across all departments, facilitated by effective communication of the importance of security (70%)



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



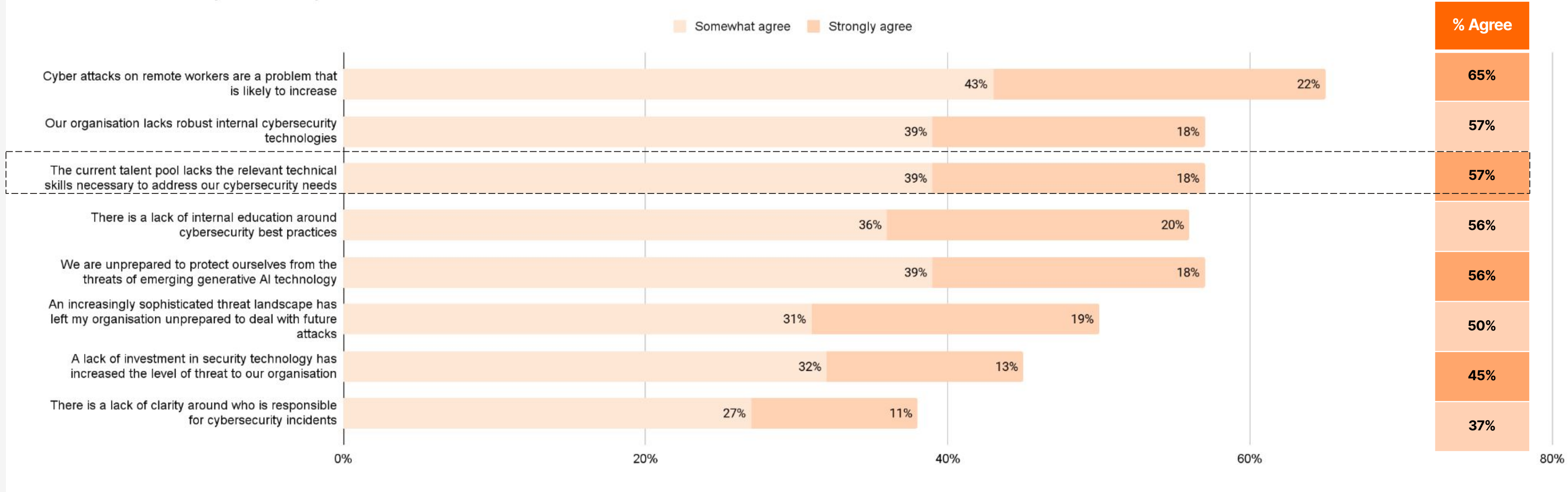
## Main Findings

# The cybersecurity talent pool

# Cybersecurity Threats

There are rising concerns over cyberattacks on remote workers (65%), an issue businesses may not be prepared for as 57% of cybersecurity decision makers think that the current talent pool lacks the relevant technical skills to address their needs

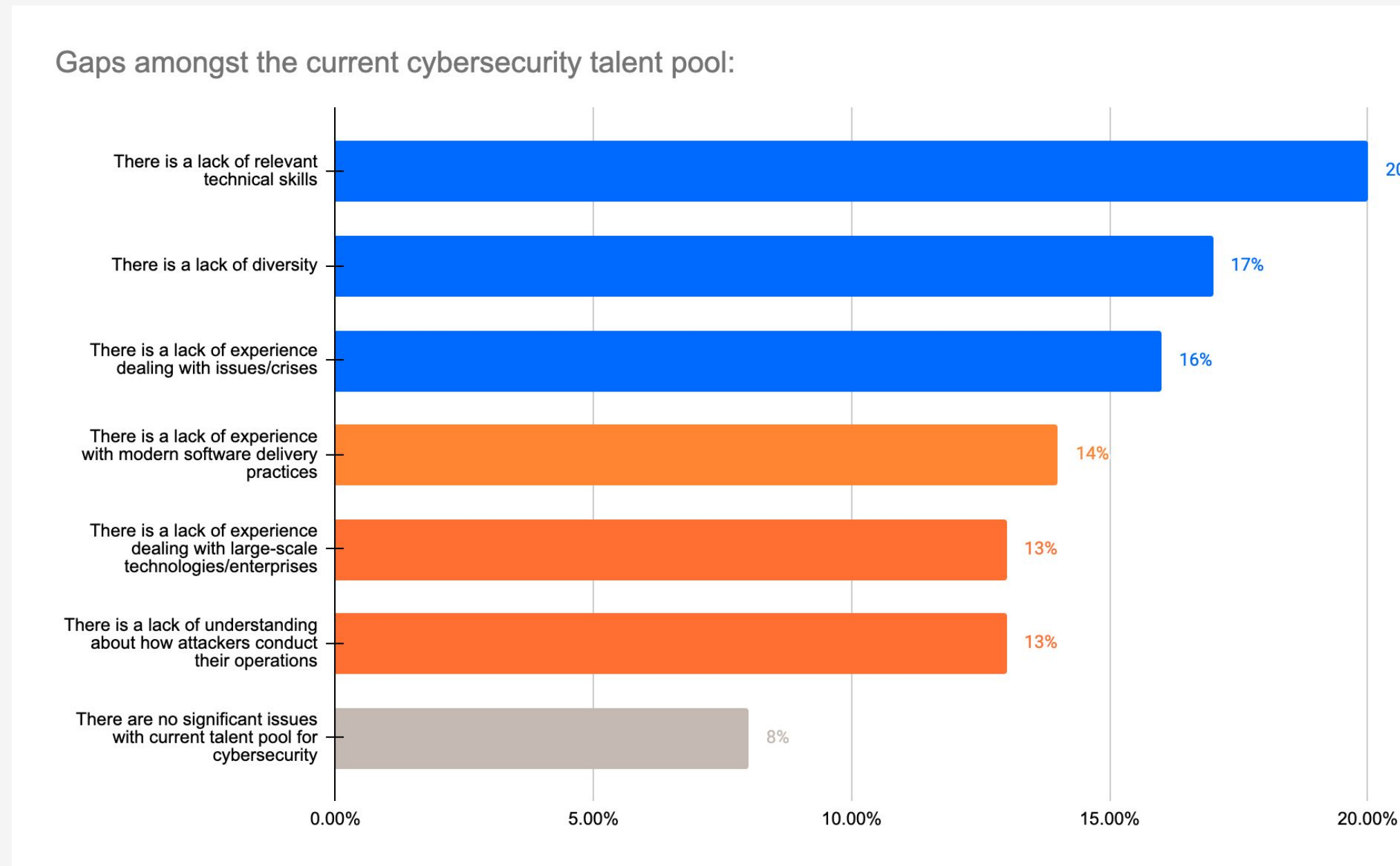
Sentiment around cybersecurity threats:



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, 92% 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

# Investment trends in cybersecurity



# Annual Spending on Web Application / API Security

On average, businesses spend \$3,147,334 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

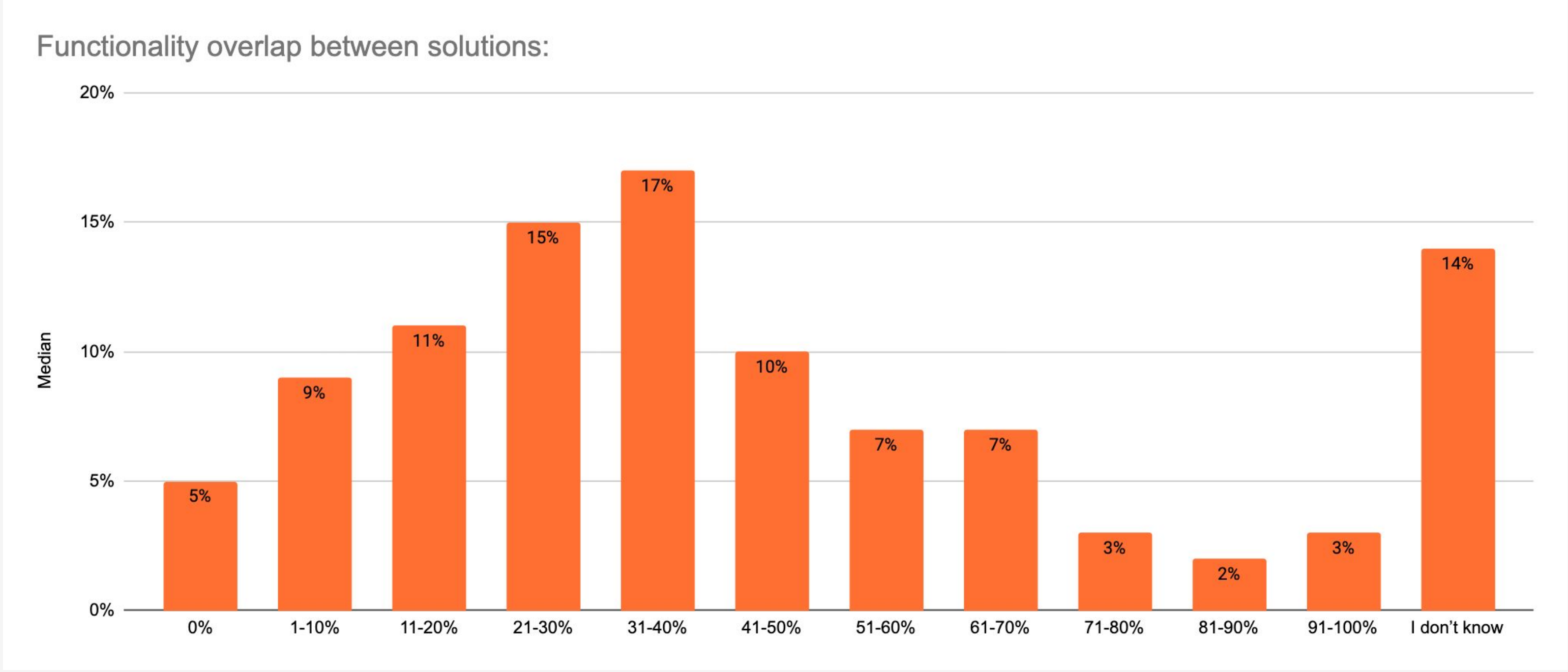


Average number of network and application cybersecurity solutions organisations rely on

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

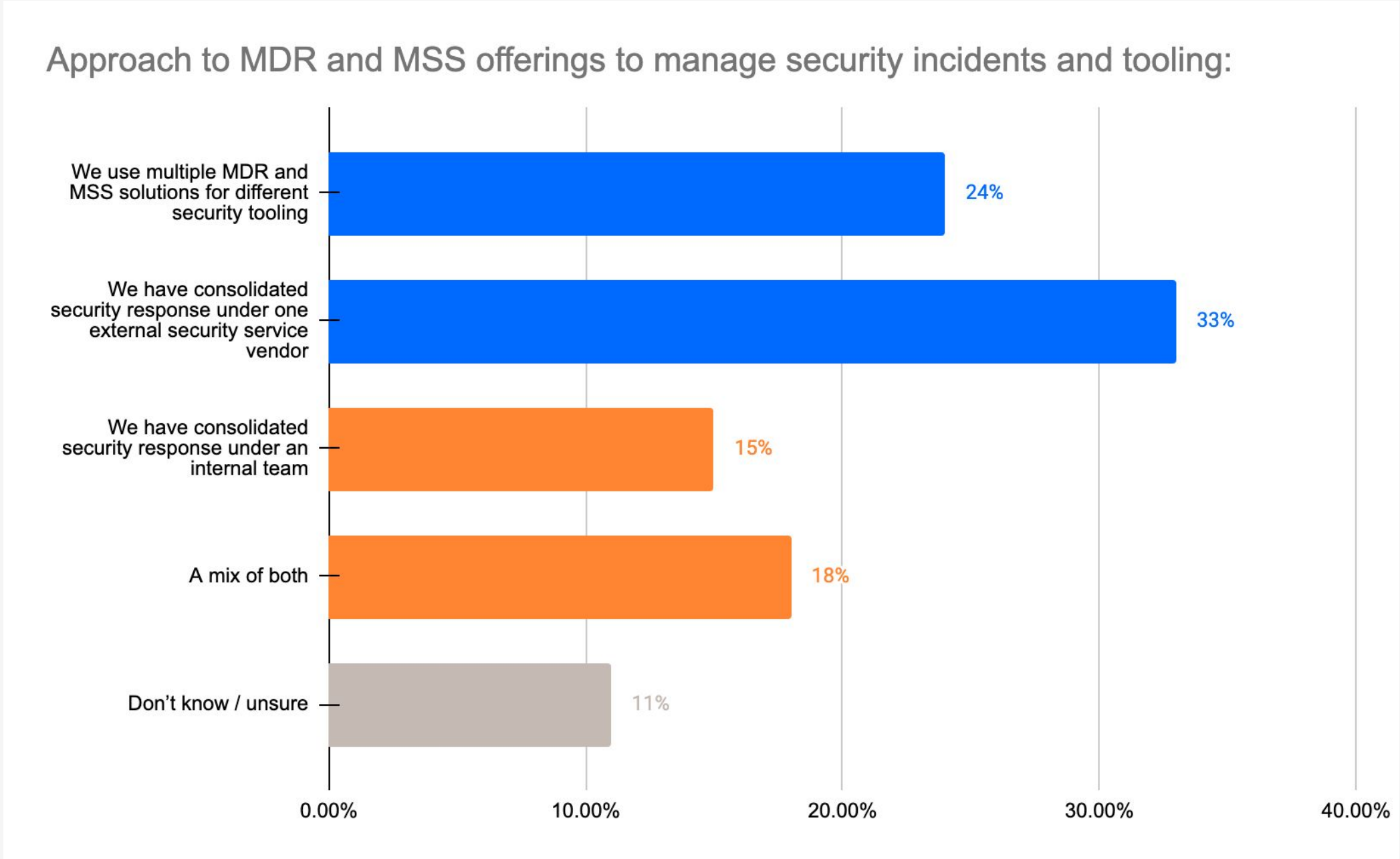
On average, 36% of these cybersecurity solutions overlap in their primary function



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

33% have consolidated their security response under one external security service vendor, whilst 24% 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

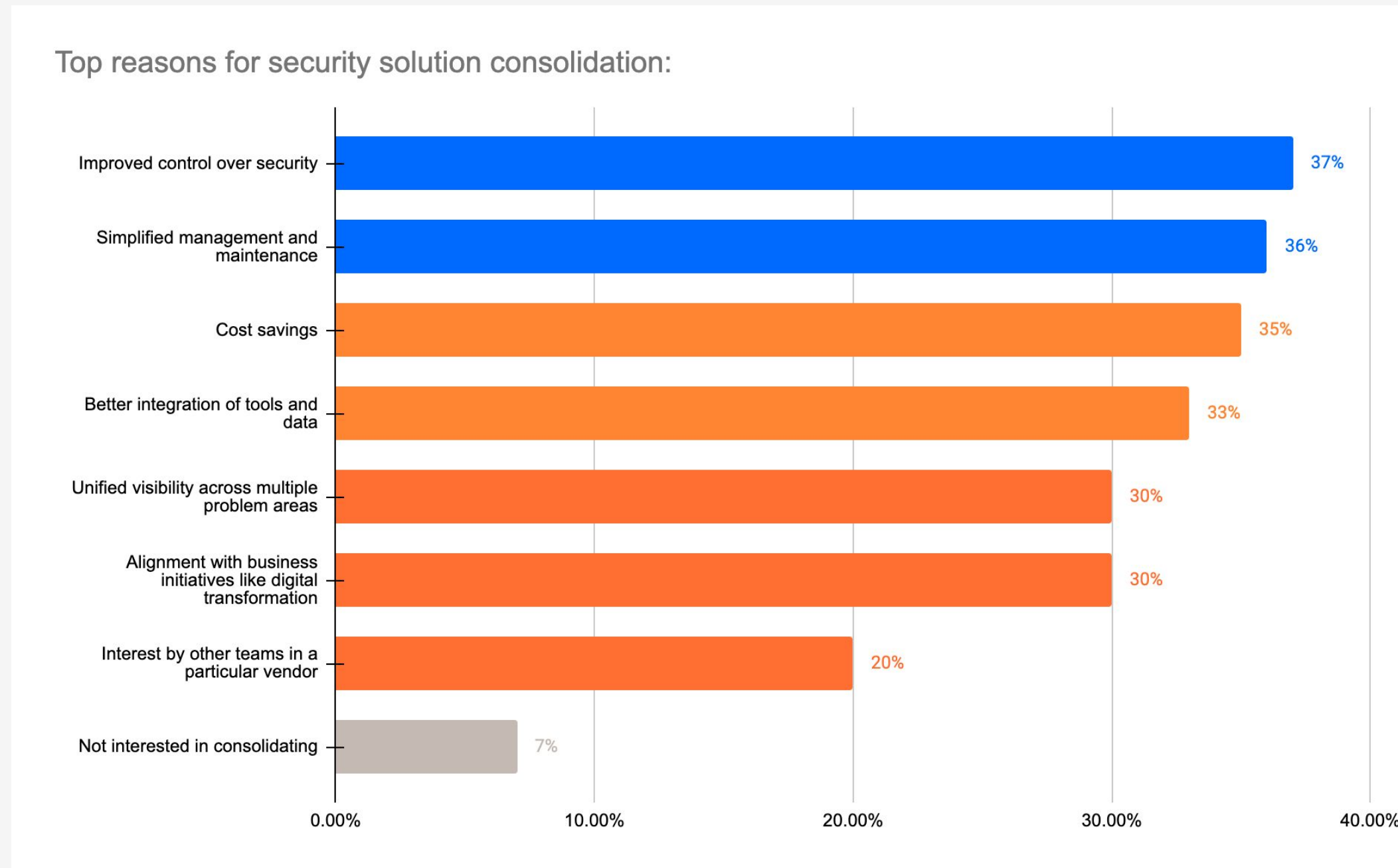


## Main Findings

# Consolidation and Integration of Security Solutions

# Reasons for Security Solution Consolidation

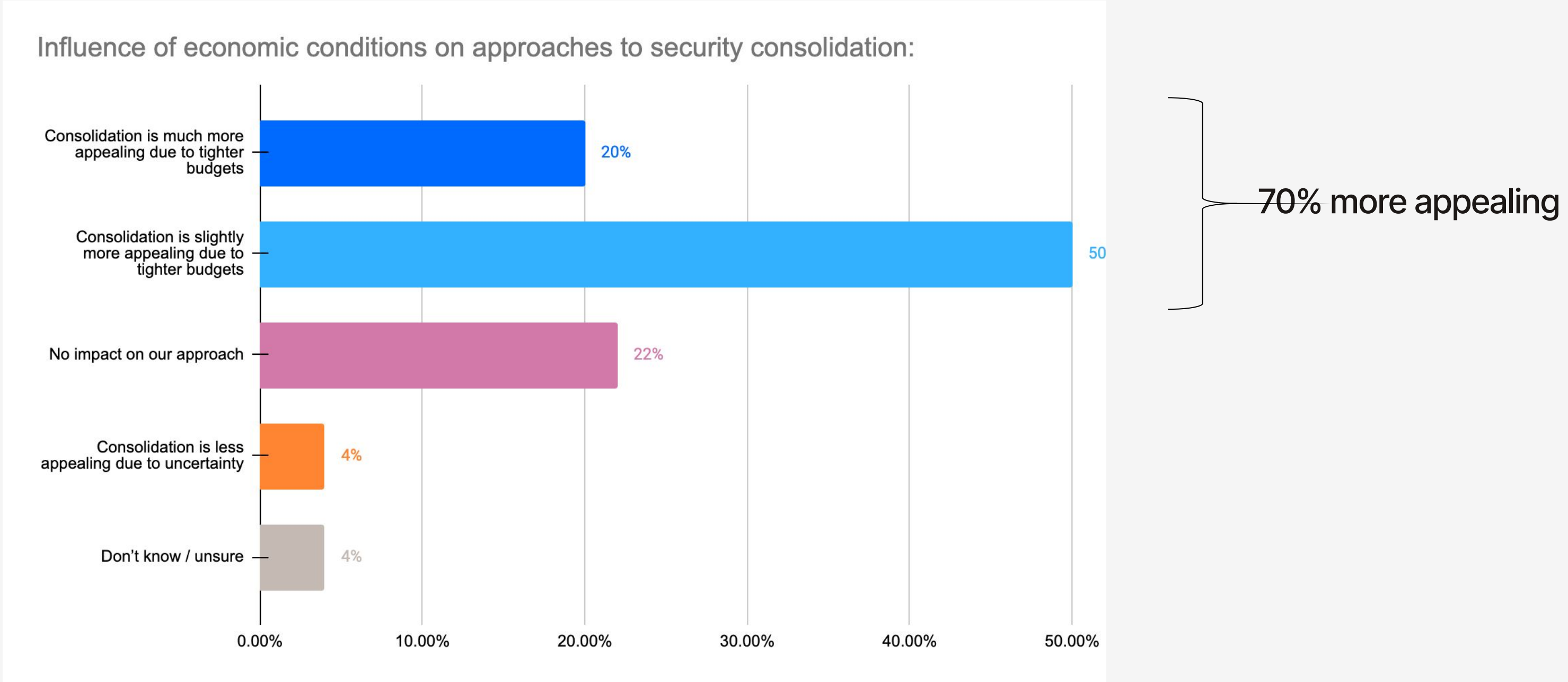
37% attribute their organisation's interest in consolidating security solutions to improving control over security, whilst a further 36% are looking to simplify management and maintenance



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

70% say that consolidation is more appealing due to tighter budgets

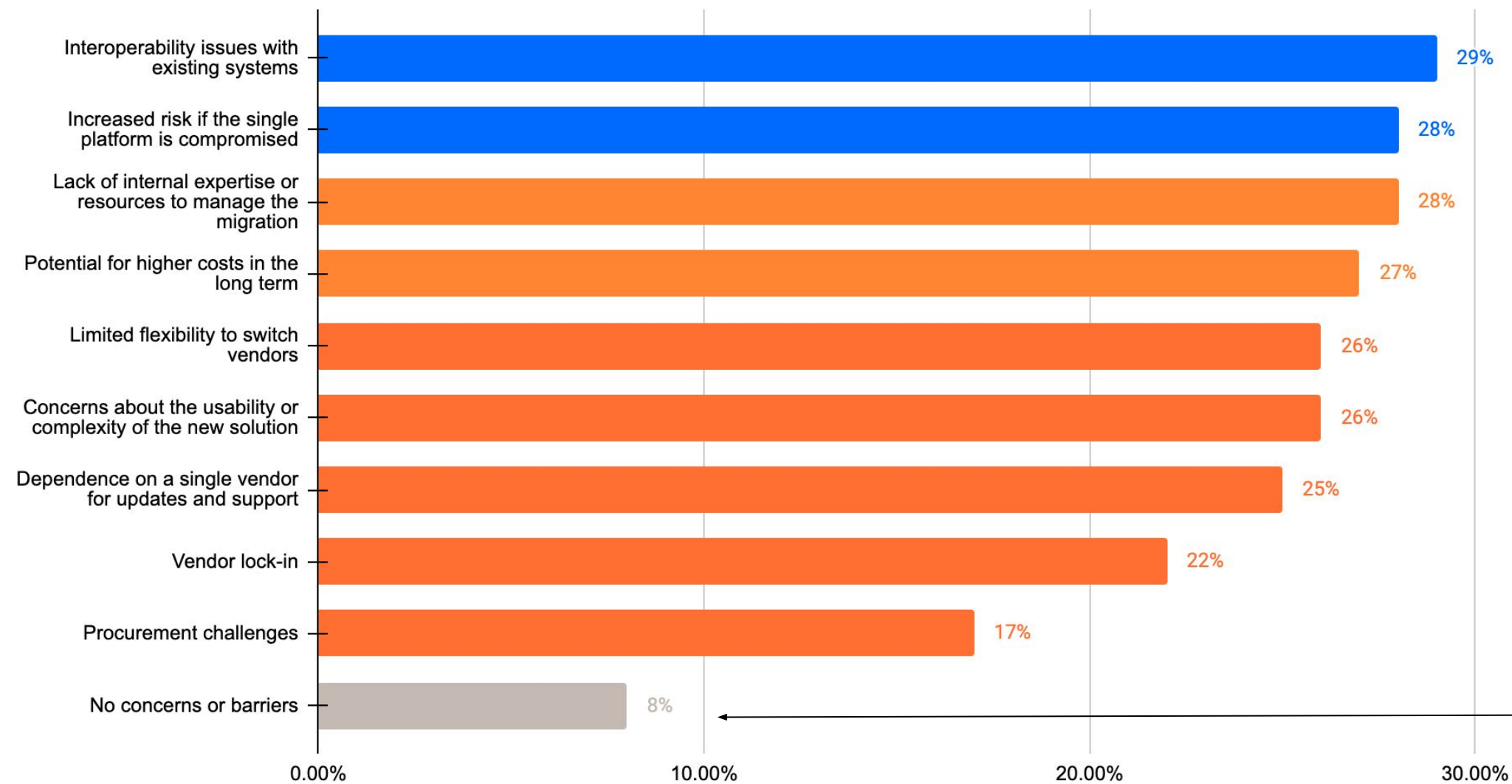


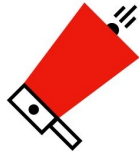
Q23b. How have economic conditions influenced your organisation's approach to security consolidation? Select one | Base: 187

# Concerns with Security Tool Consolidation

29% are concerned about interoperability issues when it comes to consolidating security tools, shortly followed by the concern about increased risk if the single platform is compromised (28%), and the lack of internal expertise (28%)

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



 **92%** of businesses have concerns or are facing barriers when it comes to security tool consolidation

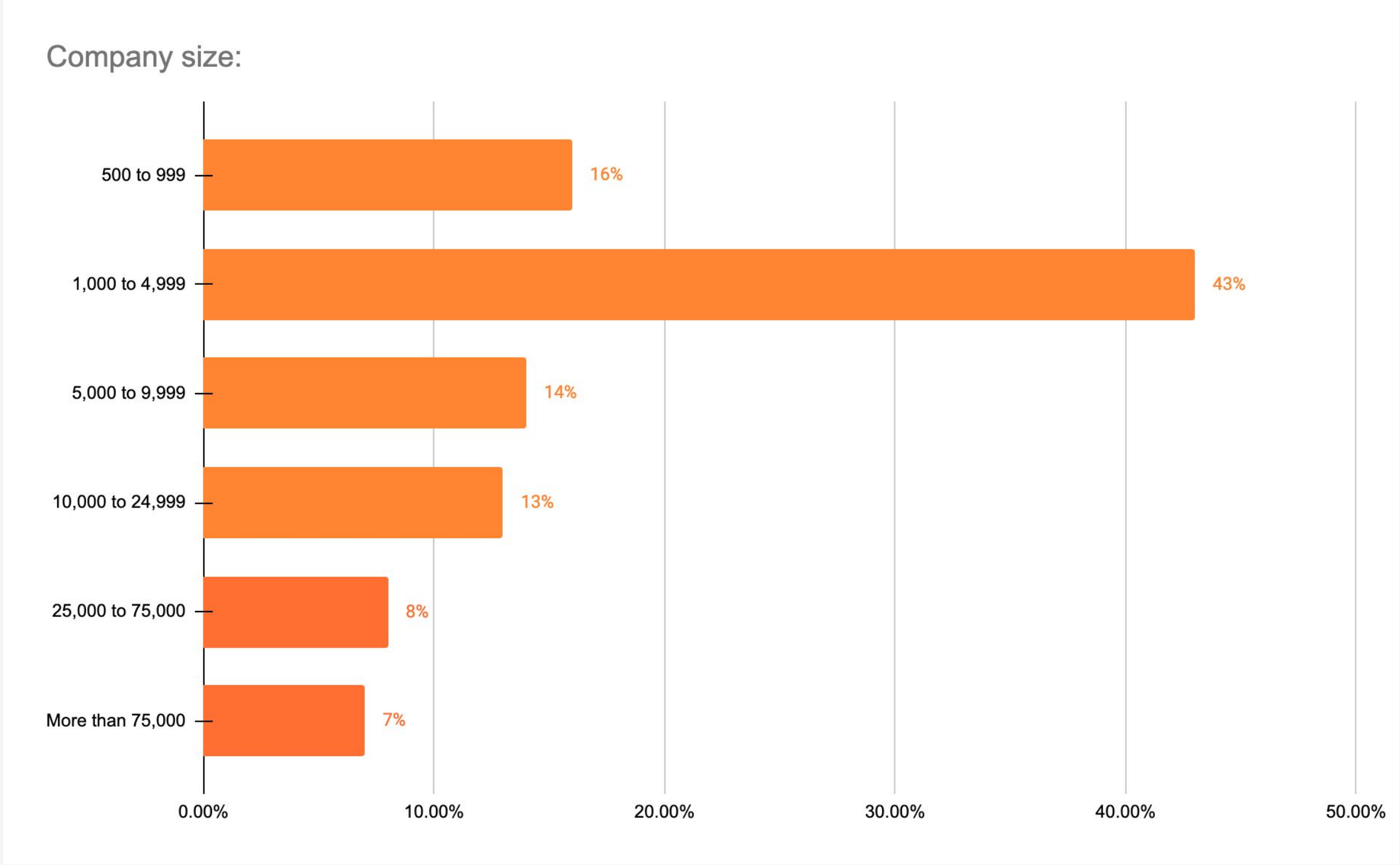
**Q24b. What are the concerns or barriers to consolidating your security tools onto a single platform/vendor, or switching to a new security solution? Select all that apply | Base: 200**



# Demographics



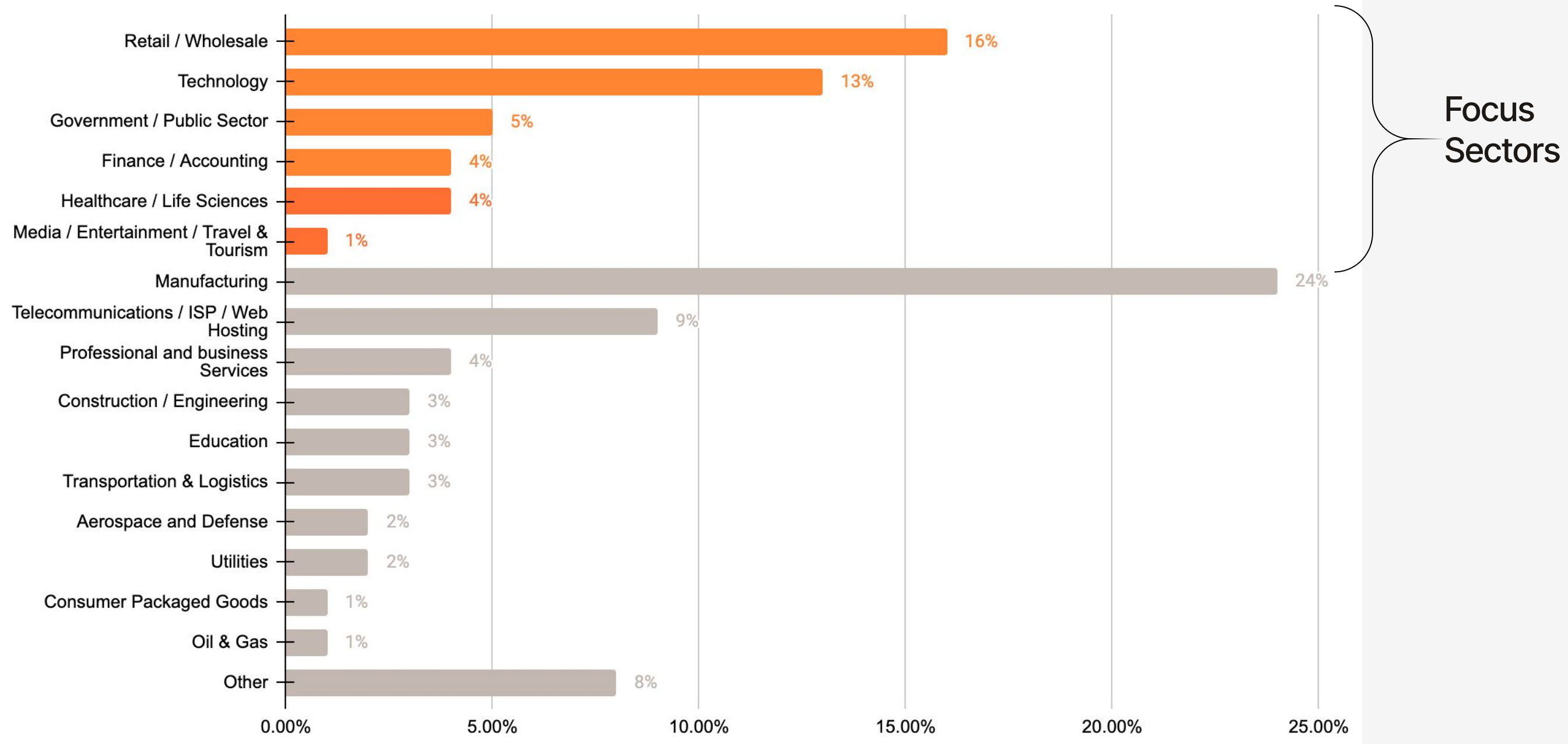
# Company size



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

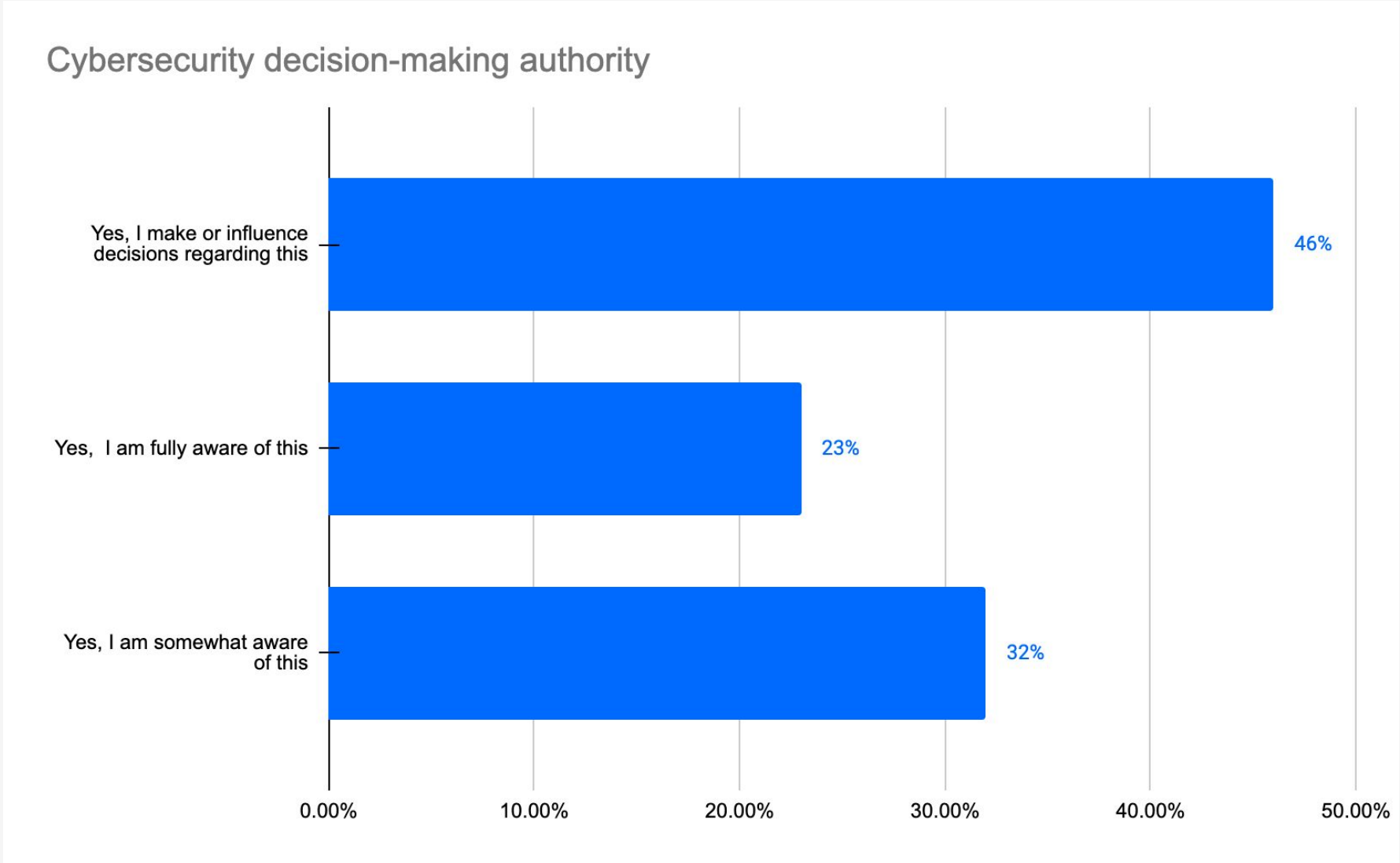
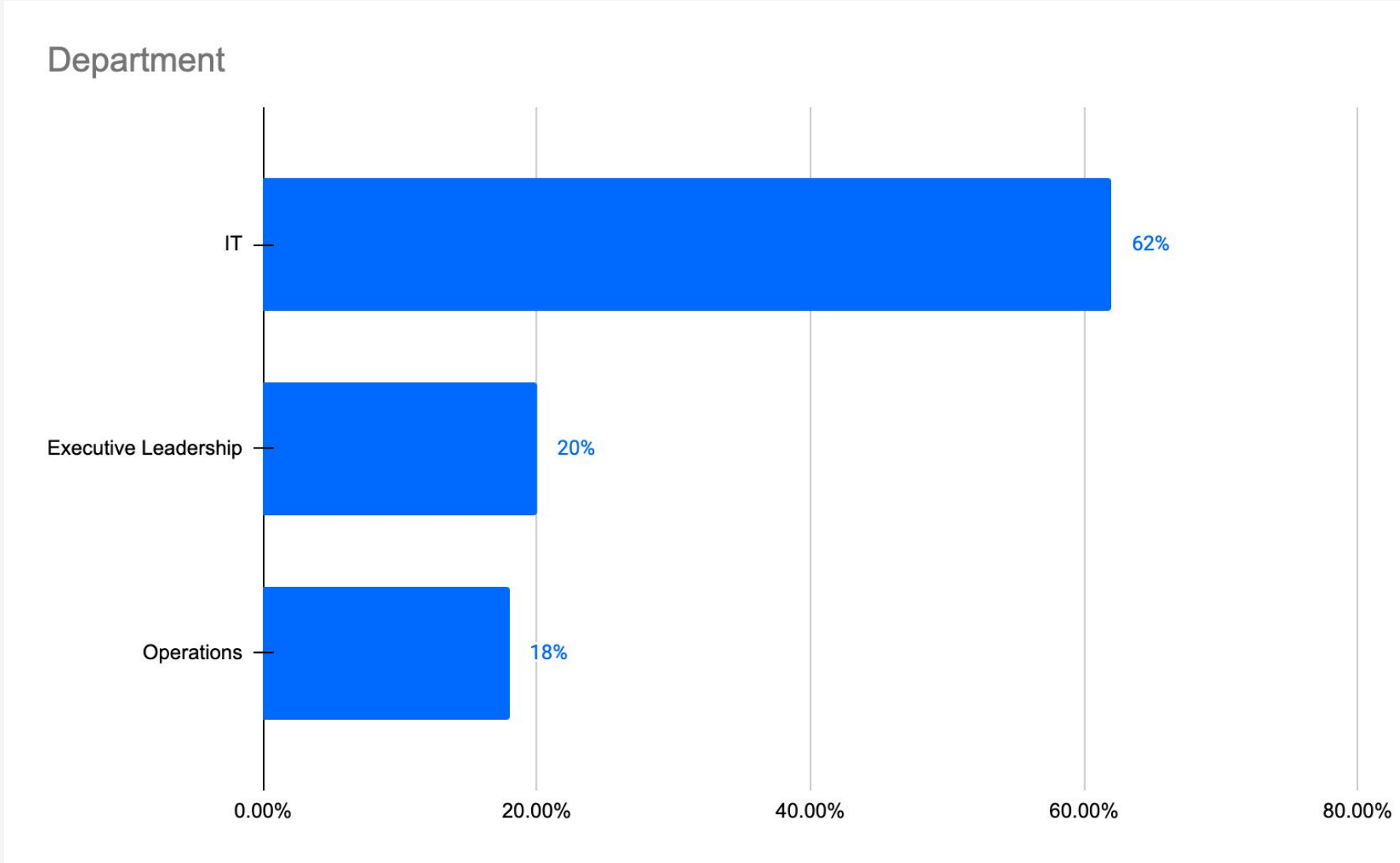
# Industry

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**<sup>®</sup>