fastly

Fastly Global Security Research 2024

Global Findings

November 2024

Research conducted by
SAPIO Research

Overview & methodology

The survey was conducted globally among 1800 cybersecurity decision makers (with 2/3 respondents directly making or influencing cybersecurity decisions) in businesses with more than 500 employees (250+ employees in Australia and New Zealand). Participants came from a range of roles across the IT, Operations and Executive Leadership functions.

At an overall level results are accurate to ± 2.3% at 95% confidence limits assuming a result of 50%.

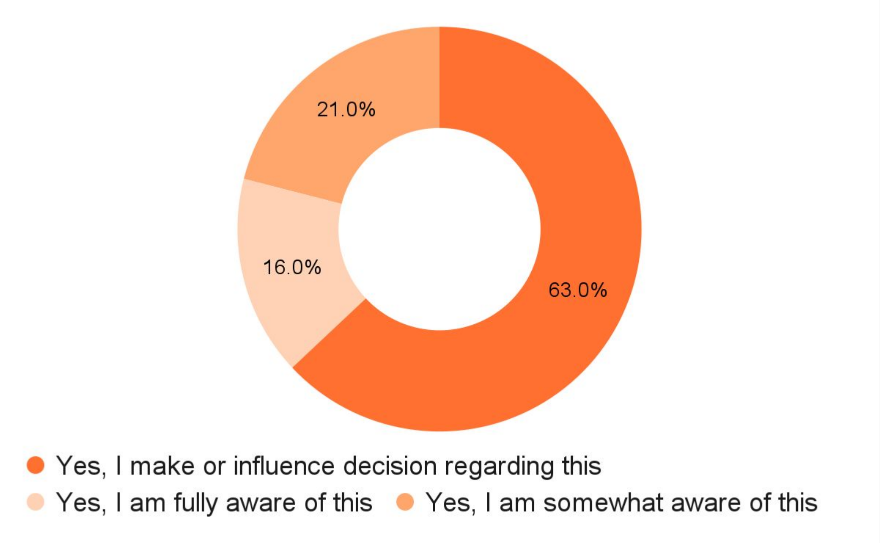
The interviews were conducted online by Sapio Research in September 2024 using an email invitation and an online survey

Respondent demographics summary – Cybersecurity Decision Makers

Seniority

Department	% of respondents
IT	51%
Operations	27%
Executive leadership	22%

Decision-making



Company Size

No of employees	% of respondents
250-999	22%
1.000-4.999	35%
5.000-24.999	26%
25.000+	17%

Primary sectors of Business

1. Retail / Wholesale - 12%
2. Technology - 11%
3. Finance / Accounting - 11%
4. Healthcare / Life Sciences - 11%
5. Media/Entertainment / Travel & Tourism - 11%
6. Government / Public Sector - 11%

Country of residence

Nordics

LATAM

UK / Ireland

Japan

DACH

AUS / NZ

US

Spain

France

Key takeaways

Key stats

Companies expect it to take **5.85 months** to recover from security incidents

Businesses have experienced **~40** security incidents in the past year, with the top factors present being **external attackers (38%)** and **software bugs (33%)**

Businesses report being reliant upon an average of **8** cybersecurity solutions, with **38%** of these cybersecurity solutions overlapping in their primary function

Organisations predict that **social engineering attacks (37%)** and **ransomware and extortion (34%)** will be their biggest cybersecurity threats in the next 12 months

Revenue loss was one of the top impacts of security incidents **(23%)**, with those reporting this suffering an average **2.98%** loss following a security incident

Almost three quarters (73%) say that consolidation of security solutions **is more appealing** due to tighter budgets

Summary & overview

1. **Response to Recent Reliability Incidents:** Following recent reliability incidents, businesses are taking a **more cautious approach** to updates and patches. We see this trend continue when it comes to re-evaluating current cybersecurity vendors and tools, with a number of businesses **considering changing vendors**. This highlights the anxiety felt by businesses as they try to navigate a landscape of constantly evolving security threats. Recovery times are **long** and use significant resources.

2. **The Impact and Aftermath of Security Incidents**: On average, businesses have experienced **40 security incidents** in the past 12 months, with the top factors present being external attackers and software bugs. The greatest impacts of these incidents are **downtime or outages** and **data loss**. Revenue loss was also a top impact, with those reporting this suffering an average **2.98% loss** following a security incident, highlighting the financial ramifications of inadequate security measures. Despite these challenges, organisations are taking proactive steps towards improving their security status following incidents, with a particular focus placed upon **training employees to reduce the skills gap**. Those suffering from DDoS attacks feel **poorly equipped** to deal with the issue. Rising automation and Generative AI skills gaps remain of **significant concern**.

3. **The state of cybersecurity and future threats:** Cybersecurity professionals predict social engineering attacks will be the biggest threat in the future, closely followed by ransomware and extortion. This highlights a significant shift towards **human-centric vulnerabilities**, where attackers exploit **psychological factors**. The top drivers of cybersecurity threats are centered around the **evolving digital landscape**, highlighting the importance that organisations cybersecurity functions are **adaptable to a dynamic threat**.

Summary & overview

4. **Shifting accountability :** There is still a lack of clarity within organisations as to who exactly is responsible for cybersecurity incidents. The rise in accountability across teams like application developers, platform and site reliability engineers suggests that responsibility for cybersecurity incidents is no longer siloed within security-specific roles. Organisations feel generally confident in the resources provided to the wider organisation to deal with lapses, but remote workers remain vulnerable and internal education is not universally sound.

5. **Investment in Cybersecurity**: The majority of decision makers are expecting their investment in cybersecurity to **increase** in the coming 12 months, particularly in technologies related to **modern authentication** and **cyber insurance**. This investment is reported to be aligned with businesses revenue and growth goals, demonstrating that **cybersecurity is becoming intertwined with strategic decision-making**. Investment in tools is high, however, this comes with the caveat of businesses having several security solutions with significant overlap between functionalities.

6. **Consolidation of Security Solutions**: Organisations desire **improved control over security** and **better integration of tools and data**, believing that consolidating their security solutions will help them reach these goals. Cost is a strong driver of consolidation with the majority reporting that consolidating is becoming **more appealing with tighter budgets**. However, consolidation comes with its concerns, particularly around the **risk of the platform being compromised**, and the potential for **higher costs** in the long-term.

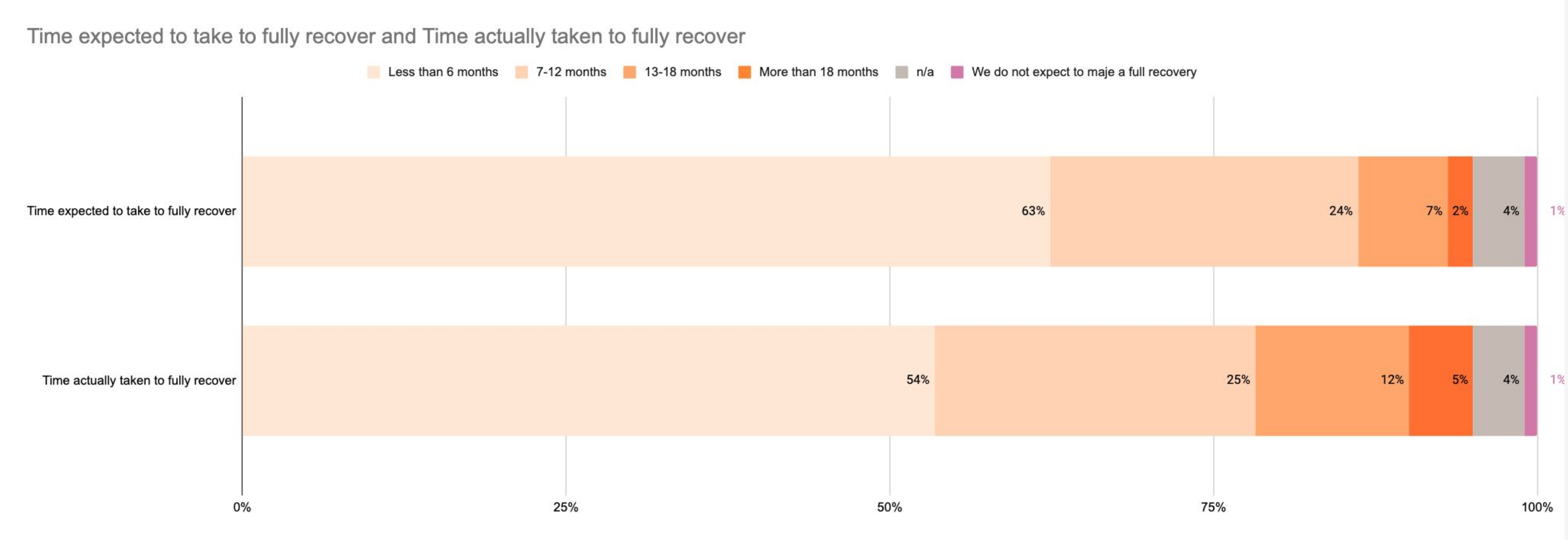
Main findings

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



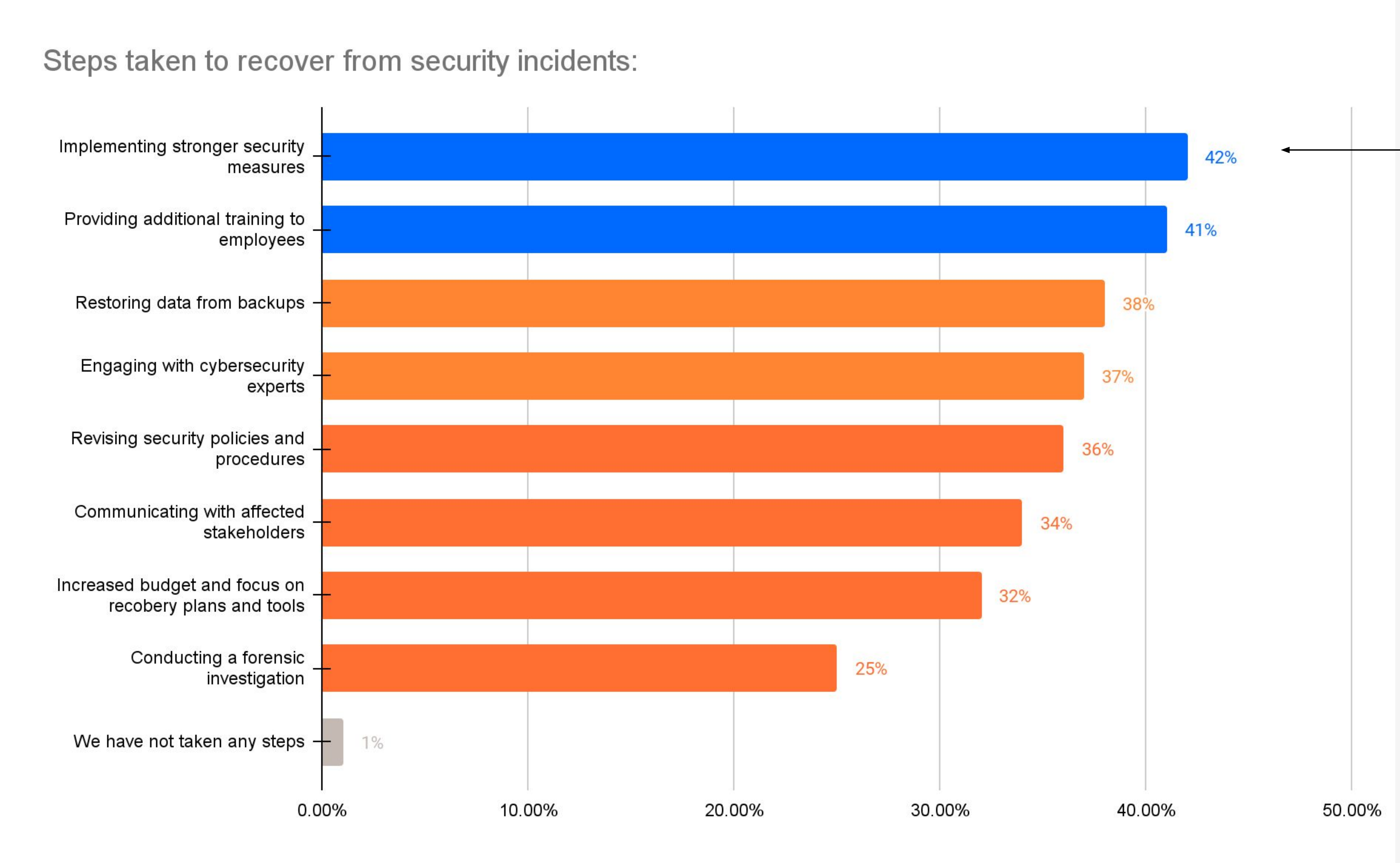
Mean: 5.9 months

Mean: 7.3 months

Q17e. How long do you expect it to take, and how long has it taken, to fully recover from each of these impacts? | Base: 1632 *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 **implementing stronger security measures (43%) and providing additional training to employees (41%)**



49% in Technology,
37% in Government / Public Sector

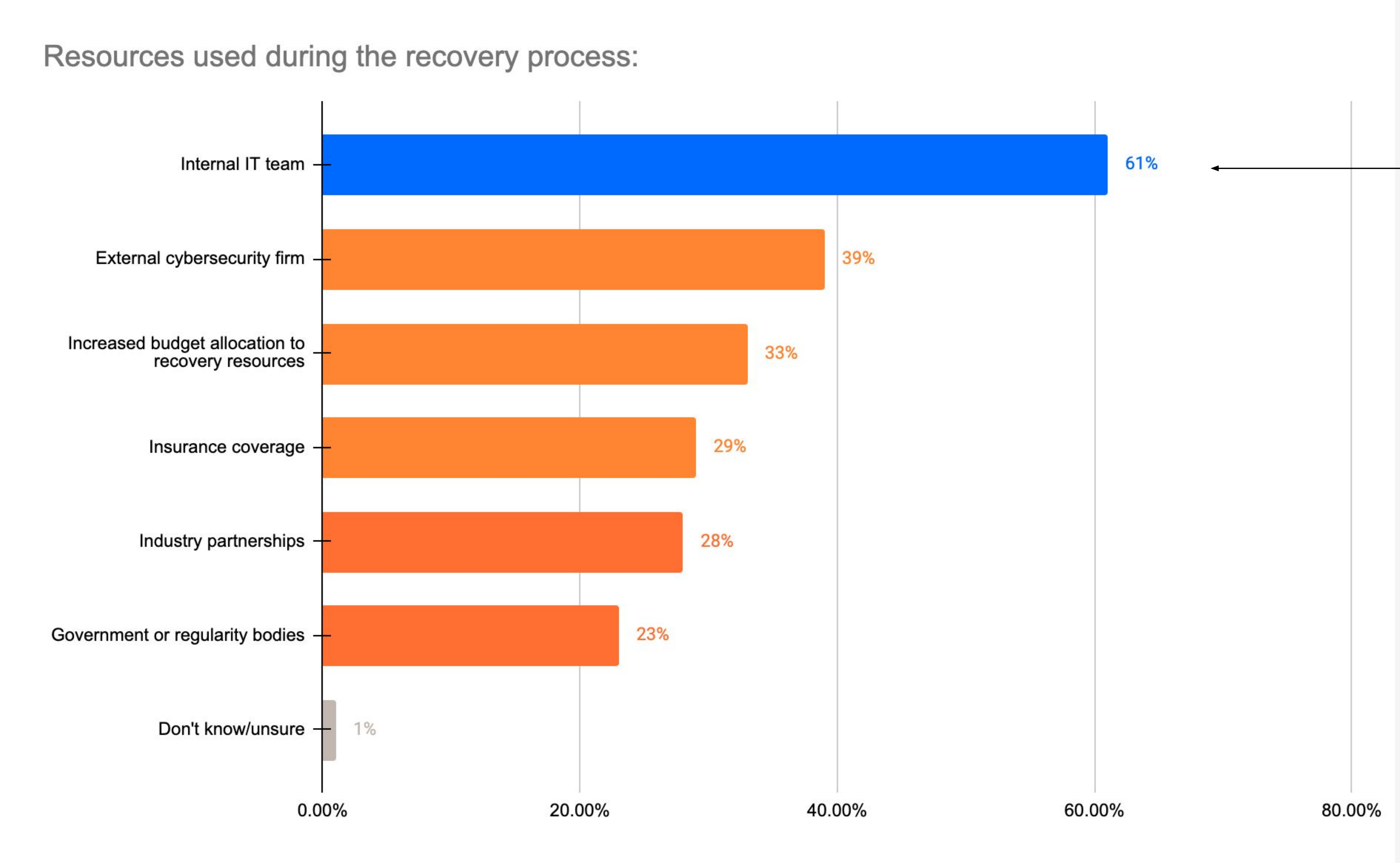
Businesses are taking a proactive approach towards improving their security status following cybersecurity incidents.

A particular focus is placed upon training employees to reduce the skills gap.

Q18. What steps has your business taken to recover from the security incident? Select all that apply | Base: 1632 *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 (61%)** for recovery following a security incident



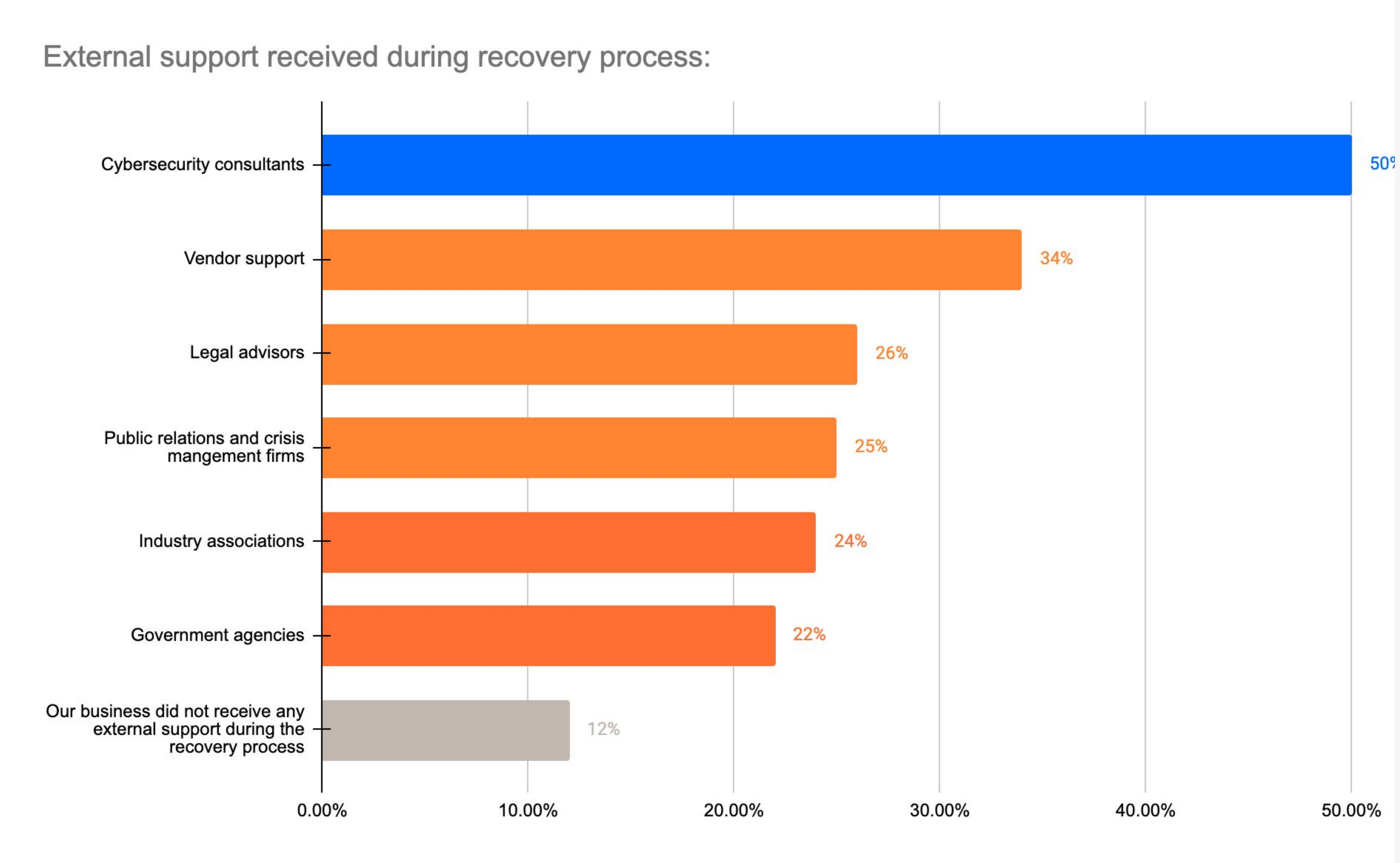
63% in organisations with 250-999 employees,
57% in organisations with more than 25,000 employees

Smaller businesses place greater reliance upon internal resource

Q19. What resources did your business use for recovery? Select all that apply | Base: 1611 (only asked to those who have taken step towards business recovery)

External Support During Recovery

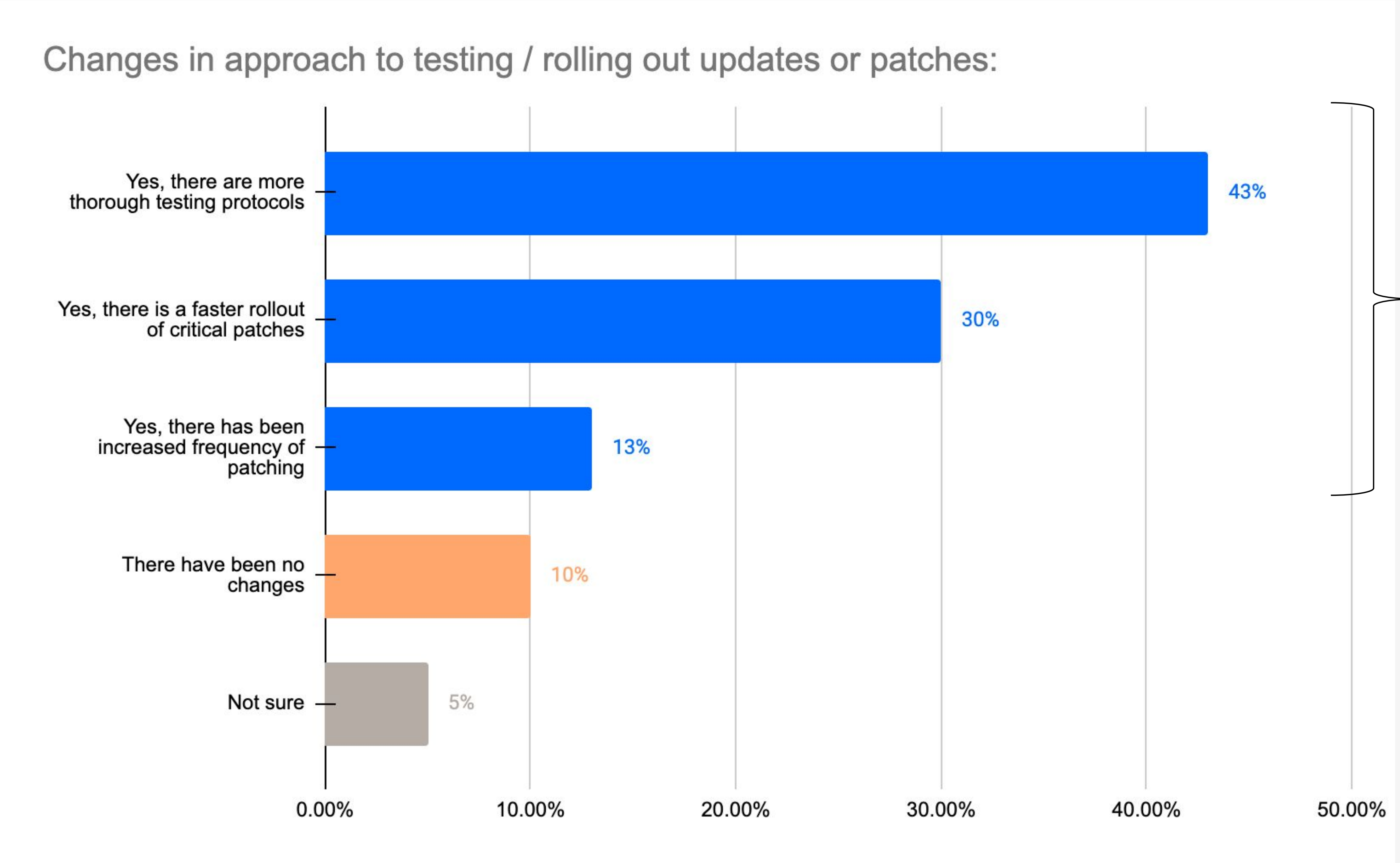
Half say their business utilised **cybersecurity consultants** during the recovery process



Q22b. What external support or assistance, if any, did your business receive during the recovery process? Select all that apply | Base: 1800

Changes in Approach to Updates and Patch Testing

86% report that recent reliability incidents have encouraged their business to **change their approach** to testing or rolling out updates or patches



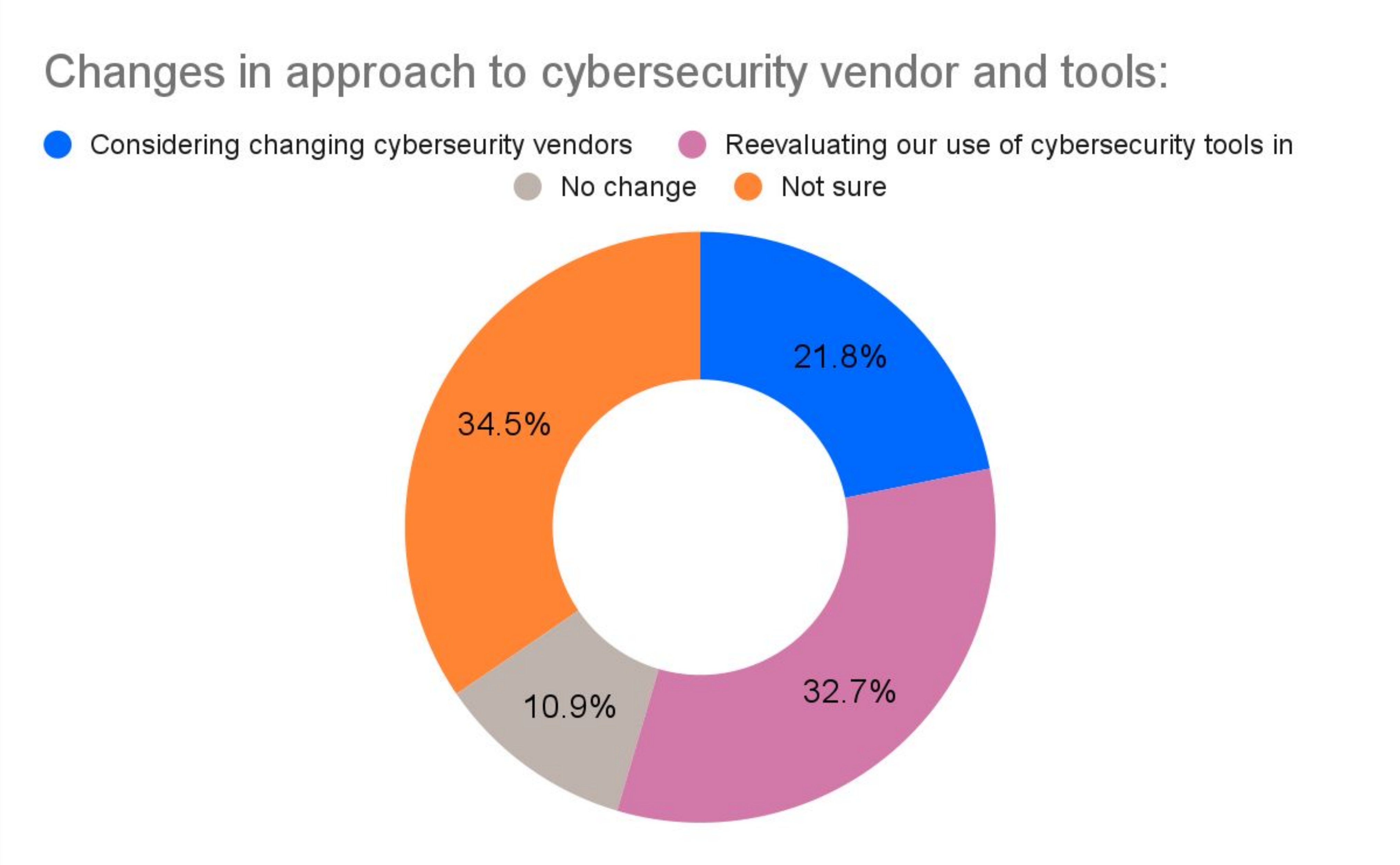
86% yes

92% in Technology,
70% in Government / Public Sector

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: 1800

Approach to Cybersecurity Vendors and Tools

Almost half (48%) are **re-evaluating their use of cybersecurity tools in general**, following the recent Crowdstrike outage, with a further **29% considering changing cybersecurity vendors**



Following the Crowdstrike outage, organisations are becoming more cautious when it comes to cybersecurity vendors and tools.

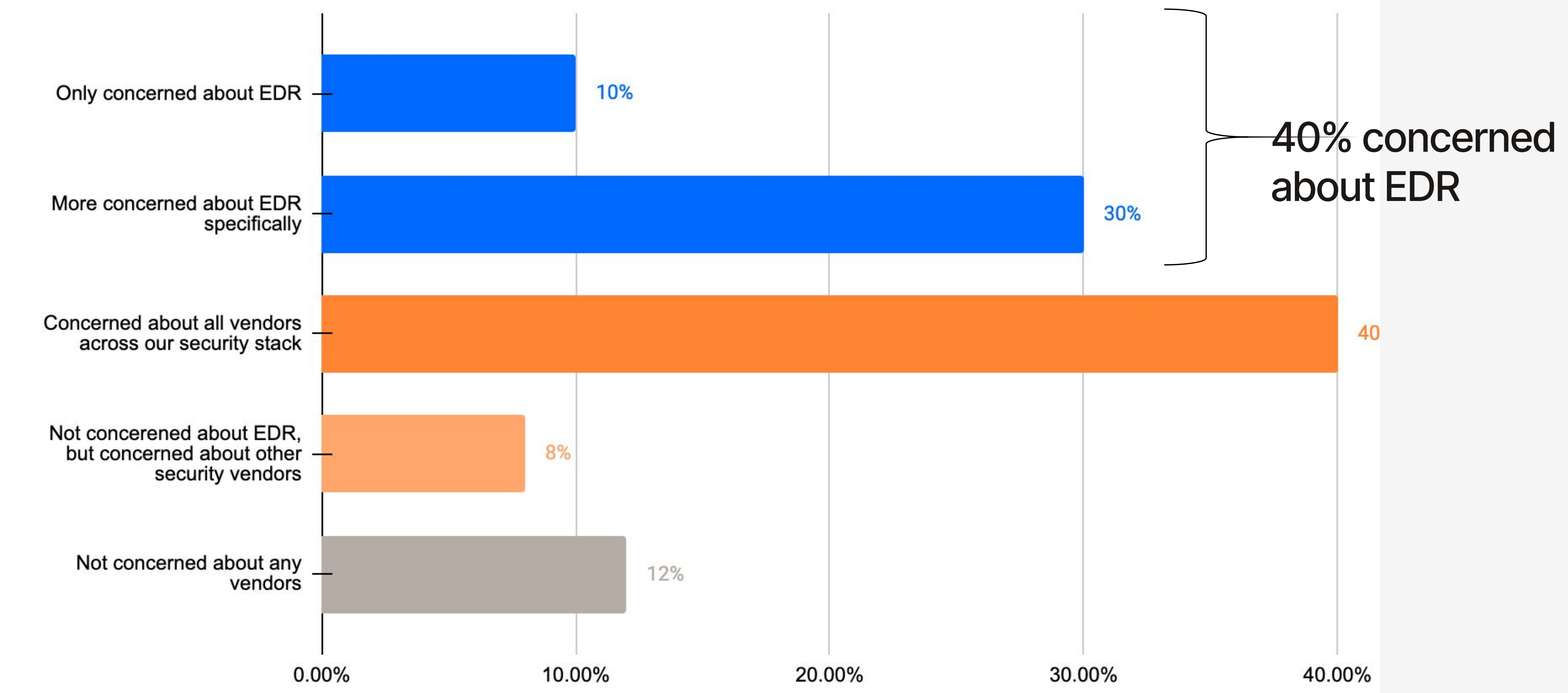
The outage has generated wide-spread anxiety leading to businesses re-evaluating their options when it comes to security

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: 1800

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 (40%)** and those **more concerned about EDR (40%)**

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



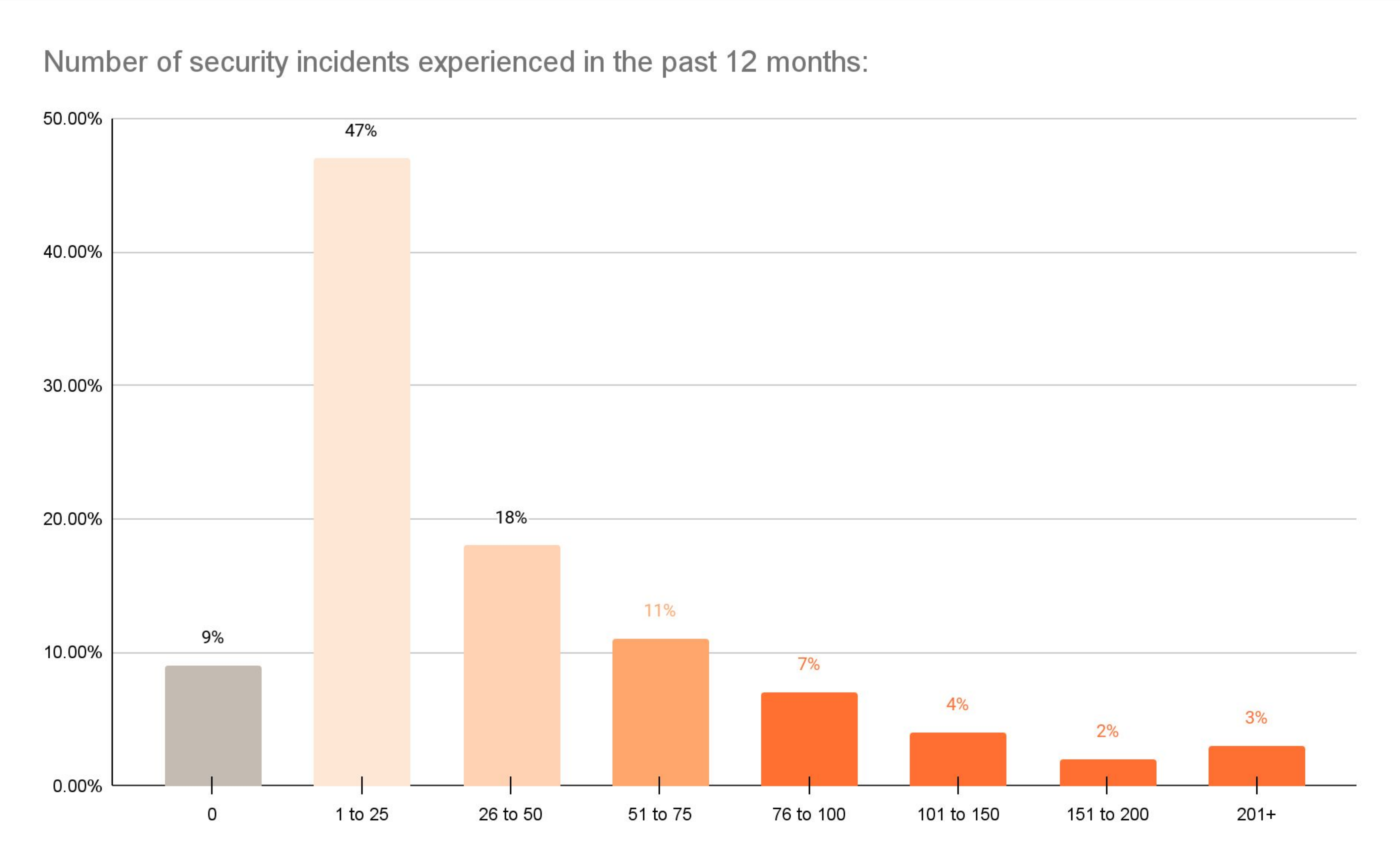
Q22a. In response to the Crowdstrike outage, to what extent are you concerned about reliability and software quality issues in EDR vendors vs all cybersecurity vendors? Select one | Base: 1800

Main Findings

The attack landscape

Number of Security Incidents in the Past Year

On average, businesses have experienced **40 security incidents** in the past 12 months, increasing to 47 in the Finance / Accounting sector



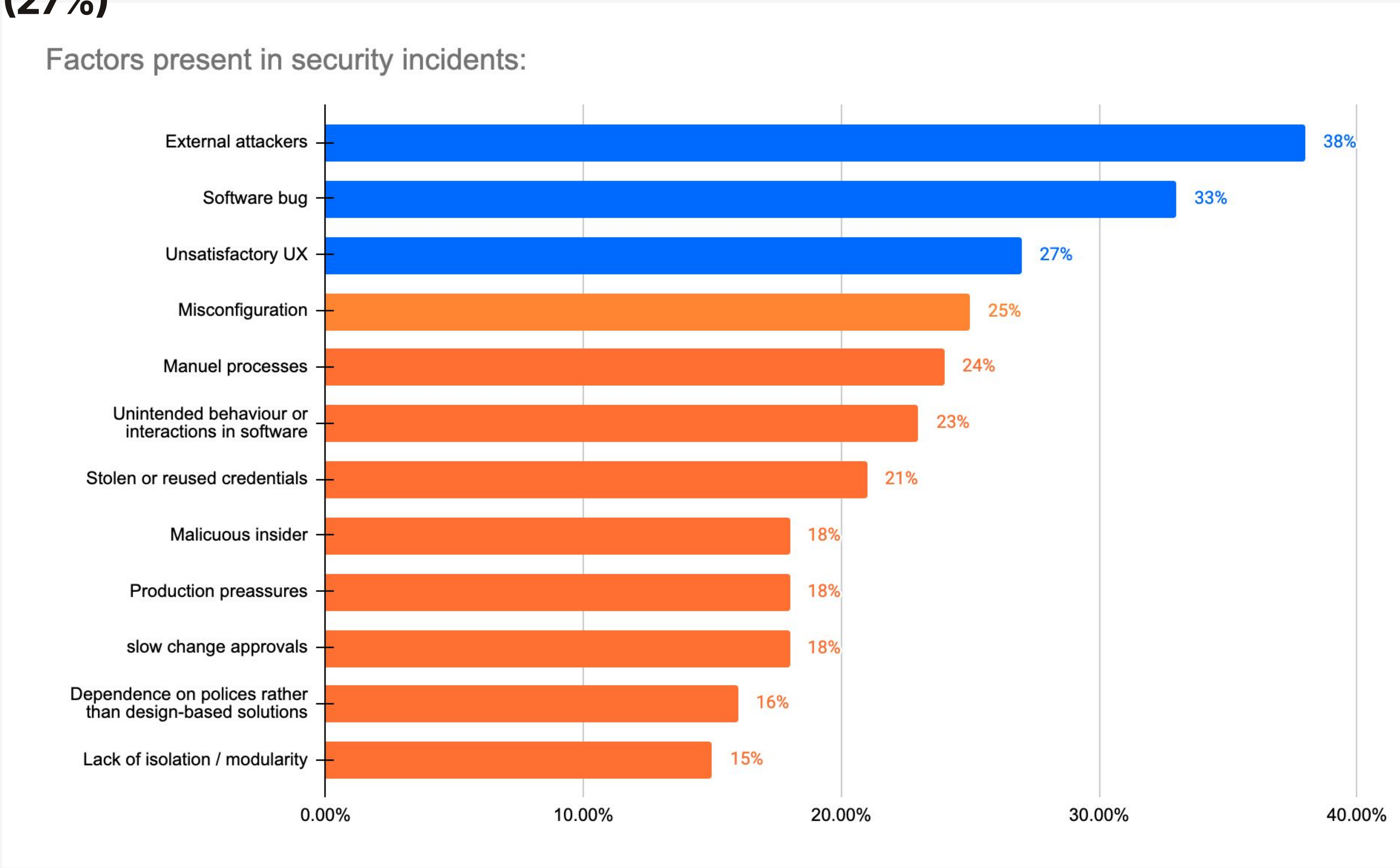
Sector	Mean
Finance / accounting	47
Government / Public Sector	42
Technology	41
Media / Entertainment / Travel & Tourism	36
Retail / Wholesale	33
Healthcare / Life Sciences	29

Mean: 40

Q15. How many security incidents, including those caused by human error, has your business experienced in the past 12 months? Select one| Base: 1800

Factors Present in Security Incidents

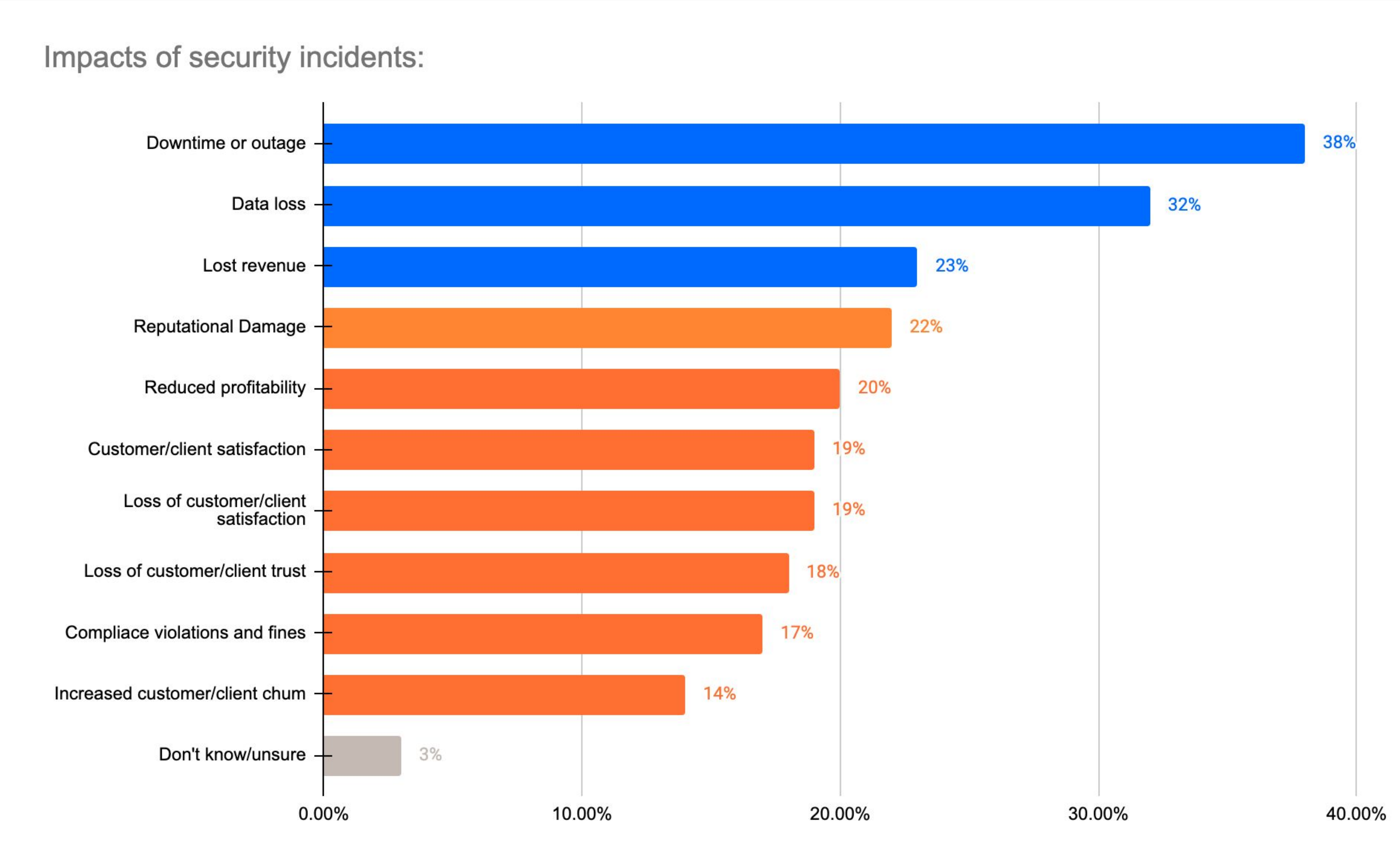
The top factors present in security incidents were **external attackers (38%), software bugs (33%) and unsatisfactory UX (27%)**



Q16. Which of the following factors were present in the security incident? Select all that apply | Base: 1632 *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 (38%), data loss (32%) and revenue loss (23%)**



Q17a. What were the main impacts of the security incident? Select top three | Base: 1632 *Only asked to those who have experienced a security incident in the last 12 months

Main Impacts of Security Incidents – Vertical analysis

The Government / Public Sector has most strongly felt the impact of **downtime or outage** following a security incident **(47%)** compared to just **33%** in the **Technology Sector**. Impacts of security incidents across verticals:

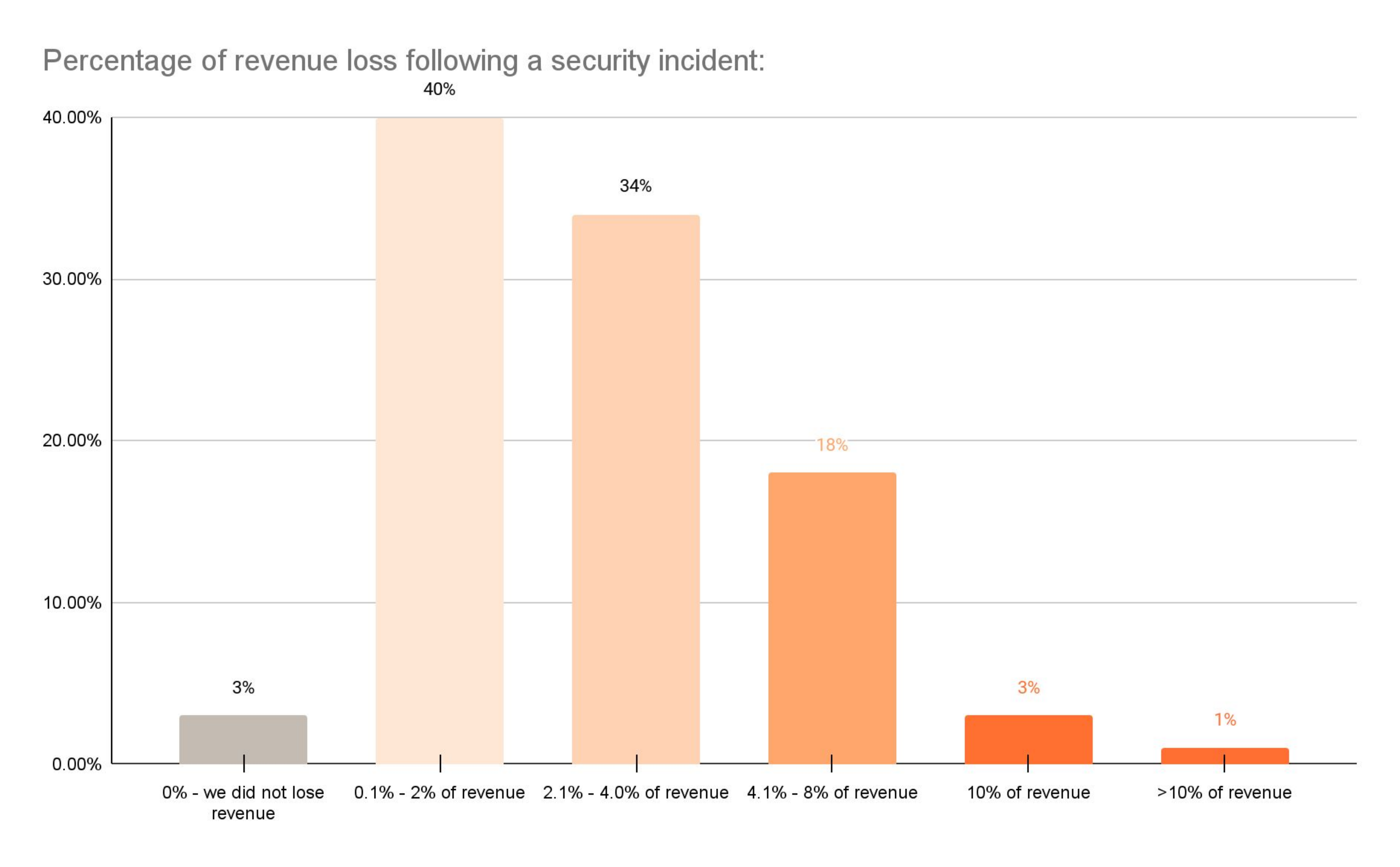
	Finance / Accounting	Government / Public Sector	Healthcare / Life Sciences	Media / Entertainment / Travel & Tourism	Retail / Wholesale	Technology
Downtime or outage	39%	47%	38%	42%	42%	33%
Data loss	28%	35%	39%	42%	24%	32%
Lost revenue	24%	11%	25%	27%	23%	25%
Reputational damage	23%	26%	18%	16%	27%	25%
Reduced profitability	23%	14%	16%	20%	25%	23%
Customer/client accounts compromised	17%	17%	19%	22%	17%	22%
Reduction in customer/client satisfaction	23%	14%	17%	19%	18%	24%
Loss of customer/client trust	19%	13%	18%	20%	19%	17%
Compliance violations and fines	21%	14%	18%	18%	16%	16%
Increased customer/client churn	16%	5%	11%	11%	15%	17%
Other	1%	1%	-	-	-	-
Don’t know / unsure	2%	7%	3%	1%	3%	2%

Q17a. What were the main impacts of the security incident? Select top three | Base: 1632

fastly

Revenue Loss from Security Incidents

Amongst those who report revenue loss as a top impact of security incidents, businesses report losing an average of **2.9%** of their revenue



Company size	Mean
250-999	2.7
1,000-4,999	3.0
5,000-24,999	3.1
More than 25,000	3.2

Revenue loss increases with company size

Q17b. Approximately what percentage of your revenue did you lose as a result of a security incident? Select one | Base: 374 *Only asked to those who lost revenue as a result of security incidents

External Support During Recovery – Vertical analysis

Government / Public Sector received very different external support or assistance during the incident recovery process compared to all other sectors. External support received during recovery process across verticals:

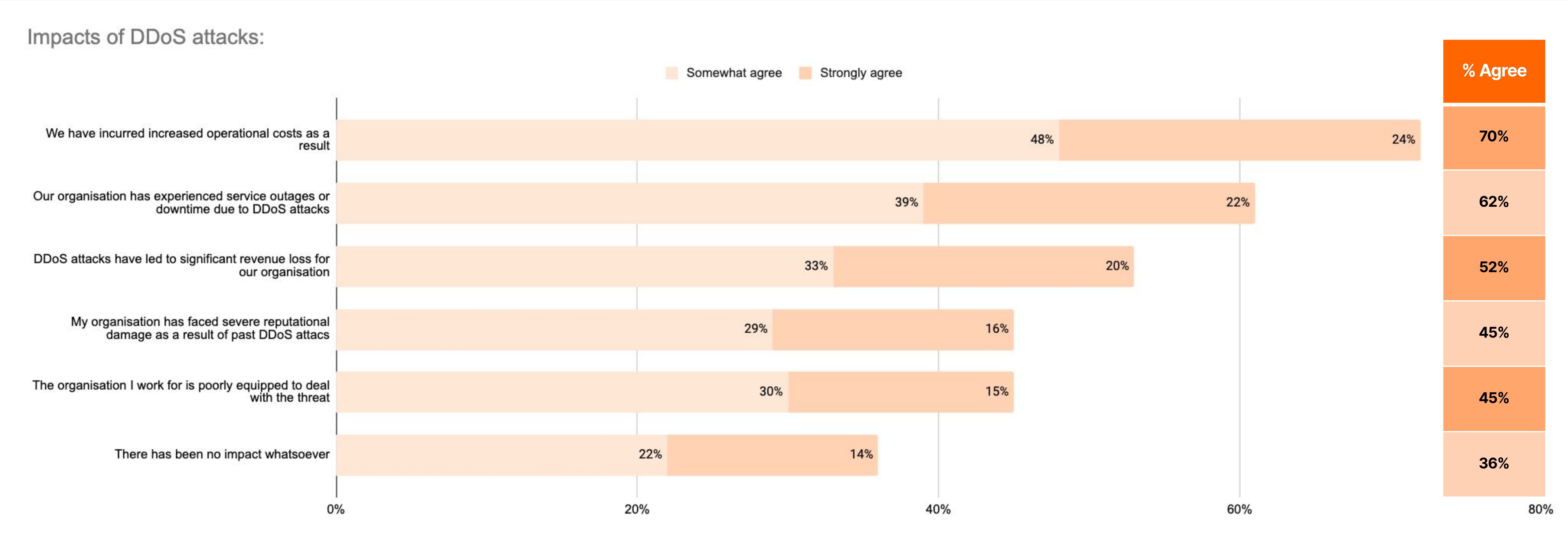
	Finance / Accounting	Government / Public Sector	Healthcare / Life Sciences	M&E / Travel & Tourism	Retail / Wholesale	Technology
Cybersecurity consultants	53%	35%	47%	56%	57%	57%
Vendor support	37%	15%	26%	39%	41%	42%
Legal advisors	25%	14%	36%	30%	26%	25%
PR and crisis management firms	27%	12%	29%	26%	22%	31%
Industry associations	19%	16%	19%	18%	27%	29%
Government agencies	21%	45%	21%	17%	14%	23%
Other	1%	-	0%	-	-	-
Our business did not receive any external support during the recovery process	12%	18%	13%	9%	13%	6%

Q22b. What external support or assistance, if any, did your business receive during the recovery process? Select all that apply| Base: 1800

fastly

Impacts of DDoS Attacks

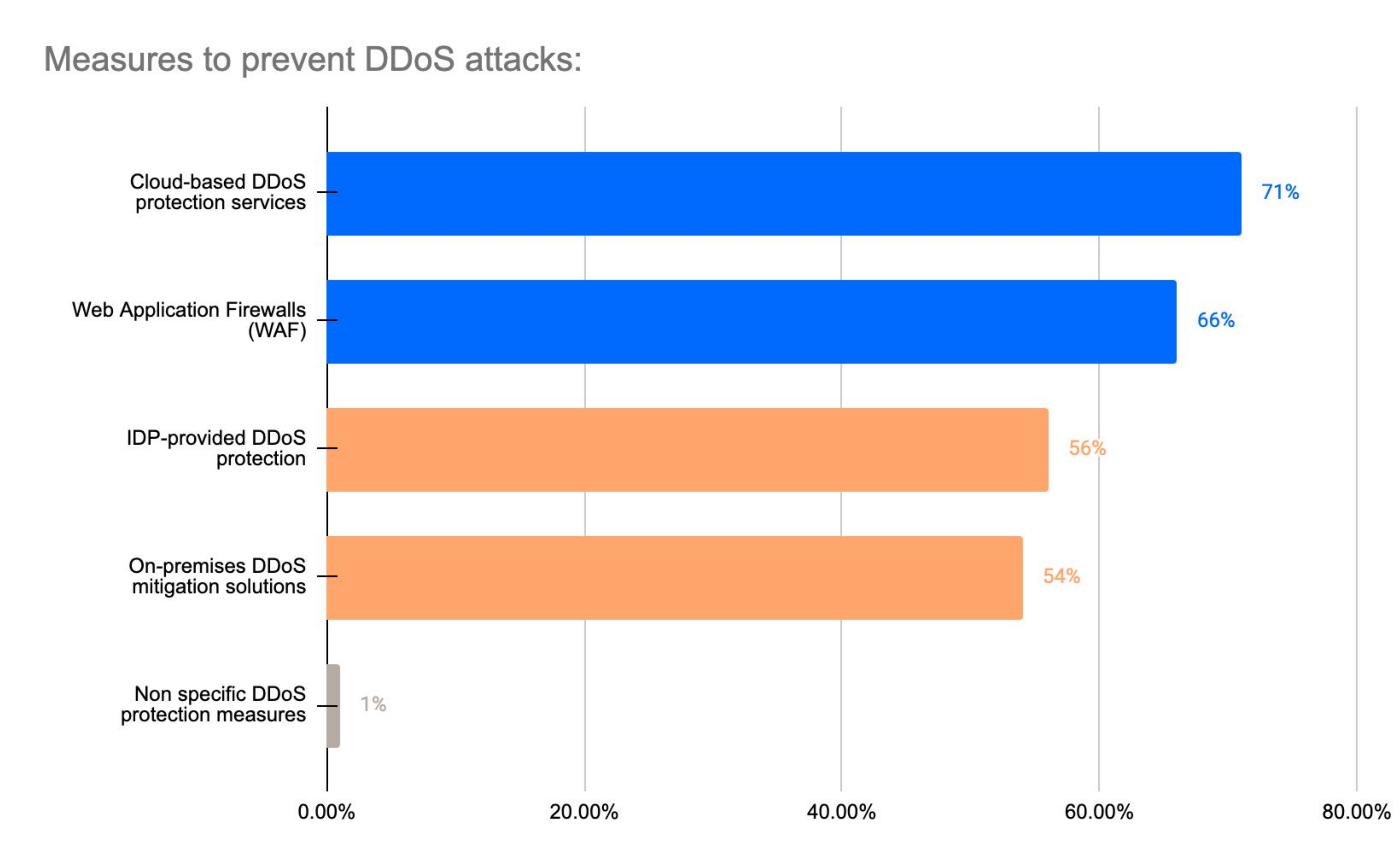
Decision makers who think DDoS attacks will be one of the biggest threats over the next 12 months are likely driven by the significant negative impacts of DDoS attacks, with **70%** saying they result in **increased operational cost** and 62% experiencing downtime or service outages



Q1b. To what extent do you agree or disagree with the following statements? | Base: 421 *Only asked to those who believe DDoS attacks are a threat

DDoS Protection Measures

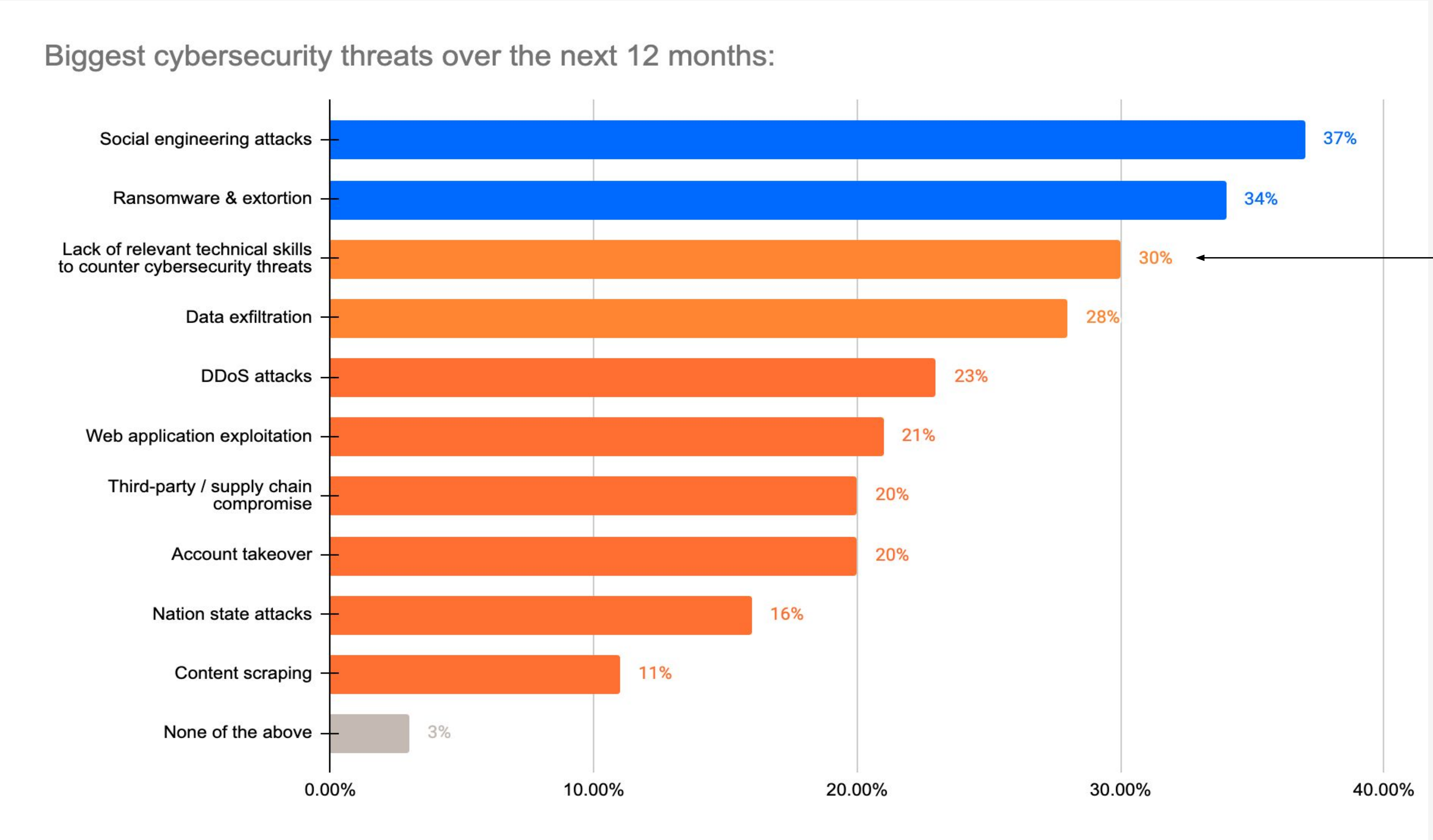
Organisations are most commonly using **cloud-based DDoS protection services (71%)** and **WAF (66%)** to combat DDoS attacks



Q1c. What measures does your organisation currently use for DDoS protection? Select all that apply | Base: 421 *Only asked to those who believe DDoS attacks are a threat

Predicted Biggest Cybersecurity Threats

Organisations predict that **social engineering attacks (37%)** and **ransomware and extortion (34%)** will be their biggest cybersecurity threats in the next 12 months, followed closely by a **lack of relevant technical skills (30%)**

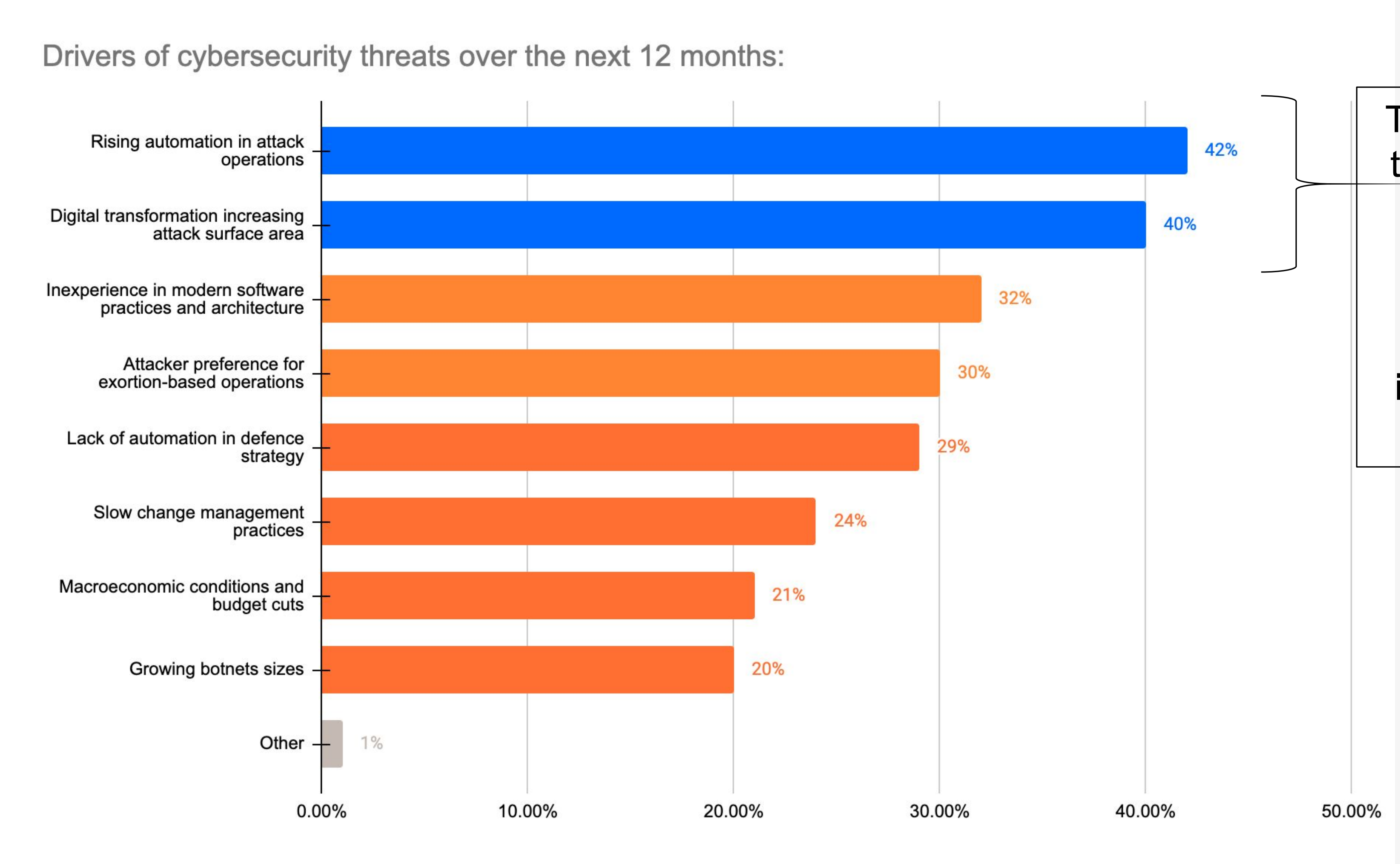


Increases to 35% for Media / Entertainment / Travel & Tourism suggesting this is a particular problem area when it comes to the talent pool

Q1a. What do you predict will be the biggest cybersecurity threat to your organisation over the next 12 months? Select top three | Base: 1800

Drivers of Future Cybersecurity Threats

Looking ahead, decision makers believe that **rising automation in attack operations (42%)** and **digital transformation increasing the attack surface area (40%)** will be the biggest drivers of cybersecurity threats



The top two drivers of cybersecurity threats to businesses over the next 12 months revolve around the evolving digital landscape.

As businesses evolve it is important that the cybersecurity function evolves with them.

Q3. Which of the following do you predict will drive cybersecurity threats to your business over the next 12 months? Select top three | Base: 1800

Drivers of Future Cybersecurity Threats – Vertical analysis

Rising automation in attack operations is particularly viewed as the biggest threat in the **Finance / Accounting** sector **(47%)**

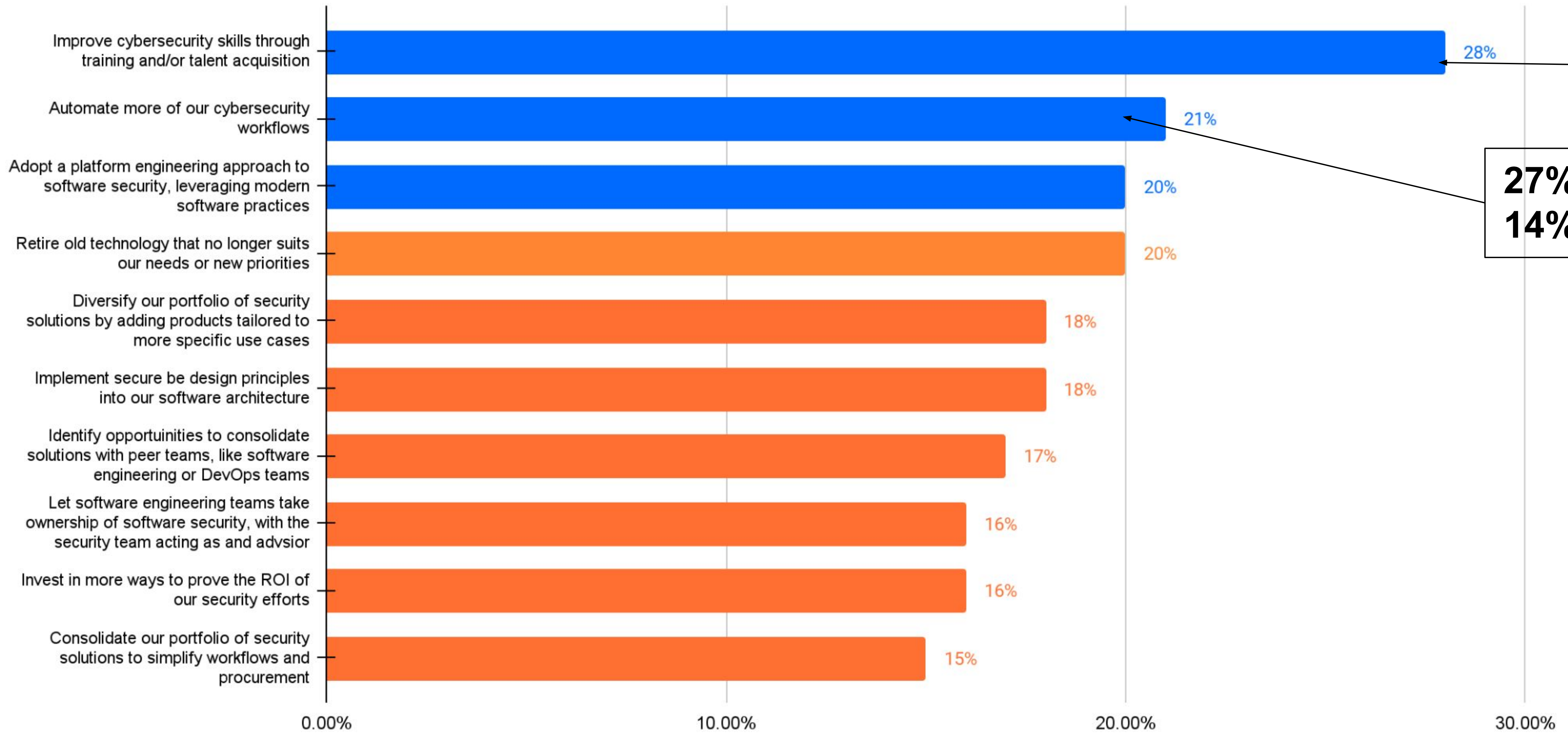
	Finance / Accounting	Government / Public Sector	Healthcare / Life Sciences	Media / Entertainment / Travel & Tourism	Retail / Wholesale	Technology
Rising automation in attack operations	47%	45%	40%	43%	38%	39%
Digital transformation increasing attack surface area	45%	40%	40%	45%	42%	42%
Inexperience in modern software practices and architecture	25%	31%	35%	32%	37%	32%
Attacker preference for extortion-based operations	29%	25%	33%	27%	33%	30%
Lack of automation in defence strategy	27%	26%	23%	35%	24%	35%
Slow change management practices	26%	26%	33%	23%	23%	22%
Macroeconomic conditions and budget cuts	24%	22%	16%	23%	21%	22%
Growing botnet sizes	24%	20%	17%	21%	19%	22%
Other	0%	1%	0%	-	1%	1%

Q3. Which of the following do you predict will drive cybersecurity threats to your business over the next 12 months? Select top three | Base: 1800

Security Priorities for the Next Year

Organisations' top security priorities for the next year revolve around **improving cybersecurity skills (28%)** and **automation of cybersecurity workflows (21%)**

Top 10 security priorities over the next year:



33% in Retail / Wholesale,
24% in Technology

27% in Finance / Accounting,
14% in Healthcare / Life Sciences

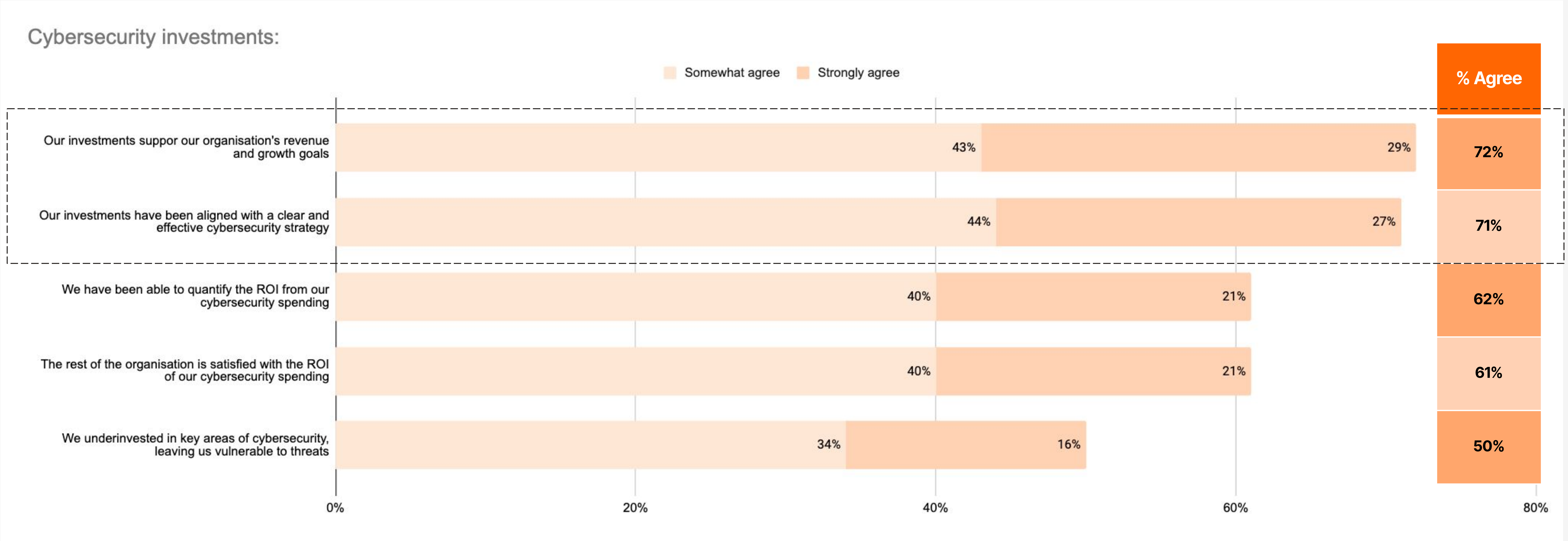
Q14. What are your organisation's security priorities over the next year? Select top three | Base: 1800

Main Findings

Is cybersecurity spending falling behind

Investment in Cybersecurity

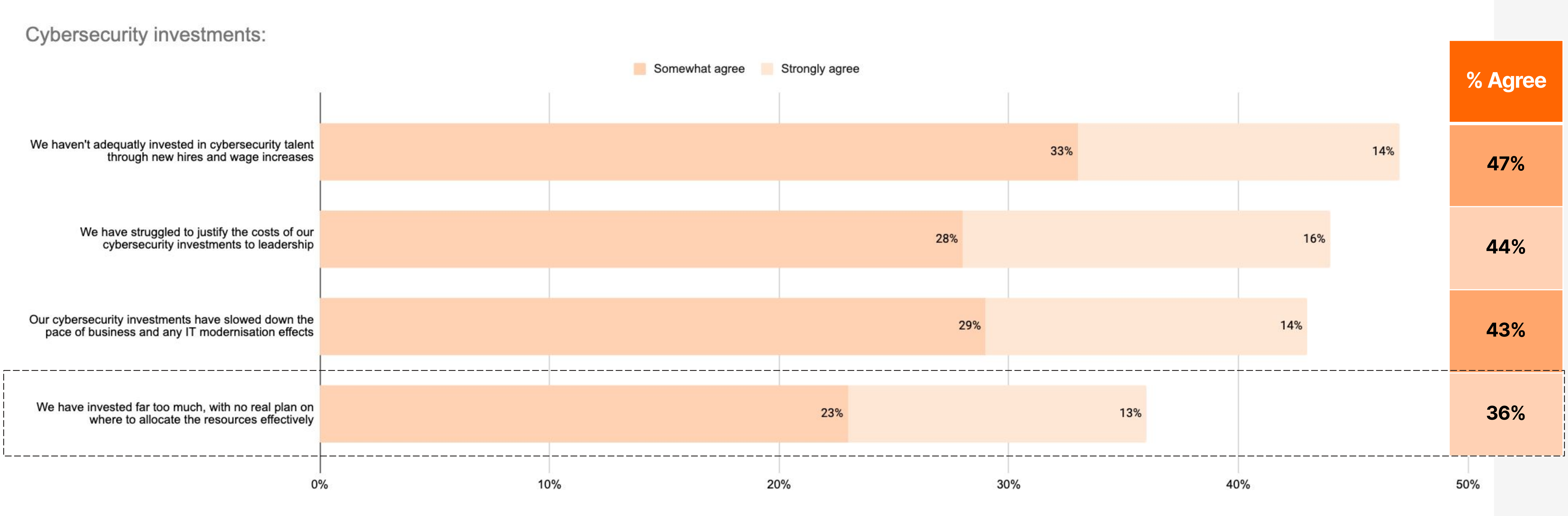
Almost three quarters (72%) agree that their investments in cybersecurity **support their organisation's revenue and growth** goals, with a further **71%** agreeing that these investments are **aligned with a clear and effective cybersecurity strategy...**



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: 1800

Investment in Cybersecurity

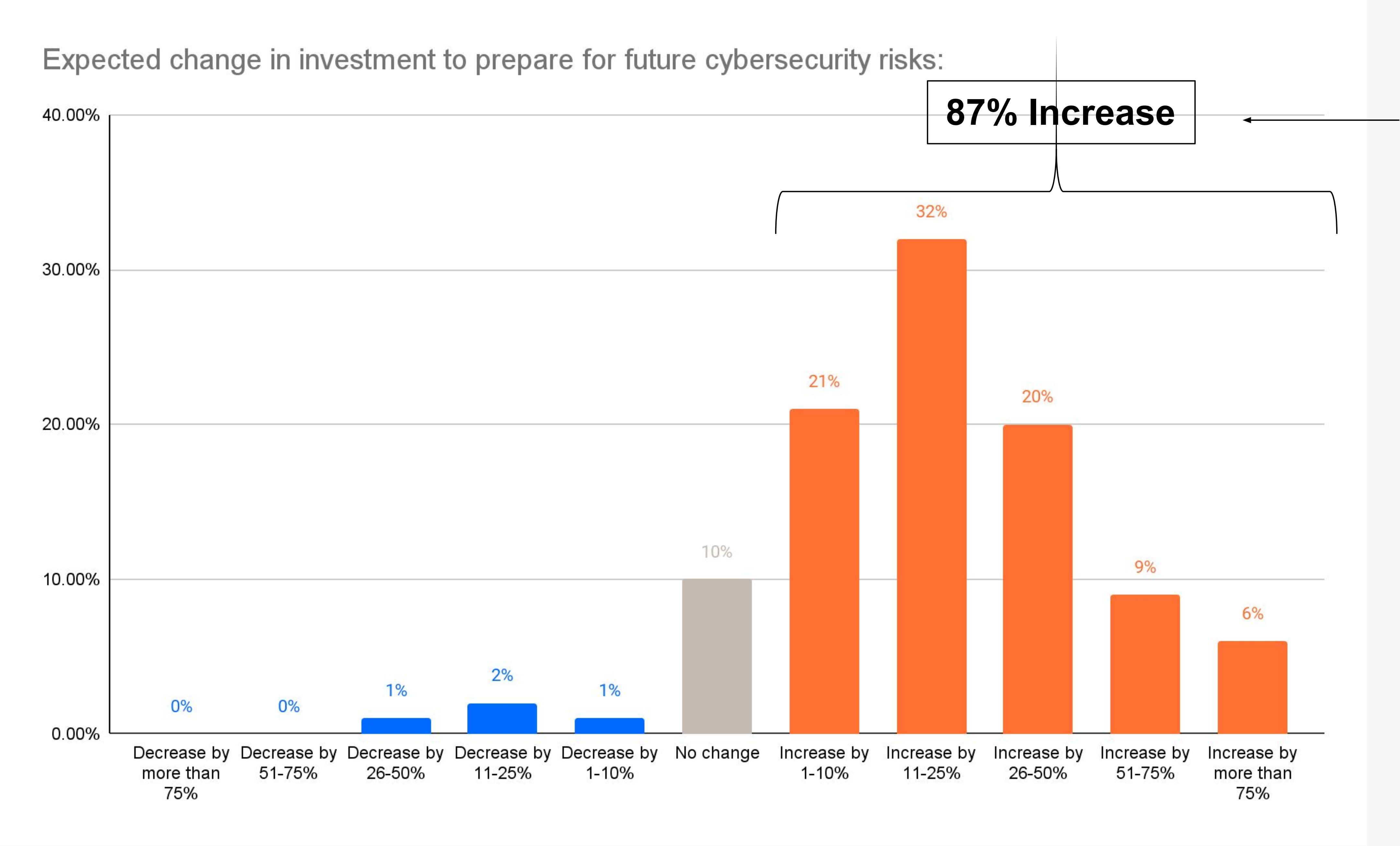
...furthermore, just **36%** agree that they have **invested too much, with no real plan on where to allocate the resources effectively**, demonstrating that organisations are actively preparing for future cybersecurity risks



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: 1800

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



91% in Finance / accounting, Media / Entertainment / Travel and Tourism and Technology

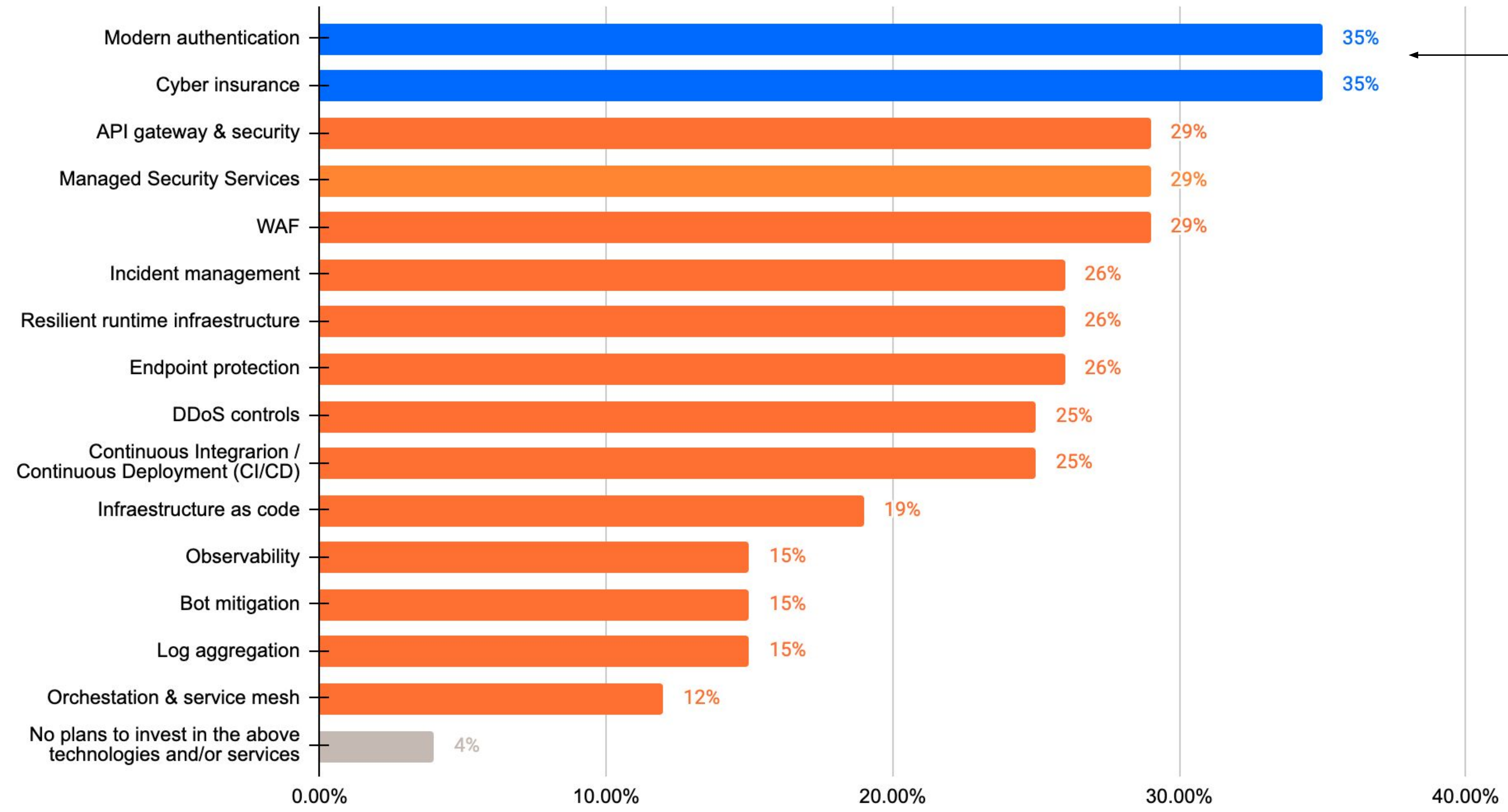
79% in Government / Public Sector

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: 1800

Planned Investments in Cybersecurity Technologies

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

Technologies organisations are planning to invest in over the next 12 months:



44% in Media / Entertainment / Travel and Tourism,
25% in Government / Public Sector

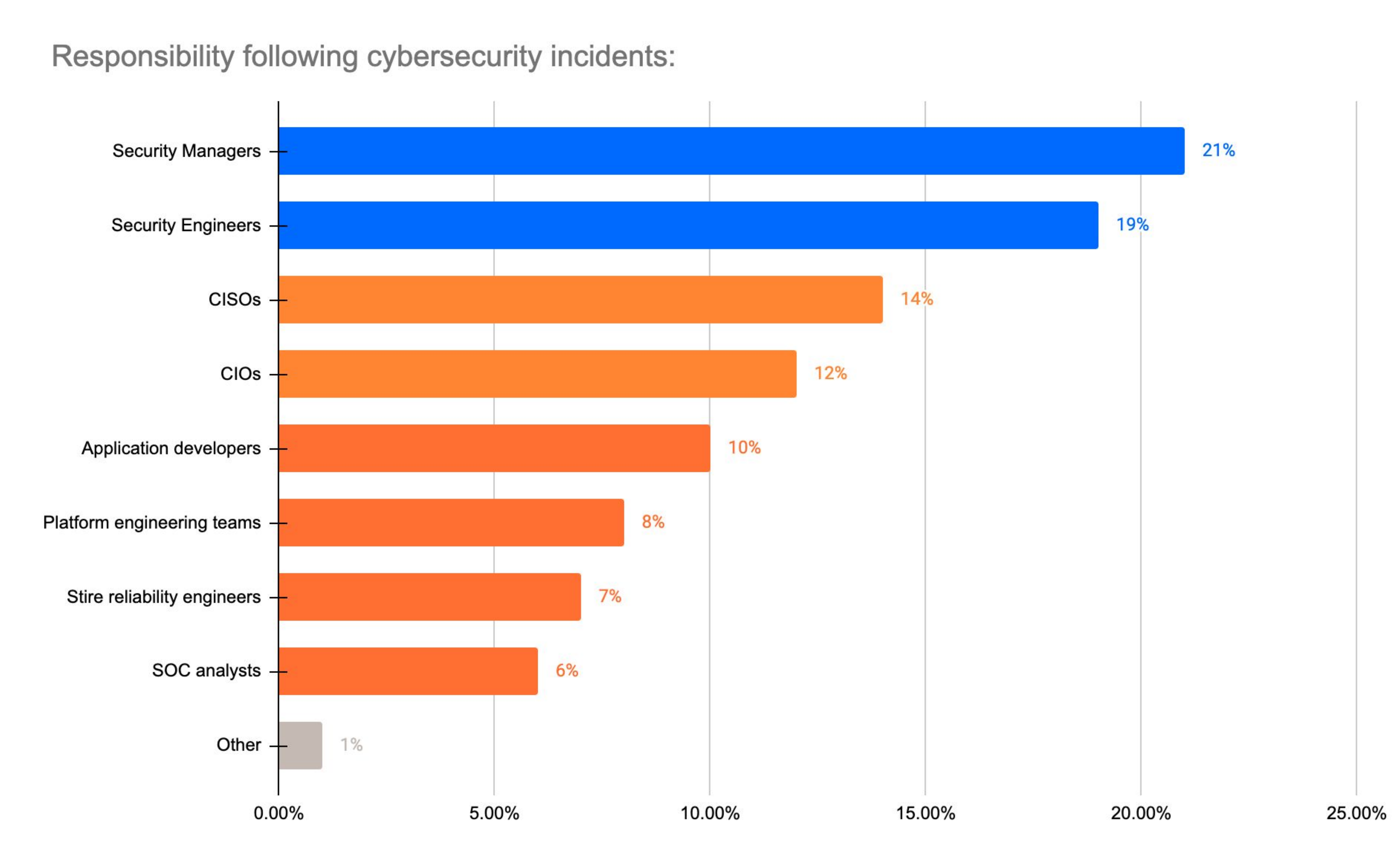
Q4. Which technologies and/or services does your organisation plan to invest in over the next 12 months? Select all that apply | Base: 1800

Main Findings

Shifting accountability

Responsibility During Cybersecurity Incidents

There is a wide spread of responsibility when it comes to security incidents, however, **Security Managers (21%)** 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: 1800

Responsibility During Cybersecurity Incidents – Vertical analysis

When comparing the data across sectors, differences can be seen in where responsibility for cybersecurity incidents is placed

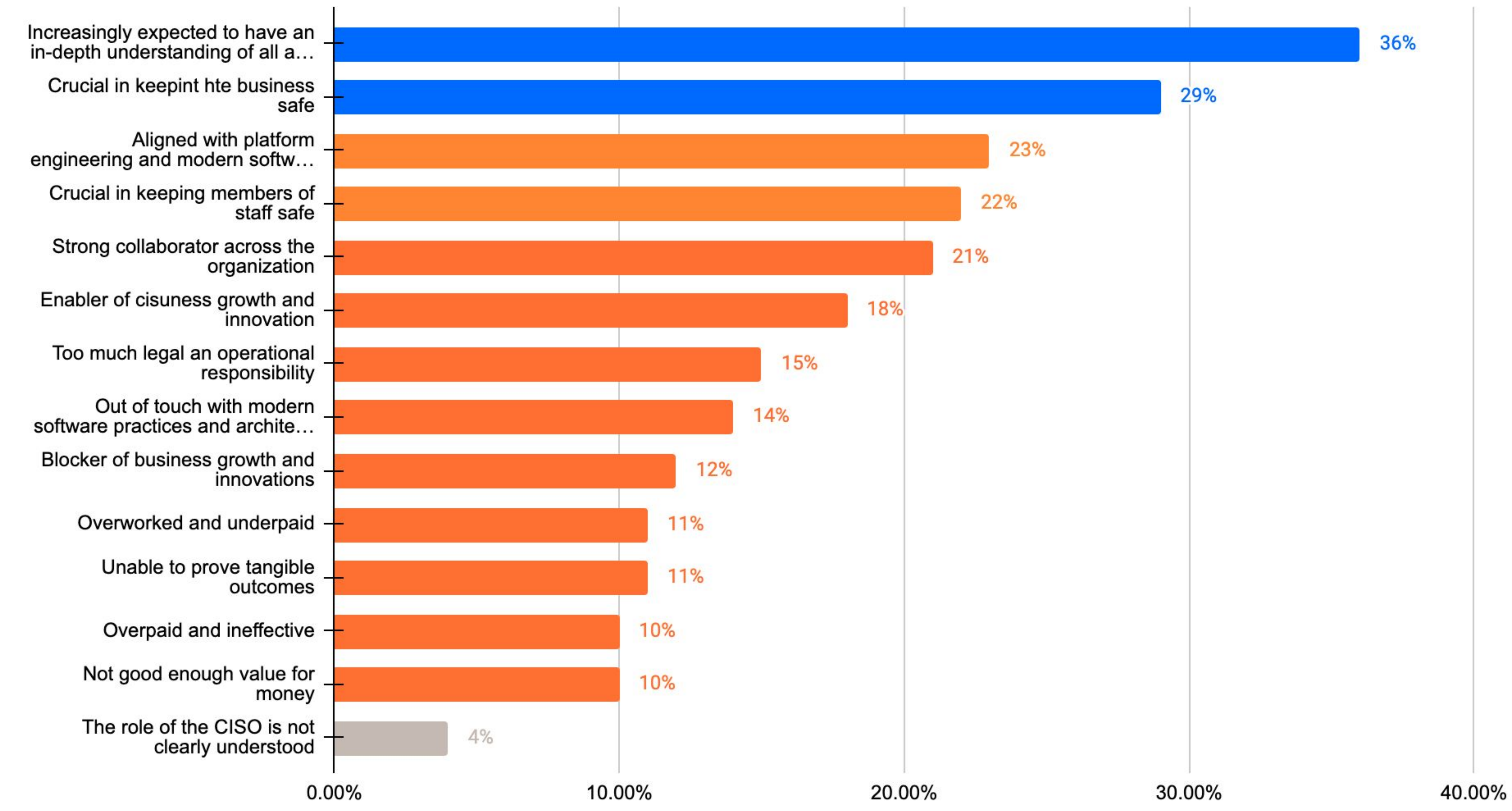
	Finance / Accounting	Government / Public Sector	Healthcare / Life Sciences	Media / Entertainment / Travel & Tourism	Retail / Wholesale	Technology
Security Managers	26%	28%	25%	20%	18%	22%
Security Engineers	20%	18%	18%	27%	17%	21%
CISOs	15%	8%	9%	11%	17%	17%
CIOs	11%	15%	13%	8%	14%	11%
Application developers	9%	9%	11%	12%	10%	10%
Platform engineering teams	6%	7%	9%	6%	9%	8%
Site reliability engineers	5%	10%	8%	8%	8%	5%
SOC analysts	5%	5%	3%	6%	6%	4%
Other	1%	3%	3%	0%	1%	1%

Q9. Who do you feel is most often held responsible for cybersecurity incidents in your organisation? Select one | Base: 1800

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 (29%)**

View of CISO role by wider organisation:

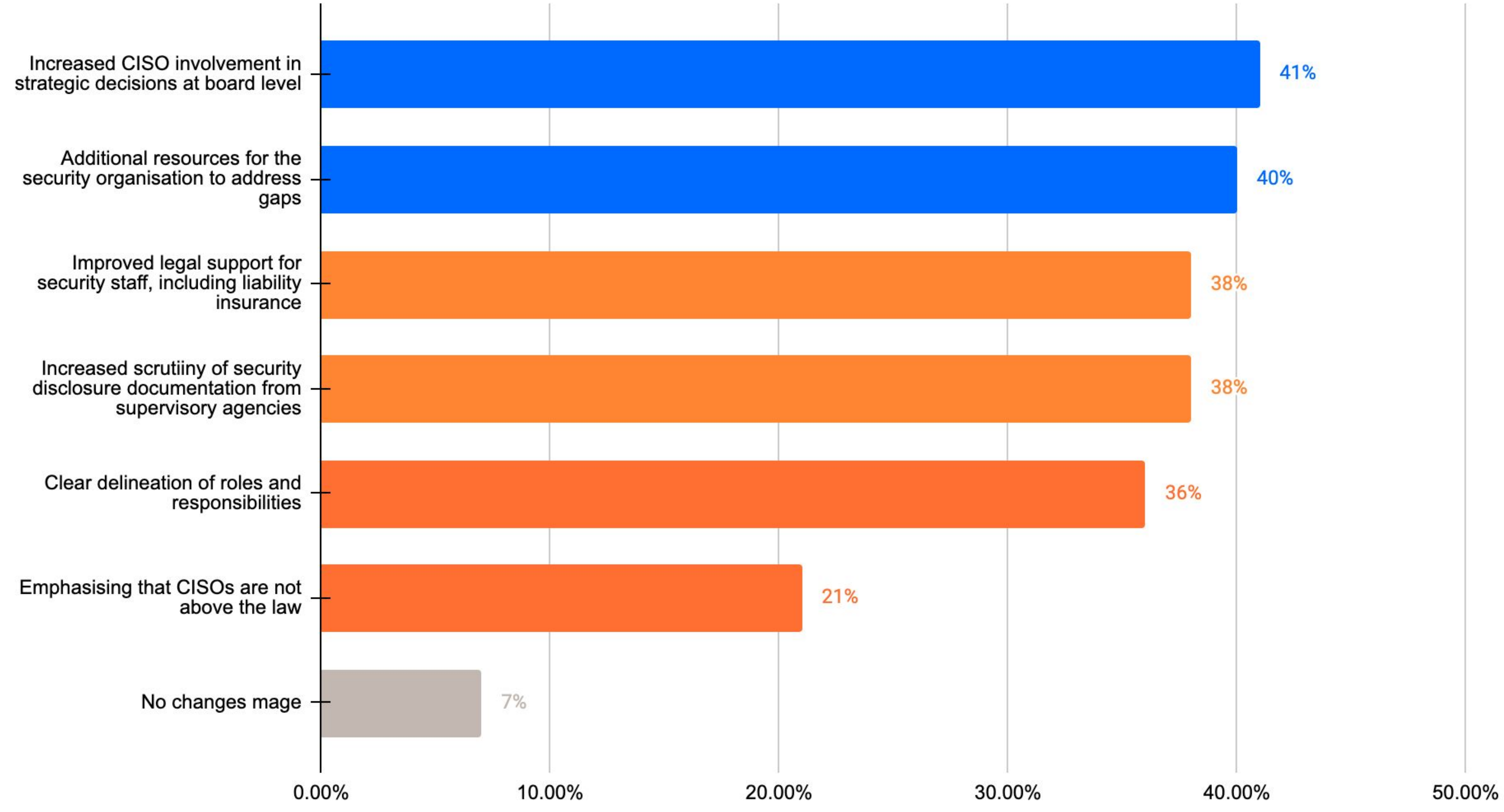


Q10. How do you think the role of the CISO is viewed by your wider organisation? Select top three | Base: 1800

Changes to Address CISO Liability

Businesses are actively addressing concerns regarding CISO liability, with **41% increasing CISO involvement in strategic decisions** and a further **40% creating additional resource for the security organisation to address gaps**

Changes made to address concerns over CISO liability:

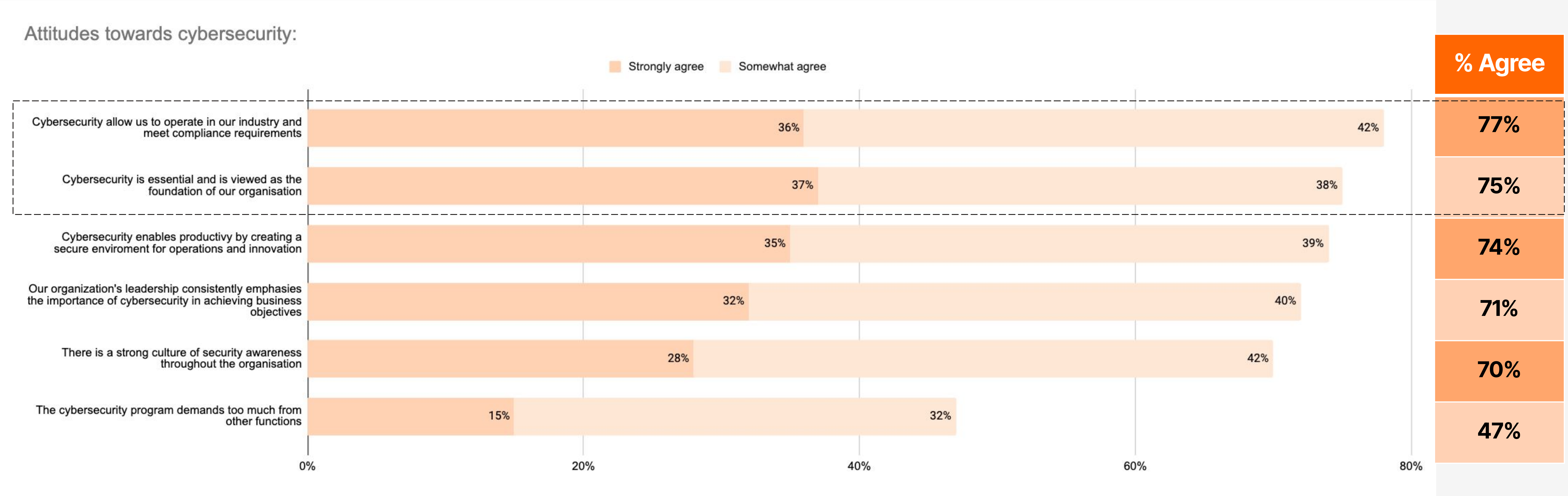


Organizations are increasingly recognizing the importance of the CISO role, reflecting a growing acknowledgment of the strategic significance of cybersecurity at the executive level.

Q12. What changes has your company made to address concerns regarding CISO liability? Select all that apply | Base: 1800

Perception of Value of Cybersecurity

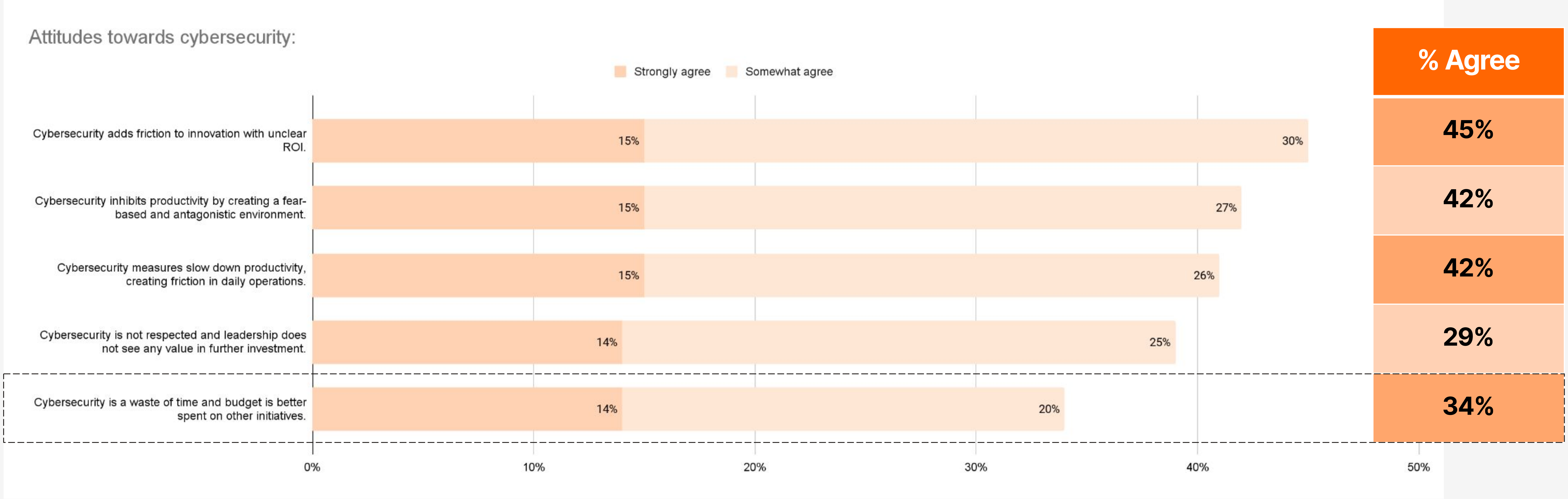
There is a strong consensus on the **essential nature of cybersecurity (75%)**, particularly when it comes to **meeting compliance requirements (77%)...**



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: 1800

Perception of Value of Cybersecurity

...this is further illustrated by only a third (34%) agreeing that cybersecurity is a waste of time, and that budget would be better spent elsewhere

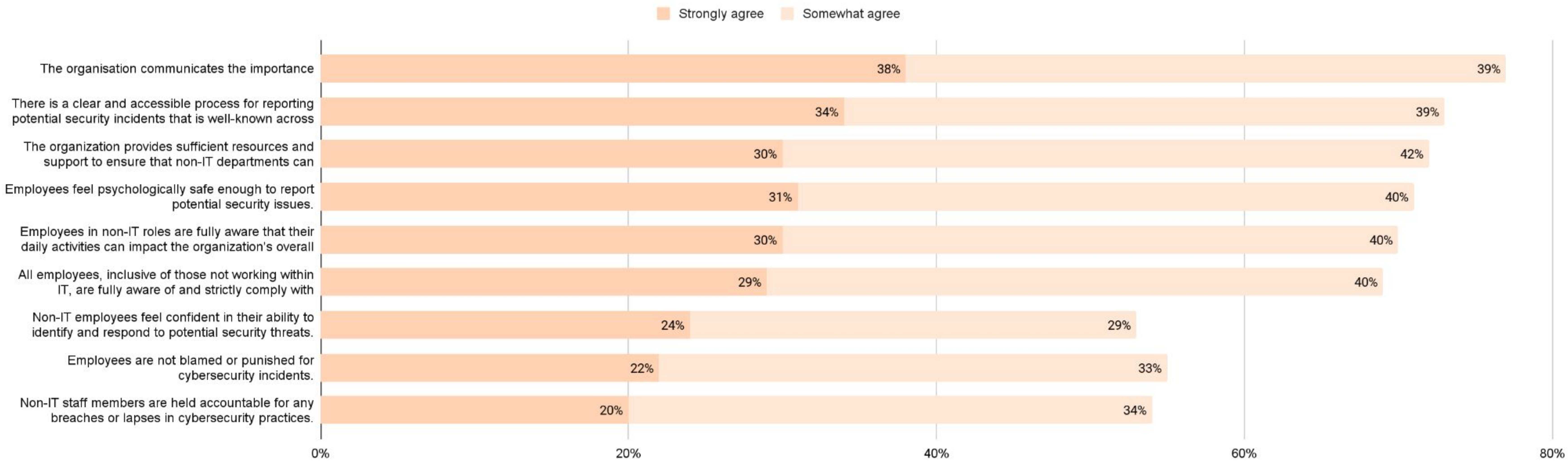


Q11. Thinking about the perception of the value of cybersecurity in your organisation, to what extent do you agree or disagree with the following statements? | Base: 1800

Cybersecurity Policies

2 in 3 businesses have a strong culture of compliance with cybersecurity policies across all departments **(69%)**, facilitated by **effective communication of the importance of security (77%)**

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: 1800

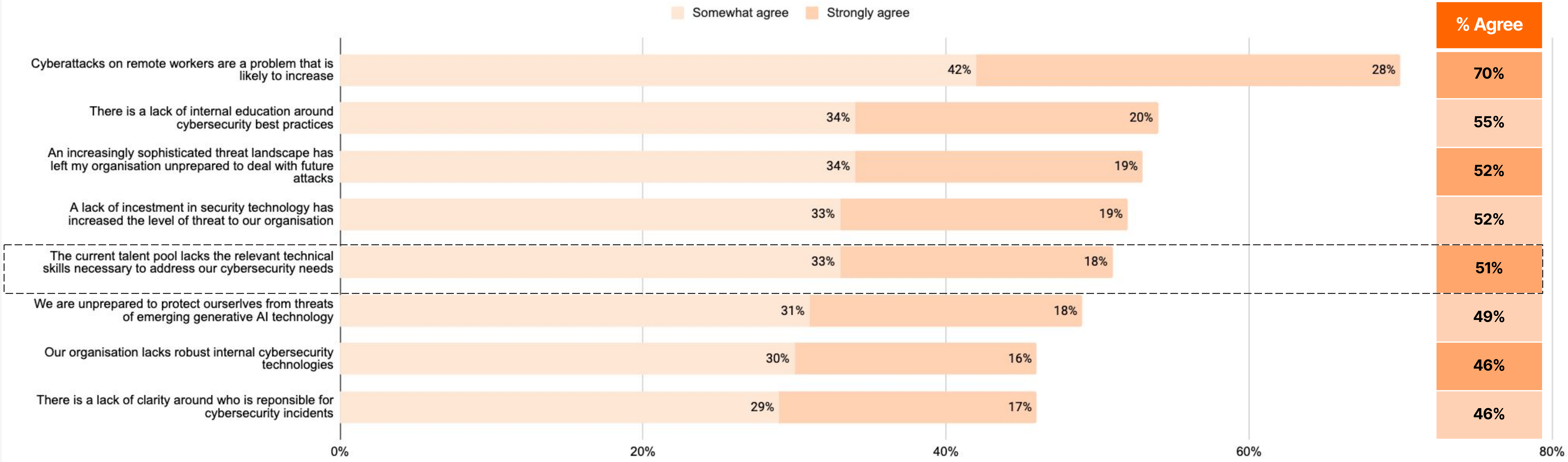
Main Findings

The Cybersecurity Talent Pool

Cybersecurity Threats

There are rising concerns over cyberattacks on remote workers **(70%)**, an issue businesses may not be prepared for as **51%** of cybersecurity decision makers think that the **current talent pool lacks the relevant technical skills to address their needs**

Sentiment around cybersecurity threats:

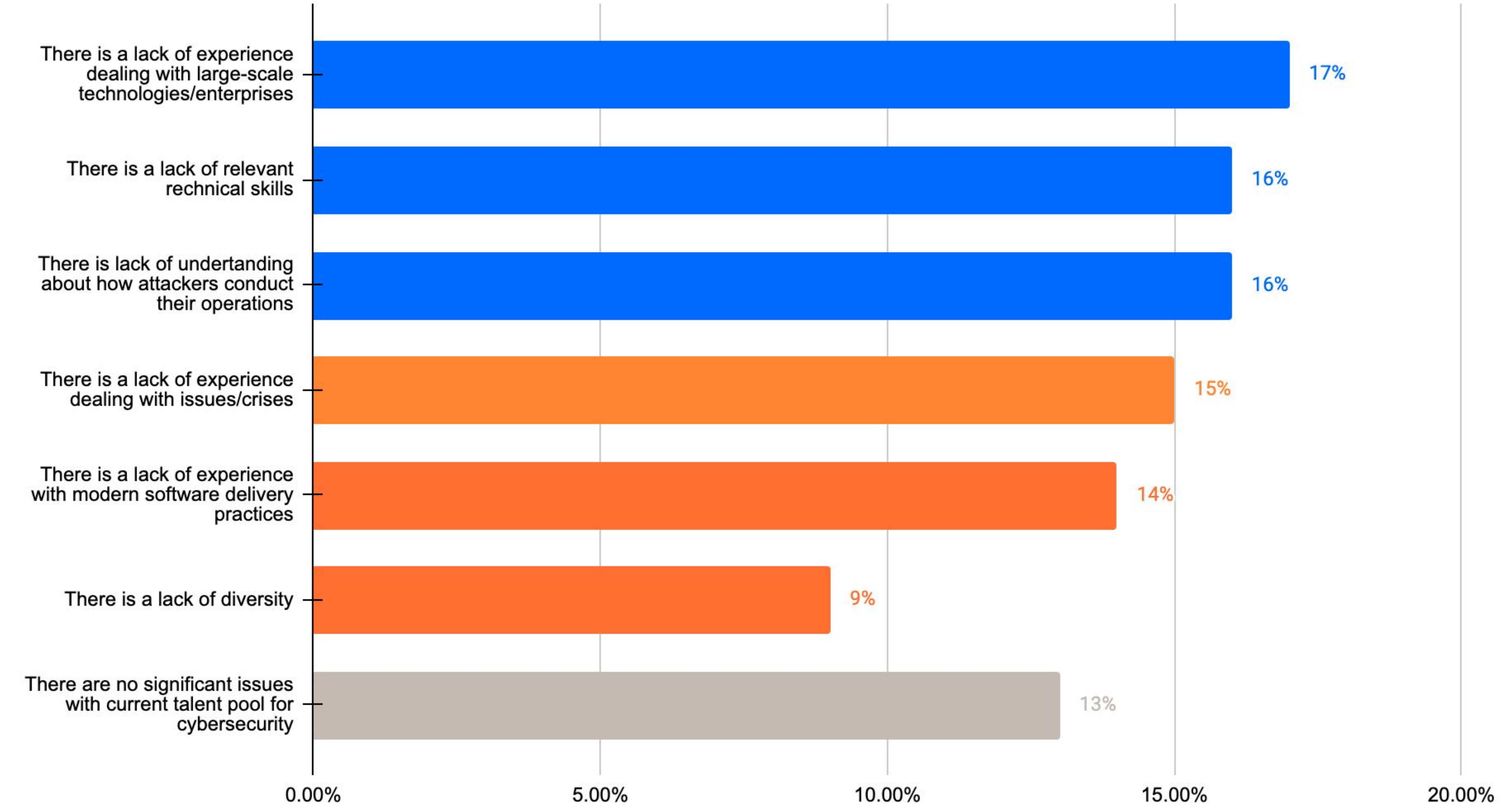


Q2. Thinking about cybersecurity threats to your organisation, to what extent do you agree with the following statements? | Base: 1800

Gaps in Cybersecurity Talent Pool

At an overall level, the gaps in the talent pool are multifaceted with there being no clear driver - however, t**he majority (87%) agree there are issues…**

Gaps amongst the current cybersecurity talent pool:



Q8. Where do you feel there are gaps amongst the current talent pool when it comes to cybersecurity? Select one | Base: 1800

Gaps in Cybersecurity Talent Pool – Vertical analysis

..but some differences begin to emerge when looking at the data across different verticals.
Gaps amongst the current cybersecurity talent pool across verticals:

	Finance / Accounting	Government / Public Sector	Healthcare / Life Sciences	Media / Entertainment / Travel & Tourism	Retail / Wholesale	Technology
There is a lack of experience dealing with large-scale technologies / enterprises	18%	14%	18%	17%	12%	19%
There is a lack of relevant technical skills	12%	19%	14%	16%	16%	15%
There is a lack of understanding about how attackers conduct their operations	19%	18%	15%	13%	17%	15%
There is a lack of experience dealing with issues/crises	16%	11%	17%	15%	14%	16%
There is a lack of experience with modern software delivery practices	17%	17%	12%	16%	14%	15%
There is a lack of diversity	5%	8%	8%	9%	9%	10%
There are no significant issues with current talent pool for cybersecurity	14%	14%	16%	14%	19%	11%

Q8. Where do you feel there are gaps amongst the current talent pool when it comes to cybersecurity? Select one| Base: 1800

Main Findings

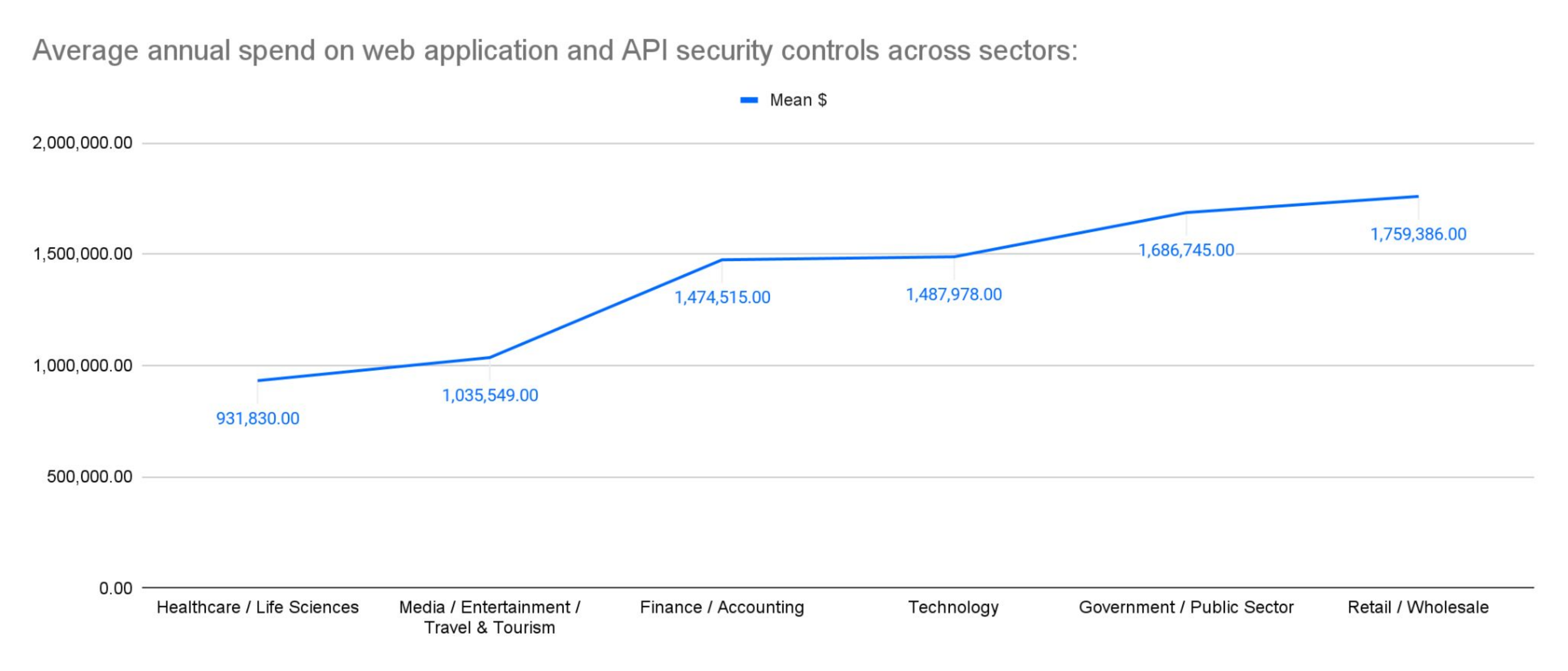
Investment Trends in Cybersecurity

Annual Spending on Web Application / API Security

On average, businesses spend **$1,578,475** annually on web application and API security controls / tools. This increases to **$1,759,386** in the **Retail / Wholesale** sector

$1,578,475

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



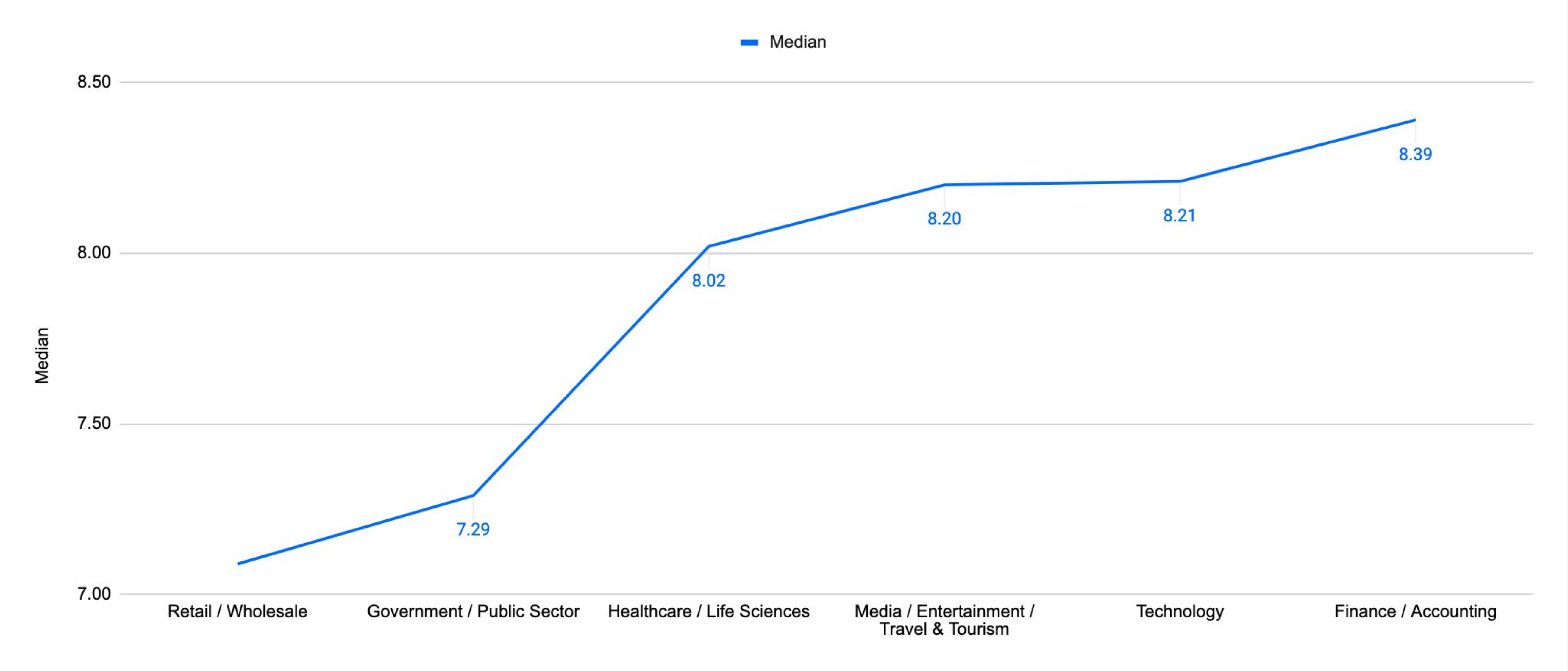
Q7a. In USD ($), approximately how much would you estimate your organisation spends per year on web application and API security controls/tools? | Base: 1800

Number of Network and Application Security Solutions

Businesses report being reliant upon an average of **8** cybersecurity solutions

8

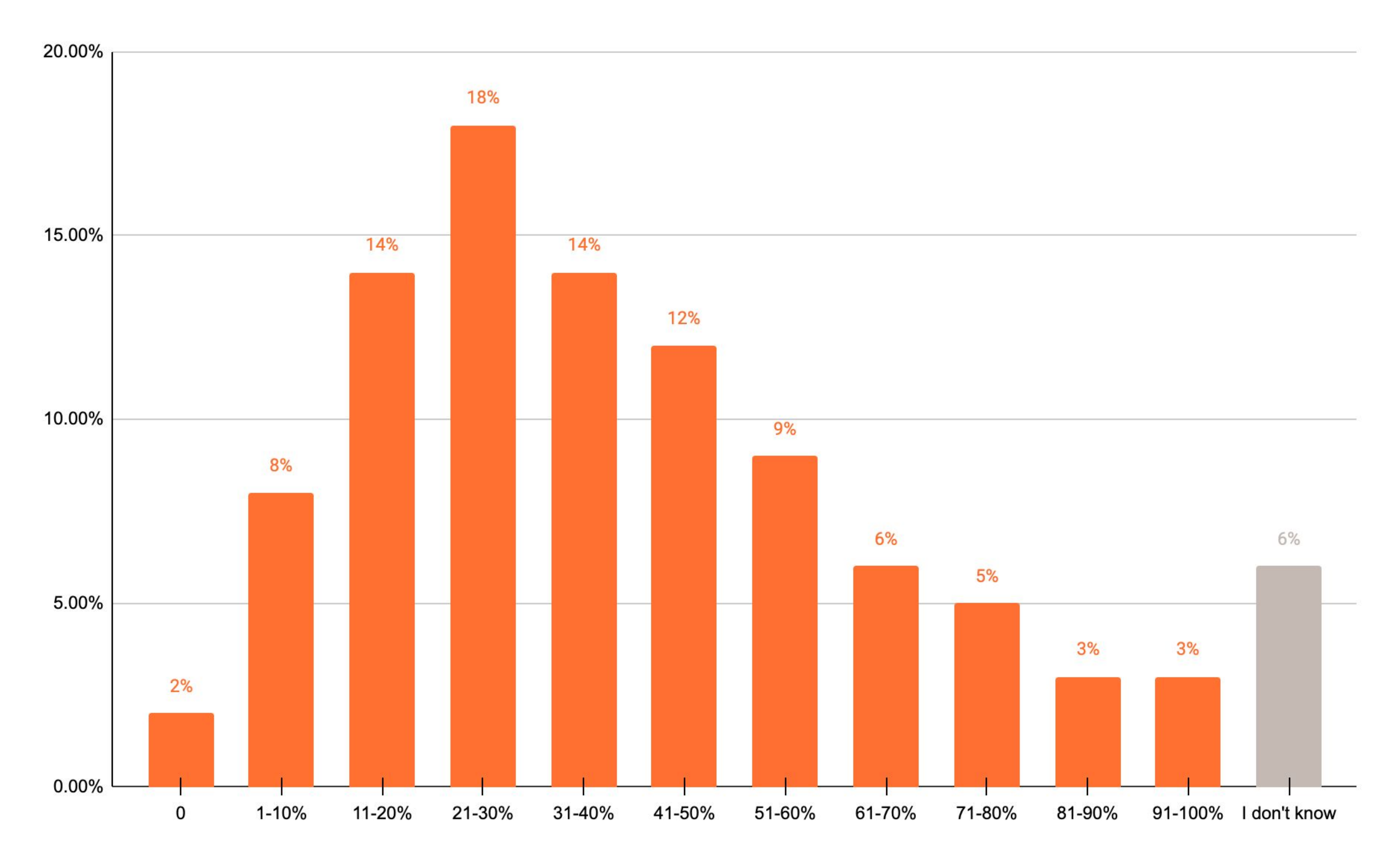
Average number of network and application cybersecurity solutions organisations rely on



Q7b. Approximately, how many network and application cybersecurity solutions does your organisation rely on? | Base: 1800

Overlap in Cybersecurity Solutions

On average, **38%** of these cybersecurity solutions overlap in their primary function, increasing to 42% for larger enterprises



Company Size	Mean
250-999	37%
1.000-4.999	36%
5.000-24,999	38%
More than 25.000	42%

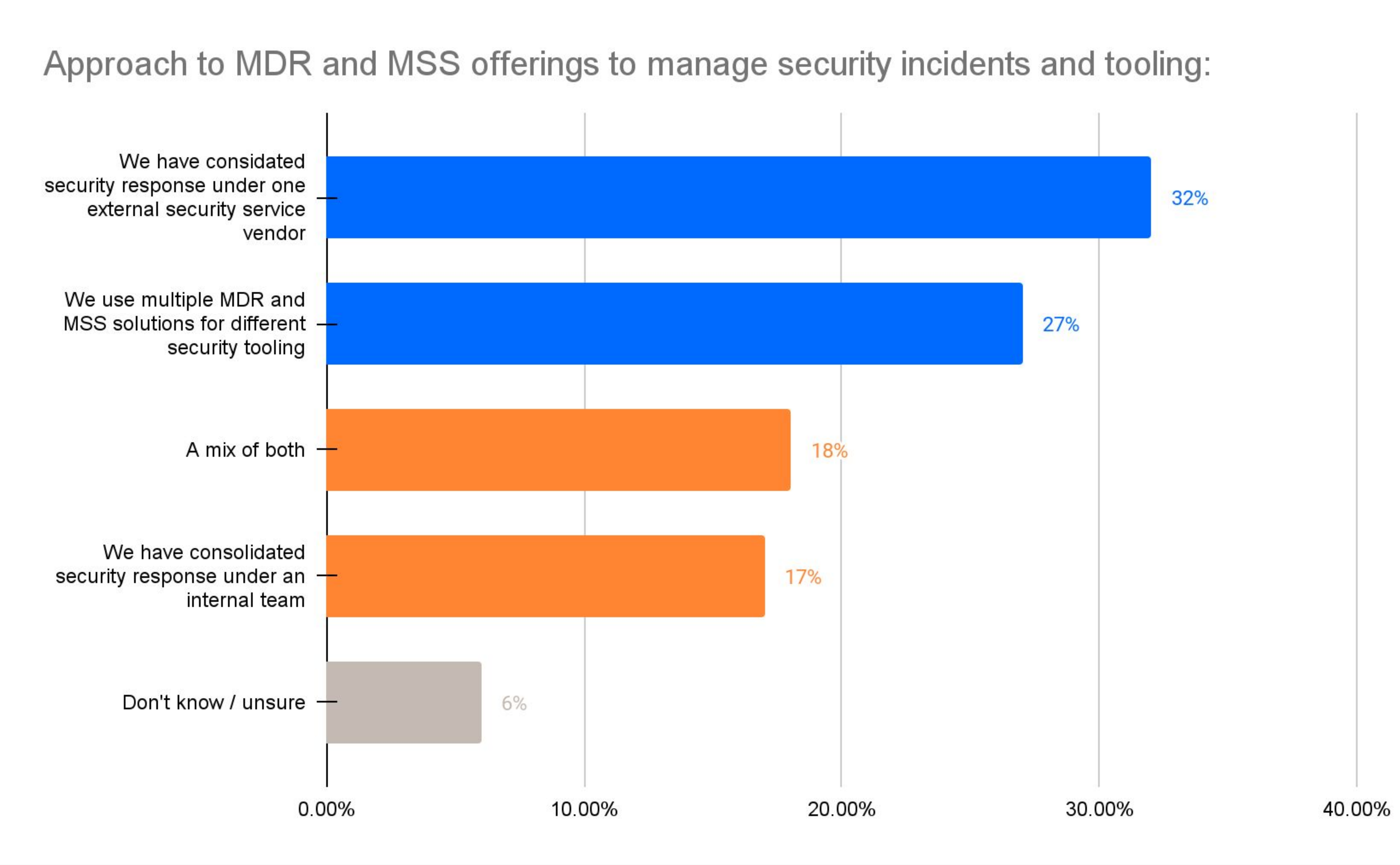
Mean: 38%

Overlap increases with company size

Q7c. Roughly, how many of these solutions overlap in their primary function? Select one | Base: 1800

Approach to MDR and MSS Offerings to Manage Security Incidents

32% have consolidated their security response under one external security service vendor, whilst **27%** 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: 1800

Approach to MDR and MSS Offerings to Manage Security Incidents

The **Finance / Accounting** sector is the only one that utilises multiple MDR and MSS solutions **more** than having a consolidated security response under one vendor

Sector	We use multiple MDR and MSS solutions for different security tooling	We have consolidated security response under one external security service vendor
Finance / Accounting	33%	28%
Government / Public Sector	15%	29%
Healthcare / Life Sciences	23%	30%
Media / Entertainment / Travel & Tourism	28%	31%
Retail / Wholesale	29%	29%
Technology	31%	35%

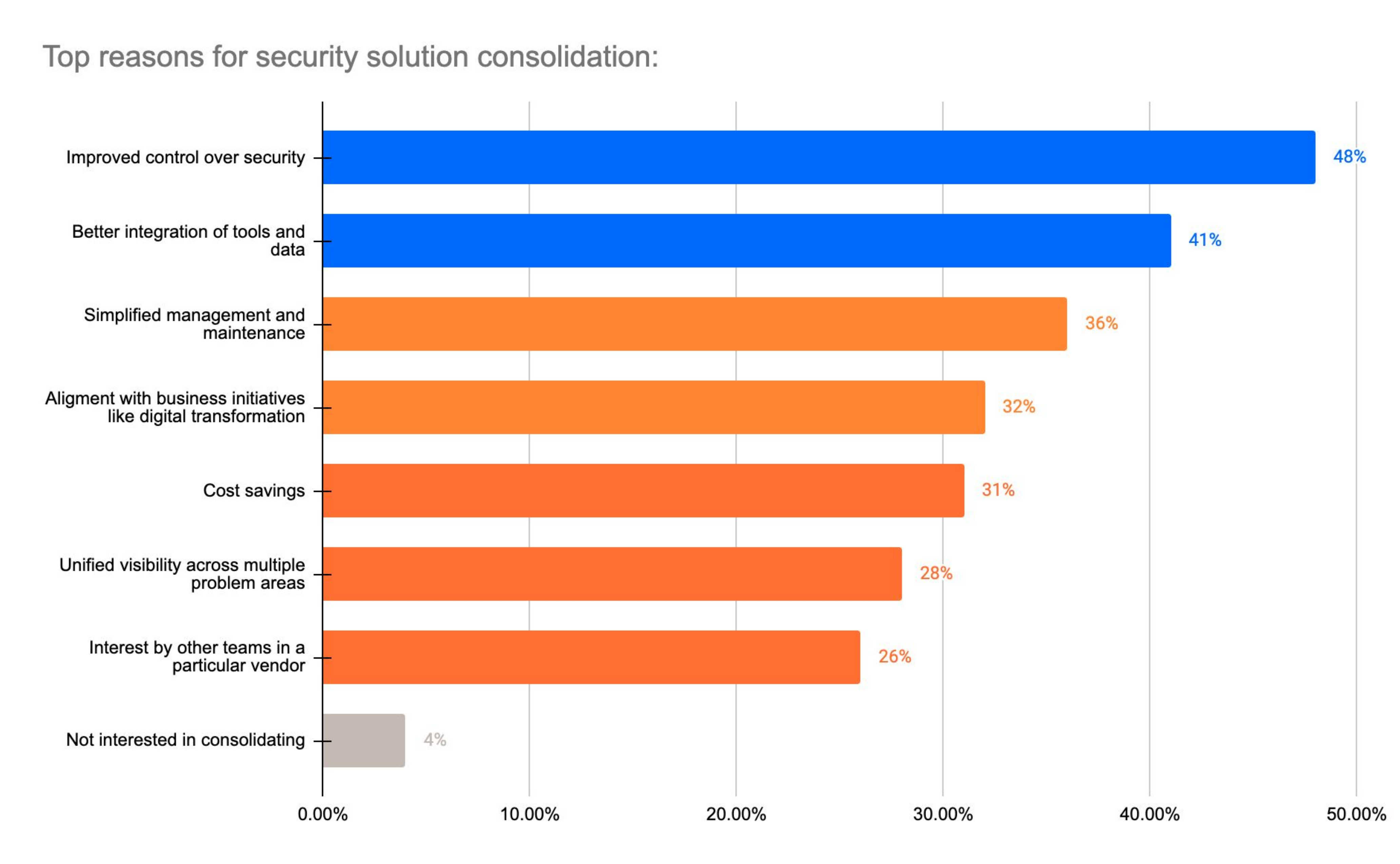
Q24a. What is your organisation's approach to Managed Detection & Response (MDR) and Managed Security Service (MSS) offerings to manage security incidents and security tooling? Select one | Base: 1800

Main Findings

Consolidation and Integration of Security Solutions

Reasons for Security Solution Consolidation

Almost half (48%) attribute their organisation's interest in consolidating security solutions to **improving control over security,** whilst a further **41% are looking for better integration of tools and data**

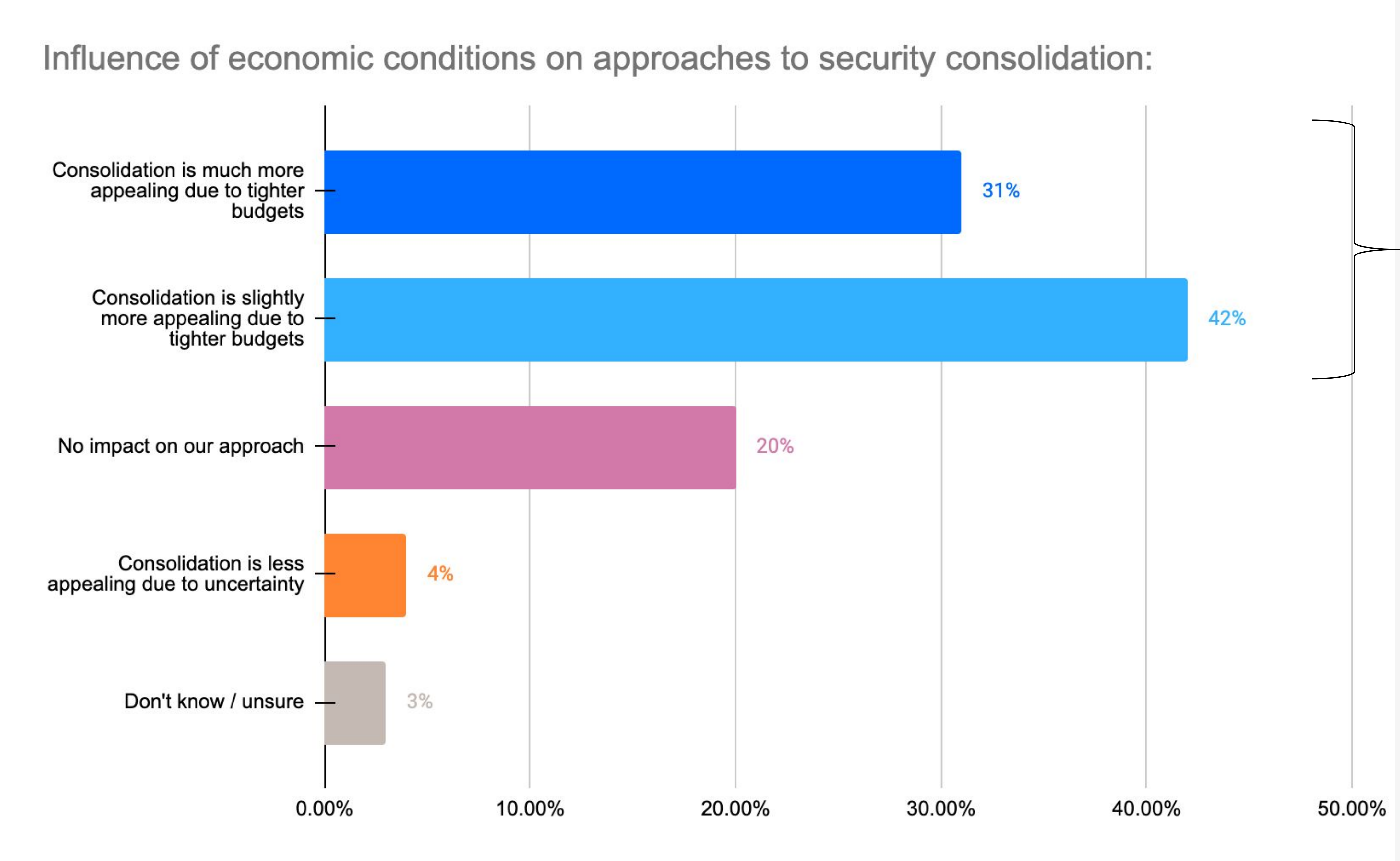


52% in organisations with 250-999 employees,
46% in organisations with 1,000-4,999 employees

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: 1800

Economic Influence on Security Consolidation

Almost three quarters (73%) say that consolidation is more appealing due to tighter budgets



73% more appealing

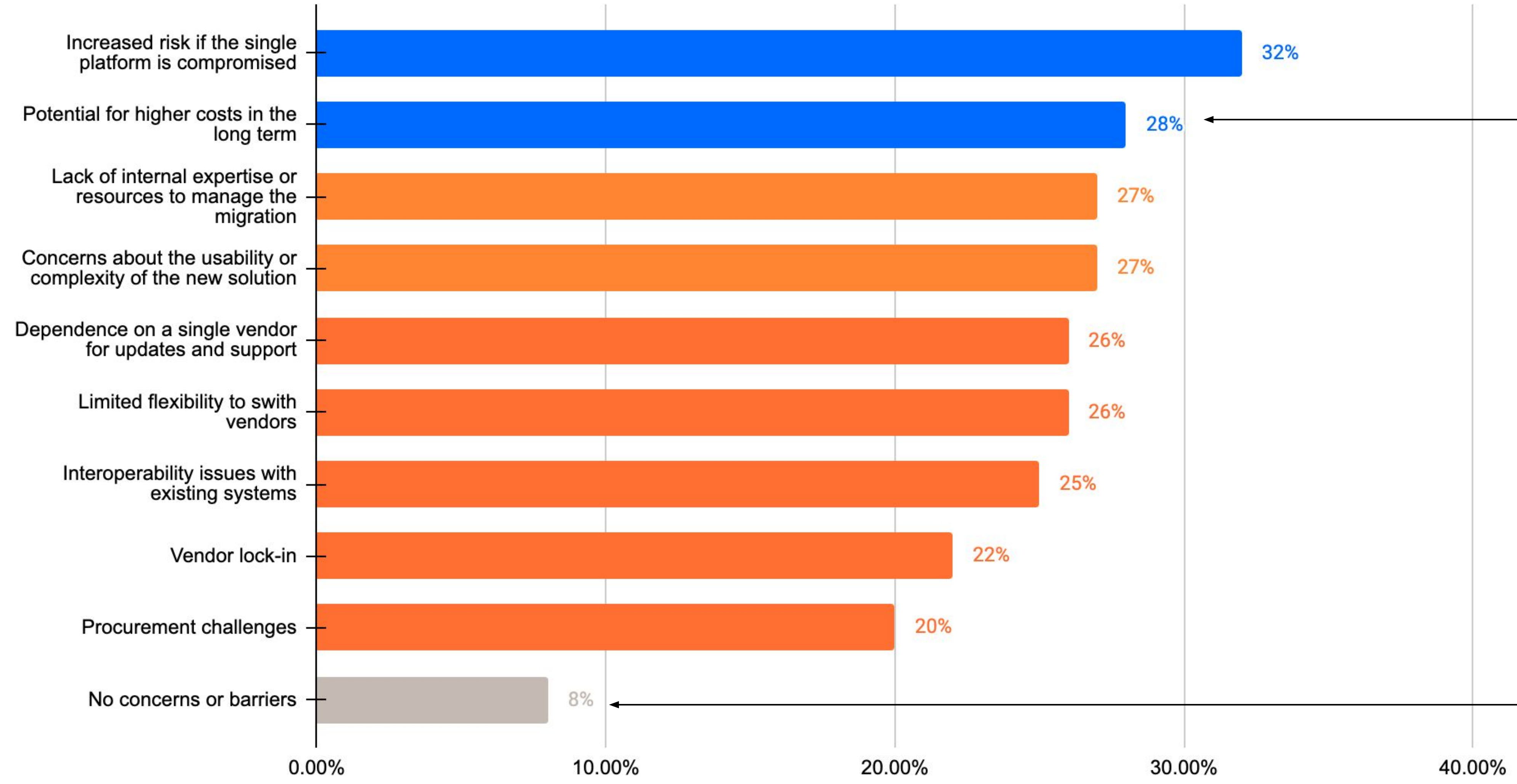
80% in Technology,
58% in Government / Public Sector

Q23b. How have economic conditions influenced your organisation's approach to security consolidation? Select one| Base: 1726

Concerns with Security Tool Consolidation

A third (32%) are concerned about **increased risk if the single platform is compromised** when it comes to consolidating security tools, shortly followed by the **potential for higher long-term costs (28%)**

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



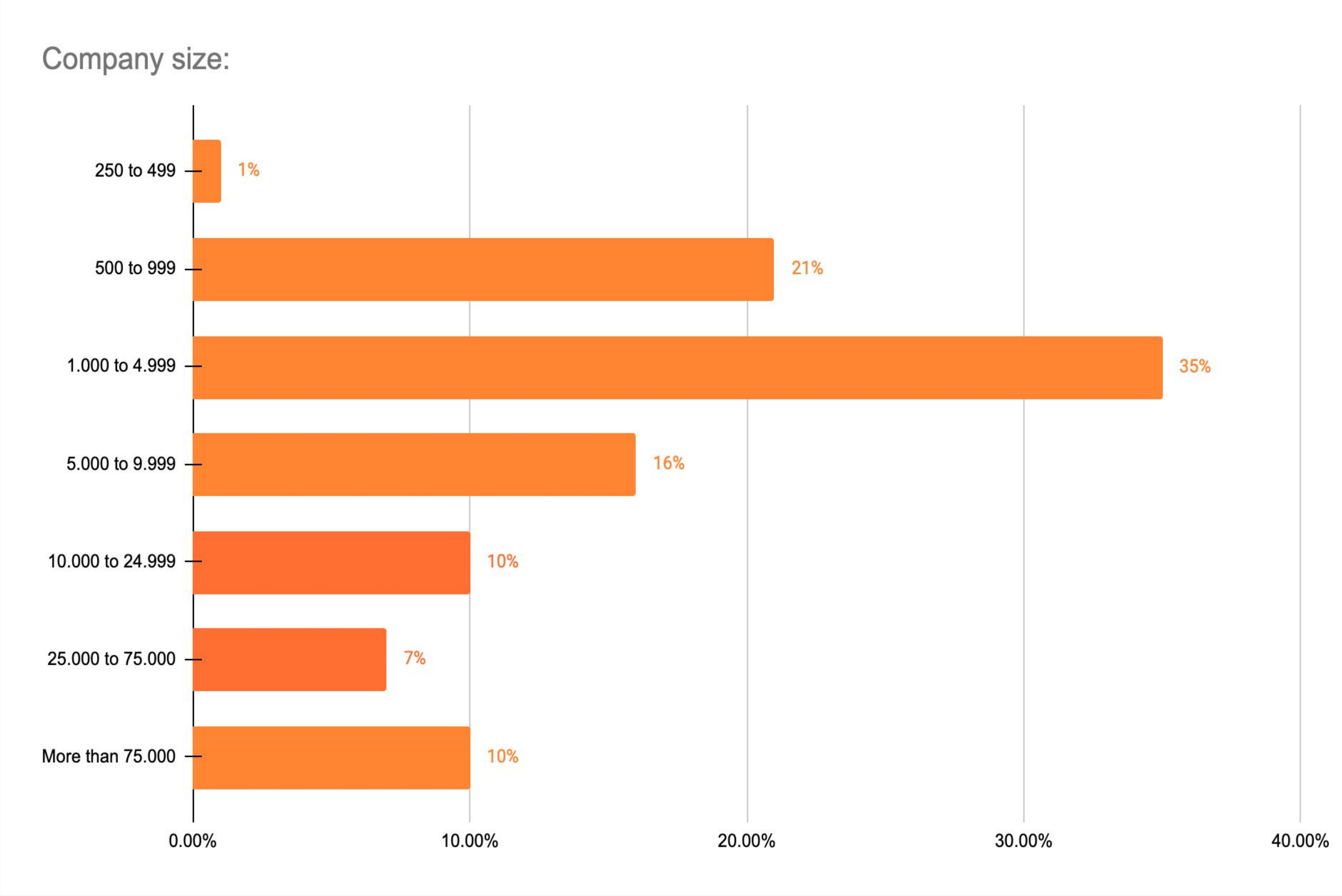
32% in organisations with 250-999 employees,
24% in organisations with more than 25,000 employees

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: 1800

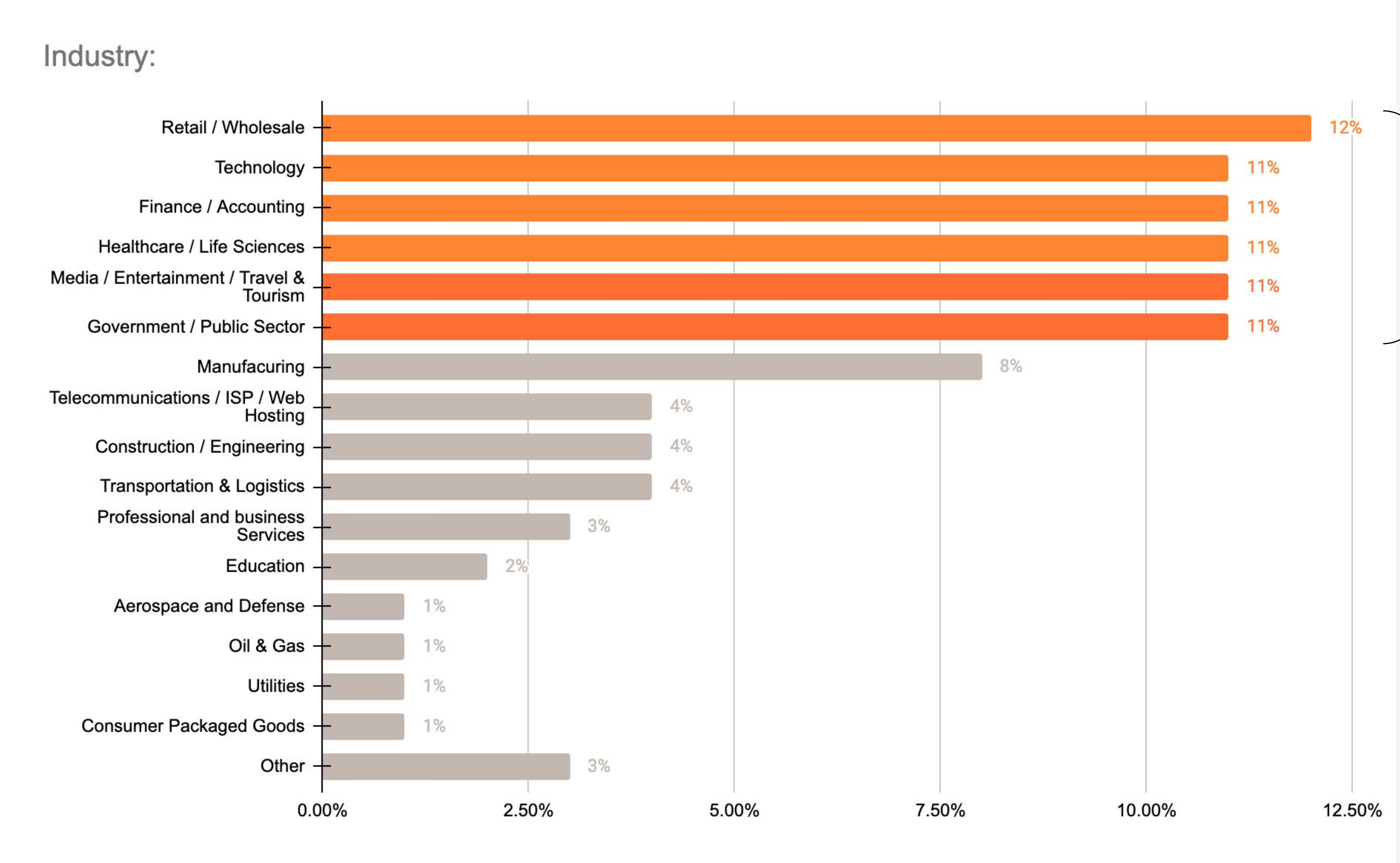
Demographics

Company size



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

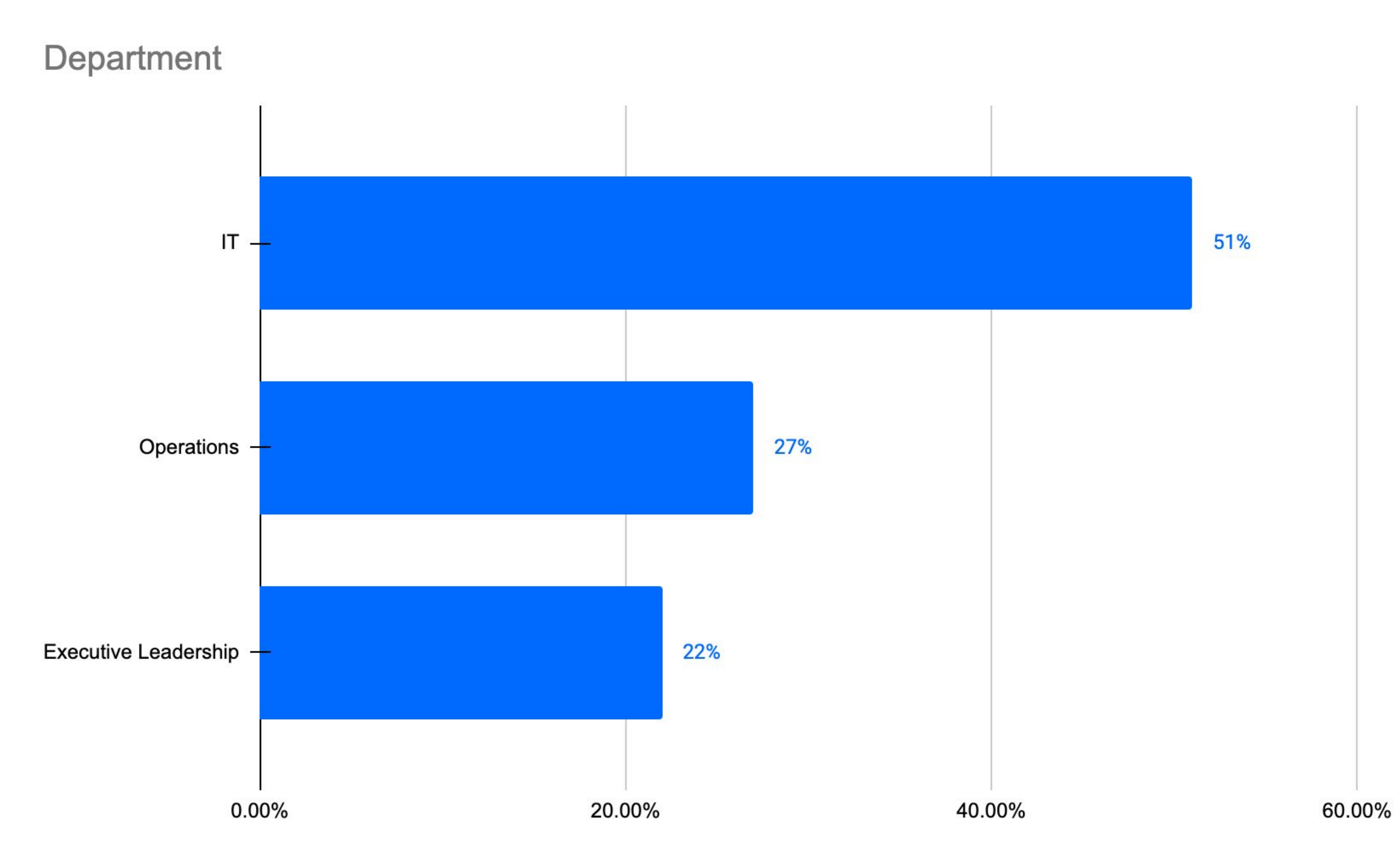
Industry

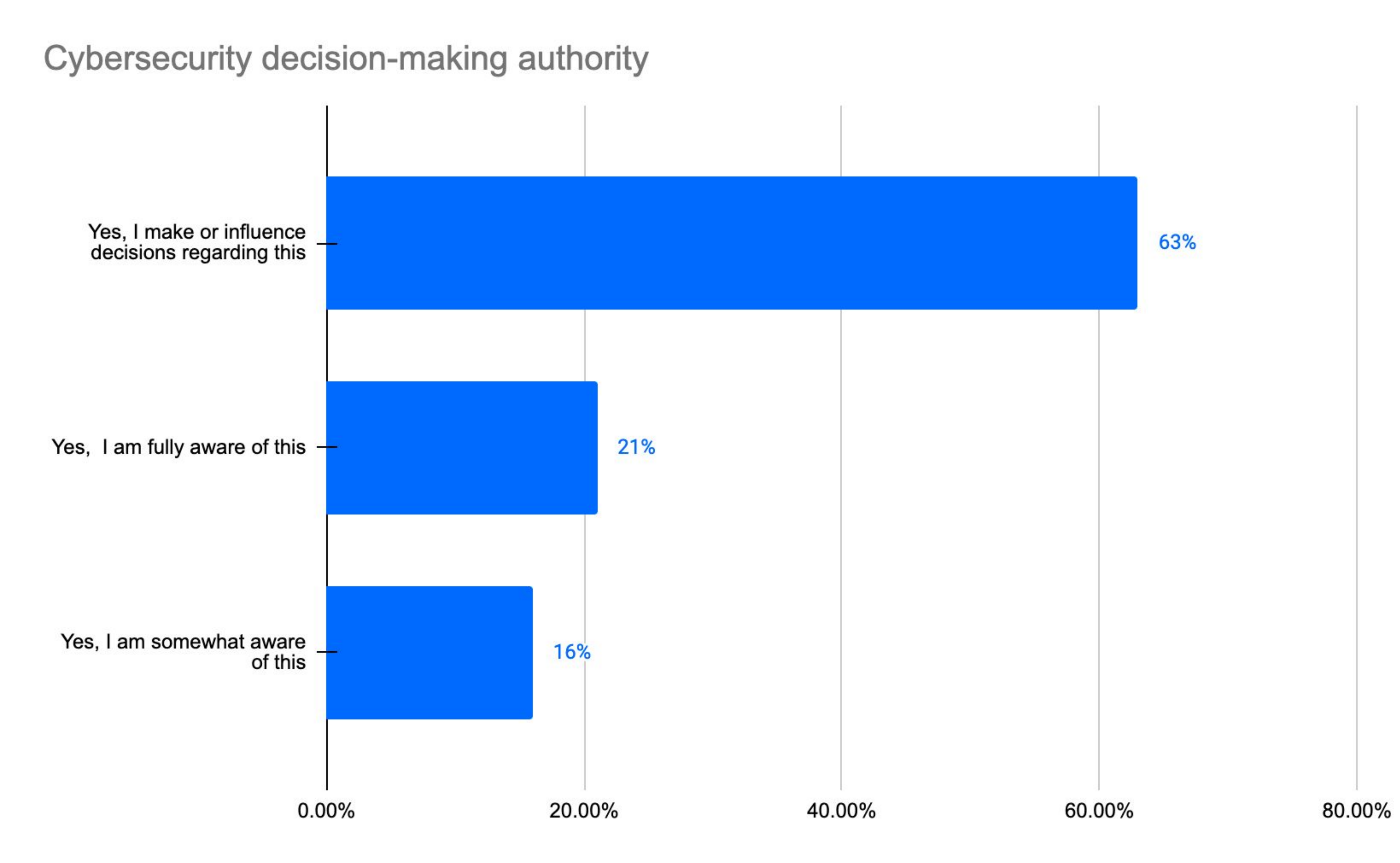


Focus Sectors

S3. Which of the following most closely describes the industry your organization is in? Select one | Base: 1800

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: 1800

Thank you!

fastly®