

A
Lynchpin
Media
BRAND



2024 LATAM CXO PRIORITIES REPORT:

Key cybersecurity trends,
challenges and priorities
for CIOs in Latin America

A CXO Priorities' report in partnership with



Contents

INTRODUCTION

3

SURVEY OVERVIEW

4

METHODOLOGY

5

SUMMARY OF FINDINGS

6

PART 1

THE ROLE OF THE CIO AND COMMUNICATIONS

8

PART 2

CIO BUSINESS PRIORITIES

16

PART 3

CIO CYBERSECURITY PRIORITIES

21

CONCLUSION

27

Introduction

Never has the pace of change been more rapid in the technology landscape. Digital tools are being used across all industries to transform the way businesses operate.

But this rapidly evolving digital landscape also presents challenges – particularly when it comes to cybersecurity. From compliance requirements to emerging threats, technology leaders must navigate a complex landscape to protect their organizations while also driving innovation and growth.

In this report, we delve into the key insights and priorities for Chief Information Officers (CIOs) in Latin America, uncovering a diverse range of concerns.

Governance, compliance and demonstrating ROI emerge as top priorities for respondents, while collaboration and communication across the C-suite are identified as critical components of an effective cybersecurity strategy. As organizations look to digital tools to drive profitability and efficiency, the role of the CIO in decision-making and strategic planning becomes increasingly prominent.

Our data identifies key priorities for CIOs in 2024, including improving IT resilience, understanding and prioritizing risk, and leveraging cloud technologies and automation to enhance security measures. These priorities underscore the strategic imperative for organizations to adapt to an increasingly digital and interconnected world while safeguarding against emerging threats.

The report provides valuable insights into the cybersecurity landscape for CIOs in 2024, highlighting the priorities, challenges and opportunities facing technology leaders. By understanding and addressing these trends, organizations can better navigate the complexities of cybersecurity and position themselves for success in an ever-changing digital environment.

Survey overview

To find out more about the current cybersecurity and IT challenges faced by CIOs in organizations in Latin America, we surveyed CIOs and Technology Leaders about their experiences and plans regarding key challenges and trends. This report aims to present an overview of the current threat landscape, explore advanced technologies and reveal how organizations plan to prioritise and invest.

Through this survey we aimed to discover:

The correlation between the **role of technology leaders** within an organization, their **communication patterns**, **primary concerns** and **rate of collaboration**.

How CIOs expect their **role to change** and their **priorities** for the **wider business**.

Routine **practices** and the adoption of **advanced technologies** within organizations.

Methodology

Total sample size: 200
CIOs and
Technology Leaders.

The **top three countries** in terms of responses were **Brazil (43%)**, **Mexico (23%)** and **Argentina (12%)**. Other countries also included Chile, Columbia, Peru, Uruguay, Ecuador, Costa Rica and Bolivia.

The **top 3 company sizes** that were surveyed were more than **50,000 employees (51%)**, **10,001–50,000 employees (37%)** and **5,001–10,000 employees (6%)**.

The **top 5 industries** that were surveyed included **Manufacturing (25%)**, **Financial Services (15%)**, **Utilities and Energy (10%)**, **Pharma and Life Sciences (9%)** and **Wholesale and Retail (6%)**.

Summary of findings

THE ROLE OF THE CIO AND COMMUNICATIONS

CIOs expect that they will face increased pressure to become **a revenue-generating part of the organization (33%)** over the next five years, as well as a requirement to become a **more strategic function within the business (33%)**.

The top two areas organizations expect to focus on to make 2024 successful are **improving IT and organizational resilience (20%)** and **understanding and prioritizing risk (15%)**.

Governance and compliance (18%) and **reporting and demonstrating ROI (13%)** are the leading professional concerns for CIOs in LATAM.

The majority of respondents will **prioritize cloud security, cyber-resilience and third-party risk management** over the next 12 months.

CIO BUSINESS AND CYBERSECURITY PRIORITIES

The top three IT priorities for the next 12 months are **cloud-first (21%)**, **cybersecurity focus and improvements (21%)** and **automation expansion (13%)**.

More than a third (**37%**) of respondents are using AI for **threat simulation and attack prediction**, while **27%** are using it for **malware detection and analysis**.

26% of respondents are **adopting AI** while **22%** have a **basic understanding of AI**.

A **quarter** of respondents said the most important role cybersecurity plays is **protecting the business and helping it to remain in business**.

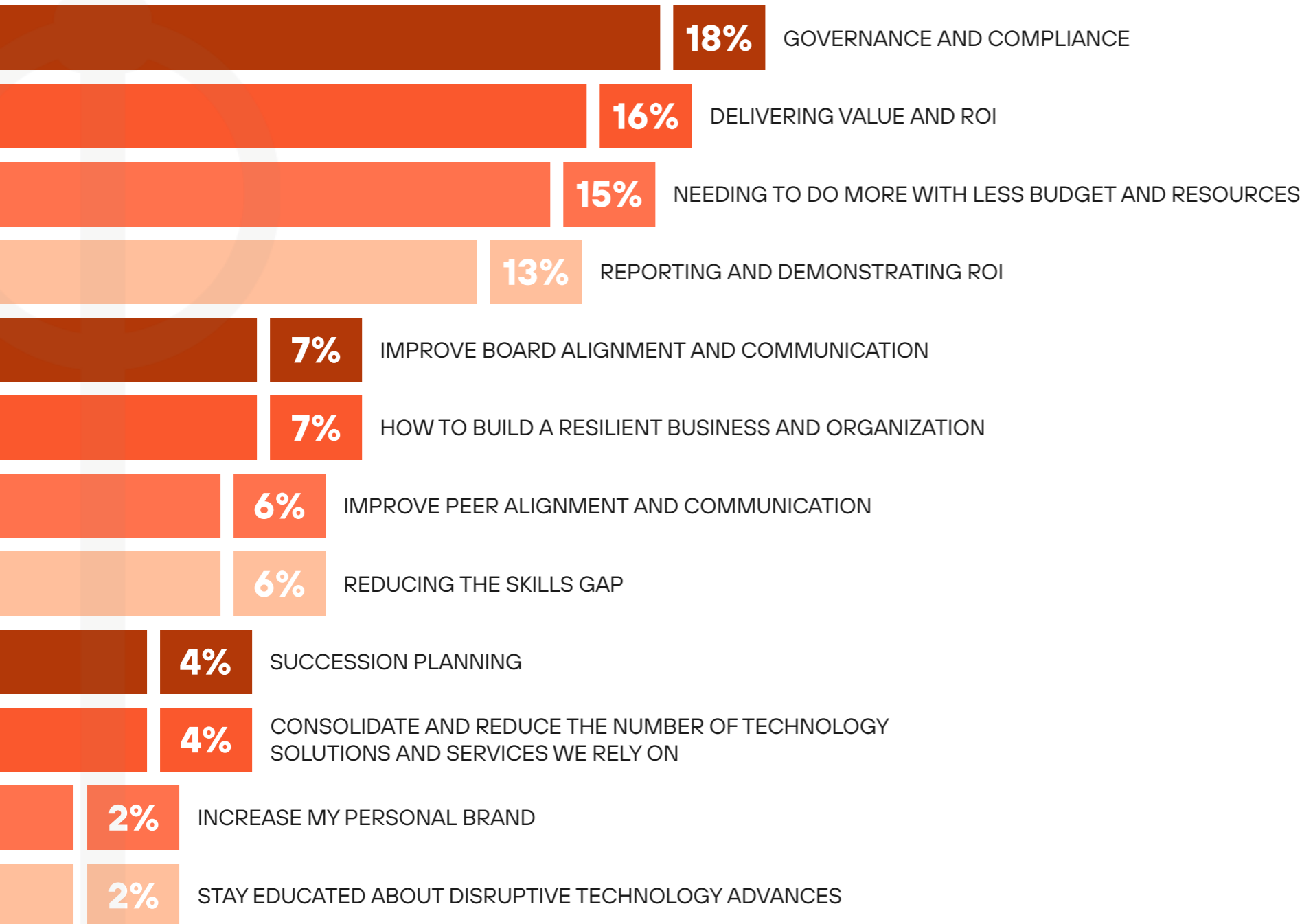
Part 1


The role of the CIO and communications





What are your primary professional concerns at the moment?



 Key insights:

Concerns are split across a range of responses, however governance and compliance received the largest share of the vote with 18%. This was followed by delivering value and ROI at 16% and needing to do more with less budget and resources at 15%.

The emphasis on ROI highlights the pressures CIOs are under to ensure technology investments can demonstrably deliver value. Compliance and governance are currently top of mind for technology leaders as international directives such as the Digital Operational Resilience Act (DORA), Cyber Resilience Act (CRA) and NIS2 Directive, as well as local regulations, require attention to avoid potential penalties.



In what ways do you think your role might change in the next five years?

 Key insights:

CIOs expect that they will face increased pressure to become a revenue-generating part of the organization (33%) over the next five years, as well as a requirement to become a more strategic function within the business (33%).

They also expect they will be required to enable business transformation. As organizations look to digital tools to increase profitability and improve business processes, CIOs expect to be under the spotlight as the decision-maker behind technology investments.

INCREASED PRESSURE TO BECOME A REVENUE-GENERATING PART OF THE ORGANIZATION

33%

BECOME A MORE STRATEGIC FUNCTION WITHIN THE BUSINESS

33%

ENABLE BUSINESS TRANSFORMATION

30%

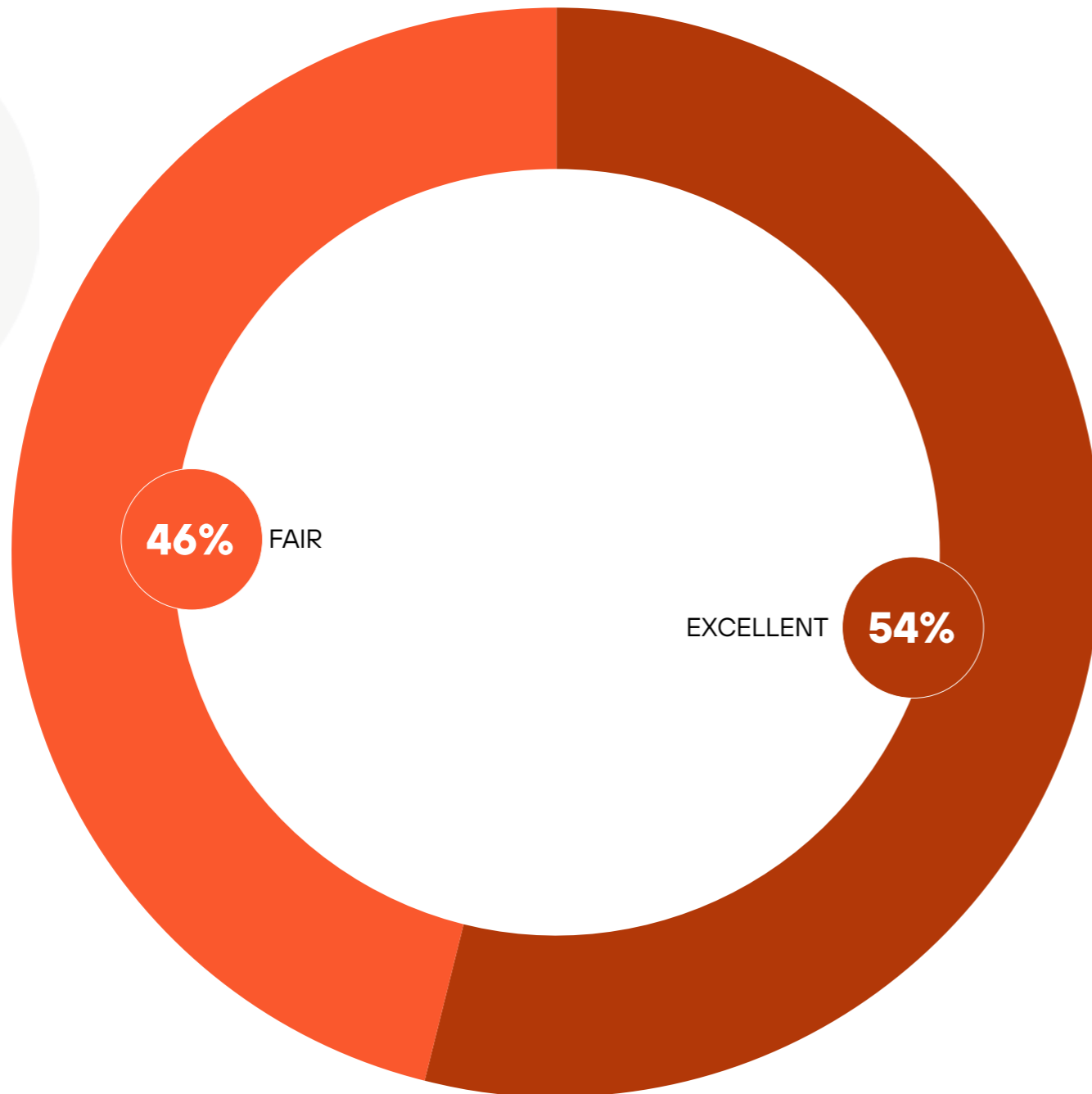
2% DRAMATIC CHANGE OF WHO CIO REPORTS TO

1% INCREASED PERSONAL LIABILITY

1% CIO ROLE WILL NO LONGER EXIST



How would you rate the collaboration between your role and the rest of the C-suite within your organization?



NEXT



Describe some of the ways collaboration with the rest of the business C-suite could improve?

This is how many times these words were used in responses.

Key insights:

Communication and collaboration are central tenets of C-suite cohesion – but neither are guaranteed. Success in this area is largely attributed to building a good company culture. This is particularly true when it comes to cybersecurity.

Our findings suggest this is widely recognised and prioritized by respondents, with more than half conceding that collaboration between their role and the wider C-suite was ‘excellent’.

However, there is scope to improve this as 46% of respondents said this collaboration was only ‘fair’. Some of the suggestions from respondents on how to improve this include:

- Ensuring cybersecurity measures support business growth and sustainability initiatives
- Enhancing communication and alignment to support digitalization efforts
- Leveraging technology for operational efficiency
- Facilitating cross-functional collaboration to strengthen cyber defense and safeguard critical assets
- Improving communication and coordination to drive Digital Transformation.

enhancing | 33

measures | 25

overall | 13

business | 38

digitalization | 20

operational | 9

aligning | 13

initiatives | 25

support | 45

sustainability | 25

efficiency | 9

ensuring | 25

strategies | 13

efforts | 20

alignment | 20

communication | 22

leveraging | 9

growth | 25

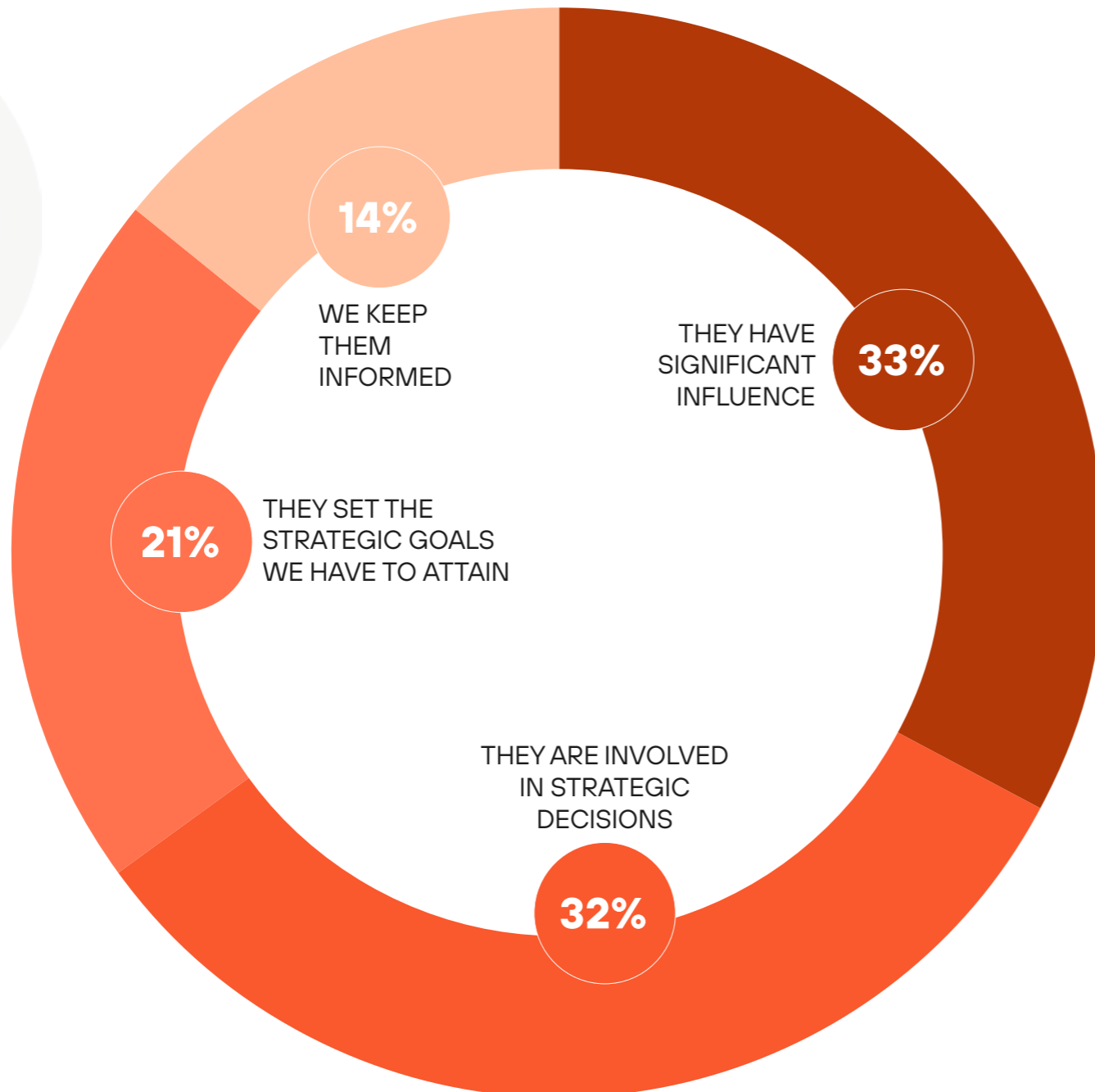
cybersecurity | 38

objectives | 13

Leveraging technology for operational efficiency.



How much influence and direction does the board have on your organization's cybersecurity strategy?



NEXT



Describe some of the challenges this presents you with.

This is how many times these words were used in responses.

Organization | 19

Positives | 16

Shortages | 12

Coping | 12

Expertise | 12

Struggling | 16

Alert | 16

Cybersecurity | 31

Fatigue | 16

Threat | 16

Gap | 12

Hindering | 16

Awareness | 19

False | 16

Hampering | 12

Training | 19

Effective | 28

Implementation | 12

Insufficient | 19

Response | 16

Under pressure from compliance and regulatory requirements, necessitating continuous adjustments to security policies and practices.

Key insights:

The findings reveal that the board has an important role in defining organizations' cybersecurity strategies. Only 14% of respondents reported a passive role for their board, in which they were kept informed but did not necessarily get involved in strategic objectives.

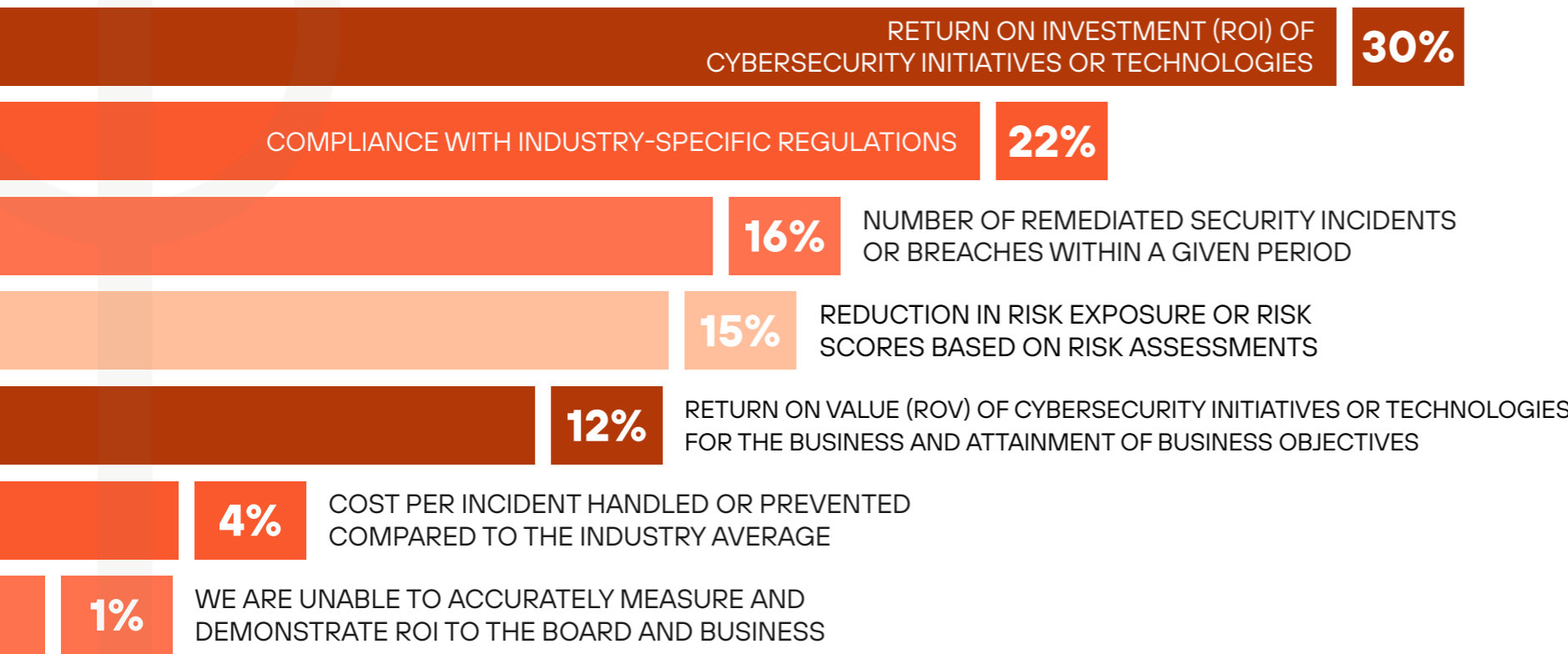
For 33% of respondents, the board has a 'significant influence' and for 32% the board is involved in strategic decisions.

The remaining 21% said the board sets their strategic goals. This is indicative of how cybersecurity is today a core business function and deeply embedded across the organizational structure. However, respondents did express some challenges, including:

- Coping with skill shortages and expertise gap, hampering effective cybersecurity strategy implementation
- Insufficient cybersecurity awareness and training across the organization
- Struggling with alert fatigue and false positives, hindering effective threat response
- Resistance to adopting new technologies in traditional industries
- Limited resources and budget allocation for IT initiatives
- Under pressure from compliance and regulatory requirements, necessitating continuous adjustments to security policies and practices.



What are some of the success metrics you use today to evaluate your security posture and demonstrate value to the business and board?



 Key insights:

On success metrics used in evaluating security posture and demonstrating value to the business and board, 22% of respondents use compliance with industry-specific regulations, indicating a strong adherence to regulatory standards.

A total of 30% measure success on the return on investment (ROI) of cybersecurity initiatives or technologies, underlining the financial aspect of security decisions. The reduction in risk exposure or risk scores based on risk assessments is a success metric measured by 15% of respondents, highlighting a proactive approach to risk management.

Other metrics such as cost per incident handled or prevented compared to the industry average, number of remediated security incidents or breaches within a given period and return on value (ROV) of cybersecurity initiatives or technologies for the business and attainment of business objectives are also considered, though to a lesser extent.

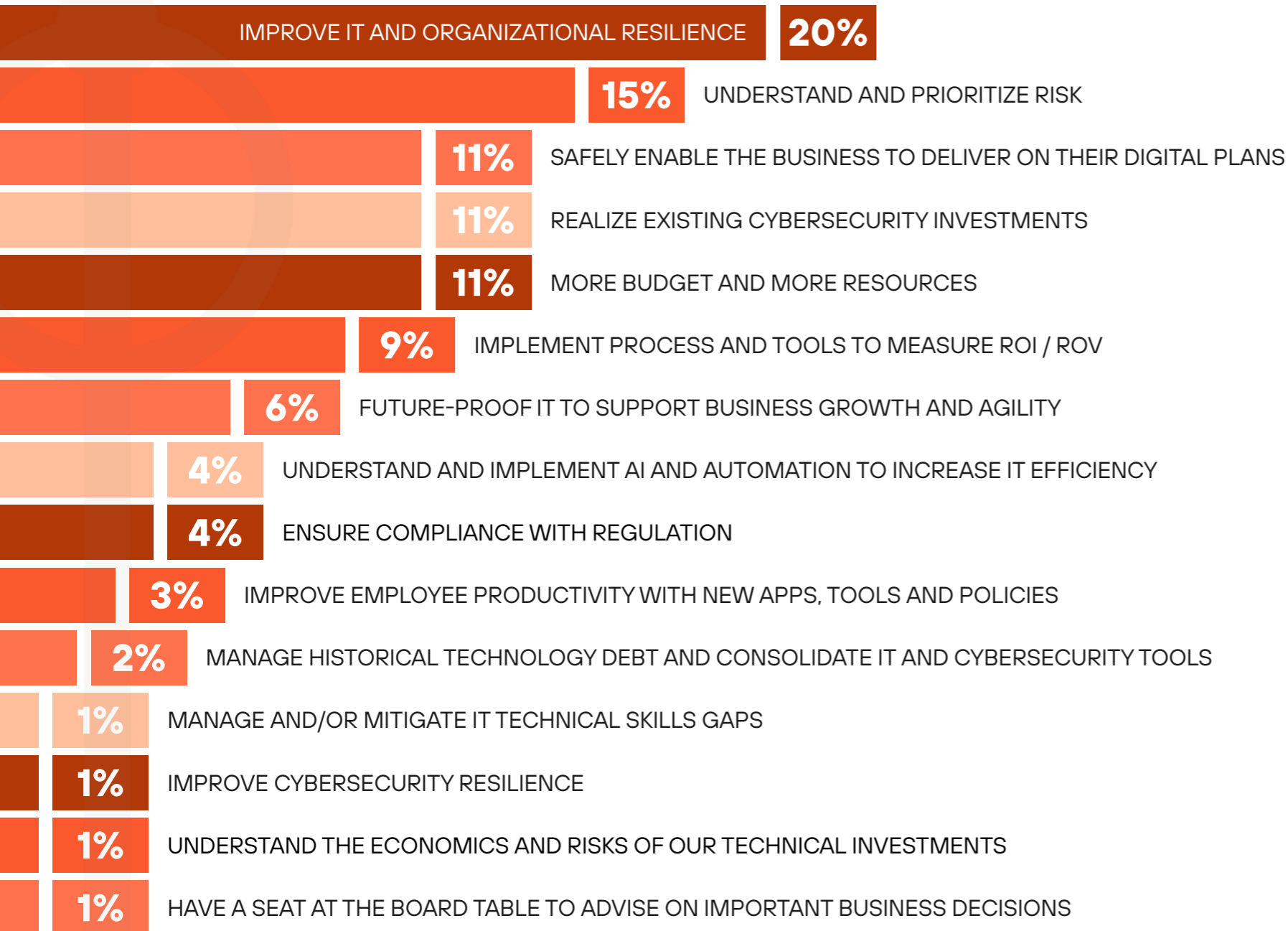
Part 2

CIO Business Priorities





What are the top five things you need to make you, and your business, successful in 2024?



 Key insights:

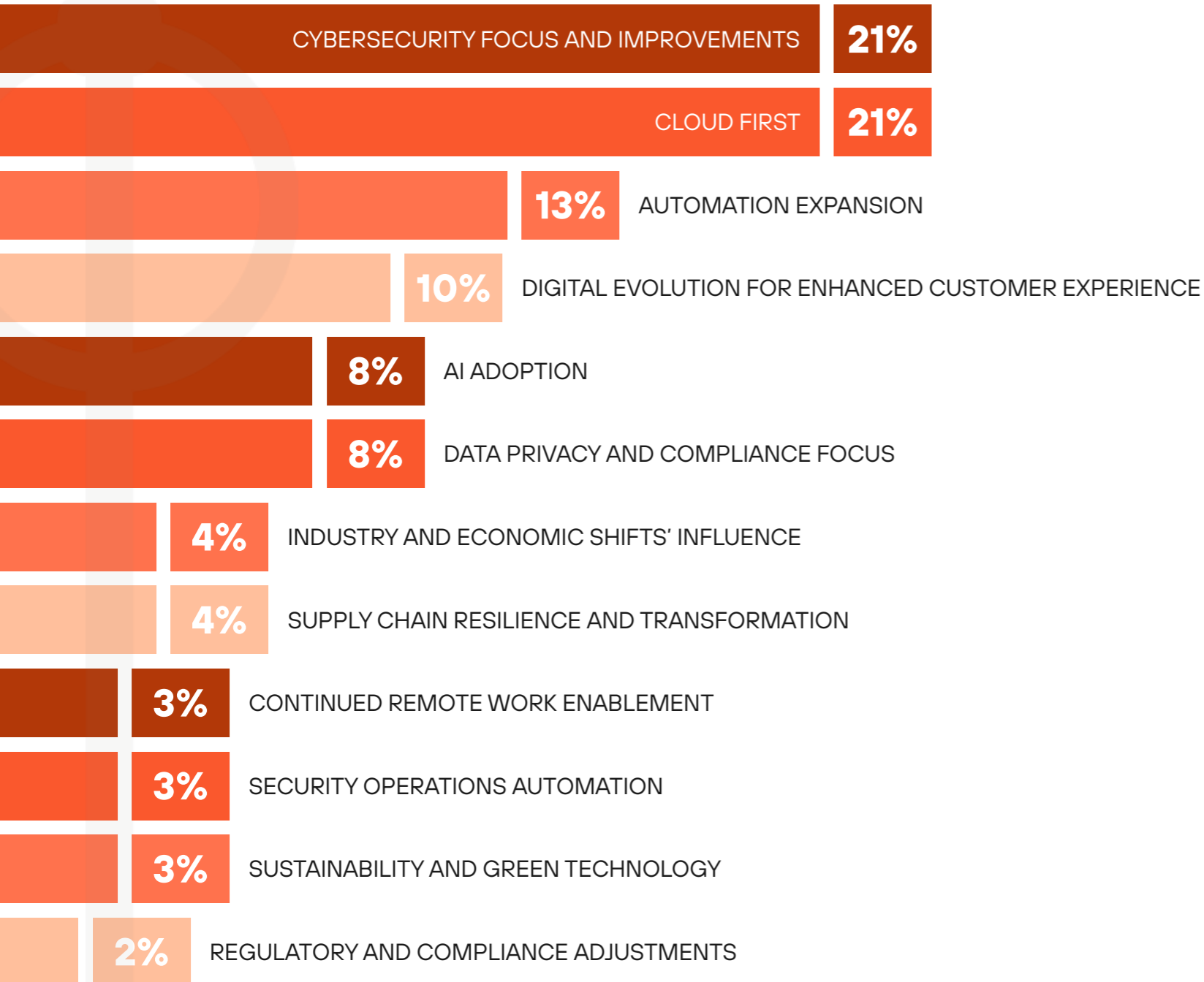
The top five focus areas to ensure success in 2024 are:

- Improve IT and organizational resilience (20%)
- Understand and prioritize risk (15%)
- Safely enable the business to deliver on their digital plans (11%)
- Realize existing cybersecurity investments (11%)
- More budget and more resources (11%)

These priorities indicate a strong emphasis on resilience, Digital Transformation, risk management, cybersecurity and resource allocation as critical factors for success in 2024.



What are your organization's top three IT priorities for the next 12 months?



 Key insights:

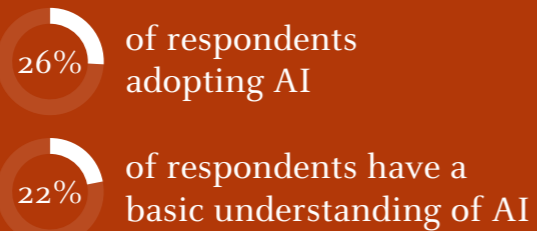
The top three IT priorities for the next 12 months are cloud-first (21%), cybersecurity focus and improvements (21%) and automation expansion (13%).

These priorities reflect a strategic focus on enhancing security measures, leveraging cloud technologies and exploring and enhancing automation initiatives to drive business growth and resilience in the evolving technological landscape.

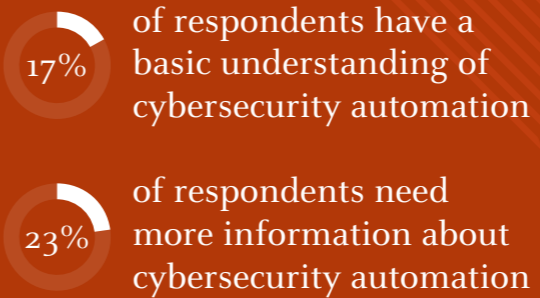


Which technology trends do you think will have the biggest impact on your future business priorities and how prepared are you to adopt them?

AI



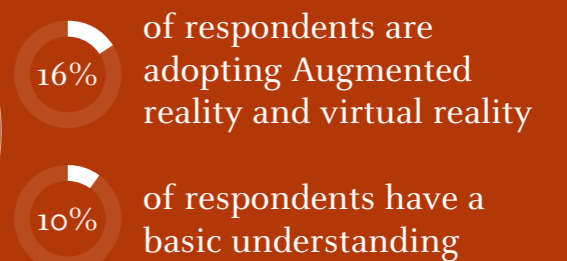
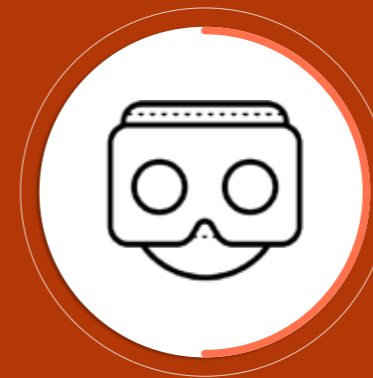
Cybersecurity automation



Sustainability



Augmented Reality and Virtual Reality



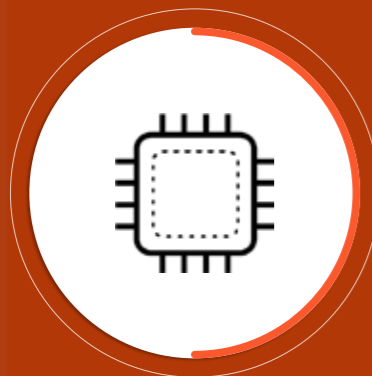
Autonomous Systems



 25% of respondents are adopting Autonomous Systems

 23% of respondents need more skills with Autonomous Systems

Quantum Computing





 12% of respondents are adopting Quantum Computing

 15% of respondents need more information about Quantum Computing

Service-based offerings



 16% of respondents need more information about service-based offerings

 15% of respondents have a basic understanding of service-based offerings

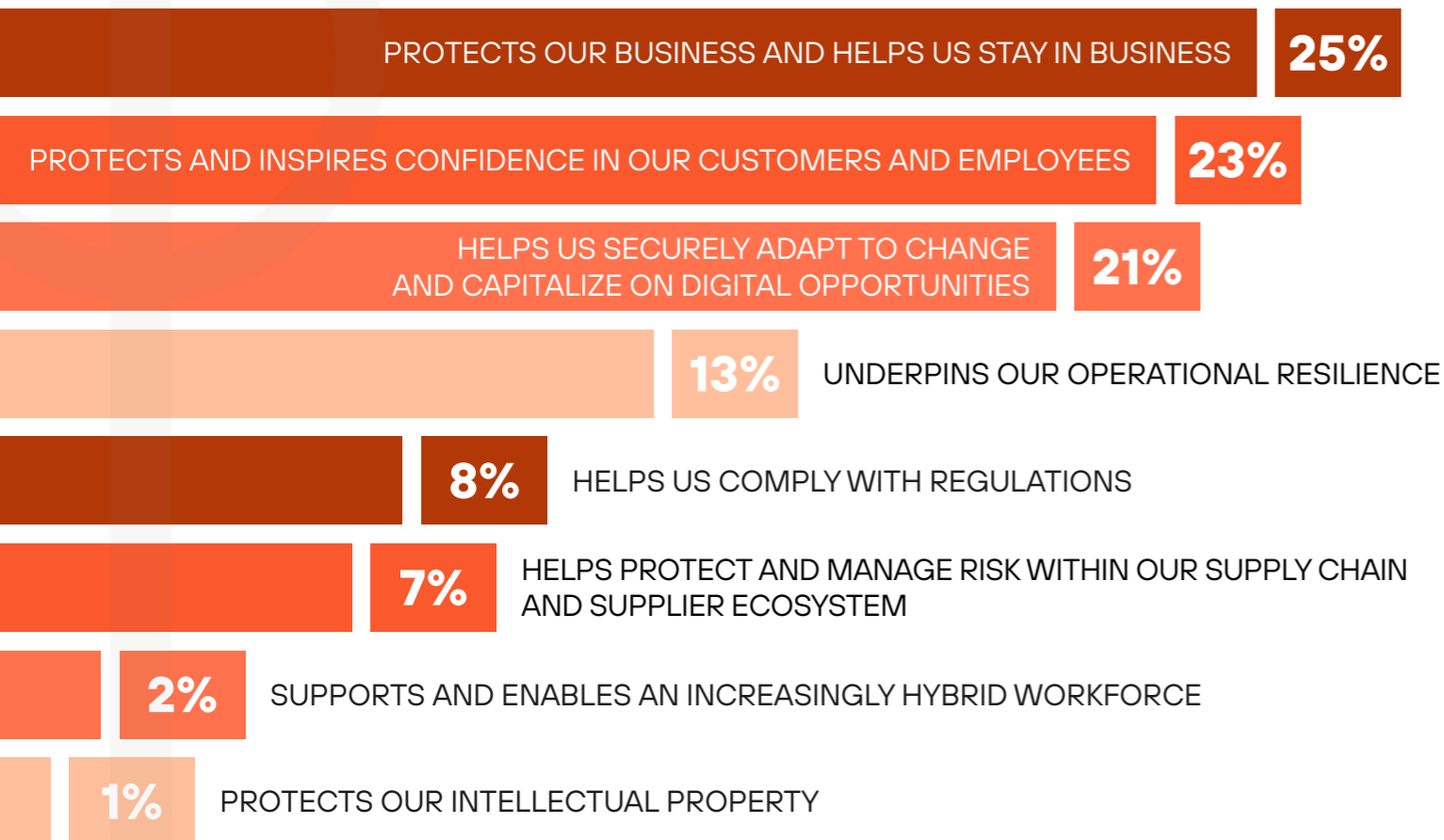
Part 3

CIO Cybersecurity Priorities





What is the most important role that cybersecurity plays in helping your organization to be successful?



 Key insights:

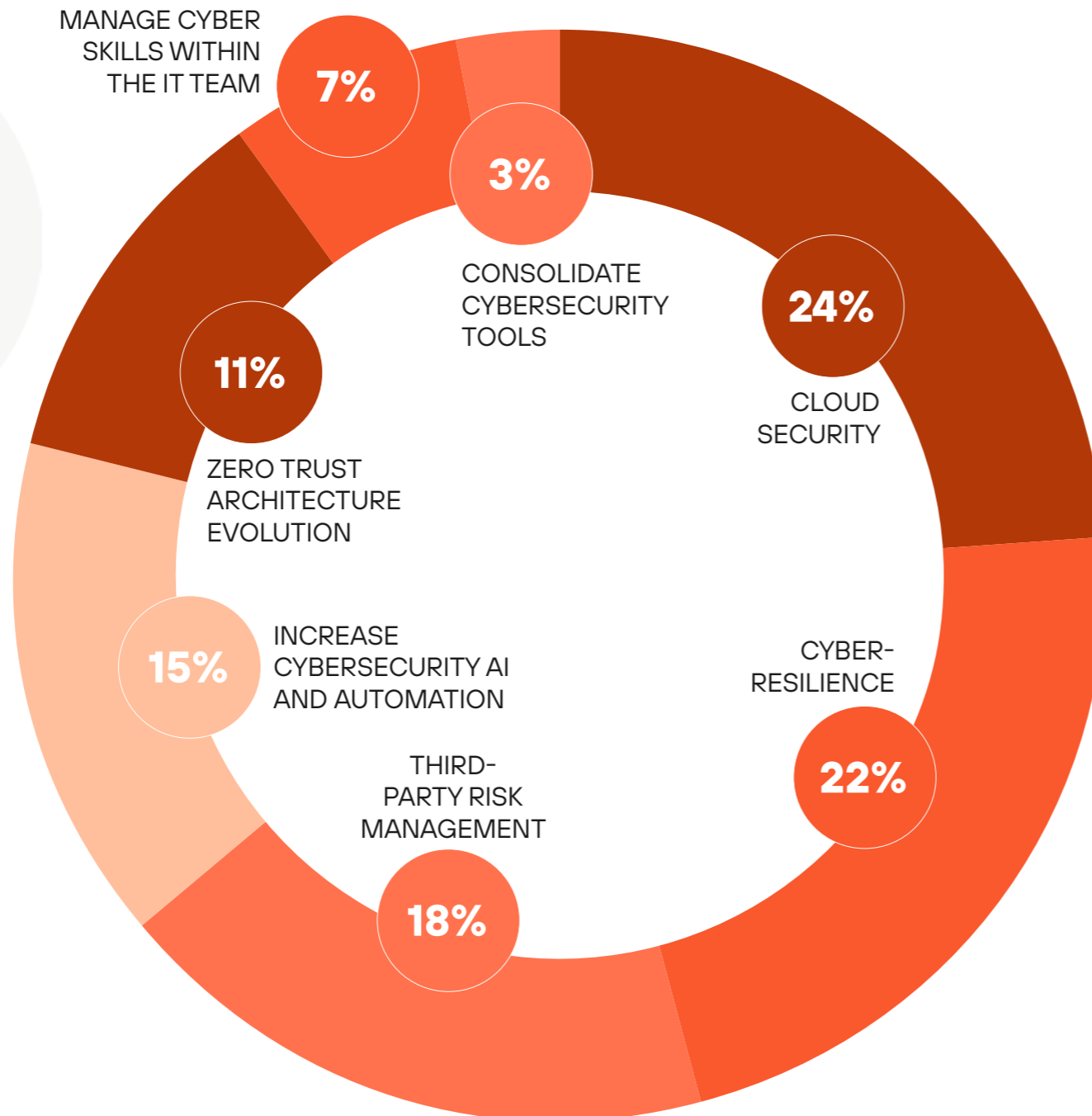
A quarter of respondents said the most important role cybersecurity plays is protecting the business and helping it to remain in business. This highlights an understanding between the importance of robust cybersecurity for determining business success, not just for CISOs but across the wider C-suite.

‘Protects and inspires confidence in our customers and employees’ took 23% of the vote – evidence that organizations are placing a large portion of responsibility on the role of cybersecurity for helping to protect and inspire confidence in their customers and employees. With 21% of the vote, was the belief that security helps organizations to securely adapt to change and capitalize on digital opportunities.

The underlying message here is that without a resilient and unwavering cybersecurity posture, customers will lose confidence and organizations will have little to no chance of investing in and capitalizing on digital opportunities, while also risking going out of business.



What are your top three cybersecurity priorities for the next 12 months?



 Key insights:

The majority of respondents will prioritize cloud security, cyber-resilience and third-party risk management over the next 12 months, while just 7% said they will prioritize the management of cyberskills within the IT team.

This suggests a primary focus on the business rather than on its people which could spark an interesting debate.

Arguably, cybersecurity skills and education underpin the backbone of an organization so it's crucial that this area of investment doesn't fall by the wayside when focusing on other areas of the business.

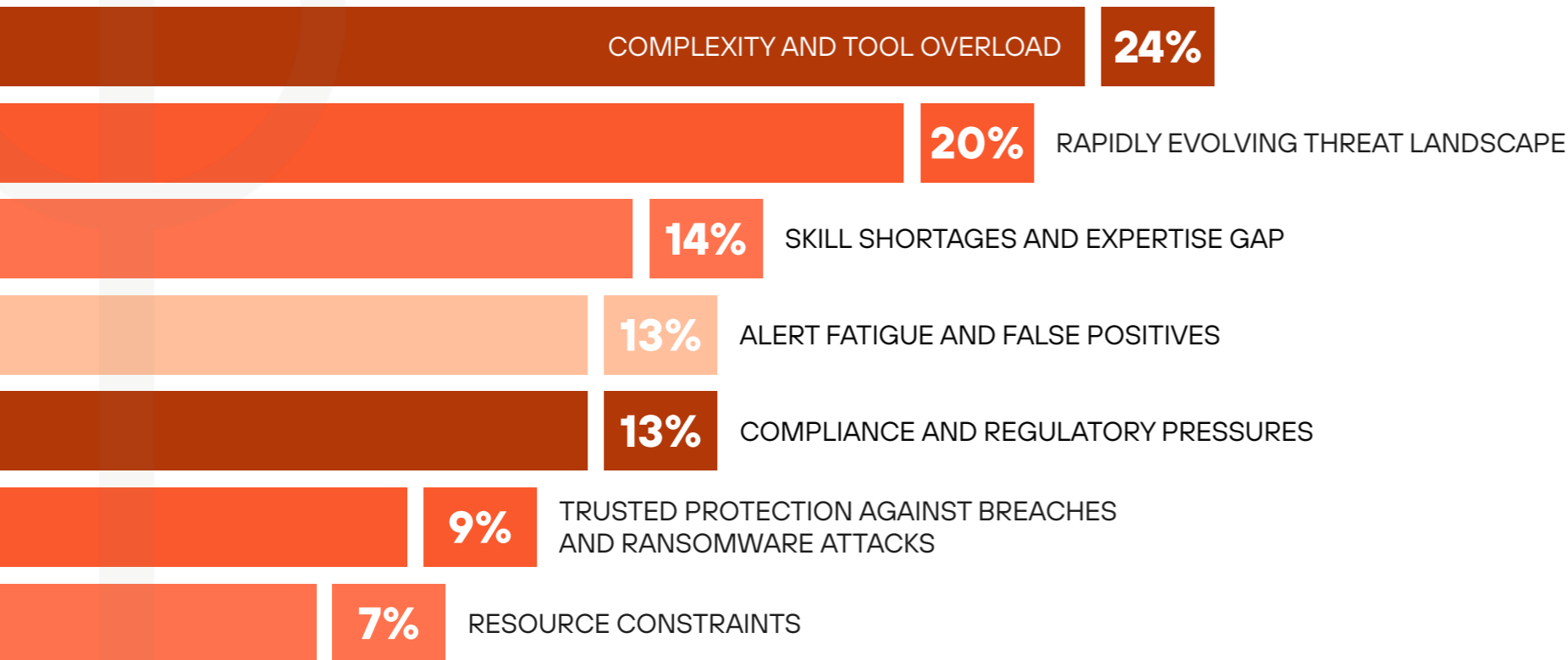


What are the most common challenges you experience in managing your cybersecurity tools and solutions?

 Key insights:

Aside from the common cybersecurity challenges we'd expect to prevail here – such as the rapidly evolving threat landscape (20%) – less of a concern for respondents in terms of challenges around tools and solutions, is resource constraints (7%).

This could suggest that organizations are investing more widely in resources such as AI and automation in order to manage such challenges.





Are you using AI and automation in any of the following applications to address a cybersecurity skills gap?



 Key insights:

AI and automation are dominating the tech landscape and organizations are eagerly looking to identify how they can use these tools to augment and streamline processes.

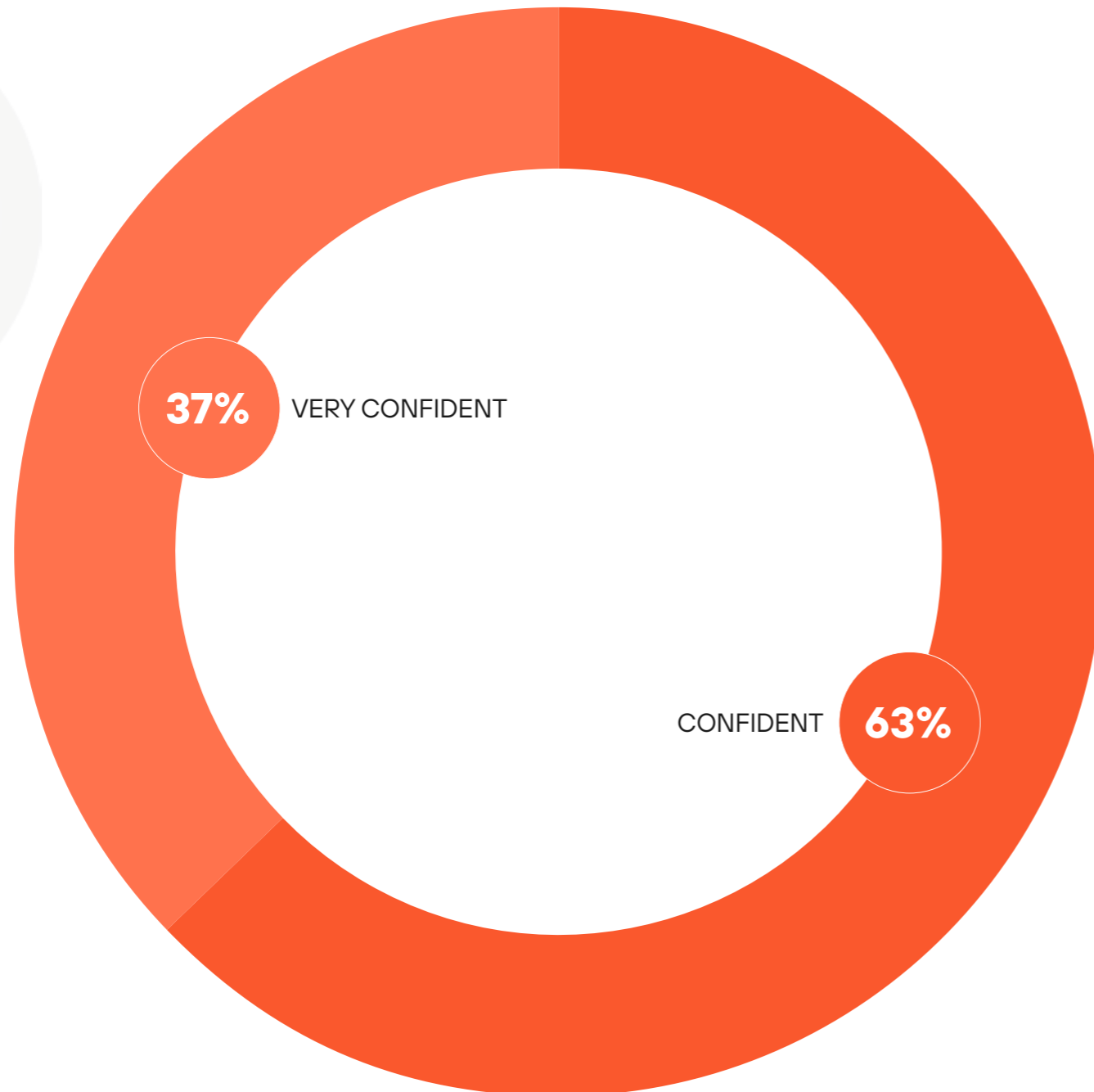
Although malicious actors are also using AI to orchestrate quick attacks, there are also many use cases for automation in enabling stronger defences too – particularly in an industry which is well-known for its skills shortage.

Indeed, more than a third (37%) of respondents are using AI for threat simulation and attack prediction, while 27% are using it for malware detection and analysis.

These results align with how many organizations are utilising AI and automation across the wider cybersecurity landscape and highlight the positive impact that the technology is having.



In the event of a cyberattack, how confident are you in your organization's ability to respond and maintain business operations while protecting critical data?



 Key insights:

Data is often referred to as the 'beating heart' of an organization which shows the gravity it holds and the importance of securing it.

Survey respondents were either 'confident' (63%) or 'very confident' (37%) in their abilities to respond and maintain business operations while protecting critical data, reaffirming the belief that organizations are prioritizing the protection of critical data as part of their strategy.

The results are reflective of business capabilities in today's landscape and help to generate a level of confidence in customers.

Conclusion

As CIOs anticipate a shift towards a more strategic role over the next five years, their focus will increasingly be on enabling business transformation through the adoption of advanced technologies.

Cybersecurity remains a top concern, with AI being crucial for threat simulation, malware detection, and automating security operations. Compliance with regulations like DORA, CRA, and NIS2 requires continuous policy adjustments with particular focus on the supply chain.

The rise of remote work and the proliferation of IoT devices has made cybersecurity a top priority for the coming year. Nearly half of the respondents are enhancing their security operations with AI and automation to address skills gaps, inspiring confidence among employees and protecting critical functions.

The report underscores the need for a culture of cybersecurity awareness and training, with AI adoption for automation and cyber resilience becoming common. Trends such as a cloud-first approach, cybersecurity focus, and automation expansion are shaping the future.

CIOs must ensure technology investments deliver measurable ROI, leveraging digital tools to enhance profitability and streamline processes. Collaboration within the C-suite and across functions is essential for strengthening cyber defences and aligning strategic objectives.

In summary, the report highlights the need for adaptive strategies addressing cybersecurity challenges, fostering awareness, emphasising ROI, and promoting collaboration. Tech leaders' strategic focus will be key to driving business transformation and ensuring long-term success.



A
Lynchpin
Media
BRAND



CxO Priorities, a Lynchpin Media brand
63/66 Hatton Garden
London, EC1N 8LE

www.cxopriorities.com

Sponsored by:



3000 Tannery Way
Santa Clara, CA 95054
info@paloaltonetworks.com

www.paloaltonetworks.com