A Lynchpin Media BRAND

CXO priorities

2024 EUROPE CXO PRIORITIES REPORT:

Key cybersecurity trends, challenges and priorities for CIOs in Europe

A CXO Priorities' report in partnership with paloalto NETWORKS

paloalto NETWORKS

priorities

A Lynchpin Media BRAND

Contents

Introduction

In the ever-evolving landscape of digital threats, cybersecurity stands as a paramount concern to businesses around the world. Europe, with its burgeoning digital economy and expanding connectivity, also faces a myriad of these cybersecurity challenges. From the relentless onslaught of sophisticated cyberattacks to the complexities of regulatory compliance, CIOs are now tasked with navigating a dynamic and high-stakes environment.

Amidst this backdrop are key trends including the rise of remote work which has transformed traditional office dynamics and presented new vectors for cyberthreats, the proliferation of cloud computing and Internet of Things which compounds the challenges necessitating robust security measures to mitigate vulnerabilities.

As CIOs in Europe grapple with these multifaceted challenges, there is the imperative to understand and act on key cybersecurity trends that will enable balancing investments in cutting-edge technologies, fostering a culture of awareness and resilience and forging collaborative partnerships within the industry.

Survey overview

To find out more about the current cybersecurity and IT challenges faced by CIOs in organisations in Europe, 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 organisations plan to prioritise and invest.

Through this survey we aimed to discover:

The correlation between the **role of technology leaders** within an organisation, 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 organisations.

Methodology

Total sample size: 250 CIOs and Technology Leaders.

The top three countries in terms of responses were United Kingdom (45%), Germany (25%) and France (9%). Other countries also included Netherlands, Sweden, Italy, Belgium, Norway and Switzerland.

The top 3 company sizes that were surveyed were more than 50,000 employees (32%), 10,001–50,000 employees (30%) and 1,001–5,000 employees (19%).

The top 5 industries that were surveyed included Manufacturing (21%), Financial Services (21%), Wholesale and Retail (9%), Utilities and Energy (9%) and Professional and Legal Services (6%).

Summary of findings

THE ROLE OF THE CIO AND COMMUNICATIONS

Governance and compliance (20%) and **reporting and demonstrating ROI** (18%) are the leading professional concerns for European CIOs.

Between-department collaboration (72%) and **collaboration itself** (68%) are revealed as the top areas of improvement if businesses want to foster collaboration with C-suite.

Managing (48%) and **navigating** (38%) the complex array of factors involved are the biggest challenges IT executives face when the board influences and directs their organisation's cybersecurity strategy.

Enhancing IT and **organisational resilience** was selected by one fifth of respondents (20%) to make their business successful in 2024.

CONTINUED

CIO BUSINESS AND CYBERSECURITY PRIORITIES

Automation expansion (29%) and **cybersecurity focus and improvements** (21%) were cited as top IT priorities for the next months.

Protecting and managing risk within the supply chain and **supplier ecosystem** were selected by 21% of respondents in helping organisations to be successful with cybersecurity.

Cloud security (24%) and **Zero Trust architecture evolution** (15%) were selected as the top cybersecurity priorities for the next 12 months.

Complexity and tool overload (25%) and **compliance and regulatory pressures** (25%) were selected are the most common challenges when managing cybersecurity tools and solutions.

Nearly half of respondents (49%) are **enhancing security operations and incident response as part of AI and automation** to address cybersecurity skills gaps.

paloalto NETWORKS

priorities

A Lynchpin Media BRAND

Part 1

The role of the CIO and communications

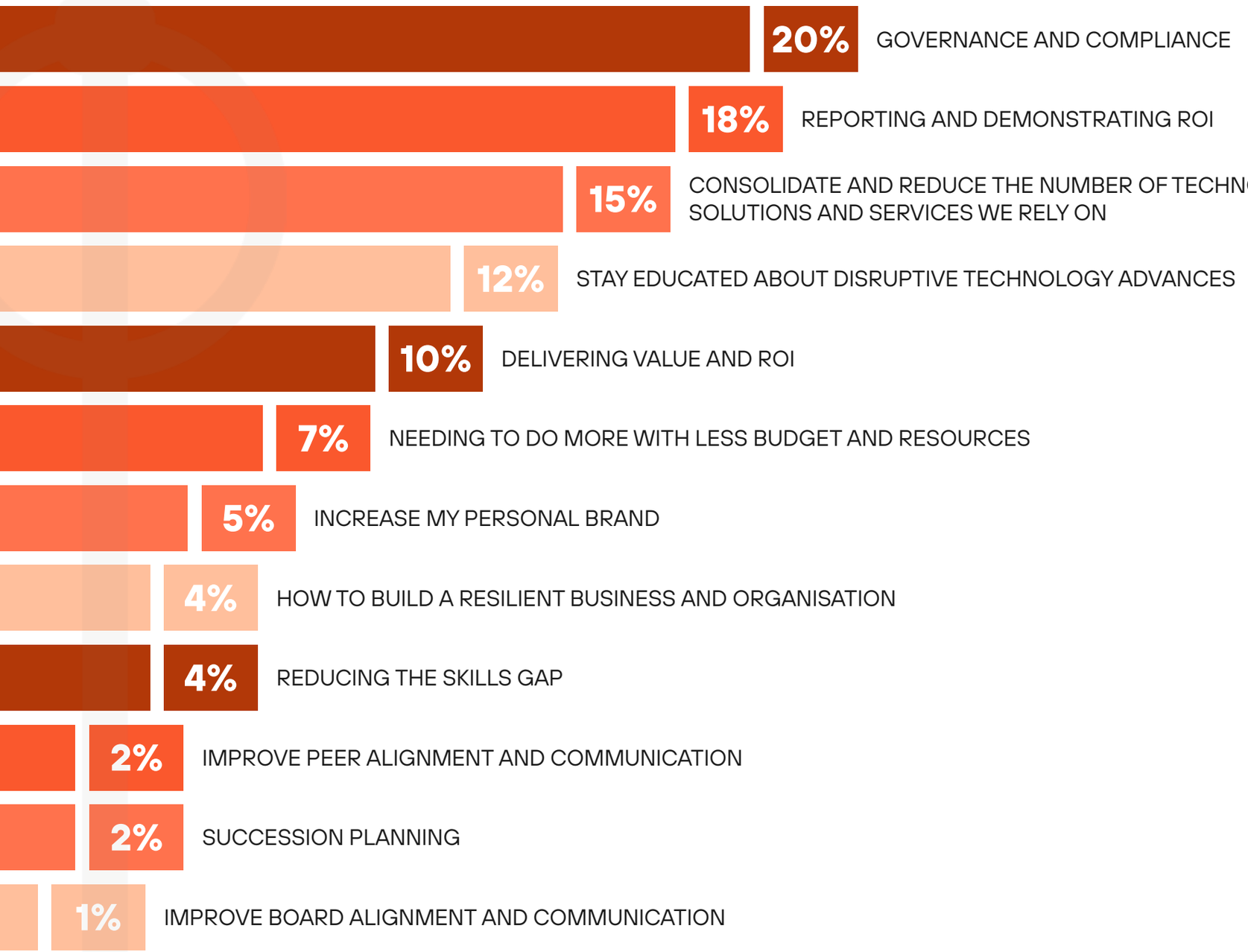
paloalto NETWORKS

priorities

A Lynchpin Media BRAND

1

What are your primary professional concerns at the moment?



Key insights:

Respondents attest that their primary professional concerns are governance and compliance (20%) and reporting and demonstrating ROI (18%).

This is closely followed by consolidating and reducing the reliance on technology solutions and services garnering 15% of responses.

Additionally, staying educated about disruptive technology advances and delivering value and ROI were notable concerns, each accounting for 12% and 10% respectively.

These findings reveal top concerns of IT professionals; rules compliance, proving value, leveraging tech and staying updated and prompts consideration of AI adoption while stressing automation's critical role in cybersecurity.

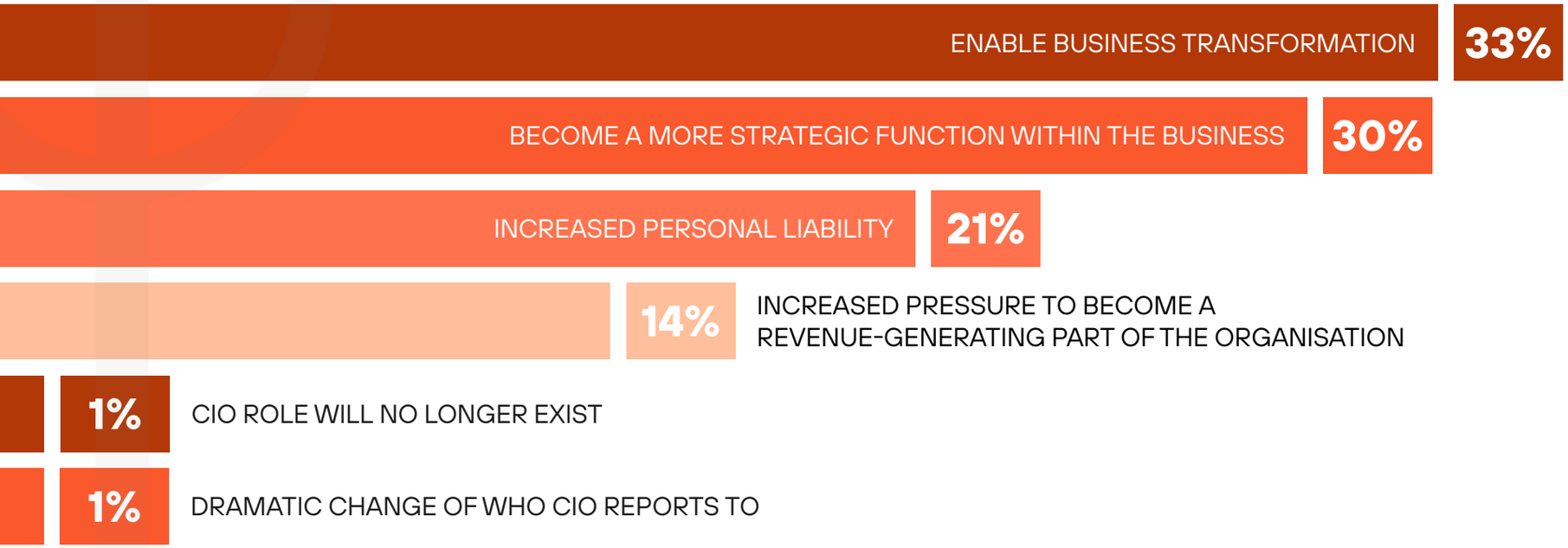
paloalto NETWORKS

priorities

A Lynchpin Media BRAND

2

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



Key insights:

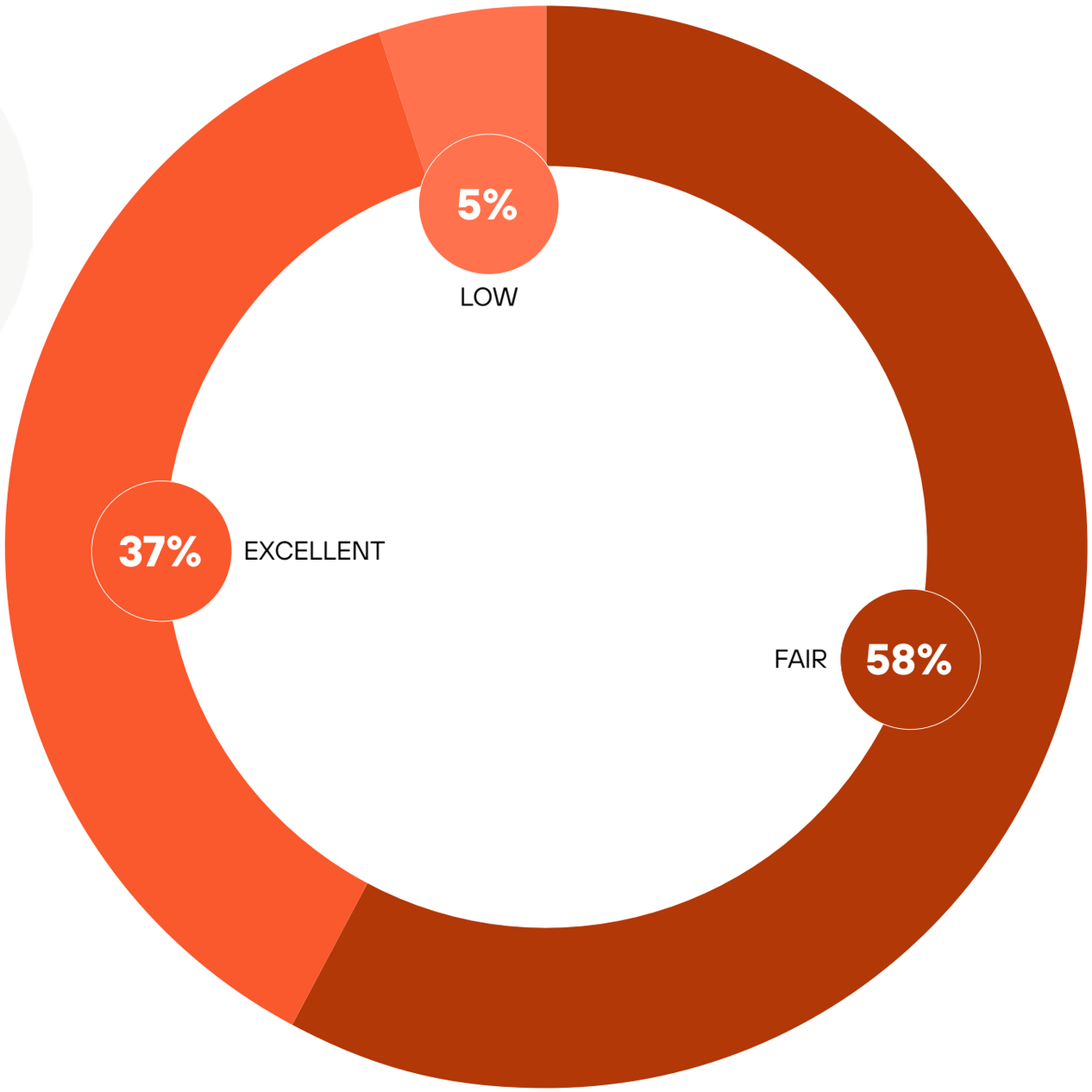
On anticipating a change in their roles over the next five years, 30% of respondents believe their role will evolve to become more strategic within the business while 33% foresee enabling business transformation as a crucial evolution.

Additionally, 21% anticipate increased personal liability, suggesting a heightened sense of accountability in their positions. Notably, only a small percentage (1%) envisage a dramatic change in reporting structure.

These insights highlight the need for proactive adaptation to evolving responsibilities and a heightened sense of personal accountability, rather than a drastic change in reporting structure.

3

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



Key insights:

While a significant portion (37%) rated the collaboration as excellent, the majority of respondents (58%) viewed it as fair. Only a small fraction (5%) perceived the collaboration to be low.

This suggests that while there is a notable level of satisfaction with the collaboration, there is room for improvement to enhance overall effectiveness and synergy with the C-suite team.

paloalto NETWORKS

priorities

A Lynchpin Media BRAND

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.

strategies | 25

operations | 17

service | 18

product | 16

hr | 16

production | 20

collaboration | 68

chain | 16

coordination | 38

marketing | 32

supply | 16

enhance | 17

suite | 33

innovation | 15

customer | 40

development | 17

"Closer collaboration across the C-suite could drive sustainability initiatives and enhance environmental stewardship."

Key insights:

Respondents were given free text and asked to choose words that best describe the ways collaboration with the business C-suite could improve.

While 72% emphasised the importance of between-department collaboration, 68% highlighted collaboration itself as a key area for improvement. This is closely followed by customer (40%), coordination (38%), suite (33%) and marketing (32%).

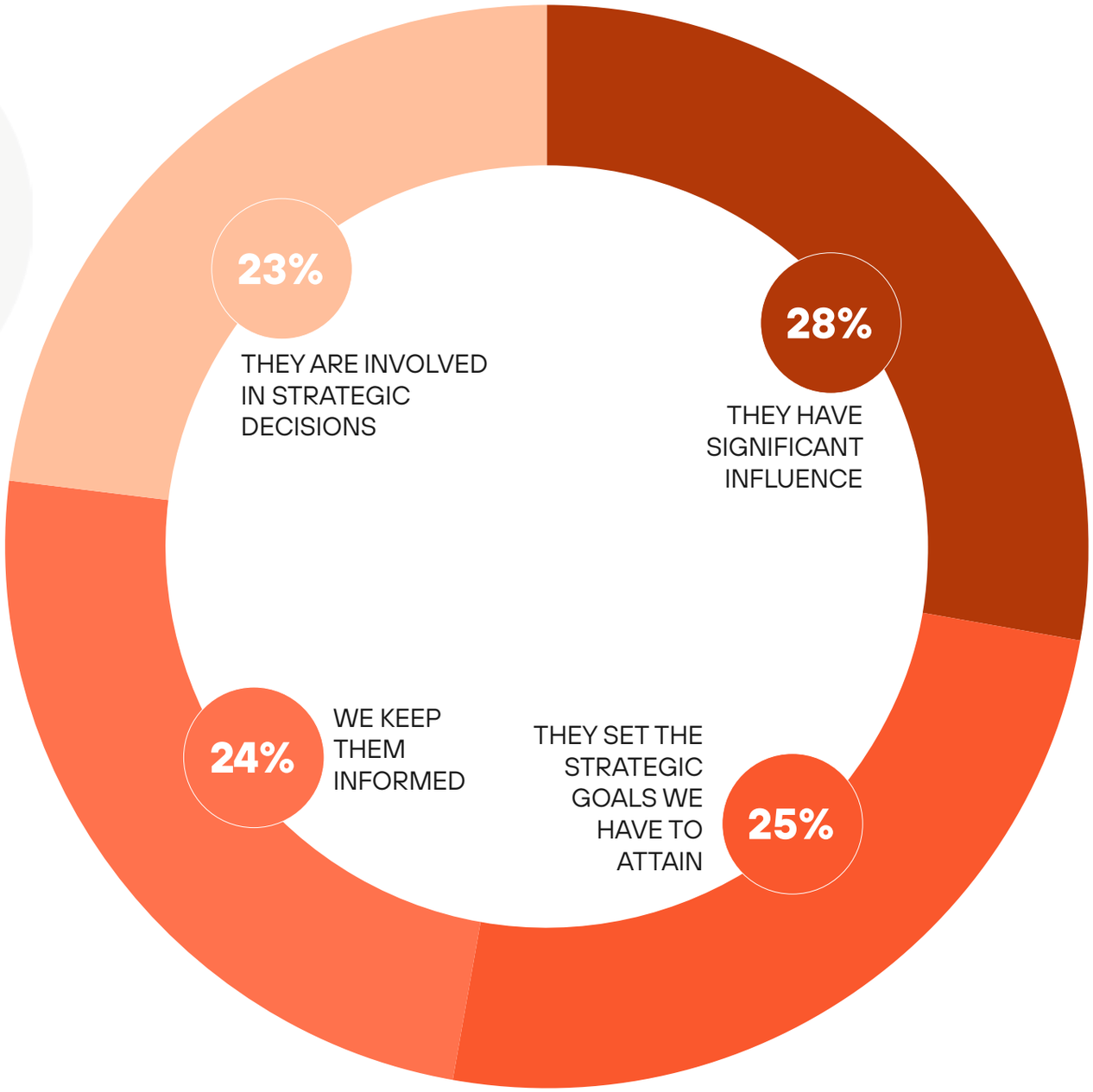
The overall data underscores the need for improved coordination and communication with C-suite. It also suggests a desire for more cohesive teamwork and aligning strategies across departments to enhance customer offerings. Overall, fostering collaboration and synergy within the C-Suite appears crucial for driving business success and innovation.

Some of the suggestions from respondents on how to improve this include:

- Collaborating effectively with the rest of the C-suite could drive efficiency and innovation in the automotive industry
- Integration of customer feedback from various departments to improve overall service quality and satisfaction
- Closer collaboration across the C-suite could drive sustainability initiatives and enhance environmental stewardship
- Enhancing cross-functional alignment for strategic decision-making.

5

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



Key insights:

While 28% indicate that the board has influence and direction on their organisation's cybersecurity strategy, 25% stated that they (the board) set the strategic goals.

Additionally, 23% mentioned that the board is involved in strategic decisions and 24% reported that they (IT executives) keep the board informed.

These findings suggest that boards play a significant role in shaping cybersecurity strategies, having either direct influence in setting goals or being involved in strategic decisions.

paloalto NETWORKS

priorities

A Lynchpin Media BRAND

Describe some of the challenges this presents you with.

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

"Collaborating effectively with the rest of the C-suite could drive efficiency and innovation."

Key insights:

Respondents were given free text and asked to describe some challenges they face when the board influences and directs their organisation's cybersecurity strategy. Chief among these are managing (48%) and navigating (38%) the complex array of factors involved.

This is closely followed by adapting (35%) strategies to meet consumer preferences and consumer concerns (35%). Notably, investing in cybersecurity is a highlighted challenge scoring 21%.

This data suggests that the board's influence on cybersecurity strategy necessitates a multifaceted approach that balances consumer needs, sustainability concerns, regulatory compliance and investment for technological advancements.

Some of the suggestions from respondents on how to improve this include:

- Navigating the retail landscape amidst changing consumer preferences, increasing competition and the rise of e-commerce.
- Adapting to changes in energy policies, reducing carbon emissions and diversifying energy offerings to meet evolving consumer preferences.
- Managing risk in a volatile economic environment, ensuring regulatory compliance and adapting to digital banking trends while maintaining customer trust.
- Handling data transfer restrictions across borders.

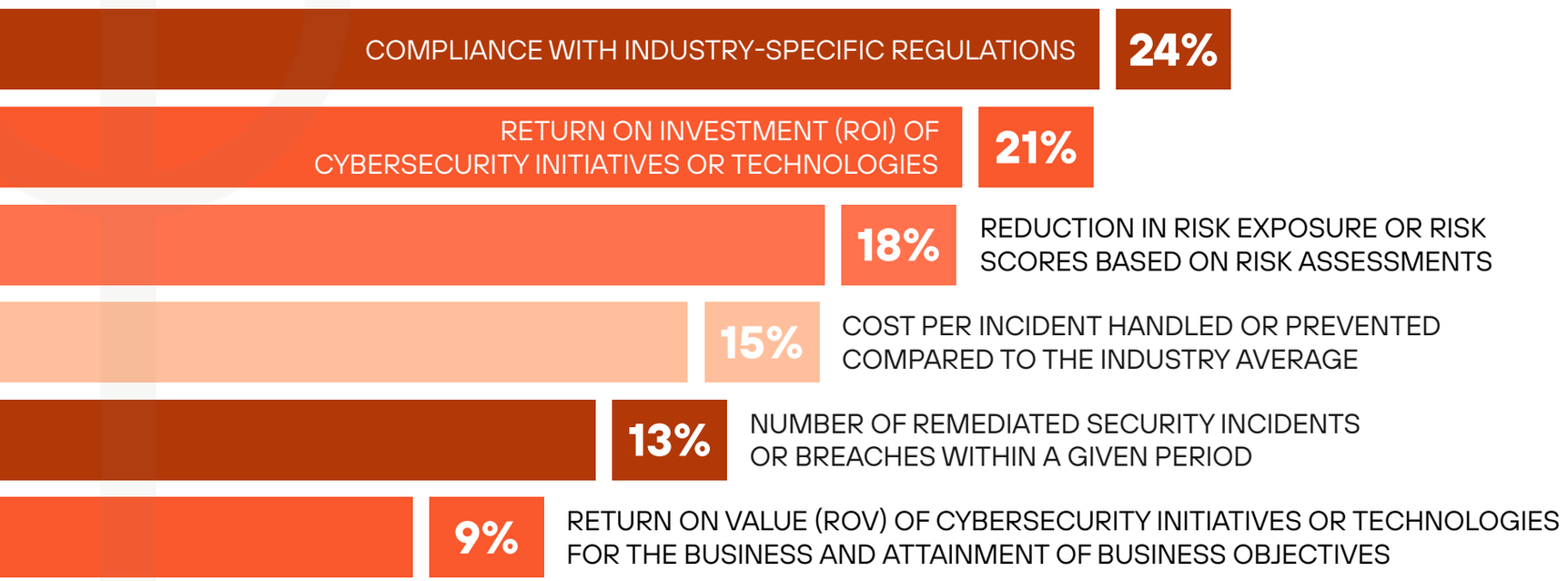
paloalto NETWORKS

priorities

A Lynchpin Media BRAND

7

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, 24% of respondents use compliance with industry-specific regulations, indicating a strong adherence to regulatory standards.

A total of 21% 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 18% 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.

paloalto NETWORKS

priorities

A Lynchpin Media BRAND

Part 2

CIO Business and Cybersecurity Priorities

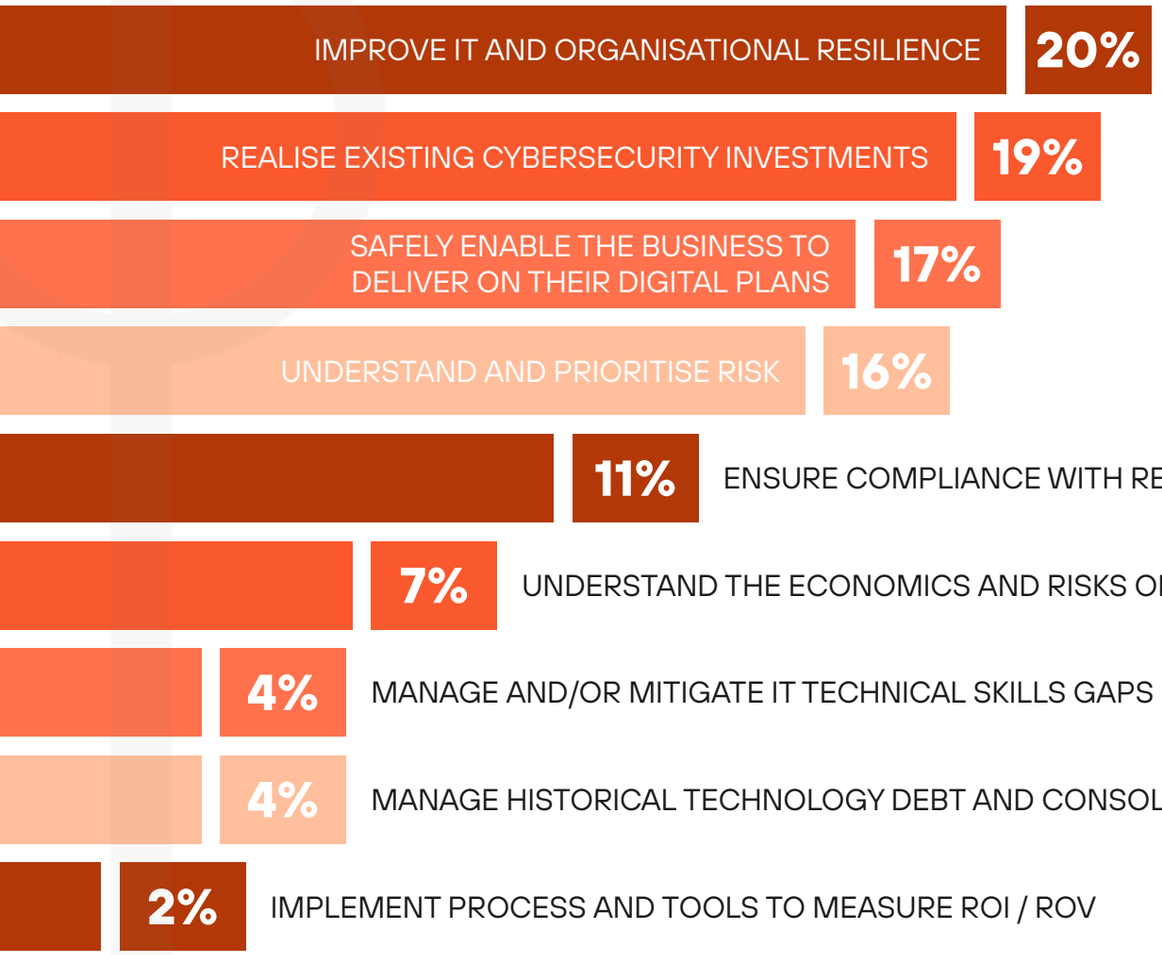
paloalto NETWORKS

priorities

A Lynchpin Media BRAND

8

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



Key insights:

Enhancing IT and organisational resilience was selected by one fifth of respondents (20%). Enabling the business to execute digital plans securely voted by 17% of those surveyed underscores the need to balance innovation with robust security measures.

Realising existing cybersecurity investments (19%) highlights the importance of maximising the effectiveness of current resources.

These findings emphasise the necessity for adaptive strategies that bolster resilience, align with business objectives and optimise cybersecurity investments for sustained success in an ever-evolving threat landscape.

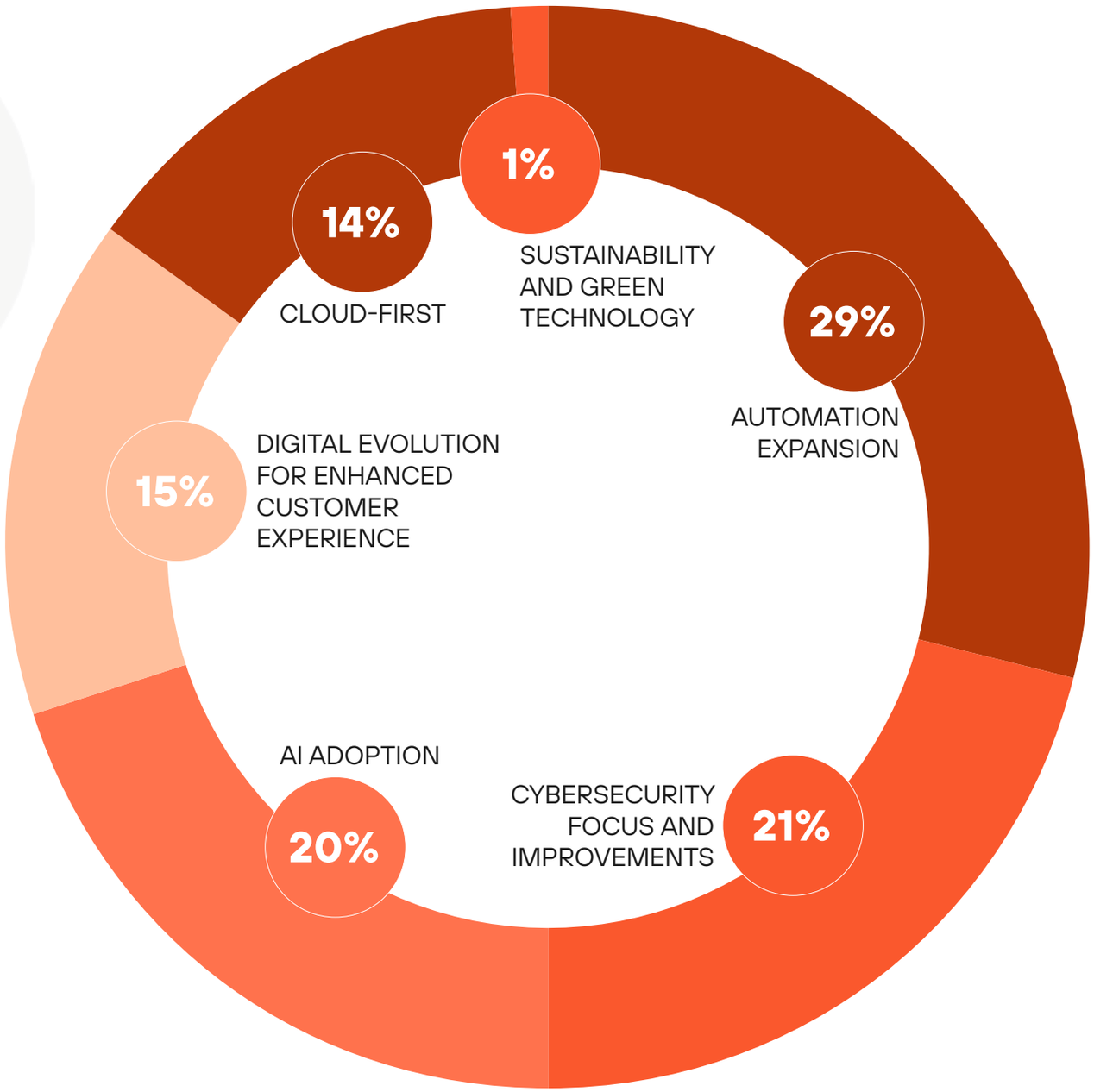
paloalto NETWORKS

priorities

A Lynchpin Media BRAND

9

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



Key insights:

Automation expansion chosen by 29% respondents signifies a strategic move towards efficiency and agility, reducing manual intervention and enhancing operational effectiveness.

Cybersecurity focus and improvements (21%) highlight the recognition of the evolving threat landscape and the imperative to fortify defences. AI adoption with 20%, underscores the pursuit of advanced analytics and threat detection capabilities for proactive security measures.

These priorities indicate a concerted effort towards bolstering cybersecurity resilience while harnessing automation and AI for enhanced operational efficiency and threat mitigation.

paloalto NETWORKS

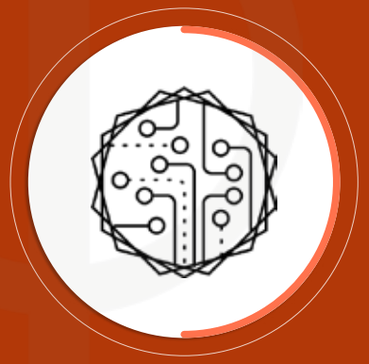
priorities

A Lynchpin Media BRAND

10

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



22% of respondents adopting AI

29% of respondents need more information about AI

Cybersecurity automation

17% of respondents adopting Cybersecurity automation

35% of respondents need more information about Cybersecurity automation

Sustainability

19% of respondents have a basic understanding of sustainability

32% of respondents need more information about sustainability

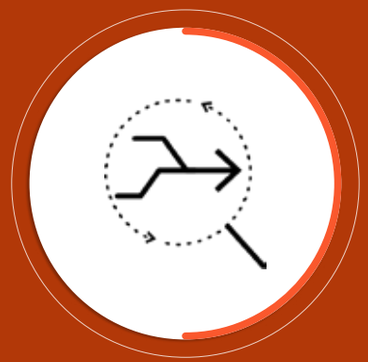
Augmented Reality and Virtual Reality

37% of respondents have a basic understanding of Augmented reality and virtual reality

21% of respondents are adopting Augmented reality and virtual reality

CONTINUED

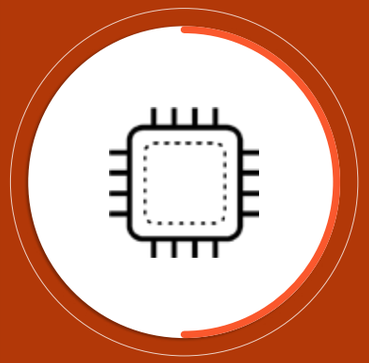
Autonomous Systems



28% of respondents are adopting Autonomous Systems

27% of respondents need more skills with Autonomous Systems

Quantum Computing



35% of respondents are adopting Quantum Computing

26% of respondents need more information about Quantum Computing

Service-based offerings

17% of respondents need more information about Service-based offerings

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

paloalto NETWORKS

priorities

A Lynchpin Media BRAND

11

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

Key insights:

Protecting and managing risk within the supply chain and supplier ecosystem selected by 21% of respondents underscores cybersecurity's vital role in safeguarding interconnected networks and maintaining trust.

Underpinning operational resilience (16%) highlights cybersecurity's fundamental support in ensuring continuous business operations amidst evolving threats.

Protecting and inspiring confidence in customers and employees, also at 16% emphasises the importance of cybersecurity in fostering trust and preserving reputation.

These findings underscore cybersecurity's multifaceted role in fortifying resilience, maintaining trust and mitigating risk for organisational success.

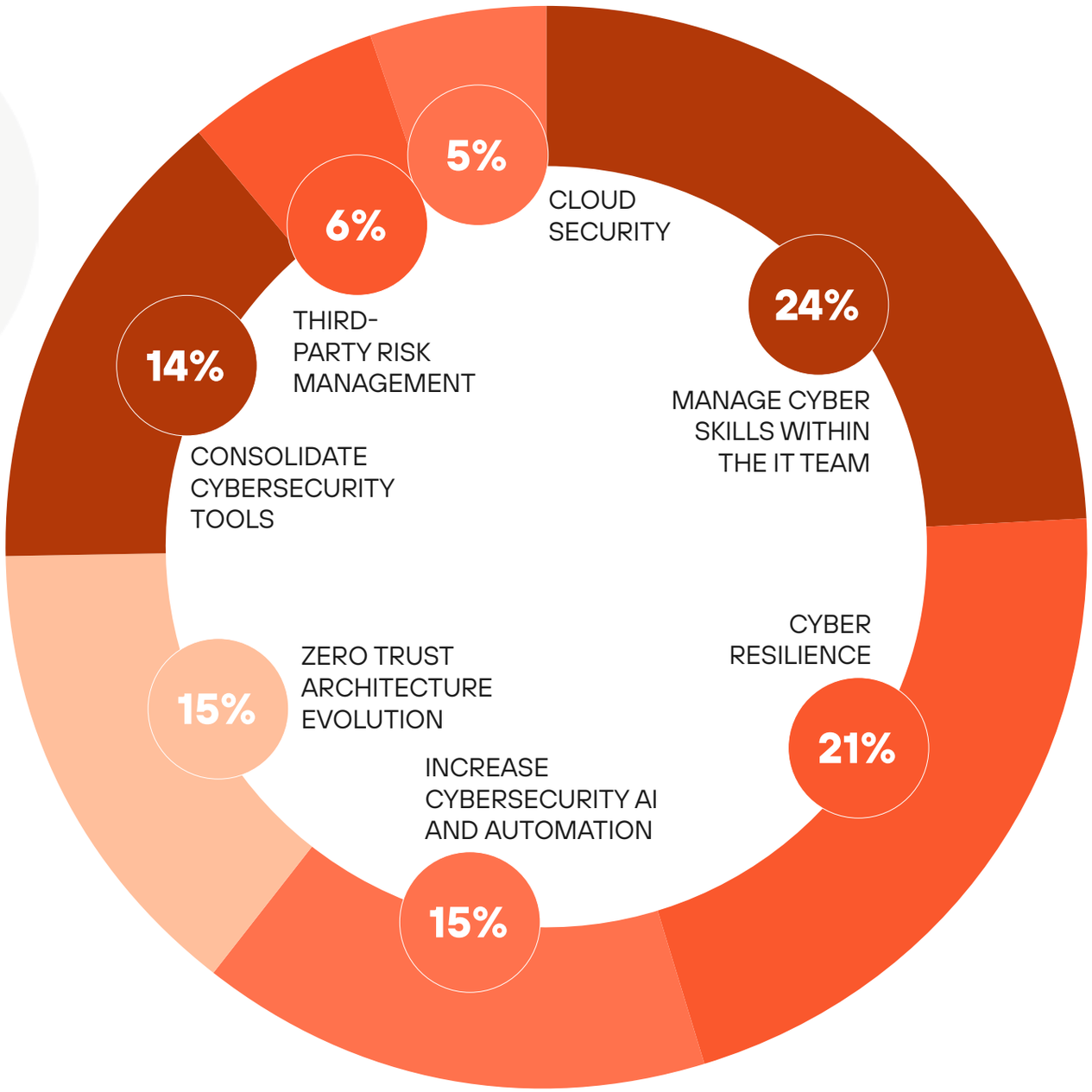
paloalto NETWORKS

priorities

A Lynchpin Media BRAND

12

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



Key insights:

Cloud security chosen by 24% of survey respondents reflects the imperative of safeguarding cloud environments amid expanding digital footprints.

Zero Trust architecture evolution (15%) underscores the ongoing shift towards a proactive and adaptive security paradigm.

Cyber-resilience (21%) highlights the importance of fortifying defences and response capabilities against evolving threats.

These priorities emphasise a holistic approach encompassing cloud security, advanced architectural frameworks and robust resilience strategies to mitigate risks and safeguard organisational assets in the ever-evolving cybersecurity landscape.

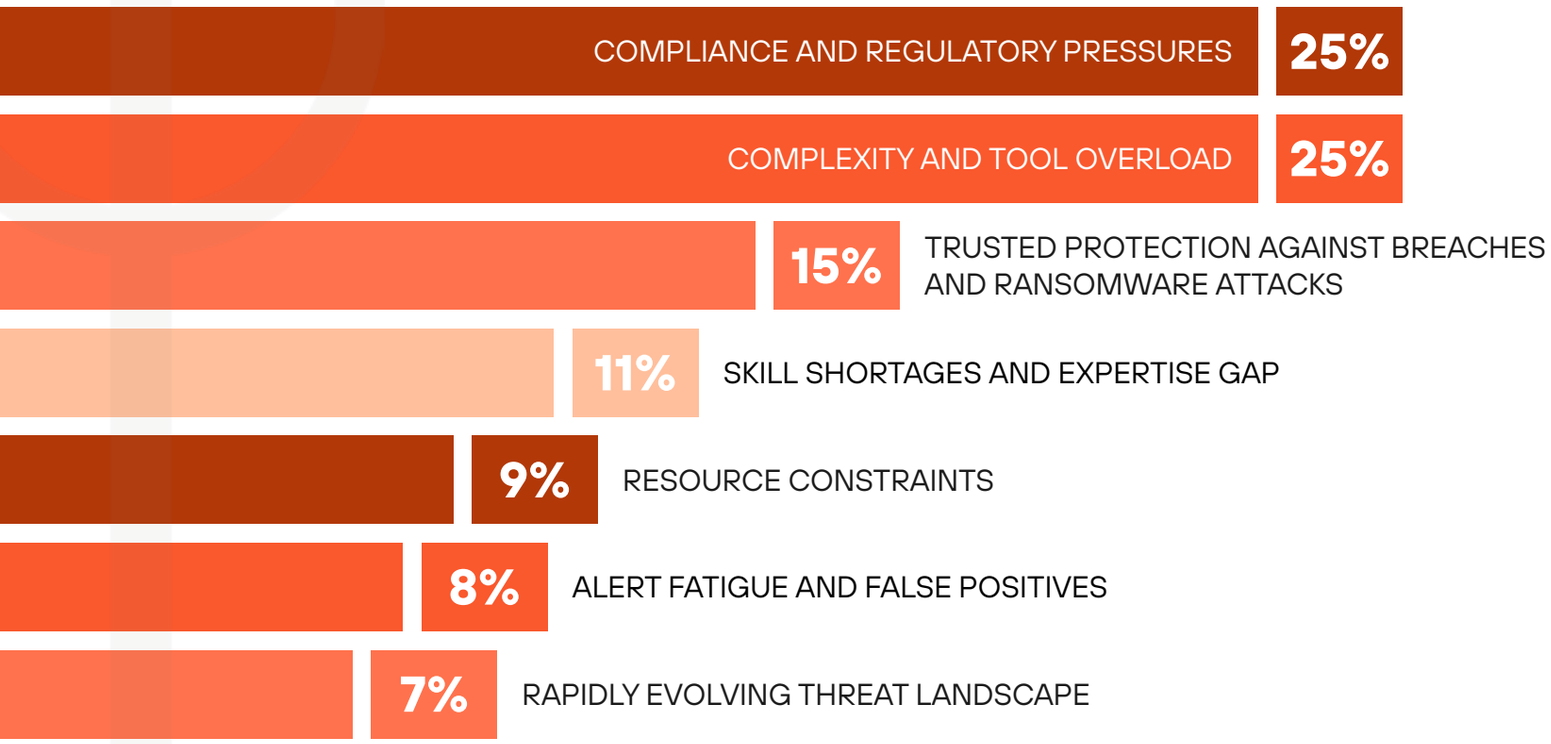
paloalto NETWORKS

priorities

A Lynchpin Media BRAND

13

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



Key insights:

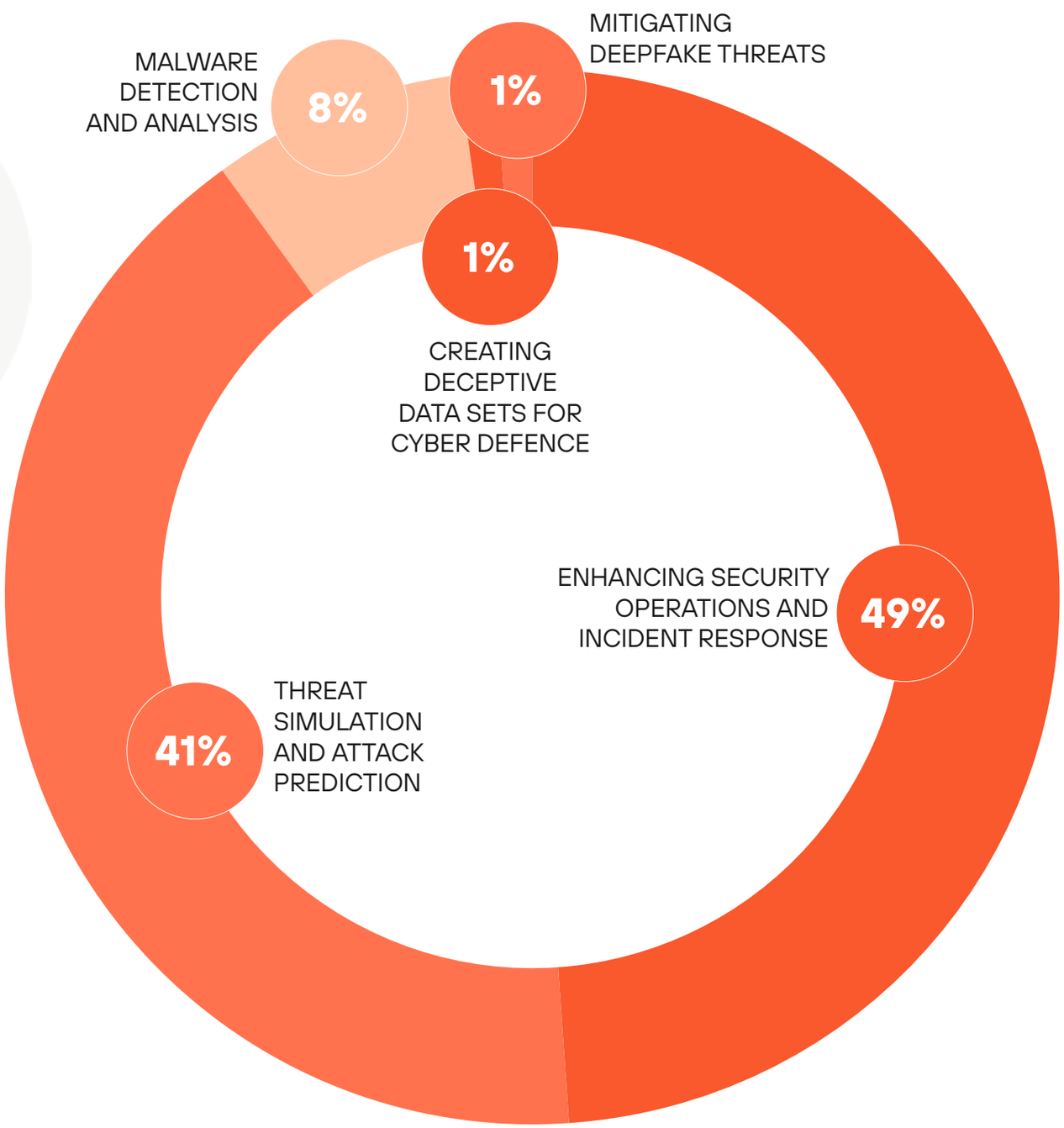
Complexity and tool overload selected by quarter of respondents shows the struggle to navigate a crowded marketplace and integrate disparate solutions efficiently.

Compliance and regulatory pressures also at 25% highlights the need to align with evolving standards while maintaining operational effectiveness. Trusted protection against breaches and ransomware attacks (15%) emphasises the perpetual battle to secure systems against sophisticated threats.

These challenges reflect the ongoing struggle to balance security efficacy with operational efficiency amidst a dynamic and demanding cybersecurity landscape.

14

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



Key insights:

Enhancing security operations and incident response, chosen by almost half of respondents (49%) reflects the reliance on automation to streamline processes and bolster incident handling capabilities.

Threat simulation and attack prediction (41%) reinforces the proactive use of AI to anticipate and prepare for emerging threats.

Malware detection and analysis (8%) underscores the growing role of automation in augmenting threat detection and response capabilities.

These findings illustrate the strategic deployment of AI and automation to address critical cybersecurity challenges and mitigate skills gaps effectively.

Conclusion

2024 underscores a transformative period for technology leaders, particularly CIOs, as they navigate an increasingly complex and dynamic landscape.

The role of CIOs is anticipated to shift significantly towards a more strategic focus and strengthening their alignment with the business to drive business transformation. This evolution necessitates a robust understanding of communication patterns, collaborative efforts, and primary concerns within their organisations.

The sophistication of cyber threats and the complexities of regulatory compliance emerge as leading concerns for European CIOs especially as NIS2 forces organisations to look at their supply chain, as well as their organisation to remain compliant. The adoption of AI to automate and enhance cybersecurity operations is seen as a critical response to the skills gap in this field. Additionally, the rise of remote work and the proliferation of IoT devices have made cybersecurity a top priority for the coming year.

The adoption of advanced technologies such as AI, automation, AR/VR, and sustainability initiatives are expected to have profound impacts on future business operations, and therefore enabling CIOs to shift to a more strategic approach. Staying abreast of these disruptive technologies is essential for fostering a culture of awareness and resilience within organisations. Over 20% of respondents highlighted the importance of enhancing IT and organisational resilience to ensure business success.

Collaboration, both within and between departments, remains a key area for improvement. Effective collaboration with the c-suite is crucial for aligning business objectives and optimising investments. Integrating customer feedback into service improvement strategies is also vital for maintaining high service quality and satisfaction.

In summary, the research highlights the need for adaptive strategies that bolster resilience, align with business objectives, and foster collaborative partnerships. As technology continues to evolve, CIOs and other tech leaders must navigate these changes strategically to drive transformation and ensure sustained success.

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