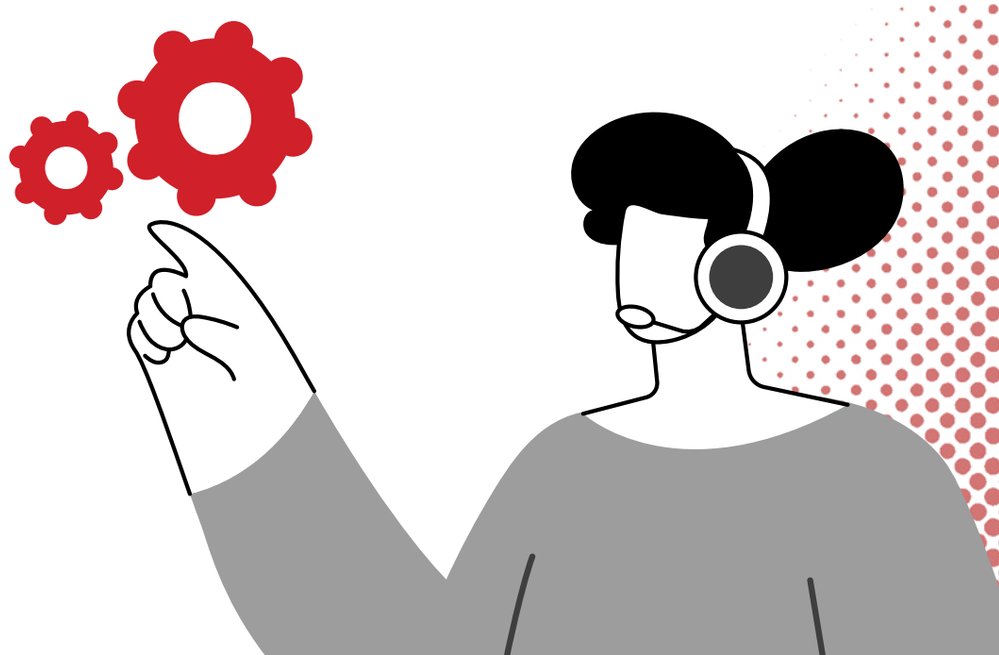
A Lynchpin Media BRAND

cxo priorities

SECURITY PRIORITIES REPORT AT GITEX 2023

A cxo priorities Report



A Lynchpin Media BRAND

cxo priorities

CONTENTS

INTRODUCTION 3

SURVEY OVERVIEW AND AIMS 4

1. THE THREATSCAPE 5

2. KEY TECHNOLOGY INVESTMENT AREAS AND SECURITY PRIORITIES 14

REPORT SUMMARY 23

A Lynchpin Media BRAND

CXO priorities

INTRODUCTION

Our digital world is more connected than ever before and while businesses are reaping the benefits of the efficiencies and growth this has provided, they are also being forced to traverse a highly sophisticated world of threat actors.

Navigating this landscape is challenging. With competing business priorities, regulatory pressures and workforce management to consider, modern CISOs and their teams must make informed decisions about where to channel investment.

In this report, we provide this insight and explore the challenges IT security leaders are currently facing, as well as their priorities looking ahead.

A Lynchpin Media BRAND

cxo priorities

SURVEY OVERVIEW AND AIMS

Through our survey of 500 industry leaders from large companies (1,500 employees plus) we obtained vital insights into security strategies for the C-suite across the region right now, as well as the key considerations for businesses when it comes to prioritising investment.

The report includes insight into the following:

- The biggest perceived threats to MENA organisations
- Key technology investment areas
- Security priorities

A Lynchpin Media BRAND

cxo priorities

SECTION 1
THE THREATSCAPE

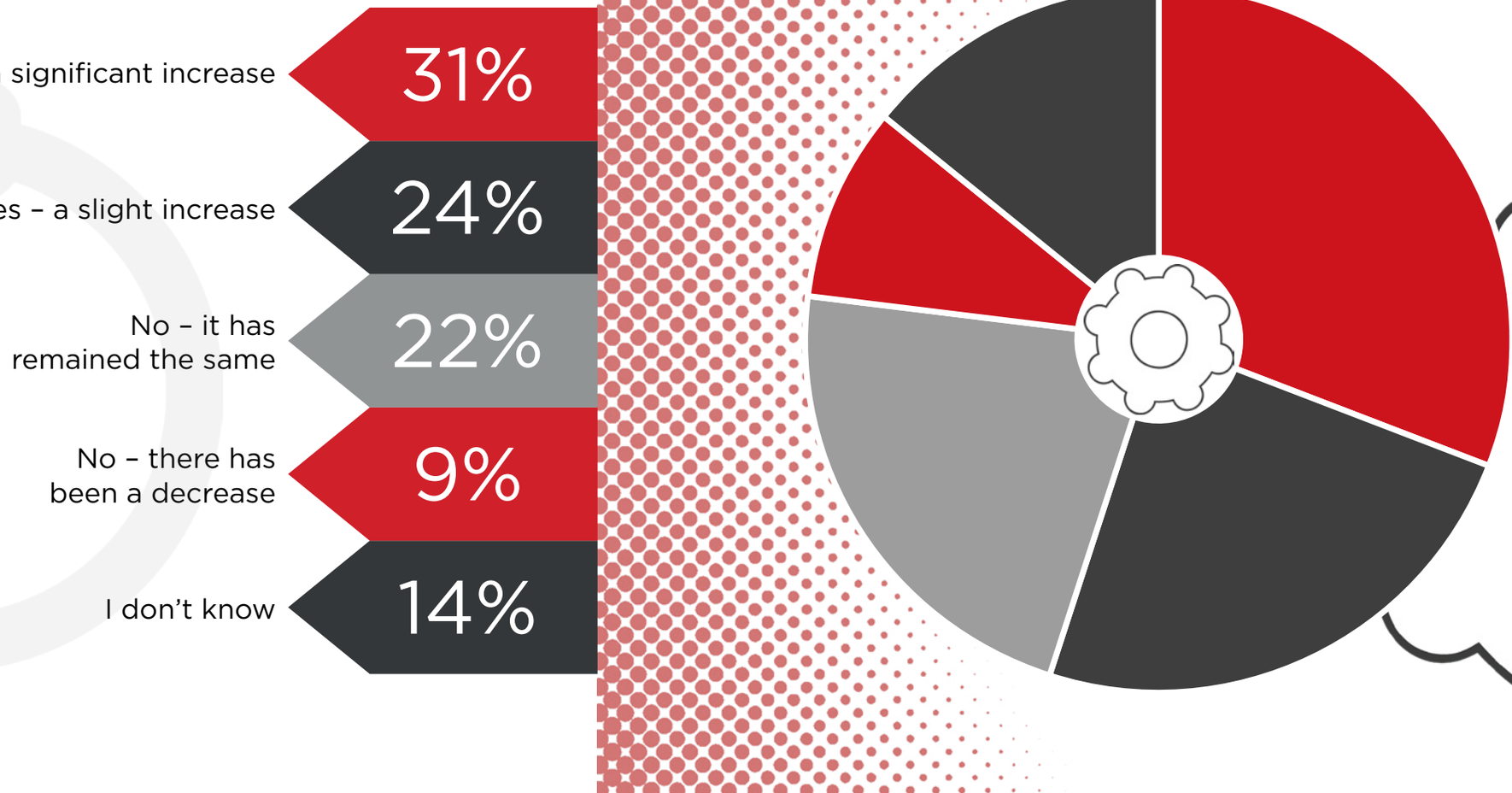
With threats coming from multiple angles, it is important that MENA organisations have full visibility and strong security measures in place when implementing new IT projects. In this section we explore security concerns, skills shortages and the wider ramifications of cyber incidents.

A Lynchpin Media BRAND

cxo priorities

QUESTION 1

Has your organisation seen a change in the number of attacks over the last 12 months?



KEY FINDINGS

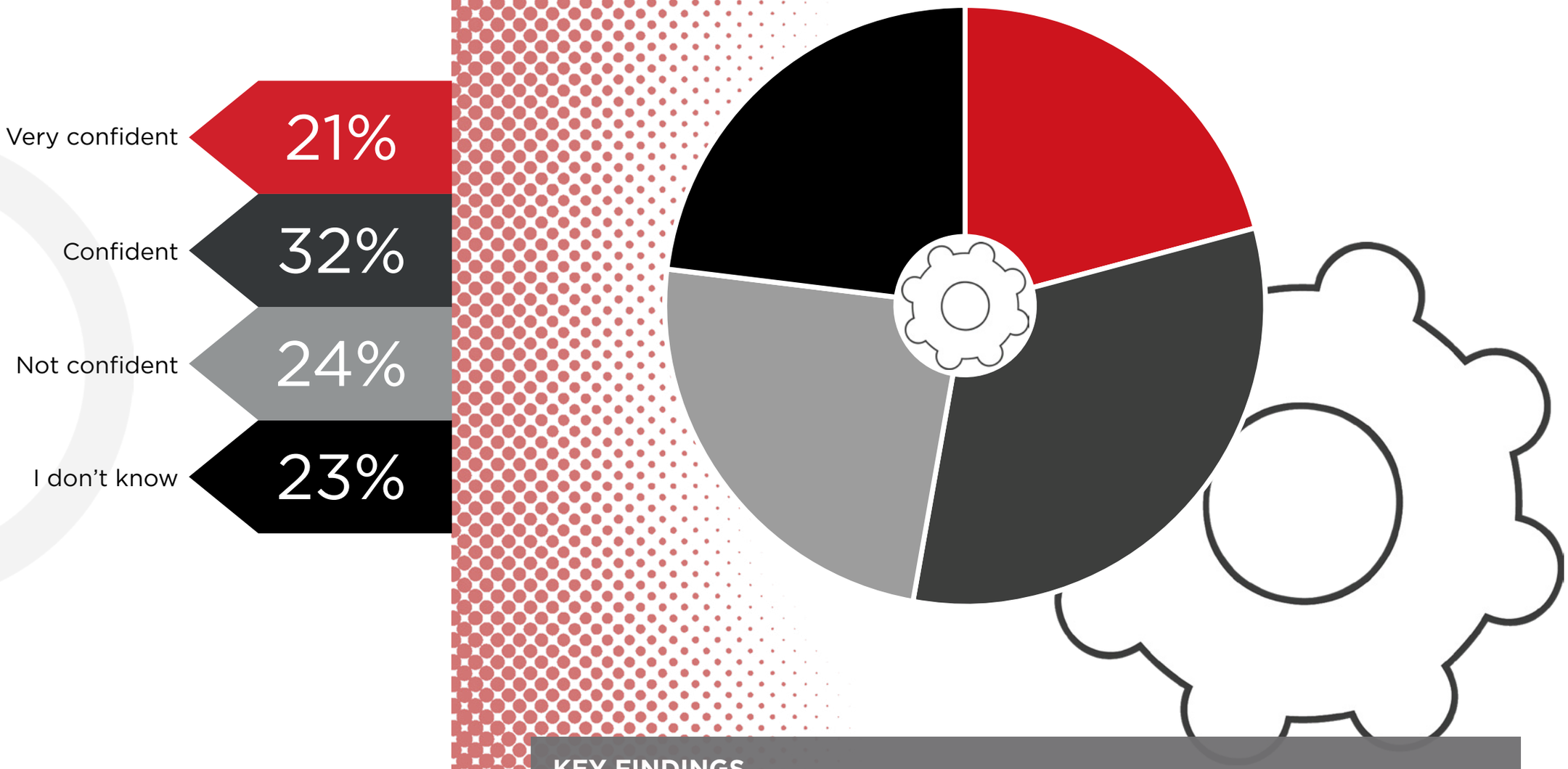
Over half of the respondents state that their organisation has seen an increase in the number of attacks over the last 12 months. Nearly a third of respondents (31%) also cite that the number of attacks has increased significantly. This highlights the need for organisations to review their current security spend and refocus their efforts where gaps exist in their ability to withstand malicious attacks.

A Lynchpin Media BRAND

cxo priorities

QUESTION 2

How confident are you that your organisation is protected from attacks?



KEY FINDINGS

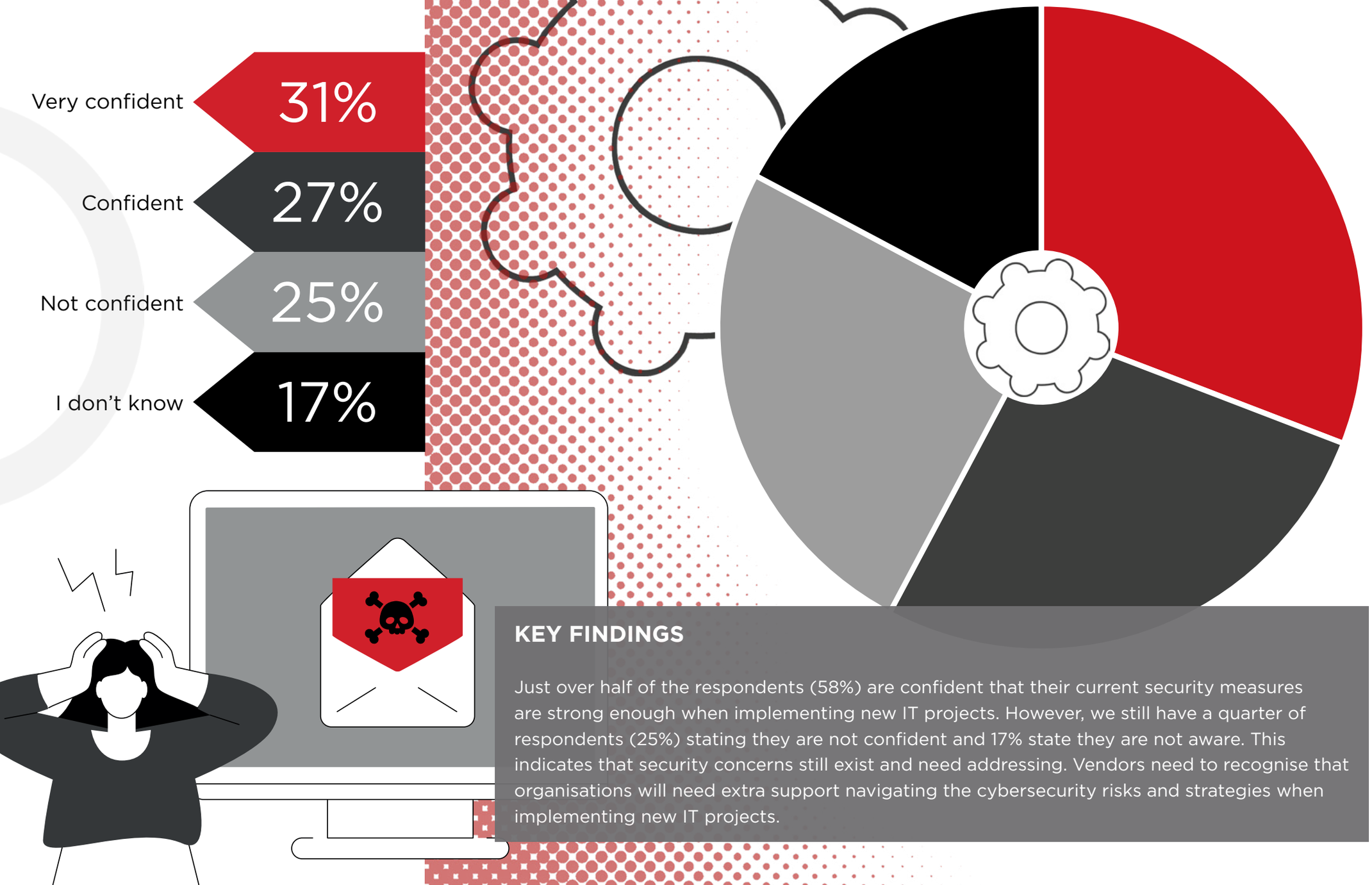
Just over half of the respondents (53%) state that they are confident that their organisation is protected from attacks. The fact that that the other half of respondents are not confident and are not aware about this area points to a real split of opinions. This suggests that there is a long way to go implementing strong security policies which leaves companies feeling unanimously confident about withstanding attacks.

A Lynchpin Media BRAND

cxo priorities

QUESTION 3

How confident are you that your current security measures are strong enough when implementing new IT projects?



KEY FINDINGS

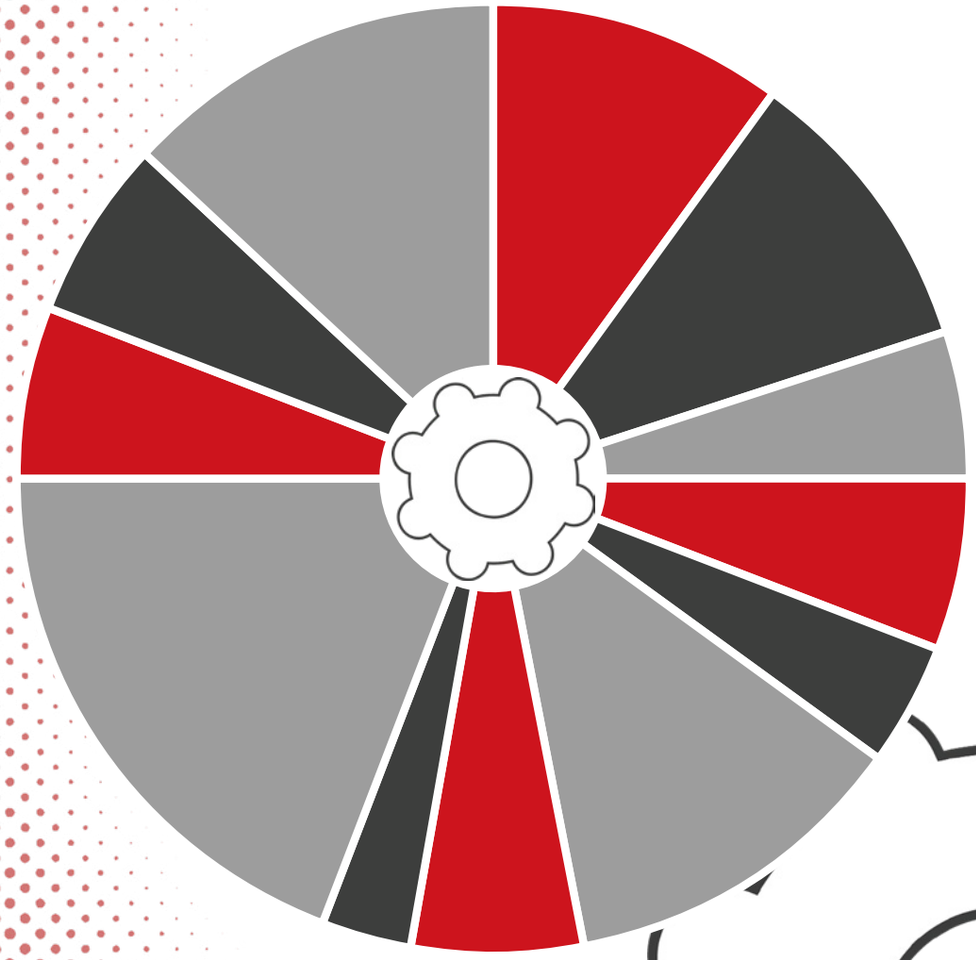
Just over half of the respondents (58%) are confident that their current security measures are strong enough when implementing new IT projects. However, we still have a quarter of respondents (25%) stating they are not confident and 17% state they are not aware. This indicates that security concerns still exist and need addressing. Vendors need to recognise that organisations will need extra support navigating the cybersecurity risks and strategies when implementing new IT projects.

A Lynchpin Media BRAND

cxo priorities

QUESTION 4

Which of the below do you consider the biggest threats to your organisation?



Email (phishing/BEC)	10%
Ransomware	10%
Malware	5%
Human error	6%
Insider threat	4%
Cloud	12%
Nation state attacks	6%
Mobile attacks	3%
Hybrid working	19%
IoT devices	6%
Deep fakes and impersonation	6%
Industrial security	13%

KEY FINDINGS

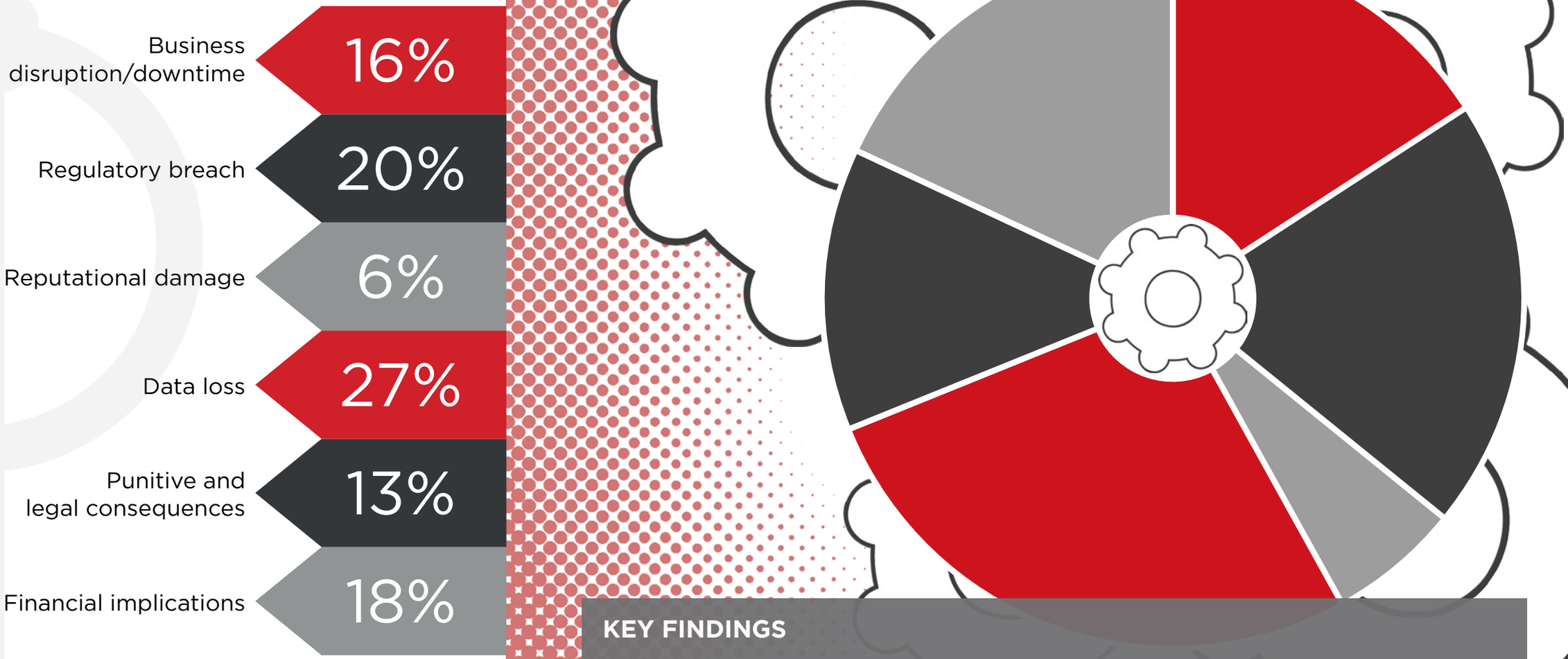
In terms of the greatest security threats, respondents cite hybrid working (19%) and industrial security (13%). This is closely followed by email and ransomware (10%). This indicates the need for building a more robust security culture beyond fixed locations. Times have changed and organisations are seeking something different in their network architecture compared to a few years ago. There is an opportunity for SASE and Zero Trust vendors who can provide solutions beyond fully on-premise hardware.

A Lynchpin Media BRAND

cxo priorities

QUESTION 5

What do you consider the biggest consequence of a cyber incident?



KEY FINDINGS

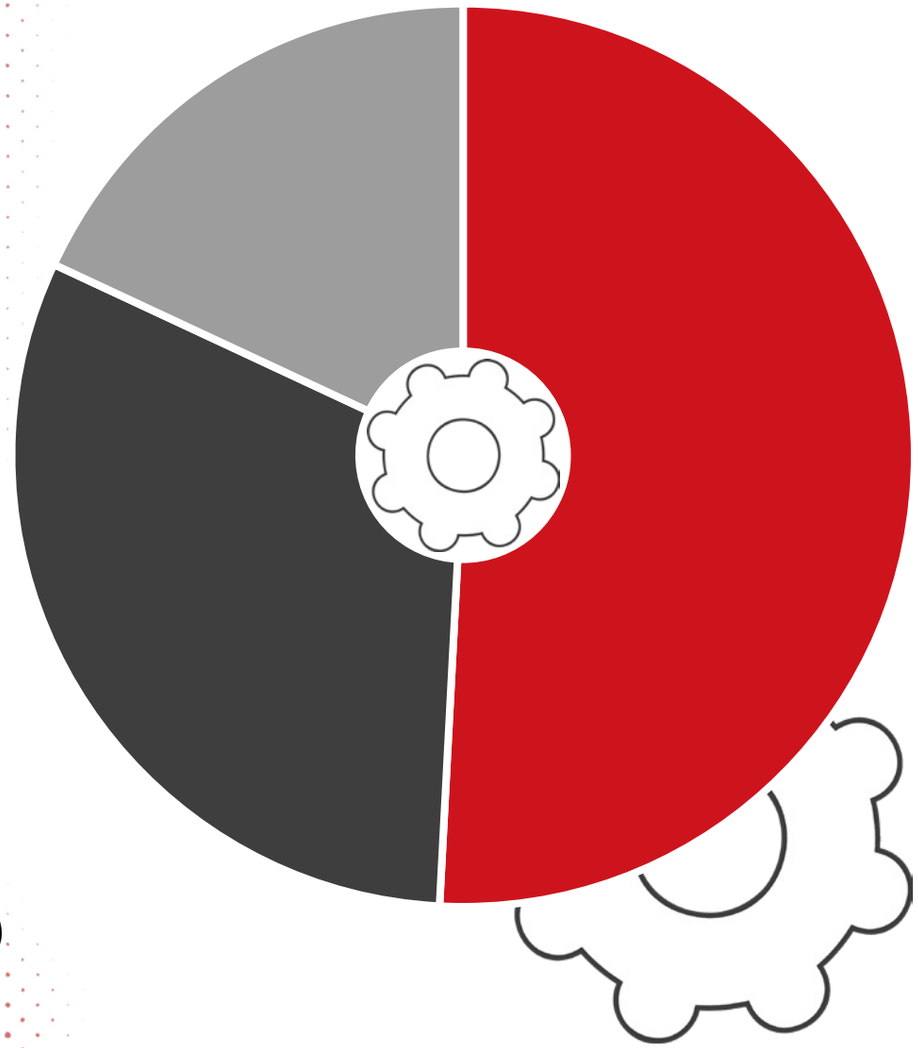
The research shows that data loss (27%) and regulatory breaches (20%) were considered the biggest consequences of a cyber incident. It is unsurprising that data loss and regulatory breaches are high priorities for businesses. They are always hot topics at board level discussions and the fact that they both scored higher than business disruption (16%) shows the urgent need to address these areas with trusted vendors.

A Lynchpin Media BRAND

cxo priorities

QUESTION 6

Do you consider your organisation to have a cybersecurity skills shortage?



Yes	51%
No	31%
I don't know	18%

KEY FINDINGS

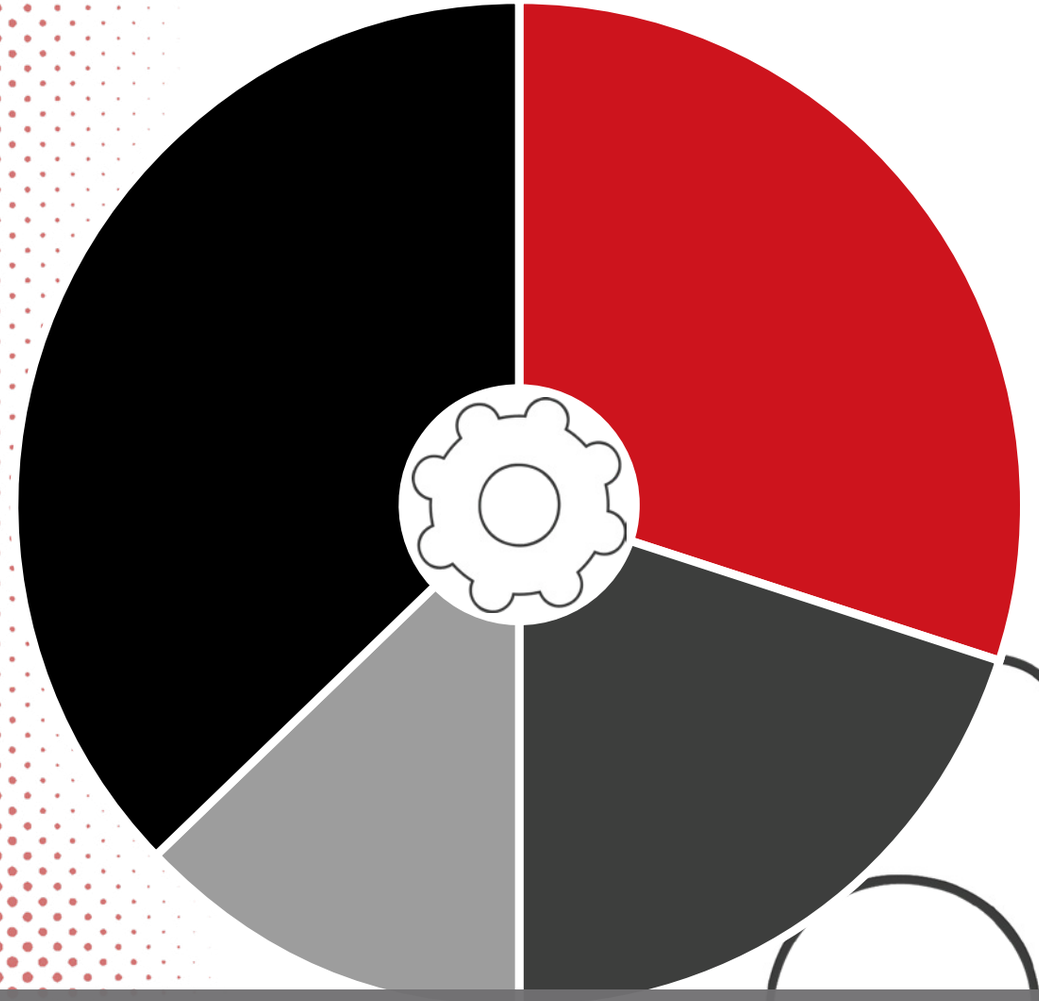
Half of the organisations surveyed (51%) stated that they have a cybersecurity skills shortage. There is a case here for a trusted security vendor which can take the lead in precise gap analysis and identify growth opportunities. A failure to address this skills gap will create workplace inefficiencies and impact staff morale. This has the potential to seriously compromise a company's ability to manage threats and result in financial losses.

A Lynchpin Media BRAND

cxo priorities

QUESTION 7

How is your organisation approaching cybersecurity skills?



Graduate schemes and apprenticeships 30%

Upskilling existing employees 20%

Introduced schemes to retain current staff 13%

Outsourcing 37%

KEY FINDINGS

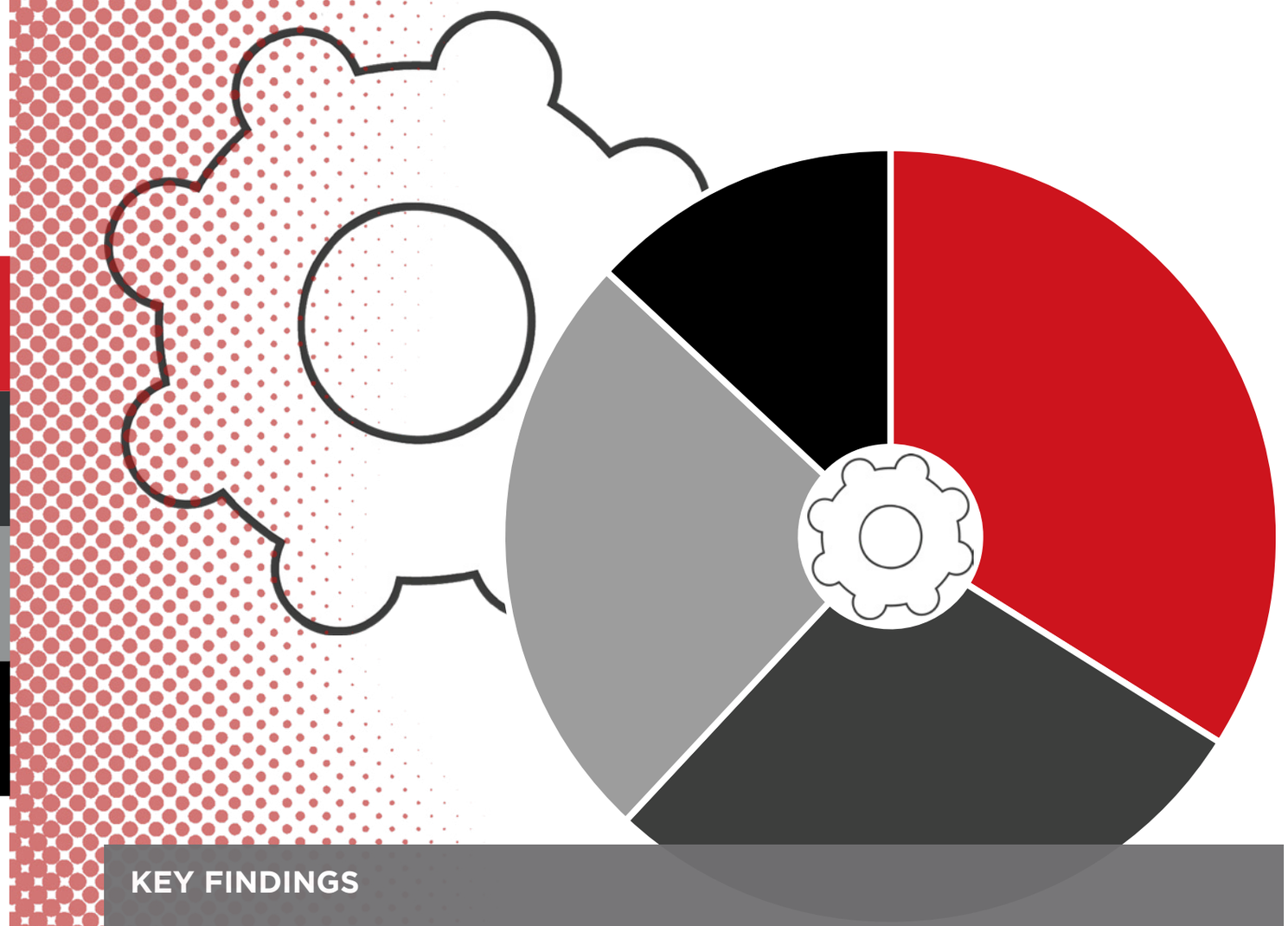
More than a third of the respondents (37%) stated that they are approaching cybersecurity skills through outsourcing. This was closely followed by graduate schemes and apprenticeships (30%). This suggests there is some way to go if companies are going to effectively manage cyber-risks through their current recruitment policies. Vendors who specialise in outsourcing cybersecurity functions and can do so cost effectively will lead the pack here.

A Lynchpin Media BRAND

cxo priorities

QUESTION 8

How have security concerns impacted your strategy around cloud infrastructure?



Security concerns have not impacted our decision — 34%

We have decided to keep some services on-premises for greater control — 28%

We have decided to go all-in with cloud — 25%

I don't know — 13%

KEY FINDINGS

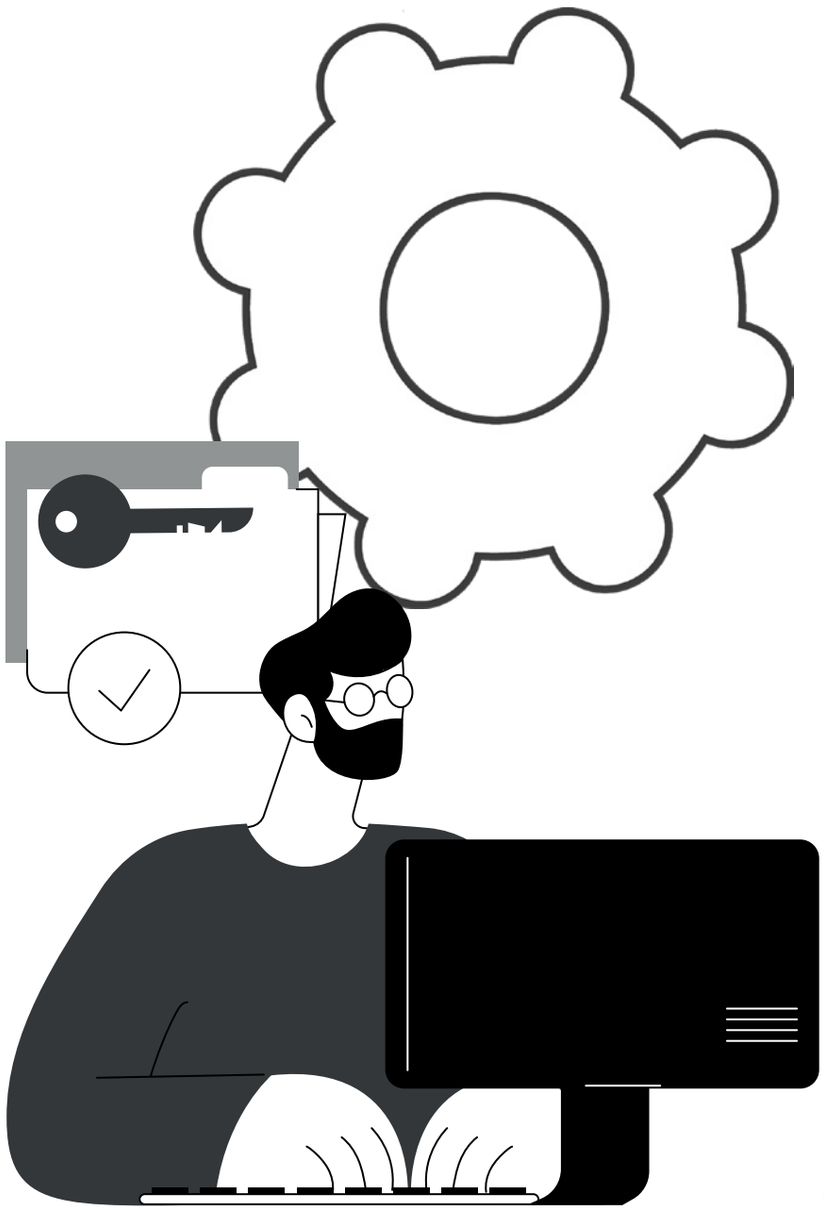
Regarding the respondents' current network architecture, 25% of respondents state they have decided to go all in with cloud. More interestingly 34% of respondents have cited that they have no security concerns in this area. This indicates the rapid move from office locations to hybrid and remote working. Vendors will need to consider security as each workforce will face different risks in different spaces and there is an opportunity to provide extra support in navigating these cybersecurity risks which are specific to hybrid working environments.

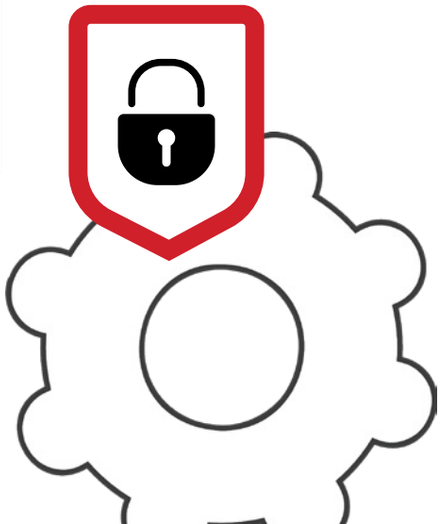
A Lynchpin Media BRAND

cxo priorities

SECTION 2
KEY TECHNOLOGY INVESTMENT AREAS AND SECURITY PRIORITIES

As businesses look to make productivity gains, there is the need to consider investment areas that balance security, cost and efficiency. In this section, we asked participants about their key areas of technology investment and security priorities. We explore their level of engagement with Zero Trust, AI cybersecurity tools and automation within their security system.



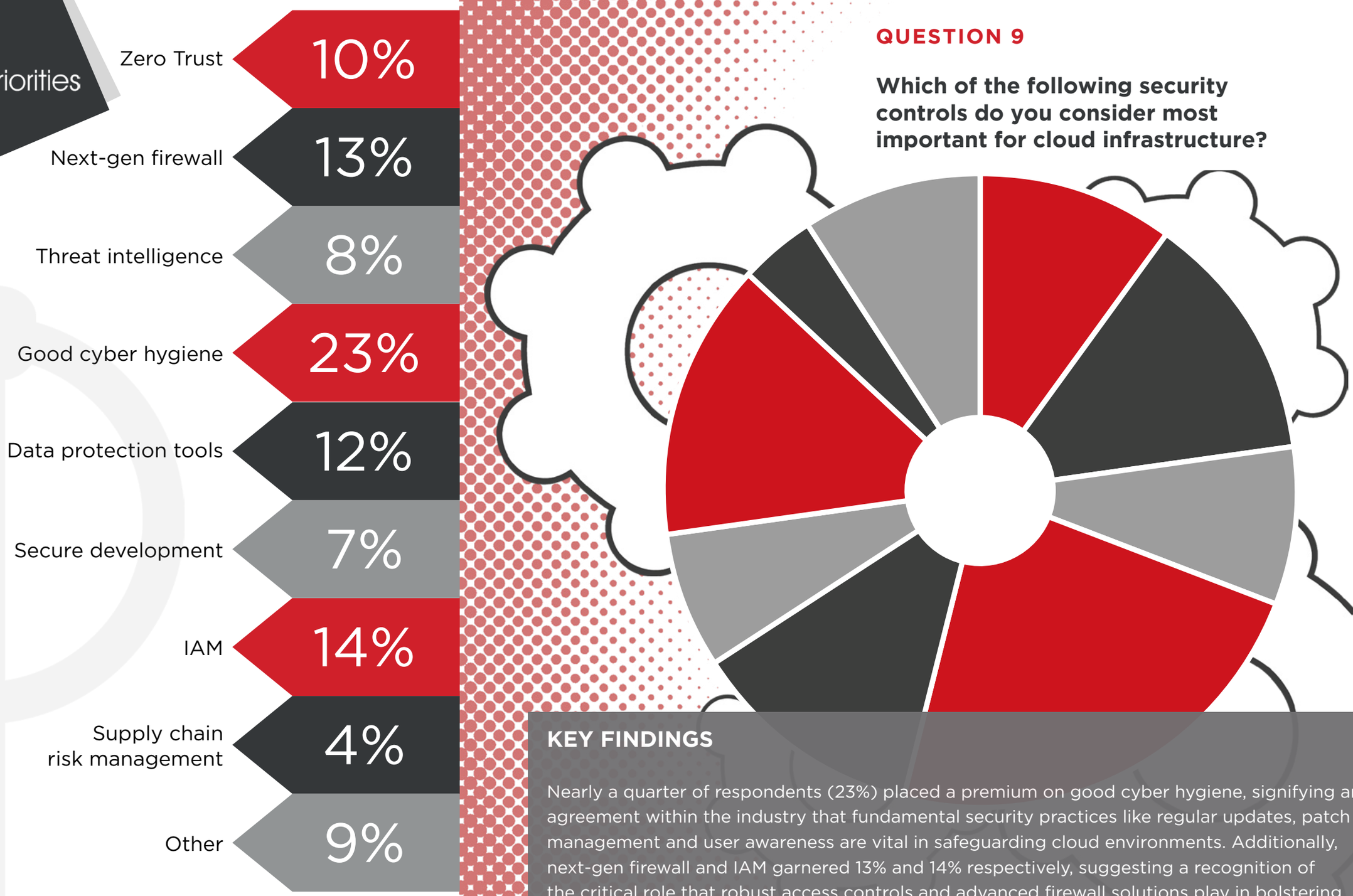


A Lynchpin Media BRAND

cxo priorities

QUESTION 9

Which of the following security controls do you consider most important for cloud infrastructure?



KEY FINDINGS

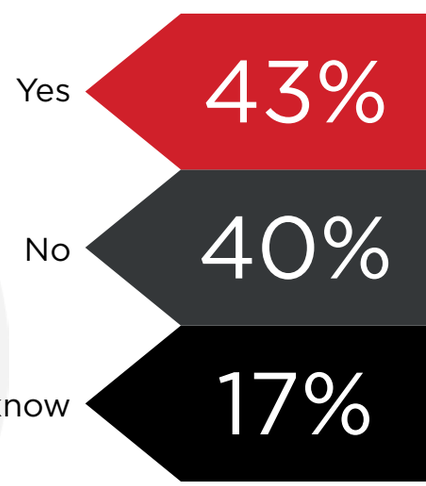
Nearly a quarter of respondents (23%) placed a premium on good cyber hygiene, signifying an agreement within the industry that fundamental security practices like regular updates, patch management and user awareness are vital in safeguarding cloud environments. Additionally, next-gen firewall and IAM garnered 13% and 14% respectively, suggesting a recognition of the critical role that robust access controls and advanced firewall solutions play in bolstering cloud security. Supply chain risk management recorded just 4%, which implies that while an emerging concern, it may not yet have achieved the same level of prioritisation in the markets. These results underscore the multifaceted nature of cloud security and the need for a holistic approach that encompasses various controls to ensure robust protection in an increasingly interconnected digital landscape.

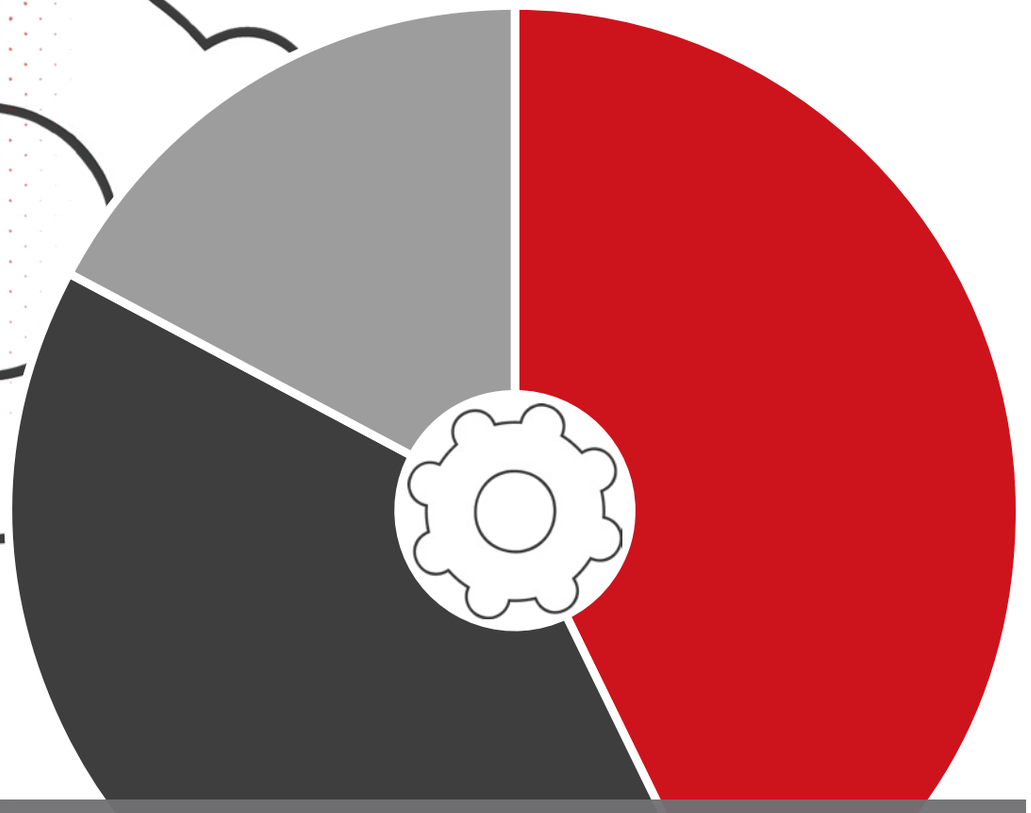
A Lynchpin Media BRAND

cxo priorities

QUESTION 10

Does your organisation currently operate with a Zero Trust approach to security?





KEY FINDINGS

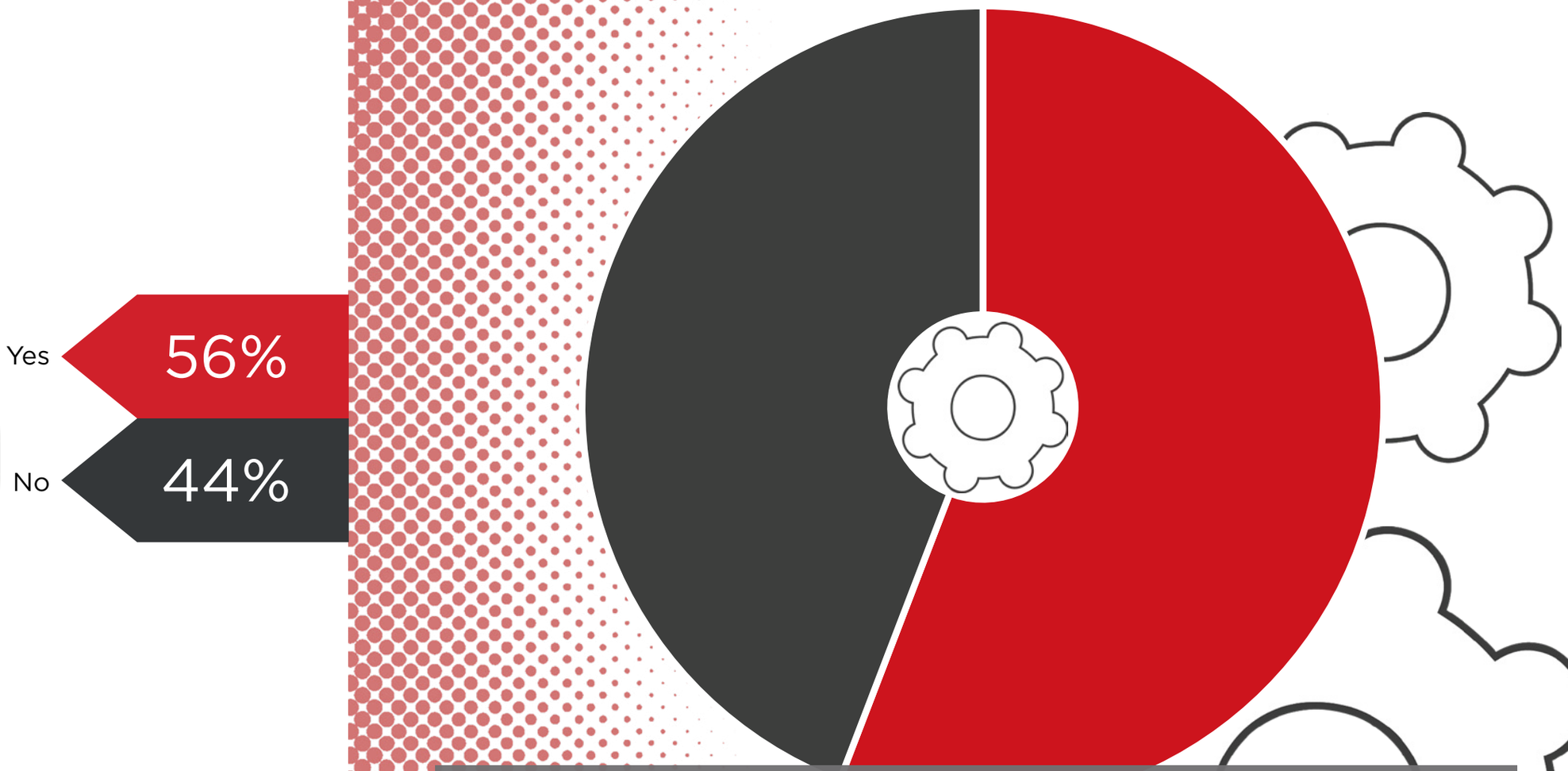
When asked about the adoption of a Zero Trust security approach, 43% of respondents indicated that they currently operate with this strategy suggesting a growing awareness and commitment to bolstering cybersecurity measures in the face of evolving threats. A further 40% answered in the negative, indicating that a substantial portion of organisations are yet to embrace the Zero Trust model. The question also uncovered 17% expressing uncertainty about their organisation’s security strategy. This reflects a potential gap in the communication of cybersecurity practices within these organisations. Overall, while Zero Trust security is gaining ground, there is still work to be done in terms of spreading awareness and ensuring a broader adoption. The diversity of approaches underscores the need for ongoing discussion and education in the security field.

A Lynchpin Media BRAND

cxo priorities

QUESTION 11

If no, does your organisation plan to implement a Zero Trust approach to security?



KEY FINDINGS

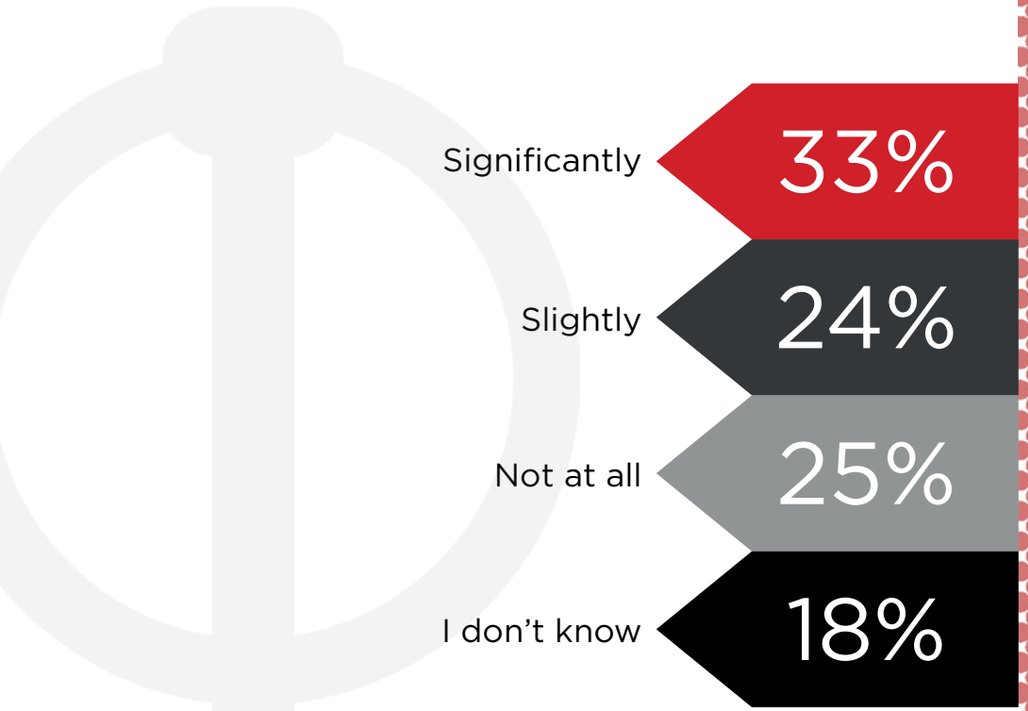
More than half (56%) of respondents answered in the affirmative indicating a significant inclination towards embracing Zero Trust while 44% of respondents indicated that their organisations currently have no plans to adopt a Zero Trust approach. The bigger insight drawn from this is the growing recognition of the importance of Zero Trust security in today's digital landscape. The majority's willingness to consider or already adopt this approach signifies a shift towards a more proactive and cautious stance regarding cybersecurity showing that organisations are increasingly prioritisng the need to protect their assets and data in an era of evolving cyberthreats.

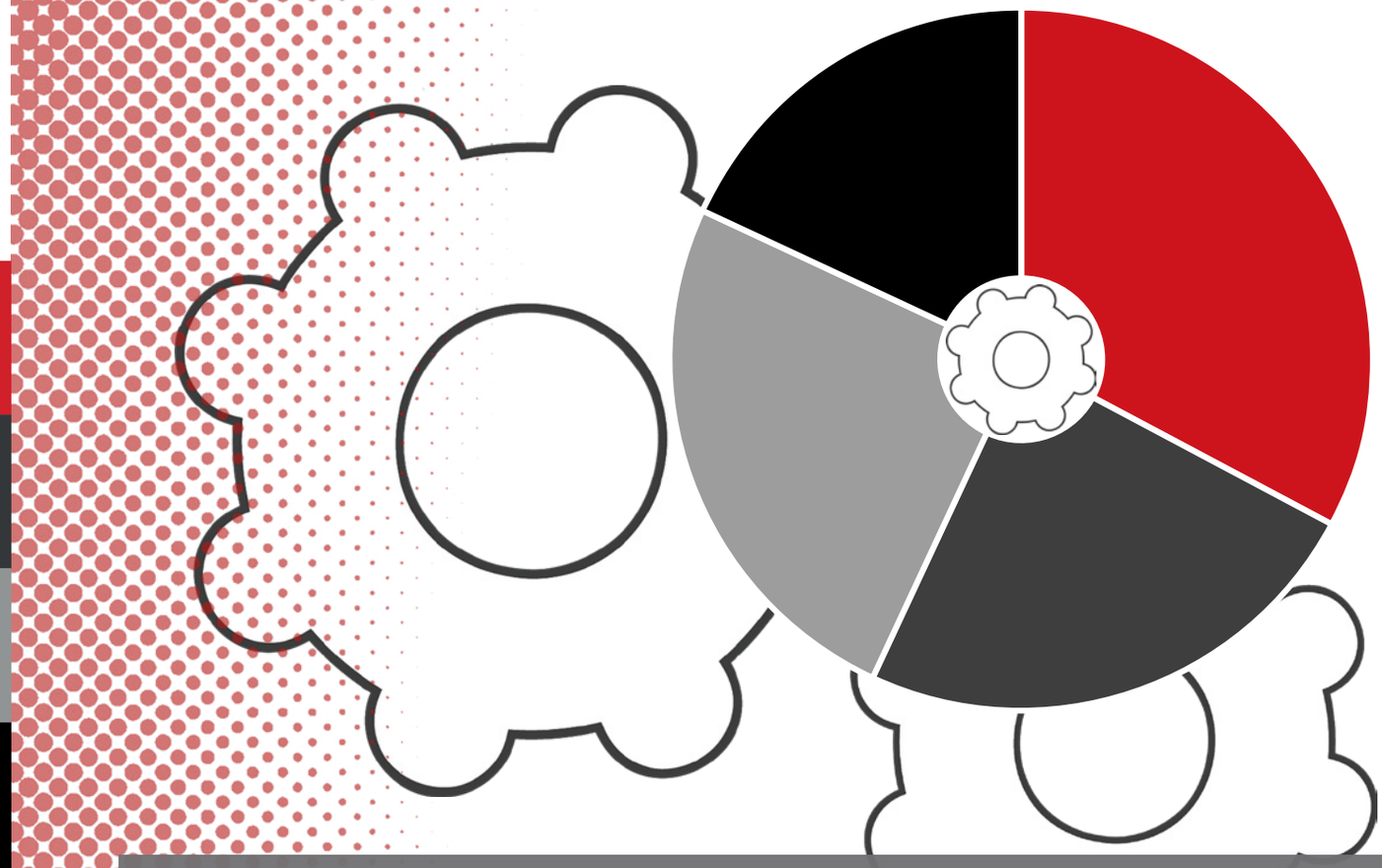
A Lynchpin Media BRAND

cxo priorities

QUESTION 12

How far do you believe automation will enhance your security capabilities?





KEY FINDINGS

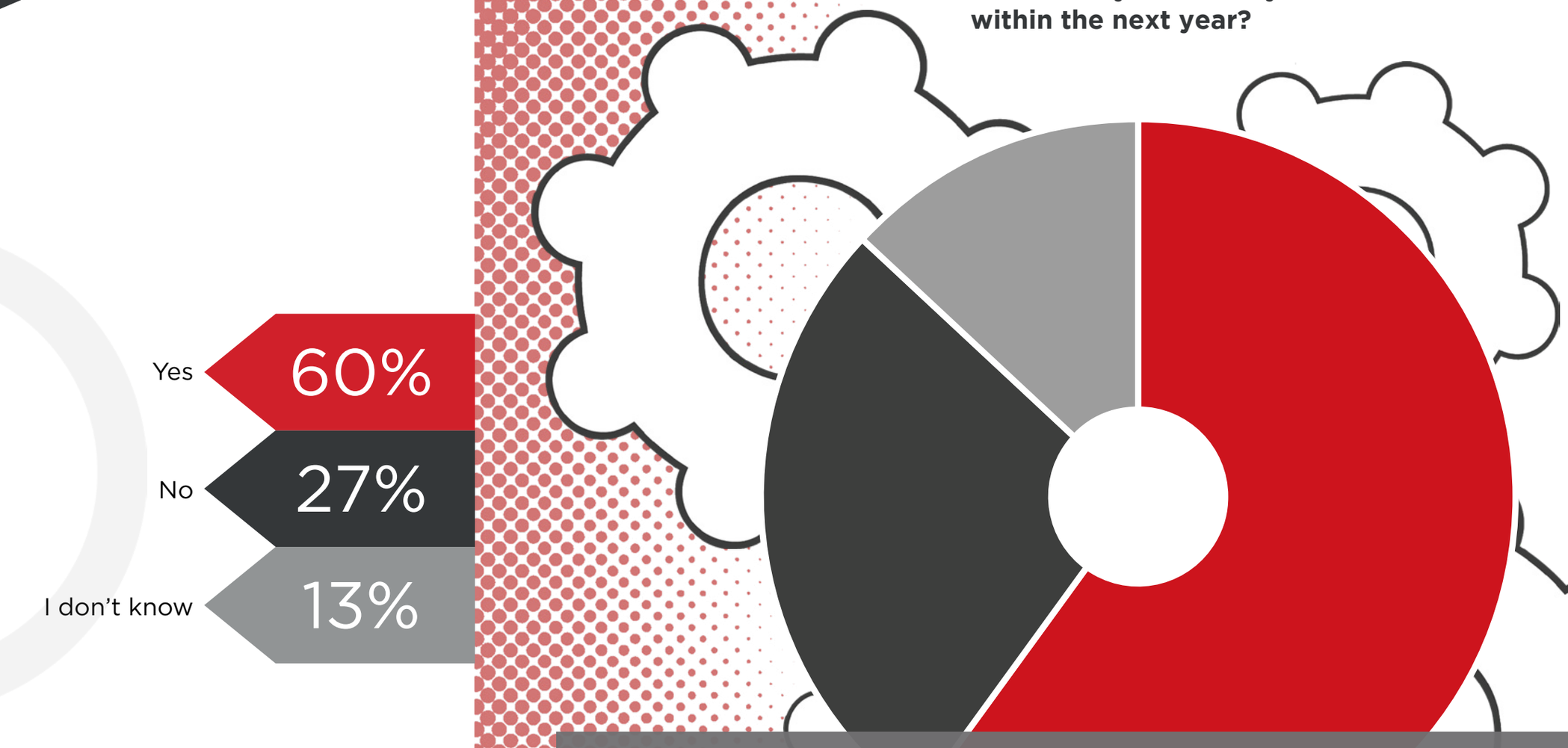
While 33% of respondents believe that automation will significantly enhance their security capabilities, 25% expressed scepticism stating that automation would not contribute at all to their security measures. A total of 24% of respondents anticipate a slight improvement in security through automation while 18% remain uncertain, highlighting the need for further exploration into the factors that shape these varying outlooks. This divergence in opinions raises questions about the perceptions and experiences of different organisations with automation. Although we uncover a division of perspectives on automation’s influence on security, there is proof of a stronger optimism in the potential benefits of technological advancements and a noteworthy percentage see potentials in automation’s ability to enhance security measures.

A Lynchpin Media BRAND

cxo priorities

QUESTION 13

Is your organisation planning to use AI cybersecurity tools within the next year?



Yes 60%

No 27%

I don't know 13%

KEY FINDINGS

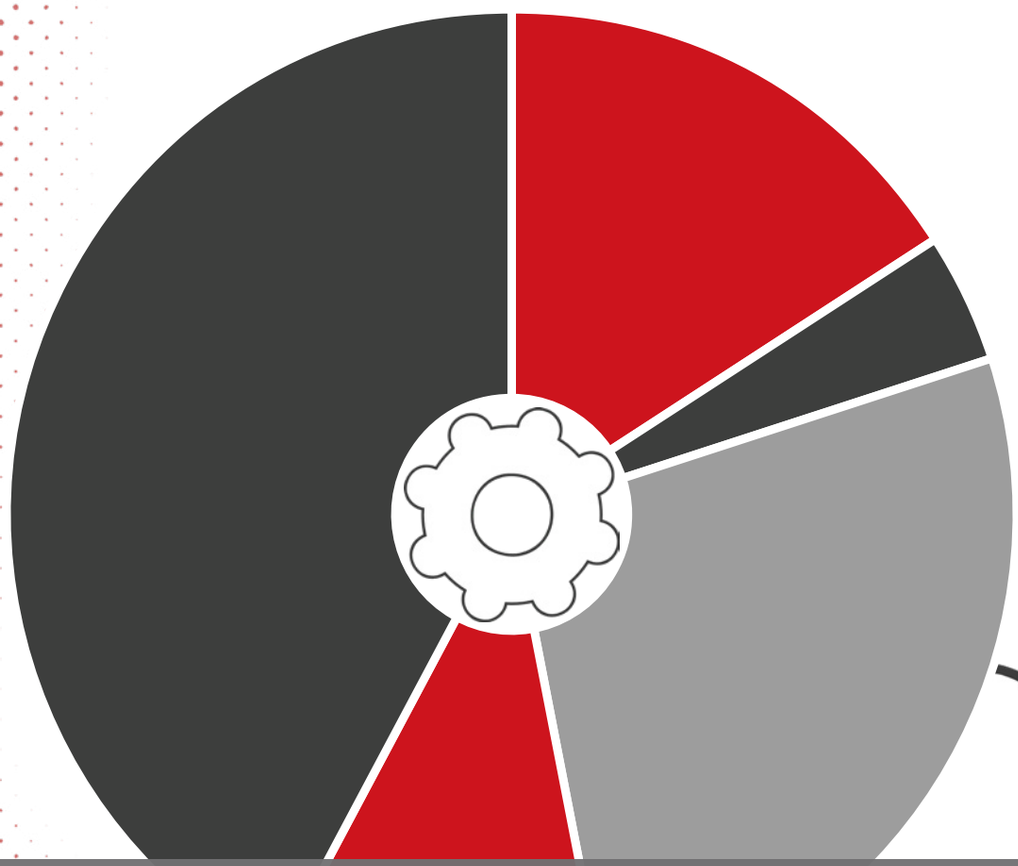
The majority of organisations (60%) plan to incorporate AI cybersecurity tools over the next year while 27% state their organisations do not have plans to implement such tools in the near future. A smaller but noteworthy segment (13%) remained uncertain about their organisation's AI cybersecurity adoption plans highlighting a degree of ambiguity within this domain.
The majority of organisations leaning towards adoption in the coming year highlights a prevalent interest in AI cybersecurity tools and reflects a growing recognition of AI's potential in fortifying digital defences. The notable proportion that remains undecided may be an indication of the need for further education and clarification in the realm of AI cybersecurity to address the hesitancy observed among some organisations.

A Lynchpin Media BRAND

cxo priorities

QUESTION 14

How do you expect your budget for cybersecurity to change in the next year?



It will increase significantly	16%
It will increase slightly	4%
It will not change at all	27%
It will decrease slightly	11%
It will decrease significantly	42%

KEY FINDINGS

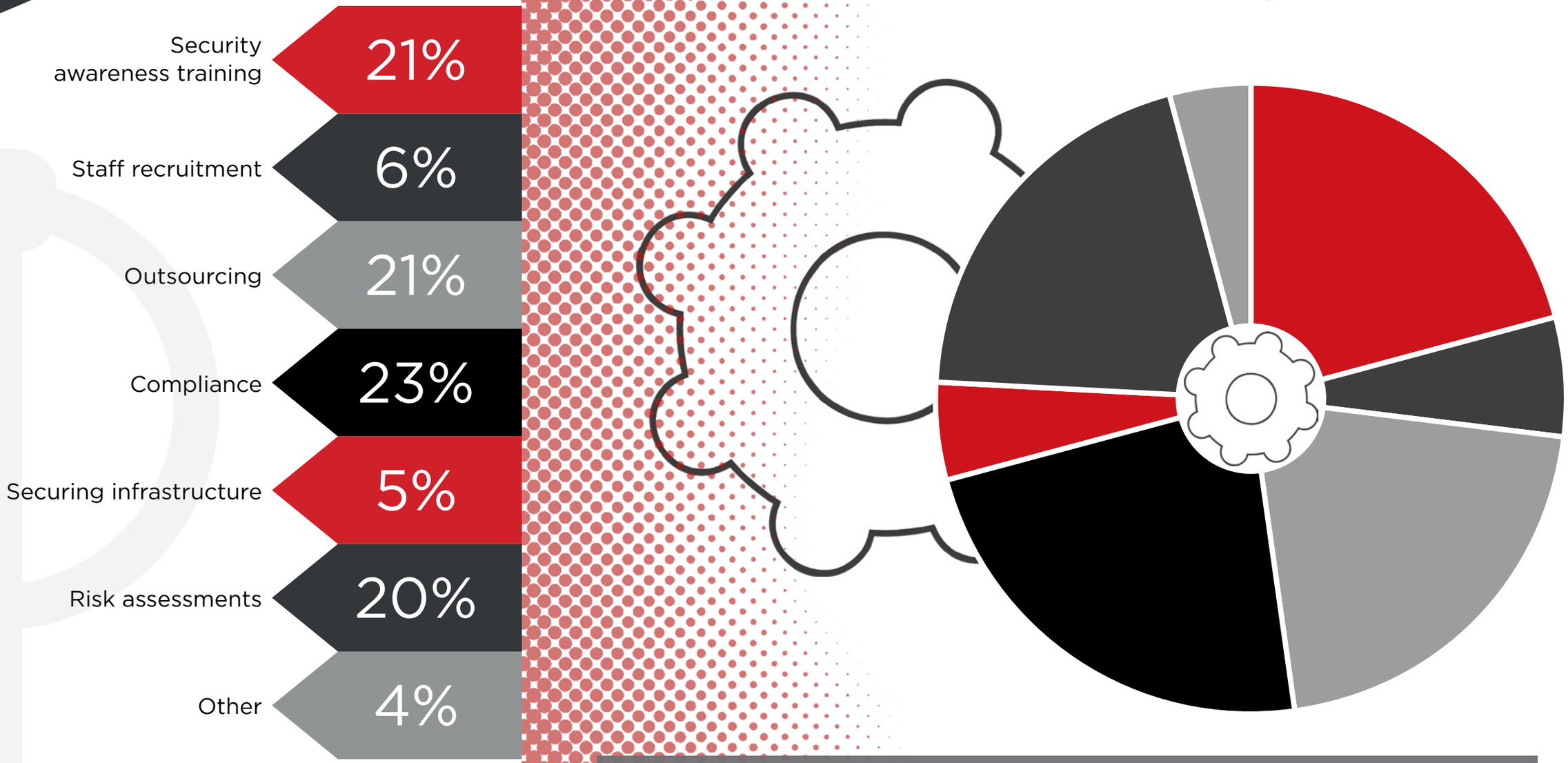
Forty-two percent of organisations anticipate a significant decrease in their cybersecurity budget indicating a potential shift in priorities or perhaps a reaction to perceived changes in the threat landscape. This sizable reduction is juxtaposed with a mere 4% who foresee a slight increase in their cybersecurity spending, suggesting a stark contrast in strategic approaches. A total of 27% of respondents expect their cybersecurity budget to remain static. This diversity in responses suggests the complex and dynamic nature of cybersecurity preparedness. It reminds organisations of the need to carefully consider budgetary adjustments to ensure effective protection against cyber threats even as they navigate a range of other factors like emerging threats and economic constraints.

A Lynchpin Media BRAND

CXO priorities

QUESTION 15

To which of the following do you intend to prioritise budget allocation in the coming 12 months?



KEY FINDINGS

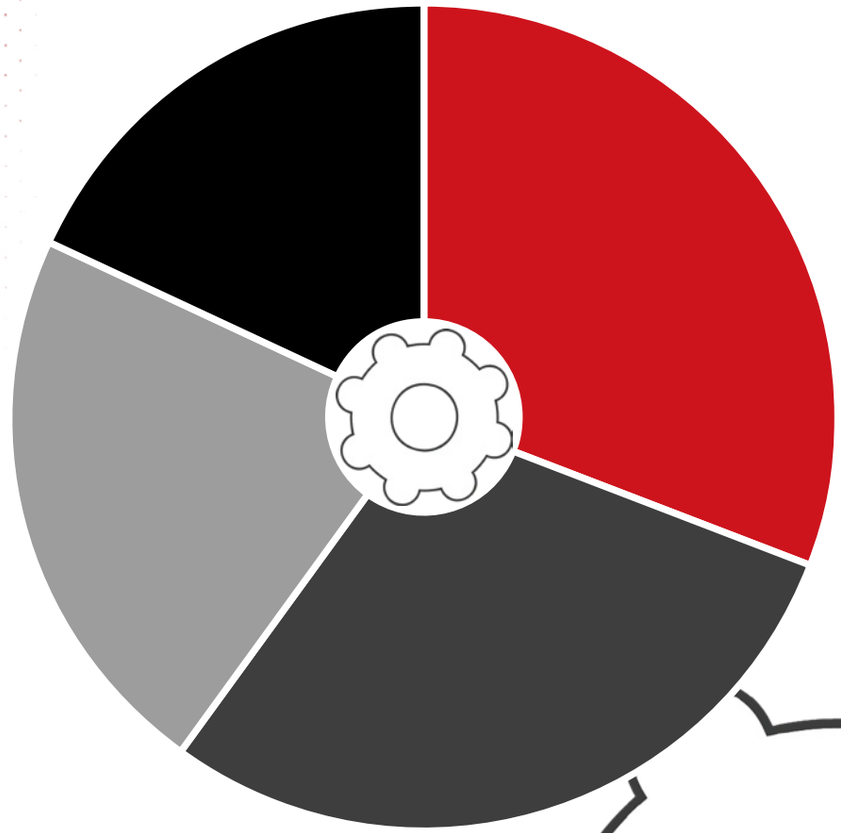
Compliance (23%) is the biggest priority for budget allocation in the next 12 months. This is closely followed by outsourcing and security and awareness training (21%), and risk assessments (20%). This highlights the growing importance of regulatory adherence in today's business landscape and a dual focus of both bolstering training and leveraging external expertise to tighten security measures.

A Lynchpin Media BRAND

cxo priorities

QUESTION 16

How challenging do you find it to demonstrate ROI for cybersecurity?



Very challenging 31%

Slightly challenging 29%

Not challenging at all 22%

I don't know 18%

KEY FINDINGS

Neary a third of respondents (31%) find it very challenging to demonstrate Return on Investment (ROI) for cybersecurity initiatives. Additionally, 29% of participants express that it is slightly challenging. This shows that organisations face some difficulty in showcasing the tangible returns on their investments in cybersecurity measures. But on the positive, 22% of respondents reported that they do not find it challenging at all, suggesting that a notable minority feels confident in their ability to demonstrate ROI for cybersecurity efforts. These results summarise the prevalent challenges in quantifying the value of cybersecurity investments, with a substantial proportion of professionals grappling with this issue.

A Lynchpin Media BRAND

cxo priorities

REPORT SUMMARY

With over half of the respondents stating that their organisation has seen an increase in the number of attacks over the last 12 months last year, it is evident that organisations are keen to advance their security policies. The findings suggest that decision-makers are keen to focus on and develop their AI, automation, hybrid working and Zero Trust strategies. However, as budgets are a constraint, providers need to offer a comfortable price point that enables organisations to derive maximum benefits.

More than half of the respondents cited a shortage in cybersecurity skills and were looking to resolve this gap through outsourcing. Being able to derive benefits from vendors who specialise in off-premise hardware would be a key driver for organisations. There is no better time for companies to have reliable partners who can create and implement hybrid working cybersecurity strategies efficiently.

Thankfully, the findings highlight that compliance, outsourcing, security and awareness training and risk assessment are top areas for investment for companies. By taking a long-term approach and securing and seeking vendors to help obtain crucial in-house management services and solid regulatory framework expertise, organisations can put themselves on the path to improved cyber-resilience and ensure a secure ethos is in place.

In conclusion organisations should consider investing in several key areas to bolster their security posture. These are; cybersecurity training, outsourcing partnerships, Zero Trust solutions, AI-powered security tools, compliance solutions and advanced analytics. Only then will they be able to compete in an increasingly hostile digital landscape.

By

Krishan Parmar,
Senior Content Strategist,
Lynchpin Media

and

Arrey Bate,
Content Strategist,
Lynchpin Media

A Lynchpin Media BRAND

priorities

Lynchpin Media

Lynchpin Media is a global technology media, data and marketing services company. We help to increase awareness, develop and target key accounts and capture vital information on regional trends.

Visit lynchpinmedia.com for more information.

priorities

CxO Priorities, a Lynchpin Media Brand
63/66 Hatton Garden
London, EC1N 8LE
United Kingdom

Find out more:
www.cxopriorities.com