A Lynchpin Media BRAND

priorities

MSSP Data Security Insights Survey 2022

A CXO Priorities' survey, in partnership with Rubrik

rubrik

priorities

A Lynchpin Media BRAND

Contents

TOPIC: Insights on data security attitudes and priorities of businesses 2022/23

ABSTRACT: The aim of this survey is to identify the pain points and attitudes of organisations struggling to deal with threats from bad actors and tackle them with limited resources. This report explores the priorities, attitudes and protection and recovery systems in place for businesses by using data from CIOs, COOs, CISOs or senior IT or cybersecurity-focused leaders.

rubrik

priorities

A Lynchpin Media BRAND

Introduction

We asked CIOs, COOs, CISOs or senior IT or cybersecurity-focused leaders across EMEA about their customer-bases' challenges, attitudes and priorities regarding their cybersecurity.

Some results were promising, with a recent development in customers understanding the importance and purpose that cyberattack prevention methods play within their business. But many remain unconcerned about the consequences of poor cybersecurity and have retained a dismissive and reactive approach to attacks.

Many security providers and those at C-level can learn something from these results. You can find key takeaways after each section, followed by a conclusion of what was discovered from this data.

The confirmed criteria for the 50 respondents.
Please use the below table:

Job titles:	CIO, COO, CISO or senior IT or cybersecurity-focused leaders
Geo:	North America and EMEA (70% North America, 30% EMEA)
Industry:	Managed services only (MSP, MSSP, CSP)
Company size:	MSPs of 200+

rubrik

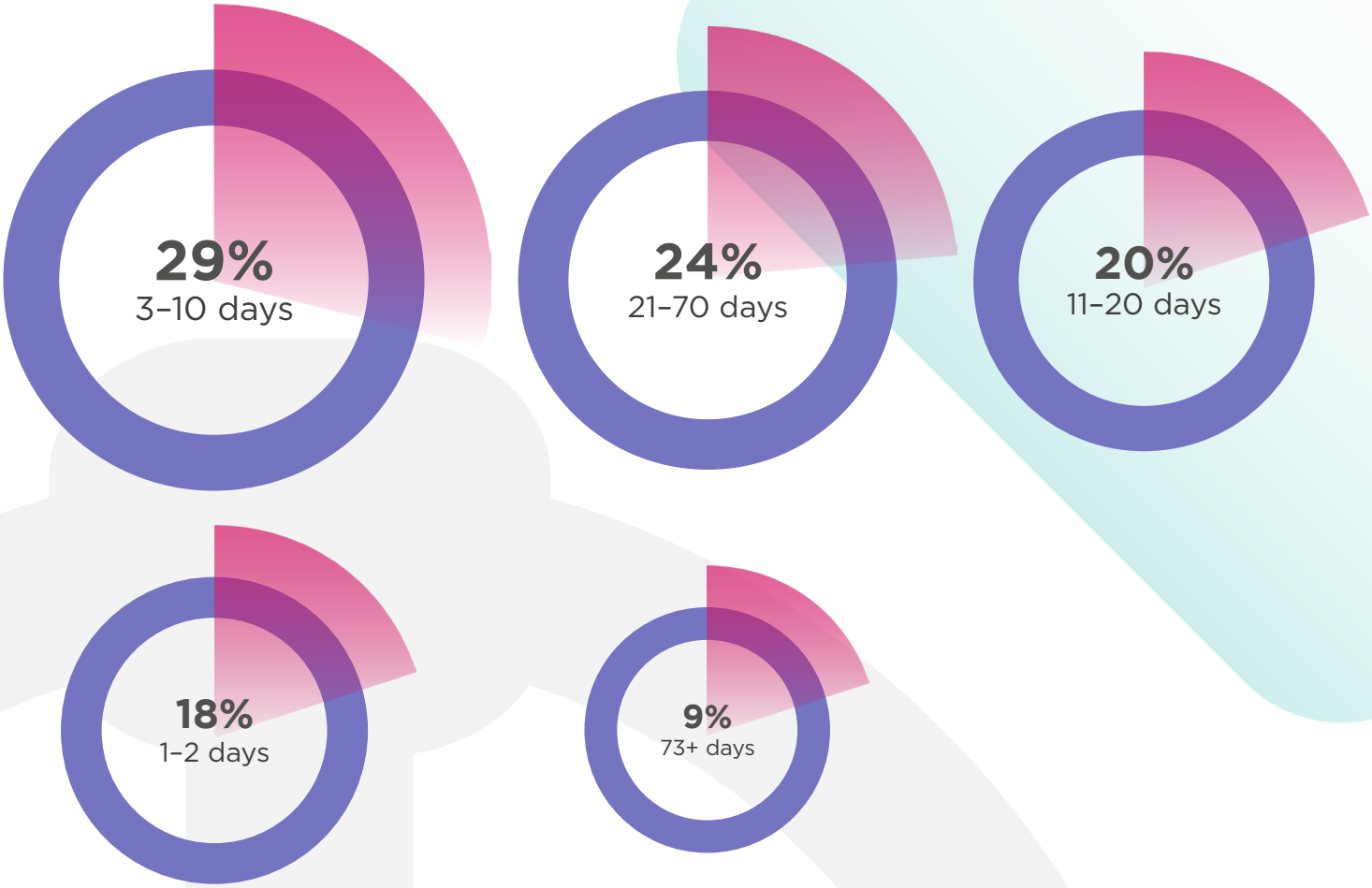
priorities

A Lynchpin Media BRAND

Chapter 1 Customer challenges and threat landscape

QUESTION 1

How long, on average, would you estimate it takes for your customer base to contain a breach?



KEY TAKEAWAY

The average amount of days it takes for the respondents' customers to contain a breach range from 3–70 days, with the majority (30%) being able to contain the breach in days 3–10. Only 18% have the ability, whether it be skills, software, resources or training, to swiftly contain the breach in the first 1–2 days.

rubrik

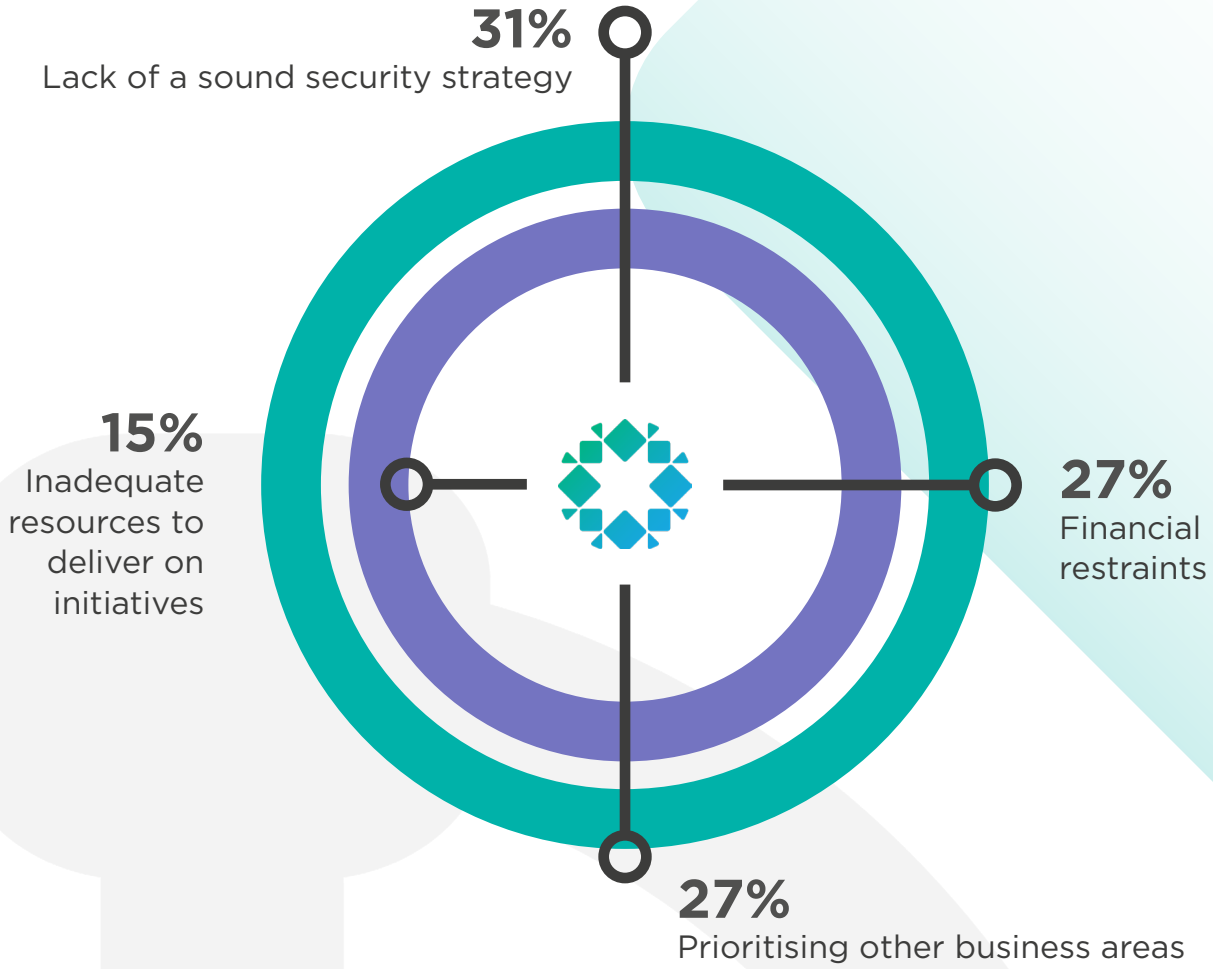
priorities

A Lynchpin Media BRAND

Chapter 1 Customer challenges and threat landscape

QUESTION 2

In your opinion what has been preventing enterprises from investing more resources into data security?



KEY TAKEAWAY

Three of the four factors preventing enterprises from investing more into data security resources are almost on par with one another. Eighty-five percent of respondents equally agreed that financial restraints, prioritising other business areas and the lack of a sound security strategy are equally accountable for the hold-back on investments in security. Only 15% consider inadequate resources to deliver on initiatives as a cause for the lack of investment in security areas.

rubrik

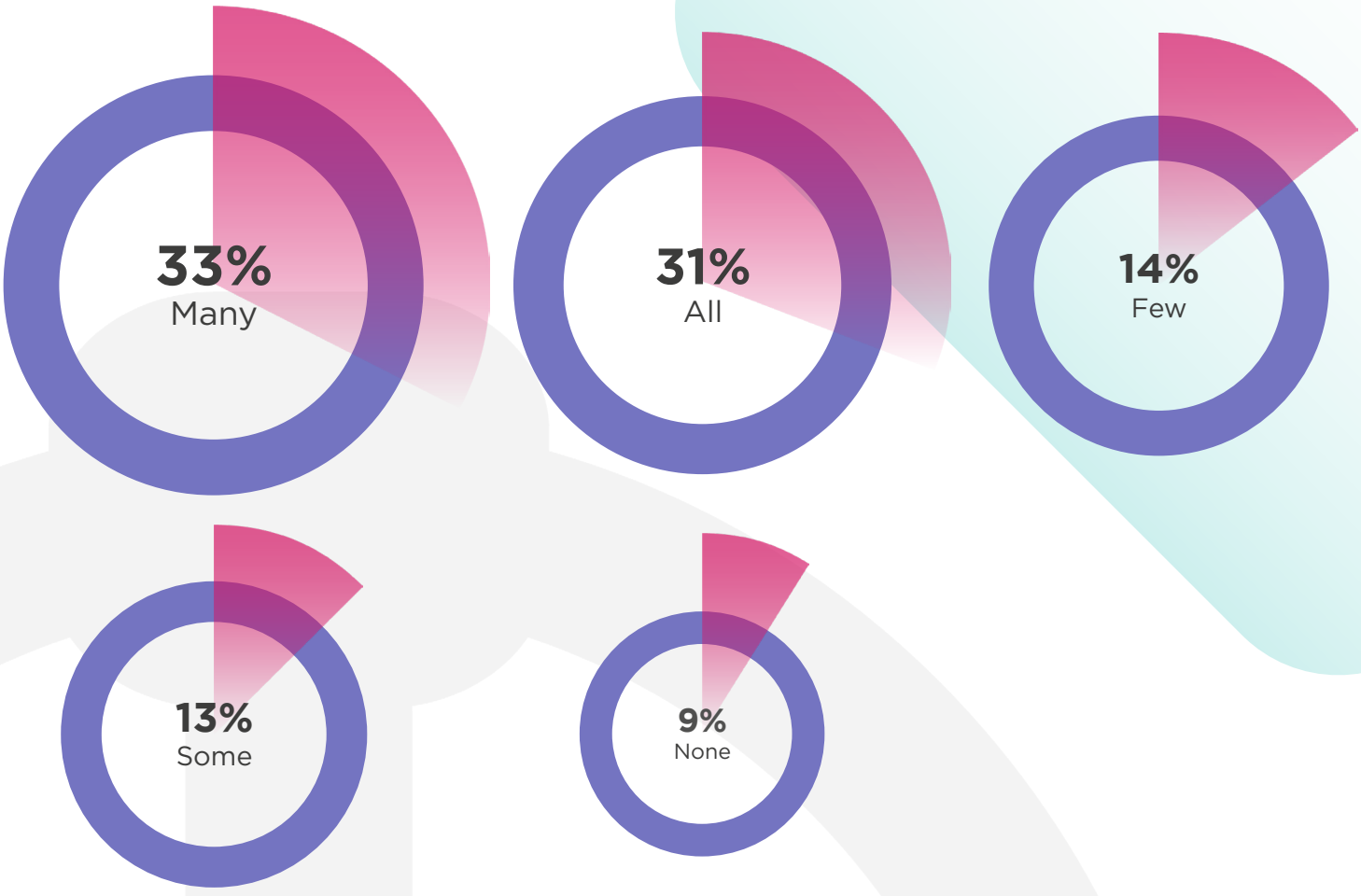
priorities

A Lynchpin Media BRAND

Chapter 1 Customer challenges and threat landscape

QUESTION 3

To your knowledge, how many of your customers already have a data recovery plan in place to address ransomware attacks?



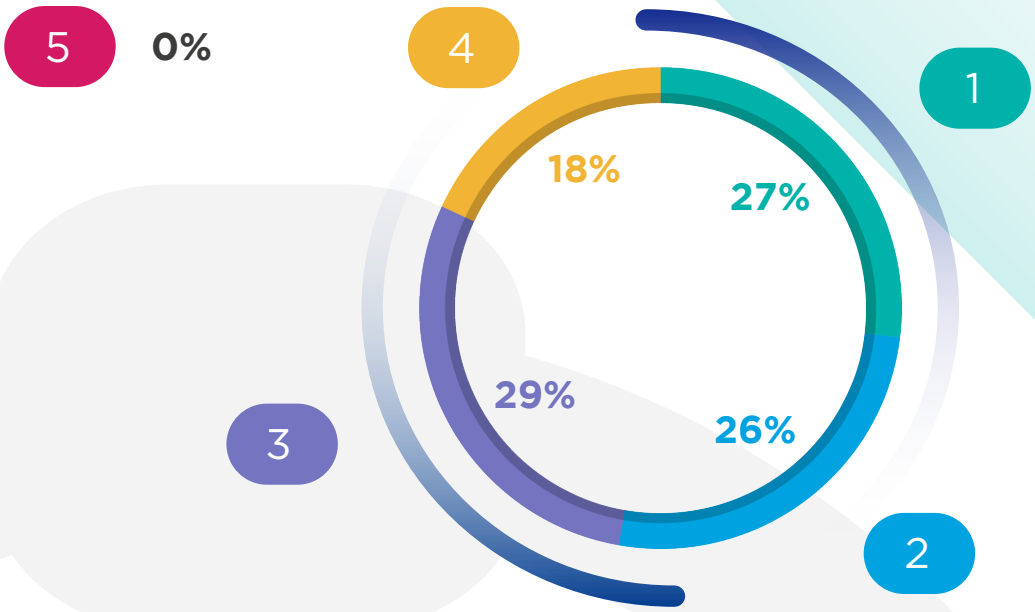
KEY TAKEAWAY

Only 31% of respondents are confident that all their customers have a data recovery plan in place, suggesting the remaining 69% have customers lacking a strategy when addressing ransomware attacks.

Chapter 1 Customer challenges and threat landscape

QUESTION 4

How have customers' perceived risk levels changed in line with the expanding attack surface? (1: They are more concerned. 5: Not concerned at all)



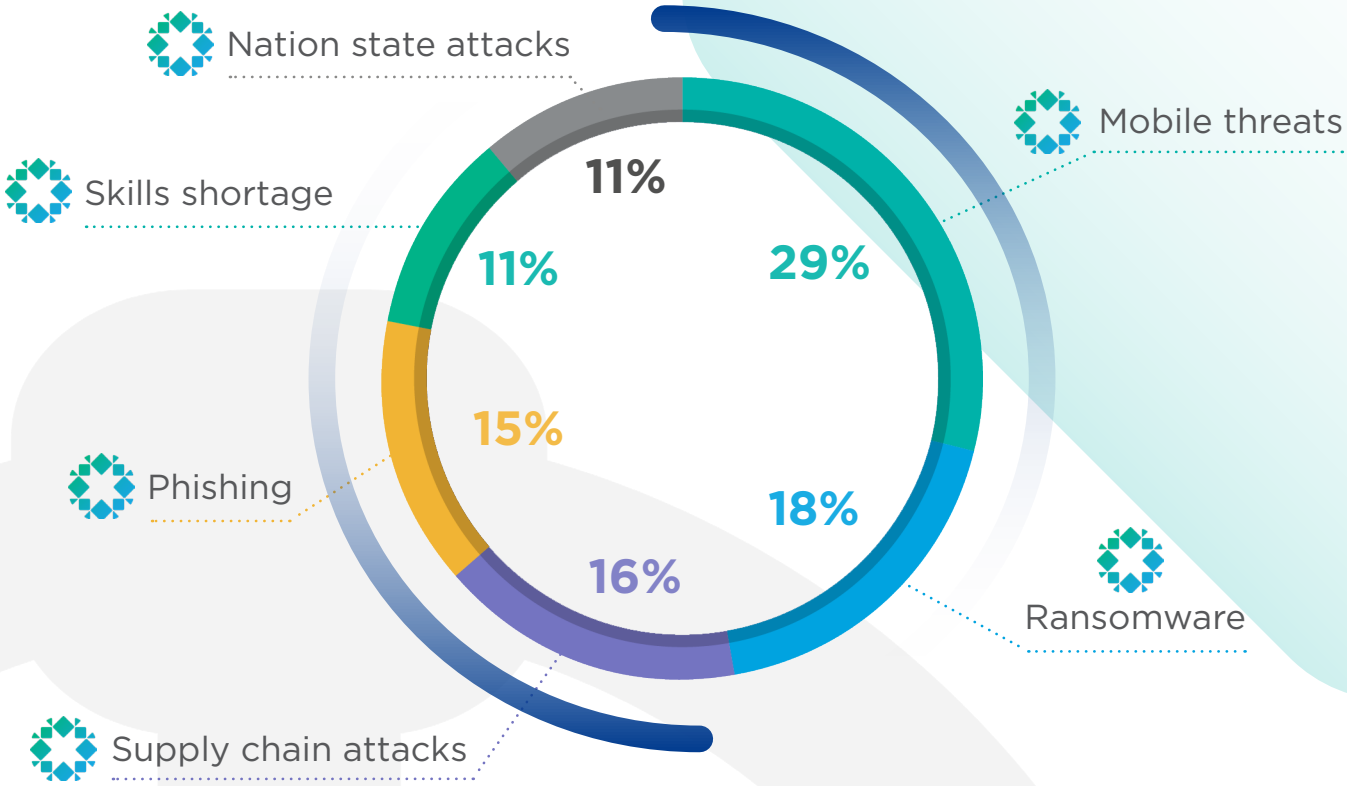
KEY TAKEAWAY

To the respondents' knowledge, their customers perceived risk levels are spread evenly between being more concerned and only slightly concerned. If the correct messaging and understanding of the expanding threat surface was reaching the ears of these customers, we should be expecting a higher rate of concern. Thankfully we can see that no respondents believe their customers are disregarding perceived risk levels completely, with almost 100% agreeing all of their client bases have some level of concern, even if it's a minority.

Chapter 1 Customer challenges and threat landscape

QUESTION 5

What are the key cyberthreats your customers are experiencing?



KEY MESSAGING

The highest rated cyberthreats faced by customers are mobile threats (29%). With confidence, we can see mobile threats are a priority threat type and a real issue for the respondents' client bases. Alongside this major concern, all the threat types presented and selected can be addressed and prevented through MSSPs.

rubrik

priorities

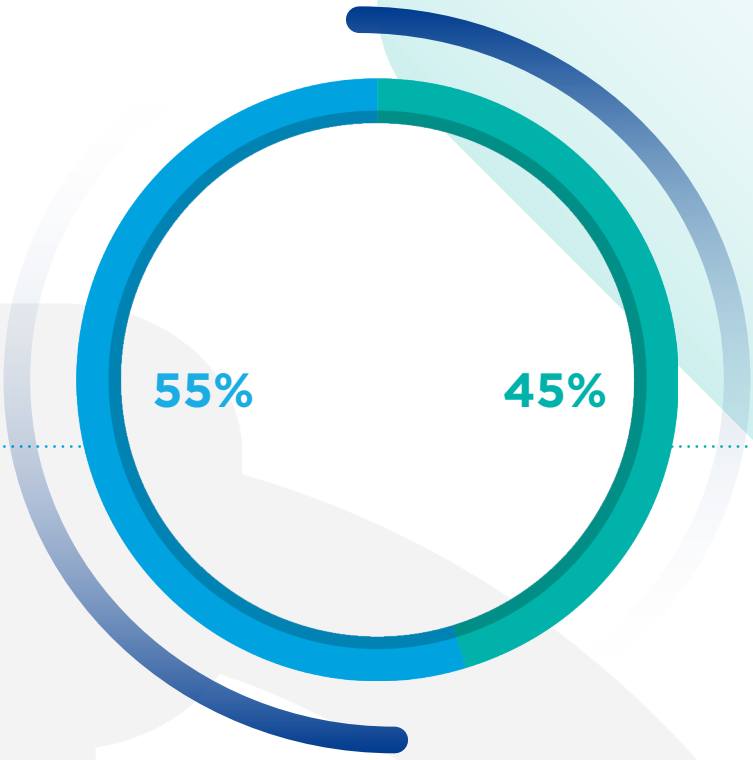
A Lynchpin Media BRAND

Chapter 1 Customer challenges and threat landscape

QUESTION 6

How confident do you believe your customers are that their current resources can adequately prevent cyberattacks?

0% Not confident at all



Medium level of confidence

Highly confident

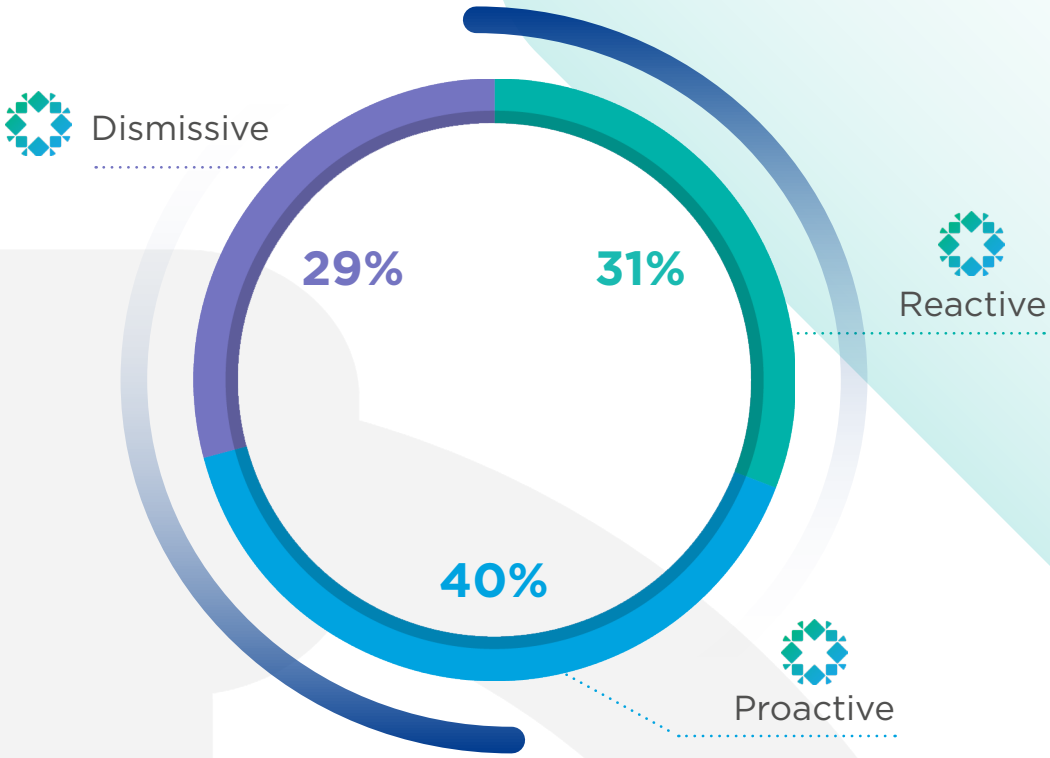
KEY MESSAGING

It is promising to see that no respondents have zero confidence in their customers' resources. However, over half (55%) of respondents retain only a medium level of confidence that their customers' current resources can adequately prevent cyberattacks. This does show there is a lack of faith in current tools, systems and processes that can be addressed and prevented through MSSPs.

Chapter 1 Customer challenges and threat landscape

QUESTION 7

In your opinion do you feel companies have reactive, proactive or dismissive approaches to cybersecurity?



KEY MESSAGING

Security industry leaders have been encouraging a proactive approach to security for years and to see that 60% of respondents feel companies have a reactive and even dismissive approach to their cybersecurity is concerning.

rubrik

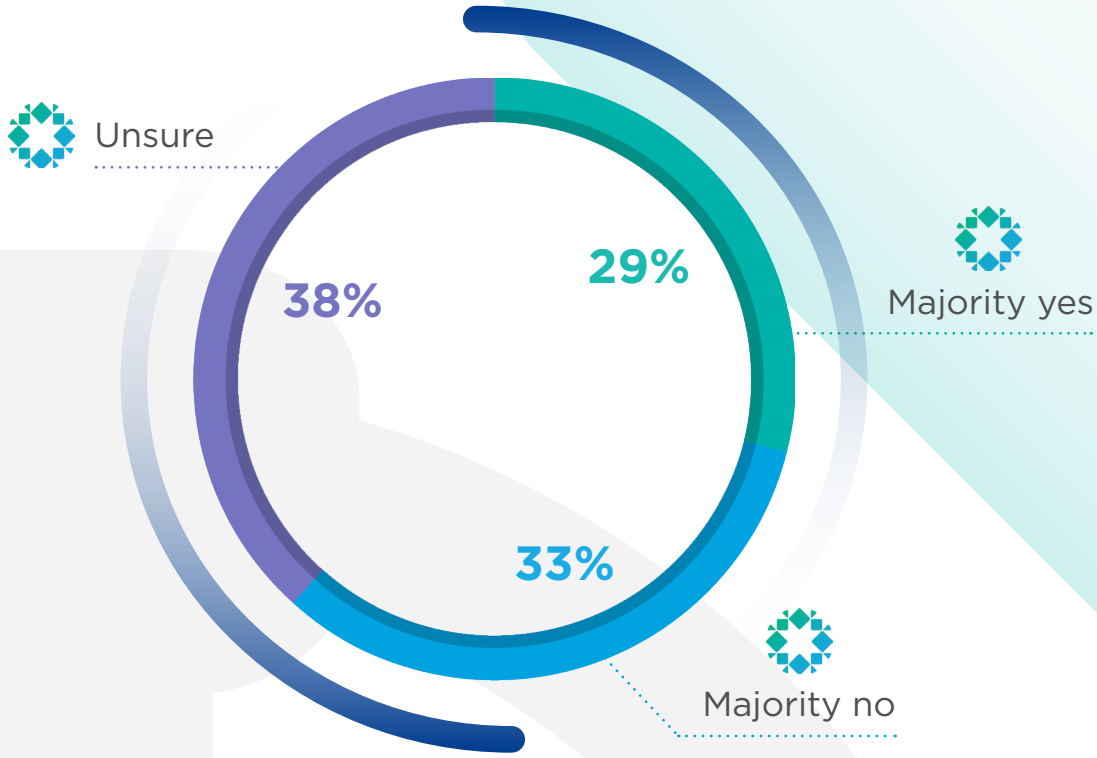
priorities

A Lynchpin Media BRAND

Chapter 2 Priorities and planning ahead

QUESTION 8

Do your customers feel increased pressure to invest in cybersecurity due to the increase in attacks?



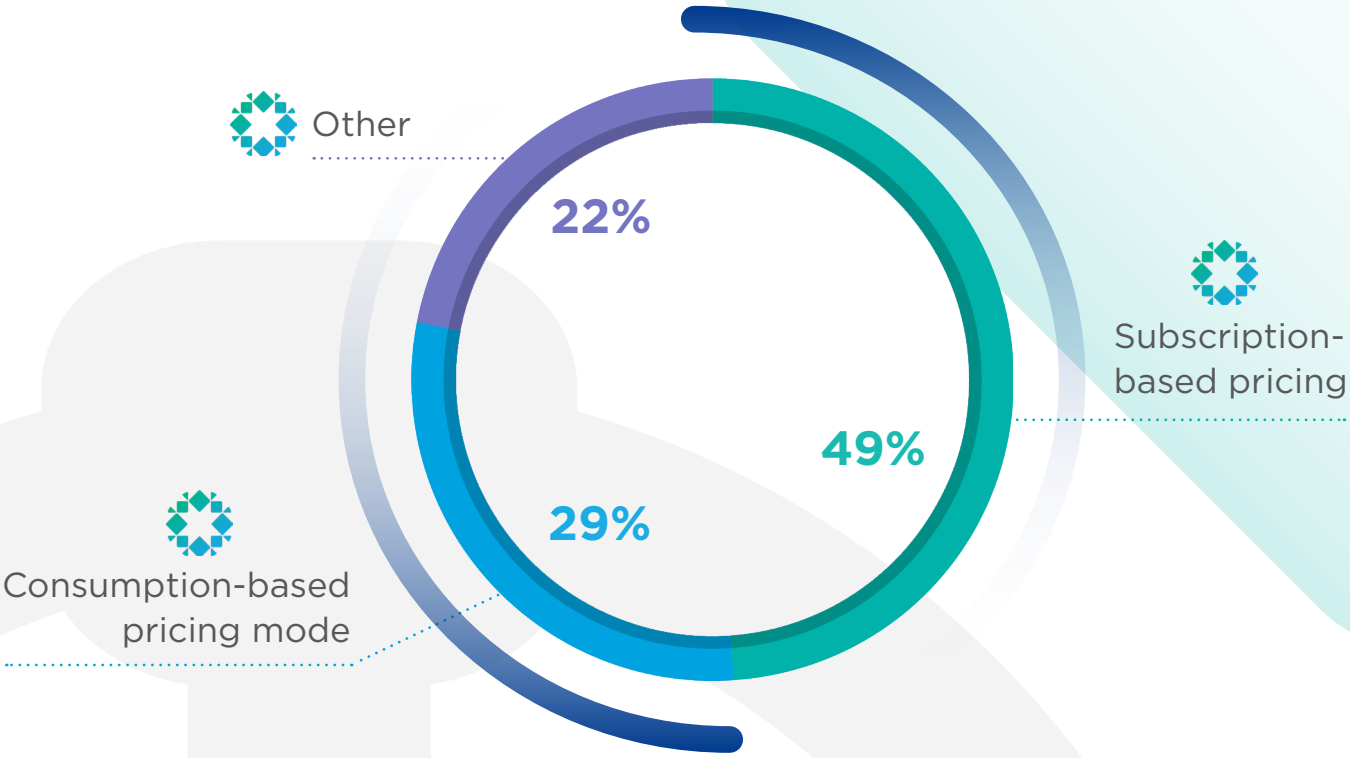
KEY MESSAGING

Even though we are seeing an ever-expanding attack surface, we can see here that there are still blocks in messaging and understanding when it comes to the importance of cybersecurity investments, with 33% of respondents saying majority of customers do not feel an increased pressure to invest.

Chapter 2 Priorities and planning ahead

QUESTION 9

What financial plan would be most attractive to customers?



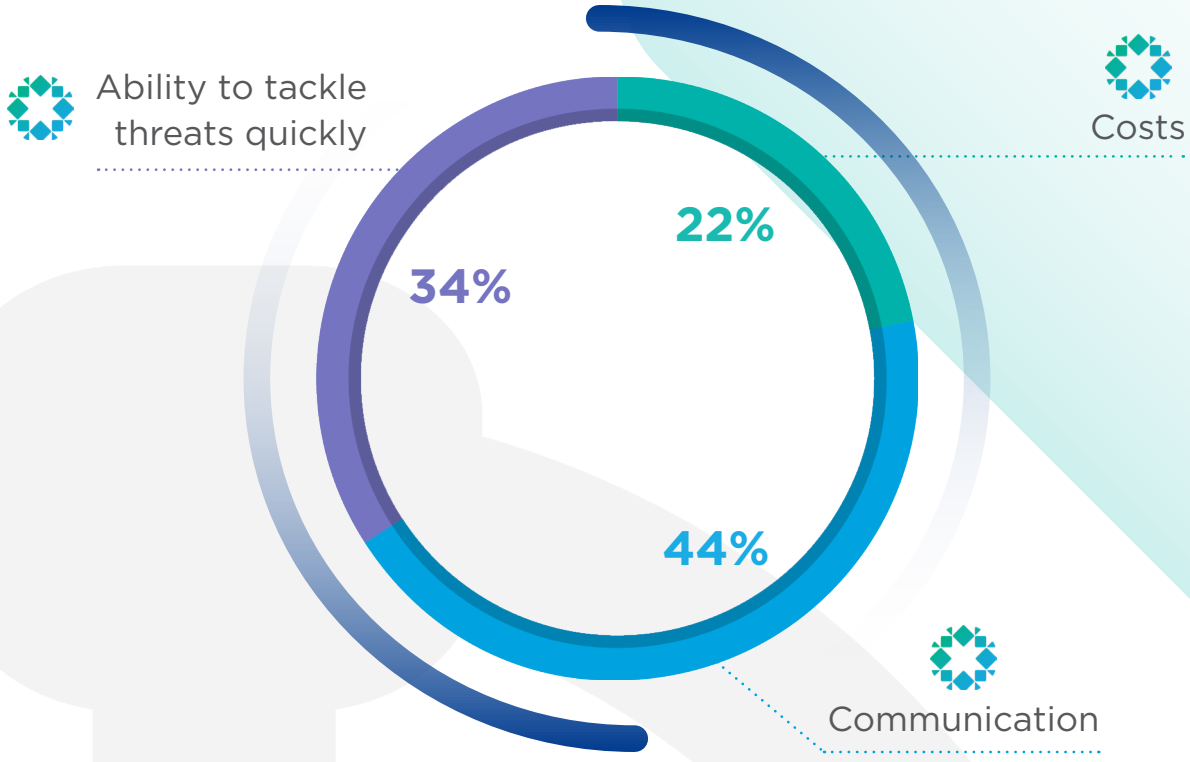
KEY MESSAGING

When investigating financial plans, subscription-based pricing comes out as the most popular of models by almost 50%.

Chapter 2 Priorities and planning ahead

QUESTION 10

What do customers highlight as the key values when choosing an MSSP?



KEY MESSAGING

Interestingly, majority of respondents (44%) feel good communication is the prioritised key value when choosing an MSSP. With reasonable costs stated as the least important of the three values, we still see 22% agreeing it is important. To zoom in on this result, we see question 9 investigating financial plans, with subscription-based pricing coming out as the most popular of models by almost 50%.

rubrik

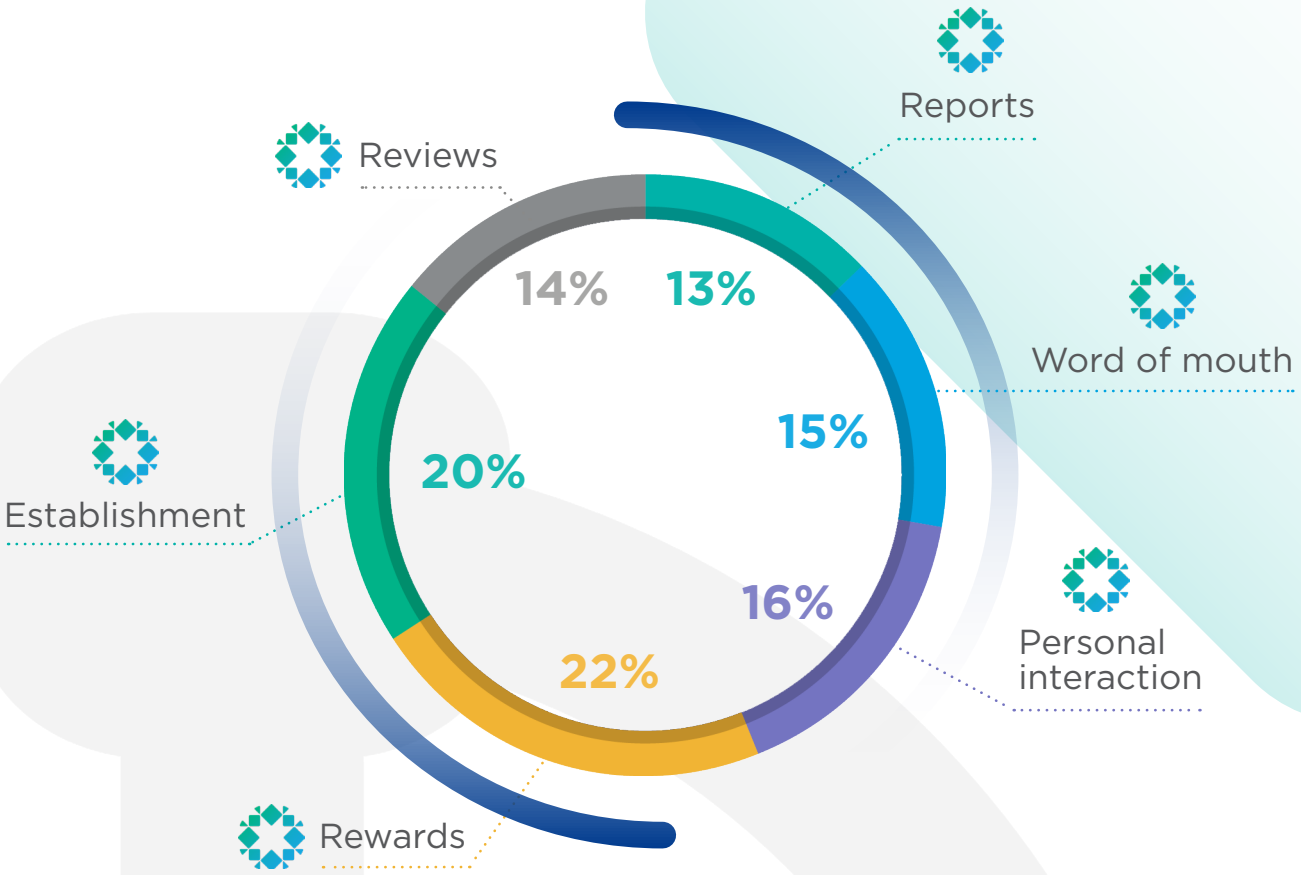
priorities

A Lynchpin Media BRAND

Chapter 2 Priorities and planning ahead

QUESTION 11

How do you find that customers assess a security partner's credibility?



KEY MESSAGING

It appears that for a security partner to have the credibility to impress a vendor it may be best to act on all these areas for the best scope. With such a wide scope of ways for customers to assess credibility it would be best to apply effort in all areas.

rubrik

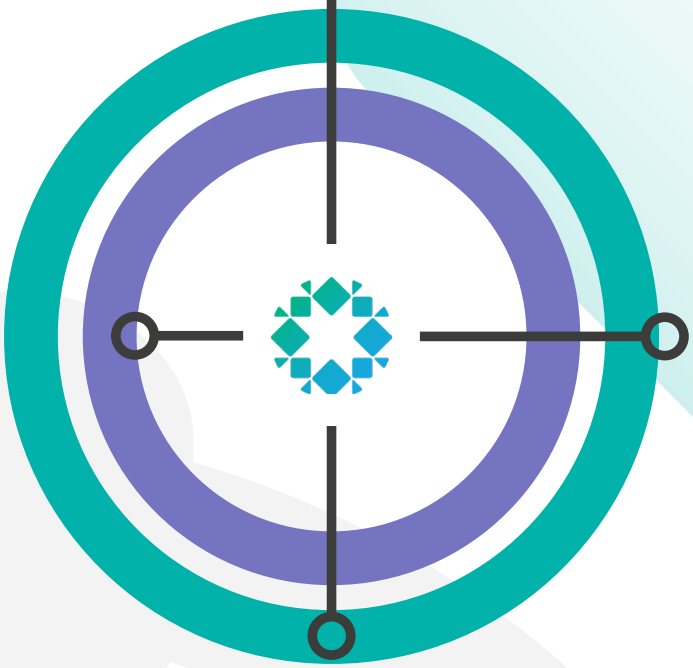
priorities

A Lynchpin Media BRAND

Chapter 2 Priorities and planning ahead

QUESTION 12

In your role, what are the key priorities for you looking ahead?



40%
Invest in new tools and technologies that ensure Business Continuity for customers

18%
Improve threat intelligence capabilities for customers

22%
Ensuring a cloud-first model

0%
Identify vendor partners with expansive support services

20%
Control costs better through alternative pricing models

KEY TAKEAWAY

A majority of respondents are prioritising their investment in new tools and technologies that ensure Business Continuity for customers in the future. Yet none of the respondents are prioritising – or potentially considering – identifying vendor partners with expansive support services. This gives us the impression that IT or cybersecurity-focused leaders do not feel the need to outsource, but instead intend to internally improve cybersecurity methods.

Conclusion

Embracing Digital Transformation is a natural process for businesses in securing their future in this digital world, but with this movement we are expectantly seeing an expanding attack surface. Understanding where businesses are, mentally and physically, with their cybersecurity efforts is important to discover ways to support them and prevent these detrimental attacks from occurring.

These results conclude that the attitudes and actions needed to improve these businesses' cybersecurity efforts do not align. The results prove there is often a lack of concern for cybersecurity and that companies are suffering because of it, primarily from mobile threats. We see that too many businesses are retaining a reactive or dismissive approach to attacks, indicating there is room for education and messaging regarding the severe consequences of a data breach, as well as the ever-expanding attack surface.

With regards to ensuring Business Continuity, majority of respondents are aiming for investment in new tools and technologies, yet none of the respondents are prioritising or potentially even considering identifying vendor partners with expansive support services. This suggests that IT or cybersecurity-focused leaders do not feel the need to outsource, but instead intend to internally improve cybersecurity methods. Suggesting providers should create a movement in attitudes to increase confidence in outsourcing and partnering with vendors. This could be done through messaging, reports, word of mouth and thought leadership to gain trust and reliability within this area. We can see that those businesses deciding to find managed security service providers (MSSP) lean towards good communication as a prioritised key value when choosing an MSSP. This shows us the communication strategies should fine-tuned if MSSPs are to reach organisations standards.

However, these findings show that a number of businesses are recognising and actioning their cybersecurity methods efficiently, by taking the results of a data breach seriously. These results show that there are no businesses that entirely dismiss cybersecurity but too many do not care enough.

Sponsored by:

20 St. Dunstan's Hill,
Suite 314
London, England EC3R 8HL

www.rubrik.com

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

www.cxopriorities.com