A Lynchpin Media BRAND

CxO priorities

A CxO Priorities report, in conjunction with BlackBerry

UNDERSTANDING THE SECURITY CHALLENGES OF SMBS

CONTENTS

INTRODUCTION

Since the pandemic, SMBs worldwide have noticed a shift towards remote and hybrid work cultures. As employees step out of the security confines of an organisation, the chances of falling prey to cyberattacks increase multifold. With critical data being shared across multiple touchpoints, securing and managing connected devices and protecting your employees has never been more crucial.

Industries across the world, irrespective of their size, are utilising technology like never before, which has led to an increase in cyberattacks and ultimately an increased awareness of cyberthreats. As organisations attempt to tackle security challenges, they cannot underestimate the ever-increasing number of connected devices. Adding to this challenge is a need to develop cybersecurity skills and invest in cybersecurity training.

As cyberthreats become more advanced, organisations often fail to create a robust security posture. Cybersecurity skills shortage can lead to devastating impacts for the organisation, including significant financial losses. With ongoing rapid digitalisation, organisations must understand the skill gap and onboard partners that can help reduce it.

As SMBs navigate the challenges of securing data across touchpoints while training their employees, the need for a reliable, external provider to mitigate risk and enhance cyber skills is growing. Through this survey, we wanted to discover the following:

> **Industries across the world, irrespective of their size, are utilising technology like never before.**

HOW ORGANISATIONS HAVE ADAPTED THEIR APPROACH TO CYBERSECURITY

GREATEST SECURITY THREATS

CYBERSECURITY SKILLS SHORTAGE AND ITS IMPACT

KEY DRIVERS FOR OUTSOURCING IT SECURITY FUNCTIONS

SCAN TO PODCAST

SUMMARY OF FINDINGS

1

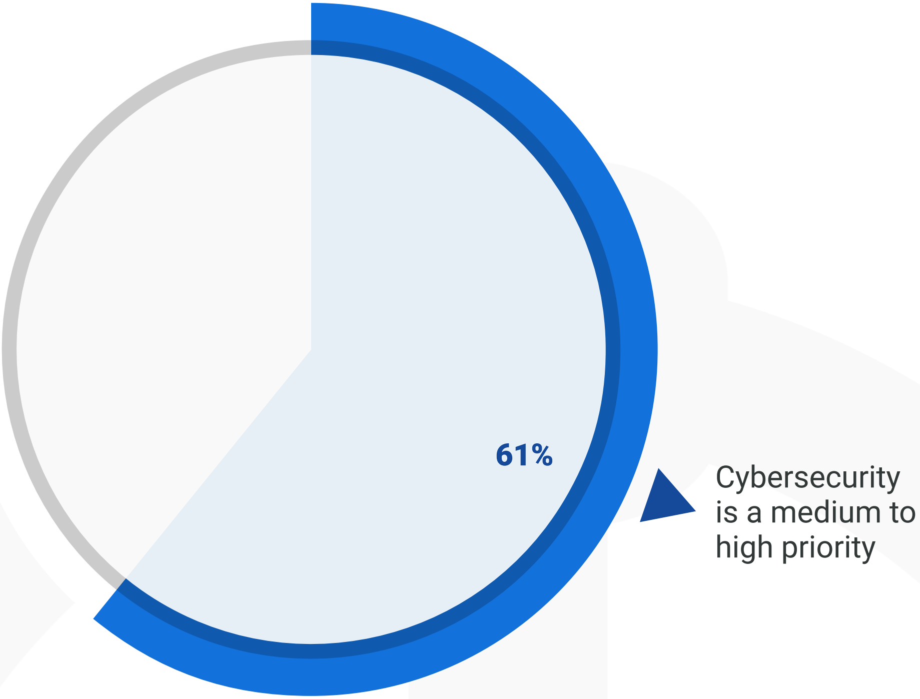
61% RESPONDENTS CONSIDER CYBERSECURITY AS A MEDIUM TO HIGH PRIORITY FOR THEIR ORGANISATION

2

3

4

5



SUMMARY OF FINDINGS

1

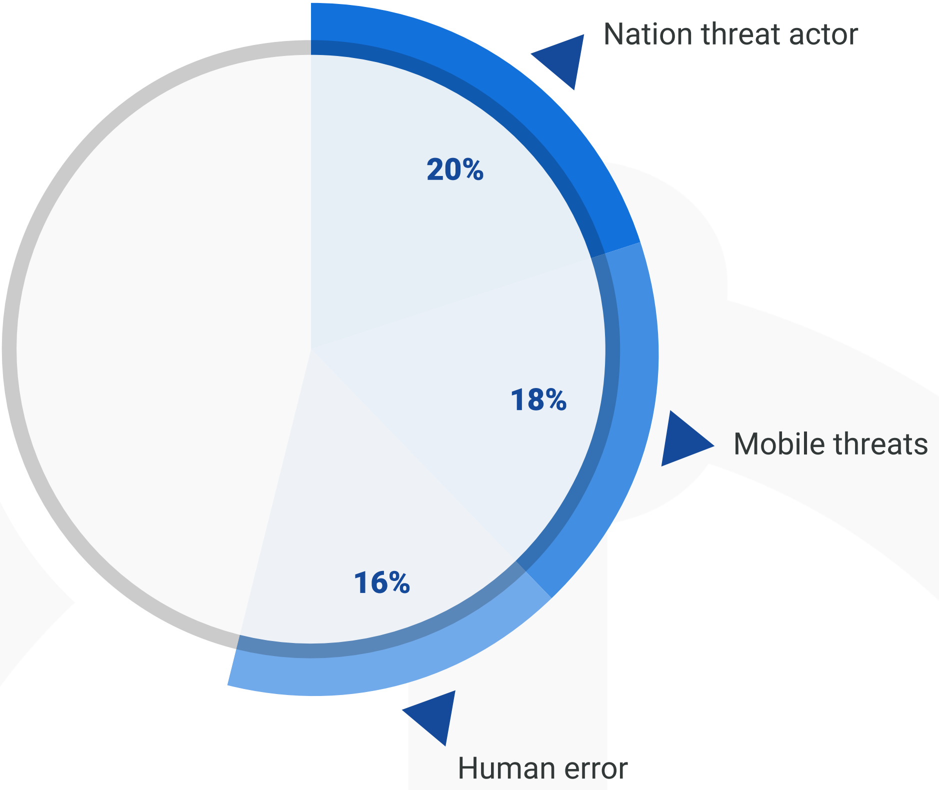
2

NATION THREAT ACTORS (20%), MOBILE THREATS (18%) AND HUMAN ERROR (16%) ARE CONSIDERED AS THE GREATEST SECURITY THREATS

3

4

5



SUMMARY OF FINDINGS

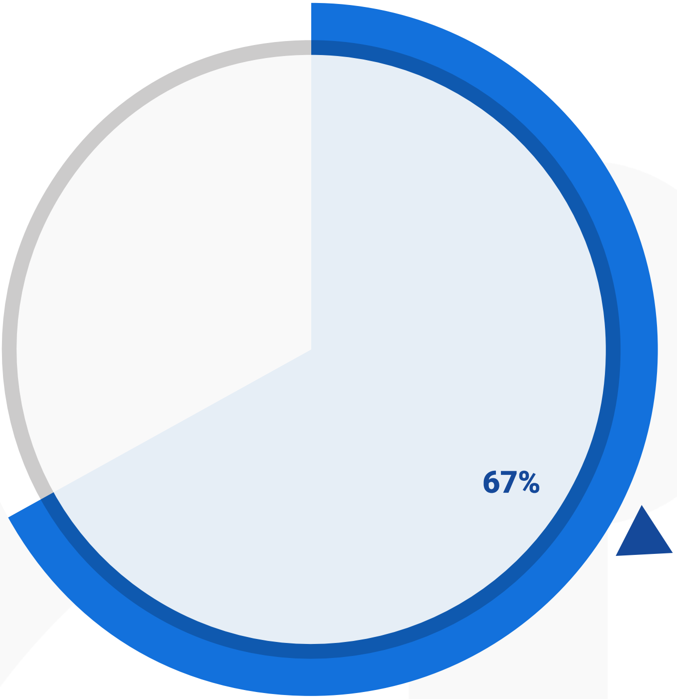
1

2

3 MAJORITY OF RESPONDENTS (67%) EITHER FACE A SHORTAGE OF CYBERSECURITY SKILLS OR AREN'T SURE

4

5



Face a shortage of cybersecurity skills or aren't sure

SUMMARY OF FINDINGS

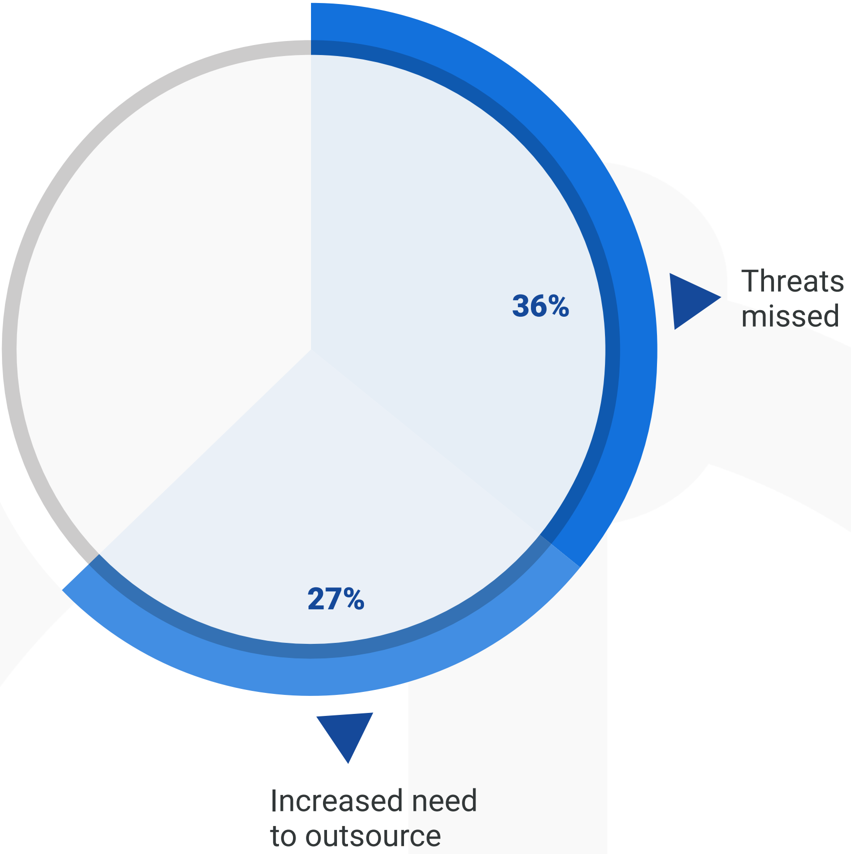
1

2

3

4 THREATS MISSED (36%) AND AN INCREASED NEED TO OUTSOURCE (27%) ARE THE MAIN CONSEQUENCES OF THE CYBERSECURITY SKILLS SHORTAGE

5



SUMMARY OF FINDINGS

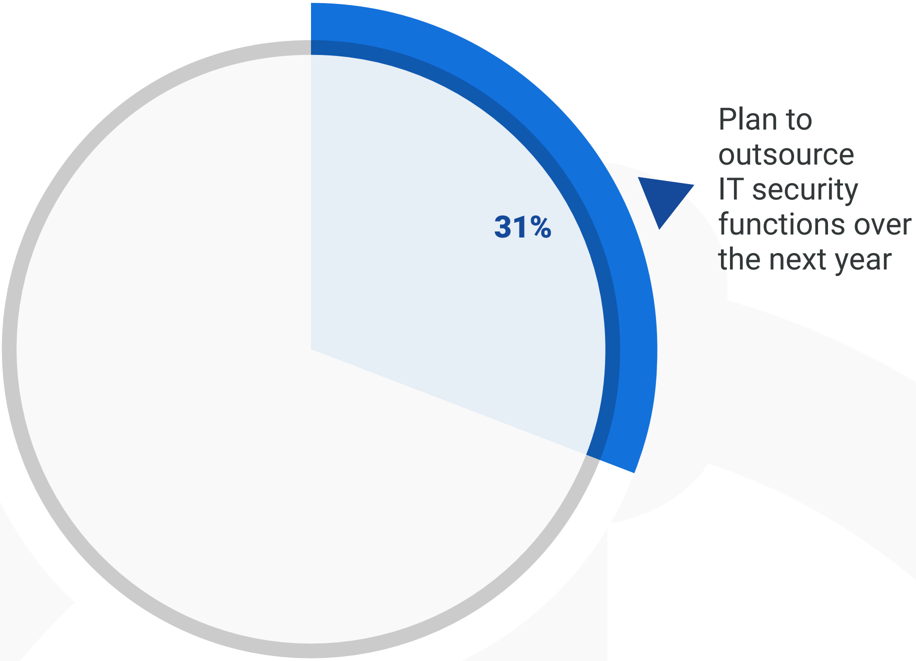
1

2

3

4

5 MAJORITY (31%) HAVE PLANS TO OUTSOURCE IT SECURITY FUNCTIONS OVER THE NEXT YEAR



CHAPTER 1
THE CHALLENGES AND THREAT LANDSCAPE

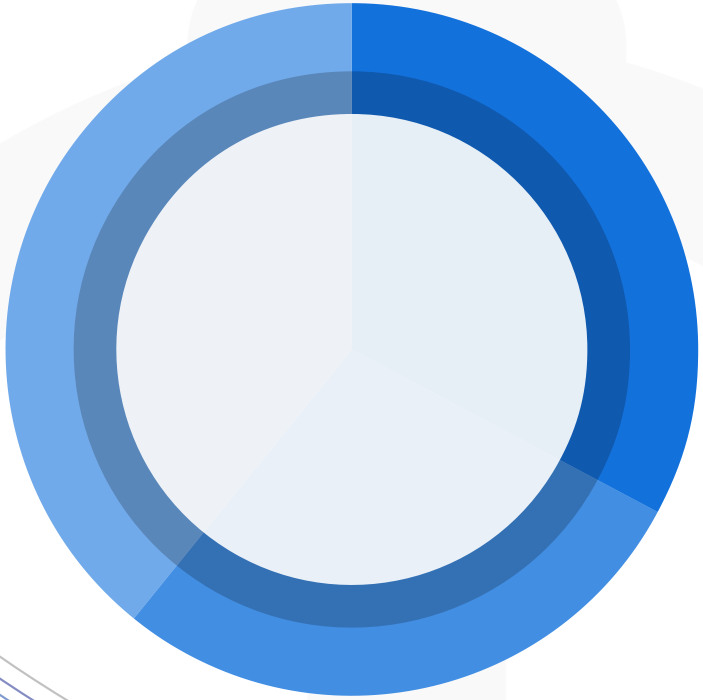
Strengthening cybersecurity has been a priority for many organisations for several years but an increase in cyberattacks alongside the adoption of a hybrid and remote work culture has triggered a need for change. With employees working from outside the safety confines of an organisation, attackers began to shift their focus leading to an increased awareness of cyberthreats. In this section, we explore the greatest security threats to organisations and whether they experience a shortage of cybersecurity skills.

SURVEY QUESTIONS

1

HOW HAS INCREASED AWARENESS OF CYBERTHREATS IMPACTED YOUR APPROACH TO CYBERSECURITY OVER THE LAST 12 MONTHS?

Cybersecurity has become a high priority for our organisation	33%
Cybersecurity is a medium priority for our organisation – we are aware of the importance but need to balance this against other business objectives	28%
Cybersecurity is a low priority for our organisation	39%



KEY TAKEAWAY

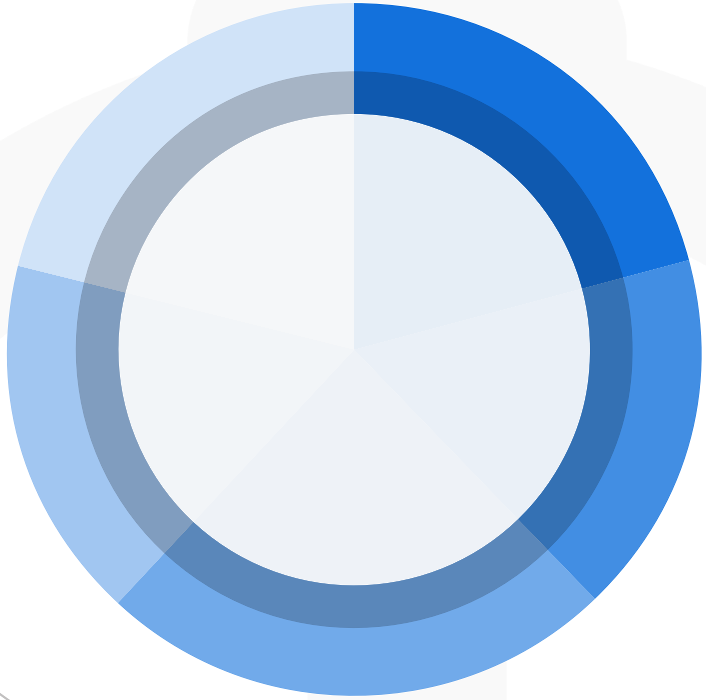
With the majority of respondents (61%) stating that cybersecurity has become a medium to a high priority for their organisation over the last 12 months, it is evident that increased awareness of cyberthreats is impacting their approach to cybersecurity. As organisations are keen to prioritise cybersecurity, there is a need for training employees and onboarding partners that can help navigate the process seamlessly.

SURVEY QUESTIONS

2

HOW HAVE YOU ADAPTED YOUR SECURITY STRATEGY IN LINE WITH INCREASED THREATS?

●	We are outsourcing more services	21%
●	We have recruited additional security staff	17%
●	We have made an investment in automation tools	24%
●	We have not changed anything	17%
●	We have made an investment in other technologies (please state)	21%



KEY TAKEAWAY

Most respondents have invested in automation tools (24%) and are focusing on outsourcing more services (21%). As organisations are keen to outsource security services and recruit additional security staff (17%), a need for establishing a more robust security culture is evident. As there isn't a one size fits all approach, external providers that can provide tailored security solutions across all touchpoints are becoming increasingly important.

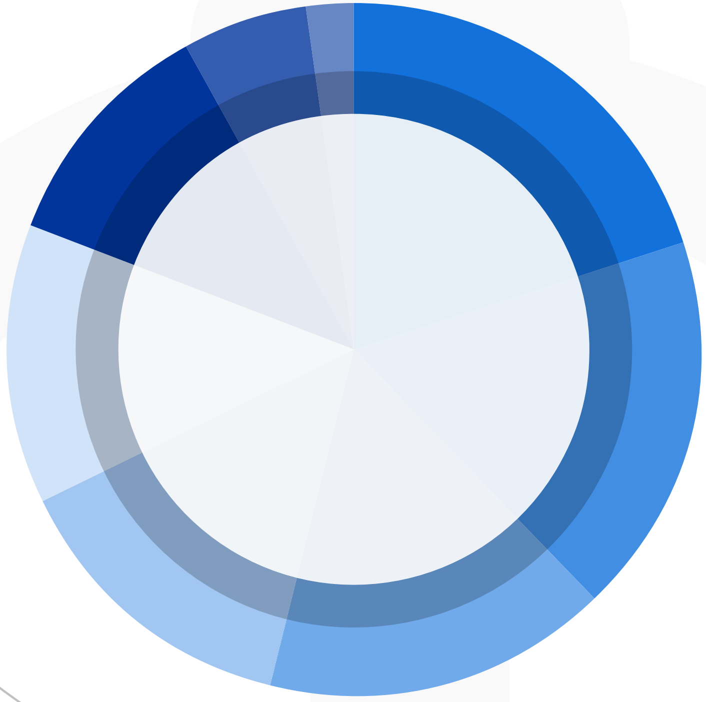
SURVEY QUESTIONS

3

PLEASE RANK THE FOLLOWING IN TERMS OF THE GREATEST SECURITY THREATS TO YOUR ORGANISATION?

RANK IN ORDER:
1– HIGHEST THREAT
8 – LOWEST

Nation state actors	20%	Supply chain attacks	13%
Mobile threats	18%	Ransomware	11%
Human error	16%	Email attacks	6%
Malware	14%	Other	2%



KEY TAKEAWAY

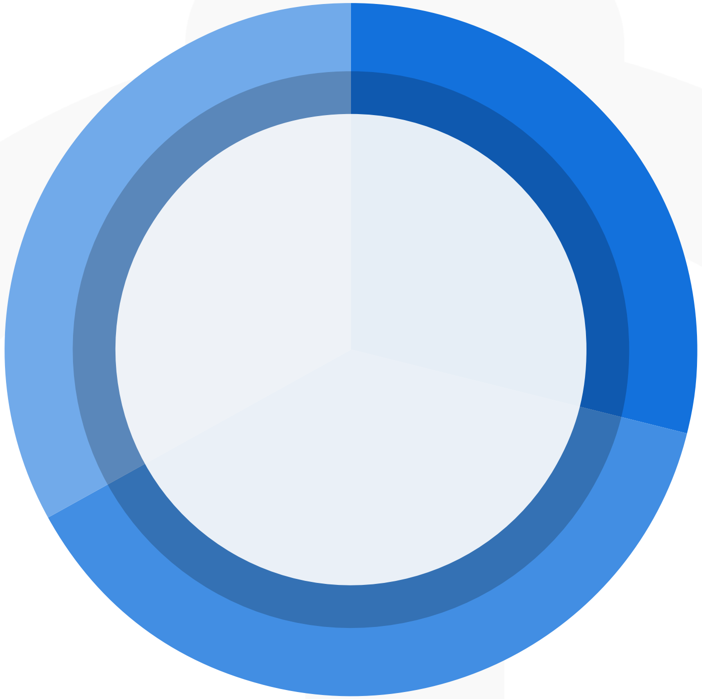
In terms of the greatest security threat, respondents cite nation-state actors (20%) and mobile threats (18%) as their biggest challenges. This is closely followed by human error (16%), highlighting the need to protect data and safeguard against threats across ever-increasing endpoints.

SURVEY QUESTIONS

4

DOES YOUR ORGANISATION EXPERIENCE A SHORTAGE OF CYBERSECURITY SKILLS?

Yes	29%
No	38%
I don't know	33%

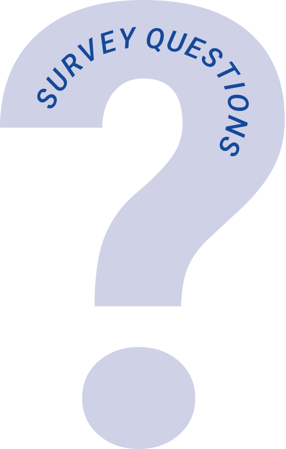


KEY TAKEAWAY

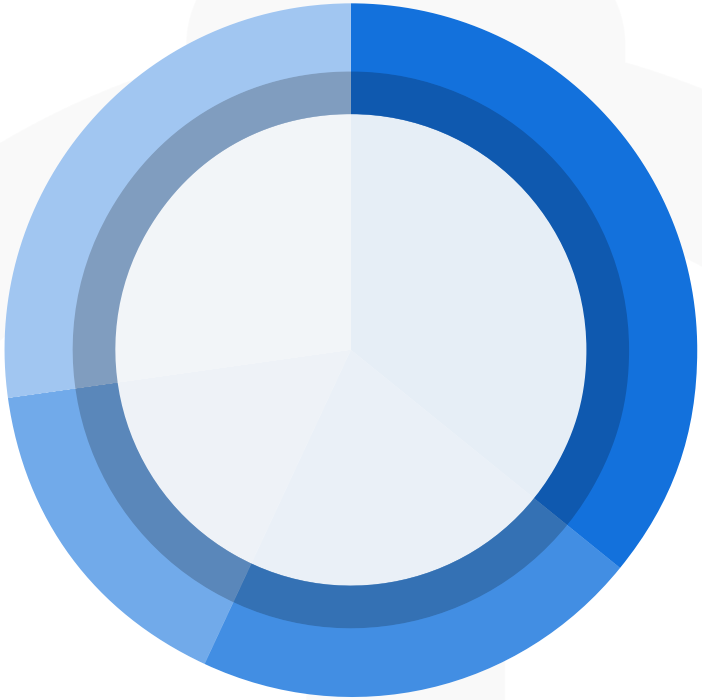
Majority of respondents (67%) either face a shortage of cybersecurity skills or aren't sure. This highlights a need for cybersecurity training to enhance employees' skills and make them less susceptible to falling victim to cyberattacks. Furthermore, organisations need to invest in filling this gap if they want to secure their connecting devices and people.

5

IF YES TO QUESTION 4, WHAT IS THE MAIN CONSEQUENCE OF THE CYBERSECURITY SKILLS SHORTAGE FOR YOUR ORGANISATION?



Threats missed	36%
More reactive approach to cybersecurity in general	21%
Impact on staff well-being	16%
Increased need to outsource	27%



KEY TAKEAWAY

Looking at the main consequence of the cybersecurity skills shortage for their organisations, threats missed (36%) rank the highest, followed by an increased need to outsource (27%). This shortage can lead to significant financial losses and organisations need to advance their capability to manage threats by investing in building a more robust security culture.

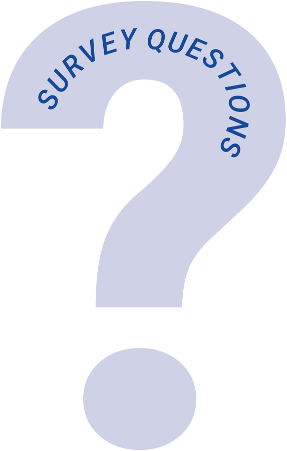
CHAPTER 2
PRIORITIES AND PLANNING AHEAD

Investment in training and outsourcing is critical, especially given the cyberskills shortage. In this section, we look at the top investment areas for organisations in the coming year and their plans for outsourcing an external provider.

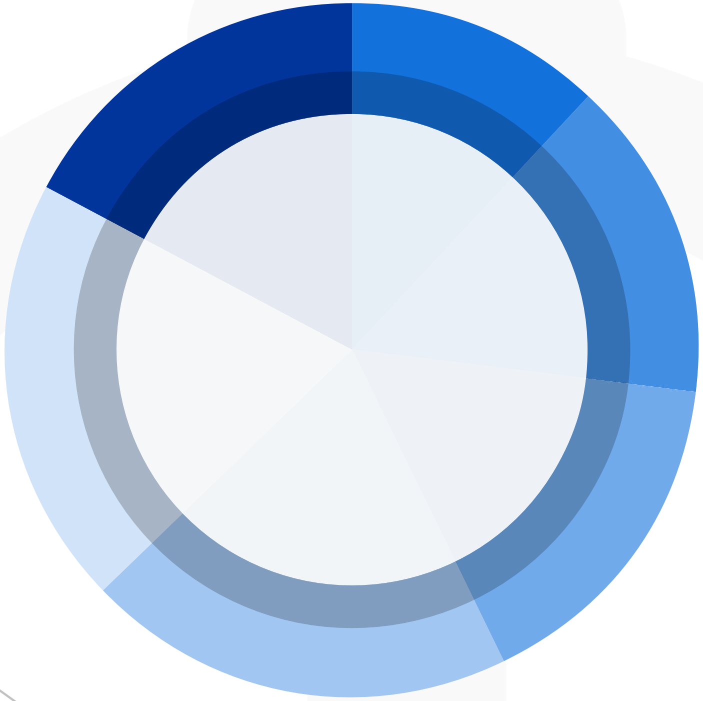
1

WHAT ARE YOUR TOP TWO INVESTMENT AREAS FOR THE YEAR AHEAD?

SELECT TOP TWO



Updating legacy tools	12%
Recruitment of cybersecurity staff	15%
Strengthening hybrid working security strategies	16%
Endpoint security	20%
Ransomware protection	20%
Outsourcing more cybersecurity functions	17%
Security training	0%



KEY TAKEAWAY

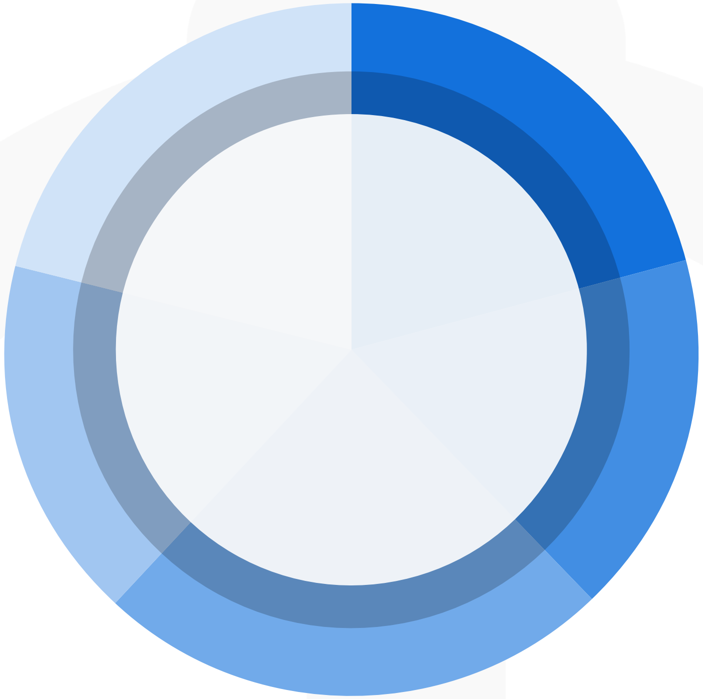
Endpoint security and ransomware protection are the following year's top two investment areas for organisations. With the increased adoption of remote and hybrid work culture, securing and managing the various touchpoints has become more challenging. As a result, organisations are realising the need for strengthening their cyber posture, especially as the data being shared across these endpoints is immense and a comprehensive approach is vital to protect as well as remediate cyber threats.

SURVEY QUESTIONS

2

HOW DO YOU EXPECT YOUR SECURITY BUDGET TO CHANGE OVER THE NEXT 12 MONTHS?

Increase by more than 50%	21%
Increase by less than 50%	15%
Stay the same	23%
Decrease by less than 50%	20%
Decrease by more than 50%	21%



KEY TAKEAWAY

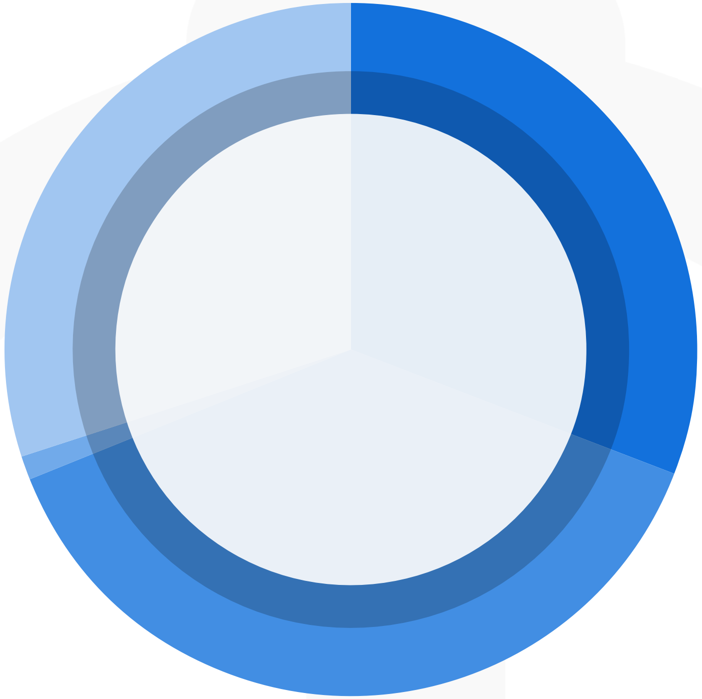
Looking at the next 12 months, 36% of respondents expect their security budgets to increase, directly contributing to protecting organisations from threats. However, 41% of respondents expect the security budgets to decrease, which can further exacerbate the cybersecurity skill shortage leading to an increase in missed threats, as stated earlier. This also indicates that organisations are looking for maximum support at less cost.

SURVEY QUESTIONS

3

DO YOU HAVE PLANS TO OUTSOURCE ANY IT SECURITY FUNCTIONS OVER THE NEXT 12 MONTHS?

Several	31%
Some	38%
None	1%
I don't know	30%



KEY TAKEAWAY

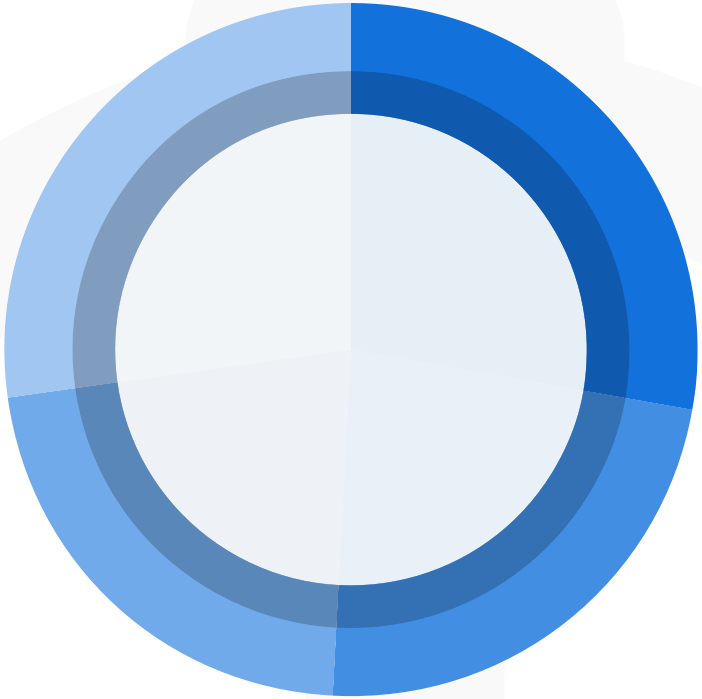
There is a growing need for organisations to have the necessary skills in-house when faced with the threat of cybersecurity. This is highlighted by 38% of the respondents citing that the ability to build the skills of internal security teams is imperative. It further highlights the importance of working with a trusted partner who can deliver tailored solutions, enabling the company to combat threats and establish a secure culture.

4

SURVEY QUESTIONS

WHAT DO YOU CONSIDER THE KEY DRIVER IN YOUR DECISION TO OUTSOURCE?

■	To combat security threats	28%
■	To fill a gap created by a shortage of cybersecurity skills	23%
■	More hands-on approach to establish a security culture	22%
■	More benefits derived from partner's expertise	27%



KEY TAKEAWAY

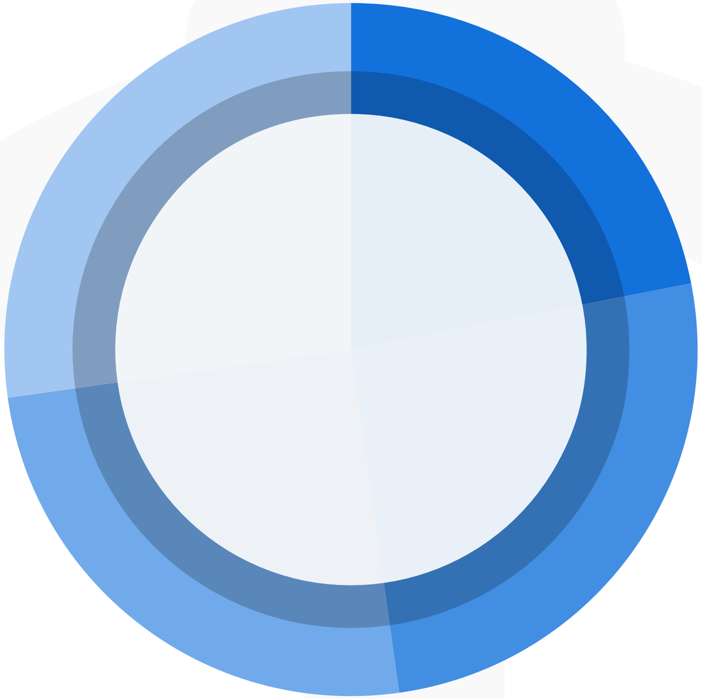
Combating security threats and deriving benefits from a partner's expertise are the top two key drivers for outsourcing. This highlights a strong need for a reliable partner to help mitigate risks across touchpoints while simultaneously keeping costs low.

SURVEY QUESTIONS

5

IN YOUR EVALUATION OF A PROFESSIONAL SERVICES PROVIDER, WHAT ARE THE TOP TWO BENEFITS YOU WOULD WISH TO SEE?

Quick detection and remediation	22%
Ease of collaboration with provider	26%
Low-touch data collection	25%
Ability to build the skills of internal security teams	27%



KEY TAKEAWAY

The ability to build the skills of internal security teams (27%) is considered the most important when evaluating a professional service provider. Organisations are keen to onboard a professional services provider but consider ease of collaboration (26%) vital. As the needs of organisations vary, a one-size-fits-all approach is not ideal. Hence, organisations must consider providers that can tailor their services to their particular needs and provide security and visibility across all touchpoints.

CONCLUSION

With a majority of respondents citing cybersecurity as a medium to a high priority for their organisations over the past year, there is no better time to invest in cybersecurity strategies that can secure numerous touchpoints and protect employees.

The consequences of a cybersecurity skills shortage can be harmful to the organisation and given how threats missed is the main consequence, investing in training is imperative. The common thing with most SMBs is that CISOs are unlikely to have equal resources and a high-security maturity level to match cyberattackers. From within, organisations should invest in employee training to ensure that companies have the appropriate skills to combat cyberthreats, know how to manage eventual risks and understand what levels of international and national support exist. Outside the organisation, would SMBs pay ransomware in the phase of an attack? Where would the bitcoin come from? Would paying be against the conventions of compliance with government policies around the market? Furthermore, as organisations are keen on outsourcing more services, it is an excellent opportunity for providers to offer a comprehensive approach to endpoint security. However, as a higher percentage of respondents expect the security budgets to decrease rather than increase, providers need to provide a comfortable price point that enables organisations to derive maximum benefits.

Another area of concern was ensuring that companies have the appropriate skills to combat cyberthreats. The findings highlight that spending on endpoint security and ransomware protection are top areas for investment for companies. By taking a long-term approach and securing a trusted partner to help obtain crucial in-house management services and provide robust threat intelligence, organisations can put themselves on the path to improved cyber-resilience and ensure a secure ethos is in place.

> “**Another area of concern was ensuring that companies have the appropriate skills to combat cyberthreats.**”

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.

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

Find out more:
www.cxopriorities.com

In conjunction with

Contact:
adabaker@blackberry.com
Webinar:
https://www.blackberry.com/us/en

Find out more:
www.blackberry.com