

UNDERSTANDING THE SECURITY CHALLENGES OF MIDDLE EAST, TURKEY AND AFRICA ENTERPRISES IN THE AGE OF HYBRID WORKING



CONTENTS

INTRODUCTION

3

SUMMARY OF
FINDINGS

4

1

THE CHALLENGES AND
THREAT LANDSCAPE

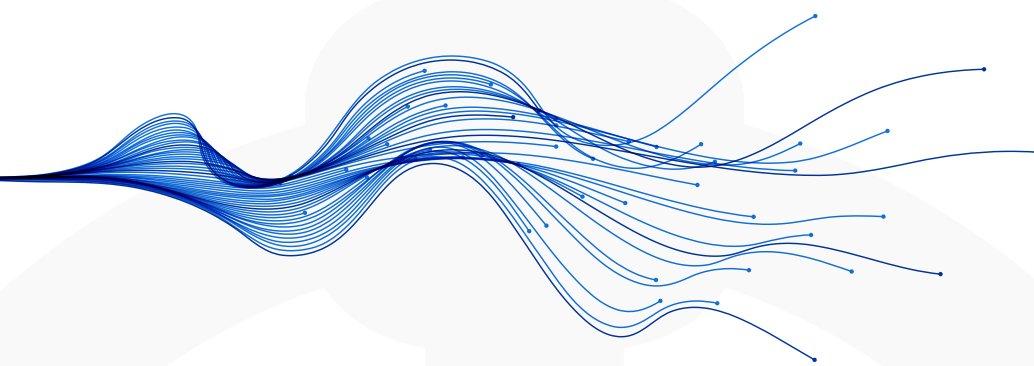
9

2
PRIORITIES AND
PLANNING AHEAD

16

CONCLUSION

23



INTRODUCTION

Since the COVID-19 pandemic, organisations worldwide have shifted from the office to the home – with most using personal devices for work – the chances of falling prey to cyberattacks have increased multifold, either through connecting to unsecured WiFi networks, lost or stolen devices or prying eyes. Personal data on employee-owned devices are routinely exposed on corporate networks and these critical vulnerabilities can easily be exploited by threat groups.

The effect is a growing number of organisations are building on weak security that is open to risks like data theft, malware, legal problems, lost or stolen devices, improper mobile management, insufficient employee training and Shadow IT.

With critical data being shared across multiple touchpoints, securing and managing connected devices and protecting employees has never been more crucial. Whether organisations are taking a hybrid or fully cloud-based approach, protecting data storage and building cloud security and other business-critical elements now requires comprehensive planning.

Through the survey, we aimed to discover:

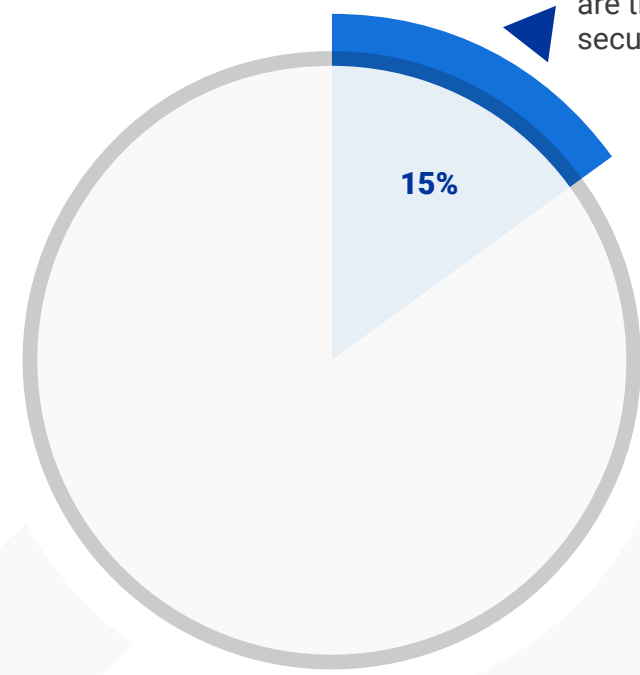
-  The greatest security challenges faced by organisations in the Middle East, Turkey and Africa Region (META)
-  The level of security preparedness when it comes to device management strategy, preventing accidental data loss and vulnerability to risks like data theft, malware, legal problems, lost or stolen devices, improper mobile management, insufficient employee training and Shadow IT
-  Organisations' priorities and proactive cybersecurity measures including actions like investment in cybersecurity technology, identifying and patching vulnerabilities, preventing data and security breaches and regularly evaluating the strength of their security posture



SUMMARY OF FINDINGS

1

IN TERMS OF THE GREATEST SECURITY THREAT, RESPONDENTS CITE MOBILE THREATS (15%) AS THEIR BIGGEST CHALLENGES. THIS IS CLOSELY FOLLOWED BY NATION STATE ACTORS, HUMAN ERROR AND EMAIL ATTACKS (14%)

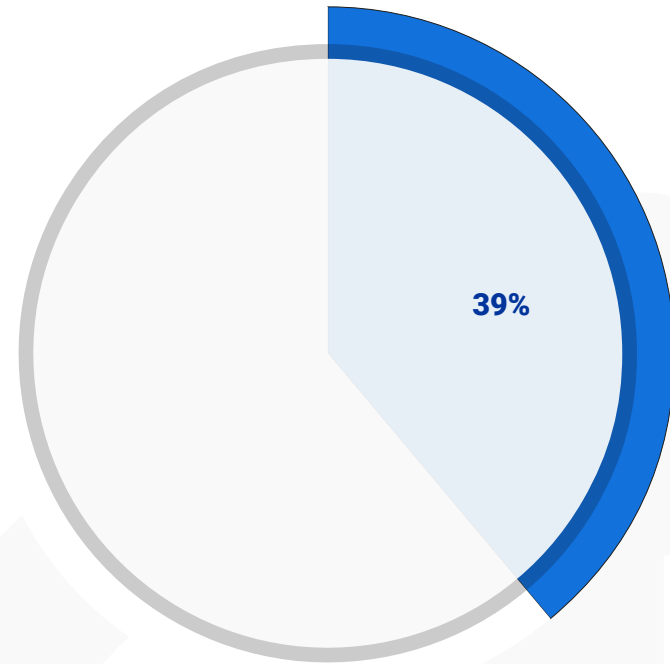


Mobile threats are the greatest security threats

SUMMARY OF FINDINGS

2

THIRTY-NINE PERCENT OF THE PEOPLE WHO USE PERSONAL DEVICES AT WORK BELIEVE THAT THEIR EXISTING DEVICE MANAGEMENT STRATEGY IS NOT SECURE ENOUGH TO PREVENT ACCIDENTAL DATA LOSS

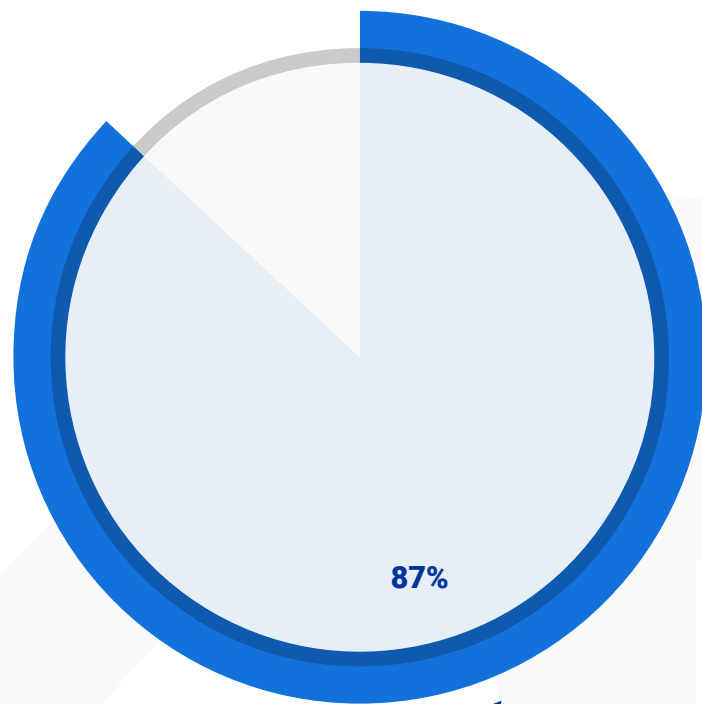


Existing device management strategy is not secure enough to prevent accidental data loss on personal devices at work

SUMMARY OF FINDINGS

3

SIXTY-EIGHT PERCENT OF RESPONDENTS ATTEST THEIR ORGANISATIONS ARE AT RISK TO SHADOW IT WHILE 32% BELIEVE THEY ARE AT A LOWER RISK

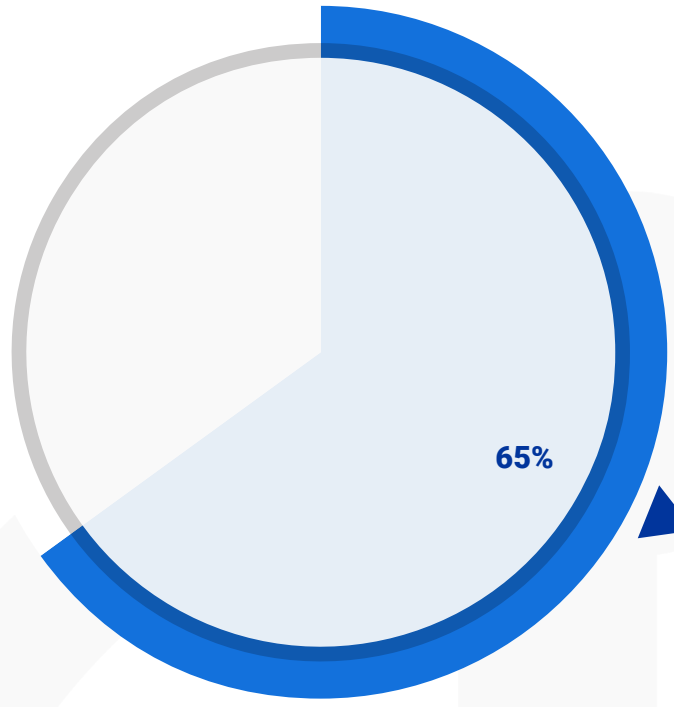


Organisations are at risk to Shadow IT



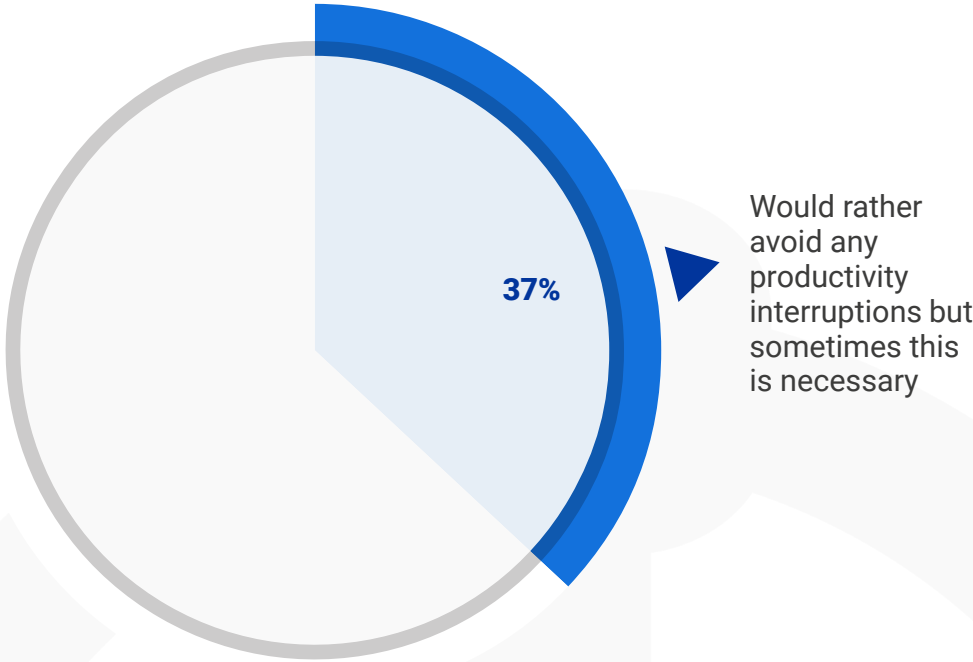
SUMMARY OF FINDINGS

4 MAJORITY OF RESPONDENTS ARE AMPLIFYING THEIR SECURITY BUDGETS FOR THE NEXT YEAR, WITH OVER HALF (65%) INCREASING THEIR BUDGETS TO TACKLE SECURITY THREATS



Increasing their budgets for next year to tackle security threats

SUMMARY OF FINDINGS



5 THE MAJORITY OF RESPONDENTS PREFER THEIR SECURITY TOOLS TO BE BOTH EASY TO USE AS WELL AS EFFECTIVE, WITH 37% STATING THEY 'WOULD RATHER AVOID ANY PRODUCTIVITY INTERRUPTIONS BUT SOMETIMES THIS IS NECESSARY'

 BlackBerry™ priorities A
Lyncph
Media
BRAND

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 office, attackers began to shift their focus, resulting in organisations having an increased awareness of cyberthreats. In this section, we explore the greatest security threats to organisations and whether they have adequate security measures in place to cover increasing entry points.

1

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



 Nation state actors	14%	 Supply chain attacks	13%
 Mobile threats	15%	 Ransomware	13%
 Human Error	14%	 Email attacks	14%
 Malware	14%	 Other	3%

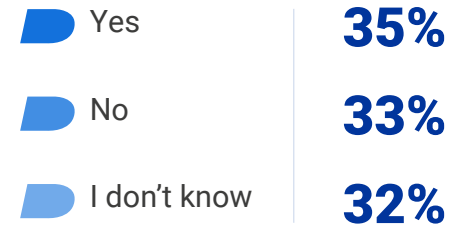


KEY TAKEAWAY

In terms of the greatest security threat, respondents cite mobile threats (15%) as their biggest challenges. This is closely followed by nation state actors, human error and email attacks (14%), highlighting the need to protect data and safeguard against threats across ever-increasing endpoints.

2

DOES YOUR ORGANISATION ALLOW THE USE OF PERSONAL DEVICES FOR WORK PURPOSES? IF YES, SEE QUESTION 3.

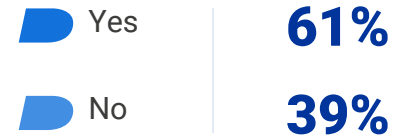


KEY TAKEAWAY

Thirty-five percent of respondents say their organisation allows the use of personal devices for work. This implies high risks to security threats due to the use of public Wi-Fi networks, poor cyber-hygiene and no protective firewalls. Not only are employees at risk of cyberthreats but their devices lack regulation. The fact that 32% don't know is concerning and a critical vulnerability that can be exploited by threat groups.

3

IF YES TO QUESTION 2, DO YOU BELIEVE THAT YOUR EXISTING DEVICE MANAGEMENT STRATEGY IS SECURE ENOUGH TO PREVENT ACCIDENTAL DATA LOSS?






KEY TAKEAWAY

Thirty-nine of the respondents who allow the use of personal devices at work believe that their existing device management strategy is not secure enough to prevent accidental data loss. This highlights how vulnerable they are to risks like data theft, malware, legal problems, lost or stolen devices, improper mobile management, insufficient employee training and Shadow IT.

4

**WHAT LEVEL OF THREAT
DO YOU BELIEVE SHADOW
IT PRESENTS TO YOUR
ORGANISATION?**



 High	28%
 Medium	40%
 Low	32%

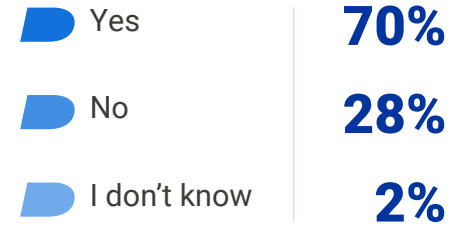


KEY TAKEAWAY

Sixty-eight percent of respondents attest their organisations are at risk of Shadow IT. This puts most organisations at risk of losing control and visibility, which could lead to data leaks, security issues, regulatory noncompliance and the impossibility of recovering information that might be lost in Shadow IT systems.

5

WITH THE INCREASING CULTURE OF REMOTE WORKING, DO YOU BELIEVE THE RISK OF LOSING DATA IS HIGHER?






KEY TAKEAWAY

In terms of the risk of losing data with remote working, the majority of respondents believe remote working puts them at higher risk (70%), highlighting the need to protect data and safeguard against threats across ever-increasing endpoints.

6



**DOES YOUR ORGANISATION
HAVE ADEQUATE SECURITY IN
PLACE TO COVER INCREASING
ENTRY/TOUCHPOINTS?**

	Yes	15%
	No	64%
	I don't know	21%



KEY TAKEAWAY

Over half of respondents (85%) indicated they are either not aware, or their organisation does not have, adequate security in place to cover increasing entry/ touchpoints. This shows the need for organisations to take data security seriously at every touchpoint and position themselves as one that's deserving of customers' trust.

CHAPTER 2 PRIORITIES AND PLANNING AHEAD

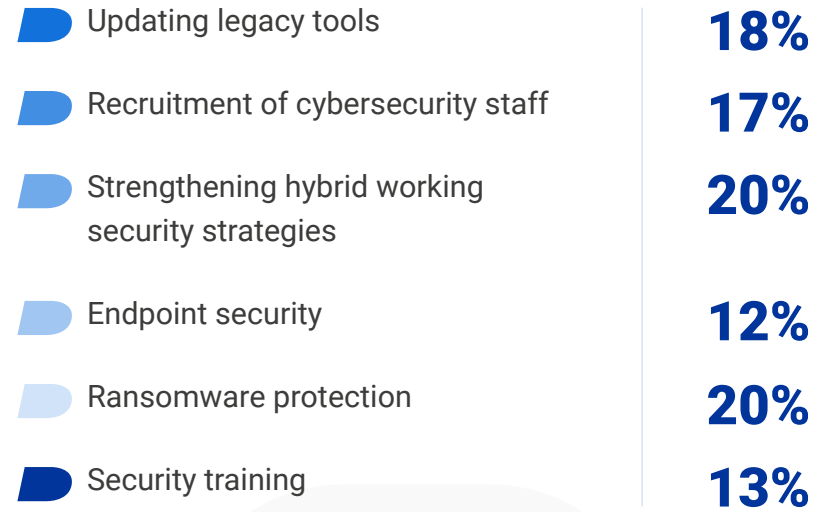


Investment in a hybrid business structure is critical, especially given the popular rise in remote working. In this section, we look at the top investment areas for organisations in the coming year and their plans for outsourcing an external provider.



7

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

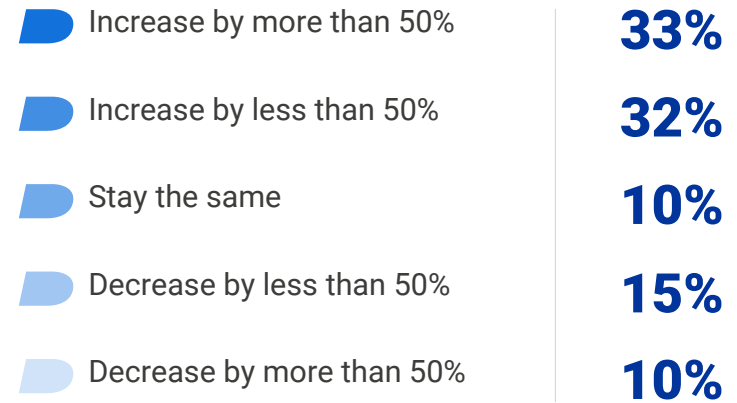


KEY TAKEAWAY

The top two priorities of investment areas for the next 12 months are strengthening hybrid working security strategies (20%) and ransomware protection (20%). With 40% of respondents selecting these priorities, it is suggested they have had previous concerns or potential issues with ransomware and that they are also leaning towards a hybrid business structure for the next year.

8

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








KEY TAKEAWAY

Majority of respondents are amplifying their security budgets for the next year, with over half (65%) increasing their budgets to tackle security threats. However, 25% of respondents are decreasing their current security budgets. This could be because the company believe a 'reactive' rather than 'proactive' approach may be more effective, or perhaps an overall annual budget is unable to stretch to their current providers.

9

WHAT ARE THE MAIN CONSEQUENCES OF THE CYBERSECURITY SKILLS SHORTAGE FOR YOUR ORGANISATION?



-  Threats Missed **17%**
-  More reactive approach to cybersecurity in general **21%**
-  Impact on staff wellbeing **14%**
-  Increased need to outsource **27%**
-  We do not have a skills shortage **21%**






KEY TAKEAWAY

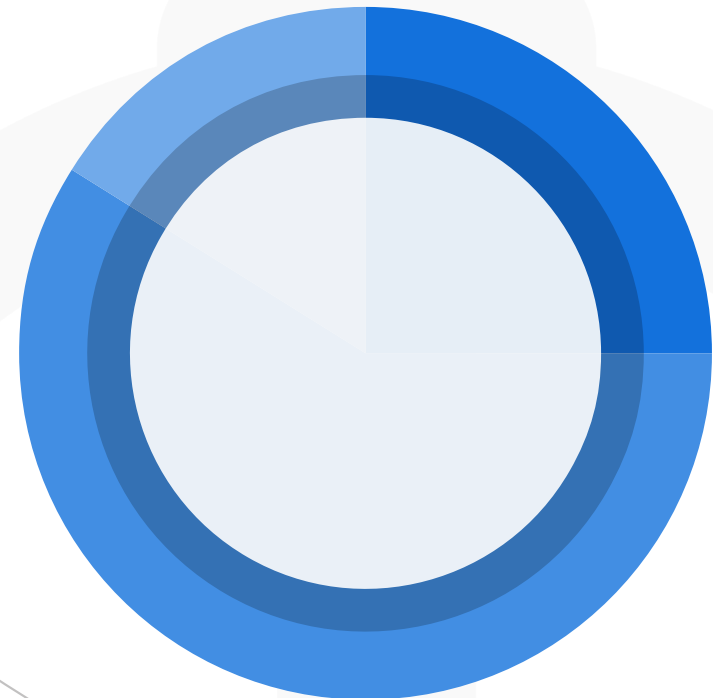
The main consequence of respondents' cybersecurity skills shortage within their organisation is the increased need to outsource (27%), suggesting their main concern is financial.

10

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



	Several	25%
	Some	59%
	None	16%



KEY TAKEAWAY

A large majority of respondents (84%) intend to outsource their IT security functions over the coming year. This suggests respondents value cybersecurity vendors' expertise, and this may also correlate with the majority (65%) of respondents increasing their budgets to tackle security threats (See chapter 2, Question 8).

11

HOW FAR DOES REACTIVE TROUBLESHOOTING IMPACT PROACTIVE CYBERSECURITY PROJECTS FOR YOUR ORGANISATION?



Frequently	23%
Occasionally	23%
Sometimes	26%
Rarely	28%






KEY TAKEAWAY

Troubleshooting appears to have an impact on the respondent's organisation's proactive cybersecurity projects, with 72% of respondents stating troubleshooting impacts them frequently or at least sometimes.

12

HOW FAR DOES THE PRESERVATION OF PRODUCTIVITY IMPACT YOUR DECISION-MAKING WHEN IT COMES TO INVESTING IN CYBERSECURITY TECHNOLOGY?



-  High – any security tool investment must be frictionless for employees **18%**
-  Medium – we would rather avoid any productivity interruptions but sometimes this is necessary **20%**
-  Low – the effectiveness of a cybersecurity tool is the priority **12%**



KEY TAKEAWAY

There does not seem to be any tipping of the scales when it comes to the preservation of productivity when choosing a cybersecurity technology. Although the majority of respondents want the best of both worlds, with 37% stating they ‘would rather avoid any productivity interruptions but sometimes this is necessary’, when it comes to the tool working effectively. It appears overall, each respondent’s priorities of the tools’ impact on employee productivity are generally divided.

CONCLUSION

Another area of concern was ensuring that companies in the META region are appropriately set up to fend off threats from Shadow IT.

With most respondents citing that their enterprise does not have adequate security to cover increasing entry points, there is no better time than now to invest in cybersecurity strategies that can secure numerous touchpoints and protect employees. This is compounded by the fact that most respondents are amplifying their cybersecurity budgets for the next year, with over half (65%) increasing their budgets. Furthermore, as organisations are keen on increasing their budgets, it is an excellent opportunity for providers to offer a comprehensive approach to endpoint security in this region.

Another area of concern was ensuring that companies in the META region are appropriately set up to fend off threats from Shadow IT. With 68% of respondents attesting their organisations are at threat to Shadow IT, this puts most organisations at risk of losing control and visibility. A strong case exists here for a provider who can add value by preventing data

leaks that have been compromised as part of a device management strategy.

The top two priorities of investment areas for the next 12 months are strengthening hybrid working security strategies (20%) and ransomware protection (20%). Almost half (40%) of respondents selecting these priorities indicate that organisations currently face potential issues with ransomware. This also grants an opportunity for META providers to build a robust strategy around more hybrid business structures for the future.

When it comes to the management of devices and mobile security it is important to remember that while it is a long-term technical challenge for enterprises, it is also cultural. By taking a long-term approach and securing a trusted partner that is ready to invest in mobile threats and personal data, organisations can future-proof their hybrid working environments.



In conjunction with



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

Find out more:
www.blackberry.com

