A Lynchpin Media BRAND

cxo priorities

Understanding how UK SMBs navigate cybersecurity challenges and optimise performance

a **CXO Priorities** report in partnership with Intel

intel vPRO

intel vPRO

CXO priorities

A Lynchpin Media BRAND

CONTENTS

INTRODUCTION

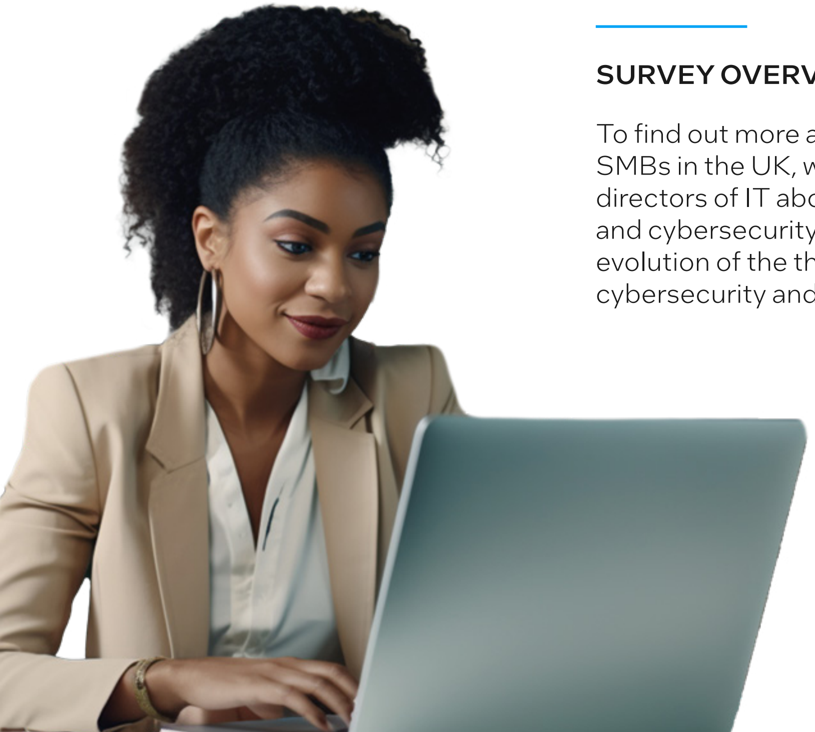
In contemporary business operations, small and medium-sized enterprises (SMBs) in the United Kingdom find themselves at the crossroads of navigating intricate cybersecurity challenges while striving to enhance overall performance.

From managing the ever-evolving nature of cyberthreats to safeguarding sensitive data, ensuring compliance with regulatory frameworks, addressing the skills gap in cybersecurity expertise and the increase of remote work which amplifies vulnerabilities, businesses now require robust measures to secure their digital assets.

The repercussions of cybersecurity challenges on these SMBs not only result in impeding operational efficiency but extend to disrupt Business Continuity, financial losses, diversion of resources away from core activities impacting productivity and the overall erosion of customer trust due to security breaches that tarnish a company's reputation. Balancing the demands of cybersecurity with optimal performance becomes imperative as organisations grapple with the multifaceted downsides of these challenges.

SURVEY OVERVIEW:

To find out more about the current cybersecurity and IT challenges facing SMBs in the UK, we surveyed IT directors, IT managers and VP/executive directors of IT about their experiences and plans regarding remote working and cybersecurity. This report aims to present an overview of the current evolution of the threat landscape, explore the complexities of managing cybersecurity and reveal how organisations plan to prioritise and invest.



THROUGH THIS SURVEY WE AIMED TO DISCOVER:

- The challenges organisations encounter in IT management
- The role and impact of cybersecurity management
- Priorities and planning

SUMMARY OF FINDINGS

To find out more about the current cybersecurity and IT challenges facing SMBs in the UK, we surveyed IT directors, IT managers and VP/executive directors of IT about their experiences and plans regarding remote working and cybersecurity. This report aims to present an overview of the current evolution of the threat landscape, explore the complexities of managing cybersecurity and reveal how organisations plan to prioritise and invest.

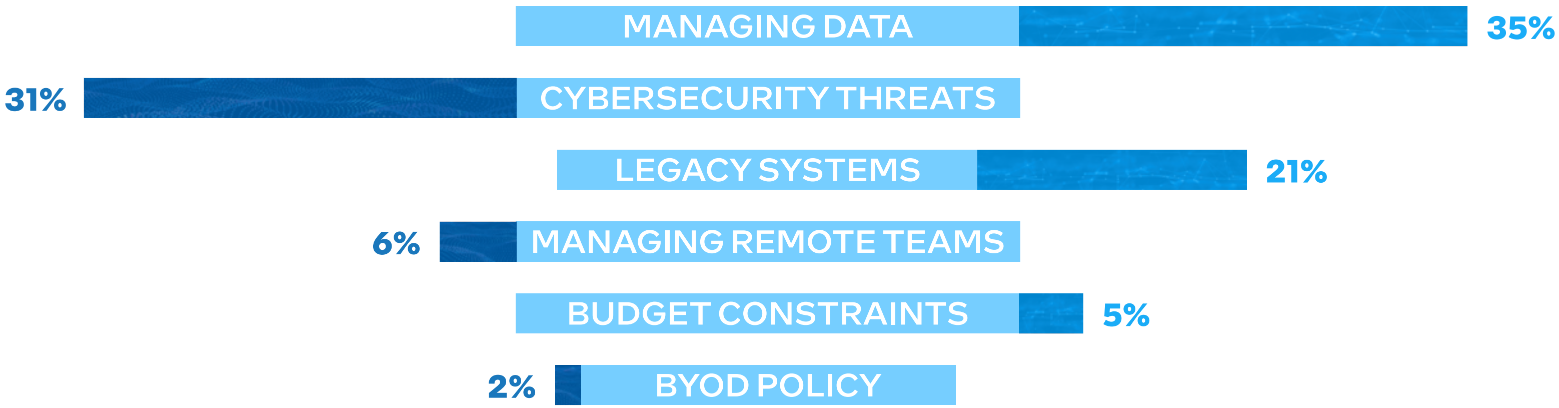
- Cybersecurity threats (31%) and managing data (35%) are the top two IT management challenges organisations face.
- Financial loss (34%) and customer dissatisfaction (25%) are identified as the biggest impacts of downtime on organisations.
- Phishing attacks (37%) and ransomware attacks (20%) are the foremost cyberthreats organisations face.
- One fifth of participants highlighted the significance of incorporating AI capabilities (20%) during an IT refresh. Improved data analysis (telemetry) (19%) and Improved PC performance (14%) were also highlighted.
- A majority of respondents acknowledged either a significant (46%) or moderate (44%) level of cybersecurity challenges faced by their organisation which highlights a wide awareness of the threats presented.
- Almost half of respondents (44%) stated significant reliance on multilevel security measures when protecting against software level attacks. Nearly one third of respondents (32%) cited using standard solutions, suggesting adherence to established security practices.
- Forty-one percent of respondents identified the increasing sophistication of cyberthreats as the most significant challenge, reflecting the evolving nature of security risks.
- More than half of respondents (54%) express a high level of confidence ('Very confident') that their organisation is protected against common types of attacks.
- Eighty-two percent of respondents indicated that they are currently using remote management capabilities.
- All respondents affirmed their capacity to remotely remediate and recover infected devices, showcasing a robust incident response capability.
- All those capable of remote remediation confirm the out-of-band nature of these operations, indicating an additional layer of security and resilience.

PART 1

IT MANAGEMENT CHALLENGES FACED BY ORGANISATIONS

Every day, SMBs grapple with a myriad of challenges in the realm of IT management and their increasing reliance on technology as a linchpin for their operations makes it paramount to understand and mitigate these challenges. In this section, we explore the IT management challenges organisations face, their impacts on downtime and business priorities during an IT refresh.

WHAT WOULD YOU CONSIDER THE TOP TWO IT MANAGEMENT CHALLENGES FOR YOUR ORGANISATION?



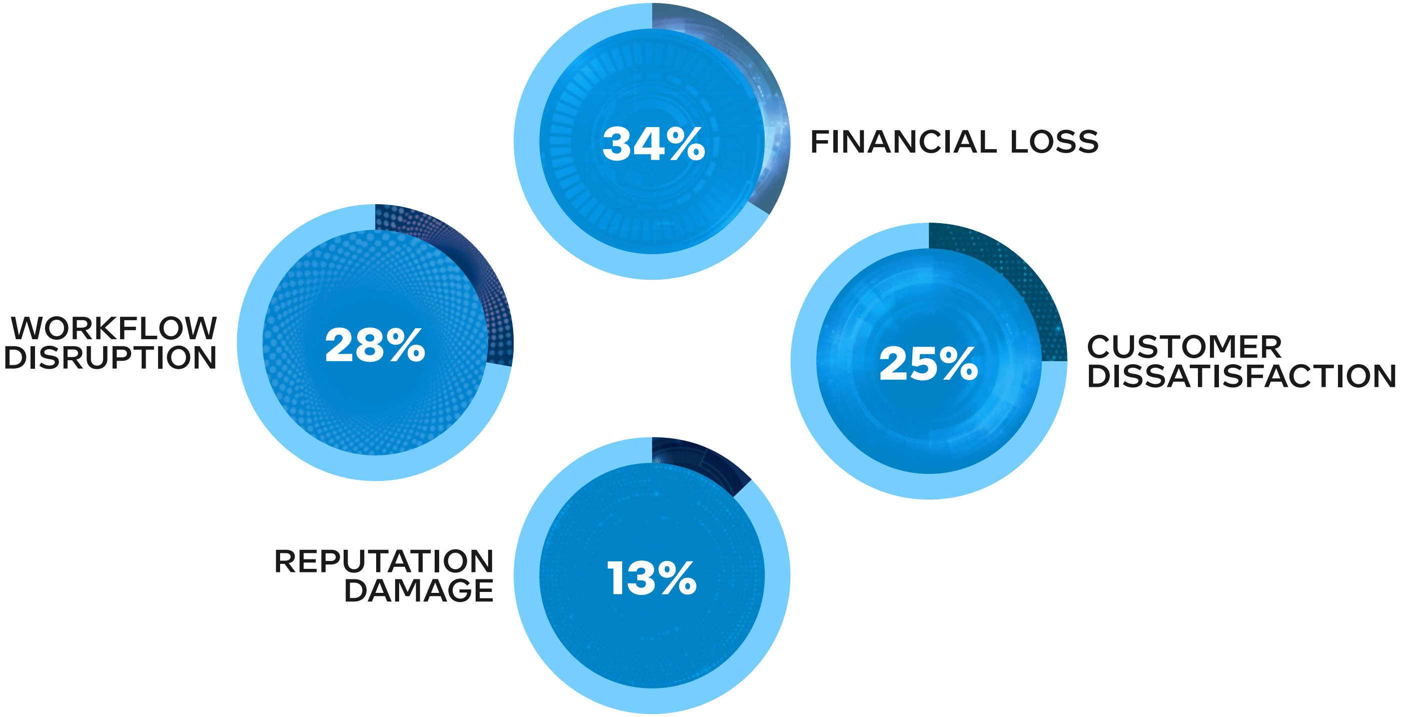
KEY INSIGHTS

Cybersecurity threats (**31%**) and managing data (**35%**) are the top two IT management challenges organisations face. Legacy systems also pose a significant challenge accounting for **21%** of responses. Budget constraints and the management of remote teams follow, with **5%** and **6%** of respondents citing these as notable challenges. This suggests a critical need for robust cybersecurity measures and effective data management strategies to address the foremost IT challenges faced by organisations in the UK.

PART 1

IT MANAGEMENT CHALLENGES FACED BY ORGANISATIONS

WHAT IS THE BIGGEST IMPACT OF DOWNTIME FOR YOUR ORGANISATION?



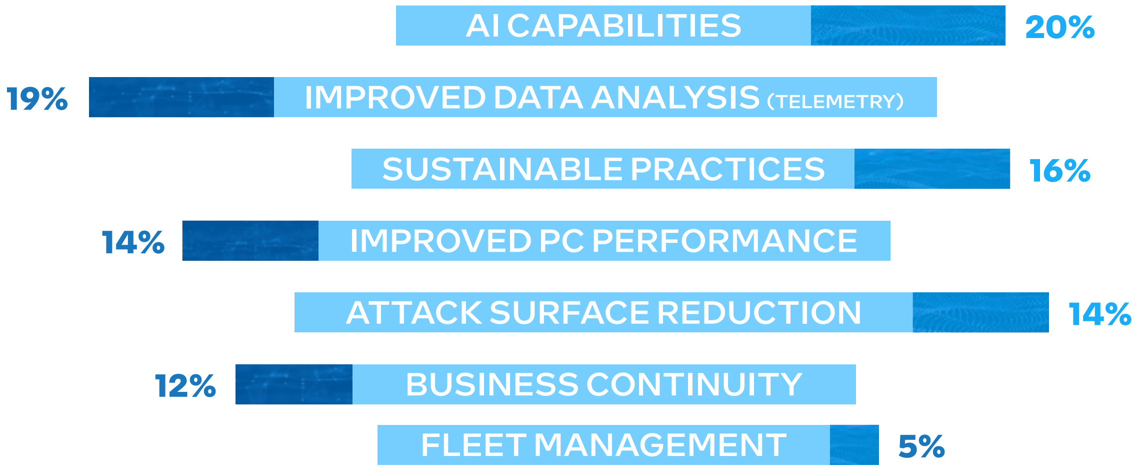
KEY INSIGHTS

Financial loss (**34%**) is identified as the biggest impact of downtime closely followed by customer dissatisfaction (**25%**). Workflow disruption accounts for **28%** while reputational damage accounts for **13%**. The overall summary brings to light the multifaceted nature of downtime's impact on organisations. It echoes the significance of maintaining seamless operations for client satisfaction and suggests that downtime has an overall negative impact on the credibility of every organisation.

PART 1

IT MANAGEMENT CHALLENGES FACED BY ORGANISATIONS

WHAT EFFICIENCIES WOULD YOU PRIORITISE DURING AN IT REFRESH? SELECT TOP TWO



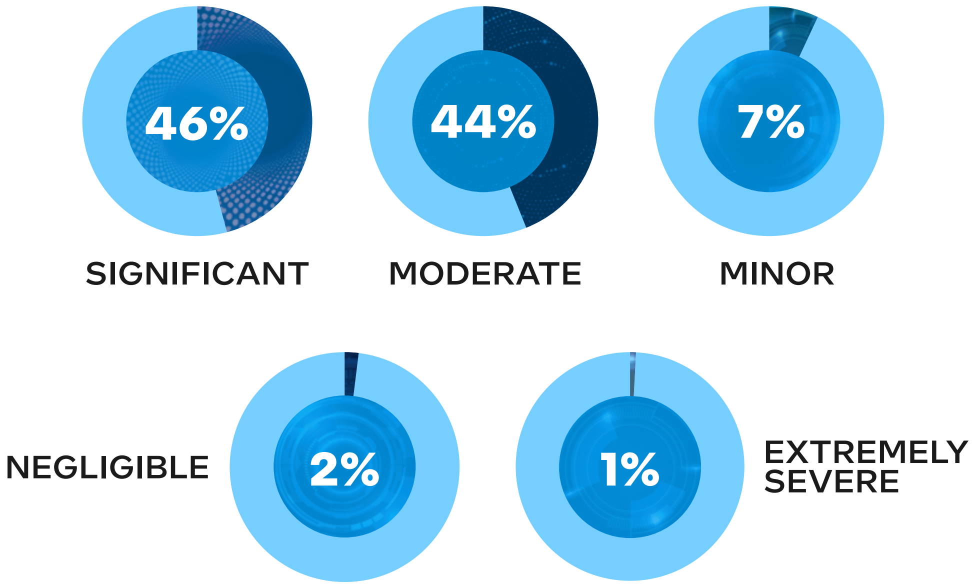
KEY INSIGHTS

One fifth of participants highlighted the significance of incorporating AI capabilities (**20%**) during an IT refresh. This is closely followed by **19%** who expressed a keen interest in improving data analysis through telemetry. Sustainable practices garnered **16%** of responses, indicating a growing concern for environmentally conscious solutions. This underscores the paramount importance placed on technological advancements such as AI, data analysis and sustainability in shaping the IT landscape. Their importance also indicates a readiness to invest in boosting these areas within an organisation.

PART 1

IT MANAGEMENT CHALLENGES FACED BY ORGANISATIONS

HOW WOULD YOU RATE THE CURRENT LEVEL OF CYBERSECURITY CHALLENGES FACED BY YOUR ORGANISATION?



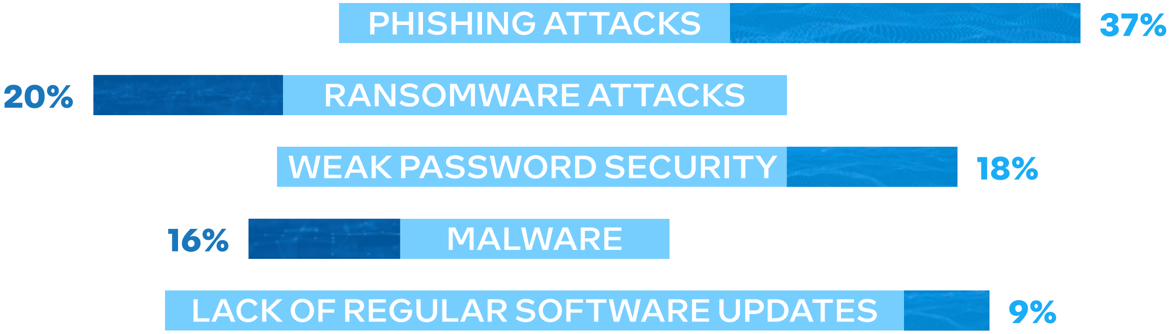
KEY INSIGHTS

A majority of respondents acknowledged either a significant (**46%**) or moderate (**44%**) level of cybersecurity challenges faced by their organisation which highlights a wide awareness of the threats presented. However, **1%** rated these challenges as extremely severe, while **7%** viewed them as minor and **2%** regarded them as negligible. The overall data underscores the diverse perceptions of cybersecurity challenges, emphasising the need for tailored strategies to address the varying degrees of concern within organisations.

PART 1

IT MANAGEMENT CHALLENGES FACED BY ORGANISATIONS

WHICH CYBERTHREATS ARE MOST PREVALENT FOR YOUR ORGANISATION? PLEASE SELECT TOP TWO



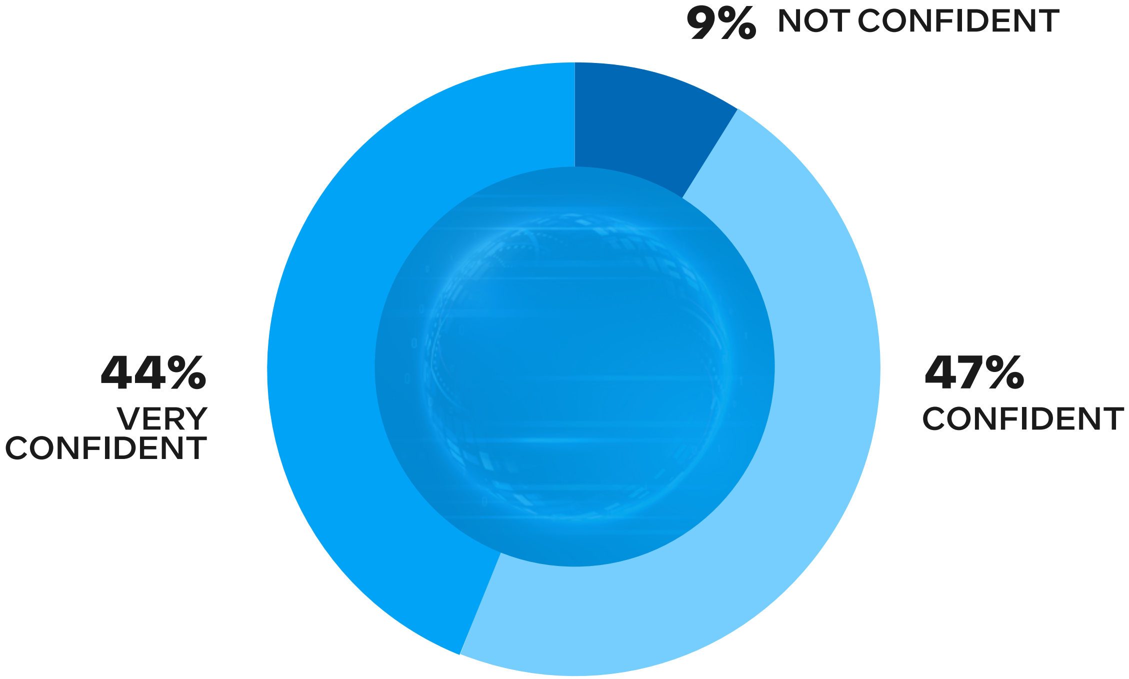
KEY INSIGHTS

Phishing attacks (**37**%) and ransomware attacks (**20%**) emerge as the foremost cyberthreats for organisations. Malware and weak password security also register as prominent issues with **16%** and **18%** respectively. This suggests a critical need for heightened cybersecurity awareness and proactive measures, particularly in addressing phishing vulnerabilities and bolstering password security.

PART 1

IT MANAGEMENT CHALLENGES FACED BY ORGANISATIONS

HOW CONFIDENT ARE YOU IN YOUR ORGANISATION'S ABILITY TO REDUCE THE ATTACK SURFACE?



KEY INSIGHTS

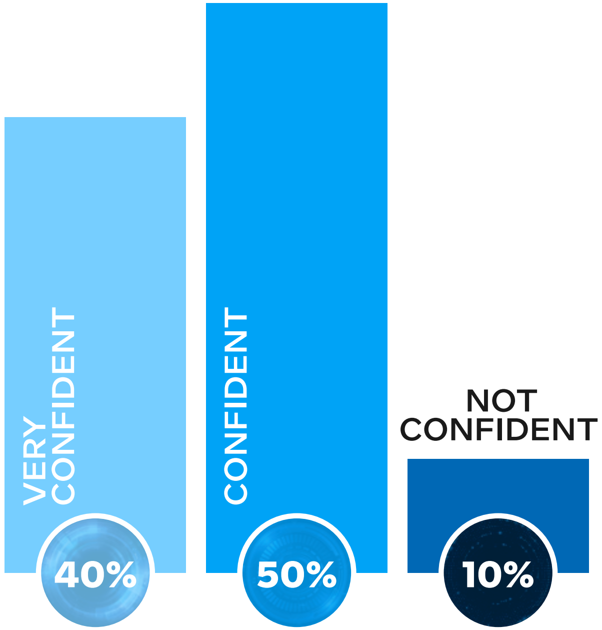
A noteworthy **44%** expressed being 'very confident' of their capacity to diminish the attack surface while a substantial **47%** conveyed a 'confident' outlook. Conversely, a modest **9%** admitted to lacking confidence while no respondents chose the option 'I don't know'. These findings suggest a generally positive sentiment with a strong majority expressing confidence in their organisation's capabilities to reduce the attack surface. It also bodes well for the overall cybersecurity posture signifying a high level of awareness of attacks which is assumed to influence annual cybersecurity budget allocations.

PART 2

PRIORITIES AND PLANNING AHEAD

In this section, we look at the top considerations for organisations in the coming year and what their key priorities will be.

HOW CONFIDENT ARE YOU IN YOUR ORGANISATION'S ABILITY PROTECT AGAINST FIRMWARE-LEVEL ATTACKS?



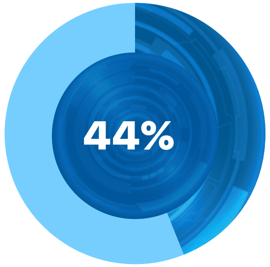
KEY INSIGHTS

Ninety percent of respondents chose 'Confident' or 'Very confident' when asked about their organisation's ability to protect against firmware-level attacks. This suggests a strong security stance and recognition of the importance of firmware protection. However, it must not be overlooked that a small minority of those surveyed (**10%**) were 'Not confident' in their organisation's ability to protect against firmware-level attacks. While the overall confidence is reassuring, addressing concerns of the less confident minority is vital to bolstering cybersecurity resilience, necessitating targeted measures and awareness initiatives.

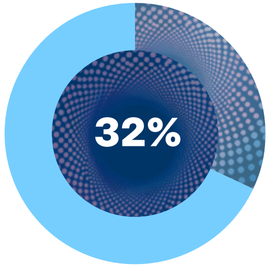
PART 2

PRIORITIES AND PLANNING AHEAD

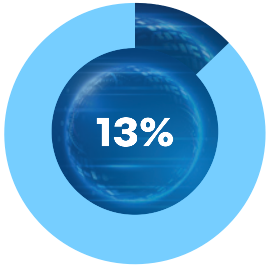
HOW DO YOU PROTECT AGAINST SOFTWARE LEVEL ATTACKS?



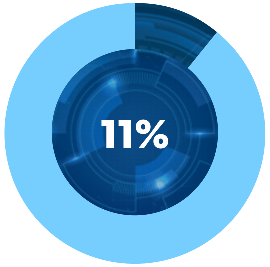
MULTILEVEL SECURITY



STANDARD SOLUTIONS



REGULAR SOFTWARE UPDATES



CUSTOMISED SOLUTIONS

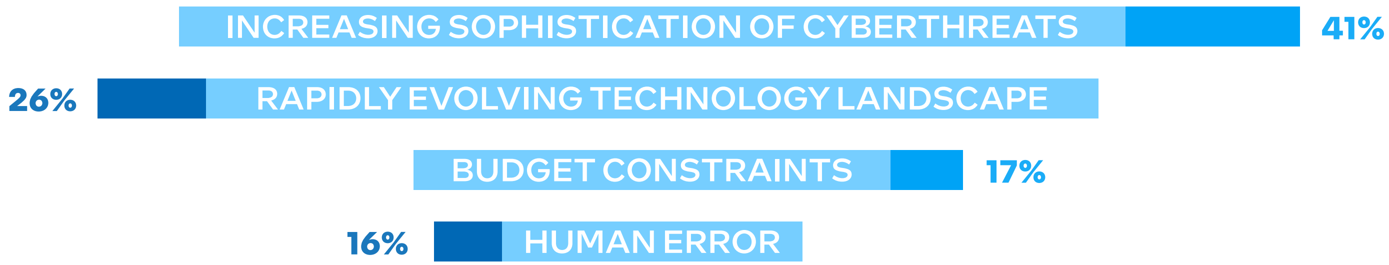
KEY INSIGHTS

Almost half of respondents (**44%**) stated significant reliance on multilevel security measures when protecting against software level attacks. Nearly one third of respondents (**32%**) cited using standard solutions, suggesting adherence to established security practices. Although there was a relatively low uptake of customised solutions (**11%**), this potentially indicates a missed opportunity to tailor defences to specific organisational needs. Regular software updates (**13%**) were acknowledged, though their importance may warrant greater emphasis. Overall, the prevalence of multilevel security highlights recognition of its importance in mitigating software-level threats, emphasising the value of a layered defence approach.

PART 2

PRIORITIES AND PLANNING AHEAD

WHAT FACTORS CONTRIBUTE MOST TO THE COMPLEXITY OF MANAGING CYBERSECURITY IN YOUR ORGANISATION? SELECT TOP TWO.

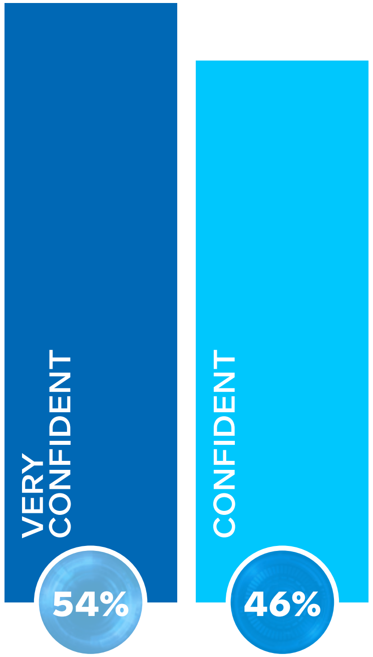


KEY INSIGHTS

Forty one percent of respondents identified the increasing sophistication of cyberthreats as the most significant challenge, reflecting the evolving nature of security risks. Rapidly evolving technology landscapes (**26%**) also ranked prominently, highlighting the difficulty in keeping pace with technological advancements and their associated vulnerabilities. Budget constraints (**17%**) and human error (**16**%) were acknowledged but deemed comparatively less impactful. These results highlight the dynamic and multifaceted nature of cybersecurity challenges. It emphasizes the importance of adopting adaptive strategies and sustainable investments to effectively mitigate evolving threats.

PRIORITIES AND PLANNING AHEAD

HOW CONFIDENT ARE YOU THAT YOUR ORGANISATION IS PROTECTED AGAINST COMMON TYPES OF ATTACKS SUCH AS CLICKING ON MALICIOUS LINKS AND DOWNLOADING COMPRISED FILES?



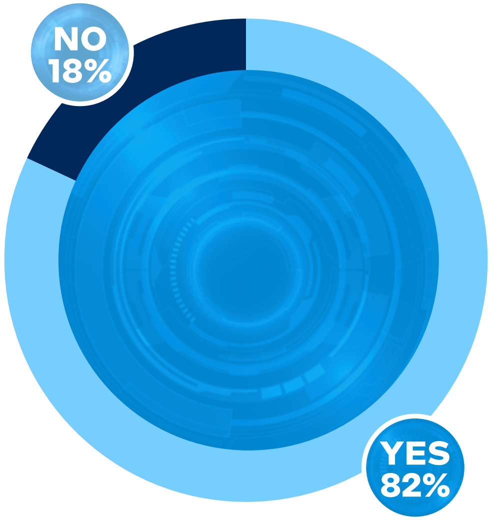
KEY INSIGHTS

More than half of respondents (**54%**) expressed a high level of confidence ('very confident') that their organisation is protected against common types of attacks. This indicates that robust security measures are in place. Additionally, **46%** of respondents felt 'confident,' suggesting a widespread belief in the organisation's ability to mitigate these threats effectively. The absence of responses indicating low confidence is reassuring, implying a strong security posture. However, continuous vigilance and updating security protocols remain imperative to uphold this confidence and ensure resilience against evolving cyberthreats.

PART 2

PRIORITIES AND PLANNING AHEAD

DO YOU CURRENTLY USE ANY REMOTE MANAGEMENT CAPABILITIES?



IF ANSWERED YES: **ARE YOU ABLE TO REMEDIATE AND RECOVER INFECTED DEVICES REMOTELY?**

100% YES

IF YES, ARE THEY OUT OF BAND?

100% YES

KEY INSIGHTS

Eighty-two percent of respondents indicated that they are currently using remote management capabilities. Furthermore, all respondents affirm their capacity to remotely remediate and recover infected devices, showcasing a robust incident response capability. Importantly, all those capable of remote remediation confirm the out-of-band nature of these operations, indicating an additional layer of security and resilience. These findings underscore the widespread adoption of remote management solutions and the advanced capabilities within organisations to address cybersecurity incidents efficiently and securely.

CONCLUSION

The findings reveal that organisations are recognising more complex cybersecurity challenges, with most expressing confidence in their ability to mitigate risks. Multilevel security measures, adherence to established security practices and remote management capabilities are key components of organisations' security strategies in combatting cyberthreats. Addressing these sophisticated cyberthreats requires a comprehensive platform built specifically for businesses which can provide multilevel security measures and robust incident response capabilities.

The high level of confidence expressed by respondents in protecting against firmware-level attacks underscores the growing emphasis on holistic security approaches. Furthermore, the reliance on remote management capabilities highlights the importance of efficient device management to ensure seamless operations. While remote management is a long-term technical challenge for enterprises, it is also cultural. By taking a long-term view and having a trusted partner ready to invest in mobile threats and personal data, organisations can future-proof their hybrid environments.

The findings also highlight the significant impact of managing data systems. Organisations are aware of the financial and operational repercussions of downtime, highlighting the urgent need for reliable and stable solutions. As organisations prioritise efficiencies like improved data analysis and PC performance, a solutions provider offering AI-powered protections will lead the pack. By addressing prevalent cyberthreats such as phishing and ransomware attacks, while also enhancing overall system performance, such a provider aligns with organisations' objectives to reduce the attack surface and safeguard against disruptions.

In summary, the findings emphasise the importance of a holistic approach to cybersecurity and IT governance. A solutions provider that integrates AI capabilities into PC platforms can effectively address these evolving challenges and enable organisations to enhance security, maximise efficiency and maintain a seamless user experience.

> **Addressing the increasing sophistication of cyberthreats requires a comprehensive PC platform built specifically for businesses.**

Intel vPro: Built for Business

New and emerging threats require a comprehensive approach to security, so Intel vPro® provides AI-boosted protections at the hardware level and throughout the stack so your business is better protected. IT is prepared for anything with a full suite of next-gen manageability tools to enable and support users no matter where they work, including more options to support a sustainable PC lifecycle. Reliable, powerful performance keeps users happy, productive, and prepared for new AI workloads.

You can get all this from any device built on Intel vPro, from a comprehensive portfolio of business class options so any type of user can enjoy a professional-grade experience.

Learn more: Intel.co.uk/vpro

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.

CxO priorities

CxO Priorities, a Lynchpin Media Brand

63/66 Hatton Garden
London, EC1N 8LE

Find out more: **www.cxopriorities.com**

Sponsored by

intel vPRO

Intel.co.uk/vpro