daisy.

STATE OF NETWORKING REPORT 2024

Ensuring network performance and security in the digital age

THE INCREASING COMPLEXITY OF NETWORK INFRASTRUCTURE

- **69%** of organisations say network security threats have increased over the last 12-18 months

The IT landscape has changed dramatically over the last few years. There's been a significant shift in where and how we work, with many organisations adopting fully remote or hybrid working. IT users expect a seamless experience irrespective of whether they are working in the office or at home. At the same time, the huge number of technologies underpinning business operations – from cloud-based applications to the Internet of Things (IoT) and edge computing – must all be supported by scalable and secure network infrastructure.

For IT network teams, this shift in working models means a continually growing demand for connectivity. They are expected to keep employees productive and deliver the digital experiences that customers expect, while reducing costs and improving operational resilience. But many are finding it hard to achieve it all, especially those burdened with legacy equipment and complex network infrastructures.

For this report, we talked to 250 IT decision-makers with responsibility for IT networks working in UK organisations with more than 250 employees. We've uncovered their views on the biggest network infrastructure challenges they're facing today and how they're managing them.

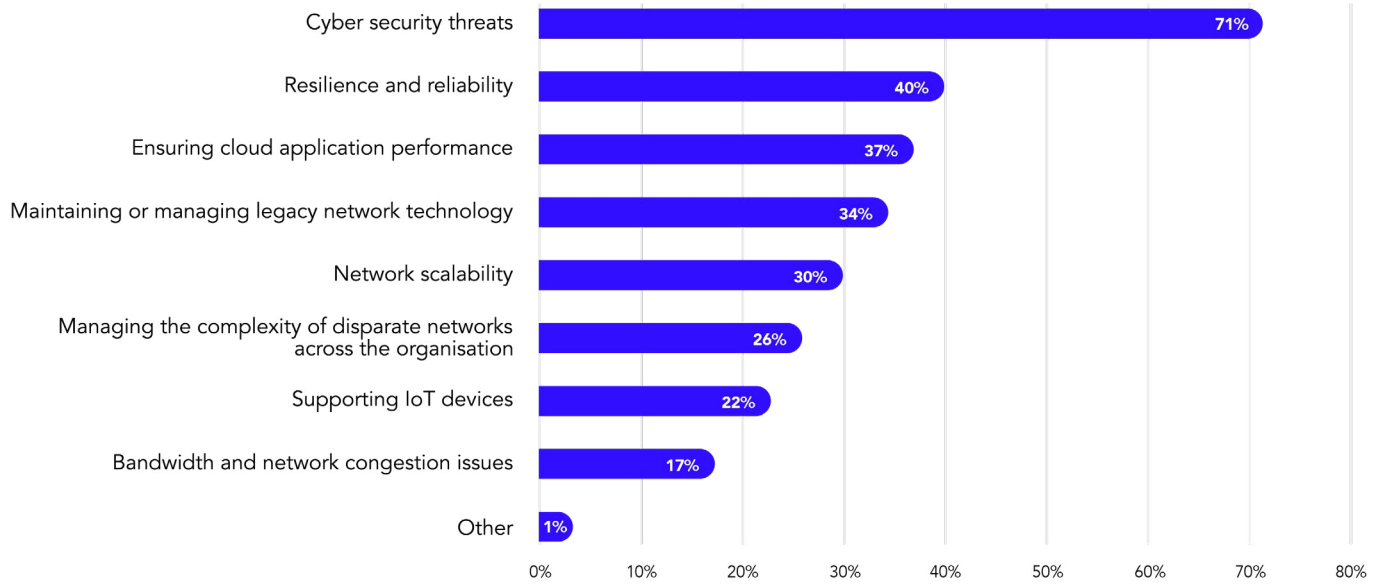
NETWORK SECURITY RISKS ARE INCREASING

As organisations become increasingly digital, cyber security and organisational resilience are hugely important. From a networking standpoint, cyber security threats continue to present the biggest challenge for IT teams. The threat landscape remains wide and varied – with ransomware, malicious scripts, brute force attacks, phishing and other identity-based hacks posing significant risks.

Today's remote and hybrid working patterns are contributing significantly to a raised threat level. At a time when the network perimeter is becoming increasingly virtual and a growing number of business processes and applications are online, it has never been so important to be able to maintain and manage a secure boundary between your network and the outside world. Simply hoping your remote employees will enable a VPN outside the office doesn't constitute a robust network security strategy.

Network resilience and reliability also continue to be an issue, as traditional wide area networks (WANs) often deliver erratic performance outside of the traditional 'office' setup. In addition, ensuring cloud application performance also presents a challenge as organisations strive to offer modern digital experiences to both employees and customers.

What are the biggest networking challenges currently facing your organisation?



- **85%** of organisations say remote/hybrid working has contributed to an increase in network security threats

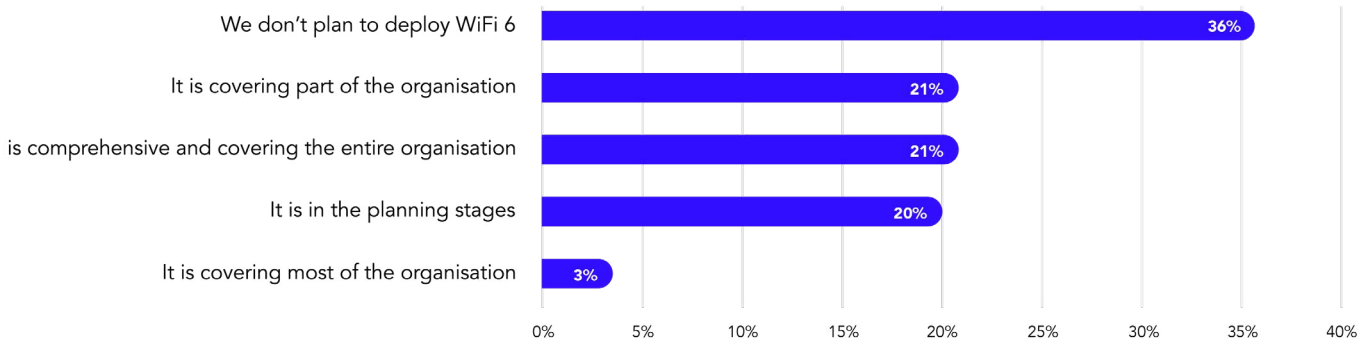
THE IMPACT OF NETWORK COMPLEXITY

As networking technology has evolved and connectivity demands have increased, many organisations have found that their networks have grown in complexity. Today, organisations have a networking landscape comprised of a patchwork of different vendor technologies, often with multiple individual networks across the organisation serving different business functions. This results in a network infrastructure that's complex and costly to manage, which is why many organisations are making simplification a business priority.

Supporting the growing organisational use of cloud applications is placing further strain on network performance. As organisations rely more heavily on the cloud, traditional WANs often lack the capabilities necessary to ensure reliable, secure, and efficient connectivity between various locations. Cloud applications are increasingly integral to modern businesses' operations; any network performance issue or downtime stands to negatively impact employee productivity and the bottom line.

It's not just remote working that's changing how we work. People are on the move in the office too. Many organisations have replaced named desks and fixed connections with hot desking and WiFi, and large meeting rooms have been turned into smaller collaboration spaces. While often organisations will have deployed the latest WiFi standard (WiFi 6) to support these changes, the cost of upgrading devices means very few have achieved comprehensive coverage of the entire business.

To what extent has the WiFi 6 standard been deployed across your organisation?



74%

of organisations say remote / hybrid working has contributed to an increase in network bandwidth and congestion issues

64%

say they have multiple individual networks that serve different business functions across the organisation

87%

of organisations say having a patchwork of different vendor technologies has created network management issues

64%

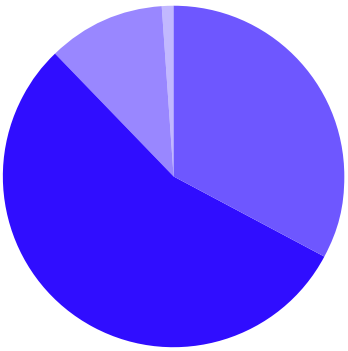
of organisations say their network is a patchwork of different vendor technologies

81%

say as the number of cloud applications their organisation uses increases, this is placing additional pressure on network performance

60%

say the cost of upgrading devices is delaying their organisation from moving to WiFi 6



88% of organisations say simplifying their network infrastructure is a priority

- It's our main priority
- It's one of our priorities
- It's a lesser priority
- We do not seek to simplify our network

LEGACY EQUIPMENT AND SUSTAINABILITY

- Organisations on average are spending **30%** of IT budgets on maintaining legacy network hardware
- On average, legacy network hardware is accounting for **34%** of organisations' overall IT power consumption

Despite the growing need to digitally transform and deliver seamless connectivity to employees and customers, organisations are spending a significant amount of budget simply to manage and maintain legacy network hardware.

Legacy hardware is also a significant factor in whether organisations can meet their sustainability goals; a significant challenge at a time when environmental, social and governance (ESG) is growing in importance. Most organisations have legacy networking equipment that consumes a disproportionate amount of power compared to modern hardware – and they're overwhelmingly looking to modernise their infrastructure as a priority.

Another area that remains problematic is disposing of networking technology in an environmentally friendly way. This is an essential business requirement, needed to comply with external legislation such as the Waste Electronic and Electrical Equipment directive (WEEE) and to meet corporate ESG goals. Yet, many organisations continue to struggle to dispose of equipment satisfactorily.

Most organisations also recognise that moving to a consumption-based networking-as-a-service model could help them realise further cost and sustainability benefits. Consuming only the resources you need – turning them on when needed, and off again when no longer required – will be a very attractive proposition for many organisations in the future.

92%

say modernising their network infrastructure will contribute to their organisation achieving its sustainability targets – **39%** say it will significantly contribute

59%

say disposing of networking technology in an environmentally friendly way presents a significant challenge to their organisation

83%

say moving to a consumption-based networking-as-a-service model would benefit their organisation – **33%** say it will significantly benefit

CONCLUSION: FLEXIBILITY IS KEY TO IT CHALLENGES

Connectivity is central to supporting organisations' current and future digital ambitions. Yet it is clear, many need to untangle their complex network infrastructures if they are to fully realise the benefits. Legacy networking equipment remains a huge cost centre, preventing organisations from reaching their sustainability goals and causing significant overspend across maintenance and power consumption.

The traditional approaches to managing wide area networks (WANs) often fall short in addressing these complex issues. However, Software-Defined Wide Area Networking (SD-WAN) has emerged and evolved into a transformative solution. This powerful technology not only solves the problem of optimising network performance but enhances security measures, giving organisations an edge in the ever-evolving threat landscape.

With SD-WAN, traditional hardware-centric networking models are replaced with a software-based approach, making it easier to manage network traffic and ensure seamless connectivity between various locations. The latest SD-WAN solutions leverage artificial intelligence and machine learning to aggregate data from various sources, enabling proactive analysis and threat detection. This empowers organisations to swiftly respond to potential security breaches, reducing detection time from months to hours.

Working with an expert partner like Daisy, you'll achieve smarter network management that makes it easy for your business to overcome its challenges and meet its core objectives. We'll give you access to innovative networking technologies that will enable you to increase efficiencies and reduce costs.

More information...

For more information about anything in this paper, please get in touch with us:

Call: 0344 863 3000
Email: enquiry@daisyuk.tech
daisyuk.tech