Network to go

According to TECHnalysis Research, around half of all companies now have some level of BYOD adoption happening in the workplace.

A rise in flexible working practices across the UK inevitably means a greater number of employees using mobile devices to access their corporate networks. RAHIEL NASIR looks at how tablets are giving headaches to network managers.

Greater flexible working could add £11.5bn annually to the economy, according to the findings of a study just released by Citrix and the Centre for Economics and Business Research.

It reveals that 96 per cent of the UK's "knowledge workers" (such as architects, software engineers, lawyers, doctors, accountants, academics, etc) who have the option of flexible working utilise the opportunity, whilst 83 per cent would do so if it was made available to them.

The researchers say if organisational culture throughout the UK changed to allow for this, there would be savings in commuter costs of £3.8bn, with a further reduction of 533 million hours spent travelling to and from work annually.

"Businesses in the UK need to look very closely at the provisions they make for flexible working," says Jacqueline de Rojas, VP of Northern Europe, Citrix. "The technology to make this happen is widely available, but we need to see a mentality shift to where it becomes an everyday part of working life. The economic argument for flexible working is quite clear – the UK as a whole needs to contribute to a culture where anywhere, anytime working is the accepted norm."

Other industry experts also confirm that the number of mobile and remote workers in the country is on the rise. For example, cloud security specialist Netskope says its latest research confirms that nearly half of all cloud app activities now originate from a mobile device. And Cisco says it's also seeing continued growth of mobile working practices, especially in a public sector being driven by austerity measures.

"Earlier this year the UK Government extended flexible working to all employees in the UK, which is further recognition of the growing trend as mobility is shown to deliver productivity gains and increased employee satisfaction," says David Goff, Cisco's manager of product sales specialists. "As mobile networks get faster thanks to Wi-Fi and 4G, those using them will be able to work faster as well."

There's yet further evidence from Vodafone. It recently conducted its own survey which asked business leaders for their thoughts on flexible working. Eighty per cent said that their staff are asking for more flexible working, and 60 per cent of employers currently give remote working capabilities to most of their personnel.

"A majority of employees in Britain now consider access to flexible working options to be almost as important as financial benefits like a good salary or pension," says Angus Flett, Vodafone's head of portfolio – connectivity. "Furthermore, these younger workers now see mobile technology as a fundamental part of their lives and they bring this expectation into the workplace."

And there's the problem. With increasing numbers of workers expecting to access corporate resources using wireless devices – both personal as well as official, and using external as well as internal networks – the IT team has its work cut out as it tries to monitor and manage them all.

The blurred lines of 'shadow IT'

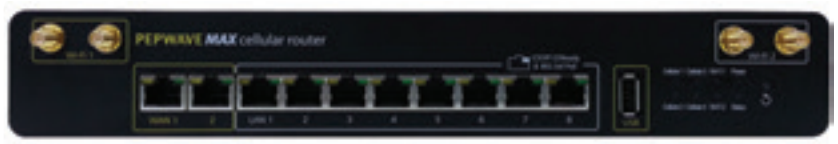
Citing an April 2014 survey from TECHnalysis Research, remote network management specialist Opengear says around half of all firms now have some level of 'bring your own device' (BYOD) adoption happening in the workplace. And it believes that figure is only likely to rise further as the benefits of enterprise mobility become more widely known.

That will lead to a whole new area beset by the blurred lines between personal and corporate usage, according to Sue Goltyakova, Netskope's senior marketing manager: "With employees seeking out their own preferred apps, which they can set up themselves, 'shadow IT' becomes a danger to the organisation and opens it up to the risk of data breaches.

"The explosive growth of mobile is fuelling an increase in the use of cloud. But the two combined are putting pressure on security teams to be aware of what cloud apps employees are using, to understand what the risks are, and to put in place policies and controls to limit exposure."

As a result, and as Cisco's Goff points out, it's imperative for IT teams to know who is connected to their network (employee, guest, contractor), where they are connecting from (secure corporate networks or coffee shops), what device they are using (employee owned or corporate provided), and what applications and data they are accessing.

He also warns that opening your network to an increasing number of devices has other implications, such as application performance, how to ensure precious corporate bandwidth is being used for the right things, and how staff collaborate with each other if the office is no longer their primary place of work.



When used with its multi-platform routers (pictured), Peplink says its SpeedFusion VPN bonding technology offers a single gateway or AP for remote clients to connect to.

Berlin-based telecoms solutions provider TELES heaps yet more woes onto this list, as technical consultant Werner Schimek explains: "Company policies used to dictate which smartphone vendor or even model was allowed but we think those days are over. Different platforms offer different ways of user interactions, and these have to be understood and supported.

"A vast diversity of devices has become the daily nightmare of the IT department. IT staff are facing support calls during installation and usage of soft clients and smartphone apps on end user devices from multiple vendors."

But it's not all doom and gloom. Rajesh Ganesan, director of product management at ManageEngine, reckons the BYOD trend is having a positive effect on the IT department's ability to control and manage the corporate network due to three main reasons: "Firstly, BYOD increases employee efficiency and mobility. This in turn has a positive effect on organisational productivity. When IT and business are aligned, better communication can take place between IT and other departments. This will lead to better management of the corporate network.

"Secondly, BYOD makes the IT department think of network security in a whole new light. The IT department has to now proactively plan and formulate the right policies. It has to comprehensively assess risks, vulnerabilities and impact to ensure security of corporate information. This makes the IT department more streamlined and better equipped to manage the corporate network.

"Thirdly, BYOD can allow IT departments to save costs. With people bringing their own devices, there's bound to be substantial cost savings for the company. These savings can be used to improve other IT processes and enable IT to play a more proactive role in managing the network."

Ganesan admits that while BYOD does make things a little hard for the IT department – such as dealing with the reality of giving access to a variety of devices while keeping the hackers away – a well-managed IT department will overcome these challenges and turn them into opportunities for growth.

Netskope's Goltyakova also highlights some positive aspects: "In some ways, having remote and mobile workers can improve the life of a network manager. Having a remote workforce which relies predominantly on cloud apps can reduce the capacity and maintenance required."

But she adds that these workers will always look for the easiest, most effective way to work, and often this means choosing their own apps without even involving IT. "So it's a double-edged sword. Network managers don't have to worry as much about keeping on-premise solutions up and running, but remote users with unsanctioned cloud apps can lead to IT having little or no visibility of the solutions in use and of where data is. It's a perfect storm of security challenges."

Are you ready for 'WYOD'?

UK enterprises are unprepared to deal with the security risks posed by WYOD – wear your own device.

In a recently published survey of IT decision makers from 100 organisations with more than 1,000 employees, 77 per cent of respondents revealed that they do not currently consider wearable technology as part of their broader mobile security strategy. Just over half admitted that they had yet to consider the impact that wearable technology could have on data security within their organisation.

While 61 per cent of IT decision makers said that they already had employees currently using wearable devices within their organisation, 37 per cent told the survey that they did not see any need to embrace WYOD at all.

The research was carried out by enterprise mobile solutions provider Accellion. Its CMO Paula Skokowski says: "With the anticipated launch of various new wearable devices in 2015, the age of WYOD is upon us. Although UK enterprises are beginning to come to terms with the need to securely enable the use of smartphones and tablets by the workforce, the next challenge is to ensure that wearables are given the same attention."

When asked what they think would be the most popular wearable devices in the workplace next year, 41 per cent said that they expected to see the *Apple Watch* in their organisation in 2015, compared to just 36 per cent opting for *Google Glass*. Email (29 per cent) is expected to be the most popular application to be used by employees on wearable devices in the coming year, followed closely by social media apps (20 per cent), internet browsing and *MS Office* applications (10 per cent each). Only six per cent consider voice calls on wearable devices to be the most appealing use.

Smartwatches from Sony and Samsung are among the most popular wearable devices in the workplace, but the Apple Watch (pictured) is expected to make a big impact in 2015.

Don't bring a virus to work

Formulating the right policy is clearly key to managing BYOD and remote workers. And of course security plays a critical role here. Every organisation should have a strong and flexible policy which protects the privacy of users as well as sensitive corporate data. Ganesan says security in a BYOD environment has become especially crucial because the number of endpoints from which threats can enter has increased.

For instance, by using a vulnerable endpoint, a hacker can easily gain access to an employee's smartphone or tablet when he or she is travelling for work. Advanced persistent threats can work with stealth and can lurk in the office network for a long time before they can be identified.

He goes on to say that other BYOD security issues that network managers have to deal include: deciding which group of employees can use their own devices; what information they can have access to; which type of devices can be included; how to demarcate the employee's office files and personal files on the same device; how to deal with loss or theft of a device; and what policies to follow when an employee quits the job.

Ultimately, safeguarding the network from mobile workers should all be part of a company's best practice procedures.

"A few years ago, network managers had to provide security, connectivity and application speed in a work environment," says Ganesan. "But now they must provide all these in any location the employee chooses to work in. After all, for employees today, work is only an activity to get done – not a place to go to."

Derek Watkins, Opengear's VP of sales for EMEA and India, says BYOD often supplements the IT environment already in place rather than totally changing it. "This means that a remote site network initially built to only handle desktops and printers now needs to deal with an influx of smartphones, tablets and laptops."

But he continues by pointing out that this added demand can easily overload existing support infrastructure, especially at remote sites with few on-premises resources. "In some cases, everything from access points and switches to controllers and routers may need to be redesigned and reconfigured with BYOD and enterprise mobility in mind."

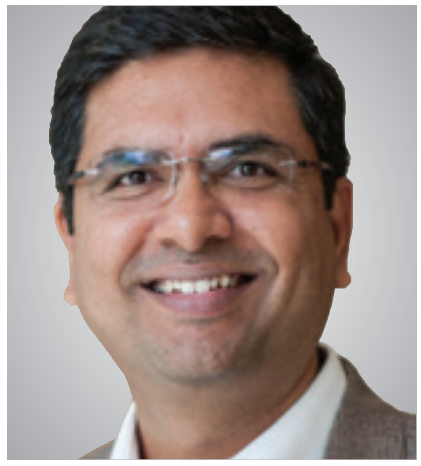
Furthermore, not only does BYOD affect the infrastructure at branch offices, but it can also place added strain on in-house data centres as well. With employees more frequently demanding access to data and files from any device, Watkins believes companies must ensure that they have the cloud infrastructure in place to support all such requests.

Vodafone agrees here. Flett says remote workers need desktop-functionality from their remote devices, and this requires cloud-based business applications – all of which need high bandwidth to function.

Peplink, which provides load balancing and VPN bonding solutions, also supports this view. While it admits security is always important, the biggest issue it sees is maintaining reliable connectivity in remote locations/dead spots or when on the move.

"Normally, attempts are initially made with USB dongles and embedded cellular connectivity in tablets and smartphones, but a number of challenges arise from this," says Peplink's 'technology evangelist' Martin Langmaid. "Firstly, contract management for increasing numbers of SIMs and their associated data plans gets very complicated quickly – even more so when BYOD is in the mix where data contracts can be owned by the staff members themselves.

"Secondly, cellular coverage can be a challenge when only one provider is being used. We've heard of cases of staff taking written notes in interviews with clients and then driving to motorway service stations or pubs with public Wi-Fi to then re-enter that data into the corporate ERPs."



"For employees today, work is only an activity to get done and not a place to go to."

Rajesh Ganesan, Director of product management, ManageEngine

Managing the apps

Are there any solutions to these myriad problems? According to Goff, the first step is to get a security policy management platform that automates and enforces secure access to network resources.

For example, he says Cisco's *Identity Services Engine* (*ISE*) delivers user and device visibility to support enterprise mobility. It shares contextual data with integrated partner solutions to accelerate their capabilities to identify, mitigate and remediate threats.

Cisco also offers its *Application Visibility and Control (AVC)* technology. Goff says that this is a suite of services in Cisco network devices that provides application-level classification, monitoring and traffic control. It's designed to improve business-critical application performance, support capacity management and planning, and reduce network operating costs.

Vodafone is the first provider globally to have embedded Cisco's *AVC* system into its network. Flett says it can automatically identify more than 1,500 different applications and report on their performance at a real-time and granular level that simply wasn't possible before.

He says *AVC* enables the network manager to drill right down into a single site from a global view to see how staff are actually using and engaging with the network. "They can build a granular view of the applications running and potentially clogging the network. The CIO can then prioritise the different applications running and pre-empt issues – if there are apps that are failing, for example, this can be picked up at site level."

Staying connected

To provide and maintain connectivity and security in remote areas, Peplink recommends the use of dedicated hardware with multiple embedded cellular modems using external antennas.

Langmaid adds that by keeping the connectivity method as a physical and corporate managed resource simplifies network management since all devices can be centrally managed. "[They] can

provide the end-to-end security, monitoring and management required as the enterprise network extends its physical and geographical boundaries.

"Also, it draws a clear line of responsibility between the end user devices and the enterprise network, where network engineers and desktop/application support analysts have a clear division of responsibility for service delivery."

This idea of central management is also crucial for ManageEngine. Ganesan says it is necessary for network managers to track all the assets assigned to staff, manage data access and passwords, and create user or department profiles from a central location. "The IT team should also be able to configure any device from this central location. This will eliminate redundancy and improve productivity."

He adds that network managers should also be able to deploy and scan apps: "In case an employee downloads a blacklisted app through their home network, it must be deactivated as soon as they enter the office network. For example, it is possible to block apps with a built-in camera function. Furthermore, IT must be able to deploy apps for all chosen user profiles which employees can then download."

Netskope's Goltyakova concurs here and says it is critical to be able to see what is on the network: "The first step should be to discover every app in use within an organisation's environment. Usually this number is far higher than expected – the latest Netskope *Cloud Report* found that there are now 579 cloud apps in use within an average organisation, many of which are totally unknown to IT.

"Secondly, activity should be monitored to look for patterns of behaviour and anomalies. What data are your employees uploading and sharing? Are sanctioned apps being chosen, or alternatives which have not been approved by the company and might not be secure?

"Thirdly, an organisation should look to set policies which are flexible and don't just mean blocking everything that 'looks a bit dodgy'. A blanket 'block' policy will antagonise users and will probably be ineffective – users are very clever these days at finding workarounds and ways to do what they want!"

"A majority of employees in Britain now consider access to flexible working options to be almost as important as financial benefits like a good salary or pension."

Angus Flett,
Head of portfolio – connectivity,
Vodafone

Opengear believes that a fundamental consideration of any network infrastructure management plan should recognise the possibility of a failure where the primary network is unavailable. Watkins says this has led to increased demand for solutions that utilise 3G/4G and even satellite connectivity as a means of providing centralised IT teams with 'remote hands' to fix issues that occur at branch level.

"The notion of a sending out an IT tech to a remote branch office – to reset or reconfigure an errant network switch or access point, for example – is an expensive and impractical solution. Any organisation relying on BYOD must have a strategy to ensure accessibility to the network as well as a fall back to meet outage scenarios which are more common than network vendors would like to admit."

Langmaid claims the only truly successful approach for reliable connectivity is to use multiple data connections from multiple ISPs and then load balance (or VPN bond) across those links. Bandwidth monitoring and management also then becomes a key element of any large scale deployment. "The IT department needs to know who its biggest data consumers are and why, and be able to identify any abuse of the systems."

He goes on to explain that *SpeedFusion*, Peplink's VPN bonding technology, bonds multiple cellular and fixed WAN connections to create what's claimed to be a highly resilient and available secure VPN connection from a remote location back to the enterprise network.

When used with the vendor's routers that can combine cellular, fixed line and satellite WAN links (from any provider), Langmaid says *SpeedFusion* offers a single gateway or AP for remote clients to connect to. "We then have a cloud management app that gives the IT department full visibility of its mobile device estate, providing centralised monitoring, reporting and management."

While predicting the future is always a risky business, one thing is for sure: bandwidth-consuming applications will keep growing. And that means network managers will need to continually look at how to balance the use of these applications to ensure the network is not overwhelmed.

Flett offers the following advice: "Network managers will succeed by getting to know their networks better. Greater visibility will lead to greater knowledge which in turn will result in better control – and better control will ultimately mean a better network. The promise of the truly application aware network will become a step closer." ■