

## The Bigger Issue - Communications and IT on the Move

### ALWAYS ON

**Keri Allan investigates the background to the exponential growth in mobile working, and how the demands of the workforce for instant connectivity are placing ever greater pressure on IT/IS departments**

Different locations, hotels or coffee shops – this is the point of mobile working, to ensure your workers are mobile. In order for this to be possible, they need to be able to traverse different networks invisibly and with their work uninterrupted.

Independent research undertaken by Damovo UK identified the growing number of mobile and remote workers as an additional pressure facing IT departments. In support, organisations have needed to scale their underlying network at the same rate as their users. The research revealed that 85 per cent of IT directors provisioned mobile access on an ‘as requested’ basis, which in turn is making support more difficult to carry out, as workers are using different devices to access the network and it is difficult for IT departments to push out network or software updates to the mobile workforce.

Unsurprisingly, this has led to nearly half of the respondents (46 per cent) saying that they have seen an increase in the number of complaints received regarding poor network or application performance, which means that IT/IS departments are having to devote even more time to resolving user problems.

But this isn't the only issue IT/IS department must overcome. Another problem that arises is the quality of connectivity – broadband 3G and voice calls. Whether working from home or travelling to a foreign country, network access is required, yet in some areas it can be a struggle to achieve.

Costs can then rocket as staff struggle to get access, as Matt Cooke, senior product marketing manager at iPass, highlights: “The main problem occurs when employees take connectivity into their own hands and do anything to get connected and access data – such as buying Wi-Fi day passes or 3G subscriptions. For example, some research by Expedia revealed that international; or five-star hotels often charge rates of up to €21ph to connect.”

### The security of data

But, of course, a crucial issue for most offices is the security of their data when workers are on the road or visiting customers.

“Remote users will always provide additional risk to a network but, for many companies, it is the only practical means to extend their workforce logistically and cost-effectively,” notes Steve Garton, director at Advent IM. “It is essential however, for management to decide whether, for example, all employees require full access to the server when away from the office, or whether parts of it can be restricted and permissions allowed on a case-by-case basis.”

Once workers are out of the premises and away from the protection of the corporate firewall, there is an increased risk that data could be intercepted – or distorted, or unauthorised users get access to the corporate network – as they communicate with the main office.

“Without the right monitoring and management tools, IT managers can't be sure how secure their corporate intellectual property actually is,” says Simon Ford, director at secure comms specialist NCP Engineering. “Conventional VPN clients require that an internet connection is already available for

remote access. More advanced VPN suites take care of, among others things, the highly secure connection to any public network and the firewall protection of the terminal.

“Central management creates transparency,” he continues. “This enables administrators to have an overview of the current status of all teleworking stations and systems at any time. This includes network access control (NAC), the central monitoring of adherence to all security guidelines prior to access to the company network.

“High availability service (Failsafe and load balancing) guarantee the high availability of secure enterprise servers. “What IT managers are looking for is single point of remote access administration, central configuration management, automated mass deployment, fewer clicks for administrators, easy change and update management and configuration locks.”

### **Myriad solutions available**

As Ford highlights, although the issues exist, there are myriad solutions out there of which IT/IS managers can take advantage.

“Passwords, firewalls, encryption and other means of network protection all play an important part in the ‘onion-layered’ approach to security, but in isolation are often proved worthless,” notes Garton. “Integration is key in bringing a strategy together, combining technical ‘soft’ and ‘hardware’, however ultimately this will not deter or prevent a determined attacker attempting to disrupt ... or even worse. It can, however provide some delay, during which time some indicators may show themselves and be detected. With this in mind companies must continue to use all of the tools available to disrupt and reduce this asymmetric threat, but also build them to comply with their central policy.

“Understanding your information may show that policies and procedures are instead what you need, not expensive encryption,” he continues. “Education is essential and needs to be worked into each and every employee’s training programme. If they are given the opportunity to work remotely, then not only do they need to learn about how to use the piece of kit, but also how to use it securely.”

Planning also plays a role. When considering remote working, the IT/IS department should focus on what equipment can be used, and put together a complete solution for availability of hardware and network access.

“IT managers must start from the very beginning when planning the roll-out of a remote working project and identify precisely which communication tools should be used across the company. This way they are able to minimise the number of support technologies needed to maintain the remote comms environment, and billing management becomes a great deal easier,” says Jon Tracey, engineering manager, EMEA, LifeSize Communications.

“Organisations should be looking to a solution that provides continuous availability of mobile applications and remote access to data. The ideal solution will provide a clone of the primary server on a passive secondary server, monitoring the performance of the entire mobile environment.” Explains Andrew Barnes, svp, corporate development, NeverFail.

“If a failure occurs, the solution will look to restart the application before either automatically switching over to the secondary server, or alerting the IT staff that a failover should be conducted. And as connections and services are transferred, users will not experience any loss of coverage.”

## Several overlooked areas

But there are still several, often overlooked and technologically neglected, areas when it comes to mobile security. PDAs and smartphones are key culprits in data loss. They are small portable and powerful and yet easily (and often) lost or left behind.

“Most corporate smart phones are synched to e-mail accounts and include many confidential e-mail and SMS communications and of course the login credentials for the corporate network,” notes Rik Ferguson, security advisor at Trend Micro.

“Mobile devices are increasingly becoming a target of mobile malware, although they are slightly helped in this respect by there not being a single platform that is more widely used than another (Symbian, Windows Mobile, Blackberry, Android, iPhone). However this is a mature area for data loss and a growth area for cybercrime. All handsets and PDAs in a commercial setting should be armed with anti-malware, device level encryption (including for any inserted cards), firewall and anti-spam (to catch spreading malware as well as nuisance messages).”

“Finally, organisations will need to think about the hardware and environmental factors as well as the software,” adds Andy McBain, product manager, Motorola EMB. “Devices taken out of the office and used on the move will frequently be exposed to rain,. Cold, heat and dust, and may often be dropped or knocked.

“Consequently, companies either need to factor in repairs, or consider more durable devices from the outset which will last longer, but may be more expensive. Also, as with any device which is taken out of the office, theft and loss is an issue. Companies need to make sure that if the devices store any kind of confidential data, that they have a way of remotely wiping them and locking them down. Which it is rare that an asset will be recovered, at least customer and company data will not be at risk.”

It's clear that there are still many issues and barriers to overcome, however this is an ever-evolving area. A number of technological advancements are just around the corner, thanks to the support from providers, as Stewart Yates, managing director of TFM Networks explains: “IS managers will benefit from the time and research providers are investing into supporting remote workers. Providers are designing fully-managed packages to overcome the issue of support.”

“Web-based applications are transforming remote working,” continues Ben Gladston, ceo of Conosco. “Soon we'll see Microsoft's web-based versions of its Office applications, which promise to work seamlessly with their desktop counterparts. Most of the clunky solutions – VPNs, offline folders and so on – will thankfully vanish. A major bottleneck has been internet connectivity, but 3G is now often faster than broadband and is good enough for work purposes; coverage is the remaining problem, but that should be sorted in most EU areas soon, although rural US is another matter.”

“In the longer term, the next generation of office workers will take this level of connectivity for granted,” Tracey concludes.

*Keri Allan has been writing about business and technology issues for the last eight years, covering a huge number of areas from CRM and ERP to consumer electronics and video games. She has an honours degree in Journalism and Sociology.  
web site: [www.keriallan.com](http://www.keriallan.com)*

The text of this article is extracted from *IMIS Journal - October 2009*