

We are all IT users now

MSPs, SaaS and the management of remote devices

Contacts:

Bob Tarzey
Quocirca Ltd
Tel +44 1753 855794
bob.tarzey@quocirca.com

Rob Bamforth
Quocirca Ltd
Tel +44 1962 849746
rob.bamforth@quocirca.com

Heidi Wieland
NTRglobal
Tel +1 805 7227413
hwieland@ntrglobal.com

BRIEFING NOTE:

This briefing has been written by Quocirca to address issues faced by organisations that have to manage an increasingly dispersed IT infrastructure.

The report draws on Quocirca's knowledge of the technology and business issues faced by organisations and provides advice on the approaches that can be taken to ease the task of IT management.

During the preparation of this report, Quocirca has spoken to a number of end users, service providers and vendors and is grateful for their time and insights.

Quocirca would like to thank NTRglobal for its sponsorship of this report.

Whether we like it or not we are all IT users now. Through the ubiquity of networks of devices that we rely on for information, security and day-to-day transactions even those who eschew technology now rely on it, even if they do not acknowledge it. The failure of these networks can lead to widespread disruption, unhappy customers, unproductive employees and lost business. Ensuring their availability, security and efficiency is a job for experts who need powerful tools to carry out the task.

- **The IT requirements of many businesses are now best measured by devices under management rather than number of employees, or even IT users**
Many devices, such as in-store video displays, security gates and wireless routers, are now part of computer networks, the management of which is just as critical to many businesses as that of traditional PC networks.
- **These networks are increasingly taken for granted by their users, many of whom would not even consider themselves users of IT**
The only way to manage such networks is remotely. Even when devices are assigned to end users, they will not have the skill, time or inclination to help manage them.
- **IP is the main network protocol that links all these devices allowing easy interaction between private IP networks and the public internet**
Using the internet protocol (IP) has wide ranging accessibility benefits, not just for users but also for managers who can access any device from anywhere given the right tools and can access centralised databases that define configurations, access rights and usage policy.
- **Keeping such networks running requires specialist skills that many organisations, especially small ones, do not have in-house**
Businesses need to focus on their core activities and managing IT can be a distraction. As they come to rely more and more on networks of increasingly diverse devices and the management task becomes ever more complex, many have now turned to managed service providers (MSPs).
- **For MSPs IT management is their core activity and they have the wide ranging experience and skills to undertake the task**
This goes beyond just the capability to manage networks of remote devices but also housing the infrastructure of servers, routers, load-balancers and so on that support them. MSPs house these in enterprise-class data centre facilities that are beyond the means of many of their customers.
- **MSP staff need access to management tools wherever they happen to be and the data that defines device usage needs to be centralised and easy to share**
Networks are part of the cloud and MSP staff work in the cloud. It makes sense to place management tools and the data they rely on in the cloud where they can be shared with customers who define access and usage policy. Software as a service (SaaS) is one of the best ways to provide this capability.

Introduction—we are all IT users now

Businesses that make most of their money selling products to other businesses (B2B) usually categorise their current and prospective customers by the number of people they employ. This makes sense if you are selling chairs to banks; one seat per employee bottom and a few extra (perhaps harder) for customers. For information technology (IT) vendors, counting employees can be misleading; after all not all employees use computers—do they?

At one level this is true as not every employee sits at a desk with a PC in any industry, although increasingly many are sitting in a van or some other remote location with a laptop or handheld computing device. The increase in the use of IT remotely by both white- and blue-collar workers has certainly led to higher PC penetration rates amongst employees in many businesses.

For the IT industry, even counting employee PC usage is becoming superfluous because of the growing number of devices that businesses rely on that are not assigned to one user or another and often don't even look like computers. Such devices are often used directly by customers that may eschew technology and consider themselves computer illiterate.

Banks have lived with this for years with their ATM networks, as have retail outlets with increasingly sophisticated point-of-sale (PoS) devices—tills, or cash registers, if you prefer. The number of such devices is growing fast and businesses of all types make more and more use of a range of off-the-shelf or purpose-built devices linked by networks that allow them to interact with their customers, often directly.



As businesses come to rely more and more on these networks the impact of

downtime becomes more serious; disgruntled customers, unproductive employees and lost sales—all unacceptable. Keeping these networks running is a job for specialists that many businesses do not have in-house, so the job of managing these seemingly unmanageable networks, as well as conventional PC ones, is often outsourced to specialist managed service providers (MSPs).

Working with MSPs is cost effective, especially for smaller businesses, as MSPs can apply economies of scale to manage multiple networks of devices for various customers and invest in the appropriate skills and tools to do so. MSPs have also built up expertise in remote systems management, which is the only practical way to keep their customers' often vast networks going.

Those networks are in the cloud, a term increasingly used to define the internet and associated private networks that link to it. Managing devices in the cloud requires tools that work in the cloud, so, just as with many other software applications, system management tools are moving online and, instead of running the software in-house, tools are being offered as a service (software as a service/SaaS). A big benefit of this approach is that this allows MSPs and their customers to share and work off the same data sets wherever they happen to be.

Specialist computer networks

There are those, even in the advanced economies, who believe they can sidestep technology. PCs, the internet, email etc. are not for them. Yet think of the average day of anyone living in a modern city (which is now over half the world's population). Just getting to work can be an unrecognised tangle with ICT.

Arrive at a railway station and the first thing we all do is check the electronic displays to see if the trains are on time and which platform to go to. We are annoyed if the screens are blank and it is necessary to track down a member of staff to ask—who probably will not know any better as they rely on the same information screens. If all is well, we proceed through electronic ticket gates, which ensure we have a permit to travel. In some cities we may use a frequent travel card, the system automatically topping up cards from our bank accounts when credit runs short and recording travel history for subsequent review.



Waiting for the train we may go to buy a newspaper and, oh yes, feeling lucky—a lottery ticket, dispensed by any one of thousands of specialist devices. Walking from the destination station to work, we remember to visit the ATM and check that our employer has paid us for the last month before we put in another day of toil. The ATM is overlooked by a surveillance camera to protect us from the increasing number of thefts from such places; one of thousands of cameras spread across the city, hopefully making it safer, but at least easier to capture criminals in action.

The employee arriving at work may be there to serve meals in the canteen or clean the windows and would not be considered an IT user, yet en route to work they have already encountered five separate IT networks, without even thinking about it.

This is just day-to-day stuff; there are many more examples. A visit to a health centre will mean a doctor calling up your records on a traditional PC network. If the news is bad you may be sent off to a specialist clinic for a scan. The specialist will access the same records as the doctor on a PC network and the scanner is likely to be linked in to the network as well, automatically associating the scan results with your overall health record.



On a darker note, should you be spotted up to no good by one of those surveillance cameras and end up on the wrong side of the law, you will pick up a criminal record that will follow you around on a conventional police PC network. If you escape a prison sentence, you may still be subject to a control order that will lead to you being monitored by a tag strapped to your leg—offenders connected to law enforcers by an invisible network.

Indeed, parts of many networks are now invisible. Whether it is a field service engineer clocking in over a 3G network or a sales person updating forecasts in a café, wireless networks drive many of these devices and wireless networks themselves need to be managed. Go to a coffee shop and the (hopefully) smiling server will no more know how to fix the



wireless access point than how to re-program the point of sale system, but if either is not running there will be unhappy customers.

Managing the unmanageable

Like it or not, supply chains, travel networks, healthcare, criminal justice and many other services, on which we all rely, are all now dependent on IT networks. If these networks, or the devices they link, fail, the service fails. Today we are all IT users.

Lorry drivers deliver goods, airport staff check in passengers and ensure security, policeman chase criminals—but they are unlikely to have the skills to manage the devices that they rely on, and certainly not the networks that connect them. Even if they did, getting involved would be a distraction from the task in hand and, anyway, many IT management tasks are mundane and need to be applied across hundreds or thousands of devices on a network. The challenge is to make sure all these devices are available and working when they are needed, and also to power them off and reduce running costs when they are not.

Such networks of devices would be unaffordable if maintenance had to be carried out by an individual on site. So most maintenance, barring actual hardware replacement or fixes, must be carried out from afar. To make things more complex, different networks will link devices running different software; secure devices using a locked down version of desktop Linux, any of the different versions of Microsoft Windows and, in some cases, Apple Macs. As well as managing the remote devices themselves there are the servers that support them.

The one thing that most networks do have in common these days is the network protocol used to connect the devices on them, which is now predominantly IP (internet protocol). The world has converged on IP because it makes it easier for the networks to interact with each other and share information and, of course, the mother of all IP networks, the internet, makes that interaction and access pervasive. Even old networks like the banks' ATM systems are being moved over from older networks to IP.



MSP value

Supermarkets specialise in selling food, banks deal with money and travel companies move people around. MSPs manage IT installations and make sure they remain up and running. MSPs don't supply their employees with food, lend them money or transport them to work—but they do train them to be IT experts.

So, with the exception of some of the largest companies that may, in effect, have their own internal MSP capability, it makes sense for IT-reliant organisations to hand off the task of keeping their increasingly vital networks of devices running to specialist MSPs.

MSPs will have experts in Windows, Linux, UNIX, Macintosh, Exchange, Lotus or whatever systems they take on contracts to manage. These experts will often have seen many problems new to an individual customer before in other customer situations and be trained to deal with them. MSPs must also abide by service level agreements and accept penalties for failing to meet them. Try imposing that sort of rigour on an internal IT department.

MSPs will host the centralised infrastructure such as servers, routers, load balancers and network accelerators that networks of remote devices rely on. They will house all this in purpose-built, energy-efficient data centres with emergency backup power supplies and fail over capabilities (i.e. a second data centre should take over if all or part of the primary one fails). In short, as well as managing IT for their customers, they provide enterprise-class facilities that many could not afford to build for themselves. Working with MSPs does not just reduce cost but reduces the risk of IT failure, allowing their customer to focus on the core skill of delivering customer value.

Case study—Satech Rodlan

Satech Rodlan is an IT consultancy that includes hardware and software maintenance in its range of services. Its client base is widely distributed and remote access to its customers' systems is the only practical way of carrying out regular maintenance. It had been relying on an on-premise system management tool with VPN connections to its customers' systems but, as its business grew, Satech Rodlan found this increasingly inefficient as connections regularly had to be reconfigured and it was not able to support off-site users, which were becoming increasingly important to many of its clients.

After a wide-reaching evaluation of new tools, Satech Rodlan selected NTRAdmin as the most cost effective way of being able to carry out support and maintenance for its customers, whether it was HQ systems, branch office equipment or remote users. Being a SaaS offering, NTRAdmin not only enabled Satech Rodlan to support the increasingly flexible working requirements of its customers, but also to ensure that same flexible working was available to its own employees.

Repetitive tasks and shared data

Vast networks of devices need to be kept up and running, which requires monitoring and maintenance. The range of tasks will vary depending on the type of devices on the network but mostly they are mundane and repetitive.

End-user PCs are some of the most complex. Not only do they need to have their systems, applications and security software kept up to date, but their use needs to be monitored to make sure it is within company guidelines and data stored on them needs to be backed up.

Robust display terminals providing information to travellers are not a big security risk as they are only used for displaying data and are usually high off the ground to thwart would-be vandals. However, they still need maintenance and there are savings to be made in power costs if they are turned off when the travel network has closed down. Indeed, the automated powering down and waking up of all types of devices is going to become increasingly attractive as organisations strive to reduce power costs and show their green credentials.

PoS devices, lottery terminals and ATMs all need to be monitored to make sure their usage is as expected but they can also be updated to make sure their users are aware of special offers, new features or heightened security risks.

Networks of wireless routers need to be monitored to make sure they can handle loads and that their security is maintained so that only authorised users can access them. Monitoring them can allow their managers to understand the most popular points of access and arrange for increased capacity to be installed where required.

When such a hardware upgrade is necessary an engineer may need to be sent on site. It is only when such upgrades are needed or when faulty hardware needs replacing that such a visit is entailed, and often the need for engineers to head out can be predicted in advance through monitoring. Consequently it is possible to make sure they have more efficient schedules.

Those engineers, once on site, will often need to access information about a device and view and modify its systems, user and security settings. In other words they need access to the same tools and data their colleagues have back in the office. That data also needs to be shared between MSPs and their customers; while an MSP might have the responsibility for keeping systems available for authorised users it may be the customers themselves that define users' rights and the policy that governs them. Tools and the data about devices under management needs to be easily shared.

The networks they are managing are part of the cloud; the engineers and users are in the cloud, so it makes sense for the data and tools to manage all these devices to also be in the cloud.

Case study—Not Just Computers

Not Just Computers is a UK-based reseller of IT systems focussed on small businesses and schools—organisations with limited in-house IT skills but are impacted the same as any other by down time. Not Just Computers aims to ensure high availability by providing high quality proactive support and it believes this is essential to winning and keeping customers.

As Not Just Computers' business has grown, ensuring it can efficiently service an increasingly distributed client base has become more and more of a challenge. To this end it needed to be able to carry out remote administration even for the smallest of sites and NTRadmin has become the key tool for enabling this, allowing pro-active checking of software, hardware and networks ensuring emerging problems are noticed early and dealt with before they have a serious impact.

SaaS-based IT management

SaaS is often narrowly thought about as a way of delivering customer relationship management and a few other business applications. It is often not appreciated just how widely used SaaS is to deliver a wide range of IT services.

These range from email management and security though web and video conferencing, IP telephony, remote customer support, office applications and off-site backup. Increasingly, systems management tools are being made available in the cloud too.

As the clear boundary between organisations and their customers continues to fade and more and more remote users become dependent on networks of remote devices to interact with employers, suppliers, retailers, transport providers and government organisations, making sure those networks are available when users need them has become paramount. This is a job for specialists who need to be armed with the right tools, which they need access to in as many locations as there are devices.

About NTRglobal

Founded in 2000 and headquartered in Barcelona, Spain, NTRglobal has grown to be a worldwide leader in enterprise-grade, cost-effective Software as a Service for remote support, remote access and remote systems management solutions. Used daily by more than 14,000 organisations around the world, NTRglobal on-demand solutions, including NTRsupport for end-to-end remote support with FirstHelp, self-service portal and NTRadmin and NTRadmin Bots for remote management of devices on the network and outside the WAN, provide individuals, small and mid-sized businesses and large enterprises with highly secure:

- Remote support for customers and employees
- Remote access to PCs and Macs
- Remote systems management
- Enterprise mobility management

NTRglobal is led by an international management team that has steadily expanded the company's on-demand technological capabilities and customer base, and has local operations in more than 20 countries, including North America, Europe and the UK, China, Russia, Dubai and Japan.

NTRglobal offers a free trial, professional services, an Integration SDK, certified salesforce.com integration and on-demand delivery and pricing that accommodates any business model. SaaS provides constant access to NTRglobal solutions that are managed and maintained inside a secure network operating centre. Self-hosted on-demand licensing enables companies to secure and manage solutions inside their own firewall.

More information is available at www.ntrglobal.com

About Quocirca

Quocirca is a perceptual research and analysis company with a focus on the European market for information technology and communications (ITC). Quocirca reports are freely available to everyone and may be requested via www.quocirca.com.