

## Remote IT management

### How SaaS-based tools provide a superior end-user service

#### Contacts:

Bob Tarzey  
Quocirca Ltd  
Tel +44 1753 855794  
[bob.tarzey@quocirca.com](mailto:bob.tarzey@quocirca.com)

Rob Bamforth  
Quocirca Ltd  
Tel +44 1962 849746  
[rob.bamforth@quocirca.com](mailto:rob.bamforth@quocirca.com)

Heidi Wieland  
NTRglobal  
Tel +1 805 7227413  
[hwieland@ntrglobal.com](mailto: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.

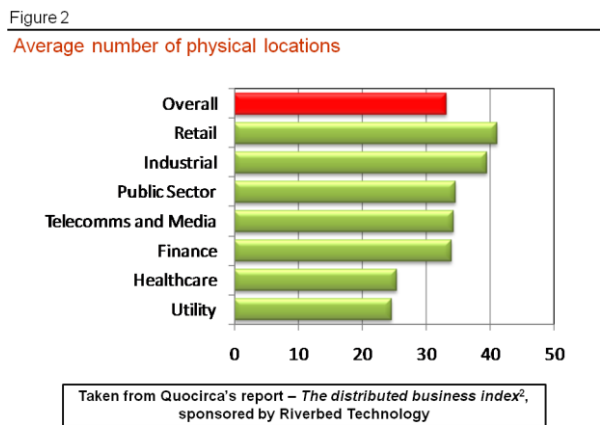
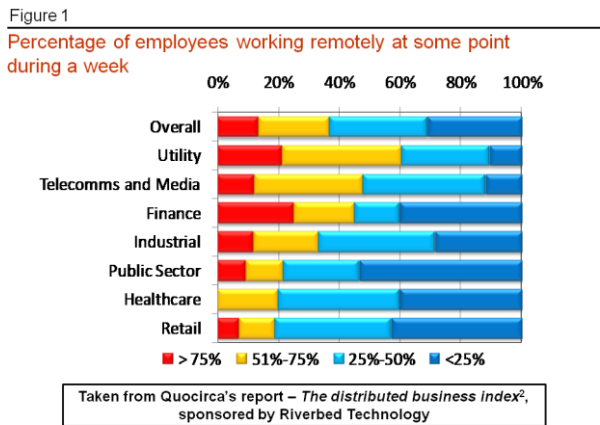
Quocirca would like to thank NTRglobal for its sponsorship of this report.

*Businesses of all sizes have to manage an increasing diversity of remote users and devices. The task ranges from simply keeping systems running to ensuring security, compliance and the achievement of environmental goals. Under this sort of pressure, IT managers and managed service providers, to which the task is often outsourced, must have flexible access to powerful tools and an ability to share the data those tools rely on.*

- **In the average business 65% of employees now regularly use IT, 20% access IT remotely at some point and many others work in branch offices**  
The IT infrastructure all these workers rely on needs to be managed remotely, not just for the sake of the employees but also for the partners, suppliers and customers they are constantly interacting with electronically.
- **Remote IT management needs to be proactive, continually ensuring the security of remote devices and the adherence of their users to policy**  
Management tools must allow IT managers or the staff of managed service providers (MSP) to run tasks that address widely dispersed groups of users as well as providing individual attention when required.
- **Those managing IT need flexible access to the tools and the data they rely on, and must be able to share data easily**  
Hardware failure and new equipment deployment will still require IT managers to leave their normal place of work and they, too, have a right to the flexibility of working that they are enabling for their colleagues—IT management tools must be accessible from anywhere.
- **The data the tools rely on must be up to date and accessible to a range of users**  
If business managers change the status of employees then this information must be immediately reflected in the actions of IT managers. MSPs must be able to easily and securely share this data with their customers.
- **Such wide ranging access to management tools and data that is held in-house behind a firewall is hard to provide**  
Just as with email, collaboration tools and many business applications (e.g. CRM), there is a strong case to be made for the deployment of IT management tools using the software as a service (SaaS) delivery model.
- **Using SaaS has additional benefits for all users of the system as it allows an aggregated view of IT usage for the benefit of a community of customers**  
Whilst the security of the data owned by individual organisations is paramount, the aggregation of anonymised data across the community is of great value, answering questions about usage trends, upgrade issues and providing advice on other commonly encountered problems.

### The travails of Average Inc.

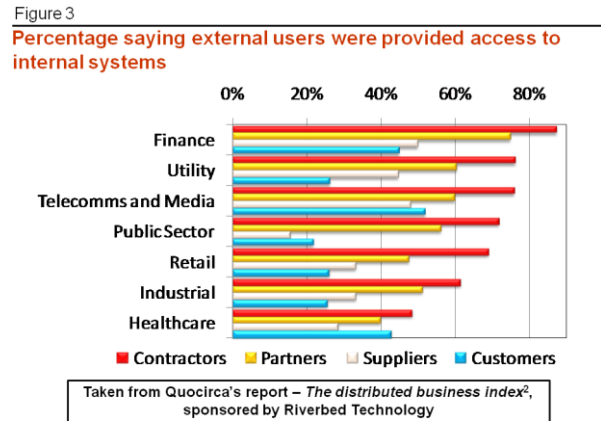
Given the diversity of businesses, describing an average one may seem a bit pointless. However, it does serve to underline the extent of a problem most businesses now face when managing their information technology (IT) and trying to keep their end-users happy. In the average business 65% of employees now use computers, 20% access IT from remote external locations (figure 1) and many others work in one of around 30 branch offices (figure 2).



Many readers will have lots of advice for how IT in such a business should be deployed, just as Quocirca did in its March 2008 report *Average Inc*<sup>1</sup>. However, whatever that advice might be, there will be a need to manage remote IT equipment. Average Inc. needs powerful management tools to keep its end-users satisfied.

To add to this imperative, often these remote users are not even employees; they may be contractors or consultants working from their own premises, or they may be customers, partners or suppliers that are given access to internal applications in order to participate seamlessly in business processes (figure 3).

IT failure means those business processes stop. More often than not a malfunction will be at the user's end rather than the application itself. Such failures need to be minimised, but will happen. Good IT management practices—and the tools to implement them—means fewer outages and faster fixes when the inevitable happens.



### Managing the mundane

Even when all is good and users are happy, IT managers cannot sit back. Good practice means a continuous round of maintenance tasks:

- Constantly checking end-user devices are secure as they come and go from the network
- Keeping software up to date on servers and PCs, sometimes across multiple operating systems
- Auditing software use to ensure licence compliance
- Checking for the use of unauthorised applications

Without remote management tools, Average Inc.'s IT staff would be among the most travel-weary employees.

For some businesses the task may seem overwhelming; it need not be—they can do most of these management tasks remotely. And, for those businesses too small to have IT staff, or at least not wanting to waste the time of the few that they do have on mundane tasks, there are managed service providers (MSP) who will do all the day-to-day stuff for them.

If Average Inc. has not taken the time to find tools for remote IT management you can be sure that their MSP will have done so. For MSPs this is their bread and butter; with tens or hundreds of organisations to keep happy, remote management tools are a must. To make their businesses viable and their services affordable, MSPs must centralise almost all management tasks.

However, neither IT managers nor MSP staff can throw away their car or van keys just yet. There will be hardware failures to fix, new equipment to be provisioned and branch users will need on-site IT training. In addition, IT managers have personal lives too and should be able to benefit from flexible working practices. For IT managers, the need to be able to do their job from a remote location at any time is just as important as it is for the users they are enabling.



## Remote management of remote users

For an IT manager to be able to do much of their job wherever they happen to be might sound like a tall order. They may well carry around their own laptop PC, but what if that fails? Furthermore, to manage remote users requires access not just to their devices but to all the data about their access rights, job role, current assignments and the configuration of their devices.

There are security considerations around the storage of such data on mobile devices and it also needs to be available to multiple managers at the same time. What if an employee has just been promoted or sacked? The actions of an IT manager must be based on real time access to a central data source that reflects the decisions being made by business managers and other IT managers or, indeed, staff at an MSP.

Some management tasks need to be carried out for individual users, such as clearing up a spyware problem on one user's PC, or enabling temporary access to the HR database for another user. The IT manager does not want to have to establish a direct link to each individual PC every time such jobs need doing; access should be automated via logical assignment of users to devices in a central database.

However, most management tasks are not carried out on an individual user's device but are repetitive and need to be applied to many simultaneously:

- Applying an emergency patch to all copies of Windows XP
- Upgrading Adobe's Creative Suite on all the Apple Macs in the design group
- Turing off all branch servers and PCs at night to conserve energy
- Waking up devices before users arrive in the morning
- Policing local email storage and archiving when necessary
- Monitoring and controlling use of USB devices
- Automatically initiating backup of all servers and PCs at convenient times



Such tasks cannot be carried out on a one-to-one basis but rely on the availability of a central data source that defines who a user is, what group they belong to, what equipment they use and which policies apply to them. Only when armed with this information is the IT manager able to initiate multi-user management tasks.

## Managing the unmanageable

To add to the burden, many IT managers are now required to take care of remote devices with no designated end users. These range from networks of printers and wireless routers to in-store video displays and remote cameras operated as part of surveillance networks. More and more such devices are linked together using IP (internet protocol) networks and therefore have an IP address making them easy to identify, access and manage with the right tools.

Unlike devices with designated end users, there is usually no one that can be called upon to provide some local assistance to help the IT manager do their job. However, the benefits of being able to manage such devices from afar are huge: think of the power saved if all the display devices at train stations are switched off overnight or the sales that will be lost if a software vulnerability shuts down thousands of devices on the network for issuing lottery tickets because the task of patching their software can not be carried out from afar.

The problem of managing remote networks of IP-based devices is discussed further in a companion Quocirca briefing, *We are all IT users now*<sup>3</sup>.

## Any time, anywhere, IT management



If the benefit of secure access to a centralised data source from anywhere, on any device and at any time sounds like something you have heard before, it will probably be due to familiarity with the benefits of the software as a service (SaaS) delivery model.

With applications delivered using SaaS there are three key areas of benefit:

1. **Reduced risk:** SaaS providers house their applications in secure locations and generally deliver the high availability promised in their service level agreements (SLA).
2. **Added value:** by their very nature SaaS applications have to be easily accessed, for those with permission to do so, from anywhere, so that they can deliver the wide ranging access required and data can be easily shared.
3. **Controlled cost:** SaaS applications are provided on some sort of subscription basis, for example a per user, pay per transaction or in some cases a simple flat monthly rate. Therefore, the cost of usage is paid for on an as-you-go basis as opposed to the large upfront licensing cost of many applications delivered on-premise.

Whilst SaaS is most commonly thought of as a way of delivering email or CRM across a diverse workforce or perhaps as the only practical way of allowing users across multiple organisations to collaborate using conferencing tools, it is less commonly thought of as a way to enable IT management, but the benefits of using SaaS for the latter are manifold.

Real time access to a comprehensive, shared, up-to-date database enables:

- Business managers to change the status of users
- IT managers to carry out support and maintenance tasks
- An MSP to share data with its customers
- Access from anywhere at any time via a web-enabled interface
- The running of standard reports that ensure an up-to-date view of the status of remote IT infrastructure and users

Whilst any SaaS provider must ensure secure access to such management tools and must safeguard the privacy of the sensitive data on which they rely, at a generic level there are plenty of benefits to be gained from providing IT management with statistics from anonymised data aggregated across many organisations. For example, what is the percentage of desktop Linux users compared to Microsoft Windows and Apple Mac? What is the most popular web browser? Are organisations installing Windows XP Service Pack 3?

Such a tool also allows IT managers to share the procedures they develop for automated tasks over and above those provided by the vendors, creating a community of interest. In many small businesses IT managers work alone and the opportunity to share ideas and experiences is welcome.

## Conclusion

All businesses, whether smaller or larger than average, are having to manage an increasing diversity of remote users. The tasks that fall on IT managers go beyond just keeping systems running, and include ensuring compliance and helping to meet environment targets. Under this sort of pressure IT managers must be given access to powerful tools.

More and more software vendors are partially or fully adopting SaaS as the preferred way to deliver their applications because their current and prospective users recognise the benefits of doing so in terms of cost control, ease of access and high service levels. These benefits apply just as much to IT management tools as end-user applications.

Whether it is the IT managers themselves or the MSPs they outsource the task to, easy access to the tools of their trade and the data that underlies them is essential. Good use of IT support and management should ensure that in one way at least the businesses they serve are above average—that is in the level of satisfaction and availability they provide to end users and the visibility they provide to business managers regarding the quality, security and value of IT.

## References

<sup>1</sup>Average Inc., Quocirca, March 2008

[http://www.quocirca.com/prep\\_aveinc.htm](http://www.quocirca.com/prep_aveinc.htm)

<sup>2</sup>The distributed business index, Quocirca, March 2008

[http://www.quocirca.com/prep\\_dbi.htm](http://www.quocirca.com/prep_dbi.htm)

<sup>3</sup>Managing the unmanageable, Quocirca, September 2008

[http://www.quocirca.com/ntr\\_rep2.htm](http://www.quocirca.com/ntr_rep2.htm)

## About NTRglobal

Founded in 2000 and headquartered in Barcelona, Spain, NTRglobal has grown to be a worldwide leader in enterprise-grade, cost-effect 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 First Help, 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, customer base, and 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 accommodate 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](http://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](http://www.quocirca.com).