



The data sharing paradox

A Quocirca small business report

September 2011

Small businesses acknowledge that enabling access to data for remote employees and users from external organisations is fundamental to ensuring the on-going efficiency of the processes that drive their businesses. However, they also worry about the risks involved. There is a need to resolve this paradox.

This Quocirca small business report looks at the degree to which small businesses are sharing data today, the ways in which they are doing so and the real and perceived risks. It goes on to look at how these risks can be mitigated.

The report draws on new primary research to look at the scale of the problem supported by data from 350 interviews with organisations with between 3 and about 100 employees in Europe, USA and Australia.

Bob Tarzey
Quocirca Ltd
Tel : +44 7900 275517
Email: Bob.Tarzey@Quocirca.com

Rob Bamforth
Quocirca Ltd
Tel: +44 7802 175796
Email: Rob.Bamforth@Quocirca.com

The data sharing paradox

A Quocirca small business report

Small businesses acknowledge that enabling access to data for remote employees and users from external organisations is fundamental to ensuring the on-going efficiency of the processes that drive their businesses. However, they also worry about the risks involved. There is a need to resolve this paradox.

Sharing data drives business value, but introduces risk	Small businesses acknowledge that enabling access to data for their own employees working remotely and users from third party organisations increases the efficiency of business processes. This rates as a more important benefit than support for flexible working. However, such sharing introduces both commercial and regulatory risk.
Data is often shared via high-cost or high-risk channels	Less than 50% of small businesses have set up their internal file servers to enable external access to data, perhaps being put off by the complexity and costs involved. This means that they resort to email, memory sticks and ad hoc cloud-based tools for sharing. Often this will be uncontrolled and unaudited.
Security remains the biggest perceived threat from using cloud-based apps	The security of personal data and intellectual property has always been and remains the biggest perceived threat from the use of cloud-based applications. However, most small businesses take a pragmatic view of the cloud, increasingly accepting it as a way of procuring and delivering many IT services, including tools for data sharing.
Enabling remote workers means enabling their devices of choice	The range of devices that remote users wish to access IT from is growing. Whilst Windows-based laptops still dominate, the growth in the use of smartphones running Google Android, Apple iOS and other operating systems is set to continue. To this must be added the current rapid rise of tablet PCs, in particular the iPad. Enabling remote and external workers means accepting data access from all these devices.
Either the device must be secure or access to data controlled	One approach to ensuring the security of remote data use is to secure the device itself but the range of devices and the fact they are often owned by employees makes this impractical and near impossible when users from third parties are involved. This means that ways must be found of ensuring sensitive data does not get copied from secure central locations to insecure devices.
There are three approaches to providing centralised data access	The first is to provide access only via secure applications that restrict data being copied to devices. The second is to provide access from the devices to virtual desktops, but there are usability problems on smartphones. The third is via controlled online file sharing services, which is cheaper than enabling access to internal servers and the most pragmatic way of sharing data with users from third party organisations.

Conclusions

All businesses, including the smallest, need to find ways of securely enabling remote access to data for their employees and the users in organisations with which they have shared business processes. Those that do not find effective ways of sharing such data will lose competitive edge. However, those that do share data, but have too little control over it, will be introducing unacceptable levels of risk into their organisations.



Introduction: the data sharing paradox

There is a paradox sitting at the heart of 21st century business processes; the effective sharing of data increases efficiency, but it also increases risk. The efficiency comes through the growing use of mobile electronic devices connected to each other and to centralised information technology (IT) resources, often via public networks. The risk comes through the potential compromise of data, either through loss of devices or interception of the data.

There is direct business risk (information getting into the hands of competitors) and regulatory risk (personally identifiable data entering the public domain, regardless of whether it is compromised or not). The second of these is becoming insidious as the compliance bodies that enforce privacy tighten their grip.

This report uses new primary research to look at the scale of this problem among small businesses (those with between 3 and about 100 employees). The report shows how small businesses currently share data, the benefits they expect to derive from this and the level of risk this introduces. It goes on to look at how small businesses can share data more effectively and how they can mitigate the risks and reduce the costs involved.

Sharing data

When it comes to the use of mobile electronic devices, the benefits cited are often to do with supporting mobile and flexible working via remote access to data and applications. However, when asked specifically about the benefits of providing external access to data, small businesses recognise that this is as much about driving efficiency and productivity as it is about flexible working (Figure 1).

Furthermore, the individuals involved are as likely to be from external organisations as employees working remotely. The majority of businesses need to share data with users from third parties and this need increases as they grow in size (Figure 2).

Figure 1: How valuable is the ability to share data externally, in driving the following:

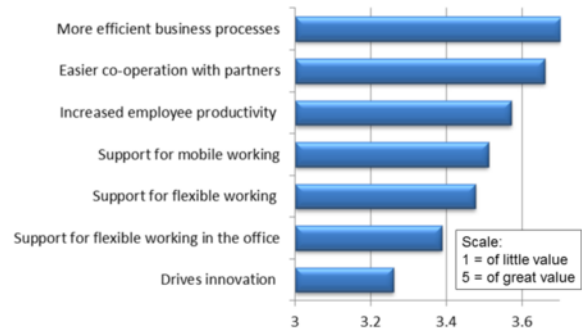


Figure 2: Do you have a requirement to share data stored on your IT infrastructure with outsiders/third parties?

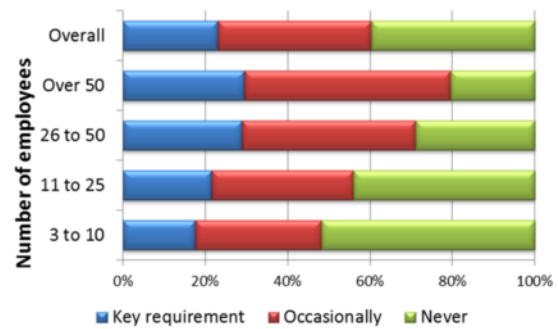
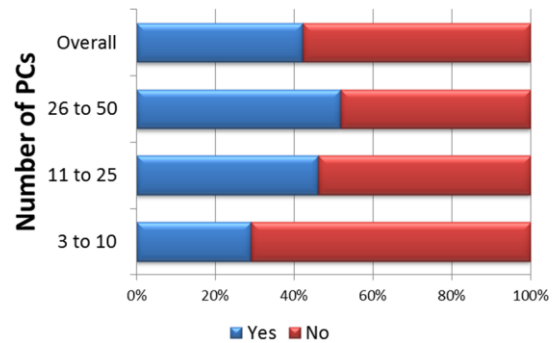


Figure 3: Do you have an in-house file server and use it for the external sharing of data?

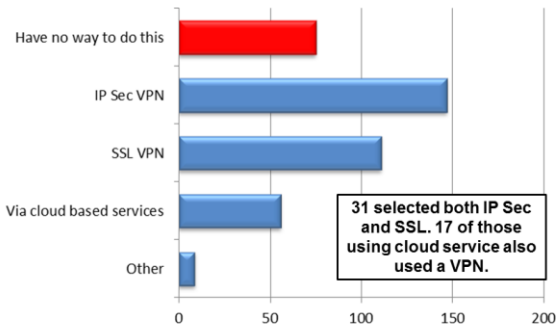


One way of sharing data externally is to provide access to internal file servers. 42% of businesses share at least some of their data this way (Figure 3). The cost associated with this includes that of the file server itself and required software plus annual maintenance charges that can amount to €1,000+ even for the smallest business. On top of this is the cost of providing access to the server from external locations, either via an IP Sec or SSL VPN; 65% of small business run at least one such device (Figure 4). When sharing data in this way, data on the file servers themselves should be fairly secure with the



right user authentication and access protection in place. However, problems can occur when data gets copied from a file server to end-points. Then, to all intents and purposes, it must be considered “in the wild”.

Figure 4: How do you provide access to your IT systems for users who are working remotely?



At least, with a single central file server, access to data can be audited and controlled and, if using a VPN device, it will be encrypted during transmission. However, the majority of data sharing is via other methods. Most small businesses admit that the main way they share data externally is via other means, the most common being email (Figure 5).

Figure 5: The main way data is shared externally (for those that do not use an in-house file server for this purpose)



Email can be audited and controlled, but rarely is, and it must be taken to include non-corporate email channels (“hey, the server’s down, I will send the document via my Hotmail account”). Furthermore, just sending data via email means it now exists on the recipient’s and, possibly, intermediate email servers, an external data store over which the data owner has no control.

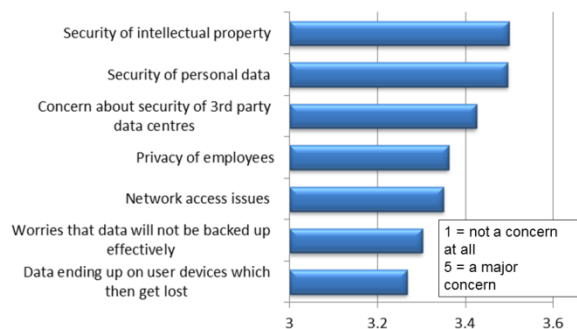
After email there are a host of other methods used. Some are fraught with risk such as sending on portable media or paper in the post. Portable media can be OK if encryption is used, but as the UK HMRC

(Her Majesties Revenue and Customs) case showed, back in 2007, when it is not the consequences can be, at least, highly embarrassing. Four years on, such negligence would almost certainly lead to a hefty fine, even if, as was the case with HMRC, there is no evidence that the data was ever compromised (the CDs used to transfer data were just lost without trace).

Turning to the cloud

Quite a few small businesses report that they use some sort of cloud-based service for sharing data. These include hosted portals such as Microsoft SharePoint, on-demand office tools like Google Apps and file storage services, for example Dropbox. The cost of using these will vary, some even being free, but all are likely to be far lower in cost than running and providing an in-house file server/VPN to do the job. The risk involved will vary depending on the service.

Figure 6: How would you rate the following issues when using a cloud based IT service?



Regardless of the actual risk associated with an on-demand service, the perception of a threat to intellectual property (IP) and personally identifiable information (PII) is rated higher than any other concern (Figure 6). Many other surveys report the same. Quocirca would argue that using a well provisioned on-demand service can be one of the most cost effective and secure ways to share data and that a greater risk is information leaking onto mobile devices.

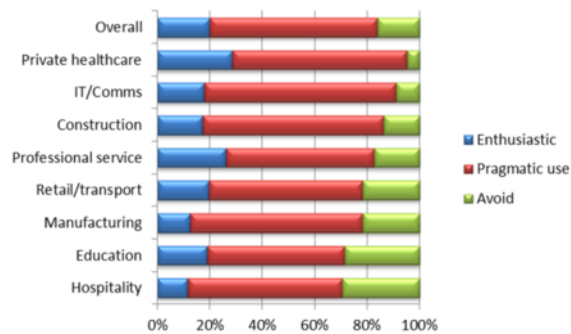
Whether one agrees with this view or not, the fact is that the perception amongst small business needs to be changed to encourage further adoption of such services. However, where there is a will there is a way. Overall, 64% of respondents take a pragmatic



view of using cloud-based services; this was fairly consistent whatever their line of business (Figure 7).

Only 16% said they would avoid cloud-based services altogether. However, even for these most conservative of organisations, such a stance is becoming less and less practical. For example, to participate in the supply chain of many large enterprises, small businesses are compelled to use on-demand trading systems.

Figure 7: What is your stance on the use of cloud based services?



Remote enablement

When sharing data with users working with third parties, there is often little or no control over the devices they will use.

Quocirca has itself been involved in projects that required access to third party data sources in the past. In one case, we were required to use only a laptop provided especially for the purpose. This was expensive for the customer and cumbersome for Quocirca. It meant we had a largely redundant laptop sitting around and, when the task involved need to be passed from one analyst to another, the laptop had to be physically handed over. Most projects are more pragmatic, and ways are found to share data on the personal device of choice.

Quocirca is a small business and its analysts are free to choose the device they use for work, providing it supports a basic set of tools and has a given level of security. In fact, we all have multiple devices, at least two and, in some cases, three or four. This is to support highly mobile working practices and varied working situations. Today, many small businesses face these same issues; lots of remote working and support of multiple devices per user with an increasingly diverse range of operating systems.

87% of small businesses have users that work remotely at some point during the week and this is true across all the countries covered by the survey (Figure 8). 88% report at least some smartphone usage (Figure 9) and, not surprisingly, this increases with mobility (Figure 10).

Figure 8: What proportion of the staff in your organization works remotely at some point during the week?

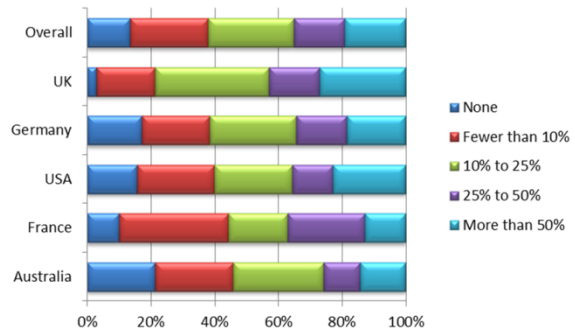


Figure 9: What percentage of your users is using smartphones for business purposes?

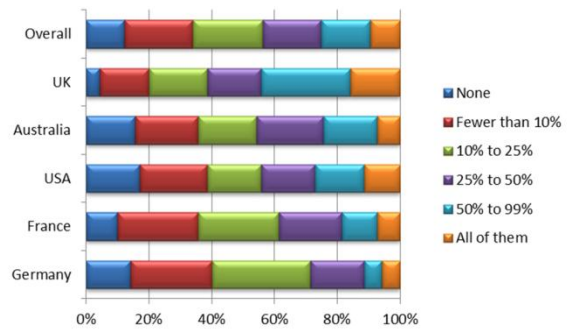
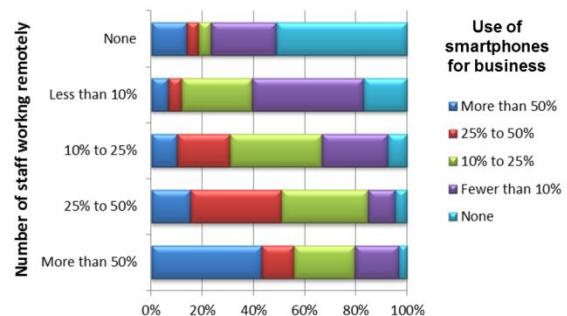


Figure 10: Remote working by use of smartphones



Despite the relative novelty of the latest wave of tablet and slate devices (led by Apple's iPad), 43% of small businesses report at least some of their employees are using them to access IT and a further



29% expect some employees will do so in the next year or so (Figure 11).

A further complication – that is evident from this research and openly acknowledged by CISOs (chief information security offices) from large businesses that Quocirca has spoken to – is that, increasingly, these devices, especially smartphones and tablets, are not owned by the business itself but are their employees’ personal devices. This is part of the so-called consumerisation of IT (Figure 12).

Figure 11: How many of your employees are now using tablet computers to access your IT systems?

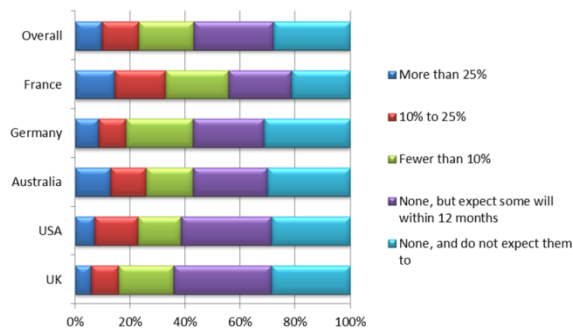
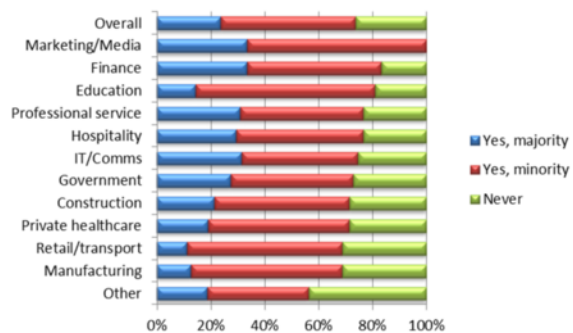


Figure 12: Do you allow employees to use their own devices to access data and certain applications?



Protecting devices; protecting data

There are two approaches to protecting data when access is needed to it from remote user devices. First, only make the data available centrally and control what can be copied to remote devices and by whom. Second, ensure that the remote device itself is secured, i.e. that if the device is compromised or lost, the data on it cannot be accessed.

To achieve this second goal requires that the data stored on the device is encrypted and that the device can be kept free from malware. Both of these goals require a degree of control over the device by the IT department. However, when the device is owned by an employee or an external organisation, this can be hard or impossible to achieve.

This means that, for many businesses, only the first option is practical for the protection of the most valuable data – access must be limited and data only viewable via a centralised service and, when deemed too sensitive, not transferable to the device.

There are three ways to achieve this and each suits a different use case:

1. Provide access to applications that allow data to be viewed and updated, but not copied. For example, just because you allow employees to read email remotely does not mean their content should necessarily be copied to a device. However, by default it often is; at least the email headers.
2. Provide a virtual desktop environment for the user. Here, they are not actually processing data on the device, but the device is simply an access tool to a desktop that is available anywhere the user can get online. There are limitations with this approach when it comes to smartphones (due to screen and keyboard size), but the software that enables this is improving fast.
3. Provide direct access to central data stores. Here, with the right products, access can be provided to view files, with caveats. Public domain documents (e.g. market materials) can be freely copied and used later offline, whilst restricted documents can only be viewed whilst online.

No one of the above approaches will necessarily solve all the needs of any businesses, but a mix of them should do.

The third option is particularly useful when sharing data with users from third party organisations. In most cases you would not want to run a virtual desktop for such users and would not want them to be users of the same range of applications that you may make available to employees.



Side benefits

The devices of external users may be beyond the control of the average small business's IT managers (if they exist in the first place!) So, having an easy, centralised way to share data with them securely is essential.

However, when it comes to the devices of employees themselves there is a side benefit provided by many central file sharing services – data backup.

The way such services work is that, when it is accepted that certain content can be stored on the user's device, the device can synchronise with that data as and when it changes. So, if one user changes a file of interest to a second user, the updated version is copied to their device next time it is online.

In reverse, this means that content created on the device itself can be backed up on the central store on a regular basis. Whether this is data created for business or personal use, such capabilities will be valued by the users. For smartphones this may be mainly photos, but for laptops and tablets documents prepared whilst working remotely can be securely copied to a central location.

Most small businesses are either relying on backups to in-house file servers (which in most cases will just be for Windows-based laptops) or just leave it to their employees (Figure 13). Few are using an online backup service, some of which are able to address all or most of the wide range of devices now in use for remote working.

Being able to do this ensures copies of newly created content are backed up in a timely manner. It also means that it should be possible to restore all data to a replacement device when the original has been lost or stolen relatively quickly (Figure 14). However, bandwidth considerations may make this impractical to achieve for remote users and sometimes it is more practical to ship new images on removable media with data restored to them rather than restore direct to the new device itself.

Figure 13: How do you backup up data from user devices?

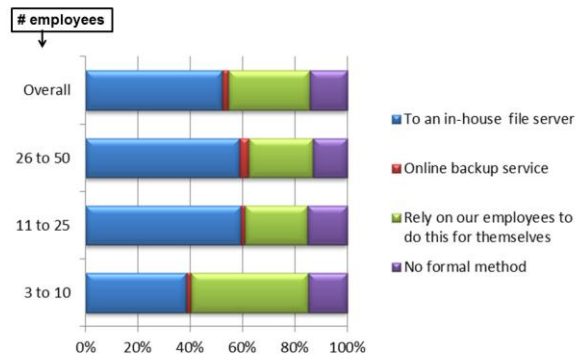
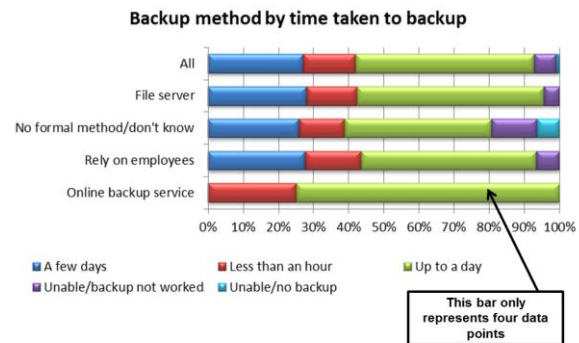


Figure 14: When you last had to replace a PC, how long did it take you to restore the data on it?



Conclusions

All businesses, including the smallest, need to find ways of securely enabling remote access to data for their employees and the users of organisations with which they have shared business processes.

There are a number of ways of achieving this. One of the most flexible is an on-demand file sharing service. This is cheaper and less complex than running and providing access to an internal server for this purpose. It is also easier to implement for employees using their own devices, or for external users, than deploying virtual desktops or specific applications to achieve the same end.

Those organisations that do not find effective ways of sharing such data will lose competitive edge. However, those that do share data, but have too little control over it, will be introducing unacceptable levels of risk in to their organisations.



Demographics

The research behind this report was based on interviews with 350 organisations across 5 countries. The breakdown of the sample was as follows:

Figure 15: Countries covered by survey

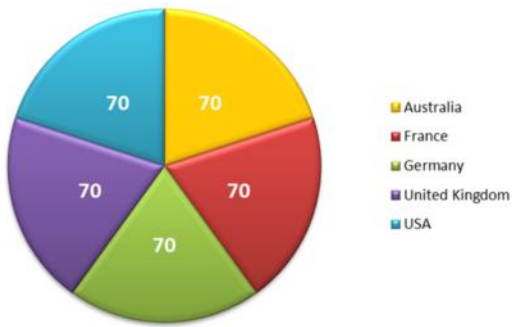


Figure 16: Business sizes covered by survey (all had 50 or less PCs)

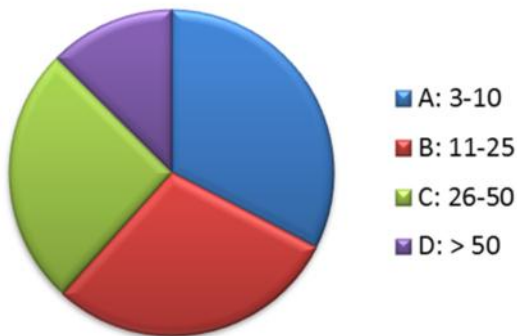


Figure 17: Number of PCs managed by organisations covered by survey

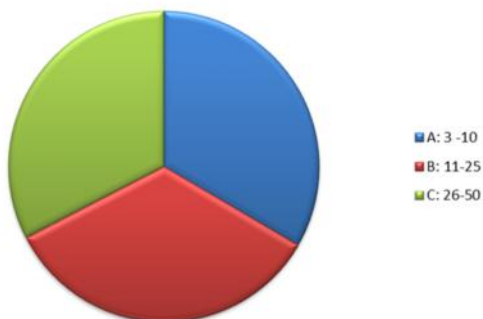


Figure 18: Business sectors covered by survey

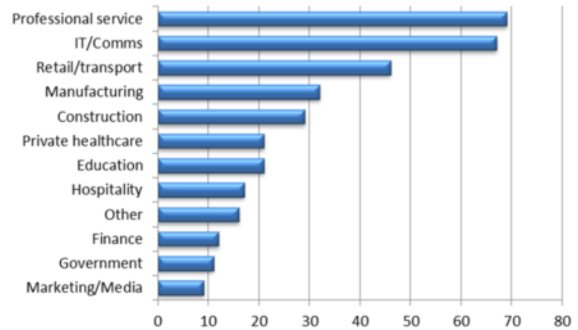


Figure 19: Job role of respondents

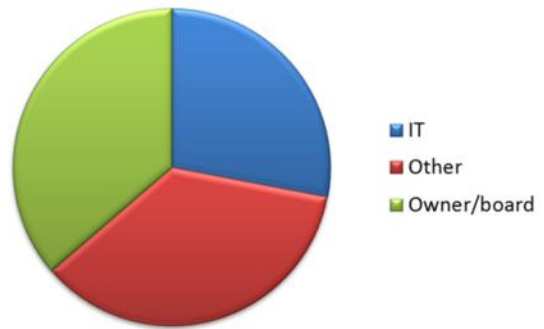
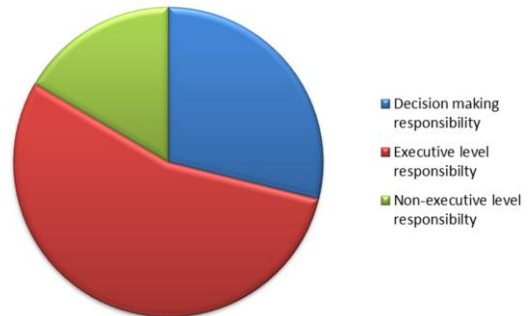


Figure 20: IT decision-making responsibility of respondents



About Trend Micro

We Secure Your Journey to the Cloud. As a global leader in cloud security, Trend Micro develops Internet content security and threat management solutions that make the world safe for businesses and consumers to exchange digital information. With over 20 years of experience, we're recognized as the market leader in server security for delivering top-ranked client, server, and cloud-based data protection solutions that stop threats faster and protect data in physical, virtualized, and cloud environments. By providing security "from the cloud" with our industry-leading Trend Micro Smart Protection Network™ and security "for the cloud" with our server, data storage and encryption technologies, we're the best choice for Securing Your Journey to the Cloud.

A History of Innovation. Since 1988, Trend Micro has pioneered innovative technologies and services that protect users against threats on new and emerging platforms and devices. Each paradigm shift in the way people communicate and conduct business online has introduced significant benefits to users while introducing new security challenges. Trend Micro was there from the start, being the first to extend threat protection from the desktop to the server and to the Internet gateway. And as cloud computing revolutionizes the way people share digital information, making access to information and computing power easier, faster and more affordable, Trend Micro is prepared. By extending security to virtualized and cloud-computing environments, businesses and consumers can securely take advantage of new technologies in the public or private cloud.

Always Focused on Our Customers' Needs. Trend Micro delivers a range of security solutions and cloud-based services that provide maximum security, flexibility, and performance with minimal complexity. Because needs evolve, and one size does not fit all, Trend Micro offers a choice of software, virtual gateway appliances, and Security as a Service offerings for consumers, small businesses and the enterprise. And because we recognize that malware isn't your only problem, Trend Micro also safeguards your critical data from endpoint to cloud with comprehensive data protection capabilities like data loss prevention, encryption, and file back-up and recovery. Your physical, virtual, and cloud servers are also protected from vulnerabilities and malicious activity through our server and application security for dynamic data centers.

Additional information about Trend Micro and its products and services is available at TrendMicro.co.uk. Or find us on Twitter in your country.



Securing Your Journey
to the Cloud

REPORT NOTE:

This small business research report has been written independently by Quocirca Ltd.

It presents new research into the current data sharing practices amongst SMBs in Europe, USA and Australia.

Quocirca would like to thank Trend Micro for its sponsorship of the report and all the survey respondents.

The report draws on the research findings and Quocirca's technology and business knowledge.

It provides advice on the approach that organisations should take to share data effectively and securely.

About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with first-hand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of an organisation's environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to provide advice on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, Microsoft, IBM, O2, T-Mobile, HP, Xerox, EMC, Symantec and Cisco, along with other large and medium-sized vendors, service providers and more specialist firms.

Details of Quocirca's work and the services it offers can be found at <http://www.quocirca.com>