

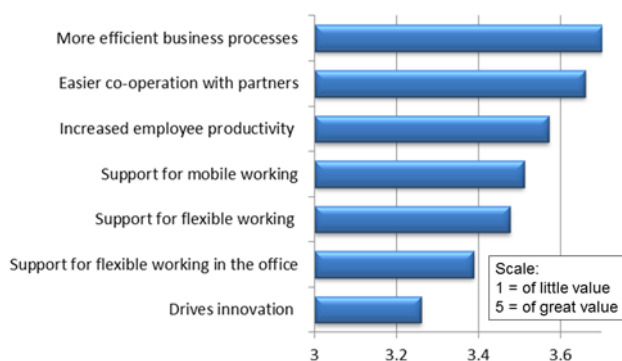
Mobilising SMB security improvements

Bob Tarzey, Analyst and Director

Quocirca Comment – October 2011

There is a paradox at the heart of 21st century business processes. The effective sharing of data makes these processes more efficient but carries an inherent risk that the data may be compromised. This applies both to providing access to data for mobile and remote employees and the sharing of data with external users. In the latter case, Quocirca research has recently suggested that improving the way business processes operate, among SMBs at least, is the primary motivation for such sharing (figure 1).

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

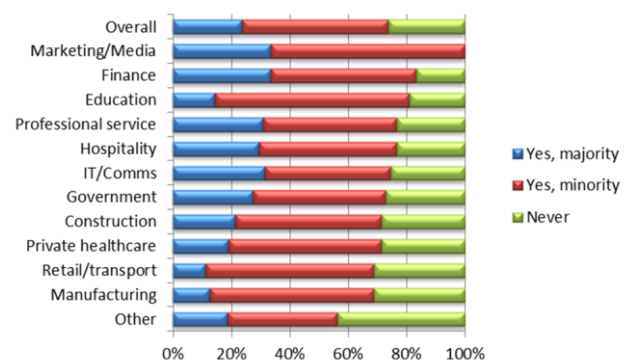


The risks involved with sharing data can be mitigated. How this is best done depends on a number of factors, including the user, the device, who owns the device, the application involved and the type of connection. Historically, users have gained access to centrally managed data and applications via employer-owned and -managed mobile PC devices using VPN connections to internal servers.

Today, many SMBs do not have their own physical servers, often turning to cloud, and while VPN access can be set up relatively easily on employer-supplied laptops, it is harder if external users are using their own devices. It is also more likely to involve smartphones and tablets than traditional PCs, due to consumerisation (figure 2). In theory, VPN access can be provided for these, but this creates a host of management issues, such as

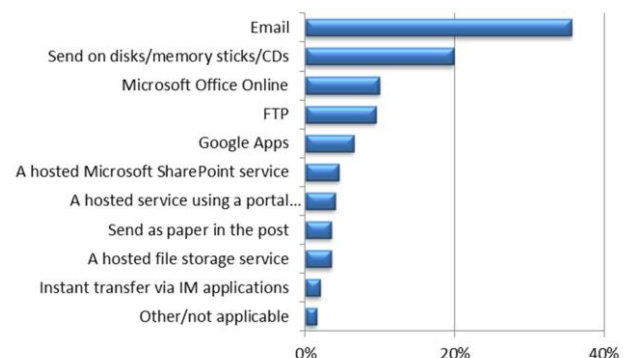
those surrounding the licensing of corporate software on externally owned devices.

Figure 2: Do you allow employees to use their own devices to access data and certain applications?



Regardless, business data is at risk, as it is most commonly shared using ad hoc methods such as email and memory sticks, over which the business has little control (figure 3). Not only can data be shared insecurely, it can also end up on those mobile devices owned by employees or outsiders, and be completely unprotected if such devices are lost or stolen.

Figure 3: The main way data is shared externally (for those that do not use an in-house file server for this purpose)



There is no silver bullet here, but there are ways of reducing the risks. A business must take as much control of its data as it can. It is possible to secure mobile devices themselves using

encryption and host-based end-point security, but again there is the problem of device ownership. It may make sense to allow employees to use their own devices - the employees will probably do so anyway - but managing the devices, and installing and licensing software on them, can be costly and difficult.

A better way of reducing risks is to impose centralised controls. That is, provide a means of accessing and sharing data that is easy to use and requires minimal modification of the user's device. There are three basic approaches:

1. Virtual desktops. Here, data is not actually processed on the device, which is used simply to gain access to the desktop, anywhere the user can get online. There are limitations to this approach when it comes to smartphones due to screen and keyboard size, but software that makes this a better user experience is improving fast (see, for example, Citrix Receiver). However, this option still requires some locally installed software.
2. Provide access to applications that allow data to be viewed and updated but not copied. Just because you allow employees to read email remotely does not mean the actual content has to be copied to a mobile device. Such applications can be provided through the creation of corporate app stores that support the range of devices employees want to use. Staff can download from there, providing their consent for installation in the process.

3. Provide direct access to central data stores. Using this approach, access can be provided to view files through the right products, with caveats. Public domain documents such as marketing collateral can be freely copied and used later offline, while restricted documents can be viewed only online, helping to protect an organisation's intellectual property. No local software is needed to do this. Offerings here include portals, such as Microsoft SharePoint, or specific file-sharing/backup services, such as Trend Micro SafeSync.

One thing is certain: no business can ignore the mobility revolution. All need a strategy to manage it. Those who embrace it with controls in place will benefit in the long term, while those who bury their heads in the sand will lag behind.

This article first appeared on <http://www.channelweb.co.uk> and in the print edition of Computer Reseller News (CRN)

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 advise 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.

Full access to all of Quocirca's public output (reports, articles, presentations, blogs and videos) can be made at <http://www.quocirca.com>