

Managing the risk for mobile IT users

Bob Tarzey, Analyst and Director

Quocirca Comment

The increasing reliance being placed by businesses on mobile IT access will nearly always lead to increased risk, at least in the short term. One of the main reasons for this is that the growth in use of mobile devices is often ad-hoc and unplanned. Of course the way mobile devices are deployed varies; the allocation of laptop computers and BlackBerry smartphones may well be planned, whilst the use of iPads and Android smartphones may be ad hoc, driven by users with their own devices.

One reaction could be to attempt to block all unplanned usage of devices. However, this is not necessarily desirable or practical. There are many benefits from allowing remote access; the flexible working they enable mean employees can be more responsive and that can lead to more efficient business processes. Try blocking access from their devices and an employee will find a work around, sending an urgent message to a customer may be done via an open social network rather than the corporate email system, where the communication can be archived and is auditable at a later date.

What risks arise from the use of mobile devices and how can their use be controlled, so that the benefits can be realised and the threats mitigated? Before addressing this it is worth pointing out that there are two broad approaches to putting controls in place:

1. On the device itself (which may be limited depending on ownership)
2. Centrally, protecting the applications and data being accessed from mobile devices.

There are four broad categories of risk – access, data, malware and business continuity. This article details how each of these can be approached and concludes with a fifth issue; an end-point management regime is needed to pull them altogether.

Security of access

This requires addressing access to the device itself and access to the network resources that the user is permitted to use. With any device a

passcode for access can be put in place; that leads to all the usual problems with password management – users forgetting them and the need to reset them.

However, the bad guys find ways around device level passwords, so additional strong authentication of the user is desirable; especially if sensitive data is to be stored on a device. Examples are bio-metrics (most commonly a finger prints), hardware tokens or a mechanism for distributing one time passwords. Strong authentication has mostly been used for laptop device access and not smartphones and tablets. In fact, smartphones can be used for enabling strong authentication of access to laptops (see below). However, with the increasing power of these devices perhaps they should require strong authentication too.

It need not be the case that gaining access to the device itself opens up the available network resources, although in some will deem this enough to do so. Others will require secondary authentication for opening up a VPN connection or gaining access to applications. Here, the management overheads need to be balance against risk. Too many passwords to remember, to many times they get forgotten. So it makes sense to use the mobile device to authenticate access to a single sign on system, but get this wrong and there is a lot at stake.

To counter this there are a range of additional measures that can be taken. These include:

- Hardware recognition – only allowing access from known devices that can be recognised through a range of characteristics or an agent installed on the device.
- Geolocation – using IP address analysis of GPS software to identify the user's location and decide if this is as expected; a UK based sales person should not be requesting access from Moscow!
- Out of band authentication – for example, sending one time passwords via an independent device to the one being

authenticated (e.g. to mobile phone to authenticate a laptop).

Security of data

Businesses worry about two types of data, with respect to security. First, there is intellectual property (IP), keeping this safe is key to competitiveness. Second, there is personally identifiable data (PID); it is a business's interests to keep much of this confidential too. However, PID is also what regulators take an interest in and many cases brought against businesses are for failure to protect PID are through the loss of unsecured mobile devices.

On the device itself, the ultimate way to ensure data is protected, should the device be lost or stolen, is to encrypt stored data. However, there are caveats. Encryption introduces management overheads for two reasons; first there is a danger that data can be lost forever if encryption keys are forgotten – management tools can provide a backup mechanism through the secure assignment and storage of keys. Second, encryption will only satisfy regulators if it can be proved a lost device was encrypted, which requires the process of enabling encryption to be audited.

It must also be recognised that encryption is not the be-all-and-end-all. Data is only ever of use if it can be decrypted and used. A user may choose to do things with decrypted data, which leads it to end up in the wrong hands, for example copying to unencrypted storage devices, printed or sent by email. So to be fully secure end-point security software can be deployed on the device itself to control what the user can do.

Perhaps the best approach is to making sure that confidential data is never stored on mobile devices in the first place by enabling only for access and viewing, not for storage. There are caveats here too – first the benefits of the user having the device, from a business perspective, can only ever be realised when the user is online. Second, users can create data on the fly, for example making notes following a customer meeting.

A final measure that can be taken is to put in place the ability to remotely disable and/or wipe devices. From the point of view of data protection, if encryption is in place then this is a "belt and braces", approach. However, being able to remotely disable devices ensures on-

going connectivity and calling charges are not incurred.

Malware protection

Many consider it irresponsible not to have anti-malware software on user end points, but actually, much of the necessary protection can be provided through central controls that limit what ends up on a device in the first place. Most obviously, it makes sense to filter email traffic before it reaches a user's device, however this is done, server based software, a network appliance or a cloud based service; the user's corporate email should be clean.

Such controls can be extended to general web access, forcing access via a central proxy that checks for URLs with a bad reputation and web borne malware. Such proxies can also be used to extend web usage policy to remote users, for example limiting access to social networks. To make such web access controls work, the user must be blocked from opening up other uncontrolled internet connections, for instance via a mobile service provider. This is of course limiting what the user can then use the device for and is not practical for user owned devices.

At the end of the day many will only feel comfortable if there is protection from malware on the device itself, as part of an end-point protection suite; users can still potentially load data from USB devices or CDs of unknown origin. Most malware is still aimed at Microsoft Windows, because of its widespread use. However, as other operating systems become more common it will become practical for data thieves to attack them too. Security software suppliers are only just starting to roll out end point protection suites for smartphone and tablet operating system and businesses are slow to deploy them. The first major compromise of Google Android, Apple iOS or some other non-Windows based system should change that.

Business continuity

The flexible working enabled through the use of mobile end points and the consequent increased efficiency of business processes, will only happen whilst the end-points and the network access they requires remains available. The theft and loss of end-points is inevitable and procedures must be in place for the rapid replacement and re-provisioning of end points. It is worth pointing out that the trend for employees to use personally owned devices to access IT has a

positive aspect when it comes to risk – they will take more care of something they own than something supplied by their employer.

The urgency to replace will depend on the job-role of a given user. A field service engineer who can no longer log faults because their smartphone has been dropped in a puddle (maybe they should have had water proof one in the first place) may be given priority over salesperson who can longer read emails because their BlackBerry has been stolen (they can always visit an internet café).

However, replacing the device itself is not enough, if the creation and storage of business data on the device is allowed, then this must be restored to. This can only be done if a rigorous backup regime has been put in place. In the past IT managers often waited until devices came back on to local area networks to perform backups. The advent of high bandwidth remote connectivity and cheap storage has led to a proliferation of cloud based services that provide continuous data protection. From consumer to large enterprise, if data is valued, there is little excuse these days for it not being regularly backed up.

Ensuring a user can do their jobs remotely and cost effectively requires that their devices are connected as often, and as cheaply as possible. This requires working with network access providers that provide multiple means of communications, reverting to the cheapest, fastest method whenever possible. For example, using public wireless access points by default and only switching to more expensive mobile networks when there is no other option.

End point management

Policing encryption, making sure backups are performed and anti-malware software is up to date and ensuring timely re-provisioning of lost devices, across communities of tens, hundreds or thousands of mobile users is challenge for any IT department. However, the management tools for achieving this have been evolving rapidly. They allow routine tasks to be automated across groups of devices or users freeing IT staff for other tasks. Such tools can be deployed on-premise but are also increasingly available as cloud based services.

That said; IT departments may still find the task daunting. Many have turned to managed service providers (MSPs) to provide data centre and desktop management services and some MSPs are now starting to provide mobile device management services too. Working across multiple customers, MSPs can scale their services up to cover tens of thousands of end points and build up the experience and expertise to ensure service levels that many IT departments would struggle to achieve for themselves.

Whether it is carried out in-house or outsourced, failing to put in place a management regime for mobile devices and thus mitigate much of the risk they represent is something that no business should overlook.

*This article first appeared on
<http://www.globaletm.com>*

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>