

A Toranet White Paper

Published: November 2011

Achieving Secure Mobility



Table of Contents

Introduction 3

Habits of a Nomad 3

Compliance Impact: Data Protection Act..... 4

Threats: Unprotected Data on the Move 5

USB Devices – Creating Policy Controls 6

Smart Mobile Devices – Manage, Secure, Enable..... 7

Effective Wireless – Achieving a Secure, Available, High Performance Solution 8

Secure Mobility – Drawing Reasonable Conclusions 10

If you have feedback, questions or comments about this white paper.

General enquiries can be sent to info@toranet.net and phone calls are welcome on 01252 811336.

Emails can also be sent to the author directly at chris.bice@toranet.net. Website: www.toranet.co.uk

Introduction

We no longer need to be working at our desks to communicate with our colleagues and business partners. The applications that support us in our roles are accessed increasingly from smaller, more portable devices like tablets and smartphones. This means we can respond to email and voicemail, access databases and other business resources wherever we happen to be.

With opportunity comes risk, however, and this stands true for mobile working. This white paper looks into the security, performance, and management considerations of an increasingly mobile workforce, and offers best practice advice and solutions to support mobile initiatives. The topics discussed are relevant to mobile workers within their normal place of work and also whilst away from their offices.

Habits of a Nomad

Organisations with home-based employees, distributed offices or campus institutions like schools, universities and hospitals, are creating a generation of nomadic workers. Most companies have at least some workers that spend little or no time in the office.

When armed with a laptop and/or smartphone, and access to a wireless network or 3G service, a permanent desk in the office becomes somewhat redundant.

For all the productivity and efficiency gains though, nomadic workers introduce new security risks that need to be understood and acted upon. For example, they will likely have their log-in credentials written down, and be more inclined to use portable storage devices like USB drives. Many will use corporate smartphones for personal use, or use personal devices for work purposes.

These same devices will be used to access the internet over unencrypted links, whilst any apps or data downloaded are unlikely to be checked by content filtering systems for malicious or inappropriate software. Over time these portable devices will become a storage repository for corporate data. Not only should consideration be given to the risk of commercially valuable information falling into the hands of a competitor, there is also the risk of corporate data being lost that cannot be recovered from a backup.

Left to our own devices most tend to take the least line of resistance. This means good practice is often overlooked if there is no way to enforce corporate policy and govern user behaviour.

Compliance Impact: Data Protection Act

Good practice, or lack of it, in mobile strategies, can impact an organisation's compliance stature.

There are numerous cases of councils, government bodies and increasingly, private companies, found in breach of the Data Protection Act, as a result of USB or mobile devices being lost or stolen.

A fine of £150,000, recently handed out by the Information Commissioners Office (ICO) to Ealing and Hounslow Councils after two laptops were stolen from an employee's home, demonstrates the consequences of not complying with the Data Protection Act.

In this instance, the laptops contained personal information relating to residents of both councils. Hounslow Council was guilty of passing personal information to Ealing Council without a written contract in place. Ealing Council was guilty of issuing unencrypted laptops to employees.

It isn't just councils that have found themselves in trouble with the ICO either; there are numerous examples of estate agents, retail outlets and mobile phone operators, for example, having received (very public) fines for inappropriate use of personal information.

Principles of the Data Protection Act

There are eight principles of the Data Protection Act that companies should follow to ensure they comply with the guidelines, specifying that personal data must be:

1. Processed fairly and lawfully
2. Obtained for specified and lawful purposes
3. Adequate, relevant and not excessive
4. Accurate and up to date
5. Not kept any longer than necessary
6. Processed in accordance with the "data subject's" (the individual's) rights
7. Securely kept
8. Not transferred to any other country without adequate protection in situ.

Further details are available from www.ico.gov.uk.

Threats: Unprotected Data on the Move

Take an average employee at an average company on an average day and there is every possibility they will represent a data security threat to their employer, their business partners or themselves. We should all give consideration to the following questions:

- How many people have left an unencrypted USB stick at a meeting, in a taxi or on a train?
- What data are employees carrying on unencrypted USB storage devices?
- How many people protect sensitive data on their smartphones with a password to unlock it?
- How many smartphones utilise a software agent to effectively block malware?
- How many mobile devices are sending sensitive data openly across public networks?
- How many companies audit employee's personal and corporate devices to establish the presence of sensitive corporate information?
- How many mobile devices are regularly backed up to preserve valuable data?

A recent study commissioned by security software provider ESET¹ found that 55% of iPhone users do not lock their device. Blackberry users offered a similar percentage.

This relaxed approach to security is a concern when factoring in the statistics. For example, it is widely reported that a mobile phone is stolen every 12 seconds somewhere in the UK. Furthermore, every year around 50,000 mobile phones are left in the back of London taxis.

Similarly, mobile malware is an increasing problem. The first reported virus to target Android devices (currently the fastest growing smartphone operating system) was reported in August 2010: since then there have been over fifty separate attacks.

Nor is Apple invincible, which has seen virus attacks on its iOS smartphones in the past couple of years. Apple has since increased device security with version 5.X of their OS, but it is still considered by some to be less secure than RIM's Blackberry.

The risk metrics will change across the various smartphone platforms as new OS versions are released and evidence of new threats emerge, but there is little doubt that smartphones and tablets will become a greater target for malicious software as they grow in popularity. Indeed, McAfee's Q4 2010 quarterly threat report² states that smartphone malware increased by 46% in 2010 compared to 2009.

The risks associated with laptop and tablet users are also a focus of consideration for organisations and their employees.

Many industry organisations support the belief that approximately 60% of corporate data resides on laptops. So while the loss of a laptop is frustrating, for many companies it is the value of the data lost that will be of most concern. Moreover, if this data is of a personal nature, then it may also result in the breach of the Data Protection Act. These same concerns apply to USB storage devices.

¹ ESET Feb 2010: <http://blog.eset.com/2010/02/10/are-you-as-smart-as-your-phone>

² McAfee Q4 2010 Threat Report: <http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2010.pdf>

USB Devices – Creating Policy Controls

Case study

Norman Defence Systems is a Scandinavian company that specialises in proactive content security solutions and forensic malware analysis tools. In July 2011, when presenting alongside Toranet at a series of road shows, David Robinson, General Manager of Norman Defence Systems UK, walked through the results of an IT security assessment carried out at a British primary school.

Over a period of one month, Norman collected USB usage metrics on a small selection of computers from different areas of the school.

The results showed that 2.8Gb of data comprising various files including XML data, PDF's, images, presentations, spreadsheets and other documents had been read from and/or written to removable media devices. When including auto-saves this amounted to over 5000 separate reads/writes in the month. Much of this activity took place during lunch time or out of school hours.

When explored, the data was found to contain personal data pertaining to staff and students, as well as administrative and teaching materials. This is an important point as the school, as well as any other organisation that holds personally identifiable information, must comply with the Data Protection Act. For organisations that fail to do so the penalties can be severe.

The results of the Norman assessment should be concerning for any organisation that doesn't have effective controls on the use of portable storage devices. It is alarming to consider that the activity recorded by Norman came from just five of the primary school's 100+ computers.

Creating Policy Controls

Some organisations ban the use of USB storage devices completely. This will mitigate associated risks but will also limit the value that can be derived from mobile working. The good news is a policy can be created and the controls do exist to enforce it. Some suggested policy and control options might include:

- Permit only files of certain types to be copied to or from storage devices
- Allow only specific storage devices to be used and reject others automatically
- Enable only authorised users to use portable storage devices
- Identify specific times when portable devices can be used to save or access files
- Set a limit on the amount of and type of data that can be copied onto portable storage devices
- Record every file that is copied to or from a portable device to provide a historical audit-trail.

Smart Mobile Devices – Manage, Secure, Enable

As identified previously in this paper, the security issues to consider when implementing corporate or employee-owned smart mobile devices are:

1. Unsecured corporate data on the device
2. The use of public Wi-Fi to send unencrypted data
3. The growth of mobile malware.

Like any computer, it is possible to monitor and even restrict the data that is allowed to reside on mobile devices. If a device does not comply with the specified policy then it can be dynamically prevented from connecting to corporate services. For example, a smartphone may need to have a particular version of its operating system or possess the ability to encrypt its data.

Manage, Secure, Enable

There are a number of independent management capabilities that can be deployed across many of the popular smartphone and tablet platforms, and which also support laptops. These provide IT management with the ability to govern these devices remotely and ensure that employees proactively conform to corporate policies. Tools can be deployed that provide:

- Antivirus and anti-malware
- Anti-spam
- Personal firewall
- Loss and theft protection
- Backup and restore capabilities
- Application monitoring and control.

Add secure VPN encrypted remote access and the device starts to look a lot safer. All these facilities are readily available in commercially available software and whilst they are gaining interest, there are still many users without adequate protection. The reality is that many companies and individuals will learn of these threats the hard way before choosing to address these areas of weakness.

Juniper is one such company that has taken a holistic approach to the issues presented by the increasing use of smart mobile devices and mobile workers. Its solution is used to provide assistance in three core areas:

1. By providing laptops, tablets and smartphones with a secure remote access facility
2. By protecting laptops, tablets and smartphones from malware
3. By providing IT management with a mobile device management (MDM) platform to manage and control these devices.

This solution also supports the increasing trend for corporate use of personally owned smartphones, tablets and laptops, often referred to in the industry as Bring Your Own Device (BYOD). Employers need effective ways to govern the data on these devices while they are being used by employees and especially when employees leave or the devices become lost or are stolen. It can be used to secure corporate data on personally owned devices by using remote wipe and remote audit of the content contained on employee's devices.

Effective Wireless – Achieving a Secure, Available, High Performance Solution

Without wireless networks, connectivity for mobile workers would be limited. This is especially the case when considering campus and office mobility. While 3G can be used for internet access, accessing corporate services requires Wi-Fi. It is important to remember that if a wireless network is used to access the internet that users will receive at least the same security and protection as LAN users. Wi-Fi is also likely to be considerably cheaper to operate than 3G.

Since wireless is increasingly the access layer of choice, users will expect it to be of equal availability and performance to Ethernet. Should the wireless network be unavailable for whatever reason, organisations need to consider the impact on their employees, productivity and customers.

When wireless networks were first introduced there was much criticism about their lack of security controls. Since 2004 when the 802.11i security standard was ratified, however, the initial technological security issues have been addressed.

Despite this and the subsequent innovations from leading manufacturers, wireless networks remain a security risk for many organisations. It is important to note that this is not a criticism of wireless network technology, but an acknowledgement of inadequate practices used in some companies.

Implementing a Secure, Available High Performance Solution

If you're thinking of implementing a mobile strategy at your organisation or reviewing current initiatives, it is worthwhile checking the foundations are in place. With many more devices accessing the network, resilience, security and performance will be of concern. Some best practice tips and considerations for implementing and managing a secure, available and high performance WLAN therefore, include:

Remove single points of failure - When downtime cannot be tolerated then a highly available wireless network is needed. This is one in which individual wireless controllers cannot be a single point of failure. Many wireless providers now offer solutions to this. For example, Juniper's clustering of WLAN controllers allow for 'hitless failover' and in-service upgrades with zero-downtime. This innovation has a direct impact on improving service availability. The controllers in a cluster do not need to be located in the same data centre which allows for site-wide redundancy to be achieved.

Bandwidth - Even an always available network needs to perform appropriately. The bandwidth provided by 802.11n allows for 300Mbps and even more at its theoretical maximum. The throughput available is not radically different to that offered by wired networks in some organisations.

Load balance - The best WLANs are clever enough to load balance across multiple access points which helps prevent a single AP becoming a bottle-neck. Furthermore the data can be offloaded by these APs directly onto the network without it needing to be routed through the controller. This is called distributed switching and, together with controller clustering and AP load-balancing, combine to create a high performance WLAN.

VPN authentication - Publicly accessible Wi-Fi such as that provided by an internet café can leave users susceptible to data leakage, unless a VPN tunnel is used to encrypt their data. Strong authentication is a

Secure Mobility – A Toranet White Paper

sensible precaution when connecting to corporate resources and web-based services from public networks.

Apply permission based access - In most organisations there will be various groups of users – ranging from employees, temporary workers and visitors – each requiring different access rights to systems, data and other resources as appropriate for them. With most wireless networks, permissions can be set for each group, and even individuals, from within the administration console of the wireless network.

Update shared wireless keys - If a shared key is used to connect to the wireless network, ensure that it is updated regularly. If not, then disgruntled ex-employee or visiting contractor could sit in the car park and continue to connect to the WLAN. The highest user authentication level is based on 802.1x and most, if not all, organisations should be using it.

Wireless network technology continues to attract innovation, and vendors regularly add new features to aid the management or reduce the cost of Wi-Fi implementations. For example Juniper's wireless access points can now be used as a remote spectrum analyser, meaning administrators needn't visit a location to investigate RF interference issues.

Secure Mobility – Drawing Reasonable Conclusions

As demonstrated by the well documented growth in smartphone and tablet use, the trend for mobile working and use of mobile devices in a corporate environment is increasing exponentially. Indeed, managing mixed mobile estates and implementing mobile strategies feature highly in Gartner's Top Ten Strategic Technologies for 2012³.

As identified in this paper though, there are some very real security threats, not to mention the haunting spectre of the ICO, which can negatively impact your mobile strategy and/or your organisation. It is likely that the ICO will continue to identify instances where the Data Protection Act has been violated, for example, before publicly handing out large fines.

However, it's important to avoid a natural inclination to enforce total network lock down (isn't that how security has always worked?!), as this will simply prevent the productivity benefits you aim to achieve. So whether you're refreshing an existing mobile strategy or starting from scratch, try to balance risk versus availability, and security controls versus employee requirements to do their job.

That said, only part of the security issue is technological: it is also necessary to address the weaknesses attributed to employee misuse and poor processes. This means the most effective approach is to adopt a strategy that considers people, process, and technology. Many of the solutions we've discussed in this paper address all three areas.

Alongside your security review, it is wise to consider network connectivity. With the exception of laptops, few mobile devices have Ethernet ports. Ad hoc consumer grade Wi-Fi zones in your organisation will struggle to deliver the Ethernet-like performance employees have grown accustomed to. As Wi-Fi becomes the primary access layer, it's critical to ensure your WLAN can perform on demand – resilience and quality of service should be high on your agenda.

In this paper, we've outlined the challenges and threats associated with mobile working, and provided best practice advice and solutions to the issues raised. Whilst we hope you found this paper useful, we welcome the opportunity to discuss in greater depth the vulnerabilities raised in this document with IT leaders interested in establishing a greater understanding of this topic.

Toranet in partnership with Norman and Juniper can help to minimise the risks associated with remote and mobile workers.

³ Gartner's Top Ten Strategic Technologies for 2012, 18.10.11