MWR INFOSECURITY

CPNI
Centre for the Protection of National Infrastructure

Mobile Devices

Executive Briefing Paper

February 2013

Introduction

Modern working practices have seen radical changes in just a few short years. Today, business is increasingly likely to be mobile – conducted using devices that might not have existed even five years ago. As such, new and exciting ways of working have evolved very rapidly and while this can bring many benefits to a business, there are also new risks that need to be appropriately managed.

This document is intended as an overview for senior executives of the various risks (and opportunities) that mobile working introduces – and of the specific policies and controls that can be used to mitigate these risks.

Also available from CPNI and MWR are two further white papers: a more technical summary for project managers, plus a detailed guide to help 'implementers' navigate the complexities of designing a robust mobile devices strategy.

MWR would like to acknowledge the help and support of CPNI in producing this Mobile Devices document and the accompanying products.

Blink and You Missed It

The speed at which mobile devices have spread has been breathtaking. Three years ago, in 2010, the iPad had not yet been released but today it is a common sight in all aspects of life. Meanwhile, many of the reasons for mobile devices becoming so popular in personal life are equally valid in the business world. Modern businesses are harnessing the power and popularity of laptops, portable USB drives, smartphones and tablets to help them work more effectively internally, and also to interact with customers in new and better ways.

Medical staff, for example, record patient details and view test results on tablets, while many airlines now offer iPads on flights instead of seat-back entertainment – and banks often allow customers to conduct their business from foyer-based tablets instead of waiting for a cashier.

There are many reasons why an organisation might seek to introduce a mobile devices policy. Perhaps senior management levels have identified business opportunities that require the use of mobile devices; or employees might be pressuring IT staff and management to be allowed to use their beloved personal gadgets for work purposes.

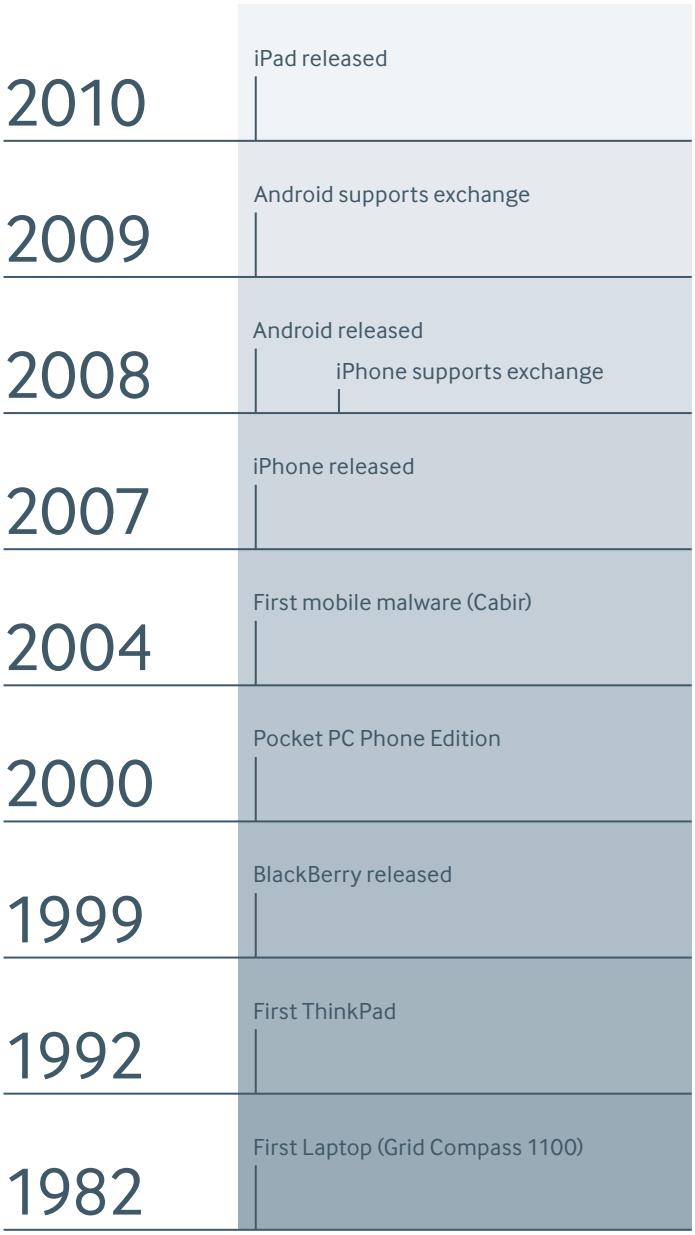
Exciting as the many business examples of mobile device use can be, they all come with risks that differ in their severity (and often nature) from risks that organisations have been managing for decades. It is simply not possible to manage those risks by applying the old risk models to the new technologies.

Hence organisations are starting to recognise the importance of constructing a mobile devices policy that enables them to understand and manage the various risks. In so doing, they can become confident that these new ways of working will not lead to data breaches or other asset compromise. Indeed, experience shows that understanding and working with employees is a critical step in managing risk – while retaining the numerous benefits possible from the business use of mobile devices.

Furthermore, many organisations accept that the radical changes of the last few years are unlikely to suddenly stop. We can expect changes in working styles and the devices already in use, as well as the emergence of new devices and fresh working styles that are currently unimaginable. Come 2020, will corporate desktops exist at all? Will all business be conducted on some form of mobile device and what will those devices be running?

It is hard to predict exactly what the future holds; but by building a firm base now, it will be simpler to support future devices and ever-evolving styles of working.

Timeline of events



Threats

Mobile devices can significantly change the threat landscape of an organisation. The changes in the nature of devices accessing corporate assets and how those devices are used can exacerbate existing threats and introduce entirely new ones. The diagram below shows the threats that can result from the usage of mobile devices in an organisation and gives examples of how those threats might occur.

Threats from corporate use of mobile devices

LOSS OF CORPORATE DATA

Physical Compromise of Device
- Device lost
- Device stolen
- Decommissioned device

Logical Compromise of Device
- Malicious app installed by user
- Compromise of user application
- Malware infects device
- Insecure corporate application enables access to data

User Action
- User stores data inappropriately
- User tricked into disclosing data as a result of social engineering

Communications Compromised
- Cleartext data intercepted in transit
- Encryption key disclosed allowing data decryption
- Insecure encrypted connection

Contamination of Device
- User accesses information beyond their privilege
- Personal and corporate data combined

TRUST RELATIONSHIP COMPROMISED

Compromised Device Used to Pivot into Secure Environment
- Wi-Fi credentials used
- Poorly secured VPN environment

SECURITY MODEL WEAKENED

Bypass of Security Controls
- User jailbreaks device
- User bypasses application level control (eg sends data to personal email account)
- User provisions own access

The Challenges

Changing Ownership and Usage Models

There have recently been fundamental changes in how mobile devices are used in the workplace – and who owns them. There is now an increasing expectation that corporate machines can be used for personal online purposes, while there has also been the emergence of BYOD (bring your own device), whereby personal machines are used as primary work devices.

However, the use of corporate machines and identities for personal purposes substantially increases the risk of a malicious attack, while using personally owned devices for corporate work presents multiple challenges.

Simply banning the use of personally owned devices for work purposes is unlikely to be the answer. Research and experience indicate that where users are not provided with that opportunity, they simply create it for themselves – in other words, mobile devices will probably be used in the organisation regardless of official policies. If users are enabled and supported by the organisation, then the risk is known and manageable. In the absence of policies, that risk is still present but unknown and unmanaged.

Jailbreaking

Jailbreaking, also known as rooting, is the act of elevating privileges on a smartphone or tablet in order to bypass restrictions that have been placed there by the manufacturer. Users jailbreak their devices in order to gain greater control, or to allow new functionality by running software that has been prohibited by the manufacturer.

As such, there are thriving jailbreak communities, particularly for iPhones, iPads, and Android devices. Jailbreaking has now been developed to the point where a person with little technical knowledge can accomplish it with ease. However, jailbroken devices present a significant risk to corporate assets as key security controls will have been deactivated or circumvented.

Technology Refresh and Disposal of Devices

At the end of their lifecycle, mobile devices such as laptops, USB drives and smartphones/tablets are generally replaced by newer devices – and that lifecycle is typically quite short.

It is vital for organisations to ensure that corporate data is not exposed once a device has been decommissioned but there are numerous examples of devices thrown away or resold with sensitive information still stored on them. Motivated attackers might even attempt to collect decommissioned devices specifically to perform data recovery.

However, traditional disk wiping methods do not necessarily translate to mobile devices, while a different challenge arises with personally owned devices. These could contain sensitive corporate information but individuals are often reluctant to destroy their devices, as they can have a significant monetary value.

Loss of Device

By their very nature, mobile devices are at high risk of being lost or stolen, with smartphones and tablets regularly targeted by thieves. A large organisation is almost certain to experience the loss or theft of corporately owned mobile devices on a fairly frequent basis, while personally owned equipment is arguably at even greater risk (since an employee will typically carry the device around at all times, including socially).

Should a device be stolen or lost, the assets contained within it may be compromised – not to mention the potential for unauthorised corporate access via the device. Many examples of public data breaches are a result of the loss of, say, a laptop or USB key.

The Challenges

Training

Although technical controls have improved substantially in recent years, research indicates that a significant proportion of employees will attempt to bypass controls that prevent them from using their devices in the manner they want.

Employees who use personal devices for work purposes are particularly likely to become frustrated with what they see as overzealous controls – and a separate issue is that while it might be possible to apply a control to a device, it could well be inappropriate from a legal or human resources standpoint.

An example of this is 'remote wipe', which allows a corporate administrator to respond to the theft or loss of the device by wiping data remotely. However, on a personal device it raises significant issues as the user's personal data will also be wiped. The user might not be aware that the device could be wiped and hence might be upset – or even litigious – should it happen. Alternatively, a user could be aware of this possible outcome and simply avoid telling security staff in the event of a loss or theft.

In short, for effective security it's important that employees not only work within the controls that have been imposed, but that they also adopt secure practices. By doing so, employees can help to significantly reduce the risk to corporate assets. Conversely, poor security practice can result in employees inadvertently putting corporate assets at risk, despite the presence of controls.

Case Study: Unauthorised USB Drive

An organisation was designing and building a new network stack, the technical details of which were highly sensitive. Ensuring the protection of all information surrounding the network design was of the utmost importance. However, the organisation discovered that a third-party contractor had been using an unauthorised USB mass storage device to transfer plans for the new network between various systems – and a subsequent investigation identified that the device had also been connected to unauthorised computer systems both at the individual's home and at the contractor's office. This meant that the sensitive information was outside the remit of the organisation's corporate security controls and could have been compromised by malware, or copied to the hard disks of unauthorised computer systems.

In this scenario it was not possible to provide any level of assurance that the information had not been leaked or otherwise compromised as a result of the contractor's actions. To mitigate the potential impact of the incident, the network stack had to be redesigned, including changes to the technologies, architecture and addressing scheme at significant cost and delay to the project. The organisation in question had implemented technical controls over the use of USB devices in its equipment and had strict policies on the use of these devices to handle its data, but failings by a third party still resulted in a significant impact on security.

Ultimately, the failings in this situation were twofold. First, there were no mechanisms for the contractor to handle the data in a manner that enabled the secure completion of the project; and secondly, the individuals concerned had not been sufficiently educated about the risks of using unauthorised USB mass storage devices. Both these areas were subsequently addressed by the organisation to ensure that a similar incident could not occur in the future.

Working from Untrusted Networks

Many companies issue staff with laptops or smartphones/tablets so that information can be captured, delivered and manipulated from any location, rather than having to return to the office before the data is processed.

To realise the full benefits of mobile working, it is necessary to allow the mobile devices to access both the internet and corporate resources. Typical connections used by mobile workers include home Wi-Fi, client/partner Wi-Fi, public Wi-Fi, and 3G/4G/mobile internet. This generally means using non-trusted network connections and hence potentially losing control of the data.

As shown in the illustration (below), home Wi-Fi and well-protected client/partner Wi-Fi tend to be more resilient to such problems but it should be understood that advanced attackers might still be able to gain access to the networks.

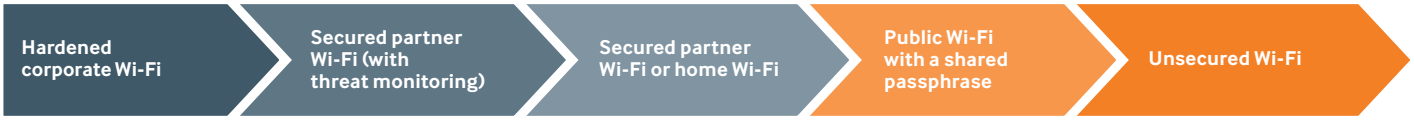
Incident Management

The prevalence of mobile devices and mobile working means that current incident management resources and policies might be inappropriate or insufficient for many modern incidents.

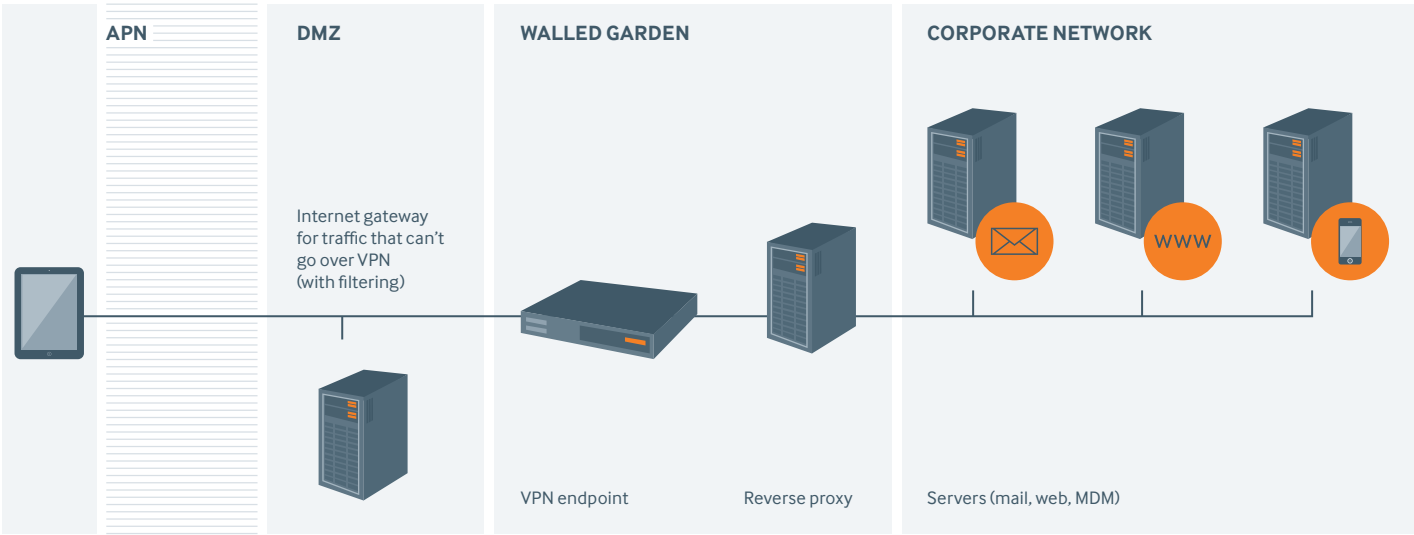
For a start, there are a huge variety of devices that need to be supported, each of which could require support staff to employ different tools and methods to manage an incident.

Furthermore, many incidents occur outside normal working hours: an employee who has his phone stolen in the early hours of Sunday morning, for example, after a night out with friends. And the device might be personally owned – by an employee who is perhaps unhappy to have support staff perform forensic analysis of a device containing personal data, while remote wiping might also prove unacceptable. Finally, if the employee is suspected of wrongdoing, then investigation, monitoring, and response could all be impeded if the devices involved are personally owned.

Risk of working from different networks



A model for secure mobile access to corporate resources



The Challenges

Software Distribution

Installing third-party software on mobile devices is a primary requirement for many users, yet the way in which the software is distributed is changing, as devices evolve. The model used for desktop and laptop operating systems, i.e. downloading or otherwise obtaining software from a range of sources, has not been transferred to modern devices such as smartphones and tablets.

In order to preserve user experience by regulating the type of software accessible, mobile device manufacturers generally allow for third-party application installation through curated marketplaces. These marketplaces allow manufacturers to restrict the types of application available and to some extent reduce malware infection of devices. However, as the mechanisms for distributing software are dependent on the device manufacturer, the risks of malware vary depending on the device in question.

Access to Data

There are major business benefits to allowing less secure devices, such as consumer smartphones and tablets, to access data. Such devices allow new methods of data entry or manipulation and can enable new working styles. For example, an employee waiting to meet a client can quickly review a proposal on a small mobile device rather than having to set up a laptop. However, as consumer mobile devices are less secure than hardened corporate machines, there can be increased risks to data.

Solutions

Changing Ownership and Usage Models

Here, above all, there is the need for a clear, coherent and encompassing policy or policies regarding mixed use (business and personal) devices.

If an organisation decides to support mixed use devices, whether corporately or personally owned, policies are required to cover what can and can't be accessed – and on which devices and under what circumstances. Employees need to fully understand what they are allowed to do; and why these policies have been adopted. It is important that users are aware of the risks to corporate assets should they not comply.

Controls to support these policies should be effectively implemented – and monitored to detect attempted bypass. If it turns out to be impossible to construct a policy that both satisfies corporate requirements and is acceptable to employees, then it is strongly recommended that the behaviour in question is disallowed, and controls are put in place to restrict and detect access that is in breach of the policy. However, it is essential that – while bypassing controls must be detected and addressed – a culture of amnesty should nevertheless be encouraged so that employees do not fear reporting security issues.

Jailbreaking

It is strongly recommended that jailbroken devices are not allowed to access corporate resources and that employees are made clearly aware of this fact. MWR believes it is worthwhile for an organisation to put all necessary effort into detecting such devices – and into preventing them from accessing the corporate network.

It is also worthwhile ensuring that users are educated as to the risks of jailbreaking devices and why it is at odds with corporate security policies; not to mention their own security needs.

Technology Refresh and Disposal of Devices

Corporate policy should include a secure erasure process, regardless of whether the drives were encrypted, with a thoroughness appropriate to the sensitivity level of data they contain. Even if no sensitive data is thought to reside on the drive, secure erasure is recommended.

If drives are to be repurposed inside the organisation, they can be wiped and then redistributed. If they are not to be reused, MWR recommends that drives are physically destroyed.

Employees should be instructed to contact IT support staff if they are upgrading their smartphone or tablet. Support personnel can then de-provision the current device and re-provision the new one. It might be wise for an organisation to collate a guide for migrating data so that employees do not have to rely on external help; and employees should be clearly instructed to securely wipe their device before disposal. Alternatively, the organisation could choose to provide a service for employees to use.

Loss of Device

A crucial technical control to mitigate device loss or theft is encryption of data. The importance of effective encryption cannot be overstated and organisations should not allow data to leave their premises on unencrypted devices. However, this can be a challenging policy to adopt as encryption is implemented in a huge variety of ways depending on the device in question.

Meanwhile, employees need to be aware of the procedure for responding to the loss or theft of a device. Part of this procedure should be to immediately inform both the organisation's security staff and the police, as there is a narrow time window before an attacker can be expected to disable the tracking and so, in that window, the police have a high chance of apprehending the thief.

Security staff might wish to remotely wipe the device. This is only possible if the device still has internet connectivity (and there could be significant legal issues if the device is personally owned). In addition, security staff will immediately want to prevent any access the device might have to networks, as well as to services such as email, to reduce the data exposed.

Training

Once policy has been decided, employee training is a key step in helping individuals to understand the controls that are in place – and, very importantly, the reasons for them. In the case of personally owned devices, it should be made clear to the employee that if they are not comfortable with the security requirements, then they should not use their personal equipment for work purposes.

Employees should be trained to understand and agree to all aspects of the policy, including those that might be seen as problematic if used – such as remote wiping. In the case of all such potentially problematic controls, it is recommended that the organisation obtain a signed agreement from the employee at the outset.

Employees should also receive training in secure practices – including the reporting of incidents, both proven and suspected. It is helpful if a culture of amnesty is adopted so that employees who have bypassed controls will not fear reporting incidents. Organisations might even wish to incentivise the reporting of incidents through social or financial rewards.

Working from Untrusted Networks

Owing to the risks inherent in connecting to untrusted networks, it is recommended that corporate devices are prevented from doing so. However, restriction of networks is not possible on all devices (notably iPhones and iPads) and so employee training is vital.

There might be a requirement for employees to work from specific networks – such as their home, or while out and about. Possible solutions are either to provide all home-working employees with a wireless access point configured to corporate specifications, or to permit specific networks for specific devices.

If devices are left in a state where they can connect to arbitrary Wi-Fi, there is a risk that employees will connect to public or otherwise unsecured Wi-Fi. For employees who are required to work from multiple locations, a 3G or 4G mobile connection is recommended, as this is generally safer than allowing arbitrary Wi-Fi connections. A potential scenario to consider is that of employees travelling abroad, where 3G/4G access might be prohibitively expensive and hence there's a need to use internet access provided by a hotel. There is currently no ideal solution to this problem.

Solutions

Incident Management

It is important that organisations develop incident response procedures and policies that are tailored to specific devices.

Employees should receive training so that they understand the procedure following an incident. The training should cover different types of incidents and the employee's expected response in each case, and should also give the employee clear contact points for queries that do not fit within the defined incidents. Employees should not be discouraged from reporting incidents through fear of reprimand, even if the employee has intentionally bypassed controls.

Response policies need to cater for both supported and 'unsupported' ownership models – in other words, when it becomes apparent that employees are using their own devices without official permission.

Where personally owned devices are used, employees need to understand what measures will be applied in the event of an incident. It could well be necessary to have employees sign additional contracts or disclaimers to cover specific eventualities. Owing to the legal difficulties of a company monitoring and analysing personally owned devices, however, it is recommended that employees are not permitted to use such devices if they work in areas that are particularly prone to investigation – such as financial trading.

Software Distribution

It is recommended that organisations with corporate-owned devices prevent the installation of third-party applications. However, many smartphones and tablets will be personally owned and the owner might not agree to have application marketplaces restricted. Organisations therefore need to calculate the risks from rogue applications, which will depend on the device in question.

Installing applications from sources other than the official marketplaces should be restricted regardless of device ownership. Where users are allowed to access marketplaces and download applications, they will require training as to the risks of such behaviour and guidelines on best practice: specifically, only to install applications from well-known companies and to recognise unnecessary permissions requests.

Access to Data

Organisations can create 'low-impact, high-value' data views that are highly useful to the relevant staff, yet minimise exposure should a device or view be compromised. For example, it might be useful to allow a salesperson to view open proposals. This data can then be collected into a view for the employee to consume safely.

Another example is the presentation of data in a form that enables management staff to make decisions without seeing the data itself. For example, a company might decide that management staff can access a graph of changes in sales figures on their iPad, but not gain access to the actual sales data. The construction of such views is likely to require the production of bespoke applications, which can bring additional risks, but it might be considered worthwhile given the flexibility it affords decision-makers.

Technical Controls

MWR has written a more detailed guide for implementers that not only covers the policy recommendations for safe use of mobile devices in an organisation but also the key technical controls that your organisation will probably want to use to secure its assets. You may wish to refer to this guide if you would like a more detailed explanation of any of the areas covered here, or of any of the technical controls available to support secure usage of mobile devices.

While technical controls are an important adjunct to help enforce your security policy, many controls are ineffective or simply not present on some devices – and, even where they are, user training is essential if the technical controls are to prove successful. The table opposite shows the controls covered by MWR's 'Mobile Devices – Guide for Implementers' and to which categories of mobile device the controls apply.

Technical controls and the device types they apply to

CONTROL	LAPTOPS	PORTABLE STORAGE	SMARTPHONES AND TABLETS
Passwords	✓	✓	✓
Encryption	✓	✓	✓
VPNs	✓	X	✓
DLP	✓	✓	✓
Patching	✓	X	✓
Asset Management	✓	✓	✓
Remote Track and Wipe	✓	X	✓
Exploit Mitigation	✓	X	✓
Data Segregation	✓	✓	✓
Antivirus	✓	X	X

Challenges and Solutions Cheat Sheet

CHANGING OWNERSHIP AND USAGE MODELS

CHALLENGES

- New ownership and usage models are becoming common in business
- Particularly common are personal use of corporate devices and BYOD
- Users often provision own access if not allowed to use personal devices

SOLUTIONS

- Organisations need to assess true rather than reported usage of personal devices
- Policies should be designed to work with the user's own desires
- Robust technical controls can prevent non-permitted usage of resources
- Encouraging a culture of openness and amnesty will help to ensure that security issues are still reported

TRAINING

CHALLENGES

- Many technical controls exist for mobile devices but require compliance from employees to be effective
- Employees that are frustrated by controls frequently attempt to bypass them
- Support exists on the internet to aid people in bypassing controls

SOLUTIONS

- Employees need to be told the reasons for controls
- Employees should be made to agree to particularly contentious controls, such as remote wipe
- Employees should be trained in secure practices
- A culture of openness and amnesty will help to encourage reporting

TECHNOLOGY REFRESH AND DISPOSAL OF DEVICES

CHALLENGES

- Devices are replaced at the end of the lifecycle, which is increasingly short
- Corporate data can be exposed on devices that have been disposed of
- Traditional disk wiping is not effective on mobile data storage
- Users are often unwilling to destroy personal devices at end-of-life as they have monetary value; plus they might seek help from third parties to migrate to new devices

SOLUTIONS

- Policies should be developed to securely erase all devices that have contained corporate data
- Devices that are not to be re-used in the organisation should be physically destroyed
- Organisations should support employees in migrating to new personal devices
- Employees can benefit from education regarding the risks of selling their 'old' mobile devices

LOSS OF DEVICE

CHALLENGES

- Mobile devices are often lost or stolen
- Many public data breaches are the result of a lost mobile device
- Personally owned devices that contain corporate data are at particular risk as they will be carried socially

SOLUTIONS

- Corporate data should only be permitted on encrypted devices
- It is worthwhile training employees as to their expected response if a device is lost or stolen
- Policies should be developed to respond to the loss of a device, such as revoking the device's access, remote wiping and collaborating with law enforcement

JAILBREAKING

CHALLENGES

- Jailbreaking is the act of elevating privileges on a smartphone or tablet to enable usage previously prevented by the OS
- Jailbreaking bypasses many important security controls, putting corporate assets at risk
- Thriving jailbreaking communities have made it possible for even relatively non-technical users to jailbreak a device

SOLUTIONS

- Efforts should be made to detect jailbroken devices and prevent them from accessing corporate resources, although this can be difficult
- Policies should ensure that all devices are running the most up-to-date version of the OS available, as this will reduce the risk of a jailbreak

WORKING FROM UNTRUSTED NETWORKS

CHALLENGES

- Mobile working can require the use of untrusted networks
- The risk of the network might not be obvious to the employee

SOLUTIONS

- Where possible, 3G/4G connections should be provided to remove the need to join untrusted networks
- It is not possible to prevent Wi-Fi on iPads and iPhones so employee education regarding the risks is vital

Challenges and Solutions Cheat Sheet

INCIDENT MANAGEMENT

CHALLENGES

- The increasing variety of devices to support means current incident management policies might not suffice
- The nature of incidents is also changing; for example, the time they take place and the type of incident

SOLUTIONS

- New response policies are required for specific devices and incidents
- Employees need to be educated as to how they should respond
- Policies should also cover the unsupported use of personal devices
- An effective response might require an agreement that has been pre-signed by the employee

SOFTWARE DISTRIBUTION

CHALLENGES

- Software is often obtained through curated app stores
- There are different risks of malware on different platforms

SOLUTIONS

- Corporate owned devices should not be allowed to download third-party software
- Installing apps obtained from sources other than official app stores should be prevented on all devices
- Employees can benefit from education regarding the risks of malware on their chosen platform

Summary and Key Points to Take Away

Mobile devices have the potential to streamline existing business processes and to introduce entirely new ways of working. However, to exploit the potential of mobile devices safely, it is vital to manage the risks that they introduce. Many of these risks cannot be managed using traditional models, as the devices and their usage differ so dramatically from traditional computing. Different methods of addressing the challenges presented by mobile working are needed – and many, if not all, these methods will need to be bespoke solutions for your organisation and its employees. The policies you design for your organisation should take the following into account:

- Mobile devices present enormous opportunities to businesses, but can also bring risk that is significantly different from the risks that a business is used to managing
- Effective mitigation of these risks requires policies that work with the user; and also require user education and effective technical controls
- There are a great many mobile platforms and devices, and they present widely differing risks; security policies need to account for these many differences

More detailed information can be found in 'Mobile Devices – Guide for Implementers, available from MWR and CPNI. This paper is designed to aid you and your staff in designing the policies that will allow your business to reap the rewards of mobile devices, while effectively managing the risks.

Contributors:

David Chismon

Tassi Carter

Martyn Ruks

Henry Hoggard

MWR InfoSecurity
Churchill Plaza, Churchill Way
Basingstoke RG21 7GP

T: +44 (0)1256 300920
F: +44 (0)1256 811227

MWR InfoSecurity (South Africa)
11 Autumn Street, Rivonia
Gauteng, 2128, South Africa

T: +27 (0)10 100 3157
F: +27 (0)10 100 3160

www.mwrinfosecurity.com
labs.mwrinfosecurity.com

Follow us on Twitter:
@mwrinfosecurity
@mwrlabs