

Security & Mobile Devices

Overview

Mobile devices/computing/technology, they are everywhere and are possibly the most widely used pieces of personal electronic equipment available in the modern world. The plethora of differing mobile devices with their abundant configuration options and application types is enough to make your head spin. There is no doubting the value added to business and personal life with your little font of knowledge nestled somewhere about your person or personal belongings. Of course if you are security conscious or worried about individual rights they can be viewed in less benign terms.

In contrast to the red braced yuppies of the 80's with their almost exclusive use of the iconic 'brick' mobile phone (that's a very loose interpretation of the term mobile) just consider the complexity of modern mobile devices in use daily and their everyman availability combined with an ease of use. I will proffer myself up as a typical example; Nokia business phone, Nokia personal phone, iPod touch, usb stick (containing lots of lovely tools my anti-virus product would love to delete), Samsung business netbook, Toshiba personal laptop, portable usb hard drive (backups!). If I was to extend into my family unit I could add PSP, DSi, iPhone, other laptops and storage media etc. There you have it lots of devices with facility to process and store reams of both personal and business information. I will take this opportunity to state that I DO NOT access my workplace either remotely or by email from handheld portable devices. Risk aversion is my personal preferred choice.

Ok, so we can now see that mobile devices are a part of our daily life in one form or another, and as with the other aspects of our daily life we must consider security. After all we routinely lock doors and windows, set alarms, wear seatbelts, cover PIN at ATMs, shred receipts, cut credit/ debit cards and all the other security decisions we make without too much thought. The devices themselves are replaceable and are not the real issue. It's the information on them and the controls in place to secure that information.

Mobile devices are a fairly recent phenomena and a great business enabler with a myriad of benefits. They are here to stay and with increasing use forecast why not develop a security culture for them now?

It is the intent of this paper to raise awareness of the security considerations for mobile device technology and more specifically how to protect the information on them with ISO27001:2005 and common Infosec best practice in mind. It is not a definitive guide but rather a handy point of reference.

Mobile computing and ISO 27001

The ISO 27001 international standard for information security management systems is a great benchmark for the implementation of security controls with a holistic approach. One area such as mobile computing may have resonance throughout the standard such as protection against malicious or mobile code, network controls, access controls, risk assessment etc. However, section 11.7 Mobile Computing and Teleworking, of the annexe within ISO 27001:2005 makes explicit reference to mobile computing and further guidelines and assistance can be gleaned from the ISO 27002:2005 Code of practice.

The gist of it can be described thusly: consider the risks when using mobile computing and apply appropriate controls. That's a fairly common sense approach and is indicative of most international standards but it doesn't really help explain what the risks are and what would help to engender a security culture for mobile technology.

So what is mobile computing and what are the devices?

Put simply, it's computing on the move and let's stay with the corporate end of things. Laptops were the first of the mobile computing devices to become established and everything has subsequently come from them. Who scoffed back in the day when computerised phones or wristwatches were mentioned? An operating system on a phone, where would the floppy disk go?

Laptops, PDAs, netbooks and mobile/smart phones are the predominant mobile computing devices used within the corporate sector. The most common usages are corporate data access and e-mail usually in conjunction with application software. That is certainly not the limit of their capability but just what they are generally used for.

I have witnessed environments where the use of media playing MP3 / MP4 type devices was prevalent and it was the web or software developers who were typically the most common users. It was understandable given their role and no-one really considered that there may be a risk, mainly due to the then limitation of the devices. The newer generation (Apple, Nokia, and Blackberry etc) change the game significantly but the risk has not been readily identified simply because of a lack of understanding of the capability of the devices and the legacy of their use as base media players.

Risk

The horror stories of mobile devices being stolen, lost or compromised in some way are legion. Everyone can conjure up a recent event. As I have alluded to earlier, mobile technology is here to stay so how can we identify the risks and what can be considered to reduce them?

One of the biggest risks from mobile devices, of course, is inherent with their portability and that is precisely the intended functionality. The ability to work outside of the corporate network has brought technology forward in leaps and bounds. Wireless and remote connectivity from almost anywhere is fantastic for information access and sharing but the risk has moved outside of the established security perimeter that has been so meticulously developed. The risks begin to accumulate. All of the security controls implemented to protect the corporate network are rendered null and void if an analysis of the risks posed by mobile computing has not been undertaken with the implementation of subsequent selected security controls.

The world has known of the risk posed by laptops for some time now and yet securing these devices has only really been considered in the wider sense in recent times. Corporate entities are now establishing strict security policies around the use of laptops with some form of cryptography used as standard. The 'damage to brand' approach has facilitated the rapid embracing of encryption methodologies. It is only a matter of time before this approach is common for all mobile devices.

Perimeter and middleware applications are everywhere from intrusion prevention/detection to anti-virus, spam and content filtering. Traditionally they have been installed to help protect the network from the bad guys and nasty things on the outside trying to get in. From personal experience, I could suggest that consideration is given to looking a bit closer to home. After all, the people who have easy access to information are usually the ones responsible for security breaches whether intentional or otherwise.

A lost mobile device with non-encrypted data or any other security controls surely is just damaging as it would be if it was stolen and can be almost catastrophic if that information is deemed to have some form of classification attached. So, not only should there be a consideration given to the physical controls to prevent theft but also the logical controls to protect the information.

Top ten tips for mobile security

The following top ten tips gleaned from the peer professional internet fora and personal experience will hopefully assist with securing your mobile devices.

Top Ten tips for mobile security

1. Device Selection

Not all devices are created equal when it comes to security. For example, iPods are built for general consumers not as concerned by security and is therefore less inherently secure than a BlackBerry device designed for enterprise users.

The degree to which security controls can be implemented on mobile devices is highly dependent upon the vendor. Consider mobile devices that have the best possible control and security on them. Just because a senior manager likes the look of a particular device is not a good enough reason for its selection.

2. Enable Encryption

Many organizations do not enforce or even set policies mandating the use of device encryption on mobile devices. Encryption is one of the most common methods used to protect the information on the mobile device and should really be used without a second thought. It gives both you and the data owner a clear sense of security. Some vendors actively publish and push their security encryption methods and credentials with Blackberry being a prime example with lots of security hints and tips readily available.

I mentioned earlier that encryption for laptops is standard best practice so why not all mobile devices?

3. Require Authentication

Mobile devices are just too easy to lose to go without proper authentication. Most users have adopted some form of authentication on their laptops, even if it is only a password, so why is this approach not applied to all mobile devices? A BIOS or start-up password for a laptop works on another level whilst still using encryption. If you can't authenticate you cannot gain access therefore the encrypted data is further protected.

4. Utilize Remote Wipe Capabilities

Applications have been developed because of the proliferation of mobile devices and their inherent vulnerabilities that give people the ability to remotely access and disable devices in the event of loss or theft. Imagine how helpful the ability to wipe information remotely from a machine could be in such a stressful scenario as loss or theft especially considering the potential damage in the event of information leakage.

5. Incident Management

Organizations should consider developing a policy and procedure set for users who have lost their devices. This is where ISO 27001 Incident Management comes into its own. An effective incident management process will make it easy for them to call the relevant people to alert staff that a device has been lost or stolen but is only effective if you launch an awareness campaign for such an event.

6. Control Third-Party Apps

Smartphones are so dangerous because they are essentially miniature computing platforms that can accept any nature of third-party applications. If you can limit the installation of unsigned third-party applications you can help to prevent the bad guys from requisitioning control of your devices. This is the basic premise of Trojans and how they attack your systems. Consider that there are many examples of Trojans being built into free apps and so called 'cool' games!

7. Network Access Controls

Enterprises should set up network access control mechanisms such as unique firewall policies, vlans, static routes etc. specifically to segregate traffic coming in from mobile devices. Mobile device users don't necessarily need access to every bit of data and area on the network, so limit exposure by only offering access on a need to know basis.

8. Use Intrusion Prevention / Detection Software (IPS/IDS)

As Smartphones and mobile devices become more and more powerful, they're likely to become another weapon in the hacker toolbox. As a result, it makes sense to have your intrusion prevention software examining traffic coming through mobile devices. After all if a standard user can install apps on an easy to hide portable device what's to stop a hacker utilising such a device with a vast array of tools?

9. Anti Virus - AV

There are many host based anti-virus applications available for Smartphones and mobile devices but consideration must be given to how they interact within the enterprise and how they are going to be managed. A device connecting into the corporate LAN may have a requirement to authenticate its security control feature or access may be denied. Blackberry Enterprise Server (BES) utilises AV to control its devices and is way ahead of other Smartphones in the security stakes.

10. Bluetooth

Bluetooth capabilities on today's Smartphones and mobile devices may make it easy to talk on a hands-free headset, share information and interconnect devices, but they're also a target for hackers, who can take advantage of its default always-on, always-discoverable settings. In order to limit exposure best practice is to recommend disabling Bluetooth when it is not actively transmitting information. You can also suggest switching Bluetooth devices to hidden mode. Organizations can limit exposure by making this company policy.