Trusted Information Sharing Network
for Critical Infrastructure Protection

# MOBILE DEVICE SECURITY INFORMATION FOR CIOs/CSOs

## Introduction

In today's business environment, managing and controlling access to data is critical to long-term business viability and survivability. Mobile devices—such as personal digital assistants (PDAs), advanced and 'smart' mobile phones, and traditional laptops—are no longer the preserve only of technology 'early adopters'. They are critical tools that provide competitive advantages for the mobile workforce and individual users, by enabling access to corporate data by users 'on the move'. Accordingly, mobile devices are increasingly integrated into corporate networks and systems, including those that underpin critical infrastructures. As mobile devices can move freely in and out of an organisation's controlled security environment, they pose additional risks to your information and systems.

This paper—developed by the IT Security Expert Advisory Group (ITSEAG), which is part of the Trusted Information Sharing Network (TISN)[1]— provides information on the risks associated with mobile devices, and a basic set of actions your organisation can undertake to manage and respond to these risks. Though mobile devices often interface with corporate systems via wireless networks, this paper does **not** discuss general issues associated with wireless security—these issues are already addressed in another series of papers issued by the ITSEAG.[2] Rather, this paper focuses on issues specific to mobile devices, above and beyond those associated with computers in general.

[1] The TISN is a forum where the owners and operators of critical infrastructure work together, sharing information on the security issues that affect them. It provides a safe environment where industry and government can share vital information on critical infrastructure protection and organisational resilience. The TISN is made up of nine different business sector groups, called 'Infrastructure Assurance Advisory Groups', which are overseen by the Critical Infrastructure Advisory Council (CIAC). The CIAC has also set up two Expert Advisory Groups—one for IT security and the other looking at Critical Infrastructure Protection in the future.

The IT Security Expert Advisory Group (ITSEAG) provides advice on technical solutions to problems identified by the nine Infrastructure Assurance Advisory Groups, as well as projecting emerging trends that have the potential to impact on all industry sectors.

[2] The ITSEAG Wireless Security papers can be accessed from: www.tisn.gov.au

**DISCLAIMER: To the extent permitted by law, this document is provided without any liability or warranty. Accordingly, it is to be used only for the purposes specified and the reliability of any assessment or evaluation arising from it are matters for the independent judgement of users. The document is intended as a general guide only and users should seek professional advice as to their specific risks and needs. This information is not legal advice and should not be relied upon as legal advice.**

**May 2009**

It is also important to note that this paper **does not** address the security concerns around mobile memory devices such as USB sticks, dedicated media players, and stand-alone digital cameras. These devices introduce a different class of risk from those discussed in this paper.

## Benefits of Mobile Devices

Mobile devices have increased in functionality, storage capacity and their general utility. The benefits of mobile devices are visible at all organisational levels of enterprises, as they provide greater mobility, accessibility and convenience. In simple terms, mobile devices are a critical enabler of the 'mobile office' concept—potentially reducing overheads and increase work productivity in a range of enterprise settings.

Mobile devices therefore represent an increasingly attractive way for enterprises to optimise their operational business outcomes, whilst simultaneously increasing workplace flexibility and decreasing infrastructure costs. In particular, to reduce costs, businesses may allow individuals to privately own mobile devices which interface with business systems, though this practice will involve the acceptance of a degree of risk by the organisation.

## Risks to Mobile Devices

Mobile devices are subject to the same sorts of threats as traditional desktop computers, with additional threats arising out of two sources—the size and portability of mobile devices, and available wireless interfaces and their associated services. Additionally, due to their generally limited processing power (as compared to desktop computers), mobile devices typically lack a range of integrated security features commonly found on desktop computers. Given this, mobile devices have become increasingly attractive as the target of malicious attack. Also, because their adoption often takes place informally and piecemeal, organisations may not recognise mobile devices as part of an organisation's infrastructure nor treat them accordingly.[3] Inappropriate controls on mobile devices raise the potential for any information on the corporate system to become vulnerable to loss, interception or capture. Collectively, these issues mean that the threat space faced by mobile devices is larger and more complex than that posed to desktop computers. This is illustrated in Figure 1 below.

[3] US National Institute of Standards and Technology***, Guidelines on Cell Phone and PDA Security, NIST Special Publication 800-124,*** page 4-1. Available at: http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf

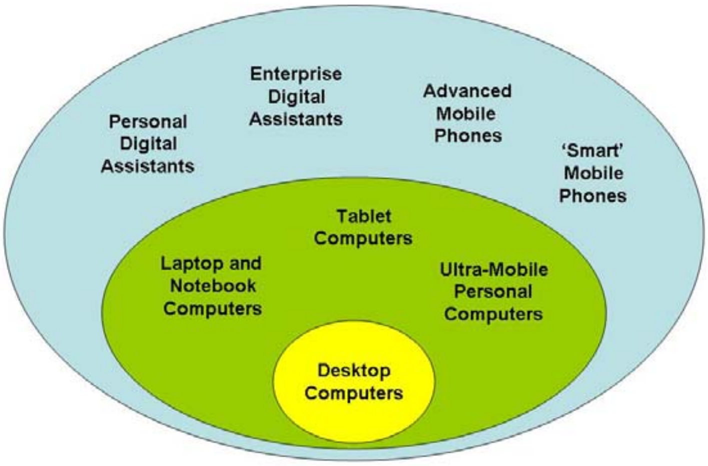
Personal Digital Assistants
Enterprise Digital Assistants
Advanced Mobile Phones
'Smart' Mobile Phones
Tablet Computers
Laptop and Notebook Computers
Ultra-Mobile Personal Computers
Desktop Computers

**Figure 1: The Mobile Device Threat Space**

Key risks posed specifically to mobile devices are as follows:

- **Loss and theft**. The small size of mobile devices means that they have a tendency to be lost or misplaced, and are an easy target for theft. If the device does not have appropriate security measures in place or activated, then gaining access to the device can be easy, thereby exposing sensitive data on the device or accessible by it. Where a mobile device has an active telecommunications service, then unauthorised calls or other expenses can continue to be charged to the legitimate user. Additionally, the mobile device unit itself may be of considerable value, and be able to be reset and reused—even if user data is wiped in the process.
- **Disposal**. When a mobile device is disposed of (for being surplus to requirements), the risk exists of sensitive data being accessed, may continue as information may remain on the mobile device. Manually resetting a device, whilst deleting data in a logical sense, may leave data still physically residing on the device until it is overwritten by new data. Software and hardware products that can recover erased data from a mobile device are readily available.
- **Malware**. Mobile devices are subject to attack by a wide variety of malware (malicious software). Such malware ranges from that which is common to desktop computers, to that which specifically targets mobile devices. Malware can be introduced to mobile devices via communications services, synchronisation with a desktop computer or network, via email or web browsing, or via infected storage media. Generally, malware writers employ social engineering techniques to prompt users to carry out the necessary actions, enabling them to download malware on the mobile device. Malware installation may lead to the compromise of sensitive information on—or accessed by— the device, or a denial of service.
- **Spam**. Mobile devices, as the result of their connection to communication services, are increasingly subject to spamming. In addition to the annoyance of receiving undesirable and unsolicited material, spam can cause users to unwittingly accept charges on their communication service. Further, spam can

be used as an adjunct to social engineering, as a pathway for the introduction of malware, and to conduct denial-of-service attacks on a mobile device.

- **Private ownership**. Allowing privately owned mobile devices to be used for business purposes may seem to be a cost-effective approach for an organisation. But the ability to control and manage privately-owned devices is difficult to achieve, increasing the security risks generally associated with mobile devices.

## Protecting the Organisation

In order to manage the level of risk associated with the use of mobile devices within your organisation, you should consider the following dimensions of security practice:

- **People**. Applying security controls to counter people-related risks such as insure behaviours and the inadvertent installation of malware, is critical for protecting an organisation’s information and systems from threats that might arise via mobile devices. The awareness and training of staff is a critical factor in ensuring that technological and procedural security controls are implemented.
- **Technology**. Whilst technical solutions cannot substitute for an integrated mobile device security policy, a range of technical actions can reduce the risk exposure of mobile devices, and mitigate the effects of security incidents when they do occur.
- **Policies and procedures**. Policies and procedures need to be developed that outline clear roles and responsibilities with respect to the employment and management of mobile devices across their entire life-cycle (acquisition, deployment, use and disposal).

Examples of specific controls across each of these areas are detailed in the following table:

| **People** |
|---|
| • Identify key roles and responsibilities with respect to mobile device security, and identify mobile device user groups and their scope of usage for risk assessment.<br>• Educate users and administrators of mobile devices regarding risks, physical control, acceptable use, permissible sensitive data storage, and response and reporting actions in the event of security incidents or loss of the mobile device. |
| **Technology** |
| • Enable authentication processes on mobile devices, particularly where they interface with wireless networks, communication services, and corporate information and networks.<br>• Encrypt data resident on mobile devices and their associated removable media.<br>• Minimise or eliminate unnecessary functionality on mobile devices—this includes controlling or restricting access to wireless communications and communications services.<br>• Install protection and detection software on mobile devices.<br>• Where possible, conduct centralised configuration control and management of mobile devices and associated software. |

- Where possible, enable remote deactivation and erasure of mobile devices.
- Where data cannot be reliably erased from mobile devices, consider the secure physical destruction of memory modules prior to disposing of the device.

**Policies and Procedures**

- Develop a plan for the acquisition, deployment and operation of mobile devices in the organisation: risk assessments and security controls are easier to conduct and implement when the organisation approaches mobile devices in a systematic fashion.
- Limit or prohibit access to corporate information and networks for privately owned mobile devices.
- Establish a mobile device security policy, which encompasses both organisation issued and privately owned mobile devices.
- Integrate mobile device security issues into the organisation's overall IT security policy.
- Review mobile device security policy, particularly after the acquisition of new mobile devices, configuration changes, and in the wake of security incidents involving mobile devices.

## Conclusion

It is essential that organisations have suitable protective measures in place to secure mobile devices. This paper provides the basic knowledge for managing and mitigating the risks associated with the integration of mobile devices into corporate networks.

Mobile device security policies should ensure that new devices cannot be introduced into corporate networks without the knowledge of IT management. In addition, remove the ability to make changes to configurations or settings which have the capability to adversely impact on the risk profile of the organisation.

Finally, implement a secure infrastructure which aligns with good practice advice, and control, manage and update the configuration and settings of mobile devices as necessary. Constant adjustments will be required response to evolving technologies, changing risk exposure, and patterns of user behaviour. **The security of mobile devices should be an integral, routine and ongoing element of an organisation's approach to securing its IT infrastructure.**

## References

- Australian Government Information Management Office, *Better Practice Guidance for CIOs – Security Considerations for the Use of Personal Electronic Devices (PEDs):* www.finance.gov.au/e-government/security-and-authentication/docs/Guidance_Use_of_Personal_Electronic_Devices_CIO_Advice_v1.0.pdf
- US National Institute of Standards and Technology, *Guidelines on Cell Phone and PDA Security, NIST Special Publication 800-124*:

  http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf
- CIO Magazine, *Mobile Security 101:*

  http://www.cio.com.au/article/268162/mobile_security_101_an_executive_guide_mobile_security?fp=4&fpid=23