TISN
FOR CRITICAL INFRASTRUCTURE
RESILIENCE

Mobile Device Security Information for Senior Executives

July 2012

Disclaimer: This paper is intended as a general guide only. To the extent permitted by law, the Australian Government makes no representations or warranties of any kind, express or implied, about the accuracy or completeness of the material and recommendations contained in the paper. Each user of the paper is responsible for deciding whether the paper is suitable for their purposes and whether the recommendations should be implemented. Users should seek professional advice as to their specific risks and needs. The Australian Government accepts no responsibility for the consequences incurred, or any loss or damage suffered, by a user or by any other person as a result of their reliance on the information contained in this paper, and to the maximum extent permitted by law, excludes all liability (including negligence) in respect of the paper or its use.

Mobile devices and portable media[1] provide significant value add to organisations through increased efficiency and productivity. However, their proliferation in the workplace is a serious and expanding threat to the security of corporate information.

According to Mr Geoff Rhodes, Chair of the IT Security Expert Advisory Group[2], "Organisations need to have strategies in place to control how mobile devices are used by their employees. Their security policies and procedures and governance measures for these devices should be based on the assumption that they are inherently insecure."

CEOs and Boards of Directors are ultimately responsible for protecting their organisation's data and information systems - not only from malicious and accidental damage, but also from unauthorised access. Company executives are required to exercise 'due care' in understanding the risks associated with deploying mobile devices and for implementing reasonable risk control measures.

Some of the major issues for consideration are:

Privacy and Legal	There are various implications, including legal issues extending to the privacy of personal information held on mobile devices. Organisations should have policies in place to manage mobile devices (including those their employees own) that are used in the workplace. Issues include: • the ability to access, wipe, recover or protect data e.g. when a device is lost or when employees cease employment; • cross-border jurisdiction; • outsourcing of mobile device management; and • use of location-based services technology e.g. GPS.
Use of personal mobile devices	Personal devices, used to connect to, or administer corporate systems, could cause security breaches e.g. deliver malware with a payload that denies the ability to manage normal operations, including critical infrastructure services. Information security policies should address 'Acceptable Use', with employees being aware of the policies and their implications.
Use of mobile device applications	Increased risk to data integrity from malware, including unauthorised access to corporate data, through: • customisation of enterprise applications for mobile devices; • use of insecure third party mobile applications; and • poor patching of end-point operating systems.

[1] Mobile device referred to in this paper include smartphones, tablet computers, laptops, PDAs, storage device (e.g. USB drives), scanners and connectivity devices (e.g. Wi-Fi, Bluetooth).

[2] The IT Security Expert Advisory Group (ITSEAG) of Australia's Trusted Information Sharing Network (TISN) - see www.tisn.gov.au) - provides advice to government and industry on emerging IT security issues. Under the umbrella of the TISN owners and operators of critical infrastructure work together, sharing information on organisational reliance issues that affect them.

Unauthorised device modification (jail-breaking)	Removal of vendor imposed limitations of the device (jail-breaking) can lead to the device being more susceptible to malware infection. Jail-broken devices, able to access and manipulate corporate data, present a higher security risk than those managed through technical security policy controls.
Information Protection and Backup	Managing corporate data on mobile devices and portable media presents difficulties, including: • the potential for data loss/leakage, especially if they are not managed under normal and centralised data backup procedures; • exposing corporate data to users, who in an uncontrolled environment, are able to access corporate information and download and backup data to mobile devices; • users avoiding and breaching security control measures for safeguarding information; and • improper/uncontrolled device disposal procedures, exposing corporate data to unauthorised access.
Cross-border Data Loss	Data can cross national borders when mobile devices: • are carried across borders for business and personal travel; and • interface with cloud computing and hosted applications (location may not be fixed or known). Data on devices crossing borders may be governed by the laws, and subject to the jurisdiction, of that location.

The ITSEAG has also developed a more detailed guidance paper ‘Mobile Device Security: Information for IT Managers’, which you should review with your CISO/CIO. Organisations can request a copy of this paper by emailing itseag@dbcde.gov.au.

****

Acknowledgement: The input of **Sense of Security** in undertaking consultations with members of the ITSEAG and drafting content is acknowledged.