NCSC Security Advisory – NCSC-ADV-201310-0019 **31 October 2013**

Mobile Electronic Device Risks

The sophistication and versatility of modern mobile electronic devices means that they are often used to extend office functionality outside of the workplace, both nationally and internationally. Modern mobile devices are capable of running numerous applications, and offer capabilities and features even beyond those commonly found on more expensive laptops and computers.

In terms of convenience, connectivity and increased productivity the benefits of mobile devices are undeniable. However, their use does not come without increasing risk and they should be used in strict compliance with corporate policy and security guidelines.

The Risks

Mobile devices are used to store and communicate sensitive, high-value, corporate and personal information and as a result they can become a target for persistent and sophisticated attack from persons wishing to implant malicious code or extract information.

Loss or Theft

The size and portability of mobile devices means that they may be easily lost or stolen. This can lead to the exposure of sensitive Information stored on the device as even complex passwords offer only limited protection.

Confidentiality

Using mobile devices in public spaces can increase the potential for information to be overheard or overseen.

Electronic Interception

Communications over wireless networks are vulnerable to security compromise and as a result voice, email and internet information can be intercepted and possibly altered. Software exists that can disable security features and even activate in-built microphones and cameras for the purpose of overseeing activities, or eavesdropping conversations.

Tracking

Many modern mobile devices contain built in GPS receivers and transmitters which may allow the precise location of the user to be determined. Use of social media sites and some applications may also reveal location information.

Malware

Just like any home or office computer, mobile devices are susceptible to threat from malicious software (malware) which can be passed onto connected networks and other computers. Gift items such as USB devices, CDs and DVDs are sometimes used to distribute malicious software.

External Storage

Using external devices such as USB drives and other storage media to store or transfer data can increase the risk of introducing malware and unauthorised data exfiltration.

The Impact

The compromise of mobile devices can result in the loss of sensitive, high-value, corporate and personal information, potentially impacting on business profitability and corporate reputation.

Risk Mitigation

The following mitigations should be considered to help increase the security of information and communications stored or transmitted using mobile devices. While this advice relates to general security around the use of mobile devices, it is important to apply when travelling overseas and working in areas where there is an increased threat:

Pre-Deployment/Travel:

- Ensure that mobile devices have been updated with security and application updates.
- Enable mobile device security features and ensure that PINs and passwords are changed. Always use complex passwords containing upper and lower case letters, numbers and symbols.
- Reduce the risk of information exposure by removing any information that is not required for the deployment or period of travel.
- Backup your information. If your device becomes compromised you may not have the opportunity to recover information from it.
- Ensure you are aware of emergency security procedures for the mobile device.

Device Handling:

- Maintain physical control of mobile devices at all times. Do not leave mobile devices unattended in places where they may be an easy target for theft or tampering.
- Avoid taking mobile devices into situations where sensitive or confidential conversation is likely. Where this cannot be avoided, turn off the device and remove the battery.
- If you have lost physical control of your mobile device (e.g. when secured outside a meeting) check with your ICT security staff for guidance prior to using it again.

Secure Usage:

- Never use personal mobile devices for official business. Use only Corporate devices with all security measures enabled for storing, processing or communicating sensitive or confidential information.
- Be vigilant at all times. When using a mobile device, make sure that conversation cannot be overheard and screen data cannot be seen by others.
- If the risk of tracking is a concern ensure any GPS capability is disabled. For extra security turn off the mobile device and remove the battery.
- Disable any features or capabilities that are not required. For example, disable wireless, Bluetooth and location services when they are not required.
- Always confirm the integrity of any new storage media with your ICT security staff prior to connecting it to your mobile device. All storage media should be regularly scanned for threats.

Email Usage:

- Never use private email accounts to store or communicate corporate information.
- Never forward email from corporate email systems to private email accounts.
- Ensure that all email connections are encrypted.
- To reduce the risk of downloading hidden malware, disable image-loading in your email application.

Internet Usage:

- Activate ‘privacy mode’ in your internet browser.
- Set your internet browser to prompt before installing cookies.
- Turn off auto-fill to prevent your browser from storing usernames and passwords.
- Never join or connect to untrusted wireless networks. Make sure that your wireless settings require manual confirmation before connecting to a wireless network.

Post-Deployment:

- Following your deployment/travel it is prudent to change all mobile device passwords.