TISN
FOR CRITICAL INFRASTRUCTURE
RESILIENCE

Mobile Device Security Information for IT Managers

July 2012

Executive Summary

Mobile devices[1] and portable media provide significant value add to organisations but risks associated with their use need to be managed. The IT Security Advisory Group[2] (ITSEAG) of Australia's Trusted Information Sharing Network (TISN) for Critical Infrastructure Resilience encourages IT Managers to examine their policies and procedures for controlling the use of these devices within their organisation and importantly, identify and address the ever increasing security risks they pose, especially to commercially sensitive information.

Mr Geoff Rhodes, the Chair of the ITSEAG, said "Organisations need strategies in place to manage how these devices are used by their employees. Organisations should regard all mobile devices as being 'tainted' and adopt a data centric, rather than device centric, approach to security. Managing the data stored on corporate owned devices is problematic, but if employees are allowed to use their own devices (Bring Your Own Devices (BYOD)) within the workplace, then managing any corporate data stored on those devices is a logistic and legal minefield."

These devices are being built with leading edge technologies that enhance their functionality, power, capacity and connectivity. However, they are usually released into the market with minimal security features which can be easily bypassed. It is expected that the use of mobile devices, including privately owned devices, in the workplace will escalate rather than decline.

Introduction

Mobile devices are changing the way people live, work and communicate, making the world more interconnected and integrated. Executives and other employees are expecting, even demanding, access to their work resources through a myriad of mobile devices. The use, and especially uncontrolled use, of mobile devices in the workplace, introduces many risks. Organisations need to assess and manage their risks because security breaches, such as the loss or theft of information assets, could have significant impact.

Currently, many organisations have difficulties in effectively managing the use of legacy mobility solutions and devices. Coping with the rapid development in mobile device technology will require IT Managers to increasingly devote more resources to strengthening security controls, which should be aligned to safeguarding valuable and sensitive information.

Organisations need a considered approach to managing the use of mobile devices, deciding which devices they can manage, within acceptable risk tolerances, and which devices should be blocked from use. Appropriate application, networking and security architectures should be in place to control the use of all devices (including unmanaged devices) that are permitted to interface to the corporate network.

---

[1] Mobile device referred to in this paper include smartphones, tablet computers, laptops, PDAs, storage devices (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.

For owners and operators of critical infrastructure, the use and integration of these devices into the corporate network is extending beyond accessing corporate data, with applications now supporting mobile SCADA and web SCADA solutions [1]. Data flows are moving beyond the perimeter of the conventional office, possibly across international and national boundaries. Organisations need to address cross-border data security issues, and be aware of relevant mobility practices and other technologies, such as cloud computing.

Other issues and risks that need to be carefully considered regarding mobility include the type of applications used, how data is protected within the device and backed up, and the data retention and disposal issues. Storing organisational data outside of the IT system in which it is being used has always been a source of risk.

Traditional information security models that assumed end-to-end ownership and device control are no longer adequate. Organisations should be focussing their attention on data centric models, rather than system or device centric models, ensuring they have appropriate security. This is particularly relevant for critical infrastructure organisations, as the information they hold and systems they manage, can be highly sensitive and of significant importance to the safety and well-being of the community.

The potential cost of a data breach can be very high, possibly resulting in the impairment of ICT and infrastructure operations and the exposure of confidential information – leading to loss of reputation. Organisations need to adapt their information security initiatives to include mobile device security, clearly understanding the extent of their exposure and associated risks.

Establishing a mobile security strategy that defines appropriate policies, procedures and technologies, mandating the approach to be used by the organisation to protect their systems and data is strongly recommended.

Risks and Issues

Mobile devices of today are effectively small computers, with the computing power, memory and storage of desktop computers from many years ago. They are prone to becoming a target for computer viruses and sophisticated mobile malware and are a threat to the confidentiality, integrity and availability of corporate systems and data. Mobile devices infected with malware can impact the security of corporate systems. They could be used as proxies to gain access to sensitive data, intercept and relay messages to attackers or even send messages to ‘premium service’ SMS numbers without knowledge of the mobile device user [2].

The risks to critical infrastructure owners and operators are elevated because mobile devices are now used to remotely manage critical infrastructure over the Internet or wireless networks[3] [1,3]. This includes the ability to control systems, view data and generate reports using mobile SCADA. This capability to perform remote management of critical infrastructure using mobile devices represents a new dimension with its own risk profile, compared to traditional systems which were limited to private networks with communications over lease line and/or private radio systems.

[3] Modern mobile devices are expected to natively have the capability to access 802.11 Wi-Fi Networks. SCADA networks that run on, or are managed over other industrial wireless technologies such as sensor networks and licensed-band networks are not in scope for this paper.

The use of mobile devices has extended the virtual boundaries of the organisation, blurring the lines between home and office by providing constant access to email (corporate and personal), business applications and sensitive corporate data. As with computers in the workplace, it is highly likely that both business and personal data will co-exist on the mobile device. Due to their size and portability, mobile devices are more prone to loss and theft. A Ponemon global study released in 2012 involving 4060 IT and IT security practitioners from 12 countries (including Australia) revealed that 51% of organisations have experienced data loss in the past 12 months resulting from employee use of mobile devices [4]. Another global survey conducted by Ernst & Young in 2010 indicates that applications and connected database and data leakage was amongst the top 5 risks from the use of mobile computing [5].

The key risks and issues associated with the use of mobile devices are discussed below.

Key Concerns

- **Use of Personal Mobile Devices.** Mobile devices, much like laptops, have become yet another endpoint connecting to the corporate network. With reference to Bring Your Own Devices (BYOD) practices, organisations may be expected to endorse the use of personal mobile devices for business purposes. While it offers potential cost savings, BYOD has its own challenges. For example, the diversity of devices presents complexities in mobile device management (MDM) strategies. The lack or inconsistency of security controls across BYOD increases the security risks for the organisation [6].

  Unmanaged mobile devices accessing corporate information could lead to corporate data leakage through connections to unauthorised wireless networks. Such devices can also play a role in a 'man-in-the middle' attack, wherein an attacker uses a mobile device to listen in on or modify legitimate communications [7]. SMS authentication systems leverage mobile devices to provide two factor-authentication (2FA) where a 'One-Time Password' is sent via text message to the user's mobile device, removing the need for a separate token. Malware on such a device may allow this information to be forwarded to attackers trying to circumvent the 2FA controls [2].

  Poor security controls on these devices may allow unauthorised access to corporate information, including sensitive critical infrastructure data, if a device is lost or stolen. Apart from technology risks presented by BYOD, a primary issue faced by most organisations is data ownership. The challenges of implementing corporate imposed security controls on personal owned devices include vagaries with securing and controlling a device that is not company owned - such as deleting sensitive data when employee is terminated, enforcing security policies and restricting the use of authorised applications [8].

  These vagaries have both legal and privacy implications. Employees expect companies to support their devices but will have reservations regarding where the company has crossed its boundaries for management of a device that he/she owns [8]. However, from a company perspective, the enforcement of security controls on all devices with access to the corporate data is imperative. Without clear policies, an organisation could lose control of its corporate systems, including SCADA systems.

- **Use of Mobile Device Applications.** The rapidly expanding market of mobile devices and their open programming platforms offer organisations significant opportunities to interact with customers and employees by redesigning websites to accommodate mobile device users. An example is the development of customised web based SCADA systems to eliminate the need for expensive SCADA control rooms [1]. Mobile device security requirements may not be fully considered, and in most cases, application functionality is chosen over security when trade-offs are to be made to applications [9]. This often opens up security weaknesses which could be exploited by malware and/or unauthorised users.

  In addition, the mobile device has become a prized target, where there are increased numbers of malware targeted at intercepting valuable data [7]. Ponemon's survey indicated that 59 per cent of malware infections are caused due to employee's use of mobile devices in the workplace and 58 per cent say that the increase in malware infection is a result of personally owned mobile devices in the workplace [4].

Related Security Risks

- **Device Modification.** Unauthorised modification of devices represents an additional level of risk. The terminology frequently applied to this practice is jail-breaking (Apple iOS devices) or rooting (Android devices) which removes vendor imposed limitations on the mobile devices. This leaves the device in an insecure state, making it more prone to malware and compromise.

  Unauthorised applications can be created to take advantage of the elevated privileges in these devices to manipulate data, e.g. report false results to central management system (critical infrastructure) and other security tools that it is reporting to. Users of these modified devices can remove any centrally applied corporate policy controls on the device, making it more vulnerable to other security threats.

- **Information Protection and Backup.** The more that organisations rely on and use these mobile devices, the more likely that these devices will contain critical information. Sensitive data on the device itself must be protected. Encryption and authentication of data has been acknowledged as a primary measure to protect confidential information [10].

  Organisations are now concerned with mobile device and data synchronisation. The loss of the device could pose operational challenges if the device or the data cannot be recovered and restored onto a new device. The challenge is how data on these mobile devices can be backed up, and the backup protected, so that they are not targeted as the weak link to bypass other more complex controls [10]. Employees, allowed to use their personal devices, may be able to perform local backups, potentially allowing the sensitive data to remain unprotected.

- **Data Retention and Device Disposal.** The amount of data that can be stored and processed in mobile devices has grown dramatically. The introduction of tablets, such as the iPad, introduced a mobile device that bridged the gap between smart phones or PDAs (too small), and laptops (too bulky and heavy). Current devices can have 64GB of native storage with further extension support to other mass storage media. This increased use of the inherent storage and computing capacity of mobile devices has created a new data retention risk. As an example, one trend is the popularity of iPad's for use by company board members to access board reports and other confidential corporate data. While the electronic copies of board papers made available on the device may be secure, annotations made to/for a document on the device itself, which constitute legal documents, are not captured or stored under corporate ownership. This is important for complying with statutory record keeping requirements and for preventing legal risks[4]. Given that the device is likely used for personal and company purposes, and with board members frequently active across various boards, the device may store vast amounts of company sensitive information and may be vulnerable to unauthorised access or insecure wireless access [11].

  Inappropriate device disposal procedures may also present the risk of sensitive information being retained on the device and unauthorised access. Corporate computing assets should be subject to company asset management procedures which should include secure disposal for assets containing sensitive data [12]. However, the execution of these procedures can often be a grey area when dealing with personal devices in the workplace. This requires clear organisational policies in order to safeguard sensitive, confidential and highly valued information (including commercial intelligence).

- **Cross-border Data Theft.** Mobile devices as a vector for data to leave the organisation is nothing new, as the inherent mobility (beginning from laptops) has always made it impossible to rely on a strong perimeter for adequate protection. The cloud computing revolution and the myriad of hosted application services that are not geographically fixed has made it easier for data to cross national borders [13]. With the increased use of mobile and Internet SCADA, the applications and data stored in mobile devices lost locally and globally, may put critical infrastructure at risk. In addition, data travelling on the mobile devices is typically subject to laws and regulations that will vary from one jurisdiction to another.

- **Privacy and Legal.** There are also inherent privacy and legal risks associated with mobile devices and with the strategies used by organisations to maintain control over the environment. Organisations may use solutions to routinely scan computers and mobile devices connecting to the corporate network in order to verify adherence to security policies and detect any unauthorised sensitive data. The implications of such scanning activities are compounded with the adoption of BYOD practices. Ultimately, the exposure of sensitive corporate data or employees' personal information can result in damage to an organisation's reputation. Company Directors have an obligation to take reasonable measures to protect their organisation's sensitive information. This duty of care may extend to protection of personal information as well.

[4] *Income Tax Assessment Act 1936:* section 262A requires entities to keep records that record and explain all transactions and other acts relevant to the Act for a period of 5 years; and Corporations Act 2001: section 286 requires companies to retain documents which disclose the company's transactions, financial position and performance for a period of 7 years after the transactions covered by the records are completed.

The popularity of geolocation or location-based services technology compounds the privacy risks with the additional information of physical location, which can be taken advantage of by people with malicious intent [14]. Such risks apply to SCADA systems as well where location based service is able to provide information such as utility location, personal or asset tracking, and route guidance information [1].

Outsourcing mobile device management creates another level of data protection and privacy risk for the organisation. This may include the geographical location of information and business functions, applicable legal requirements based on location, transparency over security controls and segregation of data and infrastructure between customers [15]. Legal issues could also arise during a security incident including ramifications to the cross border issues mentioned earlier.

Together, these issues and concerns related to the increased use of mobile devices present clear challenges to the organisation. The security threats to mobile devices have evolved to include all the threats applicable to desktops, plus new threats that are unique to mobile devices. Mobile devices need to be protected, with an even broader set of security mechanisms than those employed for traditional desktop environments.

Implementing a Mobile Security Strategy

Organisations need to closely examine the risks posed by the use of mobile devices and manage them based on their risk profile. Information security policies and procedures and corporate governance measures should extend to include mobile device security. Creating a mobile device strategy will help ensure that risks are accounted for and managed appropriately. The strategy should focus on several key areas such as data accessible from mobile devices, mobile device platform to support, centralised management methodology and best practices.

Policy Controls - First and foremost, organisations should adapt and/or extend its security policies to cover mobile device usage and risks in order to deliver effective protection of corporate information and other sensitive data. To define a policy the following points need to be addressed: [7,16]:

- Identify platforms to support and set policies for them;
- Define the business data to be stored and processed on the devices;
- Extend data disposal and retention policies to include mobile devices;
- Set terms of use of personal owned devices for business use (Acceptable Use Policy);
- Clarify ownership of data residing on personal devices and understand the organisation's capabilities for managing remote devices;
- Ensure privacy and legal implications are managed appropriately for BYOD and corporate mobile devices;
- Set restrictions on mobile application usage (business and personal applications);
- Implement centralised device backups that are protected;
- Monitor and report on the status of devices for compliance;
- Restrict the use of security compromised devices ('jail broken' devices), and
- Establish clear policies prohibiting posting of company data to forums, social networking sites, etc.

For the above items to be effective there should be consensus between the organisation and employee on data ownership and responsibilities. This will set the expectations and assist in defining, implementing and enforcing the security controls required for adequate protection of data.

Application Usage – In addition to applications such as email, contact and calendar information, the development of customised mobile applications by organisations now allow access to business-critical applications by employees and possibly by partners, suppliers and clients. As with any business application, the development of mobile applications should follow secure development lifecycle practices. Information accessed by and stored on these devices should also be classified based on security requirements which specify corresponding security controls that need to be applied to it. Information on mobile devices moves from more protected locations (internal network) to less protected areas (outside of the corporate network perimeter). Security classifications should define what applications and/or data are available for use outside of the corporate environment. Employees need to understand they are accountable for information security and accept responsibility for it. This requires Security Awareness and Acceptable Use Policies to be in place.

Platform Support - Mobile device platforms to be supported in the business environment need to be determined and should include a clear understanding of the risks including if/how BYOD practices will be permitted. The variety of device platforms present can each have an implication on organisation-wide security. However, a baseline of security controls needs to be consistently applied across all platforms. This may require the organisation to specify what platforms and device firmware versions will be allowed for use within its corporate environment in order to contain mobile device management and support requirements.

Leverage Existing Controls - Existing policies and best practices for laptops and desktops can be adopted for mobile devices. Such practices include:

- Registration and inventory of all mobile devices;
- Centralised installation and configuration of security applications;
- Managed updating of security patches [17], policies and settings;
- Device provisioning and de-provisioning process;
- Comprehensive reporting of security policy enforcement status;
- Capability to conduct forensic investigations on all device types;
- Defining roles and responsibilities for management and administrator of the devices, and
- Incorporating mobile device security in the security awareness program.

Security Controls – An effective mobile devices strategy requires strong security controls. This should include technical as well as controls from a governance and compliance perspective (refer to the 'Appendix' for a list of critical factors to consider when selecting centralised mobile device management solution). The following are the minimum security controls that organisations should consider [9,18-19]:

Security Controls	Preventive	Detective	Corrective
Access Control	• Enforce strong passwords • Use two-factor authentication	• Extend existing auditing and monitoring controls around mobile device connections	• Conduct regular reviews of devices connecting to corporate network
Data Protection	• Encrypt business data • Limit the sensitive data transferred to mobile devices, or implement least privilege access • Implement remote device management • Enable device-lockout function when the device is not in use	• Perform technical security assessments on mobile devices and supporting infrastructure with emphasis on data stored on devices • Monitor access and usage of high-risk data to identify potentially inappropriate usage	• Implement appropriate measures to eliminate or reduce the risk impact - either by enhancements in technology or by updating the policies/procedures
Application Security	• Allow only certified business applications	• Regularly monitor installed applications to identify risks to corporate data	• Remove applications identified to be untrustworthy or malicious
Fundamental Controls	• Install anti malware software • Install and manage personal firewall to permit only authorised traffic	• Regularly monitor compliance reports • Setup alerts to identify changes	• Eradicate and/or repair any devices identified to be non-complaint from company defined policy
Governance and Compliance	• Include mobile security into the organisations risk management program • Add mobile security awareness to existing employee awareness programs • Implement mobile device policies and include them in them in the Acceptable Use Policies	• Add mobile devices in the organisations audit program • Monitor and maintain logs of mobile device interactions with corporate network	• Address and mitigate any non-compliance • Incorporate mobile devices into incident response plan • Regularly review mobile device acquisition and usage

Conclusion

It is essential that organisations have suitable strategies in place for securing mobile devices. This paper provides high level information on key concerns and items to consider for a mobile security strategy.

Organisations must now focus their attention on data centric models, rather than system or device centric models, to ensure they have appropriate security coverage.

The human element will remain a critical factor in achieving effective organisation wide data security where the devices are ultimately used by people on a daily basis. Accordingly, mobile security should be addressed in employee awareness programs. Your IT policy should also govern acceptable use of these technologies. This is particularly relevant when dealing with the "Bring Your Own Device" phenomenon.

As applications inevitably move towards the cloud and the workforce becomes more mobile, the risks of adopting such platforms should be thoroughly assessed. At a minimum, consider limiting the sensitive data transferred to mobile devices, or consider view-only access.

It is also important to address the privacy and legal aspects of using personal devices in a corporate environment. Data travelling on these devices across borders may be governed by the laws, and be subject to the jurisdiction, of that location. Legal issues could also arise during an incident which will require the organisation to have the ability to respond appropriately.

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.

****

NOTE: 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[5] issued by the IT Security Expert Advisory Group (ITSEAG). Rather, this paper focuses on issues specific to mobile devices, and in particular smartphones and tablets, above and beyond those associated with computers in general.

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

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

Appendix

Critical factors to be considered for selecting a mobile devices management solution [7]:

Factors	Description
Architecture	Choose solution based on client server model which centrally controls and manages security policies, report status and deploys authorised applications.
Support for platforms	The solution should be capable of supporting variety of mobile platforms with consistent and easy to use administration console.
Feature expandability	With rapid advancements in mobile device technology and new threats ever evolving, the solution must be flexible enough to accommodate such changes in technology and incorporate capability to counter new threats.
Usability	The solution should include features that are easy to use and requires little administration and end user intervention.
Reporting and Analysis	The solution should be able to support organisational policy and regulatory compliance requirements to effectively measure solutions effectiveness in countering threats.
Deployment and Management	The solution should be efficiently deployed and easy to manage. This should also include overall efforts required for initial rollout and ongoing management of the solution.
Roles and Responsibilities	Responsibility for overall mobile security implementation effort and management and subsequent management of the solution needs to be defined. This would set the expectation upfront, particularly in a global heterogeneous environment.
Skill sets	For deployment, management and support of the solution, it is important to assess the skill sets available. As this could effectively translate into saving time and reducing cost by choosing in-house or managed service. However, this could prove to be critical in global and heterogeneous environments.

References

1. Kim T, *SCADA Architecture with Mobile Remote Components*, WSEAS Transactions on Systems and Control, vol. 5, no. 8, Daejeon, Korea, 2010.
2. Trend Micro, *Android Malware Acts An SMS Relay,* Latest Security Trends, 2012.
3. Ozdemir & Karacor, *Mobile phone based SCADA for Industrial Automation*, ISA Transactions, vol. 45, no. 1, pp. 67-75, 2006.
4. Ponemon Institute, Global Study on Mobility Risks: Survey of IT & IT Security Practitioners, Ponemon Institute Research Report, February 2012.
5. Ernst & Young, *Borderless Security: Ernst & Young's 2010 Global Information Security Survey*, 2010.
6. Bradford Networks, *Bring Your Own Device (BYOD) Unleashed in the Age of IT Consumerization*, white paper, 2011.
7. Kao, I, *Securing Mobile Devices in The Business Environment,* IBM Global Technology Services – Thought Leadership White Paper, October 2011.
8. Profitline, *The Hidden Risks of a "Bring Your Own Device (BYOD)" Mobility Model*, Profitline Mobility Whitepaper, 2011.
9. Ernst & Young, *Mobile Device Security – Understanding Vulnerabilities and Managing Risks*, Insights on IT Risk Technical Briefing, January 2012.
10. National Institute of Standards and Technology (NIST), *Special Publication 800-111: Guide to Storage Encryption Technologies for End User Devices*, Nov. 2007.
11. Better Boards, *Is The iPAD Invited To Your Board Meeting?,* http://betterboards.net/articles/ipad-board-meeting, viewed 21 March 2012.
12. National Institute of Standards and Technology (NIST), *Special Publication 800-124: Guidelines on Cell Phone and PDA Security,* October 2008.
13. Ernst & Young, *Data Loss Prevention: Keeping Your Sensitive Data Out of The Public Domain*, Insights on IT Risk Business Briefing, 2012
14. ISACA, *Geolocation: Risk, Issues and Strategies*, Emerging Technology White Paper, September 2011.
15. TISN. Securing Information in an Outsourcing Environment (Guidance for Critical Infrastructure Providers), Trusted Information Sharing Network, June 2011.
16. Jogani, A, *Governance of Mobile Technology in Enterprise*, ISACA Journal Online, 2006.
17. Defence Signals Directorate, *Strategies to Mitigate Cyber Intrusions*, Cyber Security Operations Centre, 21 July 2011.
18. Defence Signals Directorate, *Australian Government Information Security Manual*, Defence Signals Directorate Publications, August 2011.
19. Defence Signals Directorate, ISM Standards: Working Offsite and Media Usage.