

Control Essentials

Volume III, Issue VII

July 2008

Are Your Mobile Devices Keeping You Up At Night?

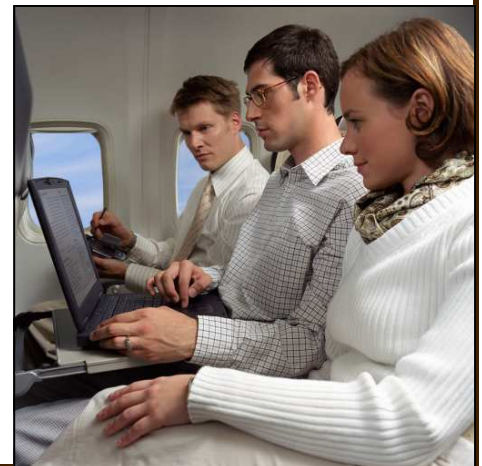
Mobile devices are increasingly becoming a huge part of almost every organization's communication arsenal given the enhanced efficiency, flexibility and productivity they bring to the global market. Over the last couple of years the use of mobile devices has grown exponentially and the trend is expected to continue due to the capacity and new features these devices are being enhanced with, which gives them the capability to perform a lot more functions irrespective of their size. However, with the many advantages of mobile devices, comes increased security threats and compliance issues every organization faces. Therefore, regulations such as Sarbanes Oxley, GBLA, HIPAA, and PCI DSS have to be complied with by ensuring that the use of mobile devices is well controlled and managed to meet expected requirements.

According to a recent study by Business Performance Management (BPM) Forum¹, over 40% of all organizations do not have formal policies and/or systems in place that deal specifically with the use and management of mobile devices, most of which projected that the use of mobile devices will increase to an average of 24% in the next couple of years in their respective organizations. More than 25% of these mobile devices used by employees were said to have very critical applications and confidential information stored on them. This opens up organizations to the various malicious threats that come with the use or misuse of these devices, thus leading to a possible security breach which could well be avoided by implementing an adequate mobile security management infrastructure.

The responsibility of securing mobile devices is a task that cannot be handled by IT alone. Even when the best technological tools are in place, not having the support of management, or implementing and enforcing adequate policies with regular training of employees on mobile security issues; it is evident that mobile device security will not be given the priority and attention it requires in an organization.

What can go wrong will go wrong

A number of things can go wrong with the use of mobile devices, from employees losing the device to a virus infecting the device. An excellent approach is to have an overview of the likely threats and risks mobile devices bring to your organization as this will assist in developing, implementing and enforcing the appropriate controls, policies and procedures needed, tailored specifically to your organization's needs.



IT Security:

- Information security design and Implementation
- Vulnerability Assessments
- Penetration Testing
- Security Breach Investigation and Remediation
- Business Continuity Planning
- Logwatch
- Training

Risk Management:

- Risk Assessment
- IT Risk Advisory
- Fraud Detection

Forensic Services:

- Computer Forensics
- E-Discovery

IT Audit Services:

- Application and System Implementation Reviews
- Internal Information Systems Audits

Regulatory Compliance:

- Bank Secrecy Act
- Gramm-Leach-Bliley Act
- Fair and Accurate Credit Transactions Act
- Sarbanes-Oxley Act
- Health Insurance Portability and Accountability Act
- Family Educational Rights and Privacy Act
- Payment Card Industry

Attestation Services:

- SAS 70 Reviews
- Other Attestation Services

Common Threats

Unauthorized Use and Access

Almost everyone has mobile devices, so what is your organizations approach to having employees connect personal mobile devices to organizational networks? The lack of adequate management oversight and control over the use of personal mobile devices on corporate networks can pose a number of problems to any organization starting with the obvious fact that the mobile device may not be properly configured to meet the security policies and requirements of the organization, and may also lack the suitable antivirus installed. Add to this the notion that such a device may be used to download proprietary company information, and you suddenly have quite a handful to deal with. Personal mobile devices should not be allowed to gain access to the corporate network. This can be done through the use of digital certificates called a policy certificate which ensures that the device trying to connect to the network is authorized and has the right policy configurations, thus restricting communication and resource access to only what is defined by the policy certificate. With mobile devices, guarding your network becomes that much more intricate due to the fact that you now need to be on the lookout for attackers from the outside as well as those within.

Virus Infection

Some mobile platforms, such as Symbian, Windows Mobile, Blackberry and J2ME have had several cases of virus infection, some can make devices unusable or unable to boot up and may even wipe out their memory or can steal contact information, address lists, message logs and call logs and also allow hackers to tap and listen to phone conversations. Viruses can spread from device to device within a short range without the knowledge of the user through any Bluetooth device. It is for this reason that it is advised to turn off mobile devices when not in use. The critical issue here is that having mobile devices on the network can serve as agents that aid the propagation of viruses if not properly managed. Some viruses that affect mobile devices can be viewed in Table I.

Mobile Device Platform	Virus	Propagation Method	Vulnerability
Blackberry	BBProxy		It uses BlackBerry devices as a gateway to gain access to the enterprise network
Symbian	Cabir worm	Bluetooth device	The message 'Caribe' is displayed on the phone's display and is displayed every time the phone is turned on
Symbian series 60	Commwarrior-A	Multimedia Messaging System (MMS).	It sends infected files under a random name to various devices listed in the phone user's address book
PocketPC platform	Duts		It attempts to infect all EXE files in the current directory (infects files that are bigger than 4096 bytes)
	Skulls		It replaces all phone desktop icons with images of a skull. It also renders all phone applications, including SMSes and MMSes useless.
Symbian	Acallno		Forwards all incoming and outgoing SMS to an external number

Loss or Theft of Device

Mobile devices are really easy to lose and are also a great target for thieves waiting to quickly grab unattended mobile devices at any given opportunity. According to Wisconsin Technology Network², about 250,000 mobile devices will be forgotten at US airports this year and only about 30% will get back to their rightful owners. There are numerous cases of lost or stolen laptops containing highly sensitive information; this seems to be a regular occurrence and is obviously not a good scenario for any organization to deal with. Unfortunately having certain confidential information such as customer data, useful contact information, credit card information, social security information, employee records or proprietary information getting into the wrong hands would give any organization bad publicity and a heavy possibility of legal issues to deal with, as many states have laws that require that any security breach that involves loss of confidential client data to be reported.

While it would be wishful thinking to believe that theft of mobile devices can be completely avoided, there are certain precautions that can be taken to mitigate the after-effects of such an occurrence –

- Employees should be trained well to know the precise steps to be taken in the event of a loss or theft of a mobile device. Organizations must implement and enforced policies, controls, procedures as well as regular security awareness programs for all employees. For instance, when an employee loses a mobile device, IT should be contacted immediately to disable the access of the device to the network and also possibly initiate a remote wipe-off of all data contained on the device. This will ensure that access cannot be gained into the company network from the device and that all important data on the device is sanitized.
- Centralized management of mobile devices can also make it easier to enforce password controls. Although these can be bypassed by reading the device memory directly, without starting the operating system, it serves as a barrier for an unsophisticated thief. Another thing that should be strongly considered is the encryption of data on the mobile device. This will make it difficult for a thief to gain access to any sensitive information on the device.
- The proper disposal of mobile devices is another aspect that organizations should have formalized and enforced control measures. Having your organization's laptop or PDA for sale on e-bay with confidential customer data left behind on it is not a very great picture. Therefore, there needs to be a formalized and enforced control of sanitizing data on mobile devices before discarding them.
- Employees should also have regular mobile security training and awareness programs where they are informed of their responsibility of securing any sensitive information they have on their mobile devices. It is important to ensure that information on mobile devices is adequately backed up and archived based on your organization's policy and compliance requirements, this way the loss of a device will not affect access to critical data or information needed for daily business operations.



Action steps

It is important that management is made to understand the importance of mobile device security. Even if your organization is not open to the risks that come with the use of mobile devices at the moment, there is no doubt that the near future will bring the concern with it. Outlined below are a few points of consideration –

- Maintain an inventory of the mobile devices in your organization and find out who they belong to, what they are used for and what applications or resources they have access to.
- Assess the possible risks and threats that come with the use of these devices in your organization and the likely impact they will have on your business.
- Ensure that you have implemented sound security measures (physical and Logical) to protect resources stored on mobile devices and comply with applicable security related regulations. Develop and enforce procedures to address various security aspects of mobile devices such as backups, archiving, dealing with lost/stolen devices, software upgrades and patching, method of disposal for old mobile devices and also the encryption of data at rest using secret key algorithm which provide only confidentiality or public key algorithm which provides both authentication and confidentiality and encrypting data in transit using Secure Socket Layer (SSL) which is relatively cheap and does not require additional client software installation or Virtual Private Network (VPN) which require client software installation and can be expensive to implement.
- Conduct regular security training and awareness programs for employees. The importance of security training and awareness cannot be overemphasized.
- Implement a mobile device management system that gives you adequate control over your mobile devices, putting into consideration some enterprise concerns which include data protection, intrusion, spyware and administrative cost. In table 2 are some mobile device management products that have features such as, authentication, firewall, anti-spyware and a consolidated administrative console for mobile devices and PCs to reduce cost this can assist your organization in implementing a more controlled mobile device environment.

PRODUCT	FEATURES
MFORMATION SERVICE MANAGER	Provides solutions for Open Mobile Alliance Device Management-based provisioning and configuration, Firmware Over-the-Air management, smartphone application management (including Linux, Microsoft Windows Mobile, RIM and Symbian OS devices), diagnostics, security management, enterprise management.
Afaria	<p>Security</p> <ul style="list-style-type: none"> Centrally enforce corporate security policies Full disk encryption for laptops Email and PIM encryption on handhelds Over-the-air encryption Temporary password recovery Management and security from a single console Update application and data as needed Manage groups or individuals Over-the-air software distribution <p>Supports Any mobile device Windows Mobile (Pocket PC, Windows Mobile 5.0, smartphone), Windows Notebooks, RIM BlackBerry, Palm OS, Symbian</p> <p>Supports Any wireless connection GPRS/EDGE/3G,W-LAN e.g. 802.11b/g, Infrared, Bluetooth</p>

PRODUCT	FEATURES
BlackBerry Enterprise Server	<p>Supports more than 100 over-the-air wireless IT policies and commands that enable IT administrators to:</p> <ul style="list-style-type: none"> Impose device lock-down Wipe data from lost or stolen devices Define and wirelessly enforce security settings such as Bluetooth® lockout and controlling access to voice calling <p>Enables IT departments to deploy wireless network and systems management solutions, including remote IT administration, workflow management for service management and server monitoring.</p> <p>Encrypted attachment viewing for S/MIME and PGP email PIN-to-PIN and SMS message auditing — enables compliance with government regulations and provides a log of all phone calls Support for S/MIME encrypted email — ensures email security is maintained during wireless transmission Other critical security features — includes support for hard deletes, backup/restore of saved messages, SNMP monitoring enhancements and enterprise device authorization</p>
System Center Mobile Device Manager 2008	<p>Encrypted access to e-mail messages and line-of-business (LOB) applications through the Internet Active Directory® Domain Services authenticated network access Device inventory and health inspection Application approval and blocking by using Active Directory Group Policy Remote device wipe to remove sensitive data from lost, stolen, or compromised devices</p> <p>Supports controlled and managed device enrollment process before a device is allowed to become a trusted device and a member of the Active Directory domain. Ensures devices follow the required policies and software package updates, supports management of device loss or theft.</p>

Table 2

Conclusion

As new vulnerabilities are exploited everyday and organizations face more targeted threats, it is critical that your organization remain at the cutting edge of mobile security. While there is no such thing as perfect security, a responsible attitude towards mobile device security will earn you good dividends in the long run.

¹ Workforce Management - The Risky Business of Mobile Device Compliance in the Workplace - *By Stefania Viscusi* (November 27, 2006)

<http://www.tmcnet.com/channels/workforce-management/articles/3774-risky-business-mobile-device-compliance-the-workplace.htm>

² Viewpoint - Risky Business: The Mobile Device Security Disconnect - *By Tyson Greer* CEO, *Ambient Insight* (November 2007)

<http://www.microsoft.com/technet/community/columns/secmgmt/sml107.mspx>

Best Boutique Risk Management Firm in South Florida.

SOUTH FLORIDA CEO MAGAZINE, 2006

KEEPING WATCH OVER YOUR BEST BUSINESS INTERESTS

ERM professionals bring a unique mix of strong academic backgrounds complemented by professional experience ranging from "Big Four" consulting firms to major corporations and prestigious professional certifications. A snapshot of ERM's pro file can be seen below:

Education

Qualifications

M. S. in Computer Information Systems
M. S. in Information Networking
M. S. in Management Information Systems
Master of Accounting Information Systems
Master of Business Administration

Universities

Carnegie Mellon University
Syracuse University
Xavier University
University of Miami
Florida International University

Certifications

Certified Public Accountant (CPA)
Certified Information Systems Security Professional (CISSP)
Certified Information Systems Auditor (CISA)
Certified Information Systems Manager (CISM)
Certified Information Technology Professional (CITP)
GIAC Security Essentials Certification
GIAC Systems and Network Auditor
Microsoft Certified Professional

Prior Work Experience

PriceWaterhouse Coopers
Deloitte
CERT® Coordination Center
SONY Electronics Latin America, Inc.
RJR Nabisco
Diageo plc
Arthur Young
Carnegie Mellon CyLab
Evertec Inc.
American Bankers Insurance Group
Chesebrough Pond's
Starboard Cruise Services, Inc.

Some of our Clients...

ABN AMRO Private Banking
Bacardi-Martini, Inc.
Carnival Cruise Lines
CitiBank
Commerce Bank
Florida Power & Light Company
Knight Ridder
North Broward Hospital District
Ocean Bank
Rinker Materials
Sylvania Lighting International
The International Bank of Miami

enterprise risk management

The Control Professionals

800 S. Douglas Road, North Tower # 835,
Coral Gables, FL 33134.
P: (305) 447 6750 F: (305) 447 6752
Email: info@emrisk.com Web: