

WHITE PAPER



Mobile Device Security

Securing the Handheld, Securing the Enterprise





Managing the Mobile Enterprise
2009

Good Technology
Phone: 866-7-BE-GOOD
Online: www.good.com

CONTENTS

- 1** Introduction
- 2** Mobile Devices: A Productivity Boon,
An Enterprise Risk
- 3** Major Security Risks
- 5** Securing the Handheld
- 10** Regulatory Requirements
- 11** Conclusion



Introduction

Professionals are increasingly realizing the productivity benefits of high-bandwidth cellular networks and a growing proliferation of sophisticated mobile devices that deliver increased computing power and improved features and capabilities. While this mobile revolution is an advantage to professionals, it is creating a tremendous security management challenge for CIOs and other IT professionals. Proprietary and confidential data is now moving outside of the secure perimeter of the enterprise and onto mobile devices that can be located anywhere in the world. What's more, these devices have a variety of data communication and storage technologies, such as email/PIM synchronization software, infrared data transmission, Bluetooth® and removable data storage. As a result, it is easy for mobile devices to become strongholds of enterprise information.

Unless actions are taken to secure this information, the mobile device represents a potentially severe security risk to the enterprise.

This white paper identifies security threats to corporate data on mobile devices and details how mobile devices can become a "backdoor" to the enterprise. This paper also details how immediate action can be taken to defend against these threats and which issues an IT security manager should be aware of while planning a comprehensive handheld security policy. While server-side and transport security is vital to an overall mobile data security plan, this white paper will focus on security as it relates to the mobile device.

Issues addressed include:

- How much of a security threat is the mobile device to my organization?
- What threats do these devices bring to the enterprise?
- What security policies should be deployed to provide adequate protection?
- Should I have any regulatory or compliance concerns?



Mobile Devices: A Productivity Boon, An Enterprise Risk

Small, powerful and connected to essential enterprise information, mobile devices have been embraced by professionals and are fast becoming a standard enterprise productivity tool. It is precisely this small size and enterprise connectivity, however, that make the mobile device a potential risk to the enterprise. While they may contain vital data similar to a desktop or laptop, mobile devices are far more vulnerable to loss, theft or malicious use.

MOBILE WORKERS—RAPIDLY INCREASING

The analyst firm IDC estimated that in 2006 there were 758.6 million mobile workers worldwide. By 2011, there will be 1 billion—a number representing a compound annual growth rate of over 5.8 percent¹. In addition, mobile data usage will continue to grow at a rapid pace, driven by the desire to access both professional and personal applications. As mobile data usage grows, so will the number of mobile professionals who will use their devices to store data.

The greatest number of mobile device users tend to be executives, managers, sales professionals and service professionals—the people who are most likely to work with sensitive, proprietary information. According to Frost & Sullivan, executives, directors and mid-level managers make up 57 percent of enterprise professionals using mobile devices; field service employees conducting installation, service and repair comprise 17 percent; mobile sales employees 16 percent; and vehicle operators make up the remaining 10 percent.²

INCREASING MOBILE ACCESS TO ENTERPRISE INFORMATION: EMAIL AND BEYOND

Access to email has been one of the major drivers of mobile device use. Today, email is still the “killer application,” accounting for the majority of mobile initiatives in organizations. Numbers indicate that there are over 100 million wireless email users worldwide, of which about 30 million are business users. It is expected that these numbers will triple by year-end 2010³. Access to other enterprise data, such as sales force automation, inventory or pricing information is also increasing, as information from backend applications is made available on mobile devices. Analyst firm Gartner predicts that the number of mobile applications deployed by enterprises to their employees will continue to grow by 30% through 2011⁴.

REQUIREMENT: ENTERPRISE DEVICE SECURITY MANAGEMENT

With great power, however, comes great risk. A recent study indicates that 30 percent of mobile devices are lost every year.⁵ Stories about stolen or hacked devices containing sensitive corporate data continue to proliferate. It's estimated that each year, potentially millions of mobile devices go missing through loss or theft, or are upgraded, exchanged or sold without first having data removed.

In a Gartner survey of 1,400 CIOs around the world, CIOs in the US and EU rated mobile workforce issues as a “top five” priority and nearly two-thirds of all CIOs expected mobile workforce spending to grow faster than overall IT budgets. Their highest ranked concern regarding wireless adoption: security.

Good Technology
Phone: 866-7-BE-GOOD
Online: www.good.com

¹IDC, Worldwide Mobile Worker Population 2007 - 2011 Forecast, Dec 2007

²Frost & Sullivan, Mobile Office Report, 2004

³Gartner, Key Issues for Mobile Applications 2009, March 2009

⁴Gartner, Gartner's View of Enterprise Mobility, July 2007

⁵SANS Institute



Major Security Risks

Mobile device risks can be summed up in two general categories: devices that are lost, stolen or held by former employees and devices currently in use and connected to the enterprise.

LOST, STOLEN AND EX-EMPLOYEE MOBILE DEVICES

If a device with confidential data is lost or stolen, the corporation is at risk from the loss or misuse of information stored on the device or its removable storage card. Often, basic security mechanisms such as a password requirement on power-up or data encryption are not utilized. As a result, the corporate data on lost or stolen devices, such as the 250,000 mobile devices that are left in U.S. airports every year, is exposed to potentially unauthorized viewing.

If a mobile professional misplaces a device in an airport or taxi, critically important data could be at risk, such as user IDs and passwords to corporate applications and servers. According to a security survey commissioned by RSA, 22 percent of users keep a list of passwords on their devices.⁶ In addition to passwords, device-stored information could also include:

- Human resource records
- Compensation information
- Business reorganization plans
- Merger and acquisition details
- Sensitive emails
- Business proposals
- Financial records
- Sales reports
- Customer information
- Product release information
- Medical reports

This information could be viewed by or sent to a wide variety of unintended recipients, such as a competitor, a business associate, a journalist or an identity thief.

When professionals leave a company, they could depart with a significant amount of confidential information on their mobile devices and removable storage cards.

Disgruntled ex-employees pose a particular risk. While reorganizations or layoffs are not everyday occurrences, enterprises could protect themselves from retaliatory activities if IT could wirelessly erase the data on multiple devices instantly or at a time of their choosing.

Good Technology
Phone: 866-7-BE-GOOD
Online: www.good.com

⁶RSA, RSA Security Password Management Survey, September 2005



UNPROTECTED DEVICES: A BACK DOOR TO THE ENTERPRISE

Even enterprise-connected devices can represent a risk to the enterprise. This can happen either when an unauthorized device is used by an authorized user, or when an improperly secured device is subject to attack.

In the first case, even corporations that spend millions protecting traditional networks and data are vulnerable to mobile professionals who are using individually purchased wireless devices for business use.

Even if the IT department doesn't know of the device's existence, the device could be capable of connecting to the network using a proper user ID and password to gain access. When the wireless device connects back to a laptop, server or to an application, the enterprise sees a trusted user and a trusted device. It is at this point that the corporation is vulnerable.

Malicious code, such as software viruses, also poses a threat to both the device and the enterprise. Malicious code accesses a device when an infected email attachment is received wirelessly or when data is transferred through the Infrared Data Association® (IrDA) port ("beaming") or over a Wi-Fi connection in a hotspot. Types of malicious code include:

- **Viruses**—A type of software program that can replicate itself and spreads by inserting copies of itself into executable code or documents. Usually propagated through a user-initiated action such as opening an attachment or running a script, viruses attempt to spread undetected through the device by attaching themselves to other files.
- **Trojan horses**—A malicious program that resembles a legitimate program. Trojan horses perform an unauthorized, harmful activity once access is gained to a user's device.
- **Worms**—A self-replicating computer program that attaches itself to another executable program; unlike a virus, a worm does not need to be part of another program to replicate itself. A worm can be designed to delete files or send documents.

Mobile device hackers target devices in order to launch larger attacks on corporate networks, with the intent of accessing business-critical information or hampering business activities. An example of such an enterprise attack is a "man-in-the-middle" attack.

In a successful man-in-the-middle attack, an attacker is able to read, insert and modify messages between two parties without either party knowing that the link between them has been compromised. Such an attack can enable other attacks when a user's authentication credentials are captured. For example, when the compromised device attempts to connect to the network, the attacker can steal the re-association requests, which contain each client's Media Access Control (MAC) address and service set identifier (SSID). With those two pieces of data, an attacker can impersonate a legitimate device on that wireless network.

Good Technology

Phone: 866-7-BE-GOOD

Online: www.good.com



SECURING THE HANDHELD

Enterprises are quickly responding to mobile security risks. Analyst firm Gartner estimates that mobile device security software spending grew from \$287 million in 2005 to over \$1 billion in 2008¹. With gigabytes of data stored on mobile devices and ActiveSync®/HotSync®, Wi-Fi, IrDA and Bluetooth communication capabilities, enterprise-wide mobile security policies and compliance are fundamental for data protection.

SECURITY POLICY RECOMMENDATIONS

To meet the mobile device security needs of the enterprise, the following security standards and capabilities are highly recommended.

USER AUTHENTICATION—BASIC

Key to any mobile device security policy is the ability to limit mobile device access to authorized users. Password protection is a basic authentication requirement and should be activated whenever the device is switched off. This most basic authentication step can typically be done by users for their own devices but, surprisingly, is often overlooked.

USER AUTHENTICATION—ADVANCED

The central establishment and enforcement of password policies provides the greatest authentication security to the enterprise. When controlling password policies from a centralized console with wireless capability, administrators can quickly and easily control policies for a broad array of users, without ever having to handle the end user's device.

Ideally, policies could establish and enforce a variety of password parameters, including minimum length and alphabetical/numeric characters. Additionally, policies should:

- Require a new password after a designated length of time.
- Require a password distinct from passwords recently chosen by the user.
- Require password entry after a designated amount of idle time or device shut-off.
- Establish a maximum limit of failed password attempts before the handheld clears all application data or requires unlock only by an IT administrator.

On the administrative side, a password reset policy needs to be implemented so that an administrator can easily and wirelessly reset the device for users who have lost their passwords.

Good Technology

Phone: 866-7-BE-GOOD

Online: www.good.com

¹Gartner, Magic Quadrant for Mobile Data Protection, Sept. 2008



DATA ERASE

Administrators should be able to set policies to wirelessly erase ("bitwipe") selected databases, applications or folders if excessive incorrect password attempts are made.

ENTERPRISE DEVICE AUTHENTICATION AND AUTHORIZATION

Enterprises must be able to control user access to enterprise networks, servers, applications and data. Corporate security policy should involve not only applications that have been pushed to and are running on mobile devices, but should also address all ad hoc requests for synchronization and data transfer.

User and device authentication requires a database of all of the authorized users, groups and devices with the appropriate IDs, passwords and certificates integrated into a security management system. The mobile device as well as the user must be able to prove that it is authorized to communicate on the network. It must not be possible for an attacker to impersonate a mobile device or a server, thereby misleading authentic services into communicating with it.

COMPLIANCE

Security policies are valueless if there is no mechanism to ensure user compliance. Effective compliance requires two measures. The first is requiring the installation of appropriate security policies or third-party software on every device prior to permitting use of the device. The second is the periodic assessment of devices to ensure that they continue to comply with requirements. To achieve these requirements quickly and effectively, wireless management and auditing is fundamental.

Without such a solution, end users would have to voluntarily inform IT that their mobile device contains confidential and proprietary corporate data. Such self reporting would be seen as onerous by mobile professionals, and few would likely comply. As a result, a significant vulnerability in enterprise security could easily emerge.



WIRELESS DEPLOYMENT AND UPDATING

Compliance with corporate security policies is rapidly assured when the security policy manager can deploy security policies automatically and wirelessly. Wireless capability is extremely important, because it ensures that security policies are deployed quickly and with little IT burden. Cradle deployment, in contrast, leaves a larger window of time when the device lacks security policies, removes the device from the user's hands and is burdensome to IT, especially when large numbers of devices are involved.

Wireless updating of security policies, device security software or required third-party applications is also important. In order to maintain the highest level of device security, enterprises require the quick updating of all devices whenever policies change or software is updated to provide greater protections. Given the rate of change of technology, wireless updating easily maintains security for a large, diverse and geographically spread population of devices. Also, a user's permission status can change as a user's role within the organization changes. Wireless updating helps IT continue to provide the level of security and permission appropriate to the user's changing role.

Ideally, wireless over-the-air capability is built into the device security solution. This ensures the appropriate and complete integration of functionality.

WIRELESS THREAT RESPONSE

Armed with an automated inventory of all mobile professionals and their authorized devices, IT and security administrators can provide instantaneous response to security breaches or threats. Such a response could include:

- Changing the security policy files
- Locking the device
- Data erase of selective files, applications and databases
- Data erase of the entire device

DATA RECOVERY

Backup and recovery planning should include backing up confidential data stored on mobile devices to an enterprise server, since regulatory agencies require documents and correspondence to be provided upon request in the event of an investigation.



INTEGRATION WITH PUSH EMAIL/PIM

It is important that a device security solution be integrated with push email/PIM vendor products. If there is no integration, a device could be locked with its data encrypted, preventing synchronization from taking place. This effectively strips away the many advantages of the “always on, always connected” productivity goal of push email/PIM applications.

Most device and server security solutions have been developed independently of mobile applications, such as wireless push email/PIM and therefore do not interoperate effectively. As a result, the user is forced to participate in an authentication process such as entering his or her username and password for every transaction pushed to the device from the server. This authentication process reduces efficiency and usability and, in many cases, is a step avoided by the end user. When the user refuses to authenticate, the device does not allow access and the value of the device erodes.

Devices can avoid authentication and still receive email when the security solution and email/PIM solution are working together in the background to resolve this conflict. Always-on PIM will be available even while the device is password-locked.

DIRECTORY SERVICES INTEGRATION

LDAP and Active Directory integration with the mobile security solution ensures that your security policies appropriately match the needs and profiles of the user community over time. The IT administrator's work is streamlined when it is not necessary to reenter and maintain user files in a separate security application. Inheriting user-group information from either LDAP or Active Directory is a significant advantage, since security policy files created for groups can be deployed quickly and easily or updated in one simple process.

ENCRYPTION OPTIONS

Data can be stored both in the device's Random Access Memory (RAM) and in external storage cards, such as Secure Digital/Multimedia Cards (SD/MMC), CF cards and PC storage cards. Since these storage cards can save gigabytes of data, most security groups want the ability to secure them with data encryption.

Even when issued by the corporation and used primarily for work, devices often store both business and personal information. For this reason, most corporations want to provide the option to encrypt personal files. It is critical that a security solution be capable of encrypting all of the device data or only select applications, databases and files.

When inserting a protected memory card into the device's expansion slot, the security product should be able to detect a protected card and prompt the user for the card's password. The user would then have access to information only if they enter the correct password.

Good Technology

Phone: 866-7-BE-GOOD

Online: www.good.com



Encryption algorithms should be Federal Information Processing Standard (FIPS) certified and designed to provide data encryption in a transparent method. Transparency ensures that the user is impacted as little as possible while providing the maximum data protection.

SELECTIVE APPLICATION LAUNCH CONTROL

In some enterprises or government agencies, it is important to restrict which applications a device is permitted to run. This need is especially great when the organization has purchased and configured all of the devices or when there is a specific field application that an organization requires.

DEVICE FEATURE DISABLEMENT

In order to limit security risks, IT administrators want the ability to control a wide variety of mobile device features. For example, to prevent hackers from penetrating a mobile device using a man-in-the-middle attack, an organization may want to disable Wi-Fi capability. Typically, IT administrators would want control over the following device capability categories:

- Data transfer—HotSync, ActiveSync, IrDA or Bluetooth. Alternatively, when the device is locked, data synchronization mechanisms such as HotSync and IrDA could be disabled automatically.
- Data storage—SD cards.
- Multimedia—Cameras, microphones and speakers.



Regulatory Requirements

Three major industries are early drivers of mobile device security: healthcare, financial services and government. Each of these industries is required by law to safeguard and maintain patient, consumer and/or financial and operational information. Recent regulations such as the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley (GLB) and Sarbanes-Oxley (SOX) act have mandated strict security and permissions control of sensitive information and have established serious penalties against violations.

While the healthcare industry has been a technology laggard in the past, it has been a leader in the adoption of mobile device security. Similarly, the GLB Act has driven banks, insurance companies, brokerage houses and other financial institutions to deploy mobile device security along with wireless applications. Audit trails, device access management and data encryption will play key roles in security best-practice management for these organizations.

Good Technology
Phone: 866-7-BE-GOOD
Online: www.good.com

HEALTHCARE	FINANCIAL	CONSUMER PRIVACY	
<p>HIPAA (US)</p> <p>Health Insurance Portability and Accountability Act</p> <p>Mandates the protection of patient records containing individually identifiable health information</p>	<p>SOX (US)</p> <p>Sarbanes-Oxley Public Company Accounting Reform and Investor Protection Act</p> <p>Mandates reforms regarding corporate financial responsibility; sets higher requirements on the control of confidential corporate financial information</p>	<p>95/46/EC (EU)</p> <p>European Union Directive 95/46/EC</p> <p>Protects individuals with regard to the processing of personal data and the free movement of such data</p>	<p>DPA (UK)</p> <p>Data Protection Act</p> <p>Ensures that personal data processing is carried out with appropriate security for the rights of data subjects; requires consent prior to disclosure of personal data to a third party</p>
	<p>GLBA (US)</p> <p>Gramm-Leach-Bliley Act</p> <p>Protects personal financial information held by financial institutions</p>	<p>SB 1386 (US)</p> <p>California Senate Bill 1386</p> <p>Requires any organization that conducts business in California and owns or licenses computerized personal information to disclose any security breach to any resident whose personal information was or is believed to have been disclosed</p>	<p>PIPEDA (Canada)</p> <p>Personal Information Protection and Electronic Documents Act</p> <p>Establishes privacy principles, such as providing adequate security for the protection of personal information collected, used or disclosed in the course of commercial activities</p>



Conclusion

Mobile devices represent a tremendous productivity advantage for today's mobile worker. The small size, large storage capacity and network connectivity of these devices, however, make unprotected mobile devices susceptible to loss, theft and misuse. As a result, unsecured devices can pose a risk to the entire enterprise. Before mobile device use becomes ubiquitous, intelligent organizations are developing comprehensive security plans to protect both the enterprise and the device.

In order to adequately secure the device from misuse or attack and to meet regulatory requirements, IT organizations must give consideration to the wireless and centralized deployment of device security policies. These policies include measures regarding authentication, data erase, encryption, application launch controls and device feature disablement. Further, compliance management is required to ensure that devices stay within enterprise security requirements over time.

When mobile device security solutions are fully integrated with email/PIM solutions; are centrally managed; and are capable of wireless deployment, updating and compliance, they can provide the level of security that enterprises require.

Good Technology
Phone: 866-7-BE-GOOD
Online: www.good.com

©2009 VISTO Corporation and Good Technology, Inc. All rights reserved. Good, Good Technology, the Good logo, Good for Enterprise, Good for Government, Good for You, Good Mobile Messaging, Good Mobile Intranet, and Powered by Good are trademarks of Good Technology, Inc. ConstantSync, Constant Synchronization, Good Mobile Client, Good Mobile Portal, Good Mobile Exchange Access, Good Mobile Platform, Good Easy Setup, Good Social Networking and Good SmartIcon are either trademarks or registered trademarks of VISTO Corporation. All third-party trademarks, trade names, or service marks are the property of their respective owners and are used only to refer to the goods or services identified by those third-party marks. Good and VISTO technology is protected by U.S. Patents 6,085,192; 5,968,131; 6,023,708; 5,961,590; 6,131,116; 6,151,606; 6,233,341; 6,131,096, 6,708,221 and 6,766,454 and the following NTP U.S. Patents: 5,436,960, 5,438,611, 5,479,472, 5,625,670, 5,631,946, 5,819,172, 6,067,451, 6,317,592 and various other foreign patents. Other patents pending.