IBM Global Technology Services
Thought Leadership White Paper

October 2011

Securing mobile devices in the business environment

By I-Lung Kao, Global Strategist, IBM Security Services

As the world becomes more interconnected, integrated and intelligent, mobile devices are playing an ever-increasing role in changing the way people live, work and communicate. But it is not just happening in personal life: Smartphones and tablets are also being rapidly adopted by enterprises as new work tools, joining existing laptops and desktops. The use of mobile devices for business has experienced an explosive growth in the past few years and will only accelerate in the near future.

And while the BlackBerry® has been the de facto mobile device for business for many years, the availability of other smartphones and tablets with broader consumer appeal, such as iPhone® and Android™ devices, is fundamentally changing the game. Employees are now bringing their own mobile devices to the workplace and asking companies to support them. These new devices offer improved hardware performance, a more robust platform feature set and increased communication bandwidth, expanding their capabilities beyond voice and email. As a result, however, this increased access to enterprise systems can also bring an increased security risk to the organization.

This paper explores how companies can more safely introduce employee- or corporate-owned mobile devices into the workplace, identify the risks inherent in their broader access to corporate data, and derive enhanced business value.

Mobility brings both advantages and risks to the enterprise

As employees bring mobile devices into the workplace, many organizations are motivated to encourage their use for business purposes, because they tend to drive:

- **Increased employee productivity**—Mobile devices can give employees access to corporate resources and enable continuous collaboration with colleagues or business partners.
- **Improved client services**—Sales or support employees who regularly interface with customers may respond more efficiently, directly increasing customer satisfaction.
- **Reduced IT cost**—By allowing employees to use, and often pay for, their own mobile devices and wireless services, companies potentially save IT spending on device purchases as well as management and communication services.

There are some cautions, however. Companies need to fully recognize that when employees connect mobile devices to the enterprise and merge both business and personal data, those mobile devices must be treated just like any other IT equipment, with appropriate security controls. If security is not addressed at the outset, these mobile devices may become a point of security weakness that threatens to disclose business information or become a new channel to introduce security threats to the company's IT infrastructure and business resources. Many IT departments are finding significant challenges in securing mobile devices, for a variety of reasons:

- A range of mobile device platforms, such as BlackBerry, Symbian®, IOS®, Android and Windows Mobile, needs to be supported, and each platform brings with it a unique security model. Other than the BlackBerry platform, most started as consumer platforms and lack enterprise-strength security controls.
- Business and personal data now coexist on the same device. Finding a balance between strict security control and privacy of personal data, particularly when the device is no longer a corporate-issued asset, can be challenging.
- Unauthorized or non-business oriented applications have the potential to spread malware that affects the integrity of the device and the business data residing upon it.
- Mobile devices are prone to loss and theft, due to their small-size and high-portability. Whenever a device is lost, corporate data is at risk both on the mobile device and within the corporate network.

- Many mobile devices are always on and connected, so vulnerability to malicious attacks increases through different communication channels.
- Mobile technology is advancing quickly and becoming increasingly complex. Many companies do not have enough resources or skills in house to fully embrace mobile technology in the workplace.

Security threats to mobile devices

The security of mobile devices has become a top concern for many IT executives. Hackers are discovering the benefits of compromising both business and personal data contained within mobile devices. Because many mobile platforms are not natively designed to provide comprehensive security, hackers have a strong incentive to develop new techniques or create mobile-centric malware specifically for these devices. In a recent IBM X-Force® security research report, mobile operating system vulnerabilities have increased significantly (see Figure 1) and exploits of vulnerabilities are also on the rise (see Figure 2).[1]

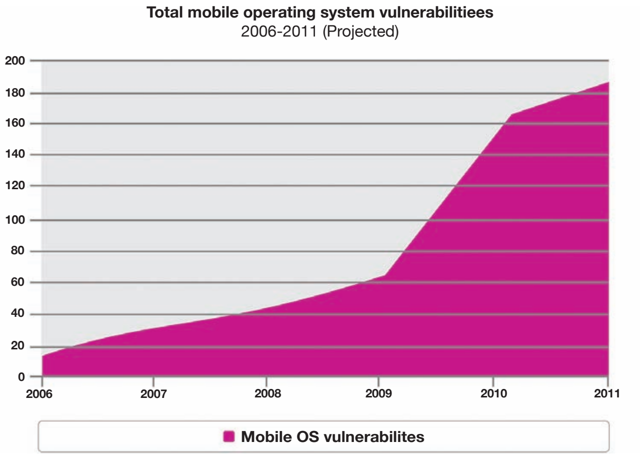

Figure 1: Total mobile operating system vulnerabilities.

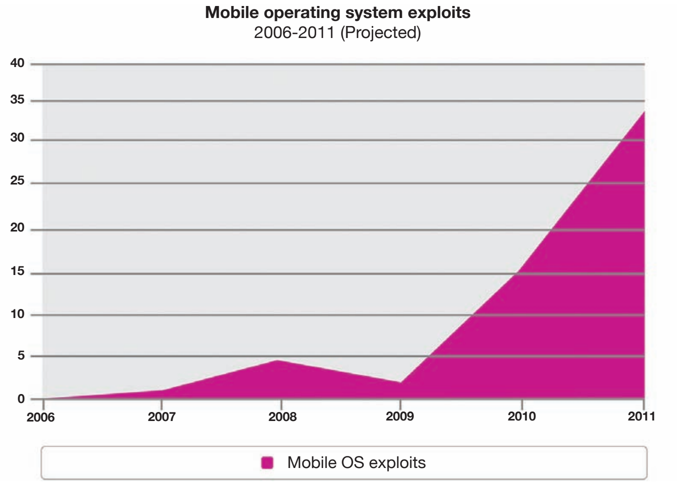

Figure 2: Mobile operating system exploits.

The latest smartphones are designed to provide broad Internet and network connectivity through varying channels, such as 3G or 4G, Wi-Fi, Bluetooth or a wired connection to a PC. Security threats may occur in different places along these varying paths where data can be transmitted (see Figure 3). When a device downloads a new mobile application from any online application store, the software may contain malware that can steal or damage data on the device and, in some cases, even disable the mobile device itself. Most mobile devices now have Internet connections, so common web-based threats that have attacked laptops or desktops may also apply to mobile devices. A device connected through Wi-Fi or Bluetooth is at greater risk because the Wi-Fi source or the other Bluetooth-enabled device may have been compromised and can play a role in a "man-in-the-middle" attack (when a hacker configures a laptop, server or mobile device to listen in on or modify legitimate communications) or other attack type.

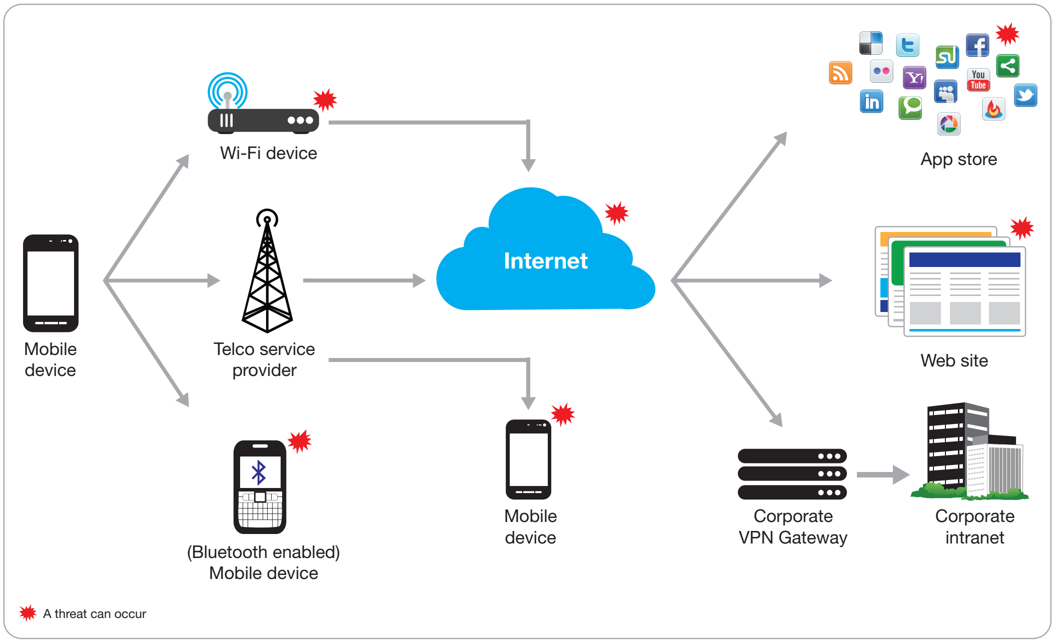

Figure 3: Flow of data transmission.

Because of the variety of communication mechanisms available and increasing use of business applications on mobile devices, the security threats to mobile devices have evolved to all the threats applicable to desktops or laptops, plus new threats that are truly unique to mobile devices. Therefore, mobile devices need to be protected with an even broader set of security techniques than those employed for traditional desktop or laptop operating environments.

No matter what the threats are, the targets that hackers try to access and exploit typically consist of one or several of the following:

- Credentials to access business or personal accounts
- Confidential business or personal information
- Phone or data communication services
- The mobile device itself

The most frequently seen mobile device security threats are:

- Loss and theft
- Malware
- Spam
- Phishing
- Bluetooth and Wi-Fi

Loss and theft

Small size and high portability make loss and theft top security concerns when a mobile device is used in the workplace. According to a mobile threat study by Juniper Networks, 1 in 20 mobile devices was stolen or lost in 2010.[2] When devices are lost or stolen, all of the data stored on or accessible from the mobile device may be compromised if access to the device or the data is not effectively controlled.

While not foolproof, some techniques can help reduce the risk of data compromise, such as using a complex password to access the device or critical data, remotely locating the device on a map using global positioning services (GPS), remotely locking the device to render it useless, or remotely wiping data on the device. Some mobile platforms natively provide these techniques, and in the event they do not, basic platform capabilities can often be augmented by functionality available in third party mobile device management or mobile security solutions.

Malware

Mobile device malware—viruses, worms, Trojans, spyware—has been on the rise over the past few years because most mobile platforms do not yet have native mechanisms to detect malware. Virtually no mobile platform available today is immune to malware. Although more established mobile platforms such as Symbian and Windows Mobile have been a proving ground for malware developers in the past few years, the Google Android platform is leading in new malware development, primarily due to its popularity and open software distribution model. The mobile threat research report from Juniper Networks also states that malware on Android grew 400 percent from June 2010 to January 2011.[3]

Malware can cause a loss of personal or confidential data, additional service charges (for example, some malware can send premium Short Message Service (SMS) text messages or make phone calls in the background) and, even worse, make the device unusable. Although quickly removed, numerous malicious applications recently found their way onto the Android marketplace. Some of these were legitimate applications that had been repackaged with a Trojan designed to gain root access or additional privileges to users' devices. Unsuspecting users may have had malicious code or additional malware installed in that single download from the applications store. Malware can then spread quickly through a wired or wireless connection to another device or a company's intranet.

Companies can significantly reduce the malware risk by adopting a similar approach to be used for both mobile devices as well as the desktop and laptop environment. In addition to advising employees to only download and install trusted applications and take appropriate actions when suspicious applications are identified, a company should run antimalware software on each employee's device to detect malware in real-time and scan the entire device periodically.

Spam

With the growth of text messaging, spam—unsolicited communication sent to a mobile device from a known or unknown phone number—is also on the rise. Spam is not only a big concern for mobile service providers because it wastes a significant amount of bandwidth, but it is also a growing security issue for mobile device users. According to the recent Global System for Mobile Communications Association (GSMA) pilot of the GSMA Spam Reporting Service (SRS), the majority of spam attacks are for financial gain, with 70 percent of reports of spam being for fraudulent financial services rather than the traditional advertising scenarios found in email spam.[4]

We feel that the most effective method to thwart spam is to define a blacklist to block spam messages either by using the functions of an antispam solution or by turning on the antispam feature on the device if it is available.

Phishing

"Phishing" is an email or an SMS text message (dubbed, "SMiShing") sent to trick a user into accessing a fake website, sending a text message or making a phone call to reveal personal information (such as a Social Security number in the United States) or credentials that would allow the hacker access to financial or business accounts. Phishing through mobile browsers is more likely to succeed because the small screen size of mobile devices does not allow for some protection features used on the PC, like web address bars or green warning lights.

The most effective antiphishing approach helps a user recognize a fraudulent website when it is presented. Some financial institutions have deployed "site authentication" to confirm to users that they are communicating with a genuine website before they enter account credentials from either a web browser or a mobile application. Two-factor authentication is also useful to thwart phishing: First, a user enters a static password, then a second authentication factor, such as a one-time password or a device fingerprint, is dynamically generated to further authenticate the user. So even if a user's static password is stolen by a hacker using a phishing technique, the hacker cannot login to the genuine site without the user's second authentication factor.

Bluetooth and Wi-Fi

Bluetooth and Wi-Fi effectively increase the connectivity of mobile devices within a certain range, but they can be easily exploited to infect a mobile device with malware or compromise transmitted data. A mobile device may be lured to accept a Bluetooth connection request from a malicious device. In a "man-in-the-middle" attack, when mobile devices connect, the hacker can intercept and compromise all data sent to or from the connected devices.

Setting the device's Bluetooth to an undiscoverable mode and turning off the device's automatic Wi-Fi connection capability, especially in public areas, can help reduce risks. To completely block incoming connection requests from unknown devices, a local firewall should be installed and run on the mobile device—another traditional security practice that can be extended to the mobile environment.

Establishing a mobile security strategy

Creating a stringent strategy that defines guidelines and policies helps lay the foundation for a more security-rich mobile environment. This strategy should focus on several key areas: Data and resources accessible from mobile devices, platform support, management methodology and best practices.

Initially, your organization should identify which business data it will allow to be stored and processed on which mobile devices. This helps determine what needs to be protected and to what degree. Many enterprises only permit employee email, contact and calendar information. Others allow access, through a browser or native mobile application, to other business-critical applications such as enterprise resource systems (ERP) or customer relationship management (CRM). Different degrees of access from mobile devices require varying levels of security controls. However, it should be noted when business data flows from a more strictly controlled location (for example, a database or a file server) to a less protected device, the risk of losing the data becomes greater.

You may also need to determine which mobile device platforms will be allowed in the business environment and, thus, need to be supported in the mobile security strategy and plan. Different mobile platforms have different native security mechanisms that need to be outlined and understood, although applying a set of security controls to all supported platforms in a consistent manner is desirable.

Another important decision is the responsibility for mobile security management work, whether using the current IT security team to handle mobile devices, or outsourcing to a managed security service provider. Multiple security technologies may need to be employed to provide comprehensive security controls for mobile devices. As such, depending on how these security solutions are delivered (on-premise or from the cloud), a company may choose to use a hybrid model for device security management.

No matter what the mobile environment, a number of mobile security policies and best-practice procedures need to be put in place and should also be identified in the company's mobile security strategic plan. Fortunately, many best practices that have been exercised for desktops and laptops can be duplicated for mobile devices, such as:

- Specification of roles and responsibilities in managing and securing the devices
- Registration and inventory of mobile devices
- Efficient installation and configuration of security applications on devices
- Automatic update of security patches, polices and settings
- Reporting of security policy enforcement status
- Employee education on securing mobile devices

Applying security controls based on a framework

Taking a broad look across the IT and business environment, IBM has developed a well-defined framework that specifies security domains and levels for applying various security technologies.

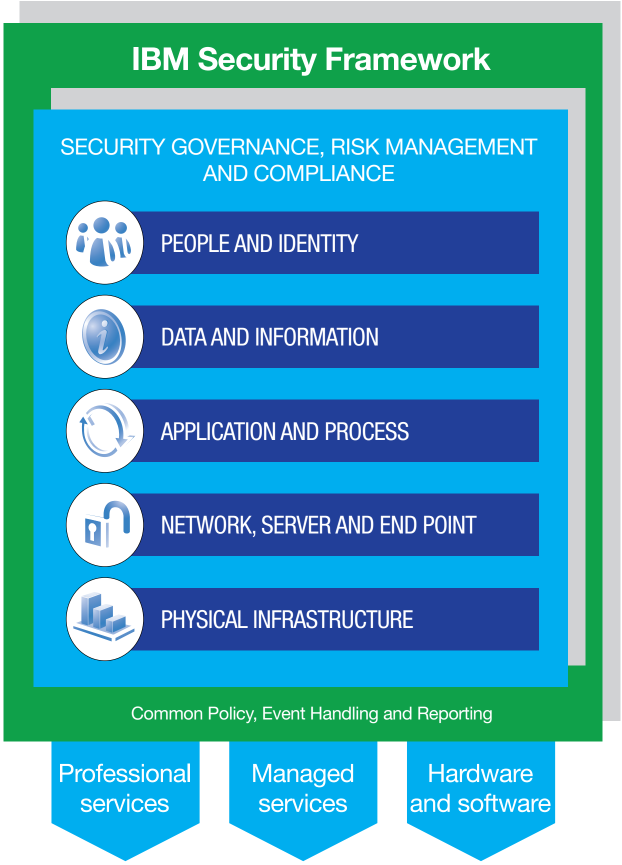

Figure 4: IBM Security Framework.

When applied to mobile devices, the framework suggests the following security controls, with actual requirements varying by deployment:

- Identity and access
- Data protection
- Application security
- Fundamental integrity control
- Governance and compliance

Identity and access

- Enforce strong passwords to access the device
- Use site authentication or two-factor user authentication to help increase the trustworthiness between a user and a website
- If virtual private network (VPN) access to corporate intranet is allowed, include capability to control what IP addresses can be accessed and when re-authentication is required for accessing critical resources

Data protection

- Encrypt business data stored on the device and during transmission
- Include capability to wipe data locally and remotely
- Set timeout to lock the device when it is not used
- Periodically back up data on the device so data restore is possible after the lost device has been recovered
- Include capability to locate or lockout the device remotely

Application security

- Download business applications from controlled locations
- Run certified business applications only
- Monitor installed applications and remove those identified to be untrustworthy or malicious

Fundamental integrity control

- Run antimalware software to detect malware on storage and in memory
- Run a personal firewall to filter inbound and outbound traffic
- Integrate with the company's VPN gateway so a device's security posture becomes a dependency for intranet access

Governance and compliance

- Incorporate mobile security into the company's overall risk management program
- Maintain logs of interactions between mobile devices and the company's VPN gateway and data transmission to and from servers within the intranet
- Include mobile devices in the company's periodic security audit

Choosing the right solution

When choosing a mobile security solution, several factors need to be taken into consideration:

- **Solution architecture**—The solution should be built on a sound client-server architecture in which the server centrally controls and manages security policies and settings for various security features. The client should be installed on the mobile device and regularly communicate with the server to enforce policies, execute commands and report status.
- **Platform support**—The solution should support a variety of mobile device platforms with a consistent, easy-to-manage administration console that is platform-agonistic to help reduce security policies across different devices.
- **Feature expandability**—Mobile device technology advances very rapidly and new mobile threats are evolving all the time. The solution must be flexible enough to accommodate future technology changes and incorporate more advanced capabilities to counter new threats.
- **Usability**—Features that are easy to use and require little user intervention can help drive acceptance by end users and increase the effectiveness of security control.
- **Reporting and analysis**—The solution needs to contain reporting and analysis capabilities, with information that helps the company to support policy and regulation compliance, recognize the mobile threat landscape and evaluate the solution's effectiveness in countering threats.
- **Deployment and management**—No matter how capable a security solution is, its value is greatly diminished if it cannot be efficiently deployed or easily managed. The company needs to carefully assess the overall efforts required for initial roll-out and ongoing management of a solution.

Another important decision in the solution choice is who will be responsible for the overall mobile security implementation effort and subsequent ongoing management. Although it is possible to have the current IT team responsible for desktop and laptop management and security also handle mobile devices, resource or skills constraints could prove challenging, particularly in a global, heterogeneous environment.

Outsourcing is another option. Leveraging the industry- wide mobile security expertise of a managed service provider can not only free up in-house IT resources, but also inject policies and procedures that can, down the road, build up internal skills without putting the enterprise at risk. In addition, an outside provider may have the ability to provide a range of delivery options, from on-premise to in the cloud, or even a hybrid solution that may better fit the enterprise's changing needs.

IBM hosted mobile device security solution provides security from the cloud

To help organizations embrace both company- and employee-owned mobile devices in a security-rich environment, IBM Security Services offers a robust mobile device security management solution. The solution, built on a client-server architecture, helps efficiently deliver mobile security services from the IBM Cloud to mobile devices on a variety of platforms.

These services can help companies address the major mobile security issues discussed in this paper with a single solution. By both leveraging existing mobile devices owned by branches and employees in different groups or geographies, and avoiding the purchase of additional hardware or software, companies can reduce capital and operational costs.

IBM Security Services provides a wide set of managed services, including:

- Requirement assessment and policy design
- Training and providing knowledge assets
- Guidance for production roll-out
- Monitoring, alerting and reporting
- Policy maintenance and calibration
- Threat intelligence sharing

The solution combines industry-leading mobile security technologies with IBM's deeper security knowledge and highly skilled technical professionals around the world to help reduce risks and better manage regulatory compliance. With IBM Security Services, companies can benefit from improved operational, financial and strategic efficiencies across the enterprise, and, most importantly, can enhance their overall security postures to increase their business competitiveness.

For more information

To learn more about IBM Managed Security Services (Cloud Computing)—hosted mobile device security management, contact your IBM marketing representative, IBM Business Partner, or visit the following website: **ibm.com**/services

Notes

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
October 2011
All Rights Reserved

[1] IBM X-Force 2011 Mid-year Trend and Risk Report, September 2011

[2] Juniper Networks Malicious Mobile Threats Report 2010/2011, May 2011

[3] Juniper Networks Malicious Mobile Threats Report 2010/2011, May 2011

[4] GSMA Outlines Findings from Spam Reporting Service Pilot press release, February 10, 2011