

## Talking Points

# The Smartphone & its risks

## How to avoid paying dearly for convenience

By Will Andrews, RSM McGladrey, USA

**Having a few key safeguards in place can reduce the risk of smartphones becoming a matter of national security.**

While smartphones often create a wave of security anxiety, the convenience they offer can't be ignored. In today's business environment, senior executives expect—maybe even demand—the ability to receive e-mail and have network access on their iPhone, Blackberry or Motorola smartphone. This makes managing smartphone risk a top priority for information technology departments everywhere.

According to a Gartner press release<sup>1</sup>, the strong growth in worldwide sales of smartphones continued in the last quarter 2009, with a 41.1% increase on the same period in 2008. Overall, 2009 smartphone sales increased 23.8% from 2008, and yearly increases in sales are certain to continue for many years to come.

These smart devices devour premium-priced multimedia services. Their network service providers are liberally doling out incentives to lower the price of smartphones in an effort to put them into as many eager, multi-year-contract signing hands as possible.

Smartphones are here to stay. Denying that fact may inadvertently cause security holes to be opened by end-users who may take it into their own hands to get the connectivity they want out of their smartphones.

Management directives, such as implementing smartphones or any other technology, must be examined objectively for risk and then the vulnerabilities must be controlled to minimize the threat to security.

### The management viewpoint

Laptops became the zenith of portable computing in the '90s because they brought mobility, connectivity and productivity to management. The need for access to e-mail and other business applications outside the boundaries of the office drove laptop acceptance into the office workstation-based business world.

Fast forward a decade and management is still attracted to mobility, connectivity and productivity. However, while laptops are currently focused on having more powerful computing performance, 17-inch widescreen experiences or 9-inch compact form factors, smartphones are focused on reducing the need to carry around a number of different

devices, such as a laptop cell phone, personal digital assistant (PDA), MP3 music player and a GPS unit – not to mention each of their associated AC adapter cords. Even though the computing power of a smartphone is no match to a business class laptop, the convenience and capabilities almost always outweigh the horsepower to the end-user. Analysts' reports support that users are trending their preferences toward smartphones over laptop computers.

### The information technology viewpoint

To understand what information technology departments fear when it comes to connecting these little devices to the network, we need to know what the phones can do. Smartphones are tiny marvels of technology. They aggregate many different types of electronic devices into a single, small and convenient unit.

Smartphones are, in fact, miniaturized business computers. Some smartphones run a mobile-phone version of the same Windows OS that runs on PCs, while others may run Blackberry OS, Palm OS or other similar operating systems. The devices may come with Microsoft Office applications such as Word, Excel, PowerPoint and that killer app—Outlook e-mail.

<sup>1</sup> Gartner Press Release: Gartner Says Worldwide Mobile Phone Sales to End Users Grew 8 Per Cent in Fourth Quarter 2009; Market Remained Flat in 2009, February 23, 2010

Let's not forget that these micro-sized computing devices may also have VPN clients to access the company's internal network. They have web browsers to surf the Internet. They have all of the capabilities of a PDA—complete with contact management, to do lists, and appointment schedulers. Also, packed into these miniature packages are television network services to the major broadcasters as well as built-in video and still cameras to be your own broadcaster. They are also equipped with MP3 music and video movie players to keep up with the latest entertainment studio releases. They have special applications for social networking sites like Facebook and MySpace.

Many devices have WiFi to take advantage of the airport and coffeehouse wireless hotspots. They may also sport Mini USB ports for connecting back to that old, bloated boat-anchor of a laptop. Micro or MiniSD memory slots are available to extend the device's storage capabilities by gigabytes when needed. The latest achievements are video teleconferencing and voice-enabled GPS to effortlessly find your way back to work from the cellular phone store after you buy your new mobile device.

Oh, and by the way, they also make phone calls.

Having all of that in the palm of your hand is enough to overload the salivary glands of any business executive and send any techie into a state of geek-nirvana. In terms of risk to security, smartphones are more than enough to send your information technology manager reaching for the industrial-sized jug of heartburn medicine.

#### A thousand points of light

The information technology organization is dedicated to limiting Internet access in or out of the company's internal network through one single point of access – the firewall. Smartphones potentially open numerous new points of entry to the network. There are several key scenarios to consider to limit risk:

1. The smartphone gets lost or stolen and subsequently there is unauthorized access to the smartphone, unauthorized access to data and unauthorized calls

2. Unauthorized access to the network
3. Administrative control to computer systems are lost
4. Sensitive data is accessed
5. Inappropriate use of the Internet

#### Managing risk

The security risk to the organization is real. A poor implementation of smartphones in the company is likely to result in breaches in security. Managing the risks associated with smartphone technology relies on implementing the right balance of operational security, technology and common sense.

In some cases the phone choice may be pre-determined. If not, consider the following criteria before making a choice for the company:

1. The ease of integration between the email application and the smartphone (e.g., integration with Active Directory and ActiveSync)
2. End-user business requirements
3. Impact of securing an additional server on the network perimeter
4. Security features provided by the phone manufacturer
5. History of security flaws associated with the smartphone technology
6. Financial stability of the smartphone manufacturer as well as the cellular service provider
7. Cost of the implementation
8. Number of employees that will be using the service. If the implementation is in place to support only one or two persons, management must be aware of the cost and the ongoing maintenance resources before proceeding.

#### Locking down the device for implementation

The process for locking down smartphones is serendipitously similar to locking down their larger counterparts, business laptop computers. If laptop security is considered

a priority of the organization, smartphone security will be easier to implement. The keystone of the smartphone security model is avoiding loss or theft. For an unsecured phone, loss or theft of the device starts a domino effect of security issues potentially impacting members, the internal network and the company's reputation. Smartphone risk can be reduced by applying the existing security controls and policies already available for these devices. Fundamental security elements to reduce risk are detailed below.

#### Theft abatement:

**Remotely erase data** - To reduce the risk of sensitive data being accessible, enable "remote wipe" functionality to delete the contents of a smartphone that was lost or stolen.

**Password access:** Enable a password policy on the smartphone. Certain password parameters may be enabled such as password length. Alphanumeric characters may also be enabled but may be problematic on certain smartphones without access to a QWERTY keyboard. Minimum password length should meet or exceed the existing standards of the organization.

**Failed password attempts:** To reduce the risk of unauthorized access to data on the smartphone, configure the device to perform a data wipe after predefined number of failed logon attempts.

**Idle timeout:** Enable password protected screen lockout or screen saver mode when a specified duration of non-use is reached.

#### Centralized management and directory services:

**Windows Mobile OS** - For smartphones using the Windows Mobile OS, use Active Directory and Mobile Device Manager to push phone and policy settings to control the security of the device over the air.

**BlackBerry OS** - For BlackBerry smartphones, use BlackBerry Enterprise Server (BES) to push mail from Exchange, Lotus Notes, or GroupWise servers, install software and manage phone settings.

**VPN:**

**VPN clients** - Disallow VPN access unless for specific business purposes. If VPN is necessary, strictly granulate access by using a group policy.

**Portable memory:**

**Mini SD and micro SD Cards** - Many companies have policies in place controlling or prohibiting the use of portable memory devices such as memory sticks and SD memory cards. To limit sensitive data from being copied or stolen from the smartphone, apply organizational controls that meet or exceed established security policy.

**Encryption:**

**File encryption** - Some smartphone operating systems or management solutions already come equipped with the capability to encrypt files on the smartphone, however, there are also third-party encryption vendors providing smartphone solutions that protect the phone as well as its removable SD cards.

**WiFi and Bluetooth:**

**Wireless security** - To reduce the risk of opening a backdoor to the company network while connected to WiFi or Bluetooth and to the cellular network at the same time, enable security policies to disable the protocols when connected using the over the air network where practicable. Limiting Bluetooth may be problematic due to various hands-free driving laws or interoperability with peripherals. Also, because Bluetooth and WiFi drain power, turning the services off until needed conserves battery life.

**Hardware security:**

**Anti-virus and firewall security** - Third-party vendors offer integrated solutions for firewall, anti-virus and anti-spam. Be aware of the limited memory space available on the smartphone before loading too many applications.

**Email attachments, data files, applications, Movies, MP3s and games:**

**Downloads** - Build on the precedents set by the laptop and desktop security policies to address download controls for smartphones. Consider the facts that anti-virus and anti-spam applications may not be as robust as their laptop counterparts, that application development for smartphones isn't as mature, those applications are primarily free- and share-ware programs. As a result, hackers finding security flaws in the code of downloadable smartphone applications may be, as yet, undiscovered.

**Monitoring controls:**

**Monitoring mobile devices** - Implement end-user and system monitoring of mobile devices. Smartphone monitoring controls are a part of many OS-based, centralized management and Exchange services. However, third-party applications are also available to provide additional device monitoring and audit trails.

**Post Implementation Controls**

Smartphones are not only an extension of the network, they are now a component of the email system – which is arguably one of the most critical components in the network environment. Its security maintenance is essential to network security. Patch management and end-user training are vital, as well as ongoing controls to ensure that smartphone security is maintained.

**Patch Management**

Enroll in smartphone mailing lists, feeds and user groups to know when firmware and OS updates and security patches are available. User groups and forums will increase awareness of end-user issues and vulnerabilities. Push patches with the same diligence the organization uses for all other critical network devices.

**Ongoing Smartphone End-User Awareness Training**

Provide ongoing training and communications covering the following topics:

- Maintaining the physical security of the device to reduce the risk of theft or misuse of the smartphone and its SD memory cards
- The impact of sensitive or customer data on the device
- Timely firmware updates
- Antivirus and firewall applications
- Policies for acceptable Internet and email use
- Downloading applications
- Best practices for device passwords

Smartphone technology is now readily available, giving us the freedom to be mobile. But this convenience is not without risk. The good news is applying the right balance of security, training and common sense will control risk and allow these devices to be an effective tool for end-users. Now that is something to phone home about.

---

To learn more about RSM McGladrey's technology risk management services, please call +1 800 648 4030, email at [TRMS@rsmi.com](mailto:TRMS@rsmi.com) or visit us online at [www.rsmmcgladrey.com](http://www.rsmmcgladrey.com).

#### About the Author

Will Andrews is a director with the Technology Risk Management Services group. Will Andrews brings over 15 years and extensive career experience in web applications and information technology (IT) security infrastructure. Will is extensively involved in conducting penetration tests, as well as assessing network security related to Windows networks, Cisco networks, e-commerce systems and Web servers. Will can be contacted on +1 415 848 5360 or [will.andrews@rsmi.com](mailto:will.andrews@rsmi.com).

#### About RSM International

RSM International is a worldwide member organisation of independent accounting and consulting firms. RSM International is represented in 76 countries and brings together the talents of over 32,00 individuals worldwide. The organisation's total fee income of US\$3.8bn places it amongst the top six international accounting organisations worldwide. Member firms are driven by a common vision of providing high quality professional services, both in their domestic markets and in serving the international professional service needs of their client base. [www.rsmi.com](http://www.rsmi.com)

#### About RSM McGladrey

RSM McGladrey is a leading professional services firm providing accounting, tax and business consulting. RSM McGladrey operates in an alternative practice structure with McGladrey & Pullen LLP, a partner-owned CPA firm that delivers audit and attest services. Through separate and independent legal entities, they work together to serve clients' business needs. Together, the companies rank as the fifth largest U.S. provider of accounting, tax and business consulting services (source: Accounting Today), with 7,000 professionals and associates in nearly 90 offices. RSM McGladrey Inc. and McGladrey & Pullen LLP are member firms of RSM International, an affiliation of independent accounting and consulting firms. [www.rsmmcladrey.com](http://www.rsmmcladrey.com)

RSM International is the name given to a network of independently owned and managed accounting and consulting firms each of which practices in its own right. RSM International does not exist in any jurisdiction as a separate legal entity. The network is administered by RSM International Limited, a company registered in England and Wales (company number 4040598) whose registered office is at 11 Old Jewry, London EC2R 8DU. Intellectual property rights used by members of the network including the trademark RSM International are owned by RSM International Association, an association governed by articles 60 et seq of the Civil Code of Switzerland whose seat is in Zug. This article is a publication of RSM McGladrey, Inc. Copyright 2009. Reprinted by permission. All rights reserved.