ASA

Annie Searle & Associates LLC

**Research Note**

# Mobile Devices & Business Security Risks

By Emily Oxenford

Copyright © 2010, ASA Institute for Risk & Innovation

Applicable Sectors: cybersecurity, information technology

Abstract: With the increasing penetration of smartphones and other mobile devices into the workforce and workplace, there are a number of security risks that must be taken into consideration. Ultimately, a business must examine what risks in particular mobile devices pose, and how to most appropriately mitigate those risks.

Keywords: mobile devices, smartphones, security, cybersecurity

## Introduction

A rising area of discussion today is the topic of technological convergence particularly in mobile devices. All over the world we have seen a tendency towards multiple communications mediums or platforms becoming more alike – overlapping in both their capabilities and uses. Previously, a mobile phone was simply a phone on the move – it was just for making calls. A camera was a separate device just for taking pictures. Slowly things like text messaging, address books, and voicemail were added, and then cameras were added into mobiles. In parallel, the PDA developed – allowing individuals, especially business users, to organize their days and information on the go. Now the mobile device *du jour* is the "smartphone", which is not only a mobile phone with all the above, but now has access to the Internet. This has changed the world.

## An Emerging Threat

There is a wide range of emerging risks and threats to be considered as smartphones in particular penetrate further and further into the workplace. In general, the more features, software, and plug-ins a device or system has, the more opportunities exist for exploitation and security vulnerabilities. A serious concern, though, is that the various security technologies, standards, and policies that have been developed for PCs often do not necessarily apply to mobile devices. This is a rapidly growing field with completely new tasks and issues to address. Mobile device security is critical yet it seems to be lacking. There are risks of malware, hacking, viruses, identity theft, malicious email, spamming text messages, downloadable software with Trojan viruses – the familiar list of risks goes on, many from the lessons learned from the PC experience.

For enterprises, company data can now easily be present on mobile devices, and this presents the problem of company data that are not within the control of the corporation. Mobile devices with cameras, texting, and email capabilities have made it so that companies must consider the security of privacy and proprietary information in new ways.

There are two types of data-states to be considered on a mobile device. "Data at rest" pertains to the physical security of the device, as well as the data stored on the device. The best practice here is to encrypt data on the mobile device using 128-bit encryption (although if the device is left unsecured and requires no password for access, in the event that it is stolen, encryption won't help much). "Data in flight" pertains to the mobile device using networks outside of the enterprise information technology department's control (Brenner).

Additionally, the explosion of mobile applications on smartphones has had an accompanying rise in security vulnerabilities – often similar to what was seen on PCs a few years back. "When using a BlackBerry, Android, iPhone or other smartphone, we tend to assume all the nifty Web apps on these devices are relatively secure. At the least, we expect that a lot of the painful security lessons we

received on PCs a decade ago have been applied to today's phone apps... our assumptions have been wrong" (Brenner). There is still a significant security gap. In fact, "Lanier and Zusman concluded that in the mobile phone Web app world there's a lack of guidance, standards and best practices for developers" (Brenner). This should be of serious concern for all companies and security professionals, in addition to individuals.

## Addressing The Issue – Or Not

As it has been seen before, similar to the earlier days of the Internet, technology is moving markedly more quickly than security, and probably will be for a while. Unfortunately the default security on smartphones is often greatly lacking. Some regulating happens through software/security updates and patches, perhaps one way industry "deals with it", though it is often up to the consumer to actually proceed with the update to secure their mobile device.

Smartphones are such a new technology that is evolving daily - this is difficult to keep up with from a security standpoint. With the proliferation of a multitude of mobile operating systems like the Symbian (Nokia), Android (Google), Blackberry (RIM), iOS (Apple) and Windows Mobile (Microsoft), it makes it very difficult to keep up with the various systems. Blackberry has a good reputation for being able to secure information in a business environment, but Apple and Google lag behind.

## Mitigating Risks

Preparing a company to face and survive through these security threats and risks is a daunting and ongoing task for anyone. At a higher level, a company is going to want to ensure that there are sufficiently broad policies in place to cover mobile devices – both company-owned, and employee-owned (but dealing with corporate information, such as with company email). A business will also have to take a critical look at the role of mobile phones in their organization. How important are mobiles to the work that needs to get done? Who actually needs access? What features and functionality do they need, and what is just nice-to-have?

From a security policy perspective it does make sense to lock down on smartphones in particular, especially considering the differences between personal versus company-owned devices. Something that should be incorporate into policy would be that it really depends on what the mobile device is being used for in business terms. There are some legitimate cost/benefit analyses one can conduct to discern what sorts of controls need to be put in place (especially post-lockdown). For example, there are often C-level executives who need to be able to track their email all the time, assuming an administrative assistant is not doing that already. One idea might be to treat mobile devices like system administrative permissions – identifying the users who have a legitimate need for them.

There are a number of methods an organization can try when attempting to integrate mobile devices into the workplace.

1) Initially, ban all smartphones on the network, keeping these devices from operating on the network while trying to assess the best policies and practices.
2) Reach out to the business-side to determine their needs and run a parallel effort to conduct a threat analysis centered on smartphones and mobile devices.
3) Provide and support an employee education program that would empower individuals and build a security-aware environment and culture for employees.
4) Consider implementing a policy that allows only Intranet and no Internet, with proxy-controlled Internet access only for approved business requirements.
5) Put a procedure in place to immediately lock smartphones out of the intranet should a zero day or significant malware attack take place.

As with any new technology, the CISO will want to apply change management principles to determine if it is right for the company. Mobile technology has a lot of advantages for individuals but it exposes organizations to risk. Individuals cannot really be blamed for wanting to take advantage of these emerging technologies, and so organizations must create secure and clear messages about the expectations and policies.

## References:

Brenner, Bill. "SecTor 2010: Touring (and surviving) the mobile app minefield". 27 October 2010. CSOonline. Web. Available at: http://www.csoonline.com/article/630265/sector-2010-touring-and-surviving-the-mobile-app-minefield

McDowell, Mindi. "Defending Cell Phones and PDAs Against Attack". US Computer Emergency Readiness Team. 27 January 2009. Web. Available at: http://www.us-cert.gov/cas/tips/ST06-007.html

Korzeniowski, Paul. "Next-Gen Devices May Integrate Cellular, WiFi Connectivity". TechNewsWorld. 07 September 2006. Web. Available at http://www.technewsworld.com/story/52822.html

Koprowski, Gene J. "Mobile Phone Converging With 'Flash', Other Apps". TechNewsWorld.com 10 June 2006. Web. Available at: http://www.technewsworld.com/story/51011.html

Tauschek, Mark. "Developing and instituting corporate mobile device policies". 09 September 2008. SearchMobileComputing.com. Web. Available at http://searchmobilecomputing.techtarget.com/feature/Developing-and-instituting-corporate-mobile-device-policies