Mobile Management & Security: Significant Distinctions
by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In the first of this two-part commentary, Rob Smith, Chief Technology Officer of Mobile Application Development Partners (M.A.D.) LLC and at MSS Managed Security Services GmbH, began with a review of the security-management problems caused by the proliferation of smart portable devices in the workplace. In this part, he offers practical advice for balancing utility and risk. Everything that follows is Mr Smith’s own work with minor edits.

* * *

So what do we do? How can we protect our resources yet still enable business and stay compliant? Well if you like hanging out at a place called jail, do nothing. But as most of us would prefer a life outside of prison, you need to not just manage but secure these devices. But how can we do that?

The obvious route to securing these devices is to do what we have done all along. Install software similar to traditional desktop anti-virus and security software and let them run in the background, constantly watching for threats.

Sound good? Well, no, it doesn’t.

Even if the idea of constantly updating your mobile workforce with signature updates to protect against the newest threats while sucking battery life seems like a good idea at first, it is technically not impossible right now as you need to be able to do true multi-tasking to enable this.

iDevices (iPads, iPod Touches, and iPhones) do not actually perform true multi-tasking. But didn’t Steve Jobs tell me they did? In some cases, yes they do. All Apple Apps for example can run constantly at any time. However, for the average developer there is no way to enable an application to always be on and always watching your device. Only a single non-Apple application can be active at any given moment. The rest of them are frozen like a Star Wars DVD when you hit the pause button on your DVD player. There are a few exceptions to this rule but none that allows an application to watch what another one is doing.

Droid is even worse. Multi-tasking is possible, but all applications are created equal. This means that everyone can talk at once but no one can control what the others are doing, making it impossible for security software to protect you.

Enter phone-management software. At last count, at least 30 different vendors provide products all essentially doing the same thing. Most are offering you the perception of control without actually giving it to you. The reason; these management tools are an extension of Microsoft’s ActiveSync.
Put your device to the porn test. Can I surf porn on the device in the office? If the answer is yes, you have just exposed yourself to a potential lawsuit for creating a hostile workplace or for sexual harassment<http://jshinn.wordpress.com/2010/03/15/employer-liability-for-employees-internet-misconduct-or-when-surfing-the-web-can-wipe-out-your-business/> . You now have also made your company lose its PCI<https://www.pcisecuritystandards.org/> or HIPAA<http://www.hhs.gov/ocr/privacy/> compliance: both require content filtering as a key requirement for compliance.

Security and network manager at any financial institution or health care provider will tell you that personal e-mail and corporate e-mail don’t play nice together.[MK adds: see for many examples an extensive collection of municipal and county policies in Washington state<http://www.mrsc.org/subjects/infoserv/email.aspx>] However, on a Droid or an iDevice, there is no native way to stop a user from adding in their Hotmail or Gmail account right alongside their corporate mail server. This once again blows compliance laws. In order to be compliant, you must either deny all personal e-mail to the device or filter it first for the usual rubbish of viruses, malware, phishing, and spam.

Management software will not stop porn or filter personal e-mail. You must have security in addition to management if you want your network to be safe and compliant. A new hope is an old solution. Make them have content filtering. Make them surf over a stateful inspection firewall. Filter their e-mail from the scum of the galaxy. In short, treat mobile devices the same way you would treat any other device on your network. BlackBerry has been doing this for over 10 years.

Isn’t it time you did it for the rest of your mobile universe?

For some specific resources, see reviews at ________________________.

* * *

Bio on Rob Smith:

Rob Smith<http://de.linkedin.com/pub/rob-smith/1/883/553> is the Chief Technology Officer of Mobile Application Development (M.A.D.) Partners LLC in Frankfurt, Germany and has brought over two decades of technology design, support and management experience to the company. He currently oversees daily operations of product design and development and sets the strategic direction of the company’s technology and engineering endeavors.


Copyright © 2010 Rob Smith & M. E. Kabay. All rights reserved.

Permission is hereby granted to *Network World* to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.