Enterprise Security
iOS vs. RIM

There is no doubt that iPhone and iPad are the "in" gadgets that are getting more and more fans and apps. From the consumer perspective, both are great to handle and use, simple, and powerful.

But how do the CSO/CISO (Chief Security Officer/ Chief Information Security Officer) and the Enterprise Technical staff look at these popular Apple products? How will they integrate this equipment in the IT Security strategy of the company?

Should we use iPhone or go for BlackBerry? Use iPad or another tablet for the Sales Team?

Should these mobile devices access the IT infrastructure of the company, or should they be banned?

If the CSO/CISO allow these mobile devices to connect, how can they ensure that they are compliant with corporate standards to minimize potential security threats? And worse still, how do you tell the CEO he can't use his iPhone or iPad to access the company wireless network because the equipment was not properly checked for appropriate apps?

From a security point of view, iPhones and iPads aren't much different from any Mac, as they can be managed, securely locked and safely erased. Integrating iPhones and iPads in the company IT Security Strategy should be as easy as integrating a MacBook Pro or a MacBook Air. Like their big brothers, VPN access, a strict apps installation policies should be used.

VPN using PPTP, L2PT, SSL VPN or Cisco IPSec are already built in as de facto standards for remote secure connection to the company network. As with any other mobile device, some extra security features should be enforced, the most important being:

User Education and Security awareness

Looking at IT from the end-users point of view, they just want their devices to work and have the latest and coolest applications. Most of the users are reckless regarding the source of the apps they install on their computers, and the IT Staff become the tyrannic little dictators that don't allow them to have that cool game/app from a free download site. The more you climb in the company hierarchy the worse it often becomes for application security. I can't tell you how many times I've seen top management wanting to access the company wireless network with an iPhone that has been jailbroken.

Jailbroken iPhone/iPads have two huge security risks. First, you grant root (superuser in UNIX/BSD based systems like the Mac OS and iOS) access to the equipment. This results in equipment with weak or no password protection. Second, the quality and security of apps that are installed from non-trusted sources rather than from the curated environment of Apple's App Store. When your users ask if they can jailbreak their iPhone/iPad, just explain to them why they shouldn't and how this might compromise the strength of the IT Security that the CSO/CISO so carefully designed.

Most if not all of the needed information regarding integrating iPhones and iPads in business can be found at http://www.apple.com/iphone/business/integration/ and http://www.apple.com/ipad/business/integration/ . These pages are very well documented and straightforward, even for non Mac users. If your IT people begin to give excuses for not knowing how to properly integrate your iPhone and iPad, look to these pages for helpful support. All the Enterprise and Security features, like remote erase, and hardware encryption using AES 256 bit are documented in these publicly available PDF files.

I've read some articles that advocate the use of BlackBerry instead of iPhone/iPad because, supposedly, BlackBerrys are more secure than iPhone. The argument was that iPhone and iPad can be hacked, and RIM have their own network. Quite obviously, I disagree for several reasons. First and foremost is that almost any equipment can be hacked, given enough time, money, resources and dedication. Second, even with their own network, RIM could never stop malicious hackers or Governments accessing the information. I recall some cases such as the one in the Middle East country where a local Government used SS8 software disguised as a software update to compromise BlackBerry and this technique can be used by any malicious hacker. Even with proprietary encryption technology, RIM can't stop eavesdropping, either by hackers or Governments, using PhoneSnoop and other similar applications. And remember the pressures placed by some countries on RIM to have governments access to text and data on RIMs network. The list goes on and on, the bottom line is that RIM's BlackBerry is not more secure than iPhone. In my opinion, the extra cost of having to pay for RIM network service is not worth the money, when the iPhone uses industry standard secure technology and information that only goes between the mobile device and the company network.

The most important question is if a device can be hacked, can people outside the company access the information in the enterprise? Sure they can, that's the point of hacking into a device or server, it's to get access to information, personal or business-related. However, with an educated and security-aware user, the risks are mitigated. A properly designed and implemented IT Security strategy along with the user education will minimize the risk. My best advise is to get feedback from your users, work with them as they can be the best way prevent security risks.

Having a Computer Security Incident Response Team (CSIRT) with education and security awareness programs for staff is the best way to have a secure network and systems. Ensure that users are sensitive to the security issues that arise from reckless use of technology.

In summary:

- IPhones and iPads can be integrated easily and securely in any enterprise network.
- User education and security awareness is a must.
- Use only Apple App Store apps.
- Design friendly user policies and encourage communication with IT Staff.
- **Ban all jailbroken devices!**

Tiago Rosado
EMEIA BDM, Apple Expert
Dognædis, Coimbra - Portugal
http://www.dognaedis.com
(+351) 93 442 03 76