WEBROOT®
SecureAnywhere™ Business
—Mobile Protection

Delivering a Secure Mobile Future

George Anderson, *Senior Product Marketing Manager*
November 2012

Contents

Introduction

In two short years we have seen an explosion of Android powered devices. Google's mobile platform is up 250% over last year and according to Google's Andy Rubin, SVP, Mobile and Digital Content at this year's Mobile Congress in Barcelona they are seeing 850,000+ activations every day!

In all there are over 300 million Google-sanctioned Android devices roaming the world, 12 million of them tablets. And, that number doesn't even include devices like the Kindle Fire that don't use Google Services, or the huge sales from competing Apple, Microsoft and Bada platforms.

New offerings and even operating systems have come and gone as vendors like HP; Apple; Google; RIM and Microsoft try to ingrain themselves. Having a common, unified and fully integrated multi-platform operating system is fast becoming the order of the day with Android 'Ice Cream Sandwich' introduced at the end of 2011 starting the integration process on Google's tablets and smartphones. Apple working hard to bring together Mac OS with iOS, and Microsoft Windows 8 (due in October) leading the charge by being the first to have a common OS across PCs; laptops; ultrabooks; tablets and smartphones. This drive from the vendors for uniformity is to make it as easy as possible for us use any device on 'their' ecosystem for everything we do, and for developers to have a single platform to create applications for. It all adds-up to a huge diversification with shifts away from PCs and feature phones to smartphones, tablets, and new form factor ultrabooks as mobile computing becomes the most common part of our lives. In the US alone 43% of all new phones are smartphone sales and the stats are similar in Europe and catching up fast in Asia.

The mobile Internet has truly arrived and is starting to deliver on the anytime, anywhere and almost anyplace access that lets us take more control over our time and lives. The ability for us to communicate; collaborate; share; work and play with friends and colleagues has never been greater, nor have the online tools and applications to help us do so become so available, or relatively inexpensive.

The charge to adopt and harness this 'perfect storm' of mobile technology to simplify our work/life balance has not however been led by IT departments, but by us just simply using, or demanding to use mobile technology in the workplace. This has led to IT scrambling around to develop mobile policies, understand what devices are being connected to their networks, and then how to secure all of the confidential information that will now be held on our personal mobile devices.

Work Is Mobile

This sea-change in Consumer IT versus Enterprise IT is also leading to conflicts of interest between 'enablement' and 'risk management' as executives and other users insist on using their personal technology for business use – often without fully grasping the significant risks this opens them, or their organization up to. More unhelpful is that the security controls have lagged behind, both from a vendor perspective, and in the implementation of sensible policies and controls over 'smart device' usage in the workplace.

With up to 70% of all employees equipped with laptops and most also using two or three Internet enabled devices it's no longer unusual for a worker to find they are home-based or remote from the office, and using a non-IT approved device, in fact it's almost become the

norm. This raises a number of security issues like the higher levels of malware infection found with remote working, the increased difficulty in monitoring and enforcing security policies and often less visibility and control all round.

In recognition of this, Gartner have predicted the endpoint security marketplace changing completely between now and 2015. They see offerings emerging that integrate centralized cloud management with mobile device security and mobile device management combined with endpoint security that extends to all mobile devices and platforms.

The BYOD Phenomenon?

In recognition of this, Gartner have predicted the endpoint security marketplace changing completely between now and 2015. They see offerings emerging that integrate centralized cloud management with mobile device security and mobile device management combined with endpoint security that extends to all mobile devices and platforms. All these smart mobile device sales have translated into a tsunami of 'Bring Your Own Device' (BYOD) users in the workplace and 'Wild West' risk levels that threaten to ride roughshod over security policies; procedures and controls. Even worse it has prompted moves in the opposite direction, where the business advantages are being quashed by too conservative mobile policies. Add to this a lot of equally unacceptable 'wait and see, sitting on the fence' and you potentially have a disastrous security situation emerging.

Just to reinforce the size of this sea change in BYOD work usage a recent Survey in the USA by Harris Interactive1 on mobile device use to access and/or store company information found:

- >80% of employed adults using a personally owned device for work
- ~24% of employed adults use their own smartphone
- ~41% using personal laptops and,
- ~47% personal desktops
- ~10% using personally owned tablets

This just confirms how 'normal' mobile access has become and the genuine advantages it brings to users in getting on with productive work. In fact, most of these mobile access methods have been in place for a while - it's the smartphone and tablet usage that's is particularly new. The same Harris interactive research goes on to report that:

- <33% of users encrypt company data
- <10% of tablet users have auto-locking enabled
- ~25% of smartphone users use auto-locking
- ~66% of laptop users do NOT have auto-locking enabled

And then concludes that best practice dictates that turning on auto-locking; password protection and enabling encryption, plus the cost of funding security awareness and user education will solve a lot of the mobile access problem.

[1] The survey was conducted online within the United States by Harris Interactive between February 8-10, 2012 among 2,211 adults (aged 18 and over) and 1,320 employed U.S. adults.

While taking these actions are wise, they only go so far, and underplay many of the risks from anytime; anywhere; anyplace network access through personal devices.

Another current Survey conducted by Decisive Analytics questioned 440 CEOs and IT executives across the USA, the UK and Germany. It found that 78% of them already allowed their staff to use their personal devices such as laptops, smartphones and tablets, but insisted that security software be installed upon them.

Even with this security technology in place almost half of these companies admitted that they had suffered security breaches because of remote or mobile access. Education on managing employee BYOD behaviour was seen as key to reducing these security threats.

Barring these security issues nearly half of the IT Executives questioned said BYOD gave hem a competitive advantage, and 70% of CEOs were certain of the competitive advantage and saw BYOD as both an employee retention and recruitment tool that offered enhanced innovation and creativity and boosted productivity.

The conclusion here was that firms had to embrace BYOD to unlock its business potential, but had to adopt flexible security policies that say yes, but not to everything, and not for everyone! Webroot's own RSA Global research survey in 2011, looking at remote users and security risks, also found a direct correlation between the increased use of remote and mobile access and a significant increase in the amount of breaches organizations experienced. Simply, the more remote users you have the greater the security risks.

Mobile Malware

Back in early 2010 Webroot saw that the needs of organizations would change dramatically as smart mobile devices proliferated and that general security risks would continue to rise. So by the end of 2010 we were offering consumers our Webroot Mobile Security for Android smartphones and tablets.

At the time, the choice of Android over Apple was deliberate. The Android platform is far more open with users able to download applications from almost any site. Android application stores are not strictly policed (unlike Apple's app store) and often lack any upfront app review process. Android as a platform is still enormously fragmented too, with different versions commonplace. Application 'permissions' (resources apps want access to on the device to operate with) often including location data, personal info contacts coupled to users not reading their terms and conditions introduces even more data theft or loss risks.

Choosing Android was prescient, as we have since seen, this platform is heavily targeted by malware with attackers' method of choice being malicious apps spread via the Android Market, or third-party app stores. Users don't even need to "download" an app to expose themselves to Android risks. Pre-installed Android apps often come with unrestricted permissions and attackers have successfully exploited the older fragmented versions of the OS and those apps to get enough permission to install malware. This is not to say iPhones and iPads are not exposed to their own vulnerabilities. Most notably, iOS devices are just as susceptible to data breach due accidental loss of theft of an iPhone or iPad.

To be fair, Google do regularly patch exploits, but many users' devices won't have the latest versions - as the carriers and the device manufacturers don't want them to be able to update, but buy the next device with the latest OS installed. With AVTest.org, an independent malware prevention testing agency, seeing Android malware growing at 450% over the first 4 months of 2012, the manufacturers and carriers should be contemplating changing that policy very soon?

During early 2012 Webroot saw the following malware among our Android users:

- 1.5% scan detections of malware
- 0.68% Install shield malware detections
- 0.88% Executions shield detections
- 0.86% File detections
- 16.2% Malicious URL detections[
- 1.88% Malicious URL detections from SMS messages (text messages)

AVTest.org also estimate there are now over 450,000 apps in the Android market, while there were less than 100,000 in July 2010! This makes it the fastest growing software market, and with the rise of new apps, the amount of malware increases too. Android malware growth is now showing a similarly high rate to that seen in PC malware over the past few years, which has been expotential.

The malware threats from Android include Phishing and Banking Trojans, Spyware, Bots, Root Exploits, SMS Fraud, Premium Dialers and Fake Installers. There have also been reports about Download Trojans, applications that download malicious code after installation, meaning that these apps are not easily detected by Google's Bouncer technology during publication in the Google Android Market.

Huge growth, plus easily exploited vulnerabilities, means there is a lot of valuable mobile data now in play making this area very attractive to cyber-criminals.

Balancing the Risks

So the situation is clear, BYOD has seen the line between corporate-owned devices and personal devices being blurred. The risks are high, and the potential for data loss and other breaches significant. What logically follows is that to avoid the types of breach others are experiencing it is essential that enforceable and realistic mobile device risk policies are put in place.

These policies and controls must also accurately reflect the level of BYOD access that fits your organization's risk profile, and be clearly communicated in writing and in other security awareness training.

So now on a practical level - what should you be considering to mandate through policy and controls to ensure that the right measures are in place to protect both corporate information as well as personal information?

A good guide to what risks to consider was published by ISACA in 2010 and titled "Securing Mobile Devices" and while not absolutely current in its thinking it is very useful and is available for download FREE at www.isaca.org.

ISACA Mobile Risks:

1. How secure are the mobile apps being accessed, and what are their permission level vulnerabilities that could be used to both compromise the device and attack the network? (This raises the need for some granular application management control.)
2. How exposed are devices to malware vulnerabilities? (The need for endpoint malware defense.)
3. The ease of loss or theft of a smart device? (The need for remote wipe, encryption, passcode, auto-lock, usage authentication.)
4. The risks to on-device data at rest storage security? (The need for local data encryption.)
5. How to back-up, synchronise and restore data? (The need for loss, theft, data corruption DR strategy.)
6. The risks to data on the move and its interception? (What sort/types of links are needed to stop interception?)
7. The risks of a visible Bluetooth connection? (The need to tie down Bluetooth visibility to stop hijacks.)
8. The risks from on-board microphones and cameras (The need to look at this from a hijack ing or eavesdropping perspective?)
9. What user authentication/access controls are needed? (The need for what authentication and to what level dependent on the data being accessed?)
10. The risks of data leakage (The need to separate and protect both Personal and Enterprise Data and look at controls over the export of data from the device via Internet, via cloud or via Bluetooth etc.)
11. Who has device administration control? (Who administrates a users' device, what controls are solely controlled by Enterprise IT, what do users get in exchange?)

This list is not exhaustive, but it starts to prioritize some of the important questions you need to answer about the use of personal devices. You of course need to add the compliance and regulatory controls that already exist over data usage and data access within your organization. And, equally vitally, you need to know how you are you going to easily manage this all?

The Future Today

And that brings us right around to where we came into this paper harnessing this 'perfect storm' of technology convergence?

Webroot's view is that endpoint security embracing all types of endpoint and web usage across PCs, servers and mobile devices is paramount. And, for ease of management and user control that should be through an integrated cloud based security suite infrastructure.

As this approach ensures the same control, protection, enforcement and accountability of users regardless of the location or the device they are using.

The solution is SecureAnywhere Business – Mobile Protection. SecureAnywhere Business – Mobile Protection, offers market leading protection and unified management for the fastest growing mobile operating systems -- Android and iOS. Powered by the Webroot Intelligence Network, the solution offers advanced antimalware detection, lost device protection, secure web browsing, and blocks unwanted calls or SMS messages that might contain malicious URLs. By integrating this into the Webroot SecureAnywhere Business platform, we are able to offer a single pane of glass from which IT administrators can control both PC and Mobile devices. A 30-day free trial is available from:

www.webroot.com/mobileforbusiness

So, if you want to understand more clearly how a new high visibility, high endpoint management control approach works, simply download the Webroot SecureAnywhere free trial and get access to the Webroot management portal - you can be up and running in a few minutes.

Summary

BYOD does raise a lot of issues as the technology is not 'owned' by IT. None the less IT does hold the access right 'keys' and should be able to strike a balance on the levels of administration rights, network access and data controls it is willing to cede in exchange for users using their personal devices for work.

Efforts will have to be made to explain why certain activities are allowed, or not, and IT Security in particular should be seen as helping the user to protect themselves and their devices as well as the organization they both work for.

The place to start is of course the development of a corporate mobile policy, quickly followed by a series of clear communications to employees about why they are being put in place and how they are so necessary to protect all parties. With that out of the way, the policy enforcement can be looked at and relevant controls to ensure that antimalware software is present on devices, and passcodes, encryption and other easy to deploy protections are in place, like remote wiping, regular back-ups etc. are all active and implemented. At the same time Mobile Device Management capabilities will become essential for those with many mobile device users to lower the management costs and simplify the monitoring, reporting and security management.

The reward for delivering a well-executed and managed 'mutual' approach to BYOD will be greatly enhanced productivity yet adequate controls over data usage and access within an acceptable risk posture for everyone.

About Webroot

Webroot is committed to taking the misery out of Internet security for businesses and consumers. Founded in 1997, privately held Webroot is headquartered in Colorado and employs approximately 350 people globally in operations across North America, Europe and the Asia Pacific region.

Webroot Headquarters
385 Interlocken Crescent, Suite 800
Broomfield, Colorado 80021 USA