Are You in Control of Your Data … or is Your *Bring Your Own Device* (BYOD) Policy Controlling You?

By: Gordon Merrill, MSIA, CISSP

Colleague and friend Gordon Merrill has been thinking about the issues of integrating personally owned devices into corporate environments. Here is the first of a series of articles on this important topic. Everything below is Mr Merrill's work with minor edits and additions from Mich.

* * *

Winn Schwartau< http://www.etcss.org/speakers/2012-speakers/ >, speaking at the East Tennessee Cyber Security Summit < Cybersecurity conference in October 2012, stated that by the end of 2020 there are expected to be 20 billion endpoints on the internet and by the end of 2050 there will be one trillion. Currently there are over 3,800 versions of just the Android mobile-device operating system < http://www.android.com/ > in use. A February 2011 report < http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/a#smartphoneos > estimated almost 500 million shipments in 2011 of *new* smartphones using Android, iOS, Symbian, BlackBerry, Bada, Windows Phone and others.

In 2011, I wrote a series of articles for *NetworkWorld's* "Security Strategies" newsletter which recommended information assurance (IA) work groups to help define some new ideas and new technology for protecting the cloud- and mobile-based technologies that are growing in popularity:

1. Is the operating system dead? (Jul 4, 2011) < http://www.networkworld.com/newsletters/sec/2011/070411sec1.html >
2. Is your company ready for 4G mobile connectivity? (Jul 6, 2011) < http://www.networkworld.com/newsletters/sec/2011/070411sec2.html >
3. Can you comply with court orders for data from the cloud? (Jul 18, 2011) < http://www.networkworld.com/newsletters/sec/2011/071811sec1.html >
4. Does your security policy reflect mobility and cloud security? (Jul 11, 2011) < http://www.networkworld.com/newsletters/sec/2011/071111sec1.html >
5. Is your company ready for legal holds and compliance with mobility and the cloud? (Jul 13, 2011) < http://www.networkworld.com/newsletters/sec/2011/071111sec2.html >

In my previous articles, I mentioned how there are still more questions than answers with the proliferation of the consumerization of IT and the multitude of new personal devices. Still companies and IA personnel are faced with the ever tightening restrictions of governmental regulations on security, while at the same time the public is demanding to use their own device, under their personal control, to access anything they want, when they want and how they want. How does a company maintain total control of their data from creation to destruction as the US Justice Department (DoJ) insists, with so many devices wanting to access and grab it? Smart Phones are smart in all that they can do and all that they can access for the consumer, but they are still very immature when it comes to letting IA personnel sleep well at night.

The user will expect to connect to your data portal within five seconds max. This is the length of time needed in a very unscientific study done in one of my classrooms to see how long it took students to fully connect to Facebook. Even though Facebook recently admitted to an average of 600,000 hacked accounts a day< http://nakedsecurity.sophos.com/2011/10/28/compromised-facebook-account-logins/ >; that is now the standard connect time that the consumer is expecting to achieve when they click on your application and access your data. You on the other hand are not allowed to have any hacks on any day, but the connection time expectations are the same. Your user will touch the icon for the data portal to your company, hope to connect in five seconds and then have full access to all the data they would have access to in the company. Think through this a minute.

What is this mobile device doing with a portal to your system and data? There is a link between you and them which may or may not be a VPN, so how is it encrypted? What data are going to the phone in order to enable encrypted data traffic? Is it a token passed to the device to authenticate the encryption? Can that also be received by someone else who is monitoring the user's smart device? If not can they still intercept the encrypted transmissions and decrypt later? Even if all of that has been secured by some yet unseen product, now what control do you have on your information after the user gets into it? Can they save it to removable memory; can they resend it from that device to; email, Facebook, cloud storage, Bluetooth devices, printers, fax, or a text with attachment? If they have the ability to do any of the above, have you maintained full control of your data from creation to destruction? According to the US Department of Justice, you have not< http://www.networkworld.com/newsletters/sec/2011/071111sec2.html >. If you are able to find a way to establish an encrypted connection with no possibility of man-in-the-middle interception with encryption so good it defeats even the Microsoft VPN issues, then you get down to what is left on the device.

So we are left with the following wish list. The user can view all the data they need to make timely business related decision from any deice they choose. The user cannot save the data, forward it, re-post it, print it, or screen shot it (although they can always photograph it with a separate device). And when they are done with their connection there is nothing left on the device that can even be forensically retrieved. So what do we need to make the BYOD have a chance of being anything more than a looming massive data, legal, and financial disaster for any company in the public trust?

So getting back to the basics, what do we want to accomplish despite the failed current models of bring-your-own-device (BYOD)? Users want to access our data for authorized reasons and we need to keep absolute control of our data from creation to destruction. What happens when the user of a BYOD accesses our corporate data and can save them, screen shot them, change them, re-post them, print them or remove them? Have we not then lost control of our data? Yes, we have. Considering that around 17 million mobile devices are lost a year < Winn Schwartau from above >, if there were any data left on the device from our company that could be forensically retrieved, we would have lost control of our data.

Microsoft has the spark of an idea wrapped in one of its features in recent Windows operating systems. We need an application that would allow users to bring their own devices to bear in accessing our data through a view-only application. The screen would only be a remote monitor, a dumb terminal if you will, showing what the user could see if inside the company or at their own desktop. This window would allow them to view, edit, change, and overwrite the data inside the company while the whole time none of that data would ever reside in usable form on or be retained on the device. Again, this technique does not stop side-channel data capture such as photographing the screen and using optical character recognition to regenerate usable data, but it is better than nothing.

In reviewing several potential software vendors for mobile security there is a big gap in how they can secure the data from hijacking (much like a man-in-the-middle attack but worse –making a second phone work on the same frequencies and SIM card channels as the hijacked phone and seeing all the texts, voicemails, data transmissions etc.) or from remaining forensically retrievable data from the mobile device if stolen. I do not see how we can certify remaining in control of our data if they either can be retrieved from stolen device, SIM chip, or recovered from sidetracking for encryption ciphering later. Several companies have software they say allows the smart phone to do some of this now, but they cannot guarantee that while accessing data they did not save it, print it, or copy it, or screen shot it.

Most of the readership of this article will be IT security or IA trained personnel. Even if not certified in Certified Information Systems Security Professional (CISSP), most have been trained in the ten domains of CISSP< https://www.isc2.org/cissp-domains/default.aspx >. The domain of *application security* stresses the need for proper application development to include the overwriting of memory used by this application to keep from leaving behind recoverable or usable data.

So here is where the work groups come in. We can find vendors who will make a form of thin client available as a small form factor virtual desktop. We need to build on that and make the connection secure, a VPN connection and an encrypted connection all within 3-5 seconds. Then we need the connection to allow the user to manipulate his/her internal company "desktop" from their mobile device. Then that "virtual connection" needs to leave all the company data inside the firewall and the "perimeter". When the user

disconnects we need the device to overwrite the memory used per Department of Defense (DoD) standards without a major hit on the mobile device, or battery life. How big is this work group?

The next installment will discuss the legal implications of a BYOD program on the company security program and their potential legal exposure.

* * *

Gordon Merrill< mailto:grmerrill@epbfi.com >, MSIA, CISSP is a cyber security professional whose career spans over three decades and has taken him to 48 states and six foreign countries. Gordon's information assurance background has included working for major computer companies such as IBM, managing IT projects for Fortune 250 companies in the risk management field, owning his own business, and working as a private consultant. along with publication of series of articles regarding the skills of an IA professional, the death of the operating system, cybersecurity threats, mobile data issues, and data security. Gordon has been the Chair of the Information Technology department at a local college, and primary instructor for the Bachelors Information System Security Department, instructing students in all ten CISSP domains. Gordon's experience and research have him most worried about eroding personal privacy and lack of potential for real data integrity.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

* * *