BYOD: An Examination Of Bring Your Own Device In Business

Chris Rose, Ph.D., Capella University, USA

ABSTRACT

There are security implications and hidden costs of Bring Your Own Device (BYOD). A recent study found that a company with 1,000 mobile devices will spend an additional $170,000 average per year if they adopt the BYOD methodology. In addition, there is the increased complexity of supporting various types of devices running different operating systems on different carriers. There is also a problem of legal liability and an organization will also lose brand identity since the number belongs to the employee and not the organization.

Keywords: Bring Your Own Device; BYOD

INTRODUCTION

In a recent survey of 600 U.S. IT and business leaders, Cisco reported 95% of respondents permit employee-owned BYOD devices in the workplace. Juniper Networks surveyed more than 4,000 mobile-device users and professionals and found that 41% who use their own device for work do so without permission from the company (Kaneshige, 2012c). New research also found that 84% of employees use the same smartphone for work and pleasure, but just 53% said they had a password protecting the phone (BusinessNewsDaily (2012).

Initially, BYOD sounds like a bargain for organizations looking to save money since if employees are willing to use their own personal smartphones and mobile devices for work then that will be less money that has to be spent by the organization to purchase technology equipment. In addition, employees get to use whatever type of phone or tablet they prefer. After all, if employees offer to use their personal computers and communication devices for work, that is less money for computer gear coming out of an enterprise's capital-expense budget. Employees also get to use their preferred hardware, and some organizations report this can result in overall higher employee morale (Joch, 2012).

FRAGMENTATION

Google has stated that just 1.2% of active Android smartphones run the latest version of Android. Some 57.5% are still running Android 2.3, a version which is almost two years old. This is caused by Google's own approach to its OS, combined with problems caused by the telephone carriers, the phone manufacturers and what the user expects from their device (Dobie, 2012).

However, this fragmentation causes tremendous support problems and when an IT department allow their users to bring various types of Android phones with various versions of the OS into their network, the problems could be catastrophic. Even if only one type of phone running one version of the OS was allowed, problems would arise if that particular phone/version /carrier combination never got upgraded by the provider. Android supports Exchange, but again the fragmentation results in no uniformity therefore security support is almost impossible. In addition, third-party apps that are supposed to enhance Android and Exchange can sometimes cause problems if a certain phone/version/carrier combination is upgraded and another is not (Lyn, 2011). The IT department will now have to manage and secure a wide range of devices including smartphones and tablets with different operating systems all accessing corporate data.

The popularity of smartphones means new models are constantly being released and even after release they are continually being upgraded. Manufacturers constantly push out new software updates with new features to change the look, feel or performance of the device. Sometimes even a new version of the OS software is pushed to the device thereby changing everything that was previously secure in the old version. However, getting a device that was previously running on one version of the OS to operate on the new version is not easy and requires a significant amount of work. The new software has to be tailored to the specific hardware within the device and even on devices that are apparently similar, if they are on different carriers there needs to be substantial customization. For example, a Snapdragon S4 device needs Jelly Bean-friendly Qualcomm drivers for the CPU and GPU.... If radio changes have been made, the new code must be certified by regional authorities, as well bodies like the Bluetooth SIG and Wifi Alliance mobile operators have great influence into what goes out on their networks" (Dobie, 2012).

SECURITY SUPPORT

"One measure to look at is how workplace smartphones are being provisioned. Forrester Research says employees choose their own smartphones 70% of the time, with 48% of the devices picked without regard for IT support. That means only 22% of the smartphones used at work in the United States are delivered as a take-it-or-leave-it device by IT." In addition, some employees will deliberately flaunt company policy and bring in devices that the IT department does not even know are on the corporate network and therefore are not managing (Joch, 2012).

However, many companies do not take the necessary precautions despite the fact there is a strong possibility for corporate security flaws to be exposed. More than 50% of the companies did not have any ability to remotely wipe a device if a phone is lost or stolen and 28% did not know if the company could remotely wipe their device. Most workers did not even know what to do if their device was lost or stolen, did not know who to contact, in fact 15% said they would contact their service providers, while 29% said they would contact their company. "The results of this survey demonstrate that companies must do much more to protect their critical infrastructure as employees work from their own mobile devices, such as tablets and smartphones, in the workplace. Companies need to have security and education policies in place that protect company data on personal devices" (BusinessNewsDaily (2012).

When IBM surveyed several hundred of their employees, many were completely unaware of what popular apps were security risks. IBM now has new complexities that they didn't have because these devices do not have as much security as BlackBerry phones. IBM updates all these devices remotely over the air so each employee's phone has to be treated differently depending on what model/operating system/carrier and what that employees job responsibilities are. "Some people are only permitted to receive IBM e-mail, calendars, and contacts on their portable devices, while others can access internal IBM applications and files" (Bergenstein, 2012).

Companies that use BYOD must invest in each platform/OS/carrier in their BYOD portfolio therefore this not only requires multi-device support but multi-department support as well since not everyone requires the same data but they somehow also have to communicate.

COST OF BYOD

The Aberdeen Group states mobile BYOD will cost about 33% more than a company-owned mobile device approach. Workers want to use their personal iPhones, iPads and Android devices instead of company-issued BlackBerry smartphones and PlayBooks . Company CIOs might think there are cost savings by not having to purchase more BlackBerrys, but the Aberdeen Group found that "a company with 1,000 mobile devices spends an extra £110,000 ($170,000) per year, on average, when they use a BYOD approach" (Kaneshige, 2012a).

"I think it could well be at the end of the day that BYOD devices are more expensive than if you have full control and the company owns the device," ..."Companies sometimes only look at the cost of the device, but when it comes down to it, [BYOD] is more expensive if you look at the total picture" (Chickowski, 2012).

There are data and connectivity costs to be considered and this will be billed to the company and this is higher than a centralized corporate device system and in addition there are hidden costs. There are substantial application and support costs since not only is the cycle of mobile apps much shorter than established mobile programs but there are substantial costs if developers have to write apps for different phone/version/carrier combinations.

Another major problem is the senior staff in a company, they already have the financial resources to purchase all the latest devices but are also have enough seniority to disregard company rules and use them at work. For example, it is doubtful that the IT worker would tell the senior VP in a major corporation that he cannot use his latest Android phone. It is difficult to stop these senior persons but they are the very persons who would have the type of confidential data that the company would want to protect. If this device was lost or stolen, that data would be compromised, therefore if the IT department cannot manage these devices, or have the ability to remotely wipe these devices, there is no real idea what type of data has been lost (Sherriff, 2012).

Research by Aberdeen shows that if a company gets a volume discount rate for a certain type of phone from one carrier, they would spend an average of $60-per-month for a smartphone's wireless voice and data services. However, the average reimbursement for BYOD is $70-per-month. If a company negotiates they can purchase hundreds or thousands of smartphones and then receive a volume discount rate, in fact, this might even include some free replacements but under BYOD the company will not get these benefits (Kaneshige, 2012a).

This might not be very important since the employees paid out of their pocket for the BYOD device, but there is a major problem with the actual wireless service. If a company supplies their own mobile devices they can buy services in bulk from a single carrier and get substantial discounts whereas the average employee would pay a much higher rate. Therefore there is the additional cost or reimbursing these BYOD employees since an employee sends in a monthly expense report for their wireless bill. Aberdeen says it takes each expense report takes about $18 to process so therefore the cost of BYOD is now about $90 per month and employees do not itemize their BYOD wireless bill so there is no differentiation between what is business and what is personal although a company might put a limit on these bills.

Whenever a company purchases devices and services in bulk they can automate deployment and management of the entire data usage, email and security deployment." Typically, BYOD brings iOS iPhones and iPads into BlackBerry shops. This means CIOs will have to invest in a multi-platform mobile device management solution and other software, maybe even a VPN (virtual private network) layer. "The cost of compliance - ensuring governance, risk management and compliance - is also more difficult when devices must be chased down individually," The IT department does not control the actions of the phone manufacturers or carriers but they are still being held responsible for supporting BYOD for employees (Kaneshige, 2012a).

BRAND

A telephone number can be a strong brand, perhaps 1-800-FLOWERS is the best example of this. This is the number that people remember; it is the number that is prominent in all their ads. But in BYOD you lose control of this important piece of your brand.

An important part of your brand can be your phone number, for example, if you owned a few hundred or few thousand of consecutive numbers such as (305)555-xxxx, this would be a part of your brand and you would own this if an employee leaves. The IT department would just wipe the device and re-provision it for the new employee. You lose all this value with BYOD.

Suppose your top salesman in your BYOD organization has been with you for the last five years decides to leave you to work for your competitor. The problem is that this is his number and he can take it with him wherever he wants. This is a critical corporate asset since this is the number that customers call when they want to place an order. Obviously these customers are still going to call the same number even when he leaves and starts working for your competitor.

There are ways around this of course, such as obtaining Google Voice numbers for all BYOD devices, but this just adds an additional layer of complexity and there is no guarantee that you can get the number of consecutive phone numbers that you want (Kaneshige, 2012d).

LEGAL LIABILITY

Suppose the IT department of a company needs to get some corporate data from an employee's personal phone or tablet, under BYOD the employee would be forced to hand over the device. Suppose, for example, child pornography is found on the device, there are a number of legal questions that would have to be considered according to (Kaneshige, 2012b).

- Does the IT team have the right to search personal information
- Does the team have an obligation to call law enforcement
- Would this finding be admissible in court
- Was the employee's privacy rights violated
- Was the BYOD policy enough to cover such a search
- Suppose it is discovered that the employee was working on something contrary to company policy, can the company remotely wipe the device
- Can the company wipe personal information
- What legal basis is there to do this

If a BYOD device that has thousands of customer's personal and confidential credit information is lost or stolen, is it the company or is it the employee who is liable? Without answers to these and similar questions, BYOD will always leave unanswered questions. When a BYOD employee gives notice or is terminated, the company has to quickly remove the device from the corporate network, with a corporate owned device this would be much easier. In addition, sometimes there might be a part-time employee or contractor who needs to connect to the corporate network, again this is much easier if it is a corporate owned system, (Kaneshige, 2012a) "In the corporate-liable BlackBerry world--which many IT organizations are now moving away from--it was relatively simple to predict and manage risk," says Dan Dearing, vice president of marketing at Enterproid" (Chickowski, 2012).

CONCLUSION

BYOD might initially sound like a bargain but the loss of brand identity, the possibility of legal liability, the difficulty of IT departments supporting different phone/version/carrier combination and the many security problems that may arise does shed a different light on BYOD.

"Blackberry is losing status as a cool and sexy device, but cool and sexy is not what IT needs. The constant attention on the enterprise that RIM delivers is what business needs". RIM's BlackBerry Enterprise Server has long worked with Exchange and BlackBerry Enterprise Server 5.0 is fully certified to work with Exchange 2010 and comes with full technical support services, which is critical for IT. With full support, IT has an almost guarantee of faster turnaround time for solution of any BlackBerry problems, and RIM can be held accountable if they don't deliver as promised. BlackBerry Enterprise Server (BES) gives control to the IT department to individually control and set policy for each BlackBerry device and even to perform remote wipes. Since BES offers all these security controls out of the box, RIM remains the only solid choice for businesses."For IT infrastructures, particularly those who must adhere to rigid corporate or government-mandated compliance requirements, the BlackBerry ecosystem is unmatched in security and manageability for smartphones" (Lyn, 2011). BYOD just cannot provide this.

AUTHOR'S INFORMATION

Chris Rose, Ph.D., Capella University, USA. Dr. Rose has written extensively about technology related issues. E-mail: drcerose@gmail.com

REFERENCES

1. Bergenstein, B. *MIT Technology Review*. IBM Faces the Perils of "Bring Your Own Device". Retrieved on August 27, 2012 from http://www.technologyreview.com/news/427790/ibm-faces-the-perils-of-bring-your-own-device/
2. *BusinessNewsDaily* (2012) Mashable Business. Using Your Smartphone for Work? You're Taking a Big Risk. Retrieved August 24, 2012 from http://mashable.com/2012/08/17/smartphone-security-lacking/
3. Chickowski,E. (2012). *Information Week Security*. BYOD: How To Calculate Hidden Security Costs. Retrieved August 12, 2012 from http://www.informationweek.com/security/mobile/byod-how-to-calculate-hidden-security-co/232800422
4. Dobie, A. (2012) *Android Central*. Why you'll never have the latest version of Android. Retrieved Sept. 16, 2012 from http://www.androidcentral.com/why-you-ll-never-have-latest-version-android
5. Joch, A (2012) *Business2Community*, BYOD: A Cost Saver or a Curse? Retrieved August 14, 2012 from http://www.business2community.com/tech-gadgets/byod-a-cost-saver-or-a-curse-0166377#kF6Qgqiwk10ugw7g.99
6. Kaneshige, T. (2012a) *ComputerWorld UK* BYOD - Five hidden costs to a bring-your-own-device progamme/ Retrieved August 14, 2012 from http://www.computerworlduk.com/in-depth/mobile-wireless/3349518/byod--five-hidden-costs-to-a-bring-your-own-device-progamme/
7. Kaneshige, T. (2012b) CIO.com. BYOD Stirs Up Legal Problems. Retrieved August 22, 2012 from http://www.cio.com/article/706086/BYOD_Stirs_Up_Legal_Problems_
8. Kaneshige, T. (2012c) CIO.com. CIO Challenge with BYOD: Don't Fall Down the Rabbit Hole. Retrieved August 24, 2012 from http://www.cio.com/article/706579/CIO_Challenge_with_BYOD_Don_t_Fall_Down_the_Rabbit_Hole
9. Kaneshige, T (2012d) CIO.com. BYOD's Phone Number Problem. Retrieved August 25, 2012 from http://www.cio.com/article/707405/BYOD_s_Phone_Number_Problem
10. Lyn, S. (2011) PCMag.com. BlackBerry Still Tops for IT. Retrieved 9/5/2011 from http://www.pcmag.com/article2/0,2817,2390526,00.asp
11. Sherriff, L. ((2012) ChannelRegister.co.uk. BYOD: The great small biz security headache. Retrieved August 23, 2012 from http://www.channelregister.co.uk/2012/06/18/byod_sme_security_research/

NOTES

