Anastasia Kwit
MIS 798 Spring Research Paper
June 4, 2012

Overview: As corporate technology environments adapt to an influx of non-standardized mobile devices and BYOD policies, Security Management has become a correspondingly sensitive and vital function within IT departments. While smartphones and tablets allow employees to increase productivity away from the formal office setting, there are serious risks to network and data assets to be addressed. Mobile Device Management applications and robust security policies to protect both business and individuals will play a critical role in addressing these risks and provide a balance between security and productivity to support business needs.

****

Just as IT departments began to feel safe exhaling with a growing sense of control of their on-premise security, the ominous public cloud rolled in, closely flanked by the speedy adoption by the masses of smartphones and tablets that all-too-easily connect to corporate networks and email systems. The onus of network and data security swelled exponentially and new challenges for security management have arisen as operational hardware and devices begin to exist outside the ownership realm of the business entity. The new dilemma is how to manage and secure equipment the business does not own, and walk the fine line of controlling devices personally owned by employees.

ITIL considers Security Management in two aspects. Clearly, the existence and implementation of security protocols and controls over information and provided services is one key. The CIA triad of confidentiality, integrity and availability are the primary objectives of these controls. Data and systems must be protected from unauthorized views or use and manipulation while at the same time not being so locked down that users are impeded from accessing the resources or so open that anyone can obtain access.[1]

More important, though, is the definition, execution and compliance with a broad-scope security policy which guides the implemented security controls as well as expectations and behavior of the business and user populations.[2] As many management teams quickly jump aboard the public cloud bandwagon and may recognize financial gains by adopting BYOD environments, it is vital for IT management to step up and stay in the loop of the business strategy. The CIO or IT Director must have an open dialogue with these management teams to expose security risks and define security policies early on. All parties must agree on the security policy to ensure top-down compliance and support.

Mobile devices stand staunchly on the front lines of the new technology trends business users are flocking to and may be causing some of the biggest headaches for IT departments. Sometimes it can be a nightmare trying to manage personal use of corporate PCs and laptops. Understandably now, it can seem impossible to convince employees that their personally-owned devices must comply with security policies if they want to connect to corporate email, applications or networks. The users may rail back that they are trying to be more productive outside of their hardwired desk space and that the business

[1] (Larson, Mani, & Smith, 2012)
[2] (Brewster, Griffiths, Lawes, & Sansbury, 2010)

should be grateful its employees are willing to be tethered by a mobile device at all. While businesses have a right to protect its assets, employees oftentimes feel a sense of entitlement to connect personal devices to the network – for both work and personal-related usage. CEOs and corporate boards will need to find a balance between data and systems protection, cost savings, productivity and employee satisfaction in the sphere of mobile device access.

Cal Pierce of Opinno interviewed Kimber Spradlin, an Endpoint Management and Security Specialist at IBM, who described three corporate views of private mobile devices. First, and becoming an obsolete option, is to ignore them. More prevalent is the second option to provide "low-level access to e-mail and calendaring systems." However, as more sophisticated smartphones and especially tablets enter the workspace, the need for access to corporate files is becoming more essential. Parallel to this rapid device adoption is the increase in security exploitations. While worker productivity may be increasing, so are the vulnerabilities and risks to corporate data and systems.[3]

As RIM's Blackberry line begins to lose its luster for both personal and corporate audiences in the iPhone and Android age, businesses should look back and recognize why RIM was once the king of corporate mobile communications. Its key competitive edge continues to be its focus on data security which caters directly to the enterprise-level corporate world as well as small and medium size businesses with high data sensitivity. All communications sent and delivered via Blackberry devices are filtered through RIM's encrypted network adding a layer of security not available on other mobile carriers such as AT&T, Sprint or Verizon.

Additionally, an implementation of the Blackberry Enterprise Server (BES) allows IT staff to directly manage all Blackberry devices connected to the network. BES allows bulk, approved and scheduled rollouts of software updates and patches to improve device security and performance. BES also provides a layer of security protocols for each local device – applications, file types and permissions can be tailored for all, some or specific devices. Furthermore via BES, access to the corporate email network on the mobile device is completely controlled by an administrator. Devices cannot be connected through corporate channels without a profile or authentication password. (It is important to note, however, that Blackberry devices can connect to corporate email servers via POP or IMAP connections if they are configured outside of a BES profile. These types of connections are not manageable via BES.) On the other hand, if a device is lost or stolen or not turned in by a terminated employee, BES allows a remote lockdown of the device, even a total wipe if required.

Yet, to enjoy all of this control, a hefty investment in RIM's Blackberry software and licensing is necessary along with proper training of BES administrators and support. For enterprise-size businesses, this is often a non-issue and Blackberry continues to hold strong in such environments. However, the high costs for operation and the consumers' taste for flashier, better designed, and oftentimes more functional devices has played a large role across the board in the downing of the once imposing RIM behemoth.

Perhaps RIM felt untouchable in its place as the number one provider for corporate devices in the early and mid-2000s. Perhaps the financial crisis of the past five years has accelerated what may have been a slow turn by consumers away from Blackberry to iPhone iOS and Android-powered devices and

[3] (Pierce, 2012)

businesses capitulating to supporting individually-owned devices. No matter. The world of a thousand personal mobile devices is here, and they all want to connect to your network. Welcome to the Bring Your Own Device (BYOD) world some IT professionals have dubbed *Bring Your Own Disaster.*

Here is where ITIL Security Management comes into play. First, a security policy must be defined for the support of mobile devices. Dialogue must occur between IT leaders, the executive team and HR management to develop a policy which protects both the business and its personnel. Gartner researchers concur that "Before making any effort to select the most appropriate tool for MDM [mobile device management], organizations need to understand their requirements and define clear policies for deployment, including corporate data and application protection on the device and back-end servers; isolation from personal content, if needed; and cost containment."[4]

Issues to tackle in an MDM policy include:

1. Define which devices will be provided and supported by the company and IT unit.
2. Define which employees are entitled to these devices and services.
3. Define whether personally-owned devices are allowed connection to the network.[5]*
4. Determine the lifecycle of corporate-provided mobile devices including procurement, upgrading, replacement, retirement and device destruction along with user costs / consequences for damage and misuse.
5. Define allowed and restricted activities, applications and data on all devices connecting to corporate resources.
6. Define what data on personal devices is owned by the company and will be deleted upon termination as well as any data that will be protected or preserved for personal users.
7. Create and enforce audits of all mobile devices for compliance checks.
8. Define and enforce disciplinary action for non-compliance with the policy.

Once a mobile device and use policy has been defined, it must be supported and enforced by all levels of management. The exceptions to the rules are more often than not the cause of service interruptions because of non-compliance.

For a truly effective mobile program, resources and time should be set aside to train the staff on proper security behaviors and business expectations. Simply getting a signature on the last page of any policy can mean very little in terms of actual understanding and ability and agreement to comply with its contents. As John Iatonna, vice president of information security at global PR firm Edelman states, "'It's a balance of privacy versus the company's security. People are very unaware of the risks that are posed with the smartphones right now,' including hacking, data capture and other security threats with smartphones. Users are typically not thinking about those kinds of risks when they use the devices."[6]

[4] (Basso & Redman, 2011)

[5] *Regarding point three, even if a decision is made to ignore BYOD and disallow personal devices, a plan still needs to be implemented to block connections from these devices.

[6] (Weiss, 2012)

IT managers need to arm themselves with steadfast arguments for investing in MDM technology as a strategy in the best interest of protecting the company. Michael Finneran analyzed a 2011 survey by *InformationWeek* and outlined the main perceived threats to corporate security:

> *The most-cited concern in our survey (at 64%) is that sensitive info will be on a device that is lost, stolen, or in the possession of someone who leaves the company. But mobile security goes beyond that. At No.2 is an infected personal device connecting to the corporate network (59%) followed by malicious apps downloaded by a user (37%) and theft of data via uploading to a personal device (36%).*[7]

Here is the quandary many IT departments currently face – providing services to enable business productivity without proper risk mitigation or behavior management on the user side. User behavior and connections must be managed to prevent the transfer of malware or illegal files to the corporate network or the wayward transfer of corporate data to personal devices. There have been scenarios where entire server infrastructures have been seized for criminal investigations due to the presence of illicit content from one user and entire email networks have crashed thanks to malware transfer from a rogue user device. Such situations can cripple a company and have severe impacts on productivity, customers and inflict hefty financial ramifications. Better to put safeguards in place than deal with the aftermath of these fiascos.

Mobile Device Management is becoming a significant function in IT departments, even if it is not yet well-developed in all IT settings. While reliance on Blackberry devices and eventually BES fades, other vendors have entered the market space and offer mobile device management applications for multiple-device environments. Impacts on the existing infrastructure usually translate to adding at least one dedicated MDM server to the environment, much like the BES solution. Finneran suggests environments that adopt BYOD practices can use funds from the individual device procurement savings to purchase MDM applications and equipment.[8]

Cost savings should also be realized as mobile devices are managed through an MDM application. Support requests for individual attention to device configuration should diminish. MDM applications will allow automation of initial mobile device configuration reducing support time from hands-on configuration to a few setup screens within the application. More robust packages should also be able to run automated health checks on devices and provide security assurance. Support of the multitude of different devices will also likely be handled by the app and major differences and slight nuances between all of these smartphones becomes less of a Google learning experience by the IT support staff.

Despite its recently former place as the number one provider in the smartphone marketplace, Apple does not provide MDM applications directly for enterprise as RIM does. Google does have a rudimentary MDM solution for true beginners or small businesses through Google Apps.[9] However, these technology giants (Apple in particular) have improved security on their devices and allow them to be managed by

[7] (Finneran, 2011)
[8] (Finneran, 2011)
[9] (Bradshaw, 2012)

third-party MDM applications with very similar tools and utilities to BES.[10] In fact, the marketplace for MDM solutions is growing and offering support for multiple mobile OS platforms, diverse levels of corporate mobile policies and infrastructure fits all within single products.

In 2011 Gartner released research on the top 23 MDM applications along with its criteria for viable solutions. Its key recommendations focus on three scenarios and are interpreted by David Strom of *ReadWriteWeb* below:

1. *Choose vendors that support a lightweight management approach, with mobile agents and server-side platforms, when your security and management requirements are limited and deep control is not accepted by employees using personal devices. Examples include Zenprise, MobileIron, BoxTone, Fiberlink and AirWatch.*

2. *Choose vendors that support a heavyweight approach to deliver secure and manageable corporate email to consumer and personal devices when strict security and compliance requirements apply. Containers can enforce stronger separation among personal and corporate content. Examples include Good Technology, Excitor and Sybase.*

3. *Users of iOS need to reset their devices for encryption -- the data protection mechanism in iOS 4 implements total device encryption, and can be triggered by setting a password to connect to Exchange Active Sync for email, calendar and contacts -- and then resynch the data.*[11]

While there are a few vendor frontrunners, there is a wide enough field to cover the variety of business sizes and models looking for MDM solutions. Many implementations are on-premise with dedicated servers, but as the world turns to cloud solutions and smaller businesses look to leverage functionality with costs, MDM vendors are out of the gate early with hosted and SaaS options and per-user subscription plans.

Alongside smartphones, tablets are infiltrating network environments. Gartner expects "that 80% of organizations will have tablets by 2013."[12] Kimber Spradlin of IBM echoes this prediction, "'You've got a platform to do legitimate work on, really it's more than just e-mail,' Spradlin said about tablets. 'But, it's a very immature market with a wide range of products. [However] in 2013 you will see a high adoption rate among medium-sized companies.'"[13]

Management of these devices should fall under the adopted MDM application. The main difference between tablets and smartphones is the use of productivity applications and data access. Employees use smartphones primarily for email (although productivity apps do exist for these devices), while the main

[10] (Apple, Inc., 2012)
[11] (Strom, 2011)
[12] (Basso & Redman, 2011)
[13] (Pierce, 2012)

purpose for tablets is to mimic to some degree a desktop experience and leverage the ability to run applications outside of the office on an easily portable device.

Unlike the Blackberry landscape where mobile device management arrived via RIM with specific corporate-minded use before the explosion of other smartphone platforms, there is no specific corporate-tailored tablet on the market. In a reversal of smartphone origins, tablets were initially designed and adopted for personal use and are finding ways to adapt to business productivity. Cisco was attempting to provide a tablet suited specifically for enterprise, but plans for the Cius product line were scrapped in May 2012 due to the BYOD trend. Specifically, iPad users beat Cius to the workplace and corporations adopted BYOD for tablets before Cius had an opportunity to infiltrate the market.[14]

There is no reason tablets should not be managed under the same BYOD policies in place for smartphones, however, specific tailoring for tablets will be needed. Consider the iPad which has no document file system. Aside from media files saved on the tablet (photos, videos and music) and attachments accessible through the email application, files to be accessed on the iPad must be saved to some external location which is generally somewhere on the public cloud – the Apple cloud or Dropbox for example. These are locations outside of the realm of the enterprise network and policies for corporate data stored on these platforms must exist. Should the files be held in the cloud only for the duration of a presentation or project? Should these cloud user accounts be required to be registered to the company instead of the user?

As with most systems and functions within the IT environment, mobile device management has its own complexities, risks and benefits which can be handled through proper application of security management. The adoption of BYOD policies brings a new challenge of managing proprietary data and access on non-proprietary equipment. The nature of mobile devices provides great opportunity for productivity while exposing business to genuine risk without the right protective architecture and policies in place. With the implementation of an MDM application solution and a well-defined and enforced security policy, IT units can help businesses mitigate the risks and take advantage of the benefits from this rapidly developing and expanding movement.

[14] (The Var Guy, 2012)

Works Consulted

Apple, Inc. (2012, March 26). *Deploying iPhone and iPad: Mobile Device Management.* Retrieved from www.apple.com: http://images.apple.com/ipad/business/docs/iOS_MDM_Mar12.pdf

Basso, M., & Redman, P. (2011, July 29). *Critical Capabilities for Mobile Device Management*. Retrieved from www.gartner.com: http://www.gartner.com/technology/reprints.do?id=1-16U0UOL&ct=110801&st=sg

Bradshaw, J. (2012, May 1). *Manage mobile devices with Google Apps*. Retrieved from www.techrepublic.com: http://www.techrepublic.com/blog/tablets/manage-mobile-devices-with-google-apps/1306

Brewster, E., Griffiths, R., Lawes, A., & Sansbury, J. (2010). *IT Service Management: A Guide for ITIL V3 Foundation Exam Candidates.* BCS.

Finneran, M. (2011, May 7). *BYOD Requires Mobile Device Management*. Retrieved from www.informationweek.com: http://www.informationweek.com/news/mobility/business/229402912

Kaplan, J. (2012, May 15). *A Reason for RIM: Why we still need Blackberry*. Retrieved from www.foxnews.com: http://www.foxnews.com/scitech/2012/05/15/reason-for-rim-why-still-need-blackberry/

Larson, I., Mani, R., & Smith, M. (2012, March - June). IT Service Management class lectures. *MIS 798* .

Pierce, C. (2012, February 21). *IBM: Enterprise mobile device management key with tablet growth*. Retrieved from www.opinno.com: http://www.opinno.com/enterprise-mobile-device-management-key-with-tablet-growth7663/

PRWeb. (2012, May 30). *Is Google Apps the Most Secure Public Cloud with New ISO 27001 Certification?* Retrieved from www.prweb.com: http://www.prweb.com/releases/2012/5/prweb9552237.htm

Strom, D. (2011, August 9). *New Gartner Report on 13 Mobile Device Management Vendors*. Retrieved from www.readwriteweb.com: http://www.readwriteweb.com/mobile/2011/08/new-gartner-report-on-13-mobil.php

The Var Guy. (2012, May 25). *Cisco Kills Cius Tablet Running Google Android; BYOD Wins*. Retrieved from www.thevarguy.com: http://www.thevarguy.com/2012/05/25/cisco-kills-cius-tablet-running-google-android-byod-wins/

Weiss, T. R. (2012, 30 May). *Mobile Device Management: Getting Started*. Retrieved from ComputerWorld.com: http://www.computerworld.com/s/article/9227346/Mobile_device_management_Getting_started?taxonomyId=15&pageNumber=1