Mobile Device Management (MDM) in Organizations

By

Diksha Barthwal

June 2016

Abstract

In the last decade, mobile and portable devices have gained popularity in a rapid pace. Smartphone and hand held devices are part of our daily life, be it work related need or personal use. This resulted in many challenges for organizations, such as the new technology like Bring you own device (BYOD), Enterprise mobility and Consumer technology (Jones, 2014). IT managers are looking for security measures to ensure productivity and efficiency in their organizations. Many solutions are developed to provide services for mobile IT in organizations and mobile device management (MDM) is one of software system available. The report, focuses on finding out the important factors that may drive the adoption of MDM in organizations. For this purpose, extensive literature review is conducted for drawing out useful findings which may suggest the current situation of MDM adoption in organization. The report concluded with the finding that organizational size and BYOD culture are important factors for the adoption of MDM.

Keywords: Mobile Device Management, MDM, MAM, BYOD, Mobile Security.

Table of Contents

Introduction

Nowadays, technology is becoming more prevalent in our daily lives, mainly due to the ubiquity of mobile and portable devices that are being deployed in many different areas such as education, businesses, healthcare and entertainment (Chircop, Colombo, & Pace, 2016). Moreover, in the last decade mobile and portable devices have become the backbone of any organization's business strategy. Due to the easiness and availability of resources like mobile devices, internet and wi-fi (Burke & Mouton, 2013) . Mobile device management (MDM) helps organizations to deploy, secure, monitor, integrate and manage mobile devices like, smartphones, laptops, tablets. The MDM provides many services like remote device administration and configuration, inventory and asset management, installation and updates on operating system and application level and cost management (Ortbach, Brockmann, & Stieglitz, 2014).

Firstly, the report discusses about the methodology used to conduct the research followed by the extensive literature review. Next, the discussion of findings and results from literature review would be done by drawing out the strong statements. Finally, the report finishes with the conclusion and recommendations for the future.

Methodology

In this section, the author discusses about the methodology used to conduct the research and how the data is collected and analyzed to draw the useful results. The scope of this research is restricted and could not go further to carry out research data collection methods like qualitative interviews and quantitative surveys. The methodology used in this research is qualitative research methodology and the data is collected through critically reviewing the peer reviewed journal articles. The papers reviewed are mostly publicly accessible data and no attempt to purchase a paid copy for our research has been made due to the limitation of research scope.

Data is analyzed, by within-study literature analysis where every component of research paper, like title, literature review, theoretical framework, results/ findings, discussion and conclusion everything is critically analyzed. It doesn't only involves analyzing the finding of the research but rather involves analyzing complete paper optimally.

Literature Review

The rapid growth of mobile devices and use of mobile apps, have been a great influence on businesses (Ortbach et al., 2014). The survey done by Accenture in 2012 reveals, 20 percent of the smartphone or mobile usage is for work related purpose (Mohr, Lalloz, & O'Brien, 2012). Its apparent, that the services provided by these kind of devices has advanced in a level that people started using them professionally and employers are more likely to leverage their advantages in organizations. Besides, new trends like BYOD and IT consumerization acting as an additional challenge for organization managing their business using mobile IT (Weiß & Leimeister, 2014). These trends offer new prospects for organizations to gain competitive advantages like cost savings in IT infrastructure or increasing efficiency by satisfied employees (Stieglitz &

Brockmann, 2012). However, organizations also facing challenges like security concerns about information being leaked whenever a business device is stolen or lost (Rhee, Jeon, & Won, 2012).

One possible solution suggested by software developers are mobile device management (MDM) system (TheEnterpriseMobilityFoundation, 2011). Mobile device management software enable IT organizations to maintain, control, automate management and reduce risks, while providing consumer mobility to the employees (Redman, 2013).

Mobile devices in organizations

Recently, the use of mobile devices and smartphones has been increased rapidly. According to the Forrester Research, mobile is the new face of engagement and by 2016, mobile devices and tablets will place power in the pockets of a billion worldwide buyers (Schadler & McCarthy, 2012). In 2007, the introduction of Apple iPhone has initiated the concept of mobile apps and unfolded the new prospects for the use of mobile devices. There are several studies done in the field of mobile devices and apps security concerns and also the development of mobile apps. Moreover, few researches are specifically done to assess the mobile technology for business purpose (Majdi, Janssen, Pei-Breivold, & Johansson, 2013). Overall, mobile devices especially smartphones have already dominated the business environment as well as personal life, resulting in lot of challenges and opportunities for businesses and their users (Ortbach et al., 2014). Organizations need to work on a mobile strategy to meet the need and demand of their business and employees. Managing mobile devices and mobile IT is a complex task for an organization and need a specific software program and new IT management strategies. Mobile Device Management (MDM) software are assisting IT departments to resolve the issues related to mobile IT and enabling them to manage mobile devices, mobile apps and impose compliance (Majdi et al., 2013).

What is Mobile Device Management (MDM)?

The challenges and problems stated in previous section shows that organizations are required to control the use of mobile device and applications. For ensuring a smooth service, enterprises need a software solution which can take care of the growing demand of use of mobile devices and smartphones in their business. To tackle these needs some companies are offering enterprise mobility management (EMM) solution, which include BYOD software, mobile application management (MAM) and Mobile Device Management (MDM) software (Redman, 2013). According to Gartner the leading MDM software providers in the market are AirWatch, MobileIron and Citrix (Redman, Girard, Cosgrove, & Basso, 2013).

Figure 1, illustrates how Mobile Device Management (MDM) architecture and operations.

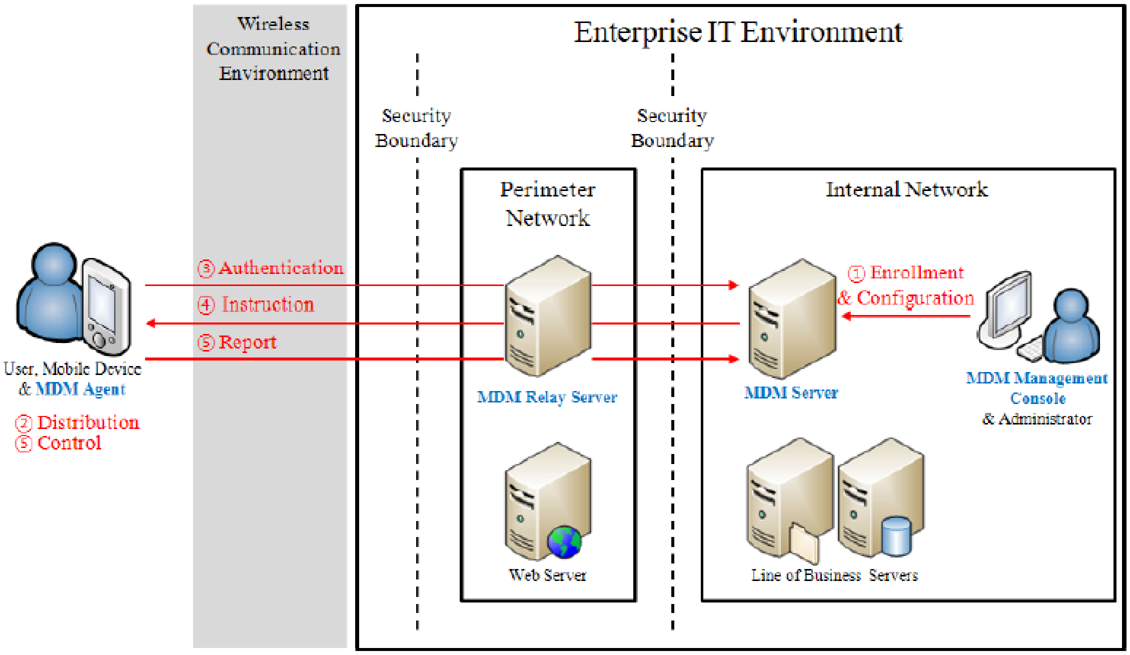

Figure 1: Typical Mobile Device Management (MDM) architecture (Rhee et al., 2012)

The basic operation steps for MDM architecture is described below:

Step 1. Enrollment/Configuration: In this step the user will register the data for their mobile device in the MDM system.

Step 2. Distribution: In this step the MDM agent will be distributed and installed in mobile device.

Step 3. Authentication: After the MDM agent is installed and run the data is sent to MDM server for authentication and matching if the data entered is correct.

Step 4. Instruction: The MDM server redirect the instruction to MDM agent in accordance with the status of mobile device.

Step 5. Control/Report: The MDM agent take care of the mobile device functionality as per the device control policy and sends the outcome back to the MDM server.

Step 4 and 5 will be repeated regularly as per the requirement during MDM operations.

After researching various literature, it is clear that MDM is the umbrella term including MAM functions (Finneran, 2011; Winthrop, 2011). It can be defined as "MDM supports centralized control of an entire fleet of mobile devices (smartphones and tablets) and mobile applications by applying and ensuring pre-defined configuration settings (Beimborn & Palitza, 2013)".

Benefits of MDM in organizations

Mobile device management MDM solutions are enabling organizations to efficiently carry out the work using mobile devices and helping them managing the all the mobile devices in their organizations. Some of the benefits of MDM solutions are stated below (Redman, 2013).

1. Easy updates of software in mobile devices automatically.
2. Administrator can manage and monitor the devices remotely.
3. MDM provides the facility to backup and restore the business data.
4. In case of lost and stolen devices, the facility to remotely disconnection and locking device to save the unauthorized access.
5. The provision of logging and reporting with password, access to enforce compliance.

Security threats of mobile device management MDM systems

With the increasing demand of new technology ideas like “Bring your own device” BYOD and mobile IT, security issues related to them becomes the most complex issue for any organization (Braunstein, 2012). There is threat of losing confidential information if any mobile device related to business has been lost or stolen. Although enterprises are adopting MDM systems to manage the data stored in the mobile devices used by employees (Rhee et al., 2012). However, it’s not necessarily confirmed that the MDM systems also provides security functions required for organizations. Below are some threats which can be important for identifying the security needs for MDM systems.

Table 1: Security threats related to MDM systems (Rhee et al., 2012)

Threats	**Description**
Disclosure	It is possible that confidential information saved in MDM system get leaked.
Software	Another possibility is modifying the operating system or application in MDM system by threat agent
Data	There is a possibility that it may change the data saved and transferred in MDM system without permission.
Malware	There are chances to infect the MDM system with malware.
Disaster	Threat agent can enable MDM system to act wrongly in case of natural disaster like floods and earthquake.

Summarizing, in literature, the main solution to managing the mobile devices in organizations are MDM systems (Beimborn & Palitza, 2013; Braunstein, 2012; Ortbach et al., 2014). However, there are very less study done to explore the factors behind adoption of MDM in organizations. This report focuses on analyzing the main factors responsible for adoption of MDM by organizations and it will be discussed in next section.

Discussion

In this section, the author discusses the main findings from the literature review and explore the factors why organizations are adopting MDM systems. After reading various good quality literature below are few factors which might drive the adoption of MDM in organizations.

Organization Size affecting adoption of MDM

The organizational context can be the significant factor for adopting Information Technology in businesses (Tornatzky & Fleischer, 1990). This generally means, the size of an organization is an important factor for driving the adoption of new technology. Various researches has identified the big organizations are more likely to adopt new technology because they have more resources while smaller organizations can’t make risky investments as they need to concentrate on their core business work, that is focusing towards gaining the organization profit (Chau & Tam, 1997). Precisely, it can be stated that the organization with large number of employees have potential to use more mobile devices than the organization with less number of employees. Furthermore, the large organizations are focused towards more structured processes, best security measures and control operations for their information technology management (Chau & Tam, 1997). Therefore, the big organizations are more likely to adopt Mobile Device Management for their business.

Bring your own device (BYOD) culture affecting adoption of MDM

Bring your own device (BYOD) is a concept use for allowing employees to use their personal devices like smartphones, tablets and laptops to finish their assigned work conveniently and with flexibility (Downer & Bhattacharya, 2016). Recent studies shows that about 70% of organizations have already adopted BYOD and experiencing benefits including more productivity, efficiency, employee satisfaction and low hardware cost (French, Guo, & Shim, 2014; Scarfo, 2012). Moreover, increased productivity and efficiency in organization through BYOD also resulting in need of managing mobile devices and IT managers may think to adopt

MDM systems (Ortbach et al., 2014). However, other argument is the organizations adopting BYOD, are usually less strict and have faith on their employees with loose business culture (Weiß & Leimeister, 2014). Hence, it's difficult to state that the BYOD will have favorable or unfavorable influence on MDM adoption.

Summarizing, the findings from literature review, it can be stated that the organizational factors such as "Bring Your Own Device" and firm size can be the most significant factors in driving the adoption of MDM in enterprises. The larger the organization, the more likely it is to adopt MDM systems. The big organization generally have very complex IT infrastructure and mobile access to the organizations application is required to manage centrally according to different user roles. For SMEs the risk of information loss is less because of fewer mobile devices and less number of user roles. Moreover, implementing the MDM solution is very complex process and takes lots of resources and efforts (Ortbach et al., 2014), therefore it would be less profitable for organizations using less number of mobile devices.

In context with the BYOD culture, the literature is not able to provide a clear picture of weather it has positive or negative impact on MDM adoption. However, it is possible that BYOD culture would have negative influence on MDM adoption because the organizations going with BYOD culture are allowing their employees full freedom to use their private devices for work purpose and implementing MDM might restrict and put harder control over the use of BYOD. Which in fact might contradict with their decision of adopting BYOD culture. Therefore, the BYOD trend would more likely to shift towards more trust on their employees and needs less control.

Conclusions and Future Recommendations

In this report, the author discusses about the current mobile technology trends like BYOD and IT consumerization and how they are influencing the adoption of Mobile device management (MDM) in organizations. MDM is an emerging requirement for organization dealing with various mobile devices and due to the challenges facing with the use of mobile devices. The report illustrates the various factors that can influence the adoption of MDM in organization. First factor is organization size and second is BYOD culture. Organization size and firm size is a significant factor which may positively impact the adoption of MDM. Large organizations are more likely to adopt MDM because of more number of mobile devices and need of standard processes and security concerns, while smaller organizations are less likely to adopt MDM due to less profit margin. However, BYOD will act as a negative factor for influencing the adoption of MDM because of organization with BYOD culture are less strict towards control and trusting more on their employees. Therefore, MDM might restrict their way of operation and hinder their growth.

The report, didn’t discussed the limitations and security consideration of MDM in detail. There is need of more research in this context as it might also help organization deciding for adopting the MDM systems. Also the findings are based on just the literature review due to the limitation of the scope of the report, however a better technique such as interview with IT managers of companies in New Zealand can be adopted for better results.

References

Beimborn, D., & Palitza, M. (2013). Enterprise App Stores for Mobile Applications-Development of a Benefits Framework.

Braunstein, C. J. (2012). Mobile device management: DTIC Document.

Burke, I., & Mouton, F. (2013). *An Investigation of the Current State of Mobile Device Management Within South Africa.* Paper presented at the Proceedings of the 8th International Conference on Information Warfare and Security: ICIW 2013.

Chau, P. Y., & Tam, K. Y. (1997). Factors affecting the adoption of open systems: an exploratory study. *MIS quarterly*, 1-24.

Chircop, L., Colombo, C., & Pace, G. J. (2016). Device-Centric Monitoring for Mobile Device Management. *arXiv preprint arXiv:1603.08634*.

Downer, K., & Bhattacharya, M. (2016). BYOD Security: A New Business Challenge. *arXiv preprint arXiv:1601.01230*.

Finneran, M. (2011). BYOD requires Mobile Device Management *InformationWeek*.

French, A. M., Guo, C., & Shim, J. (2014). Current status, issues, and future of bring your own device (BYOD). *Communications of the Association for Information Systems, 35*(10), 191-197.

Jones, N. (2014). Top 10 mobile technologies and capabilities for 2015 and 2016. *Gartner Report*.

Majdi, E. B., Janssen, A., Pei-Breivold, H., & Johansson, N. (2013). *Evaluation of Mobile Device Management tools and analysing integration models for mobility enterprise.* (Master of Science), Umeå University.

Mohr, N., Lalloz, E., & O’Brien, D. (2012). Mobile web watch internet usage survey 2012 - Accenture [White Paper]. Retrieved from https://www.accenture.com/t20151123T001914__w__/ch-de/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Local/de-ch/PDF/Accenture-Mobile-Web-Watch-Internet-Usage-Survey-2012.pdf

Ortbach, K., Brockmann, T., & Stieglitz, S. (2014). Drivers for the adoption of mobile device management in organizations.

Redman, P. (2013). Critical capabilities for Mobile Device Management software (pp. 42).

Redman, P., Girard, J., Cosgrove, T., & Basso, M. (2013). Magic quadrant for mobile device management software.

Rhee, K., Jeon, W., & Won, D. (2012). Security requirements of a mobile device management system. *International Journal of Security and Its Applications*, *6*(2), 353-358.

Scarfo, A. (2012). *New security perspectives around BYOD.* Paper presented at the Broadband, Wireless Computing, Communication and Applications (BWCCA), 2012 Seventh International Conference on.

Schadler, T., & McCarthy, J. C. (2012). Mobile is the new face of engagement. *Retrieved from Forrester Research: http://cdn. blog-sap. com/innovation/files/2012/08/SAP_Mobile_Is_The_New_Face_Of_Engagement. pdf*.

Stieglitz, S., & Brockmann, T. (2012). Increasing Organizational Performance by Transforming into a Mobile Enterprise. *MIS Quarterly Executive*, *11*(4).

TheEnterpriseMobilityFoundation. (2011). Looking beyond Mobile Device Management to mobile application and Enterprise Mobility Management. Retrieved from http://blog-sap.com/innovation/files/2012/02/Looking-Beyond-Mobile_Device_Management_to_Mobile_Application_and_Enterprise_Mobility_Management.pdf

Tornatzky, L., & Fleischer, M. (1990). The process of technology innovation, Lexington, MA. *Lexington Books. Trott, P.(2001). The Role of Market Research in the Development of Discontinuous New Products. European Journal of Innovation Management, 4*, 117-125.

Weiß, F., & Leimeister, J. M. (2014). Why can't I use my iPhone at work & quest managing consumerization of IT at a multi-national organization. *Journal of Information Technology Teaching Cases*, *4*(1), 11-19.

Winthrop, P. (2011). Mobile Application Management vs. Mobile Device Management. *theemf. org*, 05-18.