DECISION SCIENCES INSTITUTE

Evaluation Criteria For Selecting Bring-Your-Own-Device (BYOD) Platform In An Enterprise

(Full Paper Submission)

Sarah C. Odilinye
Concordia University College of Alberta
codiliny@student.concordia.ab.ca

Sergey Butakov
Concordia University College of Alberta
sergey.butakov@concordia.ab.ca

Fatemeh Kazemeyni
Concordia University College of Alberta
fatemehk@ifi.uio.no

ABSTRACT

Some organizations now permit their employees to use personal devices to connect to the corporate network - Bring Your Own Device (BYOD). While BYOD may be seen as a facilitator, it also poses a variety of risks. To manage these devices and the risks they introduce to the enterprise infrastructure, many IT vendors have developed BYOD management solutions / platforms. This paper proposes a set of guidelines for selecting and evaluating what BYOD platform is best suited for an organization, considering information security risks such as malware propagation, theft and loss of devices, unauthorized access, data leakage etc.

KEYWORDS: BYOD, Consumerization of IT, Information Security Risks, BYOD risk mitigation.

INTRODUCTION

Mobile devices are pervading everyday life and are growing in popularity in the world today as the information age of data gathering and information sharing make these devices very important. According to the International Association for the Wireless Telecommunications Industry (CTIA) report released in 2011, there were more mobile devices in the United States than people. At the same time, mobile devices have become more and more powerful, often matching or exceeding traditional PC (personal computer) performance, app diversity and capabilities (Johnson K. 2012). Also, smartphones and tablets are increasingly used in the workplace as business tools and are being integrated into the daily business processes in organizations (Clarke J et al, 2012a; Hogben G. and Dekker M., 2010). These high-capability mobile devices and their apps have become foundational tools for today's workforce, and they are more complex in their operating systems, security, use cases and ownership than older generations of computing devices (Johnson K. 2012).

A paradigm - 'Consumerization of IT (CoIT) describes an era where new information technology (IT) emerges first in the consumer market and then spreads into corporate organizations. The emergence of consumer markets as the primary driver of information technology innovation has seen a major shift in the IT industry - from the traditional company-issued devices to employee-owned devices. This results in the Bring-Your-Own-Device (BYOD) trend (Gajar P. K et al, 2013; Anderson N., 2014).

BYOD is a term that refers to employees who bring their own computing devices (like tablets and smartphones) to the workplace and use those devices to access privileged company data/information, applications and infrastructure. These devices may be purchased by the employer, purchased by the employee, or both. BYOD means any device (with any operating system), with any ownership, used anywhere (remotely or otherwise) (Anderson N., 2014). For the purpose of this research, BYOD devices are limited to tablets, mobile- and smart- phones, PDAs (personal digital assistant) etc. but does not include desktop PCs and / or laptops etc.

As the business use of smartphones, tablets and other mobile devices is on the rise, there is a shift in how enterprise IT manages and controls these devices. Implementing Bring-Your-Own-Device (BYOD) program presents organizations with a number of security, policy, technical, and legal risks.

The focus of this research paper is to present the information security risks and mitigation strategies associated with implementing a BYOD program, and define evaluation criteria based on how the risks identified are mitigated or managed to provide a BYOD platform selection process. Using security guidelines and risk classification for mobile devices identified by National Institute of Standards and Technology (NIST) and Information Systems Audit and Control Association (ISACA), this paper reviews the information security risks and threats, risk assessment, matrix. This research also reviews suggested BYOD risk mitigating features that are necessary for the secure implementation.

Paper overview: the next section reviews literature related to this research; BYOD Risks and Risks Assessment section gives an overview of the risks associated with BYOD and provides a risk assessment for mobile devices; the BYOD Platform Evaluation Criteria section discusses suggested mitigating or must-have features for secure implementation and operation of a BYOD solution; Following is a case study that evaluates Samsung KNOX using the guidelines developed. Finally, Discussion and Conclusion wraps up the paper and suggests future research directions.

LITERATURE REVIEW

The European Network and Information Security Agency (ENISA) (Clarke J et al, 2012a) categorizes the risks to include those relating to costs, legal and regulatory issues as well as those relating to data/information security - confidentiality, integrity and availability. It goes further to enumerate the information security risk factors to include - unauthorized sharing of information on employee's devices and sharing of devices, unauthorized access and unmanaged devices, inadequate security controls in application-rich mobile devices, especially if employee-owned. In a follow up document titled 'CoIT Mitigation Strategies', ENISA (Clarke J et al, 2012b) proposes a three-part risk mitigation and control strategy namely device management, application management and user and data management. Recommendations include the use of end-to-end architecture mobile device management (MDM) suites, encryption technologies, network segmentation, virtualization technologies, integrated multi-technology data loss prevention etc (Clarke J et al, 2012b).

Also, Mylonas A. (2013) proposes a risk assessment method particularly suited for smartphones. His paper includes a discussion about smartphone as an asset and a generic impact valuation, a classification of smartphone threats and an abstract risk assessment method. Contrary to traditional risk assessment methods, which treat smartphones as a single entity, this method provides a fine-grained evaluation by dividing the device into four sub-assets - the device, the data, the connectivity and the applications.

Scarfo A. (2012) proposes two models to address security concerns related to BYOD. He suggests the *Access Control* approach based on the concept that the employees are at the centre and the device is just a part of the whole system. The idea here is based on a virtualization-oriented environment and that IT is focused on service delivery and can support various devices. He also introduces the concept of data boundaries that transcend traditional network boundaries where sensitive data should be protected. The *Device Control* approach, in contrast, has at its centre, the 'device' itself where full device control is required and supported by particular APIs (application programming interface) that allow strict control of new mobile devices.

Yang et al (2013) proposed a Risk Management Quintet (RMQ) model to understand the BYOD practice. The RMQ is comprises five components - adoption of technology, controls, liabilities, user perception and user behavior. The RMQ models the relationship between components and classifies them as either control-dependent, control-independent or feedback relationship. Using the RMQ model, a quantitative analysis of a given control mechanism can be done by examining its effects on the control-dependent and feedback relationships when such control is introduced.

While previous research papers have presented the security risks, suggested some mitigation strategies and proposed models for controlling BYOD devices in the organization, this research provides a comprehensive guideline for selecting what BYOD solution is best suited for an organization using a risk assessment to assign priority to risks.

BYOD: RISKS AND RISK ASSESSMENT

BYOD Risks

Prior to implementing a BYOD program in a given organization, there is the need to conduct a risk assessment to determine what risks are tolerable and what risks they would have zero tolerance for with respect to the organization's risk appetite, tolerance and capacity.
In the specific case of implementing a BYOD program, the risks to the organization are summed in Table 1.

BYOD Risk Assessment

The general steps in a risk assessment are as follows (Information Systems Audit and Control Association - ISACA's COBIT 5 for Risk 2013; Risk Assessment Matrix, MSU 2004):

1. Identify the most important (critical) processes and functions;
2. Identify threats most likely to impact the critical processes and functions identified in step 1;
3. Determine the vulnerability of critical functions and processes to those threats; and
4. Plan and prioritize deployment of human and physical resources in order to maintain continuous operation of critical functions and processes.

The determination of critical business functions and processes may vary from one organization or industry to another, for example, what is deemed a critical function for the financial industry may not have the same priority for, say, the education industry.

Table 1 - BYOD Risks

	THREAT/RISK	DESCRIPTION
1	Lack of physical control	Devices are typically out of the organization's locus of physical control and the mobile nature of the devices makes them susceptible to theft or loss .
2	Sensitive Data leakage / data loss	Mobile devices and their operating systems often offer the convenience of copying information, such as confidential emails and attachments, from the corporate network onto the mobile device. This increases the risk for sensitive data leak through side channel attacks.
3	Use of untrusted devices, networks, applications and content	Using BYOD devices on other networks, installing third-party applications and accessing untrusted content from less secure connections puts the device at risk of attack by malicious users, jailbreaking and the device may sometimes lack the root of trust features.
4	Malware propagation	Users may install malware or infected programs and this may penetrate the network.
5	Attacks on de-commissioned devices	When an employee leaves the organization without proper device deactivation.

In ISACA's COBIT 5 for Information Security (2012), four categories are defined based on device capabilities and a risk evaluation is done based on the four categories. Tables 2 and 3 present mobile categories and the risk evaluation for these categories respectively.

Table 2 - Mobile device classification and description

CATEGORY	DESCRIPTION
1	Traditional cell phones - basic call and messaging services, no data processing, very limited data storage.
2	Early pocket PC devices, PDAs - enhanced graphics, data processing and limited storage.
3	Smartphones, Tablets - data storage and processing, transmission capabilities via alternative channels, broadband Internet connectivity
4	Newer smartphones and mobile devices with extended functions such as remote management of home intruder alert systems, wearable medical monitoring gadget that interface with the smartphone.

Tables 2 and 3 (COBIT 5 for Risk, ISACA, 2013) show a categorization of mobile devices and the risk levels associated with the devices in each category. Most BYOD devices fall under categories 2, 3 and 4.

From the tables 2 and 3, it can be deduced that information security risks increase with increasing functionality and complexity. In comparison, category 1 devices shows lower security risk while the categories 2, 3 and 4 devices, which are easily adaptable for business use, show higher security risk for theft, sensitive data leak, unauthorized data access and transmission.

Table 3 - Risk Evaluation for mobile devices

	RISKS	CAT. 1	CAT. 2	CAT. 3	CAT. 4
1	Theft	Low	Med.	High	High
2	Damage	High	High	Low	Low
3	Sensitive Data Leak	Low	High	High	High
4	Impersonation (Unauthorized Access)	Low	Med.	High	High
5	Unsafe Data Transmission	Low	High	Med.	High

BYOD PLATFORM SELECTION / EVALUATION CRITERIA

BYOD Risk Mitigation features

With the risk assessment completed, the risks are prioritized and the organization's IT is equipped with the knowledge of what features should not be compromised when selecting a BYOD platform.

Based on ISACA's *Securing Mobile Devices Using COBIT 5 for Information Security* and National Institute of Standards and Technology's (NIST) *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, the risks and threats are placed in five (5) broad categories namely;

1. Physical Control and Device Monitoring

The portable nature of mobile devices coupled with the fact that these devices are not under the direct control of the organization makes it even more susceptible to theft, loss and loss of sensitive data. Also, it may not be possible for the organization to fully secure these employee-owned devices physically.

Mitigating Feature(s) in BYOD solution:
- Remote lock and wipe capabilities in the case of lost or stolen devices.
- Selective data wipe to erase corporate data only (Souppaya M. and Scarfone K., 2012).

2. Unauthorized Network Connectivity

Many BYOD devices such as smartphones and tablets primarily connect to external networks - for example, mobile service provider networks, Wi-Fi, WiMax, Bluetooth etc. for internet access. These external networks cannot be trusted and pose a risk as they may be susceptible to eavesdropping by malicious users and, man-in-the-middle attacks.

Mitigating Feature(s) in BYOD solution:
- Functionality for managing wireless networks (COBIT 5 for Information Security, ISACA, 2012).

3. User and Device Impersonation

In the event of theft and/or loss of device, the risk of malicious users and unmanaged devices accessing corporate data on the device increases. Also, the device may be at risk of jail-breaking and rooting which makes the device elude security restrictions placed on the device.

Mitigating Feature(s) in BYOD solution:
- Robust authentication mechanisms such as token-based, network-based device or domain authentication used in conjunction with built-in device authentication such as passwords, PIN etc. (COBIT 5 for Information Security, ISACA, 2012; Souppaya M. and Scarfone K., 2012; Yang et al, 2013)

4. Sensitive Data Leakage/Loss

The risk of sensitive data leakage/loss is increased considerably as BYOD devices connect to the organization's network and may store a large amount of sensitive confidential information. Sensitive data leakage may be as a result of unintentional data disclosure by the user or malicious attacks. Also, data-in-transit is susceptible to attack and/or eavesdropping and poses a risk especially if the channel for transmission such as Wi-Fi, Bluetooth etc are unsafe and not under the control of the organization. At rest, data is vulnerable to attack or leakage if it is stored in plaintext or replicated in storage without encryption.

Mitigating Feature(s) in BYOD solution:
- On Device encryption (Souppaya M. and Scarfone K., 2012).
- Strong encryption algorithms (such as AES) for data -at-rest or -in-transit(Milligan P. and Hutcheson D., 2008)).
- Encryption of data as well as certificates and tokens (COBIT 5 for Information Security, ISACA, 2012); Gajar P. K et al, 2013)
- Virtual Private Networks (VPNs) (Milligan P. and Hutcheson D. 2008); (Yang et al, 2013).
- Application containers to separate user applications and data from corporate ones (Souppaya M. and Scarfone K., 2012).
- End device virtualization (Milligan P. and Hutcheson D.,2008).

5. Use of Untrusted Applications and Content

Installation of unverified or third-party applications such as banking apps which could be impersonated (as in phishing) to gain access to user data and authentication credentials poses a risk. Also, accessing certain websites may expose the device to malware which may be propagated through the corporate network if proper security precautions are not in place.

Mitigating Feature(s) in BYOD solution:
- Secure application container/sandbox
-Functionality that prevents unsigned applications from booting during start-up
- App Store for trusted apps only or white-listing and/or blacklisting applications
(Souppaya M. and Scarfone K., 2012).

Guidelines for BYOD Platform Selection

ISACA's COBIT 5-based audit and assurance program for BYOD (COBIT 5 for Assurance, ISACA, 2013) recommends that after a careful risk analysis and assessment has been developed, the goals of the service - in this instance, BYOD, and its corresponding service metrics should be understood before sourcing and implementing the service. Consequently, a set of selection guidelines is developed to enable a comprehensive assessment of BYOD platforms.Table 4 is a template of the guidelines for selecting a BYOD program.

Table 4 - Guidelines for BYOD Program Selection Template

Guidelines for Selecting BYOD Platform

	THREAT/RISK	DESCRIPTION AND SUBCATEGORIES	MITIGATING BYOD FEATURE	TICK (√)	RMKS
1	Physical Control and Device Monitoring	Theft and Loss of device	Remote lock and wipe capabilities	□	
		Attack on decommissioned devices	Selective data wipe (where necessary)	□	
2	Unauthorized Network Connectivity	Use of untrusted networks such as Bluetooth, cellular networks, Wi-Fi	Functionality for managing wireless connections	□	
3	User & Device Impersonation	Use of untrusted devices	Robust authentication mechanisms such as token-based, network-based device or domain authentication used in conjunction with built-in device authentication such as passwords, PIN etc.	□	
		Malicious users gaining access to device			
4	Sensitive Data Leakage	Unintentional data leakage by user	Encryption of data as well as certificates and tokens	□	
		Malicious attack on data stored on device	Virtual Private Networks (VPNs)	□	
		Unauthorized access to data	Application containers to separate user applications and data from corporate ones	□	
			End device virtualization	□	
			On-Device Encryption	□	
		Unencrypted data -at-rest or -in-transit	Strong encryption algorithms (such as AES) for data -at-rest or -in-transit.	□	
5	Untrusted Applications and Content	Installation of unverified third-party applications & Malware propagation	Secure application container/sandbox	□	
			Functionality that prevents unsigned applications from booting during start-up	□	
			App Store for trusted apps only or white-listing and/or blacklisting applications)	□	

Other Security Considerations

It is important to note that other generic security recommendations that are critical to the protection of data and information assets should not be undermined. They include:

- Creating, implementing and maintaining issue specific security policies with regards to the BYOD program.

- Installing software upgrades and patch management.
- Frequent backups and security audits; audit logs review.
- Ensuring compliance with security policy requirements including password length, complexity and expiration rules.
- Security education, training and awareness for users.

CASE STUDY: SAMSUNG KNOX

The Samsung KNOX™ is an Android-based BYOD management solution, developed by Samsung, that aims to provide data security on BYOD devices. Samsung KNOX incorporates National Security Agency's (NSA) patent technologies and uses hardware-level features to provide improved security for its operating system and applications. It also provides platform security with features such as Secure Boot, a functionality that prevents "unauthorized" apps from loading during the startup process; and Security Enhancement (SE) for Android that provides an improved system to enforce the partitioning of data based on confidentiality and integrity requirements. It incorporates a strong, flexible Mandatory Access Control (MAC) architecture into the major kernel subsystems and isolates applications and data. Samsung KNOX provides application security using the Samsung KNOX Container to provide a distinct Android environment within the mobile device, complete with its own home screen, applications, and widgets that can be used to separate corporate data from personal data (Samsung Electronics Co., 2013)

The guidelines developed in this paper have been used to evaluate Samsung KNOX. Table 5 is a test-case of Samsung KNOX. It shows how Samsung KNOX measures up against the expected security features and outlines what specific mitigating features KNOX offers. As can be seen from Table 5, the KNOX platform covers all areas of concern for BYOD. The guidelines proposed in this paper could also be used for comparative evaluation of two or more platforms.

DISCUSSION AND CONCLUSIONS

As new technologies emerge (such as BYOD), new threats and risks are also discovered. The ability to identify, assess and mitigate these risks to ensure that implementation of such technology does not pose a threat to information security requirements of confidentiality, integrity and availability is vital. It is important to note that there is no one-size-fits-all BYOD strategy available to all organizations. Although all the management components - governance, legal and regulatory and technical must be considered when developing a strategy, the exact mix of policies, controls and good practices adopted by each organization from within these elements will depend on that organization's business risk appetite, capability and tolerance.

This paper uses security guidelines and risk classification for mobile devices identified by National Institute of Standards and Technology (NIST) and Information System Audit and Control Association (ISACA) to review the information security risks and threats, risk assessment, matrix. This paper also reviews suggested BYOD mitigating features that are necessary for the secure implementation.

The result is a set of guidelines which are applicable to organizations intending to follow the BYOD trend and at the same time reduce, to the lowest possible, the risks that accompany BYOD implementation. These guidelines cover areas such as physical control and device monitoring, unauthorized network connectivity, user and device impersonation, sensitive data leakage, unsafe sensitive data storage and transmission as well as untrusted applications and content. Future work may include industry-specific guidelines and a more granular list of BYOD risk mitigating features.

Table 5 -*SAMSUNG KNOX Case-Study*

Guidelines for Selecting BYOD Platform

	THREAT/RISK	DESCRIPTION AND SUBCATEGORIES	MITIGATING BYOD FEATURE	TICK (√)	REMARKS
1	Physical Control and Device Monitoring	Theft and Loss of device	Remote lock and wipe capabilities	√	*Includes fully managed theft recovery solution.*
		Attack on decommissioned devices	Selective data wipe (where necessary)	√	
2	Unauthorized Network Connectivity	Use of untrusted networks such as Bluetooth, cellular networks, Wi-Fi	Functionality for managing wireless connections	√	
3	User & Device Impersonation	Use of untrusted devices	Robust authentication mechanisms such as token-based, network-based device or domain authentication used in conjunction with built-in device authentication such as passwords, PIN etc.	√	*Smart card authentication (Common Access Cards), Single Sign On (SSO)*
		Malicious users gaining access to device			
4	Sensitive Data Leakage	Unintentional data leakage by user	Encryption of data as well as certificates and tokens	√	*AES 256 bit,*
		Malicious attack on data stored on device	Virtual Private Networks (VPNs)	√	*Per-app VPN*
		Unauthorized access to data	Application containers to separate user applications and data from corporate ones.	√	*App containers*
			End device virtualization	√	*Containerization-ion*
			On-Device Encryption	√	*AES 256 bit,*
		Unencrypted data -at-rest or -in-transit	Strong encryption algorithms (such as AES) for data -at-rest or -in-transit	√	
5	Untrusted Applications and Content	Installation of unverified third-party applications & Malware propagation	Secure application container/sandbox	√	*Customizable Secure Boot*
			Functionality that prevents unsigned applications from booting during start-up	√	*App wrapping & app container*
			App Store for trusted apps only or white-listing and/or blacklisting applications)	√	*IT admin can define white-list or blacklist apps*

REFERENCES

An Overview of the Samsung KNOX platform, (2013) Samsung Electronics Co. Ltd, Gyeonggi-do, Korea.

Anderson N., (2014) 2014 Bring Your Own Device: Device Freedom Without Compromising the IT Network. Cisco Whitepaper. Retrieved from: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/byodwp.pdf , March 9

Clarke J. et al (2012a). Consumerization of IT: Top Risks and Opportunities, European Network and Information Security Agency (ENISA), 2012 - Technical Report.

Clarke J. et al (2012b). Consumerization of IT: Risk Mitigation Strategies, European Network and Information Security Agency (ENISA), - Technical Report.

COBIT 5 for Assurance, Information Systems Audit and Control Association (ISACA) (2013). Meadows, IL, pp. 283-318.

COBIT 5 for Risk, Information Systems Audit and Control Association (ISACA) (2013), Meadows, IL.

CTIA's (The Wireless Association) Semi-Annual Wireless Industry Survey Results December 1985 – December 2012 (2012) 2014. Retrieved from: http://files.ctia.org/pdf/CTIA_Survey_YE_2012_Graphics-FINAL.pdf, January 15.

Gajar P. K. et al (2013). Bring Your Own Device (BYOD): Security Risks and Mitigating Strategies, Journal of Global Research in Computer Science, vol.4, No. 4, pp 62 -70.

Hogben G. and Dekker M. (2010). Smartphones: Information security risks, opportunities and recommendations for users, European Network and Information Security Agency (ENISA).

Johnson, K. (2012) 2014. SANS Mobility/ BYOD Security Survey. Retrieved from: http://www.sans.org/reading_room/analysts_program/mobility-sec-survey.pdf January 15

Milligan P. M. and Hutcheson D. (2008). "Business Risks and Security Assessment for Mobile Devices", Information Systems Control Journal, vol. 1, ISACA.

Mylonas A. (2013) "Security and Privacy in Ubiquitous Computing: The Smartphone Model and Paradigm", Tech. Rep. Series: Athens University of Economics and Business, Dept. of Informatics Information Security & Critical Infrastructure Protection Research Laboratory.

Risk Assessment Matrix: Critical Incident Protocol, School of Criminal Justice, Michigan State University, USA, (2004).

Scarfo, A.(2012). "'New Security Perspectives around BYOD" in IEEE 7th International Conference on Broadband, Wireless Computing, Communication and Applications, pp 446 -451.

Securing Mobile Devices using COBIT5 for Information Security, Information Systems Audit and Control Association (ISACA) (2012), Meadows, IL.

Souppaya M. & Scarfone K. (2012) Guidelines for Managing the Security of Mobile Devices in the Enterprise, National Institute of Standards and Technologies (NIST) Special Publication 800-124 Rev. 1, US Dept. of Commerce, Gaithersburg, MD

Yang A. T., Vlas R., Yang A., Vlas C., (2013). Risk Management in the era of BYOD. IEEE Computer Society, pp. 411-416.