Analysis of Security Controls for BYOD (Bring your own Device)

Authors: David Rivera, Geethu George, Prathap Peter, Sahithya Muralidharan, Sumaya Khanum

Abstract:
This paper researches on the impact of Bring Your Own Devices (BYOD) to Organizational security. It examines the principal threats and control mechanisms covered in academic and industry literatures. The paper also identifies key areas where organizations can implement security controls in order to reduce BYOD related security threats. An analysis of the key risks and how existing control mechanisms address them is also conducted.

Keywords: BYOD, Security controls, NAC, MDM, MAM, Virtualization

Introduction:

Technological changes in recent years have led to a dramatic shift in the way organizational resources are accessed. Emergence of cloud computing and adoption of Bring Your Own Devices (BYOD) by organizations are predicted to bring in radical changes in the way an organization manages its IT security portfolio (Gartner 2013) . IBM defines BYOD as "*Employee's access to corporate information through their personally owned mobile devices*" (IBM 2012). Increased mobility, flexibility, productivity and employee satisfaction are considered as some of the key reasons for the adoption of BYOD (Kristine and Judith 2012). This environment works in favor of the organizations as well in cutting down the cost of procuring IT devices and helps avoid corporate equipment refresh cycle lags problem.

While there are considerable benefits, BYOD also introduces threats which might be beyond the scope of existing IT security control and measures. With organizational data being downloaded to user devices, BYOD expands the security perimeter of an organisation. A wide variety of mobile devices, lack of adequate security measures in these devices and the fact that the devices can often be shared increases the intensity of the issue. This triggers the urge to evaluate the validity of the existing security audits, controls and information management policies. In this paper, we review the current literature on BYOD, the potential security issues (threats), and the available control mechanisms.

Literature Review:

Consumerization refers to the trend of bringing technologies that developed in the consumer space to the Enterprise IT sector (Gartner, 2012). Consumerization of IT is poised to be an unstoppable trend and the pattern of employees preferring to access corporate resources through their own technology is gaining momentum. Adding fuel to this is an increasingly tech savvy workforce who in many cases owns more sophisticated devices than what an organization could offer (PWC 2012). Growth of this trend means BYOD devices will become organization's critical assets and protection of these devices is paramount(Brent 2012). Examination of literature on the various organizational considerations due to adoption of BYOD reflects similar notions many of which revolve around security aspect. Allowing wide variety of devices, ensuring endpoint security, protecting organizational data, preventing threats originating from user devices and enforcing company security policies have all become new dimensions with this emerging trend. (Cisco, 2012)

In 2006, only the mobile devices (laptops) that are owned by the employer were allowed to connect to corporate network/data with remote access. IT department's responsibility was to protect the data stored in the laptop and its connectivity to the corporate intranet through a robust VPN/firewall. By 2012, Most of the organisations are allowing variety of mobile devices owned by the employee/employer to connect to corporate network. These devices are embedded with all kinds of features which allow users to connect to wide variety of non-work activities (For e.g. social networking). Therefore, the responsibility of protecting the corporate data from potential risks and threats is now shared between the IT department and employees. This calls for user to draw a line between work and non-work activities (Dery and MacCormick 2012).

Threats to BYOD can be classified as direct threats like loss/theft of devices and indirect threats including interceptions of communication due to unsecured wireless network, malware attacks and location tracking (Markelj and Bernik 2012). On top of the list is the security issues associated with transmission and storage of organizational data. Memory capacity of mobile devices has scaled up significantly in the last decade and this enable vast amount of data to be downloaded. Potential accidental loss and deliberate employee theft puts at risk the most important organizational asset(Mahesh, Hooter et al. 2013)

BYOD introduces personal mobile devices which are subjected to malware attacks originating from compromised websites and illegitimate applications. While these devices have inherent security features, users often circumvent them motivated by factors like ease of use, ability to install unapproved software and migrating across carriers. The method referred to as 'jailbreak' disables the underlying security architecture thereby exposing the devices to constant security attacks (Lowell, Gail et al. 2013). Adding to the problem is the heterogeneity of the mobile platforms especially differences in the way underlying security controls are implemented making it extremely difficult for organizations to manage (Peter, Thomas et al. 2013).

Mobile device capabilities like tethering and Wi-Fi hotspots creates Rogue Access Points (RAP) which bypasses the corporate security controls to access content otherwise blocked by the organizational policies. This creates a backdoor for leaking corporate data making traditional security control mechanisms like firewalls ineffective (Mohamad and Haslina 2013).

Considering the growing list of threats due to adoption of BYOD, organizations need to reassess the effectiveness of their security framework across a broad range of factors including risks, controls, policies, organizational culture, and user awareness/training. Subsequent sections of this review focuses primarily on the security controls aspect. Security controls is defined as "*Management, operational and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity and availability of the system and its information*" (NIST, 2013). During our review we came across several security control mechanisms which could make BYOD effective.

Desktop / Application Virtualization

Virtualization refers to the separation of a resource or service from the underlying physical delivery (Vmware, 2006). Desktop and Application Virtualization can be used as an approach for delivering a secure and device independent access to organizational resources. When executed in a hosted mode, the applications run from the organizations data center delivering a continuous image to the users on their device. The delivery of services is implemented using a security broker that controls the access to the user based on their credentials; device used and related access policies. Commercially available virtualization products support strong user authentication by using tokens, certificates and smartcards. Once the user logs in, the session is completely encrypted using Secure Socket Layer (SSL) or equivalent thereby providing a secure environment.

The relevance of this approach increases with BYOD primarily due to the limited control organizations have over the security of end devices. Listed below are some of the key reasons which makes this process an efficient way to implement BYOD (Scarfo 2012)

- By managing the virtual applications and the data centrally, organizations have the capability to implement better security measures including data encryption, backups and intrusion detection.
- As the content is not stored locally in the devices, organizations has better control over its data. This also ensures protection in scenarios where devices get stolen.
- New generation virtualization solutions create local safe zones completely isolating critical process from other applications that are running in the same system thus increasing the overall security.
- Virtualization systems also implement control measures like denying copy and paste data between the virtual desktop and local folders and limiting the ability of users to print the content from the virtual session.
- Managing access to the users centrally allows earlier on-boarding and offloading of resources.

Network Access Control (NAC)

NAC allows organizations to identify user devices and apply security policies before granting access to the resources. It can function irrespective of type of device (mobile/PC/others) or the type of connection (wired/wireless). Devices attempting to connect to the network are assessed for a broad range of factors including the level of trust, type of user and user location before granting access. Combined with a host of capabilities listed below, NAC solutions could be used to implement BYOD in a controlled fashion (SANS, 2012).

- Device Fingerprinting – NAC can scan a network device and capture information on its response to various protocols allowing it to be compared against known device fingerprints. With BYOD bringing in a variety of devices and quite often multiple devices from the same user this become a much desirable feature.
- Better access control - NAC can be configured to specify what level of security features should be implemented in a device before allowing connection to the network. Thus, in addition to the authorizing the user, it also ensures the devices itself is compliant.
- Self and Auto remediation procedures can be used to resolve the policy violations in the user devices. The resolutions can be rolled out automatically with the consent of the user or by redirecting to a remediation site outside of the network thereby engaging the user to resolve the device issues.
- Guest networking functionality of NAC can be leveraged to provide access to visitors and contractors who use third party devices thus preventing them from direct access to the organizational network.
- NAC also gives the much required visibility over the users who are connected to the network including the ability to classify the devices and user profiles. It has inherent features to support exception reporting in scenarios of policy violations and unusual activity.

Even though NAC control access to organizational resources from third party devices, it cannot be a standalone solution for implementing BYOD. This is considering the limited control it has over data that the user can download to their devices which can be exposed to security threats when the same device gets used in a non-work environment. One way to limit this is by using desktop virtualization or strong security policies on the content that can be downloaded locally. Yet another option is to use NAC in conjunction with a Mobile Device Management solution (MDM) covered in the below section.

Mobile Device Management

MDM solutions can be used to comprehensively manage third party mobile devices using authentication mechanisms, data encryption and enforcing of organizational policies. The initial step in the process is to register the user and device in an MDM system following which an MDM agent gets installed on the user device. The agent has access to device information like IMEI number or MAC address which can be used while authenticating the device. Once the connection is established, the MDM server can send instruction to the agent to control the device including ability retrieve or remote wipe the contents. The agent can also control the functioning of the mobile device so as to ensure it is aligned to organizational policies and report back any exceptions to the MDM server (Keunwoo, Woongryul et al. 2012).

Access Control Mechanisms

Risk Aware Role Based Access Control (RBAC) sessions- The framework introduces risk as an additional parameter to the traditional RBAC mechanisms. Instead of operating on the basis of predefined access list for a particular role, the process relies on dynamically calculating the associated risk to allow/deny user requests. The computation of risk takes into account several factors including whether the user connects from within the organization or remotely. This methodology also requires a session risk threshold level that indicates the maximum amount of risk a session can hold to be established. This threshold is then used to limit the set of roles that a user can activate at a point it time. Even if a session gets compromised, the risk threshold will prevent the amount of damage that can happen. The research indicates this as a practical security risk mitigation control mechanism in BYOD scenarios (Zaman, Ram et al. 2012).

Traditional access control models use a static approach where in the user is either allowed or denied access. This model is found to be ineffective in the wake of IT consumerization and more specifically the emergence of BYOD. Literatures suggests emergence of a multi-tiered architectural model where in the level of access provided to the user is varies dynamically based on a calculated trust. The trust calculation factors in several factors including user identity, location of the user, type of user device, availability of security controls in the device and type of resource requested. To support same the underlying IT infrastructure should also divided in to security zones which compartmentalize the data and resource thereby making a clear division of what user can access with the calculated trust levels. The model also emphasize on need for a continuous monitoring to detect anomalies in the access pattern to prevent unauthorized access (Malcolm 2013).

Mobile Application Manager (MAM):

Mobile application manager is an identity based application policy which can be applied to protect the organisation based apps. This will help the organisation to protect the data even if the mobile device is lost, a theft or upon a termination of an employee. The manager generally downloads a form from the internet and asks to fill the unique details to the user before using the app. Thus the security is given to the data. A certain authorization details are to be filled before using the app every time which gives a remote security even when the device is accessed from different environment. This helps the organisation to track, access and secure the device used by the employees.

Enterprise Sandbox:

A common threat observed across literature on using smartphones to access organizational resource is the presence of malware. As a solution to this issue, studies suggest implementing compartmentalization within the mobile platform and controlling the information flow between the applications installed in the device. Even if one domain becomes affected by a malware it wouldn't have access to the data and resource from other domain thereby limiting the damage. By introducing information flow control the underlying services will be prompted to get user authorization before access data across domains. Implementing this model could thus enhance the security of the mobile devices (Ammar, Steffen et al. 2012)

Mobile Antivirus:

The malware like Trojan, virus may corrupt the entire device and sometimes the whole internal organisation system. Mobile antivirus can help to protect the device from malware and helps to ensure a normal functioning of a system.

Cloud Computing Management:

Strategies like BYOD do not appear just by themselves, in the case of BYOD, it came as a result of consumerization and growing. Cloud oriented trends (Scarfo 2012). Therefore, any organisation engaging BYOD will need into consideration Cloud oriented security controls. Edward (2013) presents an interesting model of a Mobility-Enabled Secure Cloud, based on the premise that Cloud oriented services provide a logical security perimeter as an isolated and highly controlled service. This model promotes the point of view that the required and feasible level of protection of a specific asset should be prioritized. Three security zones are presented in this model, the first consists of the user and all the device-specific security controls, the second is formed by the network and all the virtual protections introduced by the mobile carrier, and the third consisting in the cloud and all the possible protections the Cloud service vendor could provide. Considering the Cloud zone, the model suggests three strategies to secure the Cloud zone from the organisation side.(Edward 2013)

1. Securing the access to the cloud by introducing identity management techniques, including strong authentication. Multifactor authentication is desirable.
2. Distributing resources as pieces between multiple clouds, trying to reduce the isolated value of each piece. Therefore, if a cloud is compromised, the resources that this specific cloud hold will not have legible value until they are joined to other resources stored in another cloud or clouds. This will discourage attackers and also reduce the risk of denial-of-service attacks. Achieving this might be complex depending on the atomicity of the resources.
3. Defining cloud classes based on the different security and trust profiles a cloud service provider may enforce. This classification will help to distribute assets between distinct cloud providers considering the appropriate level of security required by this specific asset.

Additionally, information security at Cloud level is provided by the service vendor and it is defined in the form of SLAs. If there is any disagreement with any SLA, the waiver given by the provider usually does not cover the customer losses, especially when the implied SLA is security related. As response to this issue, waivers should be made according the type of business the customer runs, and a complete analysis of the security architecture the provider uses need to be done before storing sensible information at the cloud. Internet, database, server and application access along with data privacy are the main security aspects residing at the Cloud provider's architecture that should be studied before uploading any data. Data security at physical and network layer, investigation support and a highly trusted cryptography scheme are in general the main aspects to consider (Reddy, Ramakrishna et al. 2009).

Non-Technical Controls:

Along with the security controls required to be enforced to introduce BYOD into an organisation, another security aspects needs to be considered. (Thomson 2012)Literature states that security should not act as a barrier, and that introducing BYOD does not mean accepting all the risk involved. He also considers that data governance is an important aspect to take into account. Gatewood, B. (2012) adds that BYOD implementation requires an entire organisational support along with personnel training and education.

Thomson, G. (2012) uses Cisco's annual 'Connected World' study to illustrate the current trend on young IT professionals towards BYOD supporting organisations. This study states that 3 of ten young professionals admit that remote access availability influences in their decision to take a job or not, and that 71% of college students agrees that company-issued devices should not be only work oriented but also able to be used to play. To support this statement, Mansfield-Devine, S. (2012) interviewee considers that employees are more productive working with devices chosen by them. To summarize, BYOD can perform a critical role in an organisational IT hiring expectations.

When defining policies that would rule security controls, is important to define which data should be accessible (Thomson, G. 2012). In addition, Mansfield-Devine, S. (2012) interviewee states that employees must be part of the organization’s security model, and those policies should help them to understand the difference between using a device at work and using a device for work.

Methodology:

We developed an understanding on BYOD by conducting a literature review on Information Security journals and article published in leading industry portals. We further expanded our research on specific controls by referencing literature published in IEEE and MIS Quarterly Executive journals. This search criterion’s used were BYOD, Security Controls, NAC, MDM, MAM, Virtualization, Mobile Device Access Control etc. Similar search was conducted on Google Scholar to retrieve additional journals and conference publications.

Discussion:

There is considerable evidence across literature which suggests a new realm of security threats introduced by BYOD. Our analysis pointed us towards five different dimensions relating to security controls associated with BYOD.

- **Control Data** - By controlling data at source and/or using efficient delivery mechanisms to limit what employees can download to their devices.
- **Control Access –** Enhancing the existing access control methods to consider contextual factors like risk and trust levels.
- **Control Network**- Effectively managing the network by controlling and monitoring the third party devices that connects to its resources.
- **Manage devices** – Better management of user devices itself including better authentication, data handling and remote capabilities.
- **Create a supporting framework -** Non technical controls including policies, user awareness and training.

According to a recent survey conducted by KPMG, the top security concerns associated with BYOD were loss of data, unauthorized access to the organization assets, malware infections, lost/stolen devices and compliance with industry regulations. The following table shows a comparative analysis of how each control measures maps against these security concerns.

Table 1 Comparative analysis security threats against security controls

Controls	**Key Risks**				
	Data loss	Unauthorized access	Malware infection	Lost/stolen devices	Compliance
Desktop virtualization	√		√	√	√
NAC		√			√
MDM	√	√			√
MAM		√	√		√
Mobile Antivirus			√		√
Cloud computing	√				√

While individual controls can be effective in addressing specific aspects, none of them can operate in isolation to deliver a comprehensive security framework. The solution often lies in combining multiple security controls together. Factors like The choice of controls will vary depending on factors including nature of the organization, its risk appetite, level of IT security budget and compliance requirements. Organizations also need to periodically review their security controls and policies to ensure effectiveness with changing BYOD trends.

The additional investments which organizations will have to make, to implement these controls might reduce the net benefits and could also lead to additional security risks. However, aspects like employee satisfaction and productivity will contribute positively. Organizations must give due consideration to all these factors before joining the BYOD bandwagon.

There is lack of academic literature and research details available on the effectiveness of BYOD, related security threats and control mechanisms. This could be a potential area for future research.

Conclusion

This paper examines the existing literature relating to BYOD. It firstly analyses various threats introduced by BYOD and the potential impacts this could have on the security of organizational assets. The paper then focuses on a variety of control mechanisms that can be implemented to adopt BYOD securely. We also did a comparative analysis on how the existing control mechanisms will address the most common security threats. Our research concludes that a secure adoption of BYOD requires a combination of technical and nontechnical security controls to be established. To adapt to trend successfully, organizations need to be also aware of issues related to virtual and mobile world connectivity and rapidly changing technology.

References:

Ammar, A., S. Steffen, et al. (2012). Securing Smartphone Compartments: Approaches and Solutions. ISSE 2012 Securing Electronic Business Processes, Springer**:** 260-268.

Brent, G. (2012). "THE NUTS AND BOLTS OF MAKING BYOD WORK." Information Management Journal **46**(6): 26-30.

Casey, E. "Investigating sophisticated security breaches," *Communications of the ACM* (49:2) 2006, pp 48-55.

Cisco, 2012, “Bring Your Own Device (BYOD) Smart Solution Design Guide”, viewed 10th April 2013, http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/byoddg.html#wp427108

Dery, K. and J. MacCormick (2012). "Managing Mobile Technology: The Shift from Mobility to Connectivity." MIS Quarterly Executive **11**(4).

Edward, A. (2013). "From the enterprise perimeter to a mobility-enabled secure cloud." Security & Privacy, IEEE **11**(1): 23-31.

Gartner, 2012, “Gartner IT Glossary”, viewed 8th July 2013, <http://www.gartner.com/it-glossary/consumerization>

Keunwoo, R., J. Woongryul, et al. (2012). "Security requirements of a mobile device management system." International Journal of Security and Its Applications **6**(2): 353-358.

Lowell, M. J., P. A. Gail, et al. (2013). "Your Guide to Authenticating Mobile Devices." Journal of Corporate Accounting & Finance **24**(5): 51-68.

Mahesh, S. Hooter, et al. (2013). "Managing and Securing Business Networks in the Smartphone Era."

Malcolm, H. (2013). A New Security Architecture to Improve Business Agility. Managing Risk and Information Security, Springer**:** 87-102.

Markelj, B. and I. Bernik (2012). "Mobile Devices and Corporate Data security." INTERNATIONAL JOURNAL OF EDUCATION AND INFORMATION TECHNOLOGIES **6**(1).

Mohamad, N. M. and H. W. Haslina (2013). "Wireless Networks: Developments, Threats and Countermeasures." International Journal of Digital Information and Wireless Communications (IJDIWC) **3**(1): 119-134.

Neil Hawkins ,Steve Ware and Martin Hi. IBM Mobile Enterprise Services Team. Case Study: "Bring Your Own Device & Consumerisation of IT". IBM Client Technology Innovation Exchange Hursley, February 2012. IBM Corporation

NIST, 2013, "Glossary of Key Information Security Terms", Viewed 10th July 2013, http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Peter, T., Z. Thomas, et al. (2013). Mobile Device Encryption Systems. Security and Privacy Protection in Information Processing Systems, Springer**:** 203-216.

PWC, 2012, "Bring your own Device - Agility through Consistent Delivery", PWC, Viewed 10th July 2013, http://www.pwc.com/en_US/us/increasing-it-effectiveness/assets/byod-1-25-2012.pdf

Purser, S. "Why access control is difficult," *Computers & Security* (21:4) 2002, pp 303-309.

Reddy, K. B., P. V. Ramakrishna, et al. (2009). Cloud security issues. Services Computing, 2009. SCC'09. IEEE International Conference on, IEEE.

SANS, 2012, "Enabling Secure Personal and Mobile Device Use On Your Network" http://blog.forescout.com/landing-mobile-security/

Scarfo, A. (2012). New Security Perspectives around BYOD. Broadband, Wireless Computing, Communication and Applications (BWCCA), 2012 Seventh International Conference on.

Straub, D. W. "Effective IS security: An empirical study," *Information Systems Research* (1:3) 1990, pp 255-276.

Thomson, G. (2012). "BYOD: enabling the chaos." Network Security **2012**(2): 5-8.

Venter, H., and Eloff, J. H. "A taxonomy for information security technologies," *Computers & Security* (22:4) 2003, pp 299-307.

Vmware, 2006, “Virtualization Overview”, http://www.vmware.com/pdf/virtualization.pdf

White, D., and Rea, A. "Just Trying to Be Friendly : A Case Study in Social Engineering," *Journal of Information System Security & Privacy, IEEE* (4:2) 2008, p 30.

Zaman, B. K., K. Ram, et al. (2012). Risk-aware RBAC sessions. Information Systems Security, Springer**:** 59-74.

Zviran, M., and Haga, W. J. "Password security: an empirical study," *Journal of Management Information Systems* (15) 1999, pp 161-186.

Author/s:
Rivera, David;George, Geethu;Peter, Prathap;Muralidharan, Sahithya;Khanum, Sumaya

Title:
Analysis of security controls for BYOD (Bring Your Own Device)

Date:
2013

Citation:
Rivera, D., George, G., Peter, P., Muralidharan, S., & Khanum, S. (2013). Analysis of security controls for BYOD (Bring Your Own Device). Melbourne, The University of Melbourne.

Publication Status:
Unpublished

Persistent Link:
http://hdl.handle.net/11343/33338