ASA

Annie Searle & Associates LLC

Research Note

Organizational Risk of Bring Your Own Devices (BYOD)

Evan Cottingham

June 2017

Keywords: Bring-Your-Own Device; BYOD; Enterprise Security; Organizational Security; Cybersecurity; Sensitive Data; Organizational Risk

Abstract: This paper discusses the rapidly evolving, business-critical issue of "Bring Your Own Device" (BYOD) programs, and the considerations and risks applicable across organizations in all sectors. While the benefits of BYOD programs are clear, the associated risks are clearly documented as well, and must be taken into consideration by any organization considering implementing or with an existing BYOD program.

The enterprise Information Technology (IT) sector is amidst a revolution as individuals within the workforce have moved the sector in the direction by utilizing personally owned and valued technologies. This effort of the workforce population - in terms of IT – to essentially blur the lines between their home lives and work has been labeled the "consumerization of IT." The phrase "consumerization of IT" can be defined as the dissemination of information technologies that originate and emerge within the consumer market into the IT sector of business or government organizations. The driving force behind this consumerization are the workforce employees who are purchasing devices, downloading applications, and utilizing personal online services while integrating such technologies into the workplace environment and job duties.[1] Employees are increasingly recognizing the opportunities for greater individual productivity allowed by these consumer electronic products, and the market has followed, further accelerating this pattern.

The concept of "Bring Your Own Devices" (BYOD) offers a concrete illustration of the consumerization of IT movement. The core idea behind BYOD stems from consumerization, however refers specifically to the movement of consumer IT devices into organizational IT. Specifically BYOD can be defined as bringing their personally owned devices into the workplace and using these devices to connect to a company's network and access company data in order to complete their work related tasks.[2] Within the context of the consumerization of IT, BYOD has served as an initiative for organizations that wish to embrace the consumerization movement.

The growth of this movement within organizations is evidenced by the recent trend in BYOD adoption. To get a sense of the current state of BYOD adoption, Cass Information Systems Inc. conducted a study to assess the BYOD landscape within organizational IT going into 2016. In the "Cass BYOD and Mobility Study 2016," more than 200 telecommunications and IT professionals and managers were surveyed in the U.S. and Canada regarding BYOD adoption within their respective companies. Exemplifying the growing trend of BYOD use, 60 percent of those surveyed stated that the number of BYOD users within their organizations had increased from the previous year. The emergence of personal device use within the workplace is also evidenced by the 85 percent of respondents claiming that their organization contains at least some BYOD users, and the 36 percent stating that there are at least 1,000 BYOD users within their company.[3] Additionally, Gartner Inc. - an IT research and advising firm - offers insights into the future of BYOD incorporation within organizations through their own analysis of the consumerization trend. Most notably, Gartner estimates that by 2017, half of employers will require workers to utilize their personal devices for work purposes. Furthermore, Gartner predicts that by 2018, "70 percent of mobile professionals will conduct their work on personal smart devices."[4] This drastic growth trend is largely due to organizations buying into the promised benefits of permitting personal device use within the workplace. One such perceived benefit is increased employee productivity. This viewpoint asserts that allowing work to be conducted on a personal device promotes an employee's mobility during the workday. So long as a mobile device is able to connect to the company's network and access the necessary information, work related tasks can be completed away from the workplace. According to the Cisco Internet Business Solutions Group's "Financial Impact of BYOD" study, the average BYOD user in the U.S. saves 81 minutes per week at work.[5] In terms of employee efficiency, with consideration for the number of employees within an enterprise, this figure suggests a significant amount of saved time company-wide that can be focused towards other tasks or projects.

Employees have also indicated that BYOD use improves overall satisfaction. BYOD gives employees the flexibility to work on devices with which they are comfortable and familiar. It effectively eliminates the burden of being forced to learn to work with company-issued IT devices. Additionally, Samsung reports that 78 percent of employees believe that because BYOD promotes the use of a single mobile device for data access, it effectively enables an improved balance between their work and personal lives.[6] Furthermore, by eliminating the need for company-issued devices, BYOD offers costs savings and reduces IT spending on hardware purchasing, as the responsibility shifts to the employee. Similarly, repair or replacement costs become employee responsibilities as well.

Establishing a program to allow personal device use within the workplace promises an overall improvement to productivity and profitability to organizations. However, there are major security tradeoffs that must be considered. The push towards tapping into the consumer IT market through BYOD adoption is a departure from the traditional centralized IT department - personally owned consumer devices are replacing the use of company sanctioned and distributed devices. This places BYOD devices into the category of "Shadow IT" - a term used to encompass "hardware or software within an enterprise that is not supported by the organization's central IT department."[7] This lack of centralized IT support implies the overall lack of control, management, or visibility of organizations over such technologies. Re-contextualizing BYOD devices as a form of Shadow IT, such devices should not only be viewed as opportunities for profit or a competitive advantage, but also as enterprise security risks as well.

As of October 2014, according to a survey of IT executives conducted by cyber security software provider Check Point, costs of incidents attributed to personal mobile devices at work have cost organizations over $250,0000.[8] Considering this potential for significant financial loss due to insecure BYOD devices, it is imperative that organizations are aware of the risks of personal device use within the workplace. With this awareness, companies could then make informed decisions with consideration for these risks when developing their own BYOD program or policy.

The security risks associated with BYOD devices, in general, stem from the absence of organizational IT support and the lack of control that this implies. This is evident in the difficulty to track BYOD devices within an organization. Because such devices are owned by the employee and not the company, they are not included in an organization wide inventory or asset management system. In terms of security, utilizing an asset management system is a necessity simply because "you cannot secure what you do not know exists."[9] With this exclusion from an asset management system, BYOD devices may operate, handle data, or communicate over the enterprise network unbeknownst to the organization.

According to the "2014 Information Security Guide" developed by Confluence, the collaboration software branch of software company Atlassian, an asset management system provides a company with insight into what they have, where it is, who owns it, who maintains it, and its importance to the institution.[10] However, for BYOD devices such insights are often unavailable. Establishing ownership and location of a device within the company allows for the attribution of a role or responsibility to the device. This in turn allows the company to determine the criticality of the tasks it is used to complete, the data or information it handles, and therefore, the device itself. This may include information such as which operating system the device is running. If such system information is not collected, it is impossible for an enterprise to assess a BYOD device's alignment with their IT standards and consequently hinders the organization's ability to accurately assess its overall security posture.

Another security risk lies in the lack of BYOD device monitoring that exists within companies. A BYOD device brought within a workplace to access its data and do work, because it is a consumer product not owned by the company, is not initially configured by policy to report to a centralized IT monitoring system. This leaves a company's systems administrator blind to information such as the resources being used on the device, processes that are being run, programs or commands that are being executed, or who may be logged onto the device.[11] Lack of visibility for such information poses a significant security risk. This is because examining processes or executed applications/commands is an effective method of determining the presences of malicious software (malware) on the device. Due to this lack of reporting and monitoring, activity on a BYOD device within an enterprise is obscured. Therefore, it is possible that potential malicious processes or programs could execute and run on a device continuously without detection.

With the lack of visibility into BYOD devices, this leads to the risk of non-compliance. Without centralized IT support and monitoring, it is difficult to ensure that an employee's personally owned device that is brought into the workplace is compliant to the company's established IT standards or policies. This includes regulations imposed upon the security measures implemented on a device. This also includes ensuring that the operating system is up to date, any vulnerabilities are patched, and that the device has a company approved antivirus software installed on it. Furthermore, because these are personal devices, the employees themselves are solely responsible for taking these steps and doing their due diligence in these areas. The actions that employees take regarding the security of their own devices are not necessarily regulated by the company. Without the proper security measures in place, BYOD devices can become vulnerabilities in the enterprise environment.

Security is especially of concern as BYOD devices have access to a company's network and process or store business data in order for the completion of tasks. A vulnerable device with outdated security controls in the work environment puts this data at risk for exfiltration in a variety of ways. Through web browsing or downloading malicious applications, a user may install malware that may plant a backdoor - "a technique in which a system security mechanism is bypassed undetectably to access a computer or its data"[12] - onto the device, giving a malicious actor access to the business data that may be stored on the device. Similarly, a compromised device could be brought into the work environment and serve as a point of access into the company's network. Scenarios such as this give rise to breaches known as Advanced Persistent Threats (APTs) which "strive to remain undetected in the network in order to gain access to the company's...valuable data"[13] which includes "intellectual property, trade secrets, and customer data… threat actors may also seek other sensitive data such as top-secret documents from government or military institutions."[14] An inverse scenario poses similar risk. Consider, for instance, a mobile employee who wishes to work at a coffee shop. To accomplish their tasks, they might connect their device to the shop's public Wi-Fi. This certainly promotes productivity, however, network traffic in such public spaces is generally unencrypted, meaning anyone in range can view network activity (through a method known as "snooping").[15] Should the employee engage in transactions involving company data stored on their phone, there are few barriers to a malicious actor intercepting the traffic and stealing that data.

The organization's focus on addressing issues and mitigating the risks associated with personal device use should be on management and gaining improved control over such devices; and to do so begins with implementing a BYOD policy. A BYOD policy must be formulated with consideration for the risks inherent in BYOD devices and the company data or resources with which these devices would be interacting. To do so effectively, the organization should conduct an independent comprehensive risk assessment emphasizing the personal devices that would be brought into their environment. Given the numerous security risks, a risk assessment process for BYOD devices should be conducted separate from, but in addition to, the organization's overall risk assessment. With that said however, it is important to gain an understanding for the relationship of BYOD risk with the other aspects of the business. According to the Deloitte & Touche LLP publication, "Risk Assessment in Practice," assessing risk interactions is an essential component of the risk assessment process. Determining BYOD risks and how they may interact with other conditions contributes to gaining a holistic understanding of BYOD risk within the company. Deloitte offers techniques to consider when assessing risk interactions such as risk interaction matrices, bow-tie diagrams, or aggregated probability distributions.[16]

With a deep understanding of the risks and opportunities, the BYOD policy should impose regulations on such devices, especially regarding security. Compliance should be described and enforced within the policy, outlining the necessary security measures that must be in place on an employee's personal device in order to access the company network. Compliance can be enforced through the use of "quarantine networks" for non-compliant devices. If a non-compliant device attempts to connect to the organization network, an automated process could be put in place to run scripts on the device to check for insecure processes such as an outdated operating system, unpatched vulnerabilities, or the absence of antivirus software. If the device is determined to be non-compliant, it may access a quarantined network, separate from the company's internal employee network, that only permits the device to connect to resources needed for the device to become compliant - such as updating or installing antivirus software.

The integration of a mobile device management (MDM) system helps to support BYOD compliance. Such systems assist businesses in monitoring, managing, and securing employee "mobile devices that are deployed across multiple mobile service providers across multiple mobile operating systems being used in the organization."[17] MDM solutions also serve to allow the management of the applications, network, and data used by a mobile device by the organization's IT department.[18] There are MDM software options available such as those provided by AirWatch, a subsidiary of VMware. AirWatch is an industry leader and highly reputed provider of enterprise-wide mobility management software. AirWatch MDM software features options such as mobile device configuration to allow for centralized management, wrapping to allow the application of policy to mobile applications, and a device enrollment program to establish an inventory of personal mobile devices within the organization.[19]

The policy should also include an employee education and awareness program that details device compliance and proper BYOD use within the workplace. Additionally, it is equally important that the risks and ramifications of non-compliance and improper personal device use are also communicated. Heightened risk awareness should instill in employees better practices regarding the security of their device, in not only the workplace, but elsewhere as well. However, an education program alone is not effective. A culture of understanding for secure device practices must be established within the company. This makes policy implementation a matter of setting the tone at the top. To create a culture of secure and effective BYOD use, the policy must be implemented from the top level of management down in order to ensure its adoption and enforcement.

Through the risk assessment process, it may be determined that the conveniences and benefits of a BYOD program do not justify the risks. If this is the case, the organization may want to enact a policy disallowing personal devices in the workplace. Such a policy could be enforced organization-wide or within specific business units. The latter pertains to situations in which certain departments handle more sensitive company data than others. For example, a company's finance department may impose a no-BYOD policy as it handles the company accounts and relevant information. Whereas a company's development team has a BYOD program enacted as it handles data that is deemed less business critical. An organizational scenario such as this creates the need for the segregation of business units and their data. The idea behind unit segregation is that employees within one unit are unable to access the data of another. This can be accomplished through the integration of multiple separate intranets for each division. There are commercial options available for this purpose such as the Bitrix24 Company Structure tool's "Multiple Divisions" intranet feature, which allows each branch to have their own structure while departmental integration is maintained.[20] The use of separate departmental intranets is recommended when one business unit permits BYOD and another does not. Although the device would be within the same company, they do not support the same functions and therefore should not have the ability access irrelevant, highly sensitive business data.

The integration of personal devices in the workplace is projected to grow at a staggering rate in the coming years. More and more businesses are adopting BYOD programs in hopes of realizing the promised benefits to productivity and morale and gaining a competitive advantage over other organizations. However, an organization must consider the security risks involved with allowing personal devices within the workplace. With consideration for these risks, the proper mitigation measures must be put into place. In doing so, the enterprise can be well equipped to embrace the consumerization movement.

[1] Beal, Vangie. "Consumerization of IT." *QuinStreet Inc.* N.D. Accessed Dec. 2016 <www.webopedia.com>.

[2] Evans, Dean. "What Is BYOD and Why Is It Important?" *Future plc*. 07 Oct. 2015. Accessed Dec. 2016 <www.techradar.com>.

[3] "Cass BYOD & Mobility Study 2016." Cass Information Systems. 2016. Accessed Dec. 2016 <www.cassinfo.com>.

[4] Gilbert, Jake. "BYOD Security: It's Here to Stay. What Can You Do?" SailPoint Technologies. 24 May 2016. Accessed Dec. 2016 <www.sailpoint.com>.

[5] "The Financial Impact of BYOD: A Model of BYOD's Benefits to Global Companies." CISCO Internet Business Solutions Group. May 2013. Accessed Dec. 2016 <www.cisco.com>.

[6] "SAMSUNG Mobile Index Reveals BYOD Trend at a Tipping Point with Mobile Devices, Becoming Central Hub For Personal, Professional Lives." Samsung Electronics America. 8 Jan. 2013. Accessed Dec. 2016 <www.samsung.com>.

[7] Rouse, Margaret and White, Caitlin. "What Is Shadow IT (Shadow Information Technology)?" *TechTarget*. Oct. 2012. Accessed Dec. 2016 <www.searchcloudcomputing.techtarget.com>.

[8] "BYOD Security Incidents Skyrocket with Growing Adoption." *Computer Business Review*. 29 Oct. 2014. Accessed Dec. 2016 <www.bcronline.com>.

[9] "Asset Management." *2014 Information Security Guide*. Atlassian Confluence. 31 Jul. 2015. Accessed Dec. 2016 <www.spaces.internet2.edu>.

[10] Ibid.

[11] Weeks, Alex, et al. "The Linux System Administrator's Guide" The Linux Documentation Project, Free Software Foundation. 2003. Accessed Dec. 2016 <www.tldp.org>.

[12] "What Is a Backdoor?" *Technopedia Inc*. N.D. Accessed Dec. 2016 <www.technopedia.com>.

[13] "Data Exfiltration: How Do Threat Actors Steal Your Data?" Trend Micro Incorporated. 2013. Accessed Dec. 2016 <www.trendmicro.com>.

[14] Ibid.

[15] Hoffman, Chris. "Why Using a Public Wi-Fi Network Can Be Dangerous, Even When Accessing Encrypted Websites." *How-To Geek*. 02 Jan. 2014. Accessed Dec 2016 <www.howtogeek.com>.

[16] Dr. Curtis, Patchin and Carey, Mark. "Risk Assessment in Practice." Deloitte & Touche LLP. Oct. 2012. Accessed Dec. 2016 <www.deloitte.com>.

[17] Beal, Vangie. "MDM - Mobile Device Management" *Webopedia.* N.D. Accessed Dec. 2016. <www.webopedia.com>.

[18] Ibid.

[19] "AirWatch by VMware." VMware. N.D. Accessed Dec. 2016 <www.air-watch.com>.

[20] " Company Structure and Organizational Chart in Bitrix24." Bitrix Inc. N.D. Accessed Dec. 2016. <www.bitrix24.com>.