Issues in Information Systems
Volume 16, Issue III, pp. 238-244, 2015

BRING YOUR OWN DEVICE TO WORK: BENEFITS, SECURITY RISKS, AND GOVERNANCE ISSUES

Jamie Pinchot, Robert Morris University, pinchot@rmu.edu
Karen Paullet, Robert Morris University, paullet@rmu.edu

ABSTRACT

Many organizations are now allowing employees to use their own personal mobile devices to access company-owned data and applications. This concept is known as bring your own device (BYOD). BYOD blurs the line between personal and business use of devices and also presents some significant security challenges and risks for organizations. This paper explores the security risks associated with bring your own device (BYOD) to work, and presents ways to mitigate those security risks. In addition, governance and compliance issues are addressed, and recommendations for bring your own device policies are presented.

Keywords: Mobile Security, BYOD, Bring Your Own Device, Policy

INTRODUCTION

The use of mobile devices is now ubiquitous across the globe, with the number of smartphone users worldwide estimated to top two billion in 2016 [7]. The appeal of mobile computing has had a dramatic impact on both personal and business life. Many people carry their smartphones with them at all times, and depend upon their phones to stay connected to friends and colleagues, to deliver news, to play music and videos, to take photos, to track their fitness goals and habits, and even to wake them up in the morning [16]. Mobile computing has created a paradigm shift in how we live, work, and communicate. It has changed the way people consume media, and has forced organizations worldwide to become more focused on mobile technologies, both for their consumers and their employees.

With smartphones so ingrained in our daily personal lives, it is perhaps not a surprise that employees in many organizations increasingly desire the ability to use their own mobile devices for both personal and work-related interactions. It is inconvenient for employees to carry two different mobile devices (e.g. one for personal use and one for work-related use). Therefore, many employees have been reaching out to their corporate Internet Technology (IT) departments to support use of personal devices at work. This phenomenon is often referred to as the "bring your own device" (BYOD) model. Citrix [4] defines BYOD as "any strategy that allows people to use their own devices, whether occasionally, primarily or exclusively, for work" (p. 3). BYOD represents a significant change from past IT models, where organizations typically allowed employees to use only corporate-owned equipment for anything work-related, such as checking corporate email or accessing corporate applications or data.

While BYOD may keep employees happier and create other positive impacts for organizations such as increased employee productivity and higher recruiting acceptance rates, it also brings with it a plethora of security concerns [5]. If employees use personal mobile devices to access corporate data, their device becomes a possible weak point in the organization's security because it is not necessarily subject to the same security standards to which corporate-owned devices would be held. Many organizations are now struggling to balance their employees' desire for BYOD with their overall security concerns [1]. Part of the challenge for this struggle is the speed with which new generations of mobile devices are released, and consequently make their way into the workplace. Another issue stems from the fact that the BYOD model has largely been driven by employee demand rather than corporate policy makers, which has resulted in a piecemeal approach to mobile security [5].

Market projections are reporting that by 2016, 65% of smartphone shipments will be used in BYOD workplaces and 38% of companies will stop providing devices to employees [22]. Reasons for the shift in BYOD support are to keep employees happy by using a device that they are most familiar with and to lighten the weight of the IT Department.

When employees bring their own devices, they are able to use modern technology that the company does not need to use resources to provide.
However, employees bringing their own devices to work may also increase a company's risk of a data breach. If personal employee devices are permitted access to corporate networks and corporate governance policies are not in place to ensure adequate security measures are followed, those devices can be potential access points for hackers.

In 2014, there were a number of notable data breaches including a hack of Sony where information from more than 32,000 corporate email accounts was leaked to the public [11]. That same year also saw a hack of personal celebrity photos from Apple's iCloud. The breaches occurred due to a script that queried iCloud services by using the "Find My iPhone" API to find out a person's username and password. The number of attempts to guess the username and password was not set by Apple giving a person time to guess without being locked out. As a result, Hollywood celebrities photos were leaked to the public [13].

In 2013, Target's network was breached. This breach caused the credit and debit cards of nearly 40 million consumers and personally identifiable information on 70 million consumers to become compromised. This breach of information not only affected Target credit card holders, but the information of Target customers who might have paid with a bank credit card. Target expects to lose an estimated $148 million in compensation claims [12]. The attack was initiated through a remote access authentication measure of a contracted worker's credentials. The contractor's employer worked refrigeration and HVAC systems for Target and had remote network access for the purpose of monitoring store temperatures and energy consumption rates [21]. Target failed to properly secure the remote access to their servers, giving the attackers full access to payment processing systems.

Costs related to security breaches are high. Deshmukh and Wadhe [5] note that the per-incident cost of a data breach in 2009 was $6.75 million. Malware for smartphones is also on the rise [15]. Sophos' Security Threat Report [5] notes that mobile security threats have grown and matured, and malicious code targeted at mobile devices, in particular the Android platform, is mutating and getting smarter at camouflaging itself. Malware on a mobile device could also open security holes through which a data breach could occur.

Hacking and other high-tech crimes aside, there are also risks for a data breach if a mobile device is simply lost or stolen and retrieved by the wrong individual. Consider that an employee could be carrying sensitive data on an iPad that gets stolen during his or her morning train commute. Vickerman [3] describes this danger succinctly, noting "The individual will mourn the loss of cherished photos and music playlists … The company, however, may face much longer-lasting repercussions, especially if its data ends up in the wrong hands and constitutes a data breach" (p. 40). The additional security risks presented by BYOD could significantly increase the possibility of a data breach within an organization if not handled properly.

BYOD may offer potential benefits for employees, but also raises security concerns for organizations. The trade-off between benefits of BYOD and security risks is not well understood and has not been addressed much in academic literature. This paper will contribute to the mobile security literature by discussing and synthesizing what is known about both the benefits and risks of using BYOD within organizations. Techniques for mitigating risks will be explored and recommendations for successful implementation of BYOD will be presented.

BENEFITS OF BYOD

It is sometimes noted that BYOD is contributing to the "consumerization of IT" in the workplace, as employees have been the main proponents of the BYOD phenomenon. In fact, Vickerman [20] notes, "Whether you love it or hate it, you have to incorporate BYOD planning into your information governance strategy" (p. 40). This necessity is becoming a simple truth for most organizations, as organizations must react to the cultural phenomenon of employees bringing their devices to work [6].

Employees have pushed for BYOD, preferring to use personal devices in the workplace because they are easier to use, more convenient, and allow them to mix personal and work tasks [8]. A study by Singh [18] found that participants reported improved efficiency and productivity, higher job satisfaction, competitive advantage over others, and enjoyment of increased mobility when participating in BYOD in the workplace. These findings complement those found by Cisco, which was one of the first companies to adopt a BYOD policy in 2007. A survey

of 2,000 people found that 61% of employees "feel happier and thus more productive when using technologies of their choice" [2].

SECURITY RISKS FOR BYOD

Deshmukh and Wadhe [5] identify three areas of vulnerability in mobile business operations: lost or stolen devices, unauthorized data access, and gaps in device management and policy enforcement. The first vulnerability, lost or stolen devices, is highly related to physical access to a device. Mobile devices are small and easy to lose, and a lost mobile device could be a compromised mobile device. To mitigate the risk of loss or theft, mobile devices used as part of a BYOD program should follow several security best practices. First, user authentication should be required at the device level; a passcode, password, or fingerprint should be required to access the contents of the device. Also, remote lock and wipe features should be activated so that the device can be locked or wiped clean of data if determined to be lost or stolen. These features are sometimes offered as part of the device operating system software. Alternatively, remote lock and wipe features are part of many mobile device management (MDM) software packages that can be implemented by the organization. Lastly, any corporate data stored on the device should be encrypted.

Another vulnerability is unauthorized data access. This vulnerability is a threat to all networked computing systems, not just mobile devices. However, mobile devices offer some new ways in which unauthorized data access can occur. One way is for an unauthorized individual to gain physical or remote access to the device and thus to data on the device. A second, and perhaps less obvious issue, is for an authorized user to gain unauthorized access to corporate data or to make inappropriate use of corporate information. Because the employee or other individual can now access corporate data and systems on a personal device outside of the organization's office space, he or she has much more privacy in which to attempt any inappropriate access or use of company data [5]. The ability to remotely set device settings and restrictions "over the air" can help to mitigate this risk. Lastly, policy enforcement can be a significant issue for organizations using BYOD. Simply having a BYOD policy where personal devices on company premises are commonplace may also pose another risk. If it becomes common to see a variety of personal mobile devices in the office, some of which have very high data storage capacities, then it also will become more difficult to distinguish unauthorized devices that could be used to steal data from company premises [20].

Deshmukh and Wadhe [5] note that "security policies are only as good as an organization's ability to enforce them; and today's business mobility presents a challenging enforcement environment" (p. 73). One of the main challenges in enforcing policies is the fact that most large organizations support a variety of different mobile device models and platforms, each of which can have unique considerations in regard to security.

Mobile devices in general have some inherent security risks in terms of viruses and malware. Malware is malicious code that is intended to damage data or devices, or open a "back door" to allow unauthorized access to a device. Desktop and server operating systems generally receive frequent security updates. Mobile device operating systems do not all receive security updates as frequently. In addition, anti-virus and anti-malware software is not as mature for mobile devices as it is on desktop computers. Part of this is due to lack of awareness for the need for this software on mobile platforms, and also to a lack of operating system support and limited battery life on devices [15, 17].

MITIGATING THE RISKS

It is clear that the nature of mobile devices lends itself to dangers associated with loss or theft resulting in physical access to the device falling into the wrong hands. There are several strategies to mitigate security risks associated with physical device access. From a technology perspective, one obvious solution is not to allow direct installation of corporate applications or data onto an employee's device. Rather, access to corporate applications and data can be provided through enterprise mobility management software, desktop virtualization, and secure file sharing [3, 4]. If no corporate data or applications are directly installed, a layer of security will remain even if physical access to an employee's device is compromised. A user would need to login and pass authentication to gain access to any corporate applications. The use of enterprise mobility management software would enable completely device-independent computing. Employees would have the freedom to choose and use any device they wish, and IT can still maintain security and control over corporate applications and data.

Enterprise mobility management software can allow an organization to maintain a level of control over devices registered with the system. Mobile device management (MDM) software systems are commonly used to enforce corporate policies and can range from simple to complex in terms of control held over registered devices [3]. For example, an MDM system could check only for simple security mechanisms such as ensuring that a PIN or fingerprint lock is set, forcing a screen lock after a certain number of idle minutes, and allowing for remote wipe of the device if it is ever lost or stolen. More complex (and arguably invasive) MDM systems can control nearly every aspect of the managed device. This could include tracking the GPS location, allowing only certain Wi-Fi network connections, and providing a complete inventory of installed applications and data [14]. Mobile application management (MAM) software systems focus on security at the application level, rather than on the device, supporting secure, on-demand delivery of apps to devices, with tracking and monitoring to support compliance. This is often accomplished through the use of a custom app store only for use within the organization [3]. MAM systems can also allow for secure file sharing, online meetings in HD video, and other types of online collaborative workspaces [4]. When apps are managed through a MAM system, the organization can push app updates to all devices or uninstall apps automatically over the air. This gives an organization a high level of control when dealing with security issues. If an app has a security flaw, the MAM system will allow either a quick uninstall or update (with a patch) to all employees in a timely manner. In order to utilize the full MDM and MAM software capabilities, each device that will be used within the organization (both corporate and personal) must be registered.

Companies allowing BYOD may implement geo-fencing technology in order to protect corporate information. Geo-fencing uses global positioning systems (GPS) or radio frequency identification (RFID) to define a geographical boundary, which is essentially a digital barrier. Inside the geo-fence, specific device capabilities can be disabled or controlled to ensure that the organization's policies are followed. In the case of BYOD, the geo-fence boundary is usually the perimeter of the workplace. Companies that incorporate geo-fencing send alerts to the system administrator when an employee goes outside of the boundaries set in place. Geo-fencing establishes a virtual boundary in a real-world geographical area [9].

GOVERNANCE AND COMPLIANCE ISSUES

Any organization allowing BYOD should have a formal policy to define the organization's practices and requirements for BYOD. Many organizations still allow BYOD as an informal practice [4], lacking a formal BYOD policy. This is often the case because employees often bring their own devices to work, regardless of whether or not the organization has a policy in place. Citrix [4] states that, on average, 5.18 devices connect to the corporate network per knowledge worker. Some of these devices are likely owned by the organization, but others, such as personal smartphones and tablets, are also likely to be personal devices. With the rapid rise of smartphone and tablet use among consumers (and thus employees), most organizations are playing "catch up" in terms of writing policies to handle BYOD issues [6].

Several areas should be addressed in a BYOD policy. These include eligibility, allowed devices, device ownership, security and compliance, data ownership, breach investigation procedures, and device support and maintenance issues, including the right to be forgotten upon leaving the organization [4, 5, 20].

In terms of eligibility, organizations should make clear who is allowed to use personal devices and in what situations. Are all levels of employees permitted to BYOD, or are certain employees with access to sensitive data restricted? In addition, allowed (or excluded) devices should be detailed so that employees are aware that the organization can choose to allow or disallow particular devices that may be assessed as riskier than others. In terms of device ownership, Citrix [4] recommends that employees purchase personal devices on their own with no corporate involvement. This makes the issue of ownership in terms of the device very clear. It is also recommended to implement cost sharing in regard to Internet/data access for devices, where the employee pays part of the cost and the organization pays another part. Having the employee share some of the cost of the device is one of the primary benefits of BYOD for organizations.

A BYOD policy should also clearly state the requirements for security and compliance. For example, an organization may wish to require that all business applications and data reside off the device (with access through virtualization or enterprise mobility management software), that an employee agrees to maintain a PIN or fingerprint

lock on the device, that the device be registered with MDM or MAM software systems to allow for policy enforcement and other benefits such as remote wipes and automatic security updates, or that anti-virus and anti-malware software is installed and kept up to date. The policy should also give detail about what the employee is agreeing to by registering their personal device. For example, will the organization's MDM software be monitoring GPS location, installed apps, or restricting Wi-Fi access? Any monitoring of the device should be disclosed [4, 5, 20].

In terms of data ownership, it should also be disclosed if any data on the device will be considered as organization-owned data and whether the organization has the right to access it directly from the device [20]. If all corporate applications and data remain off the device as recommended, then this should not be an issue and all data residing on the device would remain under the employee's ownership.

If a breach of security or compliance regulations should occur, the BYOD policy should also cover procedures that will be followed to investigate or resolve issues related to the breach. A breach could include events such as loss or theft of the device, unauthorized access to the device, or non-compliance with security policies (such as an employee circumventing the required security mechanisms). The BYOD policy should clearly state if the organization has the right to audit and access information [4, 20].

Finally, device support and maintenance issues should be addressed in the policy. It should be made clear whether the employee or the organization is responsible for maintenance or replacement costs. This is another area where BYOD could provide benefits to the organization. If an employee is responsible for maintenance or replacement costs for a device, the device will probably be less likely to show up at the IT department with ketchup in the keyboard. Employees tend to take better care of equipment when they are responsible for the costs [4]. Another area related to maintenance involves the event in which an employee leaves the organization. The BYOD policy should clearly state the procedures that will be followed in this situation. In case of an unfriendly termination of employment, the organization should have a mechanism in place for quick termination of access to corporate applications and data [4].

CONCLUSIONS

Mobile devices have become highly embedded in our day to day lives, and people want the convenience of using one mobile device for both personal and work needs. The line between work and personal life is continuing to blur, and BYOD is one more factor that is contributing to the concept of work life balance. Organizations today are seeking ways to accommodate employees to use their own personal mobile devices to access corporate data and applications. As part of this process, organizations must address the specific security risks presented by a bring your own device (BYOD) to work program.

If BYOD is being used in an organization it is imperative to implement and enforce BYOD policies. The BYOD policy will outline the requirements and actions of device use. Items that should be included in the policy include but are not limited to:

1) Eligibility requirements for employees
2) An explanation of the types of devices authorized for use
3) Clear guidelines regarding device ownership, including who will pay for the initial device, maintenance costs, or replacement costs (employee or organization)
4) Security and compliance policies that must be followed by the employee, in detail; this should include the disclosing of any monitoring of the device that the organization intends
5) Clarification of data ownership, including what data and applications the organization owns and/or has a right to access from the device
6) Breach investigation procedures that will be followed (in the event that the device is lost, stolen, or otherwise compromised), which should include the expected actions that will be taken by both the employee and the organization in a breach situation

7) Exit strategy guidelines for when an employee leaves the organization [10]; for instance, if an employee leaves the organization, he or she should have the right to be "forgotten" and the organization should no longer access the device; conversely, the organization should have an easy way to terminate the employee's access to their data and applications remotely
8) A set of best practices which employees can use to secure their mobile device
9) Implementation of anti-virus and anti-malware software

REFERENCES

1. Bring your own device: Security and risk considerations for your mobile device program. (2013). Insights on governance, risk, and compliance. EY, 1-12.
2. Budak, J. (2012). Should you bring your own mobile device to work? Retrieved on May 12, 2015 from http://www.canadianbusiness.com/lifestyle/should-you-bring-your-own-mobile-device-to-work/
3. Cisco. (2014). Device freedom without compromising the IT network [White paper]. Retrieved on May 1, 2015 from http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/byodwp.pdf
4. Citrix. (2013). Best practices to make BYOD simple and secure [White paper]. Retrieved on April 20, 2015 from https://www.citrix.com/content/dam/citrix/en_us/documents/oth/byod-best-practices.pdf
5. Deshmukh, R., & Wadhe, A. (2012). Mobile security: Why to secure your mobile devices? *International Journal of Advances in Engineering & Technology, III (IV),* 72-74.
6. Doherty, J. (2015). *Wireless and mobile device security.* Burlington, MA: Jones & Bartlett Publishing.
7. eMarketer (2014). 2 billion consumers worldwide to get smart(phones) by 2016. Retrieved on April 2, 2015 from http://www.emarketer.com/Article/2-Billion-Consumers-Worldwide-Smartphones-by-2016/1011694
8. Garlati, C. (2011). Trend Micro consumerization report 2011. Retrieved on May 1, 2015 from http://www.cio.com/article/2395944/consumer-technology/7-tips-for-establishing-a-successful-byod-policy.htmlhttp://bringyourownit.com/2011/09/26/trend-micro-consumerization-report-2011/
9. Geofencing. (2015). Geofencing. Retrieved on May 15, 2015 from http://www.techopedia.com/definition/14937/geofencing
10. Hassel, J. (2012). 7 Tips for establishing a successful BYOD policy. Retrieved on May 14, 2015 from
11. Jakewriter. (2014). Sony security breach reportedly similar to the apple icloud celeb nude photo hack, the fappening. Retrieved on May 14, 2015 at www.kdrmastars.com/articles/62468/2014/1218/sony-security-breach-similar-to-the-apple-icloud-celeb-nude-photo-hack-the-similar-to-the-apple-icloud-celeb-nude-photo-hack-the-fappening.htm
12. LeClaire, J. (2014). *Cost of Target data breach: $148 million plus loss of trust.* Retrieved on May 12, 2015 from http://www.cio-today.com/article/index.php?story_id=111001SF8BY6
13. Lewis, D. (2014). iCloud Data Breach: Hacking and celebrity photos. Retrieved on May 15, 2015 from http://www.forbes.com/sites/davelewis/2014/09/02/icloud-data-breach-hacking-and-nude-celebrity-photos/
14. Kosht, M. (2013). MDM vs. MAM: Comparing enterprise mobile security management options. Retrieved on May 5, 2015 from http://searchsecurity.techtarget.com/feature/MDM-vs-MAM-Comparing-enterprise-mobile-security-management-options
15. Paullet, K., & Pinchot, J. (2014). Mobile malware: Coming to a smartphone near you? *Issues in Information Systems, 15(2),* 116-123.
16. Pinchot, J., Paullet, K., & Rota, D. (2011). How mobile technology is changing our culture. *Journal of Information Systems Applied Research, 4(1)*, 39-48.
17. Sethi, A., Manzoor, O., & Sethi, T. (n.d.). User authentication on mobile devices. Retrieved on April 2, 2015 from http://www.cigital.com/wp-content/uploads/downloads/2012/11/mobile-authentication.pdf
18. Singh, N. (2012). B.Y.O.D. genie is out of the bottle – "Devil or angel". *Journal of Business Management & Social Sciences Research*, 1(3), 1-12.
19. Sophos. (2013). Security Threat Report 2014. Retrieved on April 5, 2015 from https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf
20. Vickerman, J. (2013). Bring your own device to work. *Risk Management*, 38-41.
21. Vijayan, J. (2014). *Target breach happened because of a basic network segmentation error.* Retrieved on May 12, 2015 from http://www.computerworld.com/article/2487425/cybercrime-hacking/target-breach-happened-because-of-a-basic-network-segmentation-error.html

22. Wainright, A. (n.d.). 10 Stats that show it's time to prepare for BYOD network design. Retrieved on May 1, 2015 from http://www.securedgenetworks.com/strategy-blog/10-Stats-that-Show-it-s-Time-to-Prepare-for-BYOD-Network-Design