BYOD

A Growing Trend With Opportunities and Threats

Tyler Cole and Vince Patrick

Table of Contents

Executive Summary

This report was developed to provide a detailed overview of BYOD including its benefits, concerns, and countermeasures to those concerns, along with the recommendations we formulated based on our research. When researching BYOD, we discovered that it can offer advantages for various organizations by increasing employee satisfaction, increasing productivity, and saving the company money. Although it may seem easy to start allowing your employees bring their own devices, these benefits are only acquired when BYOD is implemented properly and securely.

We found that to fully benefit from the positive effects of BYOD, companies must be aware of its concerns and take the appropriate steps to reduce its negative impact on the company. While there are several concerns, the major risk is the possibility of company data being leaked or compromised. Data is one of the most important assets a company can have and the security of that data is paramount. Data security should always being taken into consideration when implementing a trend such as BYOD. When employees use and store company data on their device, it opens the door to various ways the data could be compromised including something as simple as losing the device, having it stolen, or using the device over untrusted networks. However, our research suggests that with proper tools, risks associated with BYOD can be controlled in a way that is satisfactory to most organizations.

There are many ways a company can protect themselves from the concerns of BYOD. In our report, we touch on these countermeasures and delve into specific policies and management tools that can be adopted to make sure the company is not in danger when allowing employees to bring their own devices. Moreover, we compare two popular EMM solutions, MobileIron and

Intune, to discuss their upsides and drawbacks and provide an analysis on how they might affect the companies that use them. To wrap-up our paper and demonstrate our understanding of BYOD, we explain our recommendations on how to approach and implement BYOD using the solutions we detailed.

Introduction/What is BYOD?

BYOD stands for **B**ring **Y**our **O**wn **D**evice, but its implications extend far past its seemingly simple abbreviation. What BYOD really is refers to a growing trend among organizations, both small and enterprise level, to allow employees to bring their personal devices, referring to electronic equipment such as cell phones and laptops, into the workplace for the purposes of completing work. BYOD is also commonly referred to as IT Consumerization ("Smart Protection Suites."). BYOD is a centerpiece example of blending consumers (or employees, depending on perspective) and their personal lives with their professional careers in an organization.

BYOD is generally divided into two groups: Personally owned company enabled (POCE) and Corporate owned personally enabled (COPE) ("Bring your own device”). POCE refers to devices that a person purchased and brings in for use into an organization, and is typically what one thinks of when BYOD is brought up. COPE refers to instances where an organization will purchase a device and issue it to an employee allowing for personal use. This type of BYOD is somewhat counter-intuitive, as one is not bringing in their own device, rather using an assigned device as if it was their own.

BYOD is growing rapidly in popularity. It is making employees more comfortable, and is potentially saving companies a lot of money. There are many important benefits, considerations, concerns, and technologies to consider. This paper is an attempt to discuss those things in a somewhat high-level, yet comprehensive way.

Benefits of BYOD

The idea of allowing employees to bring their devices to work might seem questionable to some, but many company executives and managers approve of this trend. According to a study done by Cisco, 69% of information technology decision makers support employees using their own device at work ("BYOD Statistics Provide Snapshot of Future"). These IT managers see first hand the benefits of BYOD, especially its positive effect on employees. Not only does it increase employee satisfaction by allowing them to use a device fit to their preferences, but it also increases their productivity due to their comfort level in using the device ("BYOD in the Workplace"). Employees usually choose a device based on what they want and like, but when corporations assign devices, this choice is taken away. BYOD, on the other hand, gives employees the opportunity to bring in a device that they want to use and already have experience with. Working on the device they most likely use every day will provide a convenience and comfort that will increase their satisfaction and perhaps alter the way they view performing their job.

Likewise, BYOD improves employees productivity because of their comfort with the device. In fact, 79% of employees surveyed believed that using their own device allowed them to perform better and efficiently while working ("Bring Your Own Risk with BYOD"). Moreover, Cisco found that when employees use their own device, it saves them up to 81 minutes per week ("BYOD Statistics Provide Snapshot of Future"). This amount of time is saved due to a combination of factors. As mentioned earlier, BYOD increases productivity and saves employees time because they know how to use the device and are less likely to ask for device support. Another time-saving benefit is that employee devices are usually up to date and offer more advanced capabilities than the devices companies can afford to buy for every employee. These newer employee owned devices can help them increase their productivity just by offering more options and versatile functionality.

The benefits of BYOD do not just affect employees as companies also see positive changes. One of these benefits is the amount of money the company saves on buying and issuing new devices to employees. According to Cisco, U.S. companies can save up to $3,150 a year per employee by allowing employees to bring their own devices ("Calculating the True Cost of BYOD"). Companies can use the money not spent on these devices to help other areas of the organization. With BYOD, organizations are not spending money on devices that employees might not even want or know how to use. Assigning company devices also takes up valuable time as employees would have to be trained on how to use the them and need IT support when something goes wrong. Also, organizations that implement BYOD can save time by not having to research and make a decision on what device to choose for their employees.

Another benefit BYOD offers for organizations is that it encourages the use of cloud storage and processing. As more employees are bringing in their own mobile devices, organizations may decide to steer away from storing data locally and switch to the cloud (BYOD advantages-"). In some cases, this is a requirement for using BYOD solutions. Therefore, the organization will see an increase in collaboration and accessibility by allowing data to be accessed right from your device. This will save employees time and the company resources, allowing them both to perform more efficiently. Being able to access work data from your personal device will also make it easier to work remotely. However, this comes with an increased risk of compromising company resources, but this liability can be mitigated with solutions discussed in the next section.

While implementing a BYOD strategy can lead to numerous benefits for an organization, it is not without its concerns. Some of these benefits are tied to specific risks that could put the company and their resources in danger. For a company to fully benefit from BYOD there must be countermeasures in place to confront these concerns.

Security Concerns and Countermeasures

While BYOD increases accessibility of company data, it negatively affects its confidentiality and integrity (“Bring Your Own Risk with BYOD”). Allowing employees to bring and use their devices for work will lead them to using and storing company data on their machine. Once an employee stores this data on the device, the company can lose the ability to monitor what data is being processed and stored on it. This is especially dangerous for companies that deal with personally identifiable information because if that information is leaked, it puts people’s privacy in danger and reflects poorly on the company. While BYOD offers the benefit of increasing productivity and saving money, the impact of a major data leakage is almost insurmountable to overcome.

One way to prevent or reduce the risk of data loss associated with employees bringing their own device is to implement a thorough BYOD policy. This policy should explain what is acceptable and unacceptable when using your device to store and transmit company data. These policies are not implemented the same at every company but in general, they should be constantly updated and made accessible to ensure employees are aware of every risk and help prevent situations where the confidentiality of the data is compromised. Although BYOD policy is essential in spreading awareness and protecting assets, only 39% of companies have a BYOD policy in place ("Ultimate Guide to BYOD Security"). Companies that refuse to implement a BYOD policy are taking on major risks and putting their data in danger.

We would recommend that every company have some sort of BYOD policy to ensure proper vulnerabilities and risks are reduced. The policy could include requiring employee-owned devices to be registered, making sure the device is not jailbroken or rooted, and requiring security updates before they can access company data ("Bring Your Own Risk with BYOD"). Having these provisions makes sure the device is secure and properly configured before it can store and access sensitive data. Policies could also address what applications are prohibited on the device, what to do with data when employee leaves the company, how to report a lost device, and identify the right company's have over certain data on the employee's device ("BYOD Policies: What Employers Need to Know"). Making sure these details are documented in a policy will help minimize problems in the future and help employees understand how BYOD affects them. Moreover, policies can require strong passwords and virtual software with use of a VPN for devices like laptops ("BYOD Policies: What Employers Need to Know"). Including these terms in the policy will help ensure proper security measures are being taken when accessing company resources. These are just some of many things that BYOD company policies can require. By making a BYOD policy that includes specific terms, the organization can express what they expect from the employees and how the devices and company data should be treated.

Another consideration to make is that an employee could very easily lose this device or allow an unauthorized person to use it and access this data ("Bring Your Own Risk with BYOD"). Phones and other personal devices are easy to misplace just like anything else. Even if one is a responsible employee, it is difficult to avoid losing an item like one's phone every once and awhile. Physical theft is also a potential risk to consider, as laptops, tablets, and phones are small, often change location, and are of high value. People take their phones everywhere they go, which means they are also carrying company data from place to place exposing the data to malicious actors. An attacker can not only steal valuable data that is on the phone, but they can use the information they gathered to launch another attack or possibly impersonate the user and access their accounts ("Bring Your Own Risk with BYOD"). This could go unnoticed by the organization as well if the employee does not inform them or the employee is unaware.

On the other hand, these risks should not keep companies away from BYOD as there are controls that can be put in place to limit these threats. To do this, an organization can adopt enterprise mobility management (EMM) solutions which encompasses mobile device management (MDM), mobile application management (MAM), and mobile content management (MCM). In BYOD, these solutions help manage devices and ensure their security. MDM focuses on securing the devices and applying policies, while MAM and MCM manage what applications each employee can access and what applications are permitted to access company data respectively ("Enterprise Mobility Management Options"). Applying these solutions can allow the organization to block unauthorized devices from their network, encrypt company's data, enforce the use of strong passcodes, install anti-malware, and erase data off the device remotely ("Guide to Mobile Device Management"). Using EMM solutions that involve these safeguards can reduce the risks associated with theft, loss, and an attack on the device.

An important issue to consider with some EMM solutions is the employee's privacy. For a number of these solutions to work, they require access to employee's personal device and the ability to monitor it. This is a problem for employees and employers both as employees do not want their privacy violated and companies have little interest in the employee's personal information. To help remedy concerns, organizations can institute policies that address what information is being monitored and ensuring that it is only essential information ("BYOD Policies: What Employers Need to Know"). Nevertheless, employees still may feel insecure about the idea of employers having the ability to view their information. To help solve this problem, EMM solutions are using the concept of containerization. Containerization involves having an environment that will allow the enterprise data and applications to be separate from the rest of the personal device ("Ultimate Guide to BYOD Security"). Having a secure container will prevent the employee's personal information from being monitored and accessed by the organization. Inside of the container, there could be apps the company uses and certain email clients that offer protected communication ("Using a Secure Container-"). To access this environment, it will require employee authentication and inside the container, the enterprise's data will be encrypted. Therefore, by using containerization, the company will protect sensitive information and decrease the risk of data being accessed from unauthorized persons ("Bring Your Own Risk with BYOD"). Also, if the device was stolen or lost, the company can erase the environment from the machine and not affect the employee’s personal information. This would also be a useful tool when an employee who has access to certain enterprise data is terminated or resigns. Moreover, these environments can allow backups of company data to ensure there will be minimal loss when environments have to be wiped off of the devices (“Using a Secure Container-”). While these solutions can limit some of the concerns of unsecured data, no controls are absolute.

Another benefit of BYOD associated with a risk is allowing employees to access, store, and transmit data directly from their device. If an employee decides to use an unsecured network to work and use company data, it can easily be intercepted (“BYOD in the Workplace”). Devices like packet sniffers are used on networks to intercept transmitted data and then the attacker can use that information maliciously. Certain EMM solutions can help manage this risk. In adopting these solutions the employee can use a secure container on their device that will encrypt the company’s data inside the work environment. Employees should still made aware of untrusted networks in BYOD policy and encouraged to not transmit any sensitive data over them.

One BYOD issue that is often overlooked is the payment of employee’s data plan. When employees use their device for work, they are using data that they pay for. Most employees would not like the idea of having to pay to do work on their phone. That is why some employers believe that reimbursement for the employee’s data can help fix this problem. The issue with reimbursement is that companies have no way of knowing what amount of data they used for work and what amount was used for personal use. One solution to this conflict would be for the organization to address reimbursement in its BYOD policy and offer to pay a fixed percentage of the cell phone bill (“Four BYOD Challenges to Consider”). This adds another cost to the company, but it is not as expensive as buying and supporting company-issued devices

Companies that refuse to adopt BYOD due to these risks will fall victim to competitive disadvantage. Risks are always going to be prevalent when dealing with sensitive data and company resources, but if you have the right controls in place, risks can be reduced and attacks can be prevented. When implementing BYOD into an organization, policies and EMM solutions will provide protection and spread awareness to help mitigate and defend against threats. There is not one clearly defined solution that all organizations should adopt, but each company must evaluate their needs and chose their options accordingly based on the solutions available.

BYOD Solutions

BYOD for Mobile Devices such as cell phones and tablets is typically what one thinks of when considering BYOD. There are many platforms that have been developed to support BYOD and mobile devices, and each one of them should be carefully considered against an organization’s needs in terms of cost and benefits. Here we discuss two of the leading EMM solutions, though it should be noted that there are many others. These two solutions were chosen based off of our findings, preferences, and previous experience with the tools. The simplest way to describe EMM is an all encompassing service that allows for an application (and relevant credentials and certificates) to be installed on a mobile device, that connects to a centralized console that can be managed and monitored to help ensure that BYOD devices are not causing unnecessary exposure to risk. MobileIron is a very popular EMM tool in the industry and it has the awards to prove it, such as the 2017 Frost and Sullivan award for EMM (“MDM &

Enterprise Mobile Solutions"). MobileIron sports important features as far as information security is concerned, such as remote inventory management, compliance management, and the ability to wipe, even selectively, corporate data from devices that fall out of compliance or otherwise pose a security risk ("Mobile Device Management"). Like most reputable EMM solutions, MobileIron is fully compliant with such important laws as HIPAA ("MDM & Enterprise Mobile Solutions"). MobileIron also has a somewhat unique feature that it offers in an attempt to help organizations cut costs in the help desk department. A self-service portal, referred to as the MobileIron BYOD Portal, presents a customizable service that allows users to register, lock (and unlock), wipe, and view the compliance status of their device ("BYOD Portal -"). This is a large departure from the way security is handled in general, because this is usually handled by an administrator or some other information security professional. This serves to aide the one of the overall appeals of BYOD: user comfortability and autonomy. Unfortunately, this feature is only available to users of the Android flavors of mobile operating systems, and not the also popular iOS platform. Another potential issue with using MobileIron within an organization is its requirement for the use of the remote desktop service, Splashtop. This could cause organizations issues if they use a different remote desktop solution, and would mean additional time and configuration for deployment. There is also a choice to be made not only in the tier of MobileIron an organization may have use for, but the consideration between operating MobileIron in an on-premise manner with MobileIron Core, or in the cloud with MobileIron Connected Cloud.

Microsoft is a player in virtually every field in IT, and it has it's own EMM solution.

As with many Microsoft products, a major selling point for Intune is the integration capabilities with other Microsoft products. Azure is Microsoft's cloud computing platform ("Manage mobile devices and apps from the cloud"), and it is integrated well with Intune, providing a dashboard that lists connected devices, their compliance status, alarms and alerts, as well as the ability to add and remove policies ("Global. Trusted. Hybrid"). Because Intune management take place in a cloud computing environment, resources in the on-premise environment are not strained with the task of managing multiple devices. Key features of Intune include the ability to automatically configure devices upon login, the ability to push applications, updates, policies, and setting without user interaction, and the encryption and trackability of shared information assets ("Global. Trusted. Hybrid"). A very impressive security feature, simply referred to as conditional access, which allows access management based on criteria such as compliance status of the device and the actual physical location of the device. Intune also include features that are somewhat standard in the EMM world, such as remote locking and wiping of devices. An important consideration with deciding to use Intune as an EMM solution is that it requires the use of Microsoft tools (such as Azure), which can create additional costs and configurations for businesses that do not already have those technologies in place. Furthermore, unlike MobileIron, Intune as a product is only offered in the cloud.

Many EMM solutions provide similar features, and the real differences come down to cost and the state of the environment to which the solution would be deployed. These, and of course the defining features of each solution, are what should be seriously considered. In our conclusion and recommendation sections, we explore these considerations.

Recommendations and Conclusion

The decision about whether or not implement BYOD in an organization is a very conditional and somewhat difficult one. As with many issues in the realm of information security, benchmarking an organization and its needs with relation to a similar organization can prove to be a powerful tool. In other words, of an organization that is similar in size, mission, scope, and industry is implementing a BYOD program, it would be beneficial for an organization to look into the "how" and "why" that the other organization has come up with.

Another important consideration is an organization's risk appetite. Even with the most loyal staff and highly technical controls, connecting outside devices to an organization's network inherently poses risks. The benefits of having employees bring in their own devices should outweigh the associated risks, as measured against the risk appetite of the organization. Ultimately, each organization must be comfortable with the decision, and make sure that research specific to their organization is accurate and informative.

Concerning the specific EMM solutions we have mentioned, we would recommend Intune to organizations that are integrated into Microsoft products. The largest benefit of using Microsoft products is their cohesiveness with each other, and the dashboards and terminology are similar and uniform, making it easier for both users and administrators to engage with the BYOD program successfully. However, choosing Microsoft in this setting can lead to higher costs for certain features. More money for more features is true for most applications in the world, but Intune is divided into tiers (similar to tiers for office 365) based on features and organizational size/capabilities. Some features that come standard in MobileIron, for example multi-factor authentication, require a higher tier (and thus a higher price) within Intune. From Tyler's own personal experience working at General Electric and trying to help implement the BYOD there, both he and many of the security professionals he worked with felt that Intune often demanded much more money for features that they felt should be standard, or that some features were simply placed in higher tiers when they should be included in lower ones. All in all Intune has many of the features an organization would be looking for, all with the familiar name and products that Microsoft offers.

For organizations that are not tightly coupled with the Microsoft family of products, MobileIron is an excellent EMM solution. As we mentioned earlier, this tool is set up well for those who wish to explore more user-centric BYOD options, and is exemplified by the self-service portal.

If an organization decides to implement BYOD, they need to ensure that their solution meets their needs. Organizations also need to create a strong information security policy around BYOD that is properly implemented and centered around the organization’s views and expectations. At the end of the day, most EMM solutions offer many of the same features, and so key criteria such as price and implementation methods should be at the forefront of the minds of decision makers. Only those who know and are invested in the organization and its needs can make the best decision.

Works Cited

Title Image: http://www.acronis.com/blog/sites/default/files/byod.jpg

"Smart Protection Suites." Trend Micro. N.p., n.d. Web. 25 June 2017. <https://www.trendmicro.com/en_us/business/products/user-protection/sps.html>.

"Bring your own device." Wikipedia. Wikimedia Foundation, 27 Apr. 2017. Web. 25 June 2017. <https://en.wikipedia.org/wiki/Bring_your_own_device>.

"MDM & Enterprise Mobile Solutions | MobileIron." MDM & Enterprise Mobile Solutions | MobileIron. N.p., n.d. Web. 25 June 2017. <https://www.mobileiron.com/>.

"Global. Trusted. Hybrid." Microsoft Azure: Cloud Computing Platform & Services. N.p., n.d. Web. 25 June 2017. < https://www.microsoft.com/en-us/cloud-platform/microsoft-intune>.

"Manage mobile devices and apps from the cloud." Microsoft Cloud-Platform - US (English). N.p., n.d. Web. 25 June 2017. <https://azure.microsoft.com/en-us/>.

"Mobile Device Management - MDM." Mobile Device Management (MDM) | MobileIron. N.p., n.d. Web. 25 June 2017. <https://www.mobileiron.com/en/solutions/mobile-device-management-mdm>.

"BYOD Portal - Self Service Enrollment and Management Portal for BYOD and corporate owned iPhone, iPad, Android, Windows Phone devices." BYOD Portal - Self Service Enrollment and Management Portal for BYOD and corporate owned iPhone, iPad, Android, Windows Phone devices. N.p., n.d. Web. 25 June 2017. <https://www.byodportal.com/>.

Lazar, Michael. "BYOD Statistics Provide Snapshot of Future." *BYOD Statistics Provide Snapshot of Future | Insight*. N.p., n.d. Web. 30 June 2017. <https://www.insight.com/en_US/learn/content/2017/01182017-byod-statistics-provide-snapshot-of-future.html >.

Beauchamp, Parker. "BYOD in the Workplace: Benefits, Risks and Insurance Implications." *The Huffington Post*. TheHuffingtonPost.com, 13 July 2016. Web. 01 July 2017. <http://www.huffingtonpost.com/parker-beauchamp/byod-in-the-workplace-ben_b_10973342.html>.

Meyer, Claire. "Bring Your Own Risk with BYOD." *Security Magazine RSS*. N.p., n.d. Web. 01 July 2017. <http://www.securitymagazine.com/articles/87016-bring-your-own-risk-with-byod>.

Lannon, Paul G., and Phillip M. Schreiber. "BYOD Policies: What Employers Need to Know." *SHRM*. N.p., 01 Feb. 2016. Web. 01 July 2017. <https://www.shrm.org/hr-today/news/hr-magazine/pages/0216-byod-policies.aspx>.

Lord, Nate. "The Ultimate Guide to BYOD Security: Overcoming Challenges, Creating Effective Policies, and Mitigating Risks to Maximize Benefits." *Digital Guardian*. N.p., 11 Oct. 2016. Web. 01 July 2017. <https://digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating>.

Phifer, Lisa. "Using a secure data container to separate work and play." *SearchMobileComputing*. N.p., Aug. 2012. Web. 01 July 2017. <http://searchmobilecomputing.techtarget.com/tip/Using-a-secure-data-container-to-separate-work-and-play>.

Mathias, Craig. "BYOD advantages: Save money, mobilize workers, embrace the cloud." ***SearchMobileComputing*****. N.p., Dec. 2012. Web. 01 July 2017. <http://searchmobilecomputing.techtarget.com/tip/BYOD-advantages-Save-money-mobilize-workers-embrace-the-cloud>.**

Mathias, Craig. "Enterprise mobility management options: MDM, MAM and MIM." ***SearchMobileComputing*****. N.p., n.d. Web. 01 July 2017. <http://searchmobilecomputing.techtarget.com/tip/Enterprise-mobility-management-options-MDM-MAM-and-MIM>.**

"TechnologyAdvice Buyer's Guide to Mobile Device Management ." ***TechnologyAdvice*****. N.p., 30 June 2017. Web. 01 July 2017. <http://technologyadvice.com/mdm-byod/>.**

Mathias, Craig. "Four BYOD challenges to consider before diving in." ***SearchMobileComputing*****. N.p., n.d. Web. 01 July 2017. <http://searchmobilecomputing.techtarget.com/tip/Four-BYOD-challenges-to-consider-before-diving-in>.**