Bring Your Own Devices

A Survey of BYOD Policies in the Workplace

Billy Short

11/2/2017

TABLE OF CONTENTS

Abstract

This document was created to understand how the implementation of a Bring Your Own Device (BYOD) policy will affect network infrastructure. There are many challenges to an Information Technology management team, more specifically those in charge of network infrastructure. BYOD may be defined exactly as it is, bring your own device. Employees may bring their own devices to work and may use them to connect to a secure network. This essentially includes all computing devices such as tablets, smart phones, laptops and many other mobile devices. Flexibility and mobility are huge factors that are driving the bring your own device movement. How will information technology management teams cope with this growing demand of resources needed to support the bring your own device policy? IT teams must ensure that at the very least, all most commonly used devices are able to flawlessly connect to the secure corporate network anywhere, anytime. In many cases, this must be seamless with other end-user devices, including laptops, phones and tablets. IT teams must also ensure the security, compatibility, and operability of these devices on the corporate network. Various operating systems are installed and updated on different devices. Network infrastructure must always be updated to be able to accommodate the latest technology, while still supporting traditional network infrastructure such as VoIP phones, fax lines and other wired infrastructure. In order to fully implement BYOD, a wireless internet connection must always be available and working in order to maintain flexibility, mobility and productivity for employees using their devices. Regardless of whether or not a corporation will endorse the idea of bring BYOD, all companies should have a BYOD policy in place. A BYOD policy will ensure that employees understand the security risks and confidentiality risks of bringing and using personal resources for company usage.

Bring Your Own Device policies are becoming more common. Information Technology teams will have to ensure that they accommodate these growing movements. This document will help teams understand how the BYOD policy will change their network infrastructure, why BYOD is the future of network infrastructure, and the risks and possible consequences of implementing BYOD in an enterprise organization.

Introduction

More and more companies and organizations are allowing employees to bring their own devices to work. In order to accommodate this, information technology management teams must be able and willing to adapt to the changing landscape to support all the different devices that employees may prefer to use. From smart phones, to tablets, laptops and other smart devices, infrastructure must be in place to allow for these devices to be successfully used in the workplace. How must a company set rules and boundaries for their employees in order to successfully implement a bring your own device policy? What must information technology teams do in order to support this in the workplace? How do companies deal with the ownership of the device? How do companies decide what is work related versus what is personal while working at and for the company on company time? Lastly, how do companies cope with the on-going security threat that pertains to bring your own device policies? The meaning of this document is to address the questions above, as well as discuss what a written policy to employees should include, and the advantages and disadvantages of organizations implementing a bring your own device policy (Gallagher, C., McMenemy).

What is BYOD ?

It is estimated that up to 74% of all companies and organizations are utilizing a Bring Your Own Device (BYOD) policy for its employees. This relatively new trend has become more and more popular for companies and is expected to continue to increase in the future. Figure 1-1 shows the development of BYOD in various countries (Steiner, P. (n.d.)). Although it is a relatively new concept in countries like the United States, the United Kingdom, France, Spain and Germany, BYOD has been widely adopted in other countries such as Brazil, Russia, India, Malaysia and Singapore. Based on this data, it is apparent that BYOD is a new paradigm in how employees work and what devices those employees choose to work with in order to do their job.

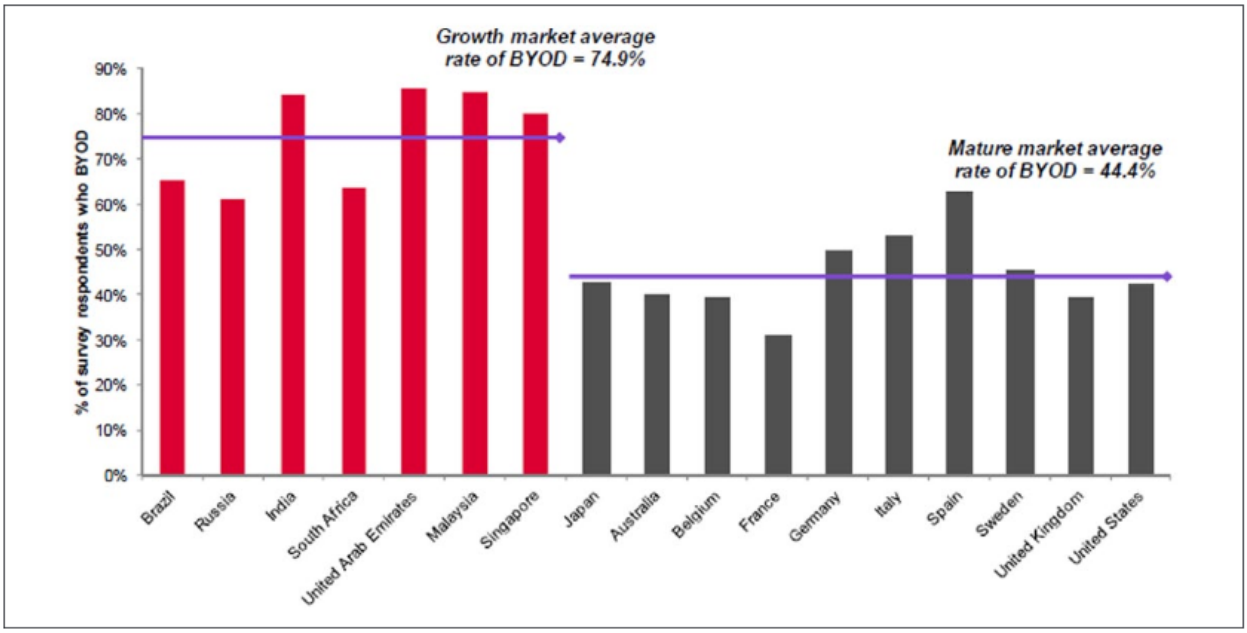

Figure 1-1

So what exactly is BYOD? Bring your own device refers to the permission of an organization to allow employees the ability to bring their preference of devices into the workplace for workplace use. These devices may include smart phones, tablets, computers, smart watches, and any other devices that may rely on wireless technology in order for employees to utilize them. With that

being said, this large growth of wireless technology means that information technology teams must have the wireless infrastructure in place in order to accommodate this influx of devices. A company essentially governs the way that employees are able to bring and use their own devices by requiring employees to read and sign a bring your own device policy. There are many different reasons why employees would want to bring their own devices into the workplace, as there are different reasons why employers would permit employees to bring their own devices for work purposes. There are also reasons why information technology management may deny permission to its employees to bring personal devices to work. The reasoning behind whether or not to allow employees to bring personal devices to work and access company material will be discussed in a later section of this writing. The more devices that are added to a network, the higher chance that there could be a breach or hole in the network security, so this must also be taken into account when discussing bring your own device policies (Olalere, M., Abdullah).

BYOD Policy Core Components

As mentioned above, the details included in a company-created bring your own device policy states how companies handle personal devices. BYOD policies vary from one company to the next. Typically, a policy's core components are unique to each company's information technology department, organization, or employee's wants, needs and requirements. After a threat assessment is conducted, any concerns, risks and threats are taken into account when creating a BYOD policy. Organizations must keep in mind the various advantages and disadvantages of implementing a bring your own device policy in order to understand what should be included in the policy itself. With that being said, security is typically the driving

factor in creating and issuing a BYOD policy. In order for an employee to begin to use personal devices for business purposes, the employee must read and sign the policy, which is usually during an employee's orientation or probationary period when they begin their position or accept a contract offer. By signing a policy, the employee is agreeing to the rules and regulations stated in the BYOD policy.

Aside from security, there are many other rules and regulations that are usually included in an organization's Bring Your Own Device policy. Other policy concepts may include an Acceptable Use section, devices and support section, reimbursement section, and risks, liabilities and disclaimers. Acceptable use refers to what an employee can and cannot do with their personal device while at work or in some cases, using their device for other prohibited activates. Devices and support refers to what types of devices are supported by the organization's infrastructure and are willing to continue ongoing support with. Reimbursement may include questions such as whether or not employee's are reimbursed for the devices they buy and bring to use for work purpose, or if these devices are lost, damaged or stolen. Any risks, concerns, liabilities and disclaimers may be included to ensure employees are aware of ideas or concepts of participating or using any BYOD devices for workplace use (Olalere, M., Abdullah, M. T., Mahmod, R., & Abdullah, A). This document will provide more detail on Acceptable Use, devices and support, reimbursement, and risks, liabilities and disclaimers in later sections.

Acceptable Use

An implementation of a Bring Your Own Device policy typically includes an acceptable use guidelines for its employees. Acceptable use refers to a set of rules or guidelines by an owner, in this case the information technology management team. Some of these guidelines may

include rules and regulations on how employees may access company network resources or internet and the way in which they should go about doing this. Many organizations require its employees to connect securely to network resources using an intermediary network such as a Virtual Private Network. A VPN ensures that the employee has a secure tunnel in order to connect to company resources securely via a remote connection. Acceptable Use also may refer to what the employee can and cannot access using company resources. An example of this is may be the growing issue of peer to peer torrents used to gain access to illegally copyrighted material. Activities such as this should not be used anywhere, especially in an organizational environment because legal actions may ensue. Because of the possibility of legal action and the threat of introducing viruses and other types of malware, many organizations proactively block well known peer to peer torrent or pirating, as well as close the most commonly used ports used for sharing these types of files. Most organization's acceptable use policy also requires that employees do not use company resources, including the company's internet service, to break or violate any laws, attempt to bypass any security measures that keeps network resources safe and secure, to ensure that employees actively monitor their company devices and keep them secure, and to report any suspicious activities with the user's account to information technology management. Organizations require its employees to sign an acceptable use document before they are permitted to access company network resources. Acceptable use is commonly included with a Bring Your Own Device policy to ensure safety and security of company and employee data and resources (Gallagher, C., McMenemy, D., & Poulter, A. (2015).

Devices and Support

Organizations are constantly changing and evolving. Information technology

management must adapt to company goals and visions in order to cope with these changes. With the growing number of devices available comes the growing need of network infrastructures to have the ability to support these devices. In regards to a Bring Your Own Device policy, many organizations limit the number and types of devices that employees are permitted to use for company purposes. An example of this is that an organization may only permit its employees to purchase and bring Android type mobile devices to access company resources due to infrastructure support limitations. By being transparent with network infrastructure limitations, employees know exactly what they can purchase that is supported by the company, resulting in less issues in learning about the devices and other technical issues. This can also help infrastructure teams to understand what areas of the network that they can improve on, such as adapting in the future towards support for other common devices such as Apple devices. Support for these devices and other information technology issues may be included with a help desk ticket system. For example, a user is having an issue with their company issued tablet. In order to receive support for this issue, the user must submit a ticket for requesting assistance for their device. A service level agreement (SLA) is attached to the ticket, requiring the help desk team to acknowledge the request ticket and provide the user assistance. The help desk ticket system helps the information technology team prioritize daily issues and provide customers with excellent customer support with their devices and other issues they may have. Another aspect about devices that information technology teams must perform is testing on potential devices that employees may bring to use as their company device. Penetration testing among other security testing should be performed to ensure that there are no security holes that the devices may open up in the company infrastructure to make resources vulnerable to attack or data breaches. Employees may be required to participate in end user training to be informed on system security

updates on cell phones, tablets, computers, and other mobile devices that employees may use. By having information of devices and support available to employees in the Bring Your Own Device policy, employees are better informed on what devices they can use with a company's infrastructure and how to receive support if they have any questions or concerns with their devices.

Reimbursement

When companies allow employees to bring their own devices for company use, what type of reimbursement is offered for those employees? A Bring Your Own Device policy should entail this information to the employee. Typically an organization offers to purchase the device that an employee may choose as their device to use for company purposes. Other times employees purchase the device of their choosing on their own, and are later reimbursed for their company purchase. One of the biggest concerns for an organization are how they handle certain ownership issues, such as who actually owns the equipment. What if an employee loses or damages the company issued equipment? The Bring Your Own Device policy dictates how these issues are resolved, and by signing this policy, the employee and organization agrees on how to settle these issues.

Risks, Liabilities and Disclaimers

Another core component that is commonly found in a Bring Your Own Device policy are risks, liabilities and disclaimers. There may be many potential risks in regards to allowing employees to use personal devices for company use. Devices may have email service set up that could contain confidential information such as company trade secrets or financial data. What if

this device was lost or stolen? A BYOD policy informs employees on how risks such as stolen or lost devices are dealt with. For example, an employee loses a company issued tablet. The first step is to contact information technology management to ensure that they are aware of this issue. If the tablet cannot be found via GPS tagging or other methods, the company may issue a remote wipe of the device, ensuring that valuable company information is not granted to anybody other than authorized employees or personnel. It is important that these steps are laid out and that the employee understands what needs to be done if a company issued device may possibly be lost or stolen to contact the information technology department as soon as possible to that measures may be taken to ensure confidential data stays safe and secure. Disclaimers may also be included within the BYOD policy. This may include repercussions towards employees from the company due to performing unlawful actions with company issued devices or knowingly participating in activities that violate laws by using company internet. With the implementation of a bring your own device policy, employees and their devices may bring unwanted risks and liabilities for the company. Some companies may weigh these risks and liabilities and may not be willing to implement a bring your own device policy due to this very reason. Risks, liabilities and disclaimers should be stated within the BYOD policy so that both employees and employers know the rules and procedures of issues pertaining to bring your own devices in an organization.

Advantages of BYOD

The biggest goal of an organization is to be successful and productive by meeting company objectives, visions and missions. Employees work to meet those business goals. Because of this, employee productivity is very important to organizations. One of the biggest

advantages of an organization that implements a Bring Your Own device policy is that it increases productivity from employees. No longer do employees have to adapt to a company's issued equipment. Users have the ability to choose what devices they prefer to use. This in turn allows employees to use whatever technology that they are most comfortable with, thus increasing productivity and morale of the employee. Employee satisfaction is very important because if employees are not satisfied in the workplace, this could lead to other issues in the workplace, decreasing the chances of meeting and reaching company goals and missions. In general, people purchase the "latest and greatest" technologies. The company benefits from this because newer devices have more security measures in place and have more features and capabilities that could further increase employee satisfaction, happiness, and overall productivity.

Overall, implementation of a bring your own device policy will help lower infrastructure costs. Because many BYOD devices are mobile devices, the need for added extensive wired networks decrease. Wired networks are expensive to contract out and install. The material and networking equipment needed are more expensive and much more limited to where it can be installed than installing wireless networks. The direct result of a decrease in need of wired networks is the increase in need of a more extensive wireless network. Wireless networks must be fast, always on and available, secure, and allow for employees to access company information whenever they require it. The advantage of the implementation of bring your own devices is that with wireless devices, the costs of installing more traditional networking methods are less than that of wireless networking methods, thus saving an organization money.

Because employees are able to choose the devices that they prefer to use in an BYOD environment, IT support required for these devices are typically less than if a company forces

devices on its users. Employees require less information technology support of a device that they are comfortable and familiar with versus devices and equipment that a company issues to an employee that they have never used before. This means that the employee must take the time to understand the new technology and become comfortable with it, potentially limiting the user's productivity until the user is comfortable with the technology. This is opposite when an employee is permitted to use equipment and devices that they are used to, requiring less IT support for these devices. Less end user training is required, providing less strain on the IT support team.

Many people must carry several technology devices with them while traveling or just in general away from the home. With BYOD, many employees have the ability to combine these devices into one, utilizing their work phone as their business and private phone, or their work computer as home and work purposes. A BYOD policy in an organization may help employees cope with the rapidly increasing amount of devices by overall decreasing the amount of technology devices needed. Many employers provided added incentives to its employees by allowing them to use their work cell phones as their personal cell phone. This means that employees do not have to pay for a cell phone bill because the company is paying for this. This increases productivity because of the added flexibility that employees have with their devices and potentially faster email responses due to allowing them to use their business cell phones personally. The simplicity of combining technology devices that is provided by a BYOD policy benefits both the company and employees.

Disadvantages of BYOD

Although there are numerous advantages of implementing a Bring Your Own Device

policy for employers, there are also some disadvantages that should be discussed when making the decision to implement BYOD. Security is by far the largest concern for employers when deciding whether or not they should implement bring your own devices for their employees. Seventy - eight percent of organizations information technology managers claim the biggest hesitation of implementing BYOD in their organization is due to security (Beauchamp, P. 2016, July 13). Security is the primary concern for organizations because organizational data is only meant for authorized people to access. Viruses and data leaks are concerning issues for employers. With the growing number of devices that are introduced to a company network due to employees being able to use their device preferences, information technology management must ensure security measures are in place to protect confidential data and organization information. Bring your own device policies may state certain precautions or minimum security requirements of devices to employees. Some of these security requirements may include that all cell phone devices must have a screen PIN code or password in order to access or unlock the phone. Many phones now offer biometric security measures as well, providing further security for these devices and limiting the possibility of unauthorized access to company resources. Also, firewalls are not present on many mobile devices, which may create holes or vulnerabilities in a network when the device connects to it. (Li, P., & Yang, L). Unsecure wireless connections can help intruders access confidential data and information that is present on some of these BYOD devices. All of these security issues must be taken into account and addressed by the organization before implementing a bring your own device policy.

Another potential disadvantage of a BYOD implementation is the cost of devices. The company must lay out who will purchase the devices and on whether the employees are reimbursed for their devices. If the company does not reimburse for employee devices, then the

cost is an advantage for the user. Repairs and depreciating of the latest and greatest devices may not be alluring to some employees.

The more devices that are permitted to be used by employees may potentially mean more issues and changes required to the wireless infrastructure to accommodate these devices. Many employers limit the types of BYOD devices that an employee may purchase and use for company purposes. The reason is that not all devices are the same. Different devices use different operating systems, and different operating systems may interact with the existing network infrastructure differently than others, or have different requirements needed. Information technology management must ensure that devices that employees buy and bring for company purposes are able to be used with existing infrastructure, or adjusted in order to support those devices. A BYOD policy typically dictates what devices an employee may bring to work for business purposes for this very reason.

Changes in the company at an employee level addresses another disadvantage of BYOD. When an employee leaves, who does the device that the employee used for both personal and business use belong to? How does a company know that the employee deletes all the information from the device before moving along to their next career opportunity? For example, an employee had a high level position at a company and had access to a lot of confidential information in emails exchanged from various employees in the company. That employee leaves the company, had purchased the phone to use for business and personal use. How can an employer ensure that company information, user passwords, and data be off the phone? When an employee moves from one position to another within an organization, that user may not need access to the information from the previous position. Does the phone number belong to the

employee or the employer? How an organization deals with these changes should be outlined in the BYOD policy signed created by the organization and agreed upon by the employee.

Mobile Device Management (MDM)

When an organization is deciding whether or not to implement a Bring Your Own Device policy, many different issues must be taken into account. How can an organization ensure that an employee is using their device for work related activities during work hours? When a device is lost or stolen, data and other confidential information must be kept confidential and safe. While employees are required to follow the minimum security requirements such as using a screen pass code or biometric security measure, the device still has confidential company information on it. To help ensure that employees are following the rules and requirements that are stated in the BYOD policy, many companies implement a Mobile Device Management system in conjunction with BYOD. A mobile device management system is an administrative tool used by organizations to monitor, deploy, secure, and integrate company regulations onto mobile devices, such as smart phones, tablets, and laptops. In regards to BYOD, an MDM solution may be placed on company owned and issued devices or personal devices. Most common devices support MDM and can be deployed wirelessly to remote devices. Companies can target certain devices within the organization to use MDM to monitor, secure and manage an employee's mobile device. (Steiner, P. (n.d.))

Mobile device management systems use a server to client relationship to push out any security updates, company changes, file transfers and many other uses for company issued mobile devices. MDM systems helps organizations remind employees that they are using

company issued devices and that their devices have company information on it. An MDM can limit what applications a user can install on their device, especially applications that are known to have security holes or issues. For example, an employee may not be using their mobile device for work purposes. An MDM can show exactly what an employee is doing on their phone during work hours, thus providing accountability for company assets in the field. Reminders can be sent to user's to install the latest operating system updates on their devices to help prevent security holes that may lead to data loss or data breaches. If an employee contacts the information technology management team and says that their cell phone has been lost or stolen, the IT management team can perform a remote wipe on the device, preventing unauthorized access to the device. If an employee chooses to leave a company or the company terminates the user, but the user had purchased the device themselves, then an MDM system can choose which files contain company data and remove them from the user's device. Any company passwords or information can be remotely removed as well, leaving only personal data and information on the device.

An MDM can interact with Microsoft Exchange server to access company email to prevent spam and other potentially dangerous attachments from spreading from one account to another. Potentially dangerous emails are automatically set into their own quarantine container, limiting the potential damage the email can cause. An MDM may also prevent users from accessing certain sites by using a secure browser. This is typically created by the organization to block known unsecure website access to users. Application catalogs may be created and employees can only choose from approved applications to install on their phone, preventing spyware or adware that can be found on many applications. Data usage may also be tracked, preventing users from using too much data and causing large overage fees for the company. In

order to prevent users from connecting to unsecure access wifi connections, MDM's can limit these to pre-determined access point SSID's, ensuring that employees do not connect to potentially dangerous wifi connections. A remote VPN connection can be installed using an MDM, creating a secure tunnel for employees to connect their device to and access company resources safely. There are many risks and liabilities that come with the introduction and implementation of bring your own devices policy. A mobile device management system can help organizations ensure that confidential company information stays safe and secure on a wide range of common mobile devices, including tablets, cell phones, and laptops (Lucas, S. (n.d.)).

Example of BYOD Policy

Here is an example of a BYOD policy of a company named Networks Unlimited Inc:

Acceptable Use

- Our organization allows business use of activities that directly or support the business of Networks Unlimited Inc
- Networks Unlimited Inc does not allow personal use on company time. Limited personal communication or recreation, such as reading or game playing may be permitted outside of working hours.
- Employees are prohibited from accessing certain websites during work hours/while connected to the corporate network at the discretion of the company that are known to have security vulnerabilities. These websites can be changed without notice.
- Devices may not be used at any time to:
    - Store or transmit illegal documents or material
    - Store or transmit other company issued material or confidential information
    - Harass others
    - Engage in illegal activities
    - Other activities that may hurt company image or against our morals or values
- The following apps are allowed: Productivity apps such as Office Applications, Weather apps, etc.
- The following apps are not allowed: Facebook, Myspace, (constantly changing sites).
- Employees may use their mobile device to access company-owned resources such as company email, calendars, contacts, and documents
- Networks Unlimited Inc has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.

Devices and Support

- Smartphones including iPhone, Android, Blackberry and Windows phones are allowed
- Tablets including iPad and Android are allowed
- Connectivity issues are supported by IT - please fill out help desk ticket and we can assist you appropriately
- Devices must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network.

Reimbursement

- The company will reimburse the employee for a percentage of the cost of the device
- The company will pay half of the phone/data plan
- The company will not reimburse the employee for roaming, plan overages, or long distance fees.

Security

- In order to prevent unauthorized access, devices must be password protected using a PIN or biometric features of the device.
- Passwords must be at least six characters and a combination of upper- and lower-case letters, numbers and symbols. Passwords will be rotated every 90 days and the new password can't be one of 15 previous passwords.
- After five failed login attempts, the device will lock. Contact IT to regain access.
- Employees are automatically prevented from downloading, installing and using any app that does not appear on the company's list of approved apps.
- Smart phones and tablets that are not on the company's list of supported devices cannot connect to the network.
- Employees' access to company data is limited based on user profiles and are closely monitored.
- The employee's device may be remotely wiped if their device is lost or stolen, quits his/her position or is terminated, or a virus, data or policy breach is detected that could affect other users adversely.

Risks/Liabilities/Disclaimers

- Networks Unlimited Inc reserves the right to disconnect devices or disable services without notification to the user.
- Lost or stolen devices must be reported to the company immediately.
- The employee is expected to use his or her devices in an ethical manner at all times and adhere to the company's acceptable use policy as outlined above.
- The employee is personally liable for all costs associated with his or her device.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- Networks Unlimited Inc reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

Please sign this form and return to your IT infrastructure team.

Conclusion

More and more organizations are deciding to implement Bring Your Own Device in the workplace. Every organization is different and each has its own unique situation. Because all organizations are different, employers should weigh all aspects of BYOD detailed in this writing to decide if a BYOD environment is best for the organization. A BYOD policy is created by the employer to detail the rules and regulations in place that employees must sign and agree to in order to access and use various company resources including company issued devices, networks, folders, and internet. A BYOD policy may include acceptable use of how employees should use their company issued devices. While there are many advantages to implementing a BYOD environment, organizations must understand the risks, liabilities and disadvantages, especially security, when deciding whether BYOD is right for the organization to reach its goals.

References

Armando, A., Costa, G., & Verderame, L. (n.d.). Securing the "Bring Your Own Device" Paradigm. Retrieved November 1, 2017, from http://ieeexplore.ieee.org.jproxy.lib.ecu.edu/document/6838866/

Beauchamp, P. (2016, July 13). BYOD in the Workplace: Benefits, Risks and Insurance Implications. Retrieved November 2, 2017, from https://www.huffingtonpost.com/parker-beauchamp/byod-in-the-workplace-ben_b_10973342.html

Best Practices: Bring Your Own Device Policies for Small Businesses. (n.d.). Retrieved October 5, 2017, from https://identity.utexas.edu/id-perspectives/best-practices-bring-your-own-device-policies-for-small-businesses

BYOD Policies: What Employers Need to Know. (2017, May 19). Retrieved September 1, 2017, from https://www.shrm.org/hr-today/news/hr-magazine/pages/0216-byod-policies.aspx

BYOD: Bring your own device. (n.d.). Retrieved September 16, 2017, from https://www.ibm.com/mobile/bring-your-own-device

Gallagher, C., McMenemy, D., & Poulter, A. (2015). Management of acceptable use of computing facilities in the public library: Avoiding a panoptic gaze? *Journal of Documentation*, *71*(3), 572-590. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/1676554922?accountid=10639

Hassell, J. (2012, May 17). 7 Tips for Establishing a Successful BYOD Policy. Retrieved November 01, 2017, from https://www.cio.com/article/2395944/consumer-technology/7-tips-for-establishing-a-successful-byod-policy.html

Is Bring Your Own Device BYOD Right for Your Enterprise? (2016, June 20). *Bioterrorism Week*, p. 130. Retrieved from

http://go.galegroup.com.jproxy.lib.ecu.edu/ps/i.do?p=HRCA&sw=w&u=gree96177&v=2.1&it=r&id=GALE%7CA455685284&sid=summon&asid=6ba12a40acc9bed6e4193980adb5a92f

Lee, J.,Jr, Warkentin, M., Crossler, R. E., & Otondo, R. F. (2017). Implications of monitoring mechanisms on bring your own device adoption. *The Journal of Computer Information Systems, 57*(4), 309-318. doi:http://dx.doi.org.jproxy.lib.ecu.edu/10.1080/08874417.2016.1184032

Li, P., & Yang, L. (2017, March 08). Management strategies of Bring Your Own Device. Retrieved November 1, 2017, from https://www.matec-conferences.org/articles/matecconf/abs/2017/14/matecconf_gcmm2017_02007/matecconf_gcmm2017_02007.html

Louise Bennett, Henry Tucker; Bring Your Own Device, *ITNOW*, Volume 54, Issue 1, 1 March 2012, Pages 24–25, https://doi-org.jproxy.lib.ecu.edu/10.1093/itnow/bws010

Lucas, S. (n.d.). The Pros and Cons of a Bring Your Own Device (BYOD) Policy. Retrieved September 15, 2017, from https://www.thebalance.com/bring-your-own-device-byod-job-policy-4139870

Net WorkBy Tony Bradley,PCWorld|Dec 20, 2011 10:42 PMPTAbout | Practical IT insight from Tony Bradley, & Tony Bradley,PCWorld|Dec 20, 2011 10:42 PMPT. (2011, December 21). Pros and Cons of Bringing Your Own Device to Work. Retrieved November 2, 2017, from https://www.pcworld.com/article/246760/pros_and_cons_of_byod_bring_your_own_device.html

Olalere, M., Abdullah, M. T., Mahmod, R., & Abdullah, A. (2015). A Review of Bring Your Own Device on Security Issues. *SAGE Open, 5*(2). doi:10.1177/2158244015580372

Steiner, P. (n.d.). Going Beyond Mobile Device Management. Retrieved from https://ac.els-cdn.com/S136137231470483X/1-s2.0-S136137231470483X-main.pdf?_tid=cf0f0102-c80d-11e7-b0a2-00000aacb35d&acdnat=1510534909_90c5a92e59f216dd6faccb46e90043ff