**IDS 493**

**Remix #6**

**BYOD POLICY**

Project Report

Old Dominion University

CYSE 250 Cybersecurity Programming and Networking

December 6, 2021

Diamond Williams, Lawrencia Agyemang, and Tim Schlang

**Introduction**

## The BYOD policy or otherwise known as Bring Your Own Device is a common rule by companies that permit employees to use their own devices in work related matters. Employees can use their mobile phones, laptops and computers to send and receive mails and other matters. Any company considering this approach has to consider the positive and negative sides and determine what fits its operations. It is a common trend in the corporate world but requires delicate balance to avert compromising the company’s data and privacy. On the other hand, it is a scenario where employees are offered convenience and the company saves on purchase of equipment and other work related machines.

## Generally, the BYOD policy has the advantage of helping a company save. It also has the benefit of helping employees find it easier to adopt into their work environment and a less steep learning curve. It also leads to more productivity because of the high employee morale arising from the ‘privacy’ window. The policy also has the capability of up-to-date technology because of frequent upgrades.

## 

## 

## Statement of the Problem

With the many benefits the BYOD policy has, the cons are still a major challenge. The work from home phenomenon has quite been on the rise which further puts a company’s system at a higher risk. This is because the employees working from home are somehow ‘unmonitored’ as compared when working from the office. Further, IT staff might find it hectic to offer personal support for all employees as compared when in the office.

## However, there are cons in this policy. The most common one is the threat it poses to company data. Duet to the personal use, many employees may not be familiar with cyber security threats thus exposing the company. The threats may arise from phishing, unregulated system upgrades, use of different software among others. It may also lead to the IT department not being productive because of the constant calls to look into employee devices, the policy may also be counterproductive if employees are using different devices, are not willing to use a standard software, or do not have a device.

**Implication**

Ransomware is a challenge BYOD faces. The risk involves hackers demanding a ransom to ‘release a company’s data which they have encrypted. Using your own devices is prone to such security threats. Many employees may not be aware of the ins and outs of IT. Thus, they may follow links, suspicious emails and when they realize it, the software has already taken over and the company’s data is on the line. Because many employees use the devices to do other personal stuff, this may increase the chances of such a threat. And if it is outside work hours, the threat has spread probably to the entire system even before the IT department comes to realize what is happening.

Phishing is another challenge BYOD has to contend with. Statistics show that since 2020, cyber-related crimes have been on the rise. The FBI reports that the rate has increased four times while the losses hit the $1 trillion mark. With people working from home it means they are more vulnerable from attacks especially if they have limited cyber knowledge and receive minimal IT support from their companies. Further, if they are using their own devices, the threat could be higher.

Phishing has been one of the common strategies the attackers use. Data opines that there was 667% increase in phishing. Over 40% of workers say they in one or another fell victim to this and put their companies in cyber-crime danger. A classic example is in 2020 when Twitter lost $100 while a Texas school lost $2.3 million due to phishing. All these point to the problem the BYOD policy faces especially if coupled with the work from home system.

BYOD comes with a DDoS challenge. It means a distributed denial of services. The strategy used here is using devices previously hacked or having malware. With each employee having their own devices, this challenge is aggravated. Meaning if employee A has a hacked device, the hacker will find it easy to infiltrate and disrupt other machines in the network. The overall result is access to company data and other crucial information which might be used negatively. A machine may be compromised and the hacker continues with the activity without the user knowing. This puts the company at high risk. Artificial intelligence is being used to carry on these attacks thus making BYOD policy weaker especially if a company has weak interception mechanisms.

Technology nowadays comes interconnected with other 3rd party apps and software. In one company you will find they use several 3rd party apps which opens up the company’s system to more risks. With the use of personal devices, the employees are also using other third party apps to run their daily lives. This puts the company in more danger. Data shows that US’s 30 top-most ecommerce retailers' systems have a weak point and are connected to over 1,000 resources. The magnitude of such a compromise in such a web is massive if any hacker finds a way into it. The situation could be made easier for say company A if one employee is using one of the resources thus opening up the company to a hacker’s field.

Cloud computing has also come with its challenges. The combination of work from home and BYOD policy has a serious security threat in cloud computing. The threat arises from everyone accessing the cloud, where hackers can scan for those with no passwords or with weak ones. The resulting damage could be great if it is a financial institution or blue chip company. Nevertheless, any hack is expensive because of the data loss or the ransom that may be demanded to restore back the damage.

**Effects to Work Environment**

Despite BYOD being a near perfect policy, it has negative and positive effects on the work environment. Some of its positive impacts are;

**Positive Effects**

* Increased productivity because each employee understands their device better
* Increased technology and efficiency due to the constant software updates
* Freedom to use referred systems and software without being forced to learn a new system
* Employees enjoy convenience especially when working from home instead of carrying and switching on multiple devices.

**Negative Effects**

* The risk of losing data when devices are stolen or if the employee leaves a company. It may expose the company to unprecedented risks if the data is used negatively.
* Legal issues for the company if the data is leaked or accessed by unauthorized persons
* There is a high security risk because not all employees understand the danger posed by some downloads, emails, and links.

**The details about the hardware (your machine) and software (include version) used in the project**

I used the machine with the following specifications Ryzen 7 3800x with 4 tb of storage and a 3080 ti for graphics and I used python idle software

I used Python idle for the software on macOS. The python idle shell version was 3.10.0. The hardware I used was a hard disk. The hard disk is the non-erratic part which suggests the data is taken care of and it doesn't get out when the system is shut down. For instance, we had the option to deal with python coding and save the shell document. The hard disk contains an electromagnet surface which is used to store huge snippets of data and can be gotten to with no issue.

**The results**

The machine gave built-in function questions. Each question will help determine if the user is able to log in. the first question will ask “is your system fully updated”?. If “Yes” is selected then the machine will give the second question to the user. Next, “Yes” will be selected again for the second question. Two correct answers in a row (yes) will give the user a network code. The user can now proceed with access to the system. On the other hand, if “no” was selected, then the user would need to contact the network administrator. An administrator will address end-clients issues and guarantee high framework accessibility. They are responsible for staying with a PC’s network running consistently and expertly.

Text

Description automatically generated

Text, letter

Description automatically generated**Conclusion**

Despite the challenges posed by BYOD policy, the threat is still there and may continue unabated. It is partly because of the pandemic that has increased the work from home routine and daily advances in technology. Further, there has been an increase in digital service demand causing many individuals to turn online. Many companies are also offering part of their services online such as learning institutions, ticketing companies, payment platforms, and governments, among others. The threat can only be minimized by employing tough measures.

Appendix

**Purpose**

The Purpose of the BYOD policy, or also called Bring Your Own Device is to allow representatives to utilize their own gadgets in business-related matters. Those exercises incorporate errands like getting to messages, associating with the corporate organization, and getting to corporate applications and data. This strategy sets up rules for worker utilization of actually possessed electronic gadgets for business-related purposes.

**Outline and Contents**

1. **BOYD Policy Introduction**

Introducing the cybersecurity problem and summarizing the policy within the business work field.

1. **Statement Of The Problem**

It might likewise prompt the IT office not being useful in light of the consistent calls to investigate representative gadgets, the approach may likewise be counter-useful in caseworkers are utilizing various gadgets, are not able to utilize standard programming, or don't have a gadget.

1. **Implications**

Since numerous representatives utilize the gadgets to do other individual staff, this might expand the odds of such a danger. The danger implies programmers requesting payment to deliver an organization's information which they have encoded.

- Ransomeware

- Phishing

1. **Effects To Work In Environment**

Notwithstanding BYOD being close to consummate arrangement, it has negative and constructive outcomes to the workplace.

**4.1. Positive Effects**

**-** Constructive outcomes expanded efficiency on the grounds that every representative comprehends their gadget.

- Better-Expanded innovation and productivity because of the steady programming.

- Refreshes the Opportunity to utilize alluded frameworks and programming without being compelled to get familiar with another framework.

-Representatives appreciate comfort particularly when telecommuting as opposed to conveying and turning on various gadgets.

**4.2 Negative Effects**

**-** It might open the organization to extraordinary dangers assuming the information is utilized adversely.

-The danger of losing information when gadgets are taken or then again assuming the representative leaves an organization.

- Legitimate issues for the organization assuming the information is spilled or gotten to by unapproved people.

- There is a high-security hazard in light of the fact that not all workers comprehend the risk presented by some downloads, messages, and connections.

**5. The details about the hardware (your machine) and software**

The python idle shell version was 3.10.0. The hard disk contains an electromagnet surface which is used to store huge snippets of data and can be gotten to with no issue. We used the machine with the following specifications: Ryzen 7 3800x with 4 TB of storage and a 3080 ti for graphics and used python idle software.

**6. Results**

The machine gave built-in function questions. The first question will ask “is your system fully updated”? If “Yes” is selected, next, “Yes” will be selected again for the second question. Two (yes) give access to network code. If “no” was selected, network administrator will address end-client’s issues and give access.

**7. Conclusions**

Despite the challenges posed by BYOD policy, threats may continue unabated. Working-from-home routine and daily advances in technology contribute much. Increase in digital service demand has caused many individuals to turn online. Companies joining the league of online service has seen the threat grow further and can only be minimized by employing tough measures.