The Cyber Collective
Enhancing Security Mindfulness
www.thecyco.com

SECURITY IN A PANDEMIC: HOW ORGANIZATIONS CAN MAINTAIN PRODUCTIVITY AND SECURITY IN A BYOD ERA

February 2021

1.0. INTRODUCTION

You ever heard of the '*Bring Your Own Device*' (BYOD) policy? It is a policy where organizations allow employees to carry out official duties and access company information using their personal devices. This includes bringing the devices to the work place, and working on them from home? Sounds familiar?

It is a popular practice; about 59% of organizations practiced it as at September 2020, TechJury has some interesting BYOD stats; you can view them here. Due to the COVID-19 pandemic, it also now appears to be a practice that will not be going away any time soon. Organizations are especially into this policy because according to an article on staffbase.com, it not only increases employee productivity but it also saves the enormous cost that would be acrued should a company attempt to buy work place devices (mobile phones and PC) for all their employees.

As reasonable as the advantages of BYOD are, this policy still isn't without its challenges; security challenges to be exact. And with the pandemic now forcing most of the world's work froce to work from home, BYOD has become more widespread, and even more dangerous.

2.0. CYBERSECURITY RISKS OF BYOD

According to Cimcor, when organizations make the decision to adopt BYOD policies, most of them are not thinking 'security' in those moments. It is mostly out of a drive to increase productivity and cut costs! However, this non-consideration doesn not make the associated risks go away. In fact, BYOD policies completely put the *Confidentiality* and *Integrity* of an organization's data under great risk, violating 2 pillars of the CIA security traid. Some of these risk factors include:

a. Third-Party and Pirated Applications

From third-party apps given undue read/write permissions to a user's device, to modified APKs, to pirated PC software; these are some of the many avenues through which sensitive data gets compromised.

Most enterprise apps (such as Microsoft and Adobe products) require paid access which users shy away from. In the event that an organization does not make available these software and services, users end up going for free pirated versions which are easily obtainable. Beyond data breaches and modification which could occur as a result of employees using pirated software to access sensitive company information, organizations are also at risk of legal fines and loss of reputation when associated with piracy activities. This blog post explores the dangers of software piracy in depth.

b. Rooted Mobile Devices

Rooting or Jail-Breaking a mobile phone means by-passing all restrictions and limitations that cell phone manufacturers may have placed on a device. It gives the user unlimited modication and configuaration access to the device. Some of the security implications of jail-breaking or rooting include inability to run updates and by extension, increased susceptibility to virus and other malware attacks. This means sensitive files being accessed on rooted devices might as well be spread out in public.

c. Unsupervised Child Access to Devices

One thing that has surely seen massive increase as a result of the pandemic is increased screen time for kids. This is as a result of virtual schooling, but also mostly because it's the safest way for kids to safely have some form of human interaction. Digital devices are now also the new baby-sitters, because they keep the little ones engaged long enough for the parents to get some work done.

It is therefore not uncommon for older folks to hand over their devices to kids to play with. Noble and convinient as the gesture is, it is not at all secure. Kids lack of cyber awareness can easily lead to drive-by attacks which could result in virus infections, ransomware attacks, etc.

d. Use of Insecure or Public WiFi

Whether it is because constantly working from a coffee shop (while using their WiFi) compromised a user's device, or neglecting to change the default username and password on their home router compromised their network; it is never a good thing when an organization's data is accessed over an insecure network. It is one of many famous recipes for a data breach.

e. Poor Security Awareness/Hygeine

According to an article by ZDNet, human error is reportedly responsible for the worst data breaches. What this implies is no matter how good your technical defenses are as an organization, you are only as secure as your most insecure human link!

It does not matter if an organization has the best data protection policies around; their cybersecurity is basically non-existent if they also have a BYOD policy and their employees frequently visit insecure websites, have poor passoword practices, do not use Multi-Factor Authentication (MFA), can not recognize a phishing email, etc.

3.0. MITIGATING BYOD RISKS

The good news is, BYOD is not hopeless and can actually be a great assest if managed properly. We discuss some ways organizations can best handle BYOD and Remote Worker policies.

a. Employ the use of File Integrity Monitoring software

File Integrity Monitoring (FIM) software regularly check on system files/states and compare them to previous versions. They are designed to flag down and send intrusion alerts the moment unauthorized or unusual changes are detected. So in the event that a device is infected with malware, FIM software can detect them in a timely fashion and alert you to promptly handle it before it negatively impacts your network. Organizations should invest in FIM software in order to effectively manage all devices on the network.

b. Protect all Enterprise Apps with Single-Sign-On (SSO) feature

A crucial benefit of SSO according to Cisco is that it ensures companies deal with fewer help desk requests for things such as password resets, lost passwords, etc. It therefore eliminates non-productive tasks while also saving support cost.

c. Use of Mobile Device Management solutions

Organizations can use Mobile Device Management (MDM) solutions to remotely monitor the security of an employee's device. When coupled with FIM software, an optimal level of control can be established. In the event that an employee’s device gets stolen or compromised, MDM can also be used to remotely wipe the device before any sensitive data on it gets stolen.

d. Consistent and Relevant Staff Trainings

Untrained employees can be the worst insider threats an organization can face. Some things to consider when organizing employee awareness trainings:

i. How to recognize phishing and other social engineering threats.

ii. Good password practices and the need for password managers.

iii. How to maintain staff values and attitudes that align with the organization's mission and ethics.

iv. The importance of VPNs and regular data backups.

v. The need to only download apps from official app stores and never third-party apps from websites or randomly distributed APKs.

vi. Ensuring employees receive regular email reminders with cyber hygeine tips on how to stay safe online.

4.0. CONCLUSION

The entire concept of BYOD is great and the advantages are undeniable, but so also are the risks involved. However, if organizations take out the time to invest in mitigation measures to balance out the risk factors, it would work best for both employers and employees. So, are you a manager or owner of an organization that has a BYOD policy? Well now you have a few more tricks up your sleeve!

REFERENCES

https://techjury.net/blog/byod/
https://staffbase.com/blog/six-advantages-byod-bring-your-own-device/
https://www.cimcor.com/blog/7-scariest-byod-security-risks-how-to-mitigate
https://www.justthetips.io/pirates-of-the-internet/
https://www.imobie.com/android-tips/disadvantages-of-rooting-an-android.html
https://www.zdnet.com/article/training-what-training-workers-lack-of-cybersecurity-awareness-is-putting-the-business-at-risk/
https://byod.cioreview.com/news/how-to-mitigate-byod-risks-and-challenges-nid-20825-cid-91.html
https://www.baselinemag.com/security/tips-for-mitigating-byod-security-risks.html
https://www.addictivetips.com/net-admin/file-integrity-monitoring-software/
https://www.cisco.com/c/en/us/products/security/what-is-single-sign-on-sso.html#~how-sso-works