**EMCS2210: Privacy and Personal Data Protection**

Pre-Work: Assignment - BYOD Program

Brian Russel Davis, [brian\_davis@brown.edu](mailto:brian_davis@brown.edu)

*Your CEO has asked that you provide recommendations on whether your company should implement a BYOD Program. The company is a public tech company that has over 800 employees. The CEO would like you to consider cost, privacy, legal, security, roll out and support the pros/cons of going to a BYOD model.*

*Write an analysis addressing the CEO’s concerns and outlining a final recommendation.*

**Position Summary**

BYOD ( Bring Your Own Device ) is a popular trend with startups in our new tech driven economy. However, as the Chief Security Officer I have assessed the pros and cons and believe it is not a fit for PAX. We operate in a highly competitive industry that is not fully legal from federal standards and need to maintain higher than normal levels of security, data integrity and confidentiality. A BYOD program makes achieving these goals challenging if not impossible.

**Implementing Device Security**

Keeping a device that contains PAX information, code, communications, strategic plans and financial information free from malware and spyware is absolutely essential. In order to achieve this type of security on a laptop or a phone the IT Department would need to have root level administrative access to the machine or device. A device owned by an employee ( and not the company ) would already have an administrative account set up. So even if PAX IT could set up an account on the device, the owner’s admin account could override the PAX IT admin access and subsequently compromise the integrity of the device and the information on the device.

**Types of Data PAX Needs to Secure**

There is more than just corporate run of the mill communications on any given PAX device. Since the team communicate cross functionally with hardware engineering, software engineering, legal, product and a myriad of trusted 3rd party vendors. In each type of device and for each type of information format, there may be a different type of storage medium. Each device and operating system ( and versions of those respective operating systems ) may handle ephemeral data differently, for example. A matrix that spelled out the risk posed to each and every type of information according to format, for every possible device, by operating system and by version would be close to impossible to construct. When I worked at NASA I built a prototype of a browser that would be able to do some of this with AI but it was highly experimental, and once again requires a great deal of control.

**Liability**

In terms of liability for the safety of the information on the device it goes both ways. What is the liability for an employee who allows information on the device to be exposed to an unauthorized third party? What is the liability of the company when an attacker uses an unsecured PAX server to access an employees personal device? If PAX is attacked, and the devices are attacked PAX’s liability may extend not only help fix, replace or repair the employees devices but also networks, devices or computer systems that are connected to the employee’s devices. The liability can snowball very quickly especially when user data it added into a catastrophic event or if the event involves criminal activity.

**Privacy and Confidentiality**

We have established that in order for PAX IT to adequately secure the device we need to have root access. Not only that but we need to ingest and analyze the communication between the device and the network. So, what happens to all the information that is pulled into the PAX ecosystem from employee’s device that may not be business related? Like if they are using their to date?

**Breach Procedure**

Lastly ( but not least ) what happens when there is a breach? If an employee device has been compromised or has compromising data on it, does PAX take the device away from the employee? What happens if the proper course of action it wiping all the devices that have been compromised and starting again, for instance in the event of a Wanna Cry Attack? Who is going to pay the cost of restoring all the data and how does the company propose it would restore data that they had no knowledge of that is personal to the employee? This creates a conflict of interest that has no easy remedy ; One that pits the personal interest of the employee against the interest of the company, it’s users and shareholders.

**Summary**

Securing the personal device of an employee is not impossible, however the effort and risk associated with securing it might not be tenable. Many small companies tend to think that at BYOD policy is a cost saving technique, but I disagree. The savings gain in not having to buy devices will be eaten up with cost of analyzing files, implementing custom software, paying staff to implement procedures and dealing with the inevitable breach.