Assignment 7 **Tyler Wilding**
COSC 4426 Due Date: 06/11/16
Prof. Biocchi –
TA: – –

Mobile Device Policy

1. Cost of purchase and maintenance of the device is the sole responsibility of the employee, a device will not be provided by the company nor will any replacement costs due to damage or increased service charges be provided.
2. The device must comply with IT's security standards. This includes but is not limited to: installing the latest updates, not installing unsafe applications, etc. These standards can be subject to changes at any time without notice.
3. Employees must attend monthly security training seminars.
4. Devices will be inspected by IT workers on a routine basis with prior notice, however in the case of a serious security event this advanced notice may be foregoed.
5. Devices will have software installed that allows for remote-wiping of the device, this also includes the ability to view or modify any files on the device. The company is not responsible for any damages and can exercise these abilities at any time without warning.
6. Accessing the company network through any potentially unsafe third-parties such as VPNs or Proxies is strictly forbidden.
7. Lost or stolen devices must be immediately reported to IT staff.

Rationale

My reasoning for not having the company provide cellphones to the users is that while it may slightly increase the security of the company, not only is it incredibly inconvienant and expensive because now all of the responsibility is on the company, but in the grand scheme of things I don't think it matters. Mobile devices are getting more vulnerable as they get more popular. Everyone having a company provided device is not going to make the device more secure, the only thing that will is the user being more educated and installing the latest updates. As it is, only 19% of Android users are on the current version of Android showing how 80% of people using an Android phone are missing out on very large security patches. This is why I make it nessecary for the users to attend security seminars, users will have to learn about how to safely browse the internet, how to identify safe and unsafe applications, etc. This education is much more beneficial and provides a bigger return on investment for the IT department.

However there are even more obvious issues than this, no matter what brand or version of android you are running, whether it is from the company or not it doesnt matter because recent hardware concerns have put these devices in jeopardy. Qualcomm chips inside many mobile phones have major issues, allowing for the attackers to gain root access and do whatever they want with the phone. This is a hardware defect and no matter how much policing you do in your company you can't solve this as it effects almost a billion phones. If you also include the most latest stories about the Linux Copy on Write (COW) attack, than any device running the Linux kernel became vulnerable for a brief moment and will be if they dont install the latest updates. For these mentioned reasons like the Linux COW exploit IT staff need to be able to access and update users phones in the event of such a sudden vulnerability.

That being said, I put in the rules that I did because mobile security is a very serious thing to consider. Mobile devices are currently seen as the #1 biggest security weakpoint with an estimated 25% of mobile phones encounting a threat every month. Mobile phones are considered such a problem, partly to do with how rapidly they are becoming large targets to attacks, with there being 9 times as many mobile bank trojan attacks in 2014 as there were in 2013. And this problem is not just an Android problem either, in 2015 there was five times as much malware for OS X devices than in 2014; and over a 250% increase in iOS system vulnerabilities.

There is just far too much that can go wrong to compromise the company that it would cost way too much to police the users to get the risk to a moderate level. Providing devices would only secure the user from installing one of the 75% of security flawwed apps, but if they browse the internet on their phone in public WiFi then what is the point. Educating workers and wiping their devices if the need arises is the only practical way I can see of a company handling mobile phone security. Users should not compromise the network using proxies or VPNs as these could easily gain access into the network and no matter what else you do in terms of security this gives an attacker direct access. These measures taken are much more beneficial in my opinion than attempting to watch what every user is doing and put in safeguards to prevent it, it is a futile effort and an invasion of personal freedom. I believe there is a line in the sand that has to be drawn where a user can choose their own device, especially since the IT department cannot really do anything to significant keep the threat of a compromise mobile device away.

References

[1]B. Thomas-Aguilar, ”23 Disturbing Statistics about Mobile Security - AirWatch Blog.” [Online]. Available: Online Link. [Accessed: 06-Nov-2016].

[2]”Dashboards — Android Developers.” [Online]. Available: Online Link. [Accessed: 06-Nov-2016].

[3]Home - Android Vulnerabilities. [Online]. Available: http://androidvulnerabilities.org/. [Accessed: 06-Nov-2016].

[4]B. Barrett, Vulnerability Exposes 900M Android Devicesand Fixing Them Wont Be Easy — WIRED. [Online]. Available: Online Link. [Accessed: 06-Nov-2016].