Mayur Suresh

CSC 301

11-14-21

Article Review #6

Article Review of The Great Wall Syndrome

I choose this article out of the rest because this starts off with history, specify ancient Chinese history. I love the ancient Chinese wars and the rise and fall of the many dynasties over the years. The article starts off with stating that just like in the ancient China where, despite the Great Wall of China protect them from outside threats it was often the internal affairs that led ancient China astray just like with companies. No matter how companies evolve firewalls it neglects the leaks from the inside such as with ports that can be accessed with USBs and other memory devices.

The article goes on to talk about the trend called “Lifestyle computing”. Although this article cannot be considered a “current event” article it does key in on certain facts and dangers that is still prominent today. It goes on to say that during that time USB hard drives or memory sticks where all in range and the amount of data it could store was at that time considered huge. The article also says due its size, capabilities and speed not only can this portray a “life easier” message but also easier to hide and can be used to copy huge amounts of data fast with no suspension. The article then goes on to talk about AUP, acceptable use policy and the lack of enforcement. The article lists a few restrictions that it considers should be placed, like certain users are not allowed to use hard drives, media players cameras and other devices that can be used to copy or transfer data unless the job requires them to use it and are given special permission to do so. The article then goes on to list why AUPs are important and why they should be heavily enforced.

Next the article goes on to talk about the enforcing the AUPs. The article lists many types of ways this can be enforced. This includes managing the devices that are used by the users, limit the use of only necessary devices and block all others, have a temporary portal or access with restricted time and educate the users (this is so weird shouldn’t this be employees? Not users.) on what is allowed and what is not. The article then lists many software that is specifically for user-management such as Microsoft’s Active Directory and Novell’s eDirectory. Then the article goes on to talk about the user-to-device association and setting rules to them. The article come with a solution that is similarly mentioned in a pervious section where certain industry /fields of work that has access to only certain devices. Then possible solutions that might be incorporated are listed such as prohibiting only certain files that can be transferred, add a traceability where there is a log of the actions that a user took.

The article ends with predictions of the future. This includes the illegal and improper activities only increasing due to the ever-growing technology specifically in the hard drive section. The article also includes that the average US consumer will own 10 to 20 disks drivers that they will use regularly. Then its ends of with another comparison of the Great wall of China.

Although this article was from the 2005 even thought that might not be ancient in normal terms it is ancient in the technology terms due to the ever-growing factor of it. The prediction at the end came true but the result was even more drastic. It is true that hard drives have grown to now be able to store terabytes of data there is not the concept of cloud-based platforms such as OneDrive, google drive and iCloud which makes it even easier to transfer data. Unlike before more and more jobs are converting to a full home/remote platform which will become even hard to limit the improper actions that was being committed in-person. It was hard enough for the AUPs to be enforced in-person it will be even harder to do it remotely.