**Andrew Dykman - Composition I w/ Instructor Newland - Homework 6 - Hacks / Cyber-Threats and Problems Caused by Them w/ Solutions**

I will begin this paper by listing some of the largest hack attacks in history and what could have been done to prevent them: First off, there is hack attack on the Sony Network, one of the most notorious hacks against one of the world's largest companies. This attack was done by submitting a seemingly harmless purchase request to the server, which actually happened to be a virus that deployed itself once past the firewalls on the Sony Network. It began to harvest user data and information, although it could not harvest credit card information due to the fact it was encrypted. Although the Sony Network did something right by encrypting the credit card information, they could have employed better H.I.D. systems past the firewalls, which would have detected the suspicious activity sooner, and prevented the user information from being sent back out of the network. They also could also have done a checksum / hash on purchases being sent in, to ensure they match the fingerprint for other purchase orders and aren't disguised viruses / hacks.

Another notorious hack was done against Lockheed Martin, one of the largest aircraft manufacturing companies in the world. This exploit was done via the VPN (Virtual Private Network) using RSA hardware tokens. It is suggested that they gained access by first hacking EMC's RSA department, the company who manufactures them. Using whatever means they gained they turned this to their advantage to exploit and enter Lockheed Martin's systems. The best way to prevent this kind of attack would be for companies to ensure that whoever they purchase their network / computer security systems from had a hack-proof network, since hackers can get into whatever company they want if they have access to the computers of the company that manufactured their security.

On to other potential threats / cyber-security risks: Of all the threats the most common are Viruses / Spyware / Malware. These proliferate in many different ways, but usually enter a computer system by the user accidently opening an infected file. This can happen in many different ways, and a virus / spyware code / malware can be embedded in any type of file. Another way they can enter a system is through the network, in the case of a "worm" type virus, which gets opened by another computer on the network and then travels to other vulnerable computers and infects them as well.

Viruses, whether they be Trojan, Worm, etc, all infect computers with some sort of goal in mind. In the case of viruses this is to wreak havoc on the computer and destroy the computer system. They can do virtually anything to wreak havoc, such as overwriting system files, filling up the disk with garbage, deleting user files and programs, taking control of the entire system from the user, etc. Their limit of destruction basically stops at hardware, although in a couple extreme cases this is possible because they could "flash" chips on the computer system, wrecking the BIOS, etc, or cause the hardware to perform in unintended ways that it can't handle such as speeding the hard disk past its RPM limits and burning out the motor if the disk motor isn't protected to go past a certain speed.

Spyware on the other hand, is a virus that steals user information, usually in the form of something like a keylogger, which sends the user information back to the hacker. It could also collect system information, or any other sort of information from the user surfing the internet. It will try to harvest whatever information it can and send it back to an unauthorized source.

Lastly, Malware, is a virus that doesn't fall in either category. For the most part, it is simply a virus that is made to annoy the user and create headaches. An example of this would be the "Windows Defender 2010" malware, which installs itself onto the victim computer, pretend to be an unauthorized antivirus program that the user didn't install and tell the user that their clean files are infected with viruses, and attempt to get them to purchase fake antivirus software. (Sidenote: I find this one to be one of the most annoying pieces of Malware ever and is near impossible to remove).

There are many ways to prevent Viruses / Spyware / Malware from getting on your computer. Among these methods are install a reputable anti-virus program, and update the signature files regularly. Also look for one that checks signature files, and that way can catch viruses that aren't in the virus definition database. Most of these commercially available programs also protect from Spyware / Malware, but for extra protection a user should install an Anti-Spyware program such as Spybot Search and Destroy, as well as an extra layer of security in the form of an Anti-Keylogger for their web-browser, such as Keyscrambler.