Brendan Marcelo
CYSE201S
Journal 5

      When evaluating motives for cybercrime, the number one motive in my opinion would be financial gain. Many people who commit cybercrimes often do it for money, for example the ILOVEYOU worm was originally used for financial gain because internet was not free in the Philippines, so the hacker turned to cybercrime initially to pay for internet. The second motive would be revenge. Various cybercrimes are motivated by revenge. Revenge hacking consists of hacking into a systems IT infrastructure and stealing or deleting sensitive data. For instance, during the Vtech data breach in 2015, the hacker accessed and exploited private data of over 5 million users because of the hacker did not agree with the company's practices. The third motive is recognition. With recognition as a motive, it gives the hackers a high level of respect due to the significance of the cyber-attack that they were able to achieve. Many hackers that have achieved high level cyber-attacks are known to be "famous" in the cyber world due to their skills. Multiple reasons follow, as cybercriminals are motivated by a mix of skill and the way they view the world in a socioeconomic standpoint. The fifth motive in my opinion would be the political motive. Often related to hacktivism, political hacking is growing but less widespread. An example of this would be the anonymous cyberattacks which attacked government websites in support of WikiLeaks and anti-SOPA protests. These attacks aim to influence public opinion and challenge authorities. Lastly, entertainment and boredom rank the lowest because it reflects the least serious intent. These hackers engage in cybercrime solely for fun and do not seek any financial gain or have political motives.