Chad Ballay

CYBR420-342

9/14/2020

**Week 1**

* *What is cybercrime?  Include both a definition along with three different examples.*

The short answer is that cybercrime is a computer-oriented crime. (Cybercrime, n.d.) This definition feels lacking just due to the expansion of computers into everything. Look at business operations. Computer usage first was limited to specific teams and tasks. Now you would be hard pressed to find a job that doesn’t use computers. Same applies to crime. As computers invade all aspects of criminal activities does that mean all crime will eventually fall under the umbrella of cybercrime? I don’t know the answer here for a better definition, but I can say that the Wikipedia answer isn’t sufficient.

Some examples:

1. Using voip/social media tools to orchestrate Romeo scams against lonely elders. (ELDERLY FRAUD SCAMS: HOW THEY’RE BEING TARGETED AND HOW TO PREVENT IT, n.d.)
2. Using cryptocurrencies to launder money. (Money Laundering in Cryptocurrency: How Criminals Moved Billions in 2019, n.d.)
3. Tricking pet owners to give their google authentication code on lost pet forums. (Epps, n.d.)

* *How does computer crime differ from traditional crime?*

The difference in my opinion is that the crime can only be done with the aid of a computer. Valet’s making a copy of the keys to high end cars was a thing a long time ago. It was only when they had to incorporate cloning the NFC/Bluetooth aspects of the car key that it becomes a computer crime. The use of the computer alone isn’t enough. The crime itself has to only be possible in its execution with the use of computers.

* *How has the nature of crime changed as a result of pervasive technology?*

The physical realm has gotten less meaningful. The limit of proximity has been greatly reduced due to the connectiveness of the world. No longer do you only look at those who are nearby. In many cases they are outside the jurisdiction of the first people who respond to the crime. Investigations become more about limiting impact than prevention or prosecution.

The scope and speed have increased. Twitter’s recent breach highlights how the failure of one support forum led to multiple verified accounts compromised simultaneously. (Twitter Breach Highlights Privileged Account Security Issue, n.d.) The intent of the attack was to siphon “donated” bitcoin off the moment it was received. Automation is a force multiplier.

* *Which problems does cybercrime pose to authorities seeking to investigate it?*

Cybercriminals are often at the bleeding edge of technology trying to use it to get a leg up. That puts them on the offensive which is a huge tactical advantage. You can’t train for everything so instead the authorities often end up being barely able to react in a timely manner. Then the authorities are tied to real world constraints like borders and jurisdictions. Cybercriminals has no compulsion to obey legal boundaries. If a lawless part of the internet breaks out then criminals have no problem using that wasteland as staging point for their attacks. It’s a tough situation.

# Works Cited

*Cybercrime*. (n.d.). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Cybercrime#:~:text=Cybercrime%2C%20or%20computer%2Doriented%20crime,s%20security%20and%20financial%20health.

*ELDERLY FRAUD SCAMS: HOW THEY’RE BEING TARGETED AND HOW TO PREVENT IT*. (n.d.). Retrieved from The Fraud Examiner: https://www.acfe.com/fraud-examiner.aspx?id=4294997223

Epps, T. (n.d.). *Beware of lost pet scam*. Retrieved from WKBW News: https://www.wkbw.com/news/local-news/beware-of-lost-pet-scam

*Money Laundering in Cryptocurrency: How Criminals Moved Billions in 2019*. (n.d.). Retrieved from Chain Analysis: https://blog.chainalysis.com/reports/money-laundering-cryptocurrency-2019

*Twitter Breach Highlights Privileged Account Security Issue*. (n.d.). Retrieved from Dark Reading: https://www.darkreading.com/attacks-breaches/twitter-breach-highlights-privileged-account-security-issue/d/d-id/1338396