Leah Drew
ENGL 211C
9/8/2019

Part 1: Proposal/Definition

Cybersecurity is a field focused on protecting networks and devices from cyberattacks. Technology is integral to our society and every business uses it in some way. Even something as simple as business that accepts credit cards needs to have a system in place to minimize the risk of suffering a cyberattack. Many companies, such as Amazon, conduct much of their business online, so they need an even more intricate security system to protect themselves. Besides the business aspect, many people may want to study cybersecurity from the angle of computer science, building programs to thwart attackers and testing security systems as "ethical hackers." Those interested in criminal justice or criminology might focus on how to handle and enforce laws surrounding cybercrime. Because cybercrime is such a new concept, legally there is a lot of uncharted territory. Cybercrime is always evolving with the advent of new technology, so regulations are hard to enforce. Similarly, psychologists may study what motivates people to commit cybercrime and how the structures of different types of cyberattacks are influenced by how our minds operate, including the psychology behind hacking or cyberbullying. The fact that so many disciplines can be used as an angle to study cybersecurity from is what makes it an "interdisciplinary field."

Because technology impacts our lives every day, studying the psychology behind cybercrime is especially important. Anyone can be a victim of cybercrime, but knowing how an attacker thinks can be beneficial for minimizing the effect of an attack. Viruses, ransomware, and phishing are some of the most common types of cybercrime the average person might encounter. What psychological phenomena do these kinds of criminals exploit, and why do they use them? How can this knowledge be used to counter, outsmart, or defend against cybercriminals?

Leah Drew
ENGL 211C
9/8/2019

A psychological approach isn't just useful for understanding cybercriminals. Being able to think ahead of the enemy means that programmers can create better antivirus programs, and businesses can identify weak points in their cybersecurity plans. This means that cybercriminals have fewer opportunities to do damage and innocent people remain safer. Psychology can also be used to identify weak points in new technology. This is especially important with smart devices, which often collect a large amount of data about a user. How might knowledge of psychology help developers make smart devices safer and harder to exploit?

Understanding and influencing employees is another way a psychological approach might be useful. Businesses are always at risk for a cyberattack from the inside. By understanding the human mind, companies can identify which areas someone with malicious intent would take advantage of, and better manage risk. What psychological phenomena influence attacks from the inside and why? How can this knowledge be used to minimize damage?

Management of cybercrime and cybersecurity affect us every day. Analyzing this topic from the angle of psychology is a new approach with much to still be discovered, just like the field of cybersecurity itself. However, compared to people studying criminal justice or computer science in the context of cybersecurity, fewer psychologists have done research on this topic. Applying psychological concepts to systems that manage cybersecurity can strengthen them, and being able to analyze the strategies and motivations of cybercriminals makes it easier to formulate countermeasures.

The increasing interest in protecting cyber systems has heightened the need for a new approach, and a psychological angle is one prominent and emerging approach to the field of cybersecurity.Most studies have focused on technical solutions to problems in order to counter cyberattacks, instead of directly studying the humans involved. The purpose of this paper is to

investigate the psychological factors that influence cybersecurity and how these factors could be used to make systems more secure.