Writing Assignment 1:
Cybercrime and Cyberterrorism

Jasmyn Wilhelm

Department of Cybersecurity, Old Dominion University

CYSE 404: Cybersecurity Strategy and Policy

Kylena Jude

16 November 2024

Question 1: Are the actions of TheDarkOverlord Solutions in this case an act of cyberterrorism?

According to Maras (2014), “Cyberterrorism involves the use of computers and/or related technology with the intention of causing harm or damage to coerce a civilian population and influence the policy of the target government or otherwise affect its conduct. Their attacks are aimed at causing specific reactions in governments and populations.” The disruptive and frightening nature of TheDarkOverlord Solutions’ might make them appear to be cyberterrorism. However, their ransom demands suggest that money is their primary motivation. There is no sign of a larger political or ideological purpose, despite it upsetting the school district and distressing parents and students. Therefore, the actions they committed do not satisfy the definition of cyberterrorism.

Question 2: Assuming this is not an act of cyberterrorism, what is it? Is it a crime under U.S. law?

TheDarkOverlord violated the Computer Fraud and Abuse Act (CFAA) by engaging in cyber extortion. By breaking into a school's system, stealing confidential information, and requesting privacy payment, the group violated the law. The ability of attackers to manipulate victims into making quick payments has led to an increase in this type of cybercrime. Their acts show the importance of stronger cybersecurity measures and the enforcement of regulations such as the CFAA to protect both individuals and organizations.

Question 3: What are some means by which TheDarkOverlord Solutions could have accessed the school district's servers?

TheDarkOverlord may have obtained access to the school's servers by exploiting vulnerabilities in the school's software or by persuading someone into divulging their password through phishing emails or social engineering. Maras (2014) teaches that hackers also use malware like spyware or ransomware to steal data or take control of systems. They may have deceived staff members by posing as someone they could trust through social engineering. It could have been made easier by poor password hygiene, such as using simple or recurring passwords. The hackers could have moved about the system once they were inside and stolen crucial information without anyone noticing.

Question 4: If TheDarkOverlord Solutions released personal information about students and teachers, have they violated the Privacy Act of 1974?

Since the Privacy Act of 1974 only applies to federal agencies and not private hackers, disclosing personal information about students and employees does not violate the law. According to Maras (2014), the Privacy Act governs how government organizations manage personal information; therefore, it would not apply to activities by groups such as The Dark Overlord. Their activities would still violate other laws intended to safeguard privacy and stop identity theft, though. Sensitive information like this may severely impact victims, even if the Privacy Act does not protect it. This demonstrates how crucial it is that businesses have rigorous safeguards in place to protect personal data.

Question 5: What if TheDarkOverlord Solutions found evidence that a teacher had been using school computers for child pornography and released that information? Would using that information for prosecution violate the Fourth Amendment?

Since the Fourth Amendment only shields against government searches and not private group acts, it would not apply if The Dark Overlord discovered evidence of a teacher committing a crime and made it public. Unless they were collaborating with law enforcement, evidence found by private citizens can usually be utilized in court, according to Maras (2014). The teacher might be prosecuted in this instance using the evidence without facing any constitutional problems. However, it might have become a Fourth Amendment issue if law enforcement had requested or assisted TheDarkOverlord in locating the evidence. Without that link, the main concern would be whether the evidence is credible and relevant enough to be used in court.

References

Cyber terrorist group outlines ransom in letter to Flathead Valley school. (2017, September 18). *NonStop Local Montana*. https://www.montanarightnow.com/news/cyber-terrorist-group-outlines-ransom-in-letter-to-flathead-valley/article_695ea923-ad20-5837-b922-e3677205e691.html

Maras, M. (2014). Computer forensics: Cybercriminals, Laws, and Evidence. Jones & Bartlett Publishers.

Vaas, L. (2017, September 21). *Hackers hold entire school district to ransom*. Sophos News. https://news.sophos.com/en-us/2017/09/21/hackers-holds-entire-school-district-to-ransom/