DCJ 720 Written assignment 1: Cyberattacks on U.S. infrastructure

Robert Chapa

Saint Leo University

Dr. Cheri Chambers

March 20th, 2022

Problem statement

This research proposes to examine how criminal cyber-gangs attack the U.S. infrastructure with efficacy.

Research Question 1

1. What were the gaps between the senior administrators and technical staff’s understanding of countermeasures for cyber threats?
   * The first reason this research is essential to answer is that evidence suggests that non-technical administrative executives make false assumptions about the security implementations by their I.T. departments (*Colonial Pipeline Co. attack: What really happened*, 2021; *Cyber storm 2020: After-action report*, 2021; Pankov, 2021; Parfomak & Jaikaran, 2021).
   * Some I.T. departments have a single cybersecurity manager. Usually, there is no oversight over this one all-powerful person.
   * The research may reveal areas of cybersecurity weaknesses.
2. How did U.S. Congress’s lack of technological understanding impact the laws that have been implemented to secure American infrastructure against cyberattacks?
   * Research reveals that Congress failed to understand the weaknesses in the current infrastructure protection laws that led to inadequacies in the Colonial Pipeline (*Colonial Pipeline Co. attack: What really happened*, 2021; Pankov, 2021).
   * Since current infrastructure laws are weak in enforcement, private infrastructure often considers their recommendations as suggestions (*Colonial Pipeline Co. attack: What really happened*, 2021; Pankov, 2021).
   * Due to a technological disconnect, Congressmen have difficulty understanding cybersecurity vulnerabilities.
3. Why do some I.T. departments fail to take appropriate countermeasures for ransomware and other cyber-attacks?
   * Given the increasing cyber threat, it is surprising that many I.T. departments are reluctant to implement appropriate countermeasures. It is essential to examine the reasons for the reluctance and formulate policy to increase compliance.
   * The research indicates that funding could be a possible reason for the lack of compliance. Executives responsible for America’s infrastructure must understand the importance of funding and the severe consequence of noncompliance (*Cyber storm 2020: After-action report*, 2021).
   * Another possible reason to examine cyber-attacks is the assertion that some senior I.T. personnel become complacent and dismiss cyber threats(*Colonial Pipeline Co. attack: What really happened*, 2021; Pankov, 2021).
4. How did new cyber threat techniques and methodologies contribute to recent ransomware attacks?
   * The evidence collected by various cybersecurity organizations in the U.S. government confirmed that a cybercriminal gang used ransomware (RaaS) to compromise Colonial Pipeline (*Colonial Pipeline Co. attack: What really happened*, 2021; Pankov, 2021). Understanding which technical applications are available and how they are used is essential to creating countermeasures for other infrastructure cybersecurity.
   * The U.S. Department of State offered a bounty for information leading to the arrest of those involved in the crimes. In the past, bounties have been successful in identifying criminals. Understanding new techniques and methodologies can help focus on where to implement the bounties (*Fact Sheet: The Biden-Harris administration has launched an all-of-government effort to address Colonial Pipeline incident*, 2021; Lyngaas, 2021).
   * Evidence suggests that cybercriminals utilize new techniques to obfuscate their activities and transactions. It is critical to understand which technologies cybercriminals use for law enforcement to bring cybercriminals to justice (Parfomak & Jaikaran, 2021).
   * References
   * *Colonial Pipeline Co. attack: What really happened*. (2021). cybertalk.org. Retrieved November 4 from <https://www.cybertalk.org/2021/06/09/colonial-pipeline-co-attack-what-really-happened/>
   * *Cyber storm 2020: After-action report*. (2021). Cybersecurity and Infrastructure Security Agency. Retrieved November 4 from <https://www.cisa.gov/sites/default/files/publications/Cyber_Storm-2020_After-Action-Report_01052021_Final.pdf>
   * *Fact Sheet: The Biden-Harris administration has launched an all-of-government effort to address Colonial Pipeline incident*. (2021). The White House. Retrieved November 5 from <https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/11/fact-sheet-the-biden-harris-administration-has-launched-an-all-of-government-effort-to-address-colonial-pipeline-incident/>
   * Lyngaas, S. (2021). *State Department offers $10M for information on Colonial Pipeline hackers*. CNN. Retrieved November 5 from <https://www.cnn.com/2021/11/04/politics/colonial-pipeline-ransomware-hacking-reward-state-department/index.html>
   * Pankov, N. (2021). *How Colonial Pipeline managed its ransomware attack: Should you contact authorities about ransomware?* Kaspersky. Retrieved November 4 from <https://www.kaspersky.com/blog/pipeline-ransomware-mitigation/39907/>
   * Parfomak, P. W., & Jaikaran, C. (2021). *Colonial Pipeline: The DarkSide strikes*. Congressional Research Service. Retrieved November 4 from <https://crsreports.congress.gov/product/pdf/IN/IN11667>