TO: Prof. Blain
FROM: [redacted]
DATE: 02/17/2022
SUBJECT: 500-Word Summary of The Emerging Cyberthreat: Cybersecurity for Law Enforcement

In the summary, I will be talking about how cybercrime affects law Enforcement and how we can prevent them. In the article, Quinn briefly talks about how law enforcement is the target of cyberattacks, that the Advanced Persistent threat (APT) is the most common malware used to access organizations' systems. APT is a sponsored group that gets access to the unauthorized network and still remains undetected. Once the hackers infect the system, they demand money, or they can shut down the entire system. The cases of hacking in law Enforcement have Increased. Personal information of many officers was leaked and that created a safety threat. Some officers also got threats of getting killed. After that, he talks about cyber security in police departments. He mentioned that police departments must protect the digital evidence they store in their system. He said it was the agency's leadership's responsibility to secure all these things. If anything happens to the data everyone will come after the law enforcement officer, not the IT professional. In the article, he also mentioned some of the strategies to prevent cyber-attacks. Some of them include an awareness training program, patching the devices and software, no older devices connected to the organization's network, backup data regularly, etc.

Furthermore, he emphasized awareness training. He talks about how we need to have Cybersecurity awareness training to prevent these things from happening. For example, if more people know about phishing emails, then they won't click on random links. He said there should be different training for each level. In other words, basic employee to the first responder to police leadership. They should get training for each device that can connect to the organization's network. He emphasized the fact that employees should know the risk of using unsecured Wi-Fi. Quinn also talks about breach response. It’s an action intended to reduce the risk of unauthorized data access. He said with the advancement of hacking techniques we should be extra cautious on how to respond to certain things, he mentioned a few steps to take as a breach response. Some of them include: identifying who is needed and why we needed them, detecting the attack, preserving digital data, protecting unaffected IT infrastructure, and recovering the system.

In addition, he said that the FBI does not recommend paying the ransom because it does not guarantee if organizations will regain the lost data. He said many companies that paid the ransom never got the decryption key in return. The statistic shows that in the past there was no company that had all the resources to prevent the attack. He mentioned penetration tests that can be used to identify the area where improvement is necessary. He concludes the article by talking about the importance of partnerships. He said there should be more partnerships among companies so that they can share information about cyber threats. Some of the important companies he mentions were healthcare, transportation, energy, etc.

Reference:

Quinn, C. (2018, December 12). *The Emerging Cyberthreat: Cybersecurity for Law Enforcement.* Policechiefmagazine.org. Retrieved February 7, 2022, from https://www.policechiefmagazine.org/the-emerging-cyberthreat-cybersecurity/

From Prof Blain: Excellent work. It's not formal, which I like although that would totally depend on who your target audience is. In fact, the first sentence probably shouldn't have "I" in it – it would be enough to simply start with "The article" and let it go at that. The tone throughout is so personable that you don't really need the "I." This is also very thorough, which is great, and very well written. Good job!