Read the following articles:

· <http://www.cbc.ca/news/technology/ransomware-europe-russia-ukraine-petya-bitcoin-1.4179683>

· <http://www.cbc.ca/news/canada/toronto/oshawa-hospital-cyberattack-1.4114758>

· <https://www.thestar.com/news/canada/2017/05/13/ontario-health-ministry-on-high-alert-amid-global-cyberattack.html>

Guidelines for writing a supported opinion paragraph (SOP)

· <http://schools.peelschools.org/sec/fletchersmeadow/studentlife/OSSLTprep/Documents/Sample_%20Writing%20a%20Supported%20opinion%20paragraph.pdf>

**Level 1: Ransomware Basics**

1. What is a ransomware attack?

A ransomware attack is a form of a harmful malware which can take over your computer and this can harm you because it doesn’t let you access your data. The data becomes encrypted and inaccessible until the demands of the cyber-attacker are met or until the attack is stopped. The attacker may demand a ransom from the victim such as a sum of money or a sum in cryptocurrencies likely Bitcoin to keep their identity hidden.

2. How does ransomware work and what does it affect?

Ransomware is often spread through emails that contain malicious attachments or through “drive-by” downloading. Drive-by downloading occurs when a user unknowingly visits an infected website and then malware is downloaded and installed without the user’s knowledge. Crypto ransomware is a malware variant that encrypts files and it is spread through similar methods and has also been spread through social media, such as Web-based instant messaging applications. Additionally, newer methods of ransomware infection have been observed. An example of this is web-surfers being exploited by infectious malware to go into an organization’s data.

**Level 2: Canada & Other Countries**

1. What was affected in Canada in the articles above?

In Canada, Lakeridge Hospital in Oshawa was affected as their computer system experienced downtime during the attack. However, the antivirus software that they had was able to deflect the attack, and no personal information of the hospitals or patients’ were seized. This hospital is one of tens of thousands of victims of an unprecedented cyber attack that hit around 150 countries prior to this. Also, Canadian health ministries were also affected in Ontario due to the cyber attack that hit Lakeridge Health in Oshawa.

2. How badly was Canada affected?

Canada was moderately affected due to the attack paralyzing many computers and networks. Many organizations and individuals were affected but the majority did not realize there were being affected with the ransomware. Many IT experts continued to work on the problem with the aim of fixing the computers for the hospital departments. But a lot of cyber attackers took over many computers, encrypted them and demanded a payment of around $300 in Bitcoin. This led to many people debating if they should pay the ransom or try to solve the problem but risk losing all their files.

3. What other countries were affected?

Countries that were hit the hardest due to the ransomware attacks were Ukraine, Russia, USA, and majority of Europe. In the United States, the malware affected many companies like drugstores, and food brands. In the U.S, the malware affected Merck and Mondelez International, the owner of food brands like Oreo and Nabisco. Ukraine’s cyber attack included top level government offices where many officials posted photos of darkened computer screens, as well as many energy companies, banks, cash machines, gas stations and other supermarkets. A major enterprise which was hit was a famous Ukrainian railway communication company known as Ukrtelecom.

**Level 3: Attack Details**

1. Where did the attack come from?

The attack seemed to have been sown in Ukraine. Researchers picking the program apart found evidence its creators had borrowed from leaked National Security Agency code, raising the possibility that the digital havoc had spread using U.S. taxpayer-funded tools. “Security vendors including Bitdefender and Kaspersky said the NSA exploit, known as EternalBlue, lets malware spread rapidly across internal networks at companies and other large organizations. Microsoft issued a security fix in March, but Chris Wysopal, chief technology officer at the security firm Veracode, said it would only be effective if every single computer on a network were patched — otherwise, a single infected machine could infect all others.”

Quote from: <http://www.cbc.ca/news/technology/ransomware-europe-russia-ukraine-petya-bitcoin-1.4179683>

2. Why was the attack started?

The attack may have been done simply to make some money off of the victims so they target many high populated areas in order to draw the most money. However, the motives of those behind the malware remain unknown. Ukraine has been a persistent target of pro-Russian hackers, who’ve been blamed twice for shutting down large swaths of its power grid in the dead of winter and sabotaging its elections system in a bid to disrupt May 2014 national elections.

3. How was the attacked stopped?

In Oshawa, the attack was stopped by the anti-virus software the hospital had installed, and nothing was stolen. The attack was stopped through companies and organizations updating their operating system to ensure they aren’t vulnerable to another attack. Some antiviruses managed to deflect the attack even though some of the malicious software forced other computers to reset.

4. How could you be affected by a ransomware attack?

I could be affected by a ransomware attack at any time by having it encrypt all of my files, including photos, documents and personal information. My desktop could potentially be locked completely. I can be affected by a ransomware attack as I can lose many vulnerable files and information. This means I could potentially lose loads of credit information, have data loss and important work information. I could potentially lose all of this information through accidentally going on an infected website, and then clicking on a clickbait link. This will affect me negatively as I will lose all of my valuable information due to most of it being stored on my computer.

5. How can you protect yourself against a ransomware attack?

To protect myself from a ransomware attack, I should read through emails very carefully in order to find out if it is a malicious link or a normal email. Having antivirus software will also be a good way to block any malicious ads and potentially ransomware. I should back up all of my files in case an attack ever occurs. I should reduce the number of important files on my computer so if the ransomware attack was successful, the attacker will only receive undesired data. It is important for me to remain vigilant to prevent these attacks from spreading to others and potentially creating a bigger problem. I should keep my computer’s operating systems up-to-date because the latest updates often patch up security holes.