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 type of attack where malware locks the data on someone’s computer (photos, documents, personal information, etc.), usually by encryption, and demands ransom (payment) from the victim.

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

Ransomware works by having a type of software seize control of a computer, encrypting its contents and rendering them inaccessible. The malware goes from one device to another using spam; for example, it could look like you got an email from someone you know, you click it, and then all your data is encrypted and the attacker demands ransom. The encryption can hold the victim’s documents, photos and other items on the computer.

**Level 2: Canada & Other Countries**

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

Lakeridge Hospital in Oshawa was affected; their computer system experienced downtime during the attack. However, their antivirus software was able to deflect the attack, and no personal information of the hospitals or patients’ were seized.

1. How badly was Canada affected?

Canada wasn’t terribly affected by the ransomware attack. Only one hospital from Lakeridge Health was affected, and it was only system downtime; nothing was stolen.

1. What other countries were affected?

Ukraine and Russia were hit the hardest. It paralyzed some hospitals, government offices and major multinational corporations. In Ukraine, victims included top-level government offices, as well as energy companies, banks, cash machines, gas stations and supermarkets. Ukrainian Railways and the communications company Ukrtelecom were among major enterprises hit. In the U.S, the malware affected Merck and Mondelez International, the owner of food brands like Oreo and Nabisco.

**Level 3: Canada & Other Countries**

1. Where did the attack come from?

The attack seemed to have been sown in Ukraine. However, the malware's origins remain unclear. 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.

1. Why was the attack started?

The attack may have been done simply to make some money off of the victims; 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

1. How was the attacked stopped?

In Oshawa, the attack was stopped by the anti-virus software the hospital had installed, and nothing was stolen.

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

You could be affected by a ransomware attack at any time by having it encrypt all of you files, including photos, documents and personal information. Your desktop would be locked completely.

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

It’s important for everyone to remain vigilant to prevent these attacks from spreading. People should keep their computers' operating systems up-to-date, because the latest updates often patch up security holes. People should also avoid clicking on suspicious links (clickbait).