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 when a certain type of software seizes control of a computer, and it encrypting its contents and rendering them inaccessible. Usually, ransomware blocks the access to the computer until a sum of money is paid.

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

Majority of ransomware is delivered via email that appears which usually entices the individual to click the link or download an attachment which leads to the malicious software. It can also be delivered via download attacks on compromised or malicious websites. However, some ransomware could also be delivered through social media. Majority of the time, ransomware does not really target individuals but they acquire many different emails or websites and use that to deliver ransomware in order to make money. Depending if the ransom is paid or not paid, attackers could also extract useful and important information from the compromised machine. This means it could possibly have usernames and passwords for internal or web resources, emails, payment information, etc.

Usually, ransomware asks for a sum of money to free your compromised PC. However, certain ransomware like “Crypto blocker” can encrypt your files and can steal possibly all your data. Furthermore, ransomware like “WannaCry” can delete your files outright and possibly “brick” your computer.

**Level 2: Canada & Other Countries**

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

In Canada, ransomware affected a hospital located in Oshawa. This hospital is one of tens of thousands of victims of an unprecedented cyberattack that hit around 150 countries prior. However, the hospital records were not breached at all and personal information of patients were safe. Also, Canadian health ministries were also affected in Ontario due to the cyberattack that hit Lakeridge Health in Oshawa.

1. How badly was Canada affected?

Canada was badly affected due to the attack paralyzing computers and networks. Many organizations and individuals were affected, majority however did not realize there were also 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. Many cyber attackers took over many computers and encrypted the information on them and demanded usually a payment of around $300 worth of Bitcoin. This led to many people debating if they should pay the ransom or risk losing all their files.

1. What other countries were affected?

Countries that was hit the hardest due to the ransomware attacks were Ukraine, Russia, USA, and majority of Europe. For the United States, the malware affected many companies like drugstores, food brands and many more. 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 came from the malicious malware known as “WannaCry”. They used a SMB protocol in order to help various nodes on a network communicate, and Microsoft implementation can easily be tricked by specially crafted packets into executing arbitrary code. This is how it managed to infect many computers.

1. Why was the attack started?

The attack most likely started due to the attackers wanting a large sum of money. The attackers target many high populated areas in order to draw the most money. Furthermore, since the attackers attacked the hospital, they most likely wanted to steal patients’ info in order to most likely commit identity theft or fraud.

1. How was the attacked stopped?

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 “WannaCry” software forced other computers to reset however.

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

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, data loss, important work information and many others. I could potentially lose all of this information through accidently going on a compromised website, clicking on a ransomware link through emails. This will affect me negatively as I will lose all of my valuable information due to most of it being stored on my computer.

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

To protect myself from a ransomware attack is to read through emails very carefully in order to find out if its really a malicious link or a normal email. Having an anti virus will also be a good way to block any malicious ads and potentially ransomware and also backup all of your files in case an attack ever happens on your home computer. Furthermore, filter out many potential compromised websites so if the ransomware attack was successful, they will only receive least or useless data.