1. What immediate impact did the Olympic Destroyer malware have on the 2018 Winter Olympics' IT infrastructure?

- All of the ticket and app systems for the Olympics went down. The malware also caused the Wifi to go down. This caused people to be unable to figure out where they were going through the Olympic area. This caused everyone related to the infrastructure to meet and get to work out a plan to fix it.

2. What were some of the key challenges faced by the IT staff during the cyber-attack, and how did they respond?

- The staff had to figure out a way to rebuild and get rid of the hacker all before the games were supposed to start the next day.
- This was tough because they had to guess and try all things when rebuilding the system just to make sure that the hackers didn't have any sort of access at all.

3. Why was the attribution of the Olympic Destroyer attack so difficult, and what did investigators discover about its origin?

- The reason why the forensics took so long is that instead of trying to cover their tracks they chose to send random signals from their code that resembled multiple different countries and sources.
- They used code that was translated into Chinese and headers usually used from North Korea.

4. What evidence pointed to Russia's involvement in the Olympic Destroyer attack, and how did researchers eventually confirm their responsibility?

- Someone looked through the delivery system for the malware. They realized that the same delivery systems were used through the same domain as some recent hacks that were sent to Ukraine. These attacks on Ukraine were targeting groups that only would have state interest and could easily be traced back to Russia.