Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
After studying different types of malware attacks, this attack is clearly a type of Denial of Service attack (DoS) called Synchronize (SYN) flooding which uses TCP connection to overwhelm a server with relentless SYN requests therefore attacking the bandwidth of the server to cause the server to slow down and crash and if the web server crashes then the employee's that work there can't access the website and neither can customers. Also since there is only one Source IP causing the attack it makes it a regular DoS attack instead of a Distributed Denial of Service attack (DDoS) which uses multiple devices to attack a server.

Section 2: Explain how the attack is causing the website to malfunction
This specific DoS SYN Flood attack can be identified if the Source IP is sending multiple SYN requests back to back from the same device. The attacker most likely used a packet sniffer to view the communication between the employee's devices and the web server and created their own source IP address to manipulate the traffic being sent to the web server by establishing a connection with the web server with their own device. This could negatively affect the company's reputation and revenue. If other customers find out there was a breach it could lead customers to seek out the competitors for business instead, therefore losing customers with a decrease in revenue to follow.