Ransomware Attack - Questions and Answers

Here are some questions and answers about the ransomware incident that affected the City of Stratford's computer systems in April.

What happened?

On Sunday, April 14, 2019, the City of Stratford became aware of a breach of its computer systems. It was determined that a malicious threat actor (attacker) was able to install and execute malware on six of the City's physical servers, as well as two virtual servers. The attacker then began encrypting the City's systems, making them unavailable for use.

What was the City's response?

After learning of the attack, the City immediately disconnected its servers from the Internet, and then disconnected all user endpoints (desktop computers, laptops, printers, etc.) from the City's network to contain the incident and prevent the risk of further infection.

Both the Stratford Police Service and the OPP Cyber Crime Unit were advised of the cyber incident soon after it was discovered.

Deloitte, an independent third party, was brought in to serve as an incident advisor, and to assist in the response to the ransomware incident. That included the use of network security tools to monitor for malicious activity or threats within the City's network.

Negotiations were initiated with the attacker to restore access to the City's information systems. On April 29, two weeks after the incident was discovered, the City returned to normal business operations.

Was any personal information compromised?

The investigation by Deloitte did not identify any evidence of loss, access or disclosure of personally identifiable information in relation to the ransomware incident.

Did the City pay the ransom, and if so, how much?

The attacker asked for a payment of Bitcoins, which is a digital currency, in return for the decryption keys to unlock the City's information systems. The City paid a total of 10 Bitcoins, which were valued at $7,509.13 each at the time, for a total payment of $75,091.30. The City has cyber insurance in place, and a claim has been submitted for all costs incurred as a result of the attack, including the ransom amount. The City's deductible for this coverage is $15,000.

Does the City have adequate security measures in place?

The City of Stratford views cybersecurity and the security of personal information as a priority, and has security measures in place that are updated regularly. That includes a strong password policy, network segregation between servers and workstations, and minimal system privileges for users in the network. Deloitte has noted that those security controls potentially limited the impact of the ransomware incident. Additional security measures have now been implemented to further reduce the risk of another attack.

What is the status of the police investigation into the incident?

The investigation by the Stratford Police Service, with the support of the OPP Cyber Crime Unit, is ongoing. In order not to compromise that investigation, the City of Stratford has been, and will continue to be cautious with the information it shares regarding the ransomware attack.