Ransomware Attack - Timeline

Prior to Apr 14

- Attacker gains access to the City's environment through an unconfirmed entry point

Apr 14, 8:01 a.m.

- **Beginning of ransomware attack** - attacker begins encrypting the City's systems

Apr 14, 1:00 p.m.

- City's servers are disconnected from the Internet to contain the incident. All user endpoints are disconnected from the City's network to prevent risk of infection

Apr 15, 2:00 p.m.

- Delotte is engaged by Siskinds LLP to provide cyber incident response services

Apr 15, 11:00 p.m.

- Deloitte deployes network monitoring tool and begins monitoring for malicious activity or threats within the City's network

Apr 17, 11:00 a.m.

- Deloitte deploys endpoint monitoring/scanning tool to monitor and assess the City's endpoints for any residual signs of malware or additional threats

Apr 17, 10:30 a.m.

- Negotiations begin with the attacker on the ransom

Apr 19 - Apr 22

- The City's physical and virtual servers are backed up to prevent potential data loss due to decryption errors

Apr 25, 1:00 p.m.

- Decryption of all the City's systems completed after receiving all decryption keys from the attacker

Apr 26, 12:00 p.m.

- Deloitte completes the scan of all the City's endpoints, which does not identify any residual signs of malware or additional threats

Apr 26, 12:00 p.m.

- All servers and endpoints are checked to ensure they are functioning together as intended

April 29, 9:00 a.m.

- The City of Stratford returns to normal business operations