Report

Subject: **Cyber Incident Report**

Department: **Corporate Services**

Division: **CAO**

Report #: **CAO-2025-008**

Meeting Date: **2025-07-14**

Recommendations

That report CAO-2025-006, Cyber Incident Report, be received.

Overview

On February 27th, 2025, the Town became aware of a cyber-attack. Due to monitoring and cyber security protocols, the impact was limited to minor disruptions in service to the public and all systems were restored within four (4) weeks of the incident. There is no evidence that the public's personal data was compromised. Evidence indicates that staff's personal information was compromised. It is estimated that the total cost to the Town will be $50,000.

Background

On February 27th, 2025, staff were alerted to an active cyber attack. The Town, as with most organizations, experiences hundreds of attack attempts on a regular basis. Thousands of companies of all sizes experience cyber breaches. Through strong protocol, processes, training and software, these attacks are routinely prevented here at the Town of Orangeville. However, given the pervasive and relentless nature of criminal cyber activity, it remains possible that an attack may eventually be successful.

Through appropriate preventative measures in place to manage the attack on Orangeville, the impact was limited. On the day of the incident our monitoring service alerted staff of unusual activity. Staff took immediate action in securing our networks, servers and data. These actions contained the threat and minimized the impact of the breach.

Town staff formed an incident response team (IRT). The IRT included the senior leadership team and representatives from Information Technology (IT), Communications, Finance and Emergency Services. The county Emergency Management Services (EMS) coordinator was invited to participate and did. Mayor

Post and Council were kept up to date with emails and meetings when the situation stabilized. Mayor Post also attended several IRT meetings. The IRT team met every two hours initially, every four hours in the following days and shifted to twice per day for much of the restoration period.

The Town promptly engaged experts, including legal, information technology and communications. Their advice was followed. As this was a criminal event, the OPP Cyber Crimes unit was contacted and attended onsite twice. The Information Privacy Commission was also contacted due to the potential data breech and their recommended protocol was adhered to.

Several servers were encrypted and some data was compromised. Systems hosted in the cloud were not impacted, and personal data compromised was limited and specific to current and former staff.

Over 70 systems needed to be restored, verified, tested and brought back online. Through proper defensive planning, IT staff were able to restore our systems using protected back up files. Restoration speed is dictated by the need to validate the backup, the data and its functionality.

Communication was shared with the public as able, and as recommended by legal counsel. These events are criminal in nature; therefore, it limited and continues to limit the sharing of information.

The incident was perpetrated by criminals designed to extort a ransom. No ransom was paid.

Analysis/Current Situation

Staff requested a Privileged and Confidential Cyber Security Incident Investigation report via our lawyer and will be using this report to inform and further strengthen our protocols in this ever-evolving form of crime.

Intentionally, the telephone system is not fully operational as it was scheduled to be replaced in 2026. Staff have elected to replace it now rather than restore and replace it later. That work is underway.

As part of the 2025 budget, Council approved an additional resource in Information Technology with deep expertise in cyber security. This position has been filled, and our internal cyber-security capabilities are increasing.

Regular monitoring confirms there is no evidence of any compromised data posted on the dark web.

Corporate Implications

With good foresight the Town's financial exposure is limited to $50,000. The Town has and continues to invest in systems and services to fortify its IT security. Sustained effort is required as cyber-security events evolve and become more pervasive.

Conclusion

The Town was subject to a cyber incident designed to extract a ransom payment. No ransom was paid. It is possible that future cyber breaches will occur and having strong protocols in place will minimize disruption and risk exposure. This event was minimally impactful on our community, and exceptionally short in duration for the internal services that depend on our IT systems. The Town of Orangeville prioritizes the integrity of Town systems and protecting sensitive and private information.

Strategic Alignment

Strategic Plan

Strategic Goal: Future-Readiness

Objective: Due Diligence

Notice Provisions – N/A

Respectfully submitted,

David Smith
Chief Administrative Officer