MUNICIPALITY OF
West Elgin

Staff Report

Report To:	**Council Meeting**
From:	**Magda Badura, Manager of Corporate Services (Treasurer)**
Date:	2025-03-27
Subject:	**2024 Cyber Incident**

Recommendation:

That West Elgin Council hereby receives the report from M. Badura, Manager of Corporate Services (Treasurer) re: 2024 Cyber Incident for information only.

Purpose:

The purpose of this report is to provide the community with details. of the cyber incident that occurred in January 2024. By sharing these details, we intend to build trust, offer transparency, and help residents gain understanding of the actions taken to resolve the situation.

Background:

On October 31, 2023, an employee reported an inability to receive emails. After consulting with our IT service provider, it was discovered that the employee's email account had been compromised. Immediately after this discovery all passwords were reset.
Upon investigation and careful review of login activity it showed unauthorized access from locations in Dallas, Texas, Charlotte, North Carolina, and Nigeria.

Later in 2023 suspicious login activities were detected, including access from New Jersey, US, Amsterdam and Netherlands. Security tools were activated to monitor and identify any suspicious activity. Our IT team acted fast to secure the account and set up alerts for further monitoring.

During this period, a staff member received fraudulent emails requesting a change in vendor banking information. Unfortunately, the staff did not verify the information via a follow-up call to the vendor and trusted the e-mail message. This led to the alteration of banking details within our financial system and the subsequent misdirection of payments to fraudulent bank accounts.

On January 10, 2024, a legitimate vendor contacted the Municipality regarding outstanding invoices. The following day, it was discovered that fraudulent payments had been made to incorrect accounts. The incident was immediately reported to our insurance provider and the Municipality’s banking institution, and the police were notified and an investigation followed.

Between November 1, 2023, and January 4, 2024, a total of $267,367.82 was transferred to fraudulent accounts.

Following the discovery of fraudulent transactions, it was confirmed that the email account was accessed by unauthorized individuals from several global locations, further emphasizing the international scope of the breach.

The incident was reported to the insurance company and the Municipality's banking institution for further investigation and potential recovery of funds. The police department was provided with relevant documentation, including email communications to assist in the investigation.

Since December 16, 2023, no further suspicious sign-ins have been detected on the Municipality's email server.

The IT team established alerts and monitoring systems to detect any future suspicious activity. A review of our Accounts Payable procedures has been initiated, including stricter controls on verifying vendor changes. Staff recommended a full review of our IT systems to identify vulnerabilities and ensure that future breaches are prevented.

We have developed staff training on how to recognize phishing attempts, verify vendor information, and follow secure communication protocols that are essential to reduce the risk of future fraud.

Regular audits of vendor changes, financial transactions and email communications are being conducted to identify any irregularities early on.

Financial Implications:

The cybersecurity breach resulted in a total of $267,367.82 being fraudulently e-transferred to unauthorized bank accounts. Following the incident, the Municipality took immediate action to recover funds.

The bank successfully recovered $72,944.19 from the fraudulent accounts.
The Municipality's insurance provider covered $194,423.63 of the loss; less the deductible applied as per the insurance policy. After accounting for these recoveries, the Municipality incurred a net financial loss of $10,000.00. This amount reflects the insurance deductible.

Alignment with Strategic Priorities:

Infrastructure Improvement	Recreation	Economic Development	Community Engagement
☐ To improve West Elgin's infrastructure to support long-term growth.	☐ To provide recreation and leisure activities to attract and retain residents.	☐ To ensure a strong economy that supports growth and maintains a lower cost of living.	☒ To enhance communication with residents.

Respectfully submitted by,

Magda Badura,
Manager of Corporate Services - Treasurer

Report Approval Details

Document Title:	2024 Cyber Incident - 2025-08-Corporate Services Finance.docx
Attachments:	
Final Approval Date:	Mar 24, 2025

This report and all of its attachments were approved and signed as outlined below:

Robin Greenall