# City of Hamilton
# Report for Information

| | |
|---|---|
| **To:** | Chair and Members<br>General Issues Committee |
| **Date:** | July 30, 2025 |
| **Report No:** | CM25008 |
| **Subject/Title:** | Cybersecurity Incident Summary |
| **Ward(s) Affected:** | City Wide |

## Recommendations

That Report CM25008, Cybersecurity Incident Summary, **BE RECEIVED** for information.

## Key Facts

The purpose of Report CM25008 is to provide details of the cybersecurity incident the City of Hamilton (City) experienced on February 25, 2024.

- The City was the victim of a cybersecurity incident that third-party experts identified as a sophisticated ransomware attack by cybercriminals.
- The cybersecurity incident disabled approximately 80 percent of the City's Information Technology (IT) systems and infrastructure.
- The City took swift action to protect systems and data and initiated a coordinated response to the incident:
    - Activated the Emergency Operations Centre (EOC) to coordinate the City's response to the incident on Sunday, February 25, 2024.
    - Informed its Insurer, relevant Law Enforcement Agencies, the Information Privacy Commissioner of Ontario, and the Canadian Centre for Cyber Security.
    - Retained technical advisor, CYPFER Canada Inc. (CYPFER), through the direction of external legal counsel and the City's insurer to provide forensic, technical, legal, recovery, restoration, immediate security enhancements, and cyber communications expertise.
    - Contained the breach within two days, isolating systems, creating a clean environment, reviewing impacted systems, and enhancing monitoring and security measures.
    - Restored systems and rebuilt from backups under technical expert guidance, with recovery efforts prioritized for the most critical systems and core services.

    - Continued to deliver most core programs and services, with nearly all restored in full or slightly modified manner by October 2024.
- Technical advisor, CYPFER, did not observe any direct forensic evidence that individuals' personal information or personal health information had been stolen by the cybercriminal.
- In alignment with third-party guidance, the City did not pay the ransom of approximately CAD $18.5 million (approximately USD $13 million).
- Even if the ransom had been paid and a decryption tool provided, its potentially limited effectiveness would likely have required significant additional time, effort, and cost to restore systems - while still posing substantial risk to the City.
- The City filed a cyber insurance claim, which its insurer denied due to policy exclusions; a third-party legal review confirmed the denial, and the City did not pursue further action but has since renewed its coverage.
- The City engaged Deloitte LLC to support recovery efforts and develop a Cyber Resilience roadmap focused on enhancing customer and employee experiences, improving efficiency, and strengthening cybersecurity.
- The City has recovered or rebuilt most of its IT systems infrastructure and is working to replace the limited number of systems that were unrecoverable.
- Technical advisor, CYPFER concluded that the City's response and recovery efforts were consistent with industry best practices for entities of similar size and complexity.

## Financial Considerations

There are no direct financial considerations as a result of Report CM25008. Details of cybersecurity-related costs are included in the City's Cybersecurity Incident Costing Report and Update Reports referenced in the Previous Reports Submitted section of this report.

## Background

The Canadian Centre for Cyber Security highlights that ransomware[1] remains a significant threat to organizations, with cybercriminals increasingly employing sophisticated tactics to maximize disruption and financial gain[2]. In recent years, many public and private organizations in Ontario, across Canada, and globally, including libraries, museums, school boards, healthcare facilities, municipalities, and public agencies, have experienced disruptive cybersecurity incidents that affected service delivery and put sensitive information at risk. According to a late 2024 study, 55 per cent of organizations in the Canadian Municipalities, Universities, Schools, and Hospitals (MUSH)[3] sector experienced a cyberattack in the previous 12 months[4].

On Sunday, February 25, 2024, the City experienced a cybersecurity incident that disabled most of its IT systems and infrastructure as a result of a sophisticated ransomware attack.

## Analysis

A detailed overview of the incident and recovery is outlined in Appendix “A” to Report CM25008 - City of Hamilton Post Incident Summary and Recovery Process Overview prepared by CYPFER Canada Inc.

After completing the third-party forensic analysis, the City submitted a claim to its cyber insurance provider. However, the claim was denied. The insurer cited policy exclusions related to multi-factor authentication (MFA), noting that MFA had not been fully implemented at the time of the cybersecurity incident. According to the policy, no coverage was available under the policy for any losses where the absence of MFA was the root cause of a cyber breach.

To assess the validity of the denial, the City retained Coverage legal counsel. The legal review confirmed that the insurer’s denial decision aligned with the policy terms in effect at the time of the ransomware attack. Based on the outcome of the third-party assessment, the City did not pursue further legal action for claims denial against its insurer.

Subsequently, the City implemented enhanced cyber controls and submitted a detailed application for cyber insurance renewal. As a result, the City successfully renewed its cybersecurity insurance coverage.

The City also engaged Deloitte Canada LLC to conduct a detailed assessment and develop a cyber resilience roadmap with costing estimates. Presented to Council at the January 15, 2025, General Issues Committee, Report CM25001 - Cybersecurity Resilience, included an Appendix outlining the estimated three-year capital, operating, and staffing costs for the City’s Cybersecurity Resilience roadmap.

### Summary of the CYPFER Report

Appendix “A” attached to CM25008 summarizes the cybersecurity incident as provided by CYPFER. The incident impacted approximately 80 percent of the City’s information technology systems, severely disrupting municipal operations and public services.

In response, the City worked quickly to take immediate action to limit the impacts of the cybersecurity incident and ensure continuity of City services. In addition, under guidance from its insurer, the City engaged CYPFER to assist in forensic investigation, cyber communications, and recovery efforts. CYPFER identified the cybersecurity incident as a sophisticated ransomware attack. Cybercriminals gained unauthorized access to an external internet-facing system, deployed ransomware, and demanded a ransom payment of approximately CAD $18.5 million (approximately USD $13 million).

The incident affected a wide range of critical City services, including Building, Planning, and Engineering; Business License Processing; Child Care; Finance and Procurement System; Freedom of Information Requests; Hamilton Fire Department; Hamilton Public Health; Hamilton Public Library; Housing and Homeless; Ontario Works Online Applications; Phone, Fax and Email access for select City services and general Customer Inquiry Channels; Property Tax Online tools, Portals, and Pre-authorized Payments; Recreation, Senior Centre, Arena, and Golf Course services; Recruitment; and Transit Scheduling.

Importantly, forensic analysis found no evidence that the cybercriminals exfiltrated (stole) personal information or health information. CYPFER's threat intelligence and recovery teams worked closely with the City to assess the impact, recover data, and coordinate a secure path forward without paying the ransom.

The City did not pay the ransom, instead, where possible, restoring systems from available backups, as well as launching a "Build Back Better" initiative to modernize legacy systems and prioritize technology upgrades.

In its report, CYPFER outlines the risks associated with paying the ransom in a cybersecurity incident, including the limited effectiveness of decryption tools, the high possibility of repeat extortion, and the legal and ethical concerns, consistent with law enforcement and government guidance.

CYPFER noted that even if an organization pays the ransom and receives a working decryptor, recovery typically still involves significant incremental time and costs. Decrypted systems still require a similar level of remediation as those without a decryptor to ensure the integrity and confirm full containment of affected systems, particularly in production environments (the operating environment that staff actively uses). Remediating and securing compromised systems, even with a working decryptor, remains a complex process involving significant time, effort, and cost, and that carries substantial risk.

CYPFER concluded that the City's response and recovery efforts were consistent with industry best practices for entities of similar size and complexity. In addition, CYPFER emphasized the need for ongoing investment in cybersecurity including staffing and City infrastructure.

**City Enhancements**

The City has successfully recovered or rebuilt most systems. However, a limited number, such as the finance business management application suite, development and permit applications and licensing, fire department records management, public health inspection application, traffic signal systems management, museum collections management solution and the utility locates application were unrecoverable. The City's recovery efforts have included significant collaboration across departments and vendors, focusing on improving cybersecurity resilience and modernizing infrastructure.

The City has embarked on significant enhancements to replace and advance capital investments in maturing cybersecurity, upgrades of legacy and end-of-life technology infrastructure, and to implement more modern systems. This includes the systems that were unrecoverable following the cybersecurity incident, as outlined in CM24004(a) Cybersecurity Incident Impact Update presented at the January 15, 2025, General Issues Committee as Appendix "A" attached to Report CM24004(a).

For further information on those efforts, see Report CM25007 Building Better: Post-Cyber Portfolio Update on the General Issues Committee Agenda dated July 30, 2025.

Throughout its response to the cybersecurity incident, the City continued to deliver most core programs and services. On October 15, 2024, the City announced that it was delivering almost all services in full, or a slightly modified manner. However, some staff will remain affected until the City replaces all unrecoverable systems.

Over the past year, the City has advanced its Cybersecurity Resilience and Build Back Better approach by implementing a range of new digital and operational solutions. A sample of these efforts include:

- **Enhanced Public Services and Customer Experience**
  - **Online Recreation and Facility booking solution** - makes it easier for residents to search, find and register for programs
  - **Customer Relationship Management Solution** - improves the customer service experience with new functionality being made available in phases as the project is implemented
  - **Telephone system replacement** - includes call wait time estimates and position in call queue information for residents and businesses accessing city services
  - **Career recruitment solution** - provides an easier, more user-friendly experience for applicants interested in applying for City career opportunities

- **Public Safety and Emergency Services Enhancements**
  - **Hamilton Fire Incidents Dashboard** - includes information about incident types, dispatched units, and general locations, which supports public safety and transparency
  - **Next Generation 9-1-1 (NG9-1-1) Network** - launched in collaboration with the Hamilton Fire Department and Hamilton Police Service, this upgrade enhances the ability to gather valuable additional incident information that can be disseminated directly to front-line responders

- **Financial and Operational System Modernization:**
  - **Interim-Term Finance and Procurement Technology Solution** - supports financial management, procurement, and reporting

- **Transit Improvements**
  - **Interactive HSR Transit Alert Map** - provides real-time service, including detours and unexpected service disruptions, all in one convenient place

- **Cybersecurity and Resilience**
  - **Ongoing implementation of the City's Cyber Resilience roadmap** - including the hiring of a Chief Information Security Officer (CISO) to both lead and continue to enhance the City's cybersecurity posture.
  - For further information on resiliency efforts, see Report CM25009 Cybersecurity Resiliency Enhancements on the General Issues Committee Agenda dated July 30, 2025.

## Alternatives

Not applicable as Report CM25008 is for information purposes only and therefore no alternatives are provided.

## Relationship to Council Strategic Priorities

3. Responsiveness & Transparency
   3.4. Modernize City Systems

Despite the impacts of the cyber incident, the City is focusing on:

- Cybersecurity Resilience – Strengthening cybersecurity to protect against future threats and mitigate risk; and
- Enhancing Internal Systems and Technology Tools to improve customer service experience and streamlining services to improve efficiency, accessibility, and service delivery while modernizing legacy technology infrastructure and systems.

The City's goal following the incident is to deliver strong, secure, and reliable public services.

## Previous Reports Submitted

- Confidential Report LS24013 Legal Update on Cybersecurity Incident – May 15, 2024, General Issues Committee
- CM24004 Cybersecurity Incident Impact Update – June 19, 2024, General Issues Committee
- CM24005 Cybersecurity Incident Costing Update – August 16, 2024, City Council
- Confidential Report LS24013(a) Legal Update on Cybersecurity Incident – November 6, 2024, General Issues Committee
- CM24005(a) Cybersecurity Incident Costing Update November 20, 2024, General Issues Committee
- CM24004(a) Cybersecurity Incident Impact Update – January 15, 2025, General Issues Committee, Public Appendices A & D, Confidential Appendices B & C
- Confidential Report CM25001 Cybersecurity Resilience – January 15, 2025, General Issues Committee
- Confidential Memo CM24004(b) - Additional Information to Report Cybersecurity Incident Impact Update, February 26, 2025, General Issues Committee
- Confidential Report CM24004(c) Cybersecurity Incident Impact Update - February 26, 2025, General Issues Committee
- Confidential Report CM25003 Procurement Authority and Standardization – May 21, 2025, General Issues Committee

## Consultation

- Chief Information Security Officer, City Manager's Office
- City Solicitor, Corporate Services
- Director Communications and Community Engagement, City Manager's Office

## Report References and Sources

- **Source 1 definition:** ransomware - a type of malicious software that encrypts (scrambles) data, rendering it unreadable to users and applications.

- **Source 2 link:** National Cyber Threat Assessment 2025-2026, Canadian Centre for Cyber Security, 2024 | cyber.gc.ca
- **Source 3 definition:** MUSH - public sector, including only municipal government or agency, hospital, or other health care organization, primary or secondary school, college or university, or school board.
- **Source 4 link:** CIRA 2024 Cybersecurity Report | cira.ca

## Appendices and Schedules Attached

Appendix A: City of Hamilton Post Cyber Incident Summary (Prepared by CYPFER Canada Inc.)

| | |
|---|---|
| **Prepared by:** | Cyrus Tehrani, Chief Information Officer (Acting)<br>City Manager's Office, Information Technology |
| **Submitted and recommended by:** | Cyrus Tehrani, Chief Information Officer (Acting)<br>City Manager's Office, Information Technology |