City of Hamilton Post Cyber Incident Summary

CLIENT NAME: CITY OF HAMILTON

DATE: JULY 30, 2025

VERSION: DRAFT 4.1

INTRODUCTION

CYPFER Canada Inc. (CYPFER) engaged with the City of Hamilton (“COH”, or “the City”) shortly after a cybersecurity incident (“cyberattack” or “ransomware attack”) compromised the City’s information technology infrastructure on February 25, 2024. The City engaged with CYPFER based on the direction of its insurer who provided information to immediately engage technical, legal, and cyber communications subject matter experts. CYPFER, COH and the City’s insurer worked closely together during the recovery process.

IMPACTED SERVICES

The cybersecurity attack impacted approximately 80% of COH’s systems. The City delivered critical services throughout its response, with all services operating in a full or modified state by October 2024. However, immediately following the cybersecurity incident, affected City services included, but were not limited to:

- **Building, planning, and engineering** online services and digital support, such as inspections, permits, and applications, online document submissions, ePLANS and ProjectDOX access, water and sewer connection requests, and zoning verification;
- **Business license** processing;
- **Child care**, such as access to the online childcare registry and fee subsidy office;
- **Finance and procurement** systems, such as accounts payable information, cheque issuance, electronic fund transfers, invoicing, payments, and payroll;
- **Freedom of Information requests**, including request timelines, processing and response;
- **Hamilton Fire Department**, including temporary disruption to select systems, such as burn permit and fire prevention service requests, computer aided dispatch back-end systems (excluding backups and redundancies), and X (Twitter) Incident Feed;

- **Hamilton Public Health** online and digital services, such as access to information databases and appointment booking;
- **Hamilton Public Library** online and digital services, such as online catalogues and digital resources, public computers, shelf-check kiosks, virtual programming, and Wi-Fi;
- **Housing and homeless** information database access;
- **Online City payments and services**, such as animal services, CityHousing Hamilton, Municipal Service Centres, museums and heritage facilities, and recreation;
- **Ontario Works** online applications and services, such as MyBenefits and the Subsidy and Support Programs Application Website;
- **Phone, fax and email access** for select City services and general customer inquiry channels, such as the City’s Customer Contact Centre and General Customer Inquiry Email;
- **Property tax** online tools, portals, and pre-authorized payments;
- **Recreation**, **Senior Centre, Arena, and Golf Course services**, such as admissions, rentals, memberships, and program registration processing;
- **Recruitment**, including online City Job Postings and Job Application system; and
- **Transit** scheduling, planning, location, and information services.

INCIDENT DETAILS & INITIAL RESPONSE

CYPFER began its investigation by collecting relevant digital traces and evidence to contain the cyber incident as quickly as possible. CYPFER also helped COH to respond and restore the City’s most critical services, at least in a limited capacity, given the extent of the cybersecurity incident. In parallel, CYPFER’s threat intelligence division engaged in communications with the threat actor (“cybercriminal” or “attackers”).

The threat actor carried out a sophisticated cyberattack on an external internet-facing server, gaining unauthorized access to COH systems. After entering the system, the threat actor conducted reconnaissance across the City’s infrastructure to identify valuable targets. The threat actor then coordinated and executed the deployment of ransomware—a type of malicious software that encrypts (scrambles) data, rendering it unreadable to users and applications. Following the encryption, the threat actor demanded a ransom payment in exchange for a decryptor tool (“decryptor”) to restore the affected files to their original state.

In addition to encrypting COH’s IT systems, the threat actor attempted to encrypt all the City’s available backups. When unsuccessful with this approach, the threat actor tried to delete the remaining backups. The threat actor’s goal was to paralyze COH’s IT infrastructure and shut down city services, forcing COH into negotiations to pay a ransom for a decryptor.

As part of the recovery process, CYPFER’s data recovery team worked to immediately help salvage all possible data sources. The CYPFER data recovery team used advanced techniques to recover data backups wherever possible.

During CYPFER’s investigation of the evidence related to the cybersecurity incident, CYPFER did not observe any direct forensic evidence that individuals’ personal information or personal health information had been exfiltrated (stolen) by the threat actor.

RANSOMWARE & RECOVERY OPTIONS

While conducting ongoing forensic and impact assessments, CYPFER and COH discussed whether to pay the ransom to obtain a decryptor. The threat actor demanded a ransomware payment of approximately $13 million USD (approximately CAD $18.5 million) in exchange for a decryptor. While the City, in consultation with CYPFER, explored all options including ransom payment, the City did not pay the ransom.

With ransomware, threat actors aim to force victims into negotiations by promising an easy decryption process. However, in CYPFER’s experience, decryptors often fail or require extensive troubleshooting, especially with large databases or real-time data. Based on CYPFER’s post-breach remediation team’s experience with the specific threat actor that executed the ransomware attack on the City, CYPFER estimates the successful decryption rate in complex environments similar to COH to be between 50% and 60%.

Based on CYPFER’s experience, 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 remediation, much like systems without a decryptor. This is essential to confirm the integrity and containment of affected systems, especially in production environments (the operating environment that is staff actively uses). Remediating and securing compromised systems—even with a working decryptor—involves significant time, effort, and cost, and carries substantial risk. CYPFER strongly recommends against returning potentially compromised systems back into production without full remediation, rebuilding, and thorough security cleansing—steps that often take longer than restoration and remediation from backups.

Had COH paid the ransom, there was a significant risk of losing $13 million USD (approximately CAD $18.5 million) without receiving a working decryptor from the threat actor. Furthermore, in CYPFER’s experience, law enforcement generally discourages paying ransom to decrypt affected systems, especially for public organizations and those using taxpayer funds. Federal and provincial agencies also recommend against ransom

payments, as they can fuel further cybercrime and may support international organized crime or terrorism. In addition, for organizations, paying a ransom does not guarantee malware removal, could encourage more attacks, and can increase the risk of future extortion attempts.

Wherever possible, the City recovered and restored its critical IT systems and infrastructure using backups and data sources unaffected by the cybersecurity incident. Because COH operates a complex, distributed IT environment across multiple data centres, buildings, and affiliated entities, remediation and recovery required significant effort and time. To further strengthen its systems, the City launched a “Build Back Better” initiative to assess legacy systems and decide whether to update or replace those already at end of life, rather than restore outdated systems. This approach allows COH to accelerate planned technology modernization investments and enhance its overall IT environment.

UNRECOVERABLE SYSTEMS

Despite significant effort by both CYPFER and COH, there was still a small percentage of the City’s systems that were unrecoverable because of the cybersecurity incident. These systems included, but were not limited to, the systems that support:

- Permit applications and licensing;
- Administration of land development applications and approvals;
- Business Management (Finance and Procurement);
- Museum collections management;
- Fire Department records management;
- Utility locates processing;
- Public health inspection; and
- Traffic signal system management.

RECOVERY AND REMEDIATION

CYPFER’s assessment of COH’s infrastructure highlighted an urgent need to upgrade various legacy IT systems that the City had kept in place due to budgetary constraints, limited staffing, and upgrade delays caused by the COVID-19 emergency. CYPFER also observed that, given the nature, complexity, and scale of COH technical infrastructure, the internal COH cybersecurity team was understaffed. As a result, CYPFER recommended that the City address this gap by hiring suitable professional cybersecurity resources.

The remediation process was particularly complex as COH prioritized restoring its most critical services, in at least a limited capacity, then rebuilding and upgrading related infrastructure and solutions without disrupting service delivery. Some legacy systems were unrecoverable due to end-of-life unsecured technologies that were no longer supported by the original vendors, requiring the City to rebuild them “from scratch” with modern technologies and net-new products within COH infrastructure.

Recovery of this complexity is a lengthy effort that takes a significant amount of time, cost, and resources. This process involved a major undertaking of software and hardware components, hardening and upgrading, following carefully assessed timelines agreed upon between CYPFER, COH administration, vendors, and partners involved in the process.

To finalize, based on CYPFER’s experience with other clients of similar size and complexity who have faced ransomware attacks, CYPFER’s opinion is that COH’s recovery process aligns with industry best practices.

END OF REPORT