CITY OF HAMILTON
EMERGENCY OPERATIONS CENTRE

TO:	Mayor and Members General Issues Committee
COMMITTEE DATE:	January 15, 2025
SUBJECT/REPORT NO:	Cybersecurity Incident Impact Update (CM24004(a)) (City Wide)
WARD(S) AFFECTED:	City Wide
PREPARED BY:	Carrie Brooks-Joiner (905) 973-0993 Pat Leishman (905) 870-2802 Kirk Weaver (905) 546-2424 Ext. 2878 Brian McMullen (905) 546-2424 Ext. 4549
SUBMITTED BY: **SIGNATURE:**	Mike Zegarac, General Manager Emergency Operations Centre Director

RECOMMENDATION

(a) That the following be referred to the Mayor for consideration as part of the Multi-Year Tax Budget:

(i) The inclusion of project capital costs identified in Appendix "A" and Confidential Appendix "B" to Report CM24004(a) as "Recovery," totalling $3.48M, in the 2025 Tax Budget;

(ii) The inclusion of project capital costs identified in Appendix "A" and Confidential Appendix "B" to Report CM24004(a) as "In Progress but Impacted," totalling $7.83M, in the 2025 Tax Budget;

(iii) The inclusion of capital project costs identified in Appendix "A" and Confidential Appendix "B" to Report CM24004(a) as "Planned but Now Accelerated," totalling $26.13M, in the 2025 Tax Budget;

(iv) The inclusion of capital project costs identified in Appendix "A" and Confidential Appendix "B" to Report CM24004(a) as "Approaching End of Life and Unplanned," totalling $14.66M, in the 2025 Tax Budget;

(v) The inclusion of estimated additional operating costs for 2025 of approximately $276.910 as outlined in Confidential Appendix “C” to Report CM24004(a), in the 2025 Tax Budget, funded through a combination of staff gapping savings, capital financing savings, or corporate year-end surplus;

(vi) The incorporation of estimated additional operating costs of approximately $12.72M, as outlined in Confidential Appendix “C” to Report CM24004(a), into the 2026 to 2027 Multi-Year forecast and the appropriate Tax Budget;

(vii) The incorporation of the requested change in staff complement of 20.25 temporary Full Time Equivalent (FTE) positions for 2025, in accordance with the “Budgeted Complement Control Policy,” as outlined in Appendix “D” to Report CM24004(a), utilizing existing staff vacancies within the organization;

(viii) The referral of the requested change in staff complement of 16.75 FTEs for 2026, 10.75 FTEs in 2027, in accordance with the “Budgeted Complement Control Policy,” as outlined in Appendix “D” to Report CM24004(a), to the appropriate Tax and Rate budget; and

(b) That the City Manager be authorized and directed to assume the authority under the “Budgeted Complement Control Policy,” to offset the additional FTEs outlined in Appendix “D” to Report CM24004(a) through the reallocation of existing FTEs within the organization.

EXECUTIVE SUMMARY

On Sunday, February 25, 2024, the City of Hamilton experienced a cybersecurity incident that disabled most of its Information Technology (IT) systems and infrastructure.

As the City continues to restore applications, this presents a unique opportunity to rebuild its infrastructure stronger and more resilient. Efforts include a focus on enhancing the customer and employee experiences, utilizing enterprise solutions, achieving efficiencies, and increasing resilience to protect against future cybersecurity incidents. City staff, with support from external subject matter experts at Deloitte LLP, have undertaken an analysis of the financial and operational impacts of the cybersecurity incident. This work encompassed four major steps:

- Define what is needed to restore services;
- Understand the impact;
- Determine the cost; and
- Define the strategy to fund the costs.

Report CM24004(a) outlines the findings and outputs from these steps and details the financial and staffing resources required from 2025 to 2027 for the City to successfully build back better and stronger.

It is estimated that approximately $52.1M in capital project costs is required from 2025 to 2027 to build back better and stronger after the cybersecurity incident. This includes:

- **Recovery $3.48M:** Recovery projects to address unrecoverable applications and/or data. These projects were unplanned and unbudgeted and are required as a direct result of the cybersecurity incident.
- **Projects Already in Progress $7.83M:** Incremental costs for projects previously approved and budgeted, which were in progress at the time of the cybersecurity incident but were impacted by delays and data loss, resulting in increased scope and costs.
- **Planned Projects $26.13M:** Projects that were already in the 10-year plan but accelerated due to the cybersecurity incident to ensure build back stronger.
- **End-of-Life Projects $14.66M:** Applications approaching end of life that were not yet budgeted in the 10-year plan but require short-term replacement/implementation to address risks and temporary mitigations put in place following the cybersecurity incident.

Five major projects account for 80% of the total capital project costs, including:

- Enterprise Resource Planning (ERP) System
- Building and Development Permit Applications and Licensing
- Asset Management
- Corporate Customer Relationship Management (CRM) Platform
- Fire Department Computer Aided Dispatch

Incremental operating costs for 2025 total $276.910 and are included in the 2025 Tax budget. The balance of $12.72M, required as the projects become operational, will be incorporated into the 2026 to 2027 Tax and Rate Budgets. Confidential Appendix “B” to Report CM24004(a) contains the project list and associated capital costs by year, and Confidential Appendix “C” outlines the associated operating costs.

Staffing requirements for the accelerated execution of the projects include 47.75 FTEs over three years (2025 to 2027), with 20.25 FTEs needed in 2025. All of the 2025 roles will be filled by utilizing existing positions, including vacancies. They will be funded through staffing gapping funds, revenue fees, and charges, as appropriate based on the type of position and program that the specific role supports. Appendix “D” provides a breakdown of staffing requirements (full time equivalents).

The 2025 Financing Plan includes:

- $14.9M from debt;
- $7.4M from levy contribution; and
- $8M from reserve.

Funding for 2026 and 2027 will be further evaluated during the 2026 and 2027 budget processes.

The City's financial management system was among the unrecoverable applications impacted by the incident. Manual processes are currently being used as a temporary measure. Replacement of the Human Resources, Financial, and Procurement systems was already planned pre-cybersecurity incident, but the incident has necessitated accelerated implementation. Coordinating the integration of these systems will result in a better, more efficient, and unified enterprise solution. Confidential Report CM24004(b) seeks approval related to the procurement process for an Enterprise Resource Planning System (ERP) solution.

The City's recovery efforts have transitioned from the immediate Response phase to the Recovery, Restore and Rebuild/Transform Phases. Building back better and stronger is the objective, with a focus on improving the customer and employee experience, improving efficiency and effectiveness, and leveraging enterprise solutions that leverage cloud-based technology and enterprise solutions. Implementation of the 21 recommended priority projects as outlined in Appendix "A" is key to achieving these objectives and building back stronger.

Alternatives for Consideration – See Page 11

FINANCIAL – STAFFING – LEGAL IMPLICATIONS

Financial: The financial strategy aligns with the Mayoral Directive to Staff (MDI-2024-03) dated October 28, 2024, to ensure prudent utilization of debt and reserves while protecting the City's credit rating to ensure long-term financial stability.

The capital investments for the projects total $30.3M in 2025, $14.5M in 2026, and $7.2M in 2027.

The financing plan for 2025 includes $14.9M from debt, $7.4M from contribution, and $8M from reserve. Funding for 2026 and 2027 will be further evaluated during the 2026 and 2027 budget processes.

The additional operating costs resulting from these investments will be phased in and reflected in the appropriate Tax Budget year (2025 to 2027) based on the respective project completion dates.

Staffing: The acceleration of multiple major technology projects and the increasing demand for IT capacity across the corporation have highlighted a significant need for additional human resources. The cybersecurity incident further revealed that IT was under-resourced for corporate operations at the time, and this capacity gap has grown during the recovery and rebuilding phases.

A need for 20.25 FTE in 2025 for technology-related capital projects has been identified, with an additional 16.75 FTEs needed for 2026 and 10.75 FTEs for 2027, totalling 47.75 FTEs over the 2025 to 2027 period.

Human Resources has developed a Resource Strategy to prioritize and meet the staffing requirements outlined in Appendix “D” to Report CM24004(a). The strategy for the 20.25 FTEs for 2025 includes:

- Utilizing existing positions, including vacancies as the primary source of FTEs;
- Funding positions from 2025 capital projects listed in Appendix “A,” except for Transit FTE (0.5), which will be funded through Transit Reserve 112204 for 2025, with a sustainable funding source in 2026;
- Setting a target start date of June 1, 2025, or later, to reduce in-year budget impacts;
- Starting positions as temporary contracts in 2025, transitioning to permanent positions as resources allow; and
- Incorporating user fee and charge increases where appropriate, supported by by-law amendments, to fund related positions beginning in 2025.

Human Resources will work with the Project Leads to prioritize recruitments related to building back better initiatives, reassign existing staff from other operational areas doing similar work and redistributing existing vacancies and associated budgets to support these projects, per Recommendation (b) to Report CM24004(a).

Legal: Legal Services will be engaged for the negotiations and preparation of the final contracts between the City and the vendors.

HISTORICAL BACKGROUND

On February 25, 2024, the City of Hamilton experienced a cybersecurity incident that resulted in the disabling of a majority of its IT systems and infrastructure.

In collaboration with external experts, the City took intentional and purposeful actions to contain the incident, secure systems and data, protect the community and staff, and ensure the continued delivery of critical services. These actions included:

- Activating the Emergency Operations Centre (EOC) on the evening of February 25th;
- Engaging the Insurer and a team of cybersecurity experts (including CYPFER, Deloitte LLP., and legal counsel);
- Containing the breach within 2 days (faster than the industry average);
- Initiating enhanced cybersecurity measures;
- Did not pay a ransom; and,
- Conducting forensic analysis, which determined that, at this time, there is no evidence that people's personal information or personal health information has been compromised as a result of the cybersecurity incident, during which our systems were encrypted.

The immediate response also involved developing manual and alternative processes to continue delivering critical services, particularly health and safety, while minimizing the overall service impacts to the public and internal operations. Throughout the incident, the City maintained core programs and services to the community, with additional services gradually resuming as it was safe and secure to do so.

By mid-to-late March, the City shifted its focus from immediate response to recovery. Efforts, guided by a customer-centric lens, focused on restoring and rebuilding critical systems to support internal operations.

In June 2024, Report CM24004 provided an overview of the cybersecurity incident, a high-level summary of the technology impacts, costs incurred to date, and a list of unrecoverable and impacted applications.

Since June, staff has continued restoring services and refining the plan to build back better.

POLICY IMPLICATIONS AND LEGISLATED REQUIREMENTS

The recommendations in this report comply with the City of Hamilton's:

Procurement Policy By-law 20-205 as amended – This Policy guides the procurement of the necessary quality and quantity of Goods and/or Services in an efficient, timely and cost-effective manner, while maintaining the controls necessary for a public agency, in accordance with the Procurement Policy as approved by Council.

Budget Complement Control Policy (Appendix "A" to FCS16024, CBP – 1) - The purpose of this Policy is to ensure that the City's staff complement is managed in an effective and efficient manner. The Policy provides guidance on transferring complement, increasing, or decreasing complement and changing complement type.

RELEVANT CONSULTATION

Report CM24004(a) was prepared in consultation with staff from all departments, Senior Leadership, and supported by Deloitte LLP., to determine that the proposed submission adopts a customer-centric approach, addresses budget pressures and risks, prioritizes investments, and aligns with Council Priorities, while building back better.

ANALYSIS AND RATIONALE FOR RECOMMENDATION

As the City continues to bring back applications and services, there is a unique opportunity to build back infrastructure better and stronger. City staff and Deloitte LLP. worked together to develop a clear understanding of the financial and operational impact of the cybersecurity incident and the resources required over the next four years.

This process included the following four steps:

Define **what is needed to restore services**	Identify and prioritize the projects that are required to restore services to citizens, including projects that support the status quo, continuous improvement and eventual transformation.
Understand the **Impact**	Clarify the impact of the incident on City priorities, projects and programs.
Determine the **Cost**	Define the expected capital and operating costs associated with those prioritized projects and related assumptions.
Define the **Strategy to Fund the Costs**	Identify the potenital sources for funding prioritized projects.

1. Define What Is Needed To Restore Services

Work has been ongoing since the February incident to identify and implement the necessary actions to restore services to the public. As part of the immediate response, an initial prioritization of all known technology applications was conducted. This process identified critical applications for immediate assessment, restoration if possible, and where needed, the development of mitigations to keep priority services functioning for the public.

In April, a comprehensive City-wide Service Priority Ranking was completed. This work evaluated the impacts of the cybersecurity incident to ensure that ongoing restoration and rebuilding work was guided by a customer-centric approach.

With the support of Deloitte LLP., a Prioritization Framework was developed to assess, rank, and categorize approximately 184 IT-related projects identified as of August 2024 to build back better. The ranking and categorization exercise organized projects into four quadrants of a matrix, identifying high-value, high-readiness projects, projects with high or low value requiring additional planning, and projects that can be delayed at this time. Both enterprise value and organizational readiness were key factors considered in the ranking process.

As a result, 21 IT-related projects were identified for priority advancement, including: 5 recovery projects which will bring back data or applications “as is” and are needed only because of the cybersecurity incident, 4 projects already in progress at the time of the incident, but impacted in their implementation, 5 projects that were already planned but now accelerated due to the incident, and 7 projects that were approaching End-of-Life but were not yet planned for replacement with the planning and implementation now accelerated.

These priority projects were moved forward into a costing exercise, the results of which are outlined in Confidential Appendix “B” to Report CM24004(a).

2. Understand The Impact

The cybersecurity incident caused significant operational impacts, with detrimental effects. A customer-centric approach has been taken, prioritizing service continuity of the most critical systems, particularly those related to public health and safety. Services have been restored incrementally as it has been safe and secure to do so.

Note: Cybersecurity evaluations and recommended enhancements to strengthen the City’s cyber resiliency are addressed separately in Report CM24006 - Cybersecurity Update.

Cybersecurity Impact on Service Delivery

As of November 11, 2024, an assessment of service delivery across City services was completed. 99% of City services are back up with approximately half fully operational and the other half available through a modified or alternate process. A breakdown of the status of service delivery is as follows:

- Services that have been fully restored: 37%
- Services that are provided through an alternate method: 50%
- Services that experienced no impact: 12%
- Services not yet restored: 1%

Services not yet restored reflect internal staff-facing HR and financial administration activities with no direct impact on citizen service delivery.

Cybersecurity Impact on Technology Applications

Since the cybersecurity incident occurred, City staff have managed impacts and delays on a project-by-project basis. Over 75% of the 230 applications have been restored, and about 70% of critical applications are back online.

The City continues to rely on short-to-mid-term mitigation solutions to maintain services. Some mitigation solutions keep processes operational including manual approaches (e.g., financial tracking and work orders) and the introduction of interim or new technology solutions (e.g., payroll).

Cybersecurity Impact on Capital Projects and Department Initiatives

In July 2024, a Budget Impact Exercise analyzed the degree to which the cybersecurity incident affected capital projects and department initiatives, highlighting the urgency to advance impacted projects.

The analysis reviewed 2,351 capital projects and 76 departmental initiatives, including those from the Capital Projects Status Report (as of February 29, 2024), net-new projects initiated post-incident, and initiatives funded from the operating budget. It gathered data on alignment with Council priorities, progress, urgency, and incident impact, as well as financial details such as approved budgets, expenditures, and any restrictions (such as third-party funding). Previously approved technology and security-related projects were also flagged for potential acceleration to leverage enterprise solutions and strengthen system resilience. Overall, the analysis showed that the cybersecurity incident did not have a significant impact on capital projects and department initiatives as staff were able to advance work using manual processes.

Where impacts were identified, these were due to:

1. Loss of access to technology applications and / or data sources
2. Temporary delay in hiring ability
3. Resource intensive mitigation strategies
4. Temporary delay of technology system upgrades
5. Resource reallocation or project backlog

This analysis was primarily manual due to the incident's impact on systems that typically store this information, many of which remained in various states of recovery.

Enterprise Resource Planning System Replacement

The City's financial management system was among the unrecoverable applications impacted by the incident. Manual processes are currently being used as a temporary measure. Replacement of the Human Resources, Financial, and Procurement systems was already planned pre-cybersecurity incident, but the cybersecurity incident has necessitated accelerated implementation. Coordinating the integration of these critical systems will result in a better, more efficient, and unified enterprise solution.

3. Determine The Cost

Following the identification of priority projects, a costing analysis was completed on the top 21 projects including capital resources required 2025 to 2027, operating impacts 2025 to 2027, and FTE requirements. These projects are included in the City's broader building back stronger roadmap and include a mix of status quo, continuous improvement, and transformational projects.

The capital project costs, incremental operating impacts and staffing resources to support these priority projects are identified respectively in Confidential Appendix "B", Confidential Appendix "C", and Appendix "D" to Report CM24004(a).

4. Define The Strategy To Fund The Costs

The project prioritization and budget impact exercises have informed the funding approach to support the priority projects and initiatives to build back stronger. This work included reviewing the total investment required to implement priority projects; reviewed existing capital projects for dollars which could potentially be reallocated; and identified other potential sources of funding.

Refer to the Financial Section of Report CM24004(a) for additional information.

ALTERNATIVES FOR CONSIDERATION

To ensure there is no impact on the City's ability and timelines to fully recover from the cybersecurity incident, staff do not recommend any alternatives at this time, however, members of Council may propose amendments to these recommendations through the 2025 budget process.

APPENDICES AND SCHEDULES ATTACHED

Appendix "A" to Report CM24004(a) - Project List

CONFIDENTIAL Appendix "B" to Report CM24004(a) - Project List with Cost Breakdown (2025-2027)

Confidential Appendix B is private & confidential in accordance with Section 239(2)(j) of the Municipal Act 2001 as it contains financial information that belongs to the municipality and has monetary value or potential monetary value.

CONFIDENTIAL Appendix "C" to Report CM24004(a) - Operating Impact (2025-2027)

Confidential Appendix C is private & confidential in accordance with Section 239(2)(j) of the Municipal Act 2001 as it contains financial information that belongs to the municipality and has monetary value or potential monetary value.

Appendix "D" to Report CM24004(a) - Staffing (FTE) Resources (2025-2027)