City of Hamilton
Report for Information

To:	Chair and Members General Issues Committee
Date:	July 30, 2025
Report No:	CM24005(b)
Subject/Title:	Cybersecurity Incident Costing Update
Ward(s) Affected:	(City Wide)

Recommendations

That Report CM24005(b) respecting Cybersecurity Costing Update **BE RECEIVED** for information.

Key Facts

- At the meeting of the City Council on November 27, 2024, Report CM24005(a) provided an overview of the Cybersecurity incident, the costs incurred to October 11, 2024, the impact on services and technology, and identified next steps.
- Staff was directed to report back to the General Issues Committee with details of the external supports and further description of the external work provided during the Cybersecurity incident.
- Staff has committed to providing regular updates to Council on the costs incurred in response to the Cybersecurity incident. Report CM24005(b) provides an update on costs incurred to June 30, 2025, as well as additional detail related to the external supports provided during the Cybersecurity incident.
- Staff continues to undertake the work required to rebuild the City's financial system. This report provides an update on progress to date and the plans still to be implemented.

Financial Considerations

Tables 1 and 2 summarize the financial impacts related to this Cybersecurity incident that have been invoiced as of June 30, 2025, by phase and cost category. The total cost incurred to date is $18.3 M. There may be additional invoices still to be received for some items that will be included in future reports. The previous Report CM24005(a) reported costs of $9.6 M up to October 11, 2024, and represented estimates and commitments known at that time. Refinements to which phase and cost category items belong in have been made, as needed.

As discussed in the analysis section below, the costs captured in this report speak to the efforts and associated costs within the four phases. More specifically this would encompass external experts as it related to IT security hardening (e.g. Cypher), Deloitte as it related to supporting vendor payments, managed services for the interim financial system, financial data rebuild, process and procedure development, interim financial system training, change management and crisis communication and development of the Cyber resiliency roadmap.

The Cybersecurity incident financial impacts to June 30, 2025, excludes the Building Better Action Plan that is detailed in Report CM25007. The Building Better Action Plan encompasses 21 projects that addresses the impact of the cyber event on existing applications and processes, including unrecoverable applications, planned projects that now need to be accelerated, and end-of-life applications.

Table 1
Cybersecurity Incident Preliminary Financial Impact
By Phase

Phase	**Cost Categories**	**Estimated**
Response	• External Experts • Other Related Costs	$2,938,542
Recovery	• External Experts • Infrastructure • Staffing	$4,178,456
Restore	• External Experts • Infrastructure	$6,495,439
Rebuild / Transform	• External Experts • Infrastructure	$4,733,185
Total		**$18,345,622**

Table 2
Cybersecurity Incident Preliminary Financial Impact
By Cost Category

Category	**Estimated**
External Experts	$14,042,862
Infrastructure	$1,731,136
Staffing	$1,149,095
Other Related Costs	$1,422,529
Total	**$18,345,622**

Background

Staff was directed to report back to the General Issues Committee with details of the external supports and further description of the external work provided during the Cybersecurity incident.

Analysis

The City's focus is now on the Recovery, Restore and Rebuild / Transform Phases. Building back better and stronger is being done with a focus on the customer and employee experience, enterprise solutions, efficiency and increasing resilience to protect against future incidents.

All goods and / or services acquired during the Emergency Operations Centre (EOC) activation, to date, have followed City policy and procedures, including the Procurement Policy. The financial impacts are being tracked across the four phases: Response, Recovery, Restore and Rebuild / Transform. It is important to note that some financial impacts may cross more than one of these phases. However, for the purposes of simplifying reporting, financial impacts have been assigned to the most relevant phase.

Response Phase financial impacts relate to the City's efforts to protect systems and to provide services with as little disruption as possible in the initial period following the Cybersecurity incident. Examples include the purchase of additional storage server capacity and equipment, such as, printers and cell phones to facilitate service continuity during the initial response period.

Financial impacts for the Recovery and Restore Phases include activities related to the testing, restoration and recovery of the various systems impacted. Future financial impacts in this area are anticipated.

The financial impacts of the Rebuild / Transform Phase include rebuilding applications and data, redesigning to meet the needs of business areas and migration to future state infrastructure that is responsive to customer needs and provides improved user experiences. Future financial impacts in this area are anticipated.

Please Note: Detailed updates on the broader portfolio of projects being undertaken as part of the City's recovery and transformation efforts are outlined in Report CM25007, which is submitted under separate cover.

Staff was directed to report back to the General Issues Committee with details of the external supports and further description of the external work provided during the Cybersecurity incident. As noted in Table 2, approximately $11.6 M in costs have been incurred for external experts. Of the $14.0 M in total external support costs incurred to date, approximately $10.9 M is associated with Deloitte's contributions across five primary workstreams:

- **Project Management** – This involved mobilizing incident response resources to ensure an immediate and strategic response to the incident. This was followed by the establishment of a dedicated team to assess response needs, identify key projects and define project plans for each project.
- **Design, Implement and Accelerate** – A team was established to support the redesign of impacted environments, accelerate recovery efforts and create the City's future roadmap for cyber maturity.
- **Change Management and Crisis Communications** – This workstream involves supporting and managing stakeholder engagement and communication, staff engagement, training, and targeted change management strategies.
- **Post Incident Support** – A team is supporting efforts to rebuild trust and confidence in impacted systems and working with the City's insurers.
- **Temporary Finance and Procurement Operations** – Implemented and supported the interim finance and procurement system solutions.

Other external experts were engaged in the containment of the breach, investigation of the cyberattack and continuous and ongoing monitoring for additional threats and vulnerabilities.

Progress on Rebuilding Financial and Procurement Systems

The Cybersecurity incident rendered the City's Business Application Suite as unrecoverable, and it was not functional. As a result, staff had to adapt and come up with alternate processes to ensure continuity of service. Many of these processes were manual and not sustainable in the long term.

Significant progress has been made in rebuilding our financial data and systems as it relates to Finance and Procurement. The City has moved forward with our medium-term solutions: NetSuite Enterprise Resource Planning (ERP) and Basware Accounts Payable automation tool. The rollout of NetSuite occurred in phases between mid-April and late June 2025. Basware is expected to be rolled out in Q3 of 2025.

Deloitte has been actively supporting Finance and Procurement staff in rebuilding data and systems. Activities include data rebuild exercises, NetSuite set up and implementation, change management, communication, and training. With the progression of NetSuite, staff is continuing to restore functionalities as it relates to

Finance and Procurement. Staff is actioning the backlog of data recovery and data entry to support the completion of 2023 and 2024 Audited Financial Statements and resumption of regular financial reporting activities to Committee and Council.

Work on the 2023 audited financial statements is ongoing, with a target completion date of late Fall 2025. Efforts will then shift to completing the 2024 audited financial statements. Preliminary 2025 budget variance reporting is anticipated in early Fall 2025.

NetSuite and Basware solutions were recommended by Deloitte and approved by the Emergency Operations Centre (EOC) on October 1, 2024. NetSuite was selected as an out-of-the-box product that would allow the City to resume critical functionality sooner than moving directly to a long-term ERP solution that would take much longer to implement.

The City has entered into the following agreements:

- Deloitte - managed services with NetSuite, for a 19-month term.
- Basware - Accounts Payable automation, for a 36-month term.

Conclusion

In summary, the City has made significant progress in restoring critical Finance and Procurement operations following the Cybersecurity incident. External experts, including Deloitte, have played a key role in incident response, system redesign, and implementation of interim solutions. To date, approximately $14 M has been incurred in external support costs, with $10.9 M attributed to Deloitte's multi-stream work. The rollout of NetSuite and Basware is advancing, with full implementation expected by Fall 2025. Staff continues to work toward completing 2023 and 2024 audited financial statements and resuming regular financial reporting. Recovery efforts remain ongoing, and future financial impacts are anticipated as systems and processes continue to mature.

Relationship to Council Strategic Priorities

Report CM24005(b) provides information on the financial impact of the City's response to the Cybersecurity incident and supports Council's priority related to Responsiveness and Transparency. Specifically, it discusses the City's efforts to build a high performing public service and modernize City systems.

Previous Reports Submitted

- CM24005 Cybersecurity Incident Costing Update August 16, 2024
- CM24005(a) Cybersecurity Incident Costing Update November 20, 2024

Consultation

- Director, Financial Services, Corporate Services
- Chief Information Officer and Director of Innovation, City Manager's Office
- Director, Enterprise Portfolio Management-Rebuild and Transformation, City Manager's Office

Appendices and Schedules Attached

N/A

Prepared by: Kirk Weaver
Acting Director Financial Planning, Administration and Policy
Corporate Services Department

Submitted and recommended by: Mike Zegarac
General Manager, Finance and Corporate Services
Corporate Services Department