




Hamilton

INFORMATION REPORT

TO:	Mayor and Members General Issues Committee
COMMITTEE DATE:	June 19, 2024
SUBJECT/REPORT NO:	Cybersecurity Incident Impact Update (CM24004) (City Wide)
WARD(S) AFFECTED:	City Wide
PREPARED BY:	Carrie Brooks-Joiner (905) 973 0993 Jenn Hohol (905) 546-2424 Ext. 7857 Brian McMullen (905) 546-2424 Ext. 4549
SUBMITTED BY:	Mike Zegarac, General Manager Emergency Operations Centre Director
SIGNATURE:	

COUNCIL DIRECTION

Not applicable

INFORMATION

Report CM24004 provides an overview of the cybersecurity incident, the costs incurred to May 28, 2024, the preliminary forecast costs, the impact on services and technology and identifies next steps.

OVERVIEW OF THE CYBERSECURITY INCIDENT

On Sunday, February 25, 2024, the City of Hamilton (City) experienced a cybersecurity incident that resulted in the disabling of a majority of the City's Information Technology Systems and Infrastructure. The Emergency Operations Centre (EOC) was activated the evening of Sunday, February 25 upon confirmation of a cybersecurity incident. The City's insurer and team of cybersecurity experts (including CYPFER, Deloitte LLP and legal counsel) were engaged to support the response, ongoing recovery and rebuilding efforts.

OUR Vision: To be the best place to raise a child and age successfully.

OUR Mission: To provide high quality cost conscious public services that contribute to a healthy, safe and prosperous community, in a sustainable manner.

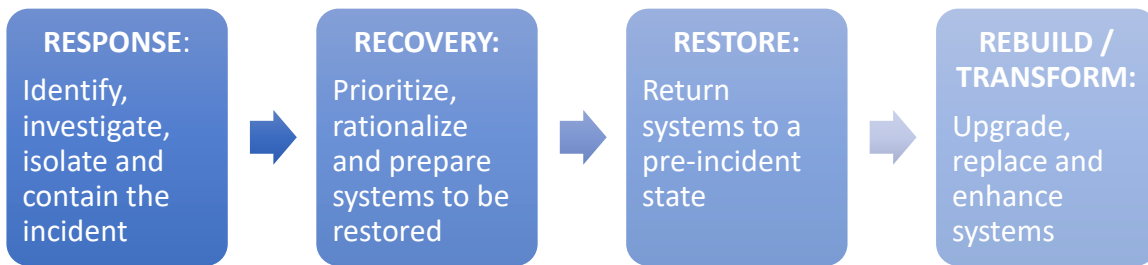
OUR Culture: Collective Ownership, Steadfast Integrity, Courageous Change, Sensational Service, Engaged Empowered Employees.

The City, in collaboration with external experts, took intentional and purposeful actions to contain the incident, protect the community and staff and ensure the continued delivery of critical services. 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.

The City is committed to making thoughtful, intentional and incremental improvements aimed at achieving a state superior to that before the incident.

Informed by the external experts, the full recovery process is expected to extend over many months. The City will progress through four main phases of effort as outlined in Figure 1 below.

Figure 1: Response, Recovery, Restore and Rebuilt / Transform



The City’s work in the Response Phase focused on containment and isolation of the City’s Information Technology infrastructure to prevent the cyber criminals from inflicting further damage. City staff also responded to the disruption of services with the development of manual and alternative processes, where possible, to continue to provide internal support to impacted service areas in an effort to limit the extent of service impacts to the public and internally.

In March 2024, the Mayor and City Manager confirmed that the City had:

- Contained the cybersecurity incident;
- Determined through forensic analysis that there was no evidence that personal data or information has been compromised;
- Not paid a ransom, and;
- Shifted from the Response Phase to the Recovery Phase.

Services and applications continue to be made available as it is safe and secure to do so.

As the City continues to bring back applications and work through the Recovery and Restore phases, the City is presented with a unique opportunity to build back its infrastructure stronger and better in the Rebuild / Transform Phase. Where applications can be recovered, restored or rebuilt staff are currently working to assess each application to determine whether it should be restored as status quo and returned to pre-incident state, improved by enhancing what previously existed (continuous improvement) or transformed. This is being done using the foundations of a customer-centric experience and optimizing an enterprise approach. This analysis is ongoing.

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

Work is underway to analyze applications and processes and is anticipated to identify opportunities to transform services and work processes. These opportunities will be detailed in future reports to Council including the identification of cost implications, funding strategies and timelines. Examples include telephone infrastructure replacement, point-of-sale system replacement and time and attendance system implementation.

In addition, staff is aware that as a consequence of the cyber security incident, there may be delays to existing capital projects and other initiatives. Staff is reviewing this and will report back to Council on projects that may have been delayed and any potential impacts.

FINANCIAL IMPACT – COSTS INCURRED

All goods and / or services acquired during the 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.

Tables 1 and 2 summarize the preliminary financial impacts related to this incident reported as of May 28, 2024 by phase and cost category.

Table 1 – Cybersecurity Incident Preliminary Financial Impact - by Phase

Phase	Cost Categories	Estimated \$
Response	<ul style="list-style-type: none">• External Experts• Other Related Costs	\$1,480,657
Recovery	<ul style="list-style-type: none">• External Experts• Infrastructure• Staffing	\$1,522,145
Restore	<ul style="list-style-type: none">• External Experts• Infrastructure	\$1,657,124
Rebuild / Transform	<ul style="list-style-type: none">• External Experts• Infrastructure	\$1,055,000
Total		\$5,714,926

Table 2 – Cybersecurity Incident Preliminary Financial Impact - by Cost Category

Category	Estimated \$
External Experts	\$2,943,950
Infrastructure	\$1,718,192
Staffing	\$924,752
Other Related Costs	\$128,032
Total	\$5,714,926

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. Early in the Response Phase, limitations in payment processes resulted in relatively small amounts of lost revenue in Recreation and Waste Disposal.

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.

OUR Vision: To be the best place to raise a child and age successfully.

OUR Mission: To provide high quality cost conscious public services that contribute to a healthy, safe and prosperous community, in a sustainable manner.

OUR Culture: Collective Ownership, Steadfast Integrity, Courageous Change, Sensational Service, Engaged Empowered Employees.

The annual operating costs and capital project costs in Tables 1 and 2 will be absorbed in 2024 budgets and reported to Council in future budget variance reports with applicable funding from existing capital work-in-progress projects or reserves, where available.

FORECAST COSTS

With a plan to continue to modernize, digitize and strengthen City's services, there were plans to invest a substantive amount to support this work which was forecasted as \$33.6 M 2025-2033 tax and rate budgets. These investments were planned to further Council's Responsiveness and Transparency Priority and the related customer experience outcomes, strengthen the City's cyber security and support transformative improvements in service delivery. Staff is reviewing the alignment of the current and forecasted investments in an effort to assess opportunities to leverage funding to support and accelerate the response to the cyber incident.

Though most applications can be recovered, restored and rebuilt there are some applications that are unrecoverable, meaning the database or application cannot be re-established or are at end of life, resulting in temporary manual or alternate processes to limit the impact on the services where possible. This is the case for key applications which are required to support the City's business management systems, processes for permits and licensing, records management in some areas and more. Appendix "A" to Report CM24004 outlines unrecoverable, impacted or end-of-life applications that have been identified to date, the service impact and the mitigations in place.

Guided by external experts, the City enhanced its cybersecurity following the incident. This included the rollout of various security enhancements to help strengthen the City's IT infrastructure to protect against potential future threats. The external experts have identified additional cyber resilience initiatives.

The estimated financial impact of cyber resilience and rebuild / transform efforts will be included in future reports to Council along with funding strategies, updates on impacted services, timelines and instances where planned projects can be accelerated and strengthen the City's systems against future incidents. Funding strategies may leverage previously approved funding for technology and security-related projects, appropriate reserves and may reprioritize some capital projects to minimize the impacts on the tax levy and rate budgets.

OUR Vision: To be the best place to raise a child and age successfully.

OUR Mission: To provide high quality cost conscious public services that contribute to a healthy, safe and prosperous community, in a sustainable manner.

OUR Culture: Collective Ownership, Steadfast Integrity, Courageous Change, Sensational Service, Engaged Empowered Employees.

To date, staffing requirements to support the Response, Recovery and Restore phases have been addressed by changing work plans, short-term assignments and contracting of external expertise. Going forward, dedicated staff will be required to advance the Rebuild / Transform Phase. The review of impacted systems and services as part of this Phase will support a customer-centric enterprise focus and, in turn, transform how the City provides services. Work is underway to identify such transformational projects and to firm-up costs, staffing requirements and timelines. Details and recommendations will be brought to Council in future reports.

TECHNOLOGY IMPACTS

The cybersecurity incident affected the City's technology which includes approximately 228 unique applications that are needed to deliver City services to varying degrees. Each application is being brought back on a service-based priority basis.

A high-level summary of the number of applications and their status in the recovery process is below:

- 228 applications impacted;
- 45% of total applications restored to date;
- 48 critical impacted applications; and
- 60% of critical impacted applications restored to date.

The City has implemented multiple short-to-mid-term mitigation solutions to limit service disruptions. Some mitigation strategies include the introduction of interim or new technology solutions such as BambooHR that was put in place to post and receive applications for City of Hamilton jobs and QuickBooks, DocuSign and Plooto which form the interim accounts payable solution. Mitigation strategies put in place have a range of associated costs that have been tracked and outlined in the financial impacts and Tables 1 and 2 of Report CM24004.

NEXT STEPS

As the City continues to bring back applications and work through the Recovery and Restore phases, the City is presented with a unique opportunity to build back its infrastructure stronger and better in the Rebuild/Transform Phase. Where applications can be recovered, restored, or rebuilt, staff are currently working to assess each application to determine whether it should be restored as status quo and returned to pre-incident state, improved by enhancing what previously existed (continuous improvement), or transformed. This is being done using the foundations of a customer-centric experience and optimizing an enterprise approach. This analysis is currently in progress.

The City's focus has moved from immediate Response to the Recovery, Restore and Rebuild/Transform Phases. Building back stronger is the objective, with a focus on the customer and employee experience, enterprise solutions and efficiency, and increasing cyber resilience to protect against future incidents. Work is underway to analyse applications and processes and is anticipated to identify opportunities to transform services and work processes.

These opportunities will be detailed in future reports to Council. Reporting back will include the identification of cost implications, funding strategies, updates on impacted services, timelines and instances where planned projects can be accelerated and strengthen the City's systems against future incidents. Funding strategies may leverage previously approved funding for technology and security-related projects, appropriate reserves, and may reprioritize some capital projects to minimize the impacts on the tax levy and rate budgets.

APPENDICES AND SCHEDULES ATTACHED

Appendix "A" to Report CM24004 – Unrecoverable and Impacted Applications