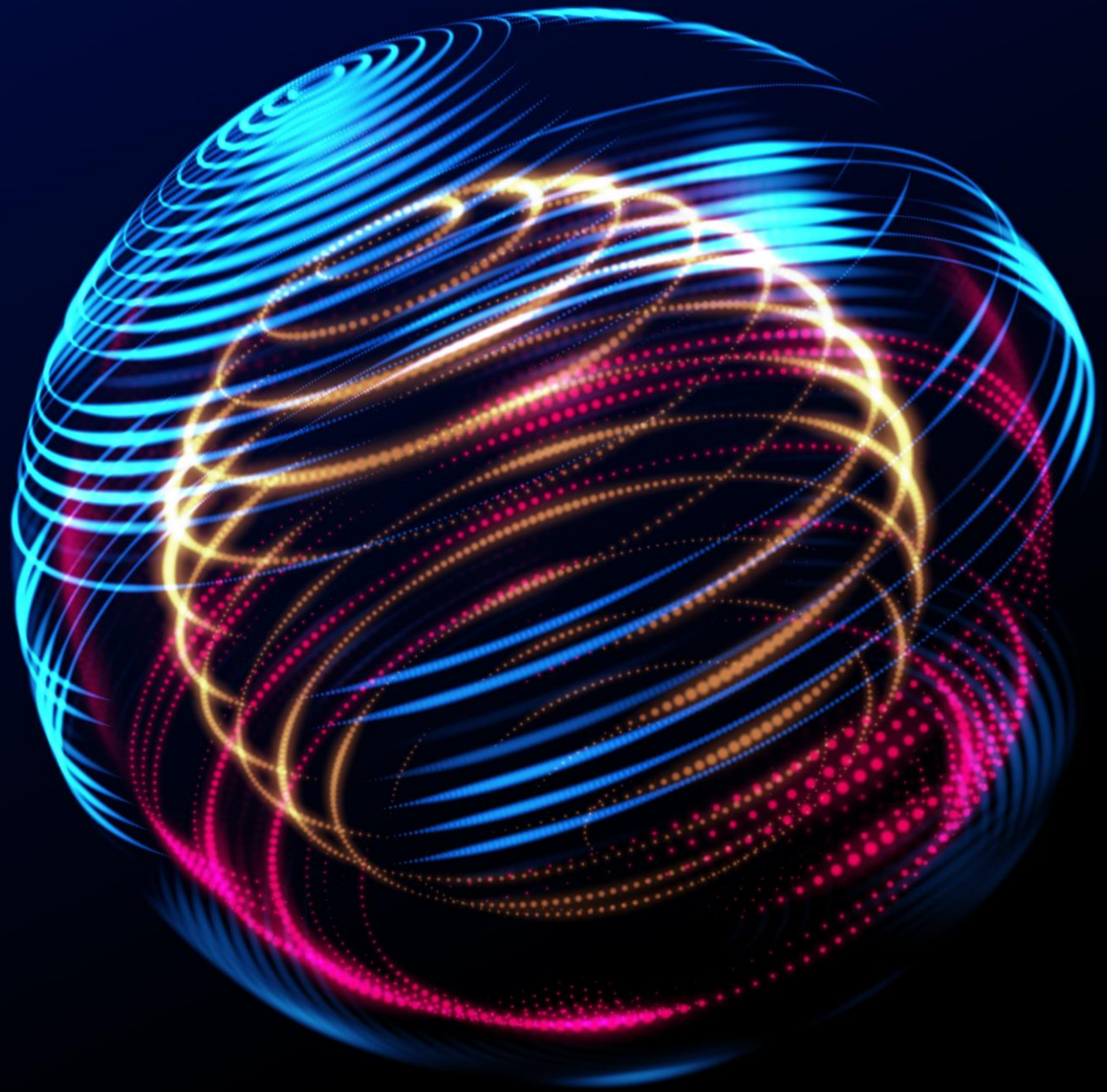
Deloitte’s Cyber Incident Recovery and Rebuild Services

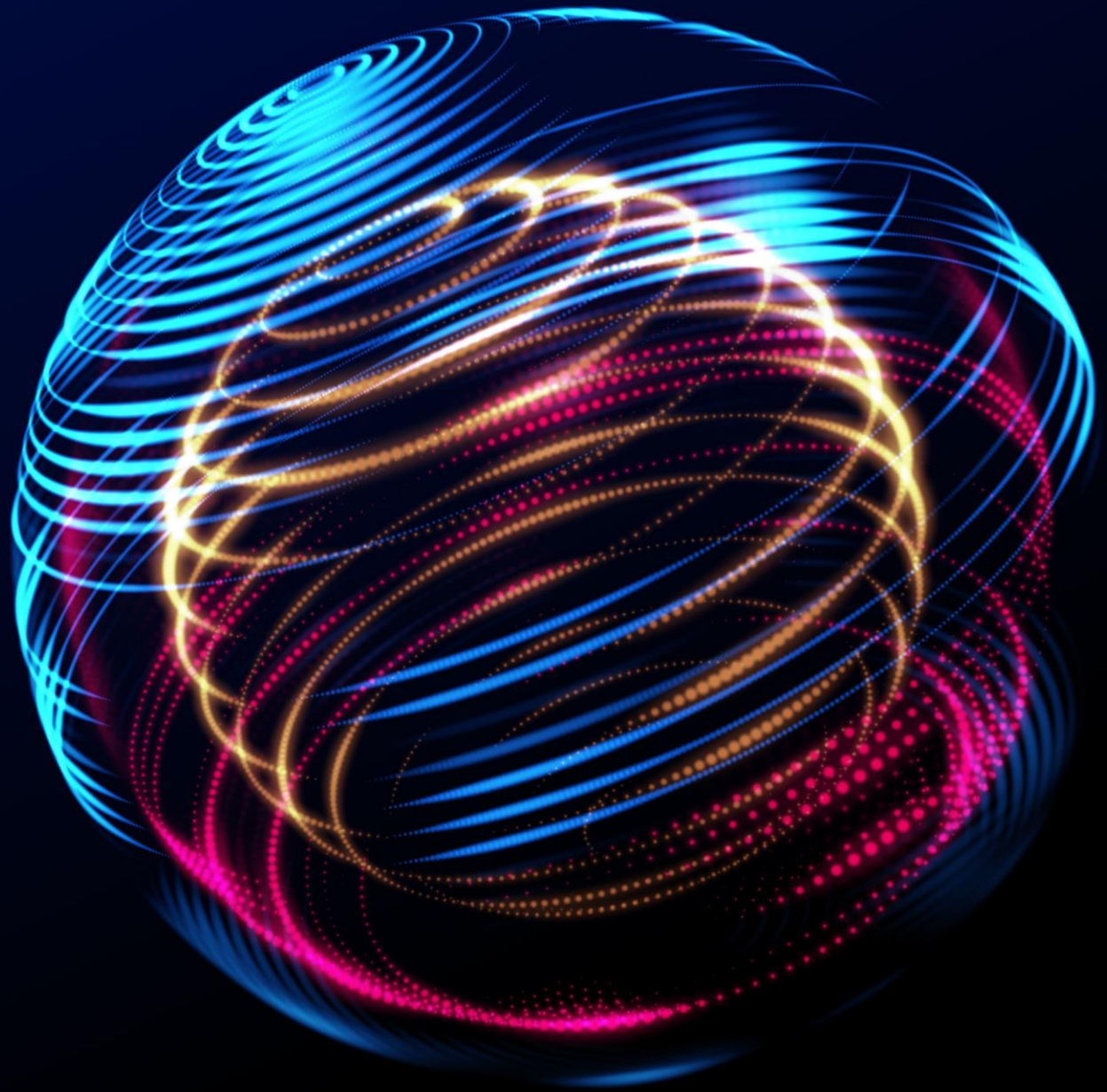
City of Hamilton
General Issues Committee

June 19th, 2024



Opening Remarks and Brief Introductions

Marnie Cluckie, City Manager



On February 25th, The City of Hamilton (“the City”) experienced a cybersecurity breach and ransomware attack that disabled many of the City’s IT systems

The City took **swift action** to **protect systems** and data

- Activated Emergency Operations Centre (EOC).
- Engaged a team of experts, insurer, legal counsel, and relevant authorities.
- Investigated to determine what systems were impacted.
- Contained the breach within **2 days.**
- Based on thorough forensic analysis, there is **no evidence that people’s personal data or information** has been compromised.

Cyber Incidents are on the rise, particularly extortion and attacks causing disruption to network, systems and device access

Financially Motivated

97% of cyber attacks in North America are financially motivated. [1]

Sophisticated Threats

Individuals or groups that intentionally cause harm to digital devices or systems are constantly enhancing their capabilities to carry out an attack undetected.

High-Value Targets

Government organizations are a high-value target for cyber crime. [2]

[1] For the period November 1, 2022, to October 31, 2023. Verizon DBIR Report 2024.

[2] Based on information provided in Sophos' The State of Ransomware Report 2023.

Cyber Incidents affect all levels of government and total billions of dollars in associated costs

ATTACK TARGETS

69%

of organizations at the **local/provincial/federal** level on average have experienced a ransomware attack in the last year across North America, **up 3% compared to the average** across all industries and sectors. [1]

RANSOMWARE COST

$3.0 Billion

is the estimated **total cost associated with ransomware incidents in Canada**, which includes an estimate of the loss caused by business interruption. [2]

[1] Sophos State of Ransomware 2023 report
[2] Canadian Cyber Incident Response Centre (CCIRC)

Deloitte was engaged for restoration and recovery activities, to advise on interim solutions, and to enable business continuity and future resilience

RECOVERY & RESTORE

Prioritizing and rationalizing across the entire application portfolio.

REBUILD/TRANSFORM

Enterprise planning that supports the desired future state of the City.

CYBER RESILIENCE

Strategy and roadmap reflecting the City's ideal cybersecurity future state.

COMMUNICATIONS

Proactive and reactive recovery plan communications strategy across internal and external stakeholders.

The City, in collaboration with external experts, responded as efficiently and effectively as possible

Deliberate and intentional approach to enable **service continuity** and best meet the needs of the community and staff

Initial response key milestones

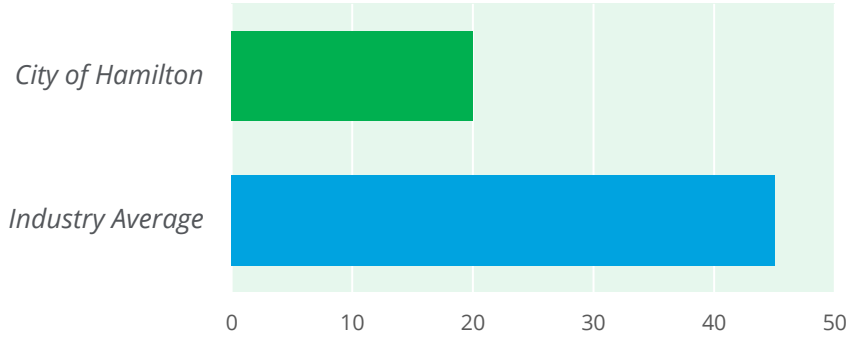
- Immediately contained the incident.
- Isolated impacted systems and created a new clean environment.
- Added enhanced monitoring on all systems.
- Initiated enhanced security measures.
- Prioritized recovery efforts on the most critical systems, particularly public health and safety.
- Following immediate efforts, prioritized core services and identified remaining recovery efforts required.

The effectiveness of the City's response to the attack was above the industry average

INCIDENT METRICS

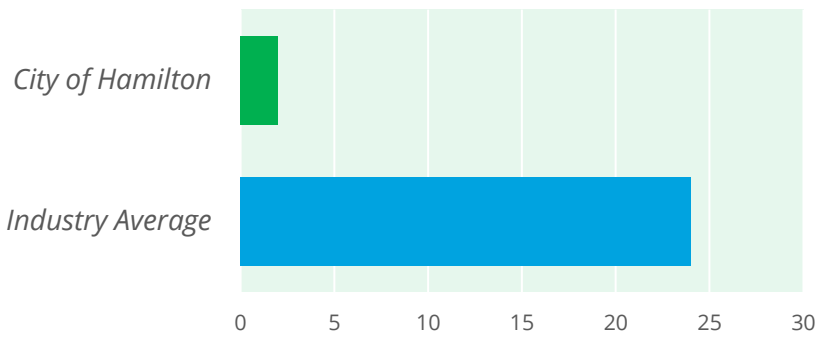
Time for the City to *detect* the incident

20 days



Time for the City to *contain* the incident

2 days



For the City, the threat actor moved **faster** than the **average of 45 days,** demonstrating increased sophistication.

For the City, the Response team **moved swiftly** to understand the threat and take appropriate actions, containing the active threat **in 2 days**.

Throughout the response, the City has taken a customer-centric approach to deliver core programs and services to the community, with more coming back regularly

CORE

Maintained critical services throughout.

ADAPTING

Supporting services through recovery or interim solutions.

CONTINUOUS UPDATES

Continuing to bring back applications regularly to further enhance service delivery.

Navigating a high level of impact, the City has been applying a strategic approach to restoration

Magnitude of Business Impact

The City has experienced a high level of operational impact due to the cyber incident.

The City has restored many of its critical applications that serve the public.

The City is strategically restoring services, identifying core systems, and considering immediate needs and the future state of City services.

The primary focus has been on critical components and fast-tracking priority systems and functionality

SERVICE RESTORATION

Ranked against impact/risk [1]:

1. Health & Safety
2. Council Priorities Alignment
3. Legislative/Contractual
4. Services Impact

PRIORITIZATION CONSIDERATIONS

- Organizational Impact
- Financial Impact
- Public Trust

RESTORATION PROGRESS

228
approximate applications impacted

45%
of total applications restored

48
of critical impacted applications

60%
of critical impacted applications restored

[1] No impact, minimal (alternatives available), medium, high.

Observations to-date

Impact

A significant breach that has had, and will continue to have, detrimental impacts to City services.

Timeline

Years not months for full recovery, sometimes requiring interim processes.

Infrastructure

Much of what needs to happen now (cyber and IT) was already planned.

Budget

Many key activities that need to happen are included in previously approved operating and forecasted capital budgets.

Opportunity

Build back stronger (customer-centric approach, improved service and efficiency, enhanced cyber resilience).

Go-forward approach

Decisions need to continue to balance key priorities, safety and security, speed, functionality and cost.

Moving forward on the path to Restore, Rebuild, Transform and Cyber Resilience

UNRECOVERABLE/ IMPACTED APPLICATIONS	END-OF-LIFE APPLICATIONS	CYBER RESILIENCE
Restore lost functionality.	Replace end-of-life applications (IT improvements or transformation) to enhance customer and staff experience.	Short-term and mid-term cybersecurity enhancements and transformation activities to protect from future attacks.

Next steps will lead with a focus on customer and staff experience, protecting against future incidents, and approaching everything through a lens of resilience

SERVICE AND IT ROADMAP

Partnering with the City to drive both immediate service restoration and enable long-term customer service enhancements.

CYBERSECURITY ROADMAP

Evaluate the City's current cybersecurity roadmap, identify enhancements, and deliver actionable recommendations.

Key considerations for the City's continued success

Invest in the future

Embrace opportunity to build back stronger.

Build resilience

Protect against future incidents.

Increase organizational agility and capacity

Innovate service delivery models.

Decrease procurement timeline

More agile models while maintaining the public interest.

Facilitate efficient decision-making

Enhance administration delegation of authority.

Focus on staff

Recognize staff capacity limitations to maintain existing services.

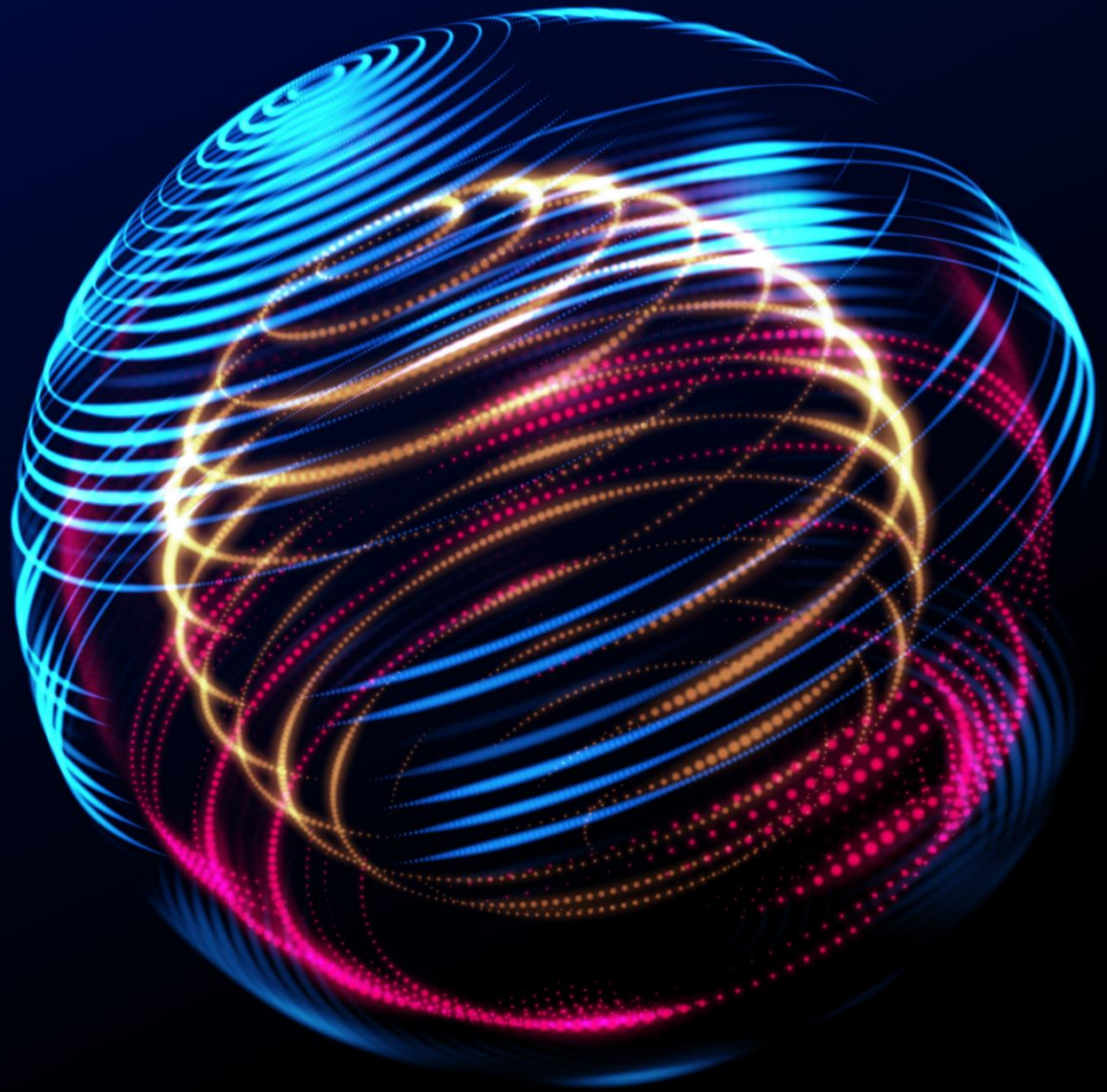
Moving forward with the City's large-scale effort to **build back stronger than ever**

SUMMARY

- Cyber incidents are on the rise in Canada, and Government organizations are a high-value target.
- The City took swift action to protect systems, and based on thorough forensic analysis, there is no evidence that people's personal data or information has been compromised.
- The City has taken a customer-centric approach in its response to deliver core programs and services to the community.
- The City has an unprecedented opportunity to build back stronger and modernize.
- There are key considerations to facilitate the City's continued success.

Thank You

Questions?



Deloitte.