Community Services Report to
Emergency Management Committee
2023 November 02

ISC: UNRESTRICTED
EM2023-1121

Status of Emergency Preparedness Focus on Risk – Cyber Risks

PURPOSE

To share information about cyber risks and the risk management strategies in place at The City of Calgary to prevent, mitigate, and prepare for these risks.

PREVIOUS COUNCIL DIRECTION

- The Emergency Management Bylaw requires the Calgary Emergency Management Agency to provide a Status of Emergency Preparedness Report annually to Emergency Management Committee. In addition, two reports and panel presentations are provided each year to allow meaningful conversations and ensure the Emergency Management Committee and Calgarians are well-informed on actions taken to address high risks for Calgary.
- Increasing cyber risks were recently addressed in the 2023 Mid-Year Principal Corporate Risk Report with Information Technology. Direction for Corporate Security was provided in the 2023-2026 Service Plans and Budgets, with an emphasis on improvements of cyber security incident response and mandatory cyber security awareness training for employees.
- Background and Previous Council Direction is included as Attachment 1.

RECOMMENDATION: That the Emergency Management Committee recommend that Council receive this report for the Corporate Record.
RECOMMENDATION OF THE EMERGENCY MANAGEMENT COMMITTEE, 2023 NOVEMBER 02: That Council receive this report for the Corporate Record.

CITY MANAGER/GENERAL MANAGER COMMENTS

GM Katie Black concurs with this report.

HIGHLIGHTS

- **To create a safe and resilient city, it is important for Calgarians to be well-informed about disaster risks and the actions being taken to address those risks.**
  If Calgarians and City employees are aware of the top disaster risks for Calgary, and understand how they can prepare, they will be able to take actions that protect themselves, their workplaces, families, and communities.

- **Cyber risks are increasing for both Calgarians and the services Calgarians rely on for health and safety.**
  The City of Calgary's Disaster Risk Assessment has determined that cyber risks are a medium risk for Calgarians with risk trending upward. Essential service providers, such as municipal governments, are attractive targets, and research shows that cyber security threats to government and public services have been rapidly increasing.

Status of Emergency Preparedness Focus on Risk ‑ Cyber Risks

- **Cyber events have the potential to cause significant disruptions and losses.** A cyber event at The City could lead to disruption of essential services, significant financial losses, exposure of Calgarians' private data, erosion of trust in technology systems, and damage to facilities and systems that could cause physical harm or loss of life.
- **There are risk management strategies in place at The City of Calgary for cyber events.** City of Calgary business units work together to implement plans, policies, and training to prevent, mitigate, and support The City during cyber events.

DISCUSSION

Identifying Risks for Calgarians

The City of Calgary completes a Disaster Risk Assessment to understand local risks and to develop strategies to reduce and manage the impact of future events. Risk is determined by the severity and frequency of an event, the number of people and assets exposed to the hazard, and socioeconomic, physical, and environmental factors. The assessment is updated annually, and a detailed *Disaster Risk Report* is released every four years with the service planning cycle.

In the Disaster Risk Assessment, risks are community focused; however, the focus of this report will be the impacts of cyber risks to The City of Calgary and operations. A significant cyberattack on The City could cause substantial impact to the community and public safety, which may require a citywide response coordinated through the Calgary Emergency Management Agency.

Cyber Risks and Service to Calgarians

Essential services provided by The City have become reliant on connectivity, creating increased vulnerability and potential impacts on public safety. A cyberattack on systems used by 911, for example, could make it difficult for Calgarians to reach emergency help. There have been recent examples of cyberattacks on municipalities. In May 2023, a ransomware attack on The City of Dallas impacted several essential services. The attack shut down websites and facilities, delayed services for multiple business lines, and required the use of manual 911 dispatch.

Although cyber risks can impact both individuals and organizations spanning all sectors, the Canadian Centre for Cyber Security has recently asserted that essential critical infrastructure services are at a particular increasing risk of cyber threats. The *2023-2024 National Cyber Threat Assessment* notes that these services are an attractive target for ransomware as there is a perception that providers will be willing to pay large ransoms to ensure continuity of services.

Cyber Risks: The City as a Target

Recent research in the *BlackBerry Global Threat Intelligence Report* shows that governments are facing a 40 per cent increase in cyberattacks in 2023. Although municipalities are not the number one target, they are an attractive target due to multiple lines of business. A joint publication by the Canadian Centre for Cyber Security and other global agencies, *Cybersecurity Best Practices for Smart Cities*, notes that technologically connected cities such as Calgary are at increased risk for cyber threats. Technological innovation can create safer, more efficient, more resilient cities; however, this also introduces potential vulnerabilities.

Potential cyber security threats to The City include ransomware events, cloud services incidents, supply chain security risks, denial of services, and business email compromise.

These threats can be caused by accidents, negligence, or disgruntled employees, and/or cyber crime, cyber espionage, or cyber terrorism and hacktivism. Artificial Intelligence and large language models (e.g., ChatGPT) have created new challenges, such as allowing threat actors to create targeted phishing emails and the ability to create more effective malware.

Preventing and Mitigating Cyber Risks at The City of Calgary

Corporate Security and Information Technology are the business units responsible for managing and assessing cyber risk at The City of Calgary and analyzing the environment for any possible cyberattacks to protect The City's information assets. They work together with other partners to identify, prevent, and mitigate cyber risks at The City of Calgary.

Strategies used to prevent and mitigate cyber risks at The City include:

- Engaging with business units throughout the organization about technology risks.
- Making The City a hard target; that is, making a threat actor use more resources.
- Investing in industry-leading cyber security tools that allow for the identification of tactics, techniques, and procedures used by threat actors.
- Leveraging external partnerships with Government of Alberta, other municipalities, other organizations, and vendors to better understand challenges and solutions.
- Monitoring of industry trends related to cyber threats and mitigations.
- Following industry best practices related to cyber security, such as National Institute of Standards and Technology, Government of Alberta, and Government of Canada.
- Protecting technology infrastructure through continuous modernization.
- Promoting resiliency through redundant infrastructure and leveraging cloud.

The City implements a range of policies and training to help prevent cyber risks:

- As of August 2022, all City staff and contractors with an email address are required to complete cyber security awareness training on an annual basis.
- City employees must safeguard assets and information, as per the Acceptable Use of City Technology Resources Policy, which is part of The City's Code of Conduct.
- The City's Information Management and Security Policy provides the foundation for other security standards to guide managers and employees on information risks.

Preparing The City of Calgary for Cyber Events

The City's *Municipal Emergency Plan* provides an overarching plan to guide response and recovery to any type of emergency. A significant cyber event could activate the overarching plan and select annexes. Attachment 2 summarizes the Municipal Emergency Plan and its annexes.

The City implements a range of plans and policies to prepare for and mitigate cyber risks:

- Regular spring and fall simulated scenario exercises validate emergency plans, procedures, policies, and communication strategies. In February 2023, a cyberattack exercise was conducted to test processes and plans.
- Information Technology has a crisis management response team and crisis management plans in place in the event of cyberattacks.
- Corporate Security has a dedicated incident response team that is responsible for the development, testing, and actioning of cyber incident response plans.

- Administration has a policy dedicated to business continuity planning, intended to ensure City services can continue operating during disruptions, such as a cyber event. Compliance with this policy was 100 per cent by City business units during the last reporting period.
- The Emergency Management & Community Safety business unit manages a public/private partnership, the Calgary Critical Infrastructure Network*,* that ensures critical infrastructure owners and operators in Calgary have a common understanding of risks, including cyber risks, and are working towards more resilient systems.

EXTERNAL ENGAGEMENT AND COMMUNICATION

☐ Public engagement was undertaken

☐ Public/interested parties were informed

☒ Dialogue with interested parties was undertaken

☐ Public communication or engagement was not required

The City engages nearly 60 Calgary Emergency Management Agency member organizations in education, training, simulated exercises, emergency response planning, and communications. The Agency consists of City of Calgary business units, government agencies, critical infrastructure operators, utilities, schools, industry groups, and community service providers.

IMPLICATIONS

Social

Cyberattacks have the potential to disrupt services to Calgarians, including social services provided by The City. The City's emergency planning aligns with the *Social Wellbeing Policy* of prevention by ensuring the social impacts of disasters are mitigated before disasters occur.

Environmental

Cyberattacks have the potential to disrupt critical infrastructure services and cause physical impacts to infrastructure, which could negatively impact the environment.

Economic

A cyberattack against The City could lead to significant financial losses. A recent report by IBM states that the global average cost of a data breach in 2023 was four and a half million US dollars, a 15 per cent increase over three years. Calgary Emergency Management Agency work addresses the *Economic Resilience Strategy*, as mitigation efforts will result in future savings.

Service and Financial Implications

Other: No anticipated financial impact as a result of this report

Planning, training, education, and operational activities for cyber risks, as well as disaster response planning and preparation exist in the 2023-2026 Service Plans and Budgets. Corporate Security has current capital budget for cyber risk prevention and response.

RISK

A cyberattack against The City of Calgary could lead to disruption of essential infrastructure services, significant financial losses, exposure of Calgarians' private data, erosion of Calgarians' trust in the technology systems, and damage to infrastructure facilities and systems that could cause physical harm or loss of life. Literature indicates that managing disaster risk is more economically, socially, and environmentally sound than managing disaster consequence.

Community Services Report to
Emergency Management Committee
2023 November 02

ISC: UNRESTRICTED
EM2023-1121

Status of Emergency Preparedness Focus on Risk ‐ Cyber Risks

ATTACHMENTS

1. Background and Previous Council Direction
2. Municipal Emergency Plan Annex Summary
3. Presentation

Department Circulation

Director	Department	Approve/Consult/Inform
Michael Tillotson	Corporate Security	Consult
Jan Bradley	Information Technology	Consult

Author: Anita Blackstaffe, Emergency Management & Community Safety

City Clerks: B. Dufault / A. de Grood