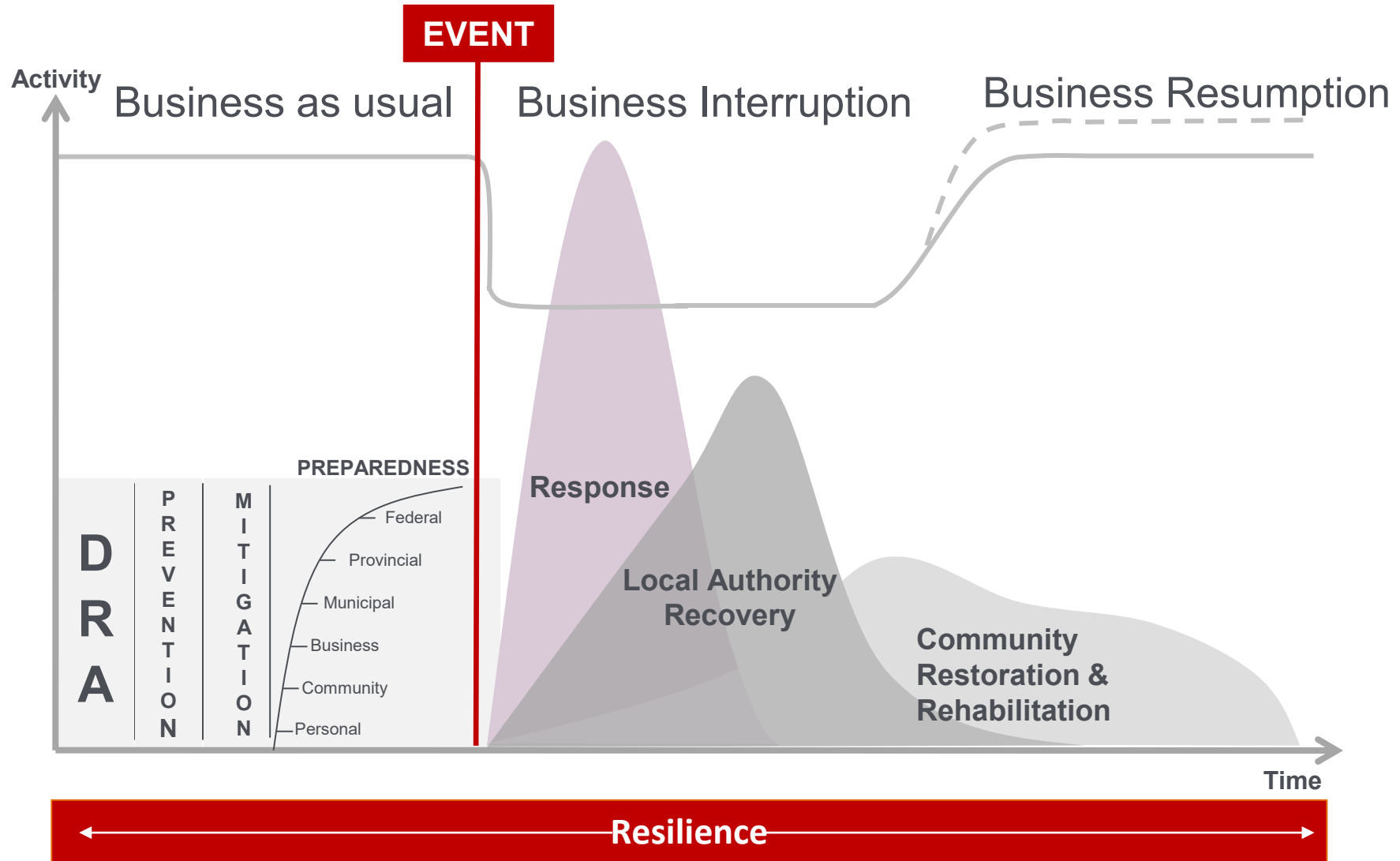2023 November 2

Status of Emergency Preparedness Focus on risk: Cyber risks

Recommendation

That the Emergency Management Committee recommend that Council receive this report for the Corporate Record.
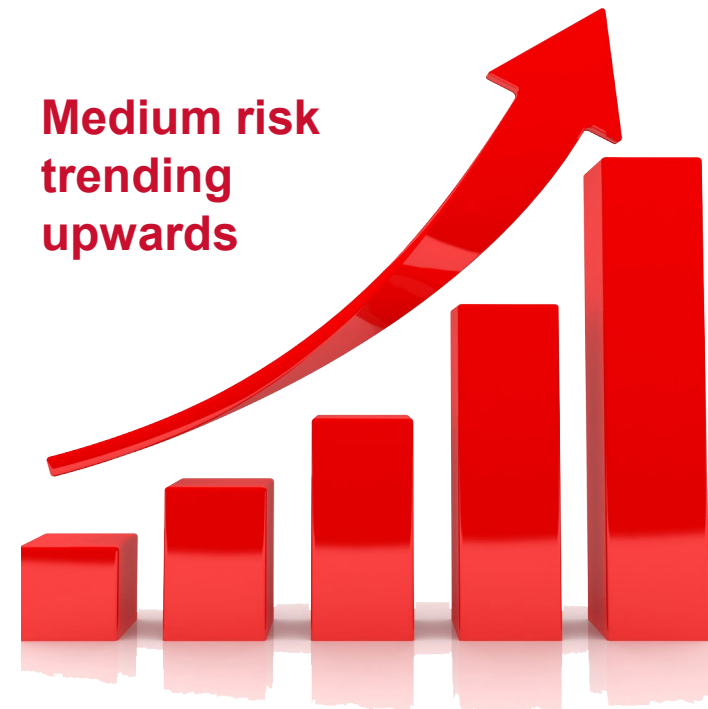
Emergency management model

Cyber risks & service to Calgarians

- Risk to public health & safety

  - Disrupt services

  - Impact public safety

  - Affect communication

Medium risk trending upwards

Prepared & ready to respond

Presentation overview

- Programs & policies to prevent harmful cyber activities

- Mitigation strategies & IT security actions

- City support for organizations with critical infrastructure

- Corporation's business continuity program

Information Security

The City is a target

- Increased attacks on municipalities & local governments

- National Cyber Threat Assessment 2023-2024: Critical infrastructure at growing risk

- 40% more cyberattacks on governments in 2023 than previous years

- Municipalities targeted due to:
  - Multiple business lines
  - Large attack surface from numerous applications & complex infrastructure

- Canadian Centre for Cyber Security + 6 global agencies: Joint guidelines on cybersecurity for smart cities
  https://www.cyber.gc.ca/en/news-events/joint-publication-cyber-security-best-practices-smart-cities#defn-cyber-threat

Cyber security threats to The City

- According to research, the average cost to a cyberattack globally is about US $4.5 million

- Cyber security threats to The City
  - Ransomware can lead to both operational or financial impacts
  - Incidents experienced by cloud services & other third parties
  - Supply chain security risks
  - Denial of Services
  - Business email compromise

How AI has changed things

- Artificial intelligence (AI) & large language models (e.g., ChatGPT) provide benefits to both organizations & threat actors

- AI allows phishing emails to be more targeted & include multiple languages

- Threat actors have created their own large language models that can be used to create a larger quantity of malware that is more effective
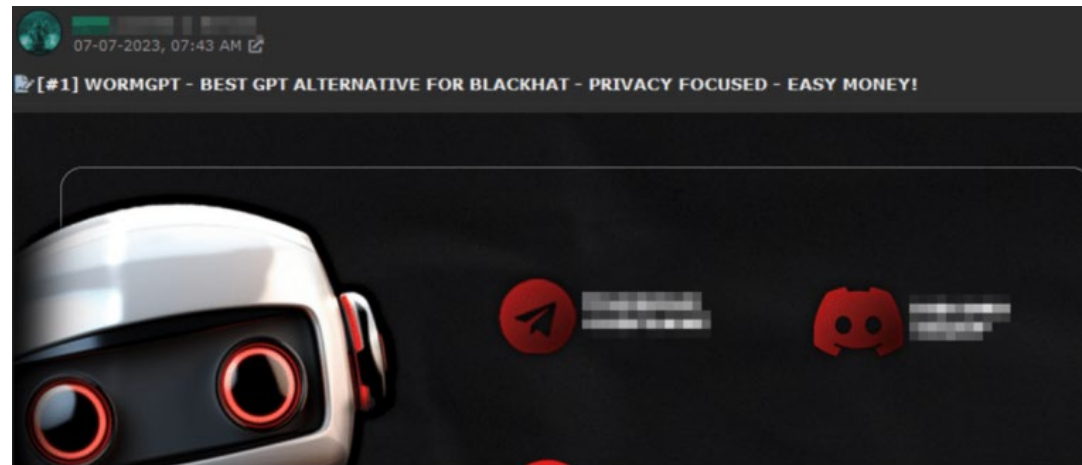

Image: SlashNext.com

What are we doing

- Making The City a hard target
  - Increase resources required for threat actors

- Capital investments in cyber security
  - Ensure efficient & effective City security operations
  - Use industry-leading tools

- Collaboration is key
  - Work closely with business partners throughout the organization
  - Cannot operate in a silo

Information Technology

According to Cybersecurity Ventures…

There is no end to cyber risk…executive board level conversations must shift to how we actively improve cyber resilience.

Types of threats

- Key characteristics
  - Inexpensive to highly sophisticated
  - Single actor to state-sponsored
  - Easily available tools & utilities
  - Significant impact/highly effective
  - Evades detection

- Types of threats
  - Accidental
  - Negligence
  - Disgruntled employees
  - Cyber crime
  - Cyber espionage
  - Cyber terrorism & hacktivism

What we are doing

- Adopting industry best practices

- Investing in continuous modernization

- Collaborating with internal partners

- Leveraging external partnerships

- Monitoring industry trends

- Expanding resiliency for critical infrastructure

Information Technology at The City

Multi-factor authentication / secure remote access

Segmentation of infrastructure & applications

Business continuity for critical applications

Real-time monitoring & logging

Robust patching & hardware lifecycles

Focus on security for application development & maintenance

Secure & compliant technology procurements

Education & training (Acceptable Use Policy)

Crisis management practices & procedures

Restoration & recovery mechanisms & processes
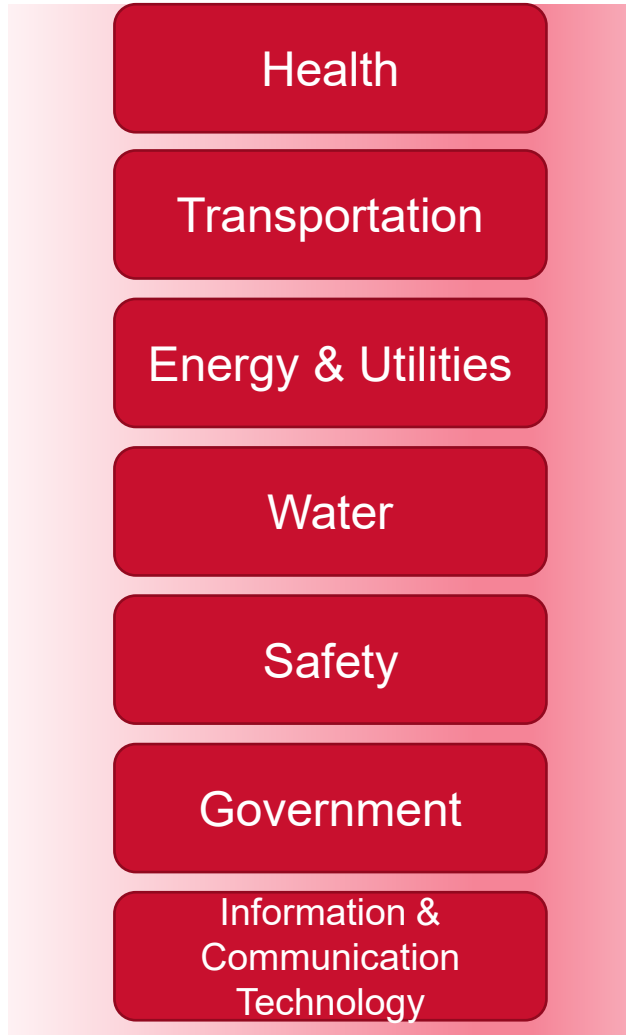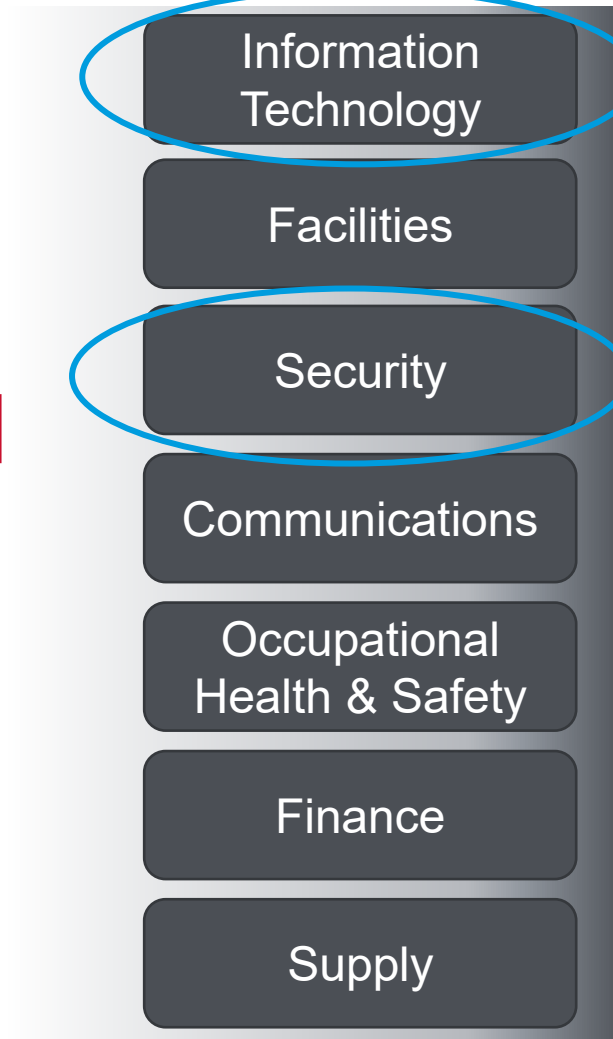
Optimization Services

Building critical infrastructure resiliency

Calgary Critical Infrastructure Network

Corporate Business Continuity of Agency Members

| Calgary Critical Infrastructure Network	Corporate Business Continuity of Agency Members
Health	Information Technology
Transportation	Facilities
Energy & Utilities	Security
Water	Communications
Safety	Occupational Health & Safety
Government	Finance
Information & Communication Technology	Supply

Customer Operations

Enable

Corporate Services

Supporting essential City service delivery

City Business Continuity Planning Policy

- Ensures City services can continue operating during disruptions

- Policy deemed effective by City Auditor's Office

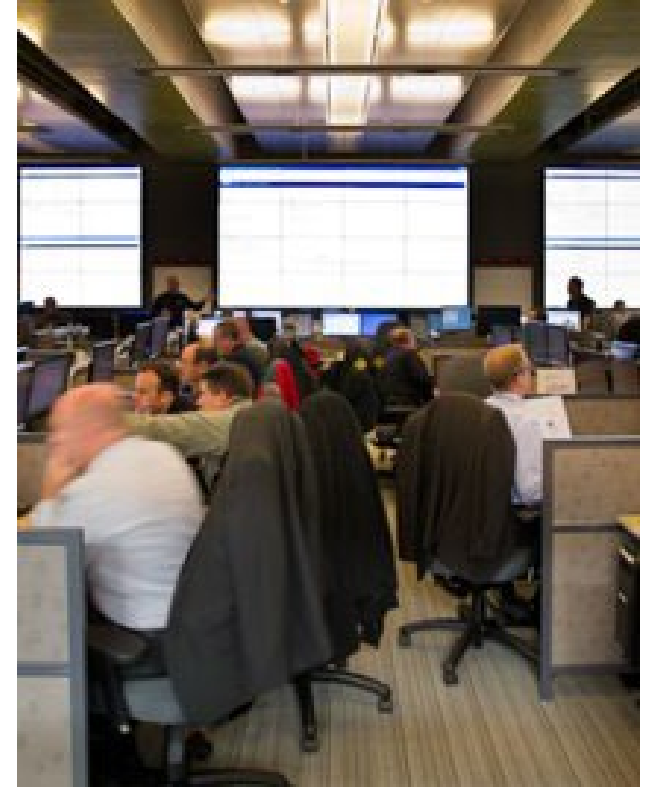- 100% policy compliance by City business units
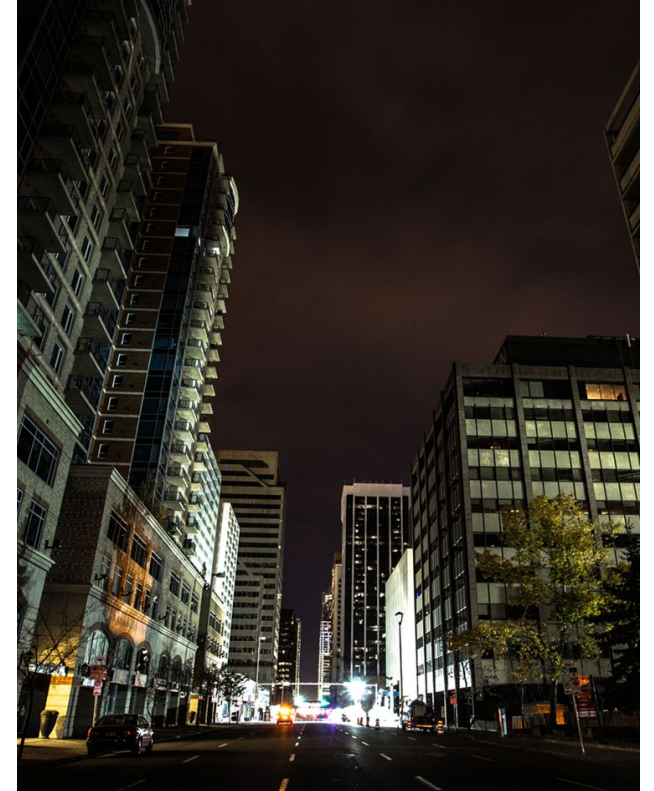
Emergency Management & 911

Building a safe, resilient City

Collaborating to maintain essential services to Calgarians

- Working together to prevent, prepare, mitigate, & respond

- Event coordination through the Emergency Operations Centre

- Cyberattack exercises

Recommendation

That the Emergency Management Committee recommend that Council receive this report for the Corporate Record.