City of Toronto
Cyber Security Program

Information & Technology

October 2019

Audit Committee October 25, 2019 - Item AU4.1

TORONTO

Context

- Ensuring business continuity of City services to residents, businesses and the public is critical.
- With new threats arising daily, there is a growing need to improve how we protect the City's network, private information and data.
- The global impact of cybercrime will cost $6 trillion annually by 2021, up from $3 trillion in 2015[1].
- Transitioning to a digitally-enabled government demands investment in cyber security across the City of Toronto.
- 90% of IT Security breaches occur because of an internal mistake and 60% are result of an internal attack.[2]
- City will use the recommendations in the Auditor General's report to enhance the City's cyber security and the detection, protection, prevention and responses to future cyber threats.

[1] Digital Government 2030: Parental Governments Augment Internal Capabilities – Gartner January 2018

[2] www.cio.com IBM and Harvard Business Review 2016

Cyber Security Measures

- The City currently uses network protection technology and cyber security practices to secure its infrastructure and has made progress on a number of initiatives to improve security and ensure the protection of our assets:
  - Established a formal Cyber Security Program in 2018, and as a result, we have a better understanding of cyber security risks and have taken steps to implement appropriate cyber security practices.
  - The City has rolled out mandatory cyber security awareness training for all City staff to help them recognize and report possible cyber threats and learn leading practices on how to safely use the City's IT systems and assets.
  - Using best practices from the Canadian Centre for Cyber Security, the City implemented enhanced password rules for City staff to create stronger passwords and to strengthen access to networks and systems.
  - The City will continue to proactively run vulnerability assessments, penetration testing and threat risk assessment services to identify and manage cyber risks.
  - A new position, Chief Information Security Officer, was implemented in 2019 with accountability to establish a business aligned cyber strategy, advise on/manage cyber risk and mature the existing cyber posture.

Moving Forward

- Continued partnership with Auditor General’s Office on activities to address recommendations and support further assessments/audits.
- Continue Cyber Security Training and next stages roll-out to ensure City staff maintain awareness and recognize cyber threats and how to safely use the City’s assets.
- Ensure effective Corporate IT security oversight and governance City wide.
- Ensure future resources/investment to support cyber security activities.
- Accelerate actions where possible and report on progress.

Questions

Lawrence Eta

Chief Technology Officer

Lawrence.Eta@toronto.ca

Kush Sharma

Chief Information Security Officer

Kush.Sharma@toronto.ca