REPORT FOR ACTION WITH CONFIDENTIAL ATTACHMENT

Cybersecurity Incidents at the City and its Agencies and Corporations: Integrated Incident Response Plan is Needed

Date: February 4, 2021
To: Audit Committee
From: Auditor General
Wards: All

REASON FOR CONFIDENTIAL INFORMATION

This report involves the security of property belonging to the City or one of its agencies and corporations.

The attachment to this report contains information explicitly supplied in confidence to the City of Toronto which, if disclosed, could reasonably be expected to impact the safety and security of the City and its services.

SUMMARY

Over the past decade, the City of Toronto, like other large organizations, is increasingly conducting business and key operations online in a networked environment. This makes operations more efficient and citizens are served better.

The purpose of this report is to communicate security incidents that occurred at a City division and a City organization and to highlight the importance and urgency for the City to have a standard incident management process developed and implemented across City divisions and its agencies and corporations.

A standard incident management process will enable the Chief Information Security Officer (CISO) to analyze these attacks and develop a coordinated response on any potential cyberattacks. This will enhance City-wide cybersecurity.

In a 2019 Report for Action[1], the Auditor General highlighted the importance and urgency for the City to develop a standard incident management process and implement it across City divisions, agencies and corporations.

We have made additional recommendations in one other report entitled "Information Technology Projects Implementation: Information Privacy and Cybersecurity Review of Human Resource System" that is also being tabled at the February 16, 2021 Audit Committee.

The confidential report attached provide more details of the nature of incident and management actions. The work performed in relation to this report does not constitute an audit conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS). However, we believe we have performed sufficient work and gathered sufficient appropriate evidence to provide for a reasonable basis to support our observations and recommendations.

This public report contains two administrative recommendations. The confidential information and recommendations are presented separately to this report in Confidential Attachment 1. The confidential report will be made public at the discretion of the Auditor General after discussing with appropriate City Official.

RECOMMENDATIONS

The Auditor General recommends that:

1. City Council request the Auditor General to provide presentations to City organizations (major agencies and corporations) on the City cybersecurity reports and lessons learned.

2. City Council adopt the confidential recommendations contained in Confidential Attachment 1 to the report (February 4, 2021) from the Auditor General.

3. City Council direct that Confidential Attachment 1 be released publicly at the discretion of the Auditor General, after discussions with the appropriate City Officials, as it contains information involving the security of property belonging to the City or one of its agencies and corporations and information explicitly supplied in confidence to the City of Toronto which, if disclosed, could reasonably be expected to impact the safety and security of the City and its services.

4. City Council request the City Manager to forward Confidential Attachment 1 to City Division Heads and Chief Executive Officers of major City agencies and corporations and request them to review and implement the recommendations that may be relevant to their respective operations.

1 https://www.toronto.ca/legdocs/mmis/2019/au/bgrd/backgroundfile-135368.pdf

FINANCIAL IMPACT

The recommendations contained in this report do not have any additional financial impact other than the amounts approved in the Auditor General's Office (AGO) budget.

DECISION HISTORY

The Auditor General recognizes the increased risks of cyberattacks and has been proactive in performing cybersecurity audits at the City. Her 2021 Work Plan includes cybersecurity audits of the City's critical infrastructure as well as the agencies and corporations. Our most recent reports are:

1. Cyber Safety - Critical Infrastructure Systems: Toronto Water SCADA System, January 24, 2020
https://www.toronto.ca/legdocs/mmis/2020/au/bgrd/backgroundfile-145342.pdf

2. Cyber Safety: A Robust Cybersecurity Program Needed to Mitigate Current and Emerging Threats, October 8, 2019
https://www.toronto.ca/legdocs/mmis/2019/au/bgrd/backgroundfile-138905.pdf

COMMENTS

According to a 2018 Statistics Canada survey, Canadian businesses were most likely impacted by cyber incidents to steal money or demand a ransom payment.[2] However, there could be far worse implications, such as the extraction of sensitive data or disruption of critical systems without the attacker leaving a footprint.

As noted, in EY's Global Cybersecurity report "How to manage cyber risk with a Security by Design approach"[3]:

“Ultimately the most damaging and lasting effect of these incidents, particularly when not quickly dealt with and mitigated, is the loss of trust between people and the organizations or institutions they depend on."

"When data confidentiality, integrity or availability are compromised, or products and services cease to perform as expected, trust built over years can be lost in a day.”

Coordinated approach across the City, going forward

There needs to be a holistic view and open communication between City organizations the Office of the CISO and the Chief Technology Officer. A One-City, unified approach

2 https://www150.statcan.gc.ca/n1/pub/85-002-x/2019001/article/00006-eng.htm

3 https://www.ey.com/en_ca/consulting/how-to-manage-cyber-risk-with-a-security-by-design-approach

requires assessments of vulnerabilities, communication on what needs to be done, and incident response protocols. Designing communication and action protocols supporting a unified best practices approach will be vital to protecting the City, its systems and information.

Following are some key actions that should be taken by the City and its agencies and corporations:

- The Auditor General typically recommends that her reports be forwarded through City Manager's Office to agencies and corporations so that they may understand the risks the City faces and consider the recommendations in light of their own organizations. It is important that these reports be shared in a timely manner.

- Share expertise and lessons learned in confidence through a centralized cyber function established through initiatives by the Office of the CISO.

- Train staff and implement processes and technology in a coordinated manner to build a unified technology environment that can support one another in protecting, detecting, responding to and mitigating the impacts of cyberattacks. The Office of the CISO can play a lead role in this initiative.

The City is moving forward in cybersecurity, but there is a continuing need to invest strategically in the City-wide implementation of a cybersecurity vision. City agencies and corporations should leverage the leadership, expertise, and tools of the Office of the CISO to protect the City from cyberattacks.

CONTACT

Syed Ali, Audit Director, IT & Strategy, Auditor General's Office
Tel: 416 392-8438, Fax: 416-392-3754, E-mail: Syed.Ali@toronto.ca

Gawah Mark, Senior Audit Manager, Auditor General's Office
Tel: 416-392-8439, Fax 416 392-3754, E-mail: Gawah.Mark@toronto.ca

SIGNATURE

Beverly Romeo-Beehler
Auditor General

ATTACHMENTS

Confidential Attachment 1 - Cybersecurity Incidents at the City and its Agencies and Corporations: Integrated Incident Response Plan is Needed