REPORT FOR ACTION WITH CONFIDENTIAL ATTACHMENT

Auditor General's Cybersecurity Review: Toronto Fire Services Critical Systems Review Phase 2

Date: May 20, 2022
To: Audit Committee
From: Auditor General
Wards: All

REASON FOR CONFIDENTIAL INFORMATION

The Confidential Attachment 1 to this report involves the security of the property of the City of Toronto.

SUMMARY

Cyberattacks are widely considered to be one of the most critical operational risks facing organizations. The Auditor General has taken a proactive approach in planning her audits and has included them in her annual work plans[1].

This Phase 2 report is an extension of our work that was underway when we issued our first report entitled "Auditor General's Cybersecurity Review: Toronto Fire Services Critical Systems Review"[2] and completes our review of critical systems at Toronto Fire Services (TFS).

At the February 2022 Audit Committee, TFS provided a public report with a confidential attachment on the implementation status of our Phase 1 recommendations.[3] This report contains two administrative recommendations. The findings and recommendations from our Phase 2 review are contained in Confidential Attachment 1.

1 https://www.torontoauditor.ca/reports/type/work-plans/

2 https://www.toronto.ca/legdocs/mmis/2021/au/bgrd/backgroundfile-172402.pdf

3 https://www.toronto.ca/legdocs/mmis/2022/au/bgrd/backgroundfile-199277.pdf

RECOMMENDATIONS

The Auditor General recommends that:

1. City Council adopt the confidential instructions to staff in Confidential Attachment 1 to this report from the Auditor General.

2. City Council direct that Confidential Attachment 1 to this report from the Auditor General be released publicly at the discretion of the Auditor General, after discussions with the appropriate City Officials.

FINANCIAL IMPACT

Implementing the cybersecurity audit recommendations will strengthen cybersecurity controls at the City. The extent of costs and resources needed to implement the recommendations is not determinable at this time. The investment needed to improve controls to manage and respond to cyber threats offsets the potentially significant costs that could result from security breaches, which could include data recovery/cleanup, financial loss, reputational damage, fines or litigation.

DECISION HISTORY

The Auditor General has conducted several cybersecurity audits at the City. The Phase 1 report included the results of a review of critical systems in Toronto Fire Services (TFS) tabled at the November 2, 2021 Audit Committee.

https://www.toronto.ca/legdocs/mmis/2021/au/bgrd/backgroundfile-172402.pdf

Her 2022 Work Plan includes cybersecurity audits of the City's critical infrastructure as well as its agencies and corporations. The Auditor General's 2022 Work Plan is available at:

https://www.toronto.ca/legdocs/mmis/2021/au/bgrd/backgroundfile-172597.pdf

COMMENTS

With cybersecurity threats evolving, TFS, like many organizations across Canada, needs to proactively identify, track and address evolving cybersecurity risks. Cyberattacks are unauthorized attempts (successful or not) to gain access to a system and confidential data, modify it in some way, or delete or render information in the system unusable. In January 2022, national cybersecurity agencies in Canada, the US and the UK warned organizations of the increased risks of Russian state sponsored attacks to critical infrastructure.

The Canadian Centre for Cyber Security advises that Canadian infrastructure critical infrastructure network operators should[4]:

"Increase organizational vigilance. Monitor your networks with a focus on the TTPs[5] reported in the CISA advisory[6]. Ensure that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior. Enable logging in order to better investigate issues or events."

TFS provides essential services to millions of Torontonians by responding to emergency calls related to fires, illnesses, accidents and many other hazards. It is the largest fire service in Canada, and the fifth largest in North America.

In her Phase 2 review of selected TFS critical systems, the Auditor General has made three confidential recommendations in Confidential Attachment 1. The Auditor General will perform a follow up review after management has implemented the recommendations. The results of the Auditor General's follow-up of outstanding recommendations will be provided to Council through the Audit Committee.

As cybersecurity threats expand and evolve, the Auditor General will continue to perform her work on cybersecurity and making recommendations to improve the security of critical systems.

Finally, we would like to express our appreciation for the co-operation and assistance we received from the management and staff at Toronto Fire Services, Technology Services Division and the Office of the Chief Information Security Officer. The timely provision of information and coordination of various activities by management has greatly helped us to complete this review.

The procedures and work performed for this report do not constitute an audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). However, we believe the work performed and information gathered provide a reasonable basis for our findings, conclusions and recommendations.

CONTACT

Syed Ali, Assistant Auditor General (A), IT and Strategy, Auditor General's Office
Tel: 416 392-8438, Fax: 416-392-3754, E-mail: Syed.Ali@toronto.ca

Gawah Mark, Audit Director (A), Auditor General's Office
Tel: 416-392-8439, Fax 416 392-3754, E-mail: Gawah.Mark@toronto.ca

4 https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-centre-urges-canadian-critical-infrastructure-operators-raise

5 tactics, techniques and procedures (TTPs)

6 https://www.cisa.gov/uscert/ncas/alerts/aa22-011a

SIGNATURE

Beverly Romeo-Beehler
Auditor General

ATTACHMENTS

Confidential Attachment 1: Auditor General's Cybersecurity Review: Toronto Fire Services Critical Systems Review Phase 2