July 12, 2021 Sent via email

John Elvidge
City Clerk
13th Floor West
100 Queen Street West
Toronto, Ontario
M5H 2N2

Dear Mr. Elvidge:

Re: Toronto Police Service IT Infrastructure: Cyber Security Assessment Phase 1

At its meeting held on June 24, 2021, the Toronto Police Services Board was in receipt of a report from Beverly Romeo-Beehler, Auditor General, City of Toronto with regard to the Toronto Police Service IT Infrastructure: Cyber Security Assessment Phase 1.

The Board received the Auditor General's report and agreed that a copy be forwarded to the City of Toronto - City's Audit Committee.

A copy of Board Minute P2021-0624-3.0. regarding this matter is attached.

Please do not hesitate to contact me at 416-808-7265 if you have any questions regarding this matter.

Yours truly,

Diana Achim
Board Administrator

Attachment: BM P2021-0624-3.0

This is an Extract from the Minutes of the Virtual Public Meeting of the Toronto Police Services Board that was held on June 24, 2021

P2021-0624-3.0. Toronto Police Service IT Infrastructure: Cyber Security Assessment Phase 1

Deputation: Derek Moran

The Board was in receipt of a report dated June 15, 2021 from Beverly Romeo-Beehler, Auditor General, City of Toronto.

The Auditor General recommends that:

1. The Board adopt the confidential recommendations contained in Confidential Attachment 1 to this report from the Auditor General.

2. The Board direct that all information contained in the Confidential Attachment 1 to the report to remain confidential.

3. The Board forward this report to City Council through the City's Audit Committee for information.

The Board received the deputation and the foregoing report.

Moved by: F. Nunziata
Seconded by: A. Morgan

REPORT FOR ACTION WITH CONFIDENTIAL ATTACHMENT

Toronto Police Service IT Infrastructure: Cyber Security Assessment Phase 1

Date: June 15, 2021
To: Toronto Police Services Board
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 Toronto Police Service which, if disclosed, could reasonably be expected to impact the safety and security of the City, its services and residents.

SUMMARY

The Toronto Police Service (TPS) employs nearly 4,800 police officers plus support staff and has a 2021 operating budget of $1.076 billion. The nature of law enforcement and the justice system, along with the sheer magnitude of this operation identifies it as an enticing target for cybercriminals intent on gaining access to confidential data in computer systems for unlawful or malicious purposes.

The International Association of Chiefs of Police in one of their recent publications of *The Police Chief Magazine* noted that:

> "*Reports of extensive data breaches or other elaborate cybercrimes are increasing worldwide. …Even more troubling, police departments are increasingly the targets of cyberattacks, either for criminal purposes or as acts of 'hacktivism'."*[1]

And that:

> *"Malicious actors use cyberattacks on law enforcement and local government in attempts to exploit sensitive information or even induce a cascading impact to critical infrastructure in a region. Emergency services are highly dependent on communications, information technology (IT), and the capability to transport*

[1] *The Emerging Cyberthreat: Cybersecurity for Law Enforcement*
https://www.policechiefmagazine.org/the-emerging-cyberthreat-cybersecurity/

essential personnel and equipment to locations where they are most needed. Computer-aided dispatching; emergency alert systems; event tracking; monitoring transportation infrastructure; and the sharing of intelligence, alerts, and operational plans are all highly dependent on the ability to transmit information via the Internet."

According to an April 2021 article in the New York Times[2], the Washington D.C. Metropolitan Police Department appeared to be the third US police force targeted in a ransomware attack in six weeks, and the 26th US government agency hit during 2021 up to the month of April. Cyber criminals claimed to have downloaded over 250 gigabytes of data. The breached files reportedly included details of disciplinary proceedings of hundreds of officers dating back to 2004.[3]

In June 2020, 38 police agencies across Canada were exposed by cybercriminals who also appeared to be targeting American police agencies[4]. The RCMP acknowledged being a target, however the other Canadian police agencies were not publicly identified. Media reports from the United States identified the compromised information from US police agencies affected by this breach as including:

"Nearly 24 years of documents, with names, email addresses, phone numbers, bank accounts involved in investigations, pictures and other data."

In September 2019, the Los Angeles Police Department confirmed that its systems had been breached and the personal information of at least 20,000 people had been exposed. The data breach included names, dates of birth, email addresses and passwords, as well as portions of social security numbers.

In a December 12, 2019 letter to the Auditor General, the Toronto Police Services Board requested that the Auditor General conduct a cybersecurity audit. Given the size and importance of TPS and the sensitivity of the information it retains, the Auditor General prioritized the allocation of resources on the request and agreed to perform a vulnerability assessment and penetration testing of the TPS IT network, systems and applications.

We have completed Phase 1 of this review. The purpose of Phase 1 was to assess TPS's ability, as a critical City agency, to manage external and internal cybersecurity threats. A Phase 2 review will be conducted in the future to review systems that were excluded from this current review.

This public report contains three recommendations. The confidential findings and recommendations to improve TPS cybersecurity controls are presented separately to this report in Confidential Attachment 1. In addition, a detailed technical report has also been provided to management for expediting actions.

---

[2] https://www.nytimes.com/2021/04/27/us/dc-police-hack.html
[3] https://apnews.com/article/police-technology-government-and-politics-1aedfcf42a8dc2b004ef610d0b57edb9
[4] https://www.cbc.ca/news/canada/ottawa/blueleaks-published-thousands-of-documents-from-canadian-police-agencies-1.5734311

The management has agreed with the recommendations contained in the confidential attachment to this report and will be providing a detailed management response to the Board in the future board meetings.

RECOMMENDATIONS

The Auditor General recommends that:

1. The Board adopt the confidential recommendations contained in Confidential Attachment 1 to this report from the Auditor General.

2. The Board direct that all information contained in the Confidential Attachment 1 to the report to remain confidential.

3. The Board forward this report to City Council through the City's Audit Committee for information.

FINANCIAL IMPACT

Implementing the recommendations in this report will strengthen information technology security controls at TPS. 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

Considering the importance of cybersecurity with respect to the confidentiality of the TPS data and IT network and systems, the Board requested the Auditor General in December 2019 to conduct a cybersecurity audit at TPS.

The Auditor General prioritized this review in 2020. The project was delayed due to the COVID-19 Pandemic, however continued to be prioritized and was included in her 2021 Audit Work Plan. The Auditor General's 2021 Audit Work Plan is available at:

https://www.toronto.ca/legdocs/mmis/2020/au/bgrd/backgroundfile-158178.pdf

This review is part of the Auditor General's overall plan to expedite the reviews of IT security systems throughout the City and its major Agencies and Corporations.

COMMENTS

With cyber threats evolving, there is an urgent need for all City of Toronto organizations, including TPS, to ensure cybersecurity programs can adapt to new threats. Billions of pieces of data are housed in various systems and computers at TPS. A single breach could have a devastating impact on its operations. A system is only as strong as its weakest link.

Increasing cyberattacks, in particular "Ransomware" are a risk for many countries. In a Five Country Ministerial Statement, Canada, the United States, New Zealand, Australia and the United Kingdom collectively stated that:

> *"Ransomware is a growing cyber threat which compromises the safety of our citizens, the security of the online environment, and the prosperity of our economies. It can be used with criminal intent, but is also a threat to national security. It can pose a significant threat to Governments, critical infrastructure and essential services on which all our citizens depend."* [5]

The United States Department of Homeland Security has issued the following advisory:

> "*Ransomware has rapidly emerged as the most visible cybersecurity risk playing out across our nation's networks, locking up private sector organizations and government agencies alike. And that's only what we're seeing – many more infections are going unreported."*[6]

Industry experts on information technology highlight features of the current threat environment:

> "*Current attacks are very sophisticated. They're evolving on an almost daily basis."* [7]

The Canadian Centre for Cyber Security stresses that:

> *"Inadequate information technology security practices provide cyber threat actors with an easy way to bring down your organization's network and give them access to sensitive information."* [8]

Cyberattacks on municipalities and police services

In recent years, many municipalities and law enforcement/police organizations in Canada and the U.S. have been affected by cyberattacks.

[5] Five Country (Australia, New Zealand, Canada, United States, United Kingdom) Ministerial Statement Regarding the Threat of Ransomware April 7, 2021
6 Department of Homeland Security – CISA Insights – Ransomware Outbreak, August 21, 2019
7 Standing Committee on Public Safety and National Security-SECU-155 April 3, 2019
8 Canadian Centre for Cyber Security, Common Employee IT Security Challenges (ITSAP.00.005)

A New York Times article[9] outlined how more than 40 municipalities in the U.S. – including large cities like Baltimore and Atlanta – have been hit by ransomware attacks. Some of these municipalities chose to pay the ransom to unlock data that had been encrypted or to restore access to systems; others did not. It can cost municipalities millions of dollars to recover from these attacks, in addition to the costs of data clean up and systems recovery.

With the level of services, extent of personal and highly sensitive data, and the critical infrastructure the organization supports, the Toronto Police Service must do all it can to protect its systems against cyberattacks and to adapt to emerging threats. Opportunities to do this at TPS are outlined in Confidential Attachment 1.

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 we have performed sufficient work in satisfaction that the evidence obtained provides a reasonable basis for our findings and conclusions.

We express our appreciation for the co-operation and assistance we received from TPS management and staff.

CONTACT

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

Suzanna Chan, Audit Manager, Auditor General's Office
Tel: 416-392-8030, Fax: 416-392-3754, email: suzanna.chan@toronto.ca

SIGNATURE

Beverly Romeo-Beehler

Beverly Romeo-Beehler
Auditor General

ATTACHMENTS

Confidential Attachment 1 - Toronto Police Service IT Infrastructure: Cyber Security Assessment Phase 1

Confidential Attachment 2: CYBERSECURITY REVIEW AT A GLANCE - Toronto Police Service IT Infrastructure: Cyber Security Assessment Phase 1

9 *Ransomware Attacks Are Testing Resolve of Cities Across America*, August 22, 2019, The New York Times