TORONTO

REPORT FOR ACTION WITH CONFIDENTIAL ATTACHMENT

Implementation of Cybersecurity High-Risk Recommendations Needs to be Expedited and Completed

Date: July 6, 2021
To: Audit Committee
From: Auditor General
Wards: All

REASON FOR CONFIDENTIAL INFORMATION

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

SUMMARY

The purpose of this report is to:

- Communicate to Audit Committee and City Council that the Auditor General has commenced a review of a Toronto Fire Services' critical system; and

- Recommend that the Chief Technology Officer continue expediting the Auditor General's prior cybersecurity-related audit recommendations, so the City is ready to prevent, detect and respond to cyberattacks.

Since 2016, the Auditor General has proactively raised concerns about evolving cyber threats to the City and its agencies and corporations. Cyberattacks are widely considered to be one of the most critical operational risks facing organizations. In previous reports, the Auditor General highlighted to City management the importance of being prepared for cyberattacks so that risks can be mitigated. The reports issued by the Auditor General since 2016 are listed in Appendix 1.

Cybersecurity threats are constantly evolving and becoming more sophisticated. With increasing numbers of cyberattacks, in particular ransomware, all types of private and public organizations and most importantly their systems and infrastructure providing critical services are at risk.

In April 2021, five countries (including Canada, the United States, New Zealand, Australia, and the United Kingdom) issued a Five Country Ministerial Statement saying:

"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." [1]

The United States Department of Homeland Security issued the following advisory in August 2019:

"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." [2]

In April 2019, industry experts on information technology (IT) highlighted features of the current threat environment:

"Current attacks are very sophisticated. They're evolving on an almost daily basis." [3]

Further, the Canadian Centre for Cyber Security notes that:

"Canada often ranks among the top countries impacted by ransomware…" and *"Over the past two years, ransomware campaigns have impacted hundreds of Canadian businesses and critical infrastructure providers, including multiple hospitals and police departments, as well as municipal, provincial, and territorial governments."*[4]

The Canadian Centre for Cyber Security also 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." [5]

With cyber threats evolving, there is an urgent need for all City of Toronto organizations to ensure that their cybersecurity programs adapt. Billions of pieces of data are housed

[1] Five Country (Australia, New Zealand, Canada, United States, United Kingdom) Ministerial Statement Regarding the Threat of Ransomware April 7, 2021

[2] Department of Homeland Security – CISA Insights – Ransomware Outbreak, August 21, 2019

[3] Standing Committee on Public Safety and National Security-SECU-155 April 3, 2019

[4] https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-modern-ransomware-and-its-evolution

[5] Canadian Centre for Cyber Security, Common Employee IT Security Challenges (ITSAP.00.005)

in various systems and computers. A single breach could have a devastating impact on its operations. A system is only as strong as its weakest link.

Cyberattacks on municipalities and police services

A New York Times article[6] 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 in order 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. Many law enforcement agencies in Canada and the U.S. have been affected by cybersecurity attacks in recent years, as well.

With the level of services, the extent of personal and highly sensitive data, and the critical infrastructure the City supports, the City must do all it can to protect its systems against cyberattacks and to adapt to emerging threats.

Cybersecurity risks continue to be a real and growing threat

Recent cyberattacks targeting public institutions and infrastructure indicate that threat actors are active and organizations like the City must be prepared to respond. The following are a few recent examples:

1. U.S. Pipeline Attack

In May 2021, a Russian hacker group was behind a major cyberattack against a major U.S. oil and gas pipeline which caused substantial disruptions throughout the Eastern United States. The group created a ransomware program to attack the Colonial Pipeline network, forcing the company to shut down all operations for nearly a week.[7]

"The shutdown caused major disruptions to gas delivery up and down the East Coast, as trucks struggled to restock gas stations, and long lines developed at pumps, especially in the Southeast. Airline operations were also disrupted." [8]

2. Florida Water Supply Cyberattack

In February 2021, cyber attackers gained access to a Florida city's water facility control system through a remote access software that was connected to the internet. The attackers attempted to raise the amount of sodium hydroxide in the water supply to dangerous levels.[9] Although the attack was detected and water quality was not affected, this shows how important it is to properly secure critical infrastructure.

[6] Ransomware Attacks Are Testing Resolve of Cities Across America, August 22, 2019, The New York Times

[7] https://www.thestar.com/opinion/contributors/2021/05/19/us-pipeline-hack-and-concerns-about-canadian-cyber-security.html

[8] https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html

[9] https://www.cnn.com/2021/02/11/us/florida-water-plant-hack/index.html

3. Cyberattacks on Law Enforcement Agencies

In June 2020, confidential law enforcement data belonging to 38 Canadian police agencies was exposed by cybercriminals who were targeting American police agencies[10]. The RCMP acknowledged being affected by the leak, however the other Canadian police agencies were not publicly identified. Media reports from the United States identified the compromised information from U.S. police agencies affected by this breach contained potentially sensitive files:

"It includes nearly 24 years of documents, with names, email addresses, phone numbers, bank accounts involved in investigations, pictures and other data." [11]

4. WannaCry Ransomware

In May 2017, the WannaCry ransomware campaign targeted computers around the world that were running Microsoft Windows. The campaign attacked the operating system by encrypting data and demanding ransom payments to restore the data. At the time, the Canadian Centre for Cyber Security[12] warned about the WannaCry ransomware campaign. This specific risk was also brought to the attention of the prior City Manager by the Auditor General. The Auditor General has since issued several cybersecurity reports outlining what needs to be done to help prevent, detect and recover from ransomware attacks.

WannaCry is just one type of ransomware. Since 2017, ransomware attacks have become more destructive and impactful to organizations.

5. COVID 19 Cyberattacks

While we understand the demands on staff and the financial burdens caused by COVID-19, it is important for all City organizations to continue working on strengthening cybersecurity and remain vigilant. They must also be supported in doing so. The International Criminal Police Organization's (INTERPOL) assessment of the impact of COVID-19 on cybercrime shows that major corporations, governments and critical infrastructure are at risk more than ever.[13]

"With organizations and businesses rapidly deploying remote systems and networks to support staff working from home, criminals are also taking advantage of increased security vulnerabilities to steal data, generate profits and cause disruption."

[10] https://www.cbc.ca/news/canada/ottawa/blueleaks-published-thousands-of-documents-from-canadian-police-agencies-1.5734311

[11] Cyber Security Today – Huge hack of police data, Instagram takeover of a popular surfer's account and more | IT World Canada News

[12] https://cyber.gc.ca/en/alerts/ransomware-wannacry

[13] https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

“The increased online dependency for people around the world, is also creating new opportunities, with many businesses and individuals not ensuring their cyber defences are up to date.”

Jürgen Stock, INTERPOL’s Secretary General also said:

“Cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by COVID-19.”

Critical Infrastructure Systems Reviews

The Auditor General, recognizing the increased risks of cyberattacks, has been proactive in performing cybersecurity audits at the City. In 2020, the Auditor General completed her assessment of Toronto Water's SCADA system and network. The report is available at:

https://www.toronto.ca/legdocs/mmis/2020/au/bgrd/backgroundfile-145342.pdf

The Auditor General is currently completing vulnerability assessments and penetration testing on critical systems and their related IT network, at Toronto Fire Services and Toronto Transit Commission.

RECOMMENDATIONS

The Auditor General recommends that:

1. City Council request the Chief Technology Officer to expedite the implementation of high-priority cybersecurity recommendations.

2. 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.

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. Her 2021 Work Plan includes cybersecurity audits of the City's critical infrastructure as well as its agencies and corporations. The Auditor General's 2021 Audit Plan is available at:

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

COMMENTS

The Auditor General is using this report to communicate to the Audit Committee and to City Council that there is a need to expedite the implementation of high-priority cybersecurity recommendations.

Cyberattack Risks

The outcomes of a cyberattack can be devastating to the City and can include:

- Inability to fulfil role of service delivery, which can include critical services like water, fire, and emergency services
- Disclosure of confidential or sensitive personal information
- Intellectual property theft
- Financial losses
- Risk of legal damages from lawsuits
- Reputational damage.

City Council continues to invest in improving cybersecurity, which includes procuring and upgrading tools, resources, licences, and services which support IT security functions. Management has taken some key actions to implement cybersecurity audit recommendations, including:

- Strengthening cybersecurity controls at Toronto Water's SCADA network. Management advised that actions have been taken or are in progress including, the implementation of multi-factor authentication (MFA) at critical entry points, improved physical security and monitoring, and improved IT access controls and monitoring.
- Creation of the Chief Information Security Officer's position. This position works with Technology Services Division to oversee and develop security policies and, also assists divisions in implementing cybersecurity audit recommendations.
- Implementing advanced threat detection and protection solutions on selected systems and networks.

For the rest of the City, some progress has been made, but there are many remaining outstanding cybersecurity recommendations. Given the importance of the recommendations, the City must do everything it can to protect against cyberattacks. A recent cybersecurity incident at a City division prompted the Auditor General to undertake a cybersecurity review of a critical system at Toronto Fire Services. Our results will be reported at the November 2021 Audit Committee.

Cybersecurity Report Recommendations

The Auditor General issued 10 reports related to cybersecurity and IT infrastructure from January 2016 to February 2021. These audits included 31 confidential and 15 public recommendations. Two additional reports[14]; one on the vulnerability assessment and penetration testing of Toronto Police Services IT infrastructure; and the other on the review of a specific complaint about inadequate tracking of software utilization; are being tabled at the July 7, 2021 Audit Committee. These new reports contain 13 confidential and three public recommendations.

The Auditor General reviews the implementation status of recommendations made through her audit and investigation reports. The current status of open recommendations for Auditor General reports on cybersecurity can be found on Table 3 in the follow-up report, which is being tabled at the July 7, 2021 Audit Committee. The report is available at:

http://app.toronto.ca/tmmis/viewAgendaItemHistory.do?item=2021.AU9.6

At its February 16, 2021 meeting, the Audit Committee recommended that:

"City Council request the Chief Information Security Officer to report to the May 31, 2021 meeting of the Audit Committee on the implementation status of all outstanding cybersecurity-related audit recommendations….".

The report is available at:

http://app.toronto.ca/tmmis/viewAgendaItemHistory.do?item=2021.AU9.7

The implementation of outstanding high-priority recommendations needs to be completed as soon as possible. We will continue to report the progress during our follow-up reviews on the implementation status of audit recommendations. The results of the review are reported to City Council through the Audit Committee.

This Report for Action communicates to the Audit Committee and City Council that the Auditor General has commenced a review of a Toronto Fire Services' critical system, and recommends that the Chief Technology Officer continue expediting the Auditor General's past cybersecurity related audit recommendations, so the City is better

[14] https://www.toronto.ca/legdocs/mmis/2021/au/bgrd/backgroundfile-168702.pdf
https://www.toronto.ca/legdocs/mmis/2021/au/bgrd/backgroundfile-168699.pdf

protected and ready to prevent, detect and respond to cyber threats. The information provided here does not constitute a performance audit conducted under Generally Accepted Government Auditing Standards (GAGAS).

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 - Implementation of Cybersecurity High-Risk Recommendations Needs to be Expedited and Completed

Appendix 1: Audit General Reports on Cybersecurity

Appendix 1: Auditor General Reports on Cybersecurity

1. 2021: Cybersecurity Incidents

Cybersecurity Incidents at the City and its Agencies and Corporations: Integrated Incident Response Plan is Needed, February 4, 2021
https://www.toronto.ca/legdocs/mmis/2021/au/bgrd/backgroundfile-163404.pdf

2. 2021: Information Technology Projects Implementation

Information Technology Projects Implementation: Information Privacy and Cybersecurity Review of Human Resource System, February 3, 2021
http://app.toronto.ca/tmmis/viewAgendaItemHistory.do?item=2021.AU8.8

3. 2020: Cyber Safety

Cyber Safety - Critical Infrastructure Systems: Toronto Water SCADA System, June 23, 2020
https://www.toronto.ca/legdocs/mmis/2020/cc/bgrd/backgroundfile-148217.pdf

4. 2019: Cyber Safety

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

5. 2019: Ransomware Attacks

Establishment of City Wide Cyber Security Breach Incident Management Procedures Required, June 2019
https://www.toronto.ca/legdocs/mmis/2019/au/bgrd/backgroundfile-135368.pdf

6. 2016-2018: IT Vulnerability Assessments, Penetration Testing and IT Infrastructure Reviews

(i) Audit of Information Technology Vulnerability and Penetration Testing – Phase 1: External Penetration Testing, February 2016
https://www.toronto.ca/legdocs/mmis/2016/au/bgrd/backgroundfile-90751.pdf

(ii) Audit of Information Technology Vulnerability and Penetration Testing – Phase II: Internal Penetration Testing, Part 1 – Accessibility of Network and Servers, October 2016
https://www.toronto.ca/legdocs/mmis/2016/au/bgrd/backgroundfile-97617.pdf

(iii) Information Technology Vulnerability Assessment and Penetration Testing - Wrap-up of Phase I and Phase II, March 2017
https://www.toronto.ca/legdocs/mmis/2017/au/bgrd/backgroundfile-101892.pdf

(iv) IT Infrastructure and IT Asset Management Review: Phase 1: Establishing an Information Technology Roadmap to Guide the Way Forward for Infrastructure and Asset Management, January 2018
https://www.toronto.ca/legdocs/mmis/2018/au/bgrd/backgroundfile-112385.pdf

(v) Information Technology Infrastructure and Asset Management Review: Phase 2: Establishing Processes for Improved Due Diligence, Monitoring and Reporting for Effective IT Projects and Asset Management, June 2018
https://www.toronto.ca/legdocs/mmis/2018/au/bgrd/backgroundfile-118363.pdf