TORONTO

REPORT FOR ACTION WITH CONFIDENTIAL ATTACHMENT

Cybersecurity Audit of Toronto Community Housing and Toronto Seniors Housing Corporations – Phase Two: User Access Management and Event Logging

Date: September 13, 2024
To: Toronto Community Housing Corporation Board of Directors
From: Auditor General
Wards: All

REASON FOR CONFIDENTIAL INFORMATION

Confidential Attachment 1 and Confidential Attachment 2 to this report involves the security of the property of the City of Toronto or one of its agencies and corporations.

SUMMARY

The Auditor General's 2024 Work Plan included a cybersecurity audit of the Toronto Community Housing Corporation (TCHC). TCHC also provides information technology services to Toronto Seniors Housing Corporation (TSHC) which is integrated with TCHC's enterprise information technology infrastructure and environment. As such, we also included TSHC's systems in our audit scope.

Phase One of this cybersecurity audit, focused on an assessment of the overall network security and select critical systems, was presented at TSHC's July 18, 2024, Board meeting and TCHC's July 30, 2024, Board meeting. The Phase One public report is available at:

Cybersecurity Audit of Toronto Community Housing and Toronto Seniors Housing Corporations – Phase One: Overall Network Security and Cybersecurity Assessment of Select Critical Systems (torontohousing.ca)

This Phase Two audit focused on the assessment of user access management and network and system event logging across the technology environment. The confidential findings and recommendations are contained in Confidential Attachment 1 to this report.

Confidential attachment 1 includes our Phase Two audit findings covering both TCHC and TSHC, with recommendations to TCHC as they also provide technology services to TSHC. We have provided the confidential technical report to TCHC's management with

details of specific technical information to guide them in implementing our recommendations.

The Auditor General will be making a confidential presentation at the TCHC's September 23, 2024, Building Investment, Finance and Audit Committee meeting and at the TCHC's October 18, 2024, Board of Directors meeting.

A separate cover report will be provided to the TSHC's Board of Directors for their information. The Auditor General will also be making a confidential presentation at the TSHC's October 17, 2024, Board of Directors meeting.

RECOMMENDATIONS

The Auditor General recommends that:

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

2. The Board forward this report including the Confidential Attachment 1 to City Council for information through the City's Audit Committee.

3. The Board recommend City Council authorize the public release of Confidential Attachment 1 to the report from the Auditor General at the discretion of the Auditor General, after discussions with the appropriate Toronto Community Housing Corporation, Toronto Seniors Housing Corporation, and City Officials.

FINANCIAL IMPACT

Implementing the audit recommendations will strengthen cybersecurity controls at TCHC and TSHC. 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's 2024 Work Plan included TCHC's cybersecurity audit and is available at:

Auditor General’s Office 2024 Work Plan and Budget Highlights (toronto.ca)

COMMENTS

Cybersecurity is a critical risk for all organizations. Within the past few years, there has been an increase of cyberattacks on the City's agencies, such as the Toronto Zoo,

Toronto Public Library, and Toronto Transit Commission. The Auditor General has been conducting cybersecurity audits of the City and its agencies and corporations since 2015 and included a cybersecurity audit of TCHC in her 2024 Work Plan.

This Phase Two cybersecurity audit of TCHC and TSHC focused on the assessment of user access management and network and system event logging across the technology environment.

User Access Management

User access controls are important in the overall management of cybersecurity. The Active Directory provides centralized authentication and authorization for network resources, manages users and network permissions, such as creating and deleting user accounts and providing access permissions to network resources.

An example that demonstrates the importance of user access management is the well-known and sophisticated “SolarWinds” attack. Active Directory played a part in this large-scale cyberattack. The attack was initiated through a malware inserted into a software update which affected multiple U.S. government agencies, critical infrastructure entities, and private sector organizations in 2020.[1] Research from industry experts found that attackers used the Active Directory to move laterally within the organization.

Event Logging

The Canadian Centre for Cyber Security in its December 2022 publication described the logging of computer activities and events as:

“Logging is the process of collecting data that represents specific activities, events, error conditions, or the general status of an information system or network. The goal is to capture security-relevant data for system administrators to gain insight on how systems are behaving, and to support investigations of potential or actual breaches."[2]

Proper event logging will help an organization identify indicators of compromise and take corrective actions in a timely manner to minimize the impact of a security incident. Logging records are also important to investigate a potential or actual breach once it has occurred and identify the cause of the breach.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

1 Eviction Guidance for Networks Affected by the SolarWinds and Active Directory/M365 Compromise | CISA

2 Network security logging and monitoring - ITSAP.80.085 - Canadian Centre for Cyber Security

The Auditor General will re-test cybersecurity controls at TCHC and TSHC after management has fully implemented the recommendations.

CONTACT

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

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

Cecilia Jiang, Senior Audit Manager, Auditor General's Office
Tel: (416) 392-8024, E-mail: Cecilia.Jiang@toronto.ca

SIGNATURE

Tara Anderson
Auditor General

ATTACHMENTS

Confidential Attachment 1: Cybersecurity Audit of Toronto Community Housing and Toronto Seniors Housing Corporations – Phase Two: User Access Management and Event Logging

Confidential Attachment 2: Confidential Presentation to Toronto Community Housing Corporation's Building Investment, Finance and Audit Committee and the Board of Directors