# 21.

**STAFF REPORT**
**INFORMATION ONLY**

## Cybersecurity Report

**Date:** February 26, 2024

**To:** Toronto Public Library Board

**From:** City Librarian

## SUMMARY

The purpose of this report is to provide the Toronto Public Library Board with a final report on the investigation into the Toronto Public Library's (TPL's) cybersecurity attack.

When TPL became aware of a cybersecurity incident on October 28, 2023, staff immediately initiated measures to mitigate potential impacts by shutting down the technical environment including all internal and external networks and systems. Third-party legal counsel with expertise in cybersecurity were engaged to collaborate with third-party cybersecurity technical experts to advise on containment, conduct forensics, and assess the impact. In addition, the cybersecurity experts supported staff's planning for and implementation of additional proactive measures to safeguard TPL's data and information systems. The privileged and confidential report from legal counsel, including its appended technical input from the third-party cybersecurity experts, outline the support the experts provided in response to the incident, their forensic analysis of the cyberattack, and the privileged and confidential input given to support TPL in rebuilding its technical environment for optimum security.

Cybersecurity has become a pressing issue for public and private organizations globally as cyber incidents have become more prevalent and pervasive. TPL has proactively prepared for cybersecurity issues by prioritizing cybersecurity since January 2021 with Board approval of TPL's Digital Strategy 2020-2024. This commitment to achieving a safe and secure IT environment, including a targeted level of protection from internal and external cybersecurity threats, has been advanced through:

- the IT Security, Risk & Governance Program;
- the establishment of an Information Security Policy requiring annual security reports to the Board;
- participation in the City CISO Cybersecurity Confirmation Program;
- TPL's Enterprise Risk Management Program;
- more rigorous updating of application software, hardware, and patching;
- IT staff dedicated to cybersecurity; and
- mandatory cybersecurity training for all staff.

The post-incident work to rebuild TPL's technical environment resulting from the cybersecurity attack has accelerated TPL's Digital Strategy and advanced security measures planned in TPL's digital strategy roadmap.

The full-scale shutdown of TPL's technical environment, and the ensuing work to secure the IT network and its many systems, resulted in the suspension of many core library services including the tpl.ca website and access to the library catalogue, holds, and Your Account services; public computing and printing; and access to some digital materials and databases. However, during these outages, many of TPL's online and in-branch services remained available and have been well-used by the public since the attack began. All 100 branches remained open with access to staff expertise, collections including staff-assisted borrowing and returns of materials, study space, programming, and Wi-Fi. Access to e-content and online programs continued to be available through TPL's landing page.

Service restoration, which has been a complex and detailed process involving enterprise-wide analysis and coordination, is nearing completion. Staff have worked tirelessly to restore all services as quickly as possible. The complexity of the task, given TPL's extensive network of 100 library branches, a multi-service Data Centre, and more than 5,000 staff and public computers, makes this task

much more difficult and means there must be a gradual and measured approach to protect and reinstate services.

## FINANCIAL IMPACT

The City of Toronto is covering the financial impact of TPL's cybersecurity incident. Any residual financial impact will be accommodated within the approved 2024 operating and capital budgets.

The Director, Finance & Treasurer has reviewed this financial impact statement and agrees with it.

## ALIGNMENT WITH STRATEGIC PLAN

To enable TPL's Strategic Plan 2020–2024, a safe and secure IT environment is essential for both staff and customers. Consequently, the Digital Strategy 2020–2024 includes a priority to "adopt a modern security approach to improve cybersecurity and TPL's overall security position".

## EQUITY IMPACT STATEMENT

Measures to advance the security of TPL's technical environment, such as the IT Security, Risk & Governance Program, and the additional measures implemented following the cybersecurity incident, will enable equitable access to technology in a secure manner that protects the privacy and confidentiality of customers and staff.

## DECISION HISTORY

At its January 25, 2021 meeting, the Board approved the Digital Strategy 2020-2024. As identified in the Digital Strategy Action Plan 2021, there is a focus on IT Security Advancement.

At its December 6, 2021 meeting, the Board approved the Information Security Policy and TPL's participation in the City of Toronto Confirmation program.

At its September 19, 2022 meeting, the Board received an update to the Risk Register.

At its March 27, 2023 meeting, the Board received the IT Security – Annual report and update on the City of Toronto's Cybersecurity Confirmation Program.

At its October 30, 2023 meeting, the Board received a privileged and confidential in camera verbal update on TPL's October 28th, 2023, cybersecurity attack.

At its November 13, 2023 Special Board meeting, the Board considered a privileged and confidential in camera report, and approved plans for moving forward in response to the cybersecurity attack.

At its December 4, 2023 meeting, the Board received a privileged and confidential in-camera verbal update on the work underway to rebuild and secure TPL's technical environment services because of the cybersecurity attack.

At its December 4, 2023 meeting, the Board received an update on the Risk Register.

At its January 29, 2024 meeting, the Board received a privileged and confidential in camera verbal update on the timelines for restoring services because of the cybersecurity attack.

## ISSUE BACKGROUND

Cybersecurity has become a pressing issue for public and private organizations globally as cyber incidents have become more prevalent and pervasive. In recent months, several public sector organizations in Ontario and elsewhere have experienced cybersecurity incidents, including libraries, museums, school boards, hospitals, and healthcare centres.

TPL has proactively prepared for cybersecurity issues by prioritizing cybersecurity since January 2021 with Board approval of TPL's Digital Strategy 2020-2024. This commitment to achieving a safe and secure IT environment, including a targeted level of protection from internal and external cybersecurity threats, has been advanced through:

- the IT Security, Risk & Governance Program;
- the establishment of an Information Security Policy requiring annual security reports to the Board;
- participation in the City CISO Cybersecurity Confirmation Program;
- TPL's Enterprise Risk Management Program;
- more rigorous updating of application software, hardware, and patching;
- IT staff dedicated to cybersecurity; and
- mandatory cybersecurity training for all staff.

When TPL became aware of a cybersecurity incident on October 28, 2023, staff immediately initiated measures to mitigate potential impacts by shutting down the technical environment including all internal and external networks and systems. Third-party legal counsel with expertise in cybersecurity were engaged and asked to retain and collaborate with third-party cybersecurity technical experts to advise on containment, conduct forensics, and assess the impact. In addition, the cybersecurity experts supported staff's planning for and implementation of additional proactive measures to safeguard TPL's data and information systems. The privileged and confidential report from legal counsel, including its appended technical input from the third-party cybersecurity experts, outline the support the experts provided in response to the incident, their forensic analysis of the cyberattack, and the privileged and confidential input given to support TPL in rebuilding its technical environment for optimum security (attachment 1).

The City of Toronto's Chief Information Security Office (CISO), and City Legal, were informed, and a report was filed with Toronto Police Service. Additional stakeholders including TPL Workers Union CUPE Local 4948 were informed. Public statements have been posted and updated regularly on TPL's website landing page. Within hours of the cybersecurity incident being identified, TPL's Incident Management System was launched and the emergency management unit, the Library Operations Centre (LOC), was up and running to coordinate business continuity plans including communication channels, issues to be

resolved, staff supports, service and operational workarounds, and service restoration. TPL's Privacy Breach Protocol was also initiated.

## COMMENTS

Prior to the cybersecurity incident, TPL was at a Developing Level of Maturity with its IT security program, which is typical of most public sector organizations. Since the attack in October, TPL has matured its information security program by implementing additional security controls, updated some hardware and software applications, and introduced new processes. In fact, the post-incident work to rebuild TPL's technical environment has accelerated TPL's Digital Strategy and advanced security measures planned in TPL's digital strategy roadmap. In other words, as part of the rebuilding and restoration work, TPL has not simply replicated the former environment but rather used this attack as an opportunity to accelerate plans. Subsequently, TPL's IT security program maturity level has increased when assessed within the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).

Throughout this incident, TPL staff has had tremendous support and worked closely with legal counsel, third-party cybersecurity experts, and City CISO staff. Legal counsel has provided strategic advice on managing the incident, advising on communications responsive to the incident and stakeholders involved, and on actions to be taken associated with all elements of the cybersecurity incident including the privacy breach. The threat actor's demand for a ransom was denied.

**Governance**
An Incident Management System governance structure was executed immediately to manage the emergency response and the complexities of the incident, expedite decision-making and ensure an enterprise-wide business and service approach was established. The structure was comprised of the following components:

The *Cyber Response Leadership Team (CRLT)* included the Senior Leadership Team, privacy and communications managers. The team acted as the senior decision-making body, engaged with legal counsel, developed organizational priorities, and orchestrated communications including regular reports for Library Board information and/or approval.

Reporting daily to CRLT is the LOC. Leading the business continuity plan, this team coordinated emergency operations and workarounds, coordinated, and distributed internal communications, liaised between business operations, service owners and technical recovery staff. LOC led the service recovery plan as approved by CRLT.

The *Management Response Team* is comprised of Library Management and key stakeholders to support LOC's work. The team received and distributed internal communications to staff, directed engagement with staff and brought forward questions and issues from frontline operations to ensure business and service continuity plans were maintained as much as possible.

**Forensic Report**

Third-party experts conducted a forensic analysis to determine how the cyberattack happened, and have advised and supported actions to ensure containment, the cleansing and restoration of the technical environment, enhanced security, and remediation efforts. This work has included the installation of additional security controls, enhanced processes, and protocols.

The forensic analysis has led TPL to conclude that the attackers breached a vulnerability in an internet-facing server, exfiltrating and encrypting data from a file server. TPL's quick action to isolate the environment immediately on discovering the attack led to containment on October 29, 2023, reducing further potential exposure. TPL has addressed these occurrences by rebuilding its network and implementing the enhancements summarized in "Lessons Learned" below. The enhancements will improve TPL's management of vulnerabilities and give TPL a significantly improved ability to detect and respond to security events and incidents.

The incident has also led to further collaboration, advice, and support from the City's CISO staff throughout this incident with plans to strengthen this relationship on a go-forward basis, engaging on cyber threat management and monitoring, cyber resilience, engagement, and vulnerability management.

**Privacy Breach**

Based on evidence gathered through the cybersecurity investigation, a privacy breach was announced on November 15, 2023, indicating that personal data

was stolen. TPL advised that it believed current and former staff employed by TPL and the Toronto Public Library Foundation (TPLF) from 1998 were impacted. Information related to these individuals was likely taken, including:

- name, social insurance number, date of birth and home address;
- copies of government-issued identification documents provided to TPL by staff.

Given the nature of the information exposed and to give peace of mind, TPL offered two years of complimentary credit monitoring to current and past TPL and TPLF employees.

Although cardholder, volunteer, and donor databases were not affected, some data about these groups likely resided on the compromised file server. TPL is currently engaged in an e-discovery process with third-party assistance to determine who is affected and how. A preliminary e-discovery process determined some data on dependents and family members of staff has been impacted, and as a result TPL offered two-years of complimentary credit monitoring protection to impacted current and former staff. The larger e-discovery process to investigate whether customer, donor or volunteer data has been taken from the affected file server is underway and will take more time to complete. TPL will continue to be transparent and notify those affected as appropriate in light of any findings.

A final report will be sent to Ontario's Information and Privacy Commissioner.

**Service Continuity and Restoration**

The full-scale shutdown of TPL's technical environment, and the ensuing work to secure the IT network and its many systems resulted in the suspension of many core library services including the tpl.ca website and access to the library catalogue, holds, and Your Account services; public computing and printing; and access to some digital materials and databases. However, during these outages, many of TPL's online and in-branch services remained available and have been well-used by the public since the attack began. These include:

- All 100 branches remained open with access to staff expertise; collections including staff-assisted borrowing and returns of materials; study space, programming, Wi-Fi and drop-in programs such youth hubs. Branches continued to be important public spaces for vulnerable populations,

especially during the colder weather, with access to warm spaces, washrooms and staff supports.
- Library materials continued to be borrowed and returned with almost 1 million checkouts of physical materials borrowed since the attack.
- New library memberships were processed, and expired library cards were extended. More than 20,000 new library card memberships have been processed since the attack.
- Most of TPL's digital collection remained available, including ebooks and audiobooks; the music library of classical, jazz and world music; newspapers and magazines through Press Reader; and streaming services such as Kanopy and Hoopla. Borrowing of ebooks and e-audiobooks surpassed 11 million in 2023, a result of increased usage of the digital collection during the outage.

Service restoration has been a complex and detailed process involving enterprise-wide discussions and analysis. Staff have worked tirelessly to restore all services as quickly as possible. The complexity of the task, given TPL's extensive network of 100 library branches, a multi-service data centre, and more than 5,000 staff and public computers, makes this task much more difficult and means there must be a gradual and measured approach to protect and reinstate services. Nevertheless, substantial service restoration is nearing completion:

- Staff computing, access to most shared drives and TPL's library management and accounting software have been fully restored;
- TPL's website was partially restored January 29th. Remaining website functionality will be restored by the end of February;
- Public computing was restored February 5th with 9,298 customers using the service in the first 4 days; public printing will be available by mid-March;
- The process for checking-in over 1 million returned items is well underway with customers starting to receive holds pick-up notification the week of February 12th;
- Most services in Digital Innovation Hubs have been restored.

**Lessons Learned**

The cybersecurity attack has provided many opportunities to learn and improve, as well as reflect on aspects of TPL's response that have been invaluable to the recovery process.

Legal Advice and Counsel – It was critical to have legal counsel with cybersecurity expertise on board as quickly as possible to engage technical consultants and advise on:

- internal and external communications;
- legal obligations and best practises having to do with issues such as privacy breaches and identity theft; and
- legal privilege.

Cybersecurity Specialists – Having access to immediate technical support from cybersecurity specialists was essential. The specialists reported to legal counsel so TPL could receive critical advice regarding:

- containment;
- forensic assessment;
- re-building and service recovery of the technical environment;
- appropriate security assessment and consulting for go-forward plans.

Business Continuity Plans – TPL had established proactive plans for business continuity using the City's Incident Management System. This proved essential with the launch of LOC, TPL's emergency operations team, on day 1 of the incident. LOC acted as a business liaison team that collaborated with the technical teams, providing support for:

- internal corporate communications distribution;
- priority-setting for service recovery and restoration;
- coordination of service orchestration across business teams.

Technical Improvements – Through this incident, TPL has learned and developed from having received the advice of third-party technical experts. The recovery work has allowed the acceleration of TPL's security roadmap and other improvements with:

- a complete rebuild of the network within the Data Centre, extending to the branch (campus edge);
- the rebuilding and restoration of enterprise applications into network segments;
- implementation of advanced threat monitoring and threat hunting with the deployment of Extended Detection and Response, a more robust antimalware solution;

- an improved patch management regime with process improvements ensuring security updates are applied in a timely manner;
- enhanced log management and aggregation of logs into a Security Information and Event Management (SIEM) system;
- increased security controls across user and service accounts;
- a planned review of records retention and associated processes.

## CONCLUSION

The rise in data security and ransomware incidents affecting organizations dedicated to community well-being, including hospitals, school boards, and libraries like TPL, is a disturbing reality. Public sector organizations are increasingly becoming targets, whether motivated by financial gain or sheer malice. In the case of public libraries, dedicated to equity, access to information, intellectual freedom, and openness for all, this represents an attack on the very essence of civil society. This attack reminds everyone to stay vigilant in the face of a danger that is unfamiliar to many.

## CONTACT

Steve Till-Rogers; Director, Digital Strategy & CIO;
Tel: 416-393-7104; Email: stillrogers@tpl.ca

Shawn Mitchell: Director, Policy, Planning & Performance Management;
Tel: 416-395-5602; Email: smitchell@tpl.ca

## SIGNATURE

_____

Vickery Bowles
City Librarian

## ATTACHMENTS

Attachment 1: Privileged and Confidential: Report from Legal Counsel with technical attachment