REPORT FOR ACTION WITH CONFIDENTIAL ATTACHMENT

Cybersecurity Incident Report

Date: May 17, 2024
To: Board of Management of the Toronto Zoo
From: Director, Finance, Technology, and Innovation
Wards: All

REASON FOR CONFIDENTIAL INFORMATION

The attachment to this report involves receiving advice that is subject to solicitor-client privilege.

SUMMARY

This report will provide an update to the Board of Management on the cybersecurity incident that affected the Toronto Zoo in January 2024. This report appends a privileged and confidential report that summarizes the results of the investigation into the cause of the attack.

RECOMMENDATIONS

The Director of Finance, Technology, and Innovation recommends that:

1. The Board of Management of the Toronto Zoo receive this report for information.

2. The Board of Management of the Toronto Zoo direct that the privileged and confidential information contained in the Confidential Attachment 1 remain confidential in its entirety, as it is advice that is subject to solicitor-client privilege.

FINANCIAL IMPACT

The primary costs associated with responding to the cybersecurity incident at the Toronto Zoo, including the mobilization of third-party cybersecurity experts to support containment, recovery and investigation efforts, are covered as part of the support

provided by the City of Toronto to its agencies and boards. Additional net costs for replacement of hardware systems corrupted during the incident, and not already budgeted for in 2024, are estimated at approximately $140,000. Coverage for these costs will be sought through the City of Toronto and/or will be managed within the approved 2024 operating and capital budgets.

DECISION HISTORY

Following the cybersecurity incident at the Toronto Zoo detected on January 5, 2024, the Board of Management received privileged and confidential updates on the status of the incident and investigation at is meetings on February 9, 2024 and March 28, 2024.

COMMENTS

In January 2024 the Toronto Zoo was impacted by a cybersecurity incident, joining the growing number of public and private sector organizations worldwide who have been affected by cyber crimes.

Background

The Toronto Zoo's 2022 Master Plan sets out an ambitious vision for the Zoo as a conservation science focused destination providing exceptional guest experiences. Technology is an integral enabler of this vision, and a Technology Master Plan was developed and included as an appendix to the Master Plan. The Technology Master Plan identified key building blocks for the Zoo's IT strategy with a focus on fixing the basics, building flexible platforms and strengthening security. These areas have been a primary focus of the Zoo's Technology team in recent years with upgrades and enhanced security measures implemented across the Zoo's network.

With respect to cybersecurity the Toronto Zoo collaborates with the Office of the Chief Information and Security Officer (CISO) at the City of Toronto. The Zoo participates in CISO's Confirmation Program available to City boards and agencies, including the provision of mandatory annual cybersecurity training for staff and the conducting of test (e.g., phishing) exercises. The Zoo also coordinates with CISO on key actions required to ensure Zoo systems and networks are meeting industry standards with respect to cybersecurity.

Cybersecurity incident response at the Zoo is led by the Director of Finance, Technology and Innovation in collaboration with the Chief Executive Officer, Senior Director of Strategic Communications and Guest Experience and the Director of Human Resources (the Zoo’s privacy officer). The Director, Finance, Technology and Innovation further coordinates with the Director of Threat Management at CISO regarding response to a cyber incident, including mobilization of third-party resources (in accordance with the City’s insurance coverage).

The Zoo’s Manager of Technology leads the technical response related to containment and restoration of Zoo systems and networks. Zoo Technology staff follow the Cybersecurity Incident Response process with respect to assessing, notifying and escalating an incident as required.

Cybersecurity Incident

On January 5, 2024 the Toronto Zoo became aware that its network and devices were experiencing a ransomware attack. Zoo Technology staff took immediate action to contain the incident and to assess the scope of impact. This included contacting CISO, through which third party experts in cybersecurity incidents were mobilized.

The Zoo was able to confirm that primary systems related to site security, admissions and payroll remained unaffected during the incident allowing the Zoo to remain operational with minimal impacts to animals and guests. The main impact to the Zoo related to lost access to shared and personal network data and documents, in addition to corrupted devices.

Shortly following confirmation of the cybersecurity incident and initiation of containment measures, the Zoo reported the incident to the Toronto Police Service. It later notified the Information and Privacy Commissioner of Ontario (IPC).

Incident Investigation

As part of the Zoo's response to the cybersecurity incident, the Zoo's external cybersecurity counsel worked with technical cybersecurity experts to conduct a privileged investigation including into how the attack occurred. The attackers gained access to the Zoo's network on December 27, 2023 via a virtual private network session prior to initiating the ransomware attack on January 5, 2024. Further details on the results of the investigation are described in confidential and privileged Attachment 1.

Recovery and Restoration

In accordance with the Zoo's Cybersecurity Management Action Plan developed in collaboration with CISO, several cybersecurity enhancements to the Zoo's network were underway at the time of the incident. In response to the incident, the Zoo has expedited a number of system upgrades, many of which had been initiated and/or scheduled for deployment in 2024, in support of recovery and restoration efforts. The effect of these enhancements is to harden the Zoo's network further to the latest security standards to reduce vulnerabilities identified through the containment and investigation processes. This includes strengthened controls on network access, expanded monitoring and detection capabilities, and improved system redundancy. The Zoo also continues to work to recover/restore data and files that were encrypted during the incident. This includes retaining a third-party expert in the recovery of data following cyber attacks.

The Zoo's Technology team continues to work with CISO to ensure that the Toronto Zoo's network is being built and maintained in accordance with cybersecurity industry standards, to facilitate staff training and to conduct tests of security measures and procedures.

Data Breach

As part of the investigation, the Toronto Zoo worked with CISO and third-party experts to assess risks associated with the personal data of employees, volunteers and guests. The Zoo was able to confirm that current systems do not retain credit card or payment information of guests. However, employment records of current and former employees and a limited number of volunteers of the Zoo were identified as likely stolen during the incident.

On January 17th, the Zoo confirmed a data breach following a report made to the IPC. The announcement included a notification to all current and former employees and volunteers of the Toronto Zoo back to 1989 along with an offer of credit monitoring protection for a two-year period. Current and former employees and volunteers have until July 17, 2024 to enrol in the credit monitoring service.

The Zoo continues its efforts to recover data and files that were corrupted and/or stolen during the incident. An interim report has been filed with the Information and Privacy Commissioner of Ontario (IPC). Additional reports will be submitted to the IPC once a more fulsome review is completed of recovered records to determine any additional notification requirements to affected parties.

Lessons Learned

As the Toronto Zoo becomes more technologically advanced, its exposure to risks associated with increasingly digital workplaces has expanded. The upgrades that were made in key systems prior to the cybersecurity incident were instrumental in allowing the Zoo to remain operational with minimal impact to our animals or guests. Still, the incident has highlighted several key learnings for the Zoo:

1. Importance of City of Toronto support - The availability of legal counsel and third-party cyber experts through CISO was instrumental to the Zoo's ability to quickly respond to the incident. This included rapidly mobilizing a team of City and third-party experts to support and coordinate efforts related to containment, investigation and recovery. The availability of these resources saved critical time and costs. It also helped to ensure that notifications to the appropriate authorities, including the Toronto Police Service and Information and Privacy Commissioner of Ontario, could be completed in a timely and fulsome manner.

2. Communications - Regular, timely and transparent communications to Toronto Zoo staff, volunteers, members and the public was key to building and maintaining trust, ensuring awareness of exposure risk, and providing certainty in the ability of the Zoo to support the safety of its animals, employees, volunteers and guests. The Zoo was committed to notifying those who were potentially impacted by the cybersecurity incident and initiating protective actions (including the provision of credit monitoring services) at the earliest opportunity following confirmation of a data breach.

3. Expediting cybersecurity investments and training - At the time of the incident the Toronto Zoo was continuing to implement multiple planned system upgrades as part of

its cybersecurity work with CISO. Additional work was planned in future years based on budget availability. The Zoo has reprioritized its technology plans in key areas to advance additional security measures. The cybersecurity incident has also underscored the importance of staff training. The Zoo has taken a renewed commitment to prioritize mandatory annual cybersecurity training and ensure all staff are completing it in a timely manner.

The cybersecurity incident at the Toronto Zoo highlighted the present and ongoing risk that malicious cybersecurity incidents pose to the Zoo's operation. The Zoo is committed to continuing work with the City of Toronto to harden the network and critical systems further with the latest security measures to ensure the safety of our animals, staff and guests.

CONTACT

Jamie Austin
Director of Finance, Technology, and Innovation
jaustin@torontozoo.ca
(416) 392-5914

SIGNATURE

Jamie Austin
Director, Finance, Technology, and Innovation

ATTACHMENTS

Confidential Attachment 1 - Confidential Cyber Attack Forensic Investigation Report