Information and Privacy Commissioner,
Ontario, Canada

Commissaire à l'information et à la protection de la vie privée,
Ontario, Canada

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT MR21-00114

Toronto Transit Commission

April 5, 2024

Summary: The Toronto Transit Commission (TTC) was the victim of a cyberattack. A threat actor gained access to its systems via a phishing attack, used malware to encrypt these systems, and exfiltrated data. The TTC notified the IPC, its employees, and the public of this privacy breach. It was later able to restore nearly all of its systems from backups and hired experts to determine the information that had been exfiltrated, and how the attack occurred. They found that the TTC's failure to install a patch for a known security vulnerability contributed to the attack.

In this report, I conclude that the TTC did not have reasonable security measures in place to prevent unauthorized access to the personal information on its systems. However, the TTC put additional security measures in place following the attack. It also implemented detailed revised guidance on scanning for vulnerabilities and installing patches. These set out timelines and state who is responsible for these tasks. Based on the measures that the TTC has taken since the breach, I am generally satisfied with their response to the breach, though I recommend that they implement guidance on using encryption as a default.

Statutes Considered: *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M. 56; R.R.O. 1990, Reg. 823.

Orders and Investigation Reports Considered: Privacy Complaint Report PR16-40

BACKGROUND:

[1] In late 2021, the Toronto Transit Commission (the TTC) contacted the Information and Privacy Commissioner of Ontario (IPC) to report a breach of personal information

under the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act*). A threat actor had gained access to the TTC's information technology (IT) systems, and then used malware to encrypt the TTC's IT systems, as well as transferring data out of those systems, including personal information. The TTC discovered the breach as it was happening and activated its information technology security protocols to contain the threat.

[2] The TTC then sent out a press release notifying the public of the breach. The notice stated that "the incident did not cause significant service disruption" and that there was no risk to employee or customer safety. The notice also set out the services that were impacted, including next vehicle information, para-transit bookings, and employee email.

[3] Over the following days, the TTC was able to restore a great deal of its systems from backups. This restoration continued and by two months after the incident, the TTC stated that its IT division had restored 95% of its systems, and that all critical systems were operational.

[4] The TTC also provided a public update (the Update) on the cybersecurity incident within two weeks. In that Update, the TTC noted that based on its investigation to that point, the threat actor may have stolen the personal information of approximately 25,000 past and present employees. This information could include the employees' names, addresses, and social insurance numbers (SIN). The Update stated that the TTC was continuing to investigate whether "a small number of customers and vendors may also be impacted" and that they would notify those individuals when they had further information. The TTC stated that the investigation was ongoing but noted that "there is no evidence at this time that any of this personal information has been misused." Finally, the Update referred employees to a credit agency's identity theft program and stated that more information would be provided on the TTC's website shortly.

[5] The TTC also notified the 25,000 past and present employees about the incident directly by letter, which included an offer of credit monitoring for those affected.

[6] The TTC later informed the IPC that they had engaged a third party to analyse the records that may have been exfiltrated. They determined that the number of individuals who may have been affected was fewer than the 25,000 initially estimated, and that no customers or vendors were impacted. The TTC provided an updated list of the types of personal information affected by the incident, which included:

- Full name
- Phone number
- Email
- Age

- Employment history
- Marital status
- Medical conditions
- Driver's license

[7] In addition, the TTC noted that for a very small number of records (less than 1% of the total number of affected individuals), the data exfiltrated may have also included their criminal history, immigration information, financial information, and social insurance number.

[8] The TTC stated that a small TTC file sample and partial file tree may have been posted on the dark web for approximately twenty-four hours before being removed. The TTC also advised that it had not been able to verify that this information had actually been posted. The TTC has continued monitoring the dark web since that time and has not found evidence of subsequent publication or sale of TTC data.

ISSUES:

[9] As a preliminary matter, the TTC has stated, and I agree, that the information accessed by the threat actor is personal information pursuant to section 2(1) of the *Act*. Further, the access to and transfer of this personal information by the threat actor, who was not an agent of the TTC or acting on its behalf, was not a use or disclosure of personal information authorized under the *Act*.

[10] I identified the following issues in this investigation:

1. Did the TTC have reasonable measures in place to prevent unauthorized access to personal information within its systems in accordance with section 3(1) of Regulation 823 of the *Act*?

2. Did the TTC respond adequately to the breach?

DISCUSSION:

Issue 1: Did the TTC have reasonable measures in place to prevent unauthorized access to personal information within its systems in accordance with section 3(1) of Regulation 823 to the *Act*?

[11] Section 3(1) of Regulation 823 of the *Act* states:

> Every head shall ensure that reasonable measures to prevent unauthorized access to the records in his or her institution are defined, documented and put in place, taking into account the nature of the records to be protected.

[12] In Privacy Complaint Report PR16-40, Investigator Lucy Costa stated that section 3(1) of Regulation 823 did not mandate a "one size fits all" approach, noting:

> ...It does not set out a list of measures that every institution must put in place regardless of circumstance. Instead, it requires institutions to have "reasonable" measures and ties those measures to the "nature" of the records to be protected. It follows that the same security measures may not be required of all institutions. Depending on the nature of the records to be protected, including their sensitivity, level of risk and the types of threats posed to them, the required measures may differ among institutions.
>
> Furthermore, simply because a breach occurred does not by itself mean that reasonable measures were not in place. The standard set out in section 4(1) is not perfection but reasonableness. It is therefore possible for records to be accessed in an unauthorized manner and yet the measures in place still be reasonable.[1]

The Phishing Attack

[13] The TTC's forensics investigation found that the threat actor gained access to its system by first compromising a trusted third party's system. The threat actor then inserted themselves into email correspondence between this third party and the TTC. A TTC employee clicked on a malicious link that seemed to come from the third party, and this allowed the threat actor to access the TTC's systems via malware. The TTC provided the IPC with a more detailed explanation of how the attack occurred, but asked that those details not be published, due to security concerns.

[14] Information available online showed that a security patch to address a vulnerability that was exploited during the incident had been available for several months prior to that incident, and its availability had been widely publicized.

[15] In July 2019, the IPC published a Technology Fact Sheet addressing phishing attacks, such as the one described above, titled *Protect Against Phishing* (the Fact Sheet).[2] The Fact Sheet notes that a common red flag for a phishing message is the inclusion of a suspicious link and provides the following advice for dealing with this type of attack:

---

[1] See paras. 72-73 of Privacy Complaint Report PR16-40.

[2] https://www.ipc.on.ca/wp-content/uploads/2019/07/fs-tech-protect-against-phishing-e.pdf

> Never click on suspicious links. Hover your mouse over parts of the message without clicking on anything. If the underlying hyperlink looks strange or does not match what the link description says, do not click on it — report it. Note that images can also contain suspicious links.

[16] The Fact Sheet provides detailed guidance on protecting against phishing attacks, which includes the following:

- Segment networks that contain sensitive data from other networks. You can limit the impact of compromised computers and accounts by restricting their access to other networks or systems. For example, public-facing webmail servers should be isolated from intranet systems or human resources databases.

- Use threat intelligence and endpoint protection tools. Advanced tools can detect, and in some cases, prevent attackers from gaining a foothold inside your network by flagging unusual patterns of system behaviour, such as irregular login attempts and large file downloads.

- Enable encryption on documents, devices, and databases that contain sensitive information, by default, to provide an extra layer of defence against unauthorized access, use, and disclosure by attackers.

- Conduct regular phishing awareness and training. Send simulated phishing attacks to employees to test their awareness and knowledge of how to respond. Routine tests raise awareness of security issues and help identify employees who need additional training.

Measures in Place at the Time of the Incident

[17] The TTC rolled out cybersecurity training in 2021, prior to the incident; this training was mandatory for internal system users. The employee who clicked on the malicious link had taken this training the month before the cybersecurity attack. The TTC provided the following description of this training:

> The course is a 31-minute "Need to Know" series which is intended to provide TTC employees with fundamental knowledge on information security terminologies and threats such as phishing, password, malware, Internet-of-Things, mobile security, and other security related topics. Upon completion of this course, participants should be able to:
>
> - Understand the employee's role in protecting TTC information security
>
> - Identify different types of social engineering, see the red flags of an email, and understand the common threats associated with cyber attacks

- Various definition on malware, ransomware, phishing emails
- Actions upon identifying these threats.

[18] The TTC states that, in addition to the testing, it had standards in place to address vulnerabilities and patch management, endpoint security protection, email protection, and firewalls. The TTC also conducted penetration testing of its environment in 2018 and developed its Cybersecurity Program following this testing.

[19] When I asked the TTC to provide me with guidance documents related to computer security and incident response at the time of the incident, they provided the following policies:

- IT Systems Security Control
- New Employee Familiarization
- Information Management
- Computer Security - Assets and Information
- TTC Cloud Computing[3]

[20] The TTC later provided me with an additional policy in place at the time of the incident - the Vulnerability and Patch Management Standard (the 2021 Patching Standard). The TTC also provided a draft version of a revised Patching Standard (the 2023 Patching Standard) that they anticipated having in place soon.

[21] The 2021 Patching Standard is most relevant to the attack, as the threat actor exploited the TTC's failure to patch a known vulnerability. It sets out that server owners should ensure that they are aware of new patch releases and are required to document the severity rating of the new patch, either obtaining this from vendors or, if necessary, calculating this rating themselves. This calculation should be based on the importance of the business, the classification of data on the server, and the level of risk if a compromise were to occur. The policy recommends automated patch distribution in order to expedite the process. The policy also provides expected timelines for patch application, from one day for zero-day critical patches on critical production environments to 60 days for low severity patches.

[22] This policy states that routine vulnerability scanning should occur "on a schedule or ad-hoc basis," noting that the frequency and comprehensiveness of such scanning should be rooted in a risk-based analysis of the security of information systems. Remediation and mitigation should be prioritized based on the severity and "impact on

[3] The TTC did also note that it was in the process of drafting additional relevant policies at that time. Those draft policies were not in place at the time of the incident but are addressed later in this Report.

the confidentiality, integrity, or availability of TTC information system."

[23] Of the remaining policies, only one – *IT Systems Security Control Policy* – specifically addressed cybersecurity concerns. It requires that the TTC's computing systems: eliminate or mitigate threats identified in specified publications; authenticate and authorize user identities; and use encryption controls per approved standards. It also required that TTC coding standards be updated every two years to guard against commonly known software vulnerabilities. These requirements acknowledge the threats posed by cyberattacks, but the general nature of this policy means that it does not itself include the granular detail of the steps needed to prevent an attack or respond as required. However, the greater issue is that these steps, other than those relating to patch management, are also not set out in any other guidance documents in place prior to the incident that the TTC provided to this office.

[24] Regarding the other policies in place, the *New Employee Familiarization Policy* includes computer security as one of the practices and procedures that that new employees are required to review when beginning their job but makes no further reference to computer security of any sort.

[25] The *Information Management Policy* states that personal information must be protected in accordance with *MFIPPA* and that the "TTC is responsible to ensure legal requirements are followed for the collection, storage, integrity, security and authorized disclosure of Personal Information under its control." That policy also specifies that the TTC uses a classification scheme to separate information into confidential, internal, and public and that the TTC must protect the information "by applying security measures commensurate with the information classification."

[26] *Computer Security - Assets and Information* lists data integrity, privacy, and handling of data in accordance with security concepts as some of the purposes of the policy. It requires employees to safeguard information assets against disclosure of information to third parties and loss and requires employees to report any known or suspected weaknesses in computer security. While this policy does provide statements on information security protections, it does not specifically address matters relating to cyber attacks, much less patches for vulnerabilities or phishing cautions.

[27] *TTC Cloud Computing Policy* requires that the TTC's Information Security Office perform privacy impact assessments, and threat and risk assessments, for confidential data sets. The Information Security Office is responsible for specifying the security requirements for data protection. This policy also sets out the CSA Security, Trust and Assurance Registry levels required for public data and confidential data but does not specifically address cyber threats.

Analysis

[28] The phishing attack in this case was pernicious and difficult to spot. Phishing

attacks often look like they are from a trusted source, but upon further inspection can be seen to be from an impersonator. Here, the threat actor actually took over the trusted third party's email address, so employing the usual signs to look for in authenticating an email address would not have helped. However, the specific vulnerability identified by the TTC,[4] which was exploited during the incident, was a publicly known security vulnerability of significant concern, with a patch available for months prior to the attack. At the time of the attack, the TTC had the 2021 Patching Standard in place, which required that the server owners remain up to date on new patches. Under this policy, a vulnerability of this nature should have been patched within days, not months. It is not clear why the TTC failed to identify and/or deploy this patch, contrary to its own 2021 Patching Standard.

[29] The TTC is a large, sophisticated, public-facing organization. It should have up to date and effective security measures in place to protect the personal information it holds, as well as other confidential or sensitive data. None of the above policies set standards for endpoint security protection, email protection, and firewalls - the measures that the TTC stated were in place.

[30] The TTC acknowledged that while documented standards were not in place, it did utilize an endpoint security system at the time and was in the process of replacing it with a different endpoint detection and response system. If the TTC did have additional protections in place, they did not provide me with the details of these, and the lack of guidance documents indicates that it did not formally mandate those measures.

[31] Section 3(1) of Regulation 823 of the *Act* requires that security measures to prevent unauthorized access to records are "defined, documented and put in place." Based on the information made available to me, I find that the TTC did not have reasonable security measures documented and in place, as required under Regulation 823 of the *Act*.

Issue 2: Did the TTC respond adequately to the breach?

[32] The IPC has published guidance on best practices for institutions to respond to privacy breaches. *Privacy Breaches: Guidance for Public Sector Organizations*[5] (the Privacy Breach Protocol) states that organizations should take steps to identify the scope of the breach, contain it, and notify those affected. They should also investigate the breach to determine not just how it occurred, but the steps can that be taken to prevent similar breaches in future, including training. As such, remediation of the breach and steps taken to improve training also form part of the breach investigation.

Scope and Containment

[33] The TTC discovered the cybersecurity intrusion shortly after it started. Soon after the attack, the TTC sent emails to all employees, noting that its "IT systems are

[4] I will not name the vulnerability and associated patch due to security concerns.
[5] https://www.ipc.on.ca/wp-content/uploads/2019/09/privacy-breach-protocol-e.pdf

experiencing some issues" and asked that all employees and contractors log off the TTC IT system until further notice. The day after the attack, the TTC informed employees that it had been the victim of a ransomware attack. Employees were told not to log in to TTC computers and were advised that they would not have access to email or work programs until further notice. Shortly after that, the TTC developed a priority order to have TTC devices "cleaned" via security patches and by validating that the endpoint detection and response solution was active. The TTC provided "Dos and Don'ts" for those employees who received the patches.

[34] In the two weeks following the breach, the TTC determined that the threat actor may have taken the information from as many as 25,000 TTC employees, former employees, and pensioners. The TTC was later able to determine the type of personal information that may have been accessed, including names, contact information, demographic information, employment history, medical conditions, and driver's license information. The TTC later revised the number of affected individuals to less than 70% of the earlier estimate, based on data analysis.

[35] As part of its security protocols, the TTC immediately engaged a forensic investigator, who determined the amount of data exfiltrated, which files were potentially exfiltrated, and the method of exfiltration. The TTC also obtained additional information regarding the data exfiltrated, the specifics of which the TTC has requested remain confidential, due to security concerns.

[36] As previously noted, the TTC stated early in its communications with the IPC that some TTC data had been posted on the dark web for a short time before being removed. Later communications were not as clear whether this posting had occurred. The TTC stated that it has continually monitored the dark web since that time and has not found evidence of subsequent publication or sale of TTC data.

[37] Regardless of whether this information was posted or otherwise available on the dark web, the reality is that once data is stolen, it is beyond the TTC's control. In such situations, one should assume that it is being used by bad actors and take steps accordingly. While dark web monitoring can be useful in discovering a breach or determining its extent, it doesn't change the fact that institutions cannot remove personal information posted by bad actors. Given this, I am satisfied that the TTC has adequately determined the scope of the breach and taken the steps available to it to contain the breach.

Notification

[38] As noted, the TTC sent out the Update on the cybersecurity incident, providing a preliminary outline of the types of information that may have been stolen, setting out the approximate number of individuals affected, and noting that those affected were past and present TTC employees. The Update stated that "impacted individuals will receive a letter with more information" and that employees were encouraged to sign up for an

identify protection service that the TTC had arranged. Employees had to provide only their names in order to do so, and this service provided identity theft insurance coverage over the next three years. The TTC later reported to the IPC that approximately 12,000 individuals enrolled in that service. The Update also included a FAQ section, addressing questions relating to the breach.

[39] The TTC stated that they would be sending a second notification letter to those affected, to clarify the types of information involved. The TTC subsequently provided the IPC with de-identified copies of these notification letters. For the majority of those affected, these letters described the results of the investigation as follows:

> It was found that some personal information of current and former employees was accessed or taken in this incident. However, most of the information that was accessed can be categorized as driver's license information and/or occupational health and workplace information, including absence reports.

[40] The TTC sent a modified version of this letter to the minority whose SINs were taken, stating "[we] are reaching out to inform you that there is evidence that some of your financial information was compromised, specifically your Social Insurance Number."

Investigation and Remediation

[41] The TTC learned of the breach as soon as it occurred and took immediate action to secure their systems and restore them from backups. The TTC states that they hired industry-leading information technology experts to ensure that the systems were restored in a secure manner. This included ensuring the appropriate patches were in place before restoring compromised systems. The TTC also retained cybersecurity and forensic experts to investigate the breach itself. In addition to discovering how the breach occurred, these experts also made efforts to find the threat actor and track what happened with the data following the breach.

[42] The TTC stated that following the incident, it engaged a third party to perform penetration testing and vulnerability assessment in relation to the TTC's information technology environment. This agent identified solutions for all vulnerabilities identified. Continuous monitoring has been in place since the incident, and they have not found any identified vulnerabilities within the TTC's external environment.

[43] The TTC also provided a list of updates to its security measures that it was planning to take or had already implemented. This included enhancing monitoring and detection, in order to focus on network and end point devices protection, and integrating the threat management program, so that it was implemented under one roof. The TTC identified a number of security solutions that would be updated, including vulnerability and patch management, and stated that it would be implementing segregation of critical assets. The other measures listed were good steps to take to prevent network intrusions but

were not specific to a phishing attack. Given this, and the fact that the TTC expressed security concerns with those measures being made public, I will not provide further details on these steps.

Updated Guidance

[44] Following the breach, the TTC put in place additional guidance, in the form of the following policies:

- Cybersecurity Policy
- Cybersecurity Training Policy
- IT Vulnerability Management Policy
- Identity and Access Management Policy

[45] The TTC provided the IPC with draft versions of the above policies, which I will discuss in more detail. The TTC stated that they expected that these drafts would be finalized by the end of the first quarter of 2024. Given that the incident occurred in October 2021, I asked the TTC for the reason for the two-year plus delay. The response was that this time was required "because of internal processes required to review within such a large institution as the TTC and because these policies address more than just the specific incident."

[46] As noted above, the TTC also provided the IPC with the 2023 revision to its Vulnerability and Patching Standards. As this attack occurred chiefly due to the exploitation of a known zero-day vulnerability, I will address that policy and the relevant revisions to it first.

2023 Patching Standard

[47] The 2023 Patching Standard emphasizes the importance of security updates and patches, calling these "the second line of defence to safeguard TTC information and information systems." It cautions that a lack of security patches could expose TTC infrastructure to unauthorized access and system exploitation, potentially resulting in the critical safety systems not being available or personal information being disposed of without authorization.

[48] The 2023 Patching Standard requires that all TTC assets be maintained with the latest security patches and threat protection. It also requires the TTC to conduct regular vulnerability scanning and assessment to ensure that critical patches and updates are "detected and applied in a timely manner." If the scans pick up any open vulnerabilities, these should be shared with TTC and relevant third-party stakeholders; in the case of critical vulnerabilities, this should occur within 48 hours of their discovery.

[49] Vulnerabilities should be remediated within two months of the fix being publicly released, except for zero-day and actively exploited vulnerabilities. For these, the TTC has put in place a step-by-step process, in which it has 24 hours to assess the potential impact, severity, and affected systems or assets, and put temporary mitigation measures in place, such as isolating affected systems or deploying intrusion detection/prevention systems. Once they become available, critical patches must be deployed within 72 hours and non-critical patches within a week. Following this, the TTC should verify the effectiveness of the fixes via vulnerability scans or penetration tests in the two weeks following the patch's release. The TTC should also conduct long-term remediation by assessing the root cause or underlying vulnerability that allowed the zero-day or active exploitation to occur and develop long term remediation measures.

[50] The need to identify patches and the general timelines for deployment of patches are consistent between the 2021 and 2023 versions of this policy. However, the failure to patch the vulnerability that contributed to the attack was not due to a deficiency in the 2021 Patching Standard, but rather a failure to implement it. The new IT Vulnerability Management Policy (discussed below) now provides clearer guidance on who is responsible for patching the TTC network. I also note that the 2023 Patching Standard policy provides guidance that I find clearer and easier to read than the 2021 Patching Standard.

TTC Cybersecurity Policy

[51] This policy sets out the roles and responsibilities of various bodies and departments throughout the TTC. Under this guidance, the Chief Information Security Officer (CISO) Office is responsible for designing and implementing adequate security controls, maintaining and operating a secure computing environment, and identifying security risks, among other responsibilities. The CISO Office is also accountable for cybersecurity incident management, including developing the incident response plan, and incident containment and mitigation processes. The Cybersecurity Policy sets out the principles that CISO Office is to follow for threat identification, protection, and response.

[52] Under the Cybersecurity Policy, all TTC employees, contractors, and service providers must immediately report any known or suspected cybersecurity incidents, including phishing, viruses, malware, and ransomware. They are provided a dedicated email address to report these to. The Cybersecurity Policy also states that Information Technology Services shall conduct vulnerability scanning and patching of the network and computing assets in accordance with TTC's Vulnerability Management Policy (discussed below).

IT Identity and Access Management Policy

[53] The policy states that the TTC follows the need-to-know principle and the least privilege principle. TTC employees will have access to the technologies used to fulfill their roles and responsibilities but will be provided with only the minimum privileges necessary

to do so, as authorized by the appropriate supervisor or manager. Passwords must be set in accordance with the TTC Identity Protection Standard. Individuals with elevated privileges may only access sensitive data for the purpose of the specific task they require it for, and when doing so, must use a different password for the privileged account than they use for their regular user account.

IT Vulnerability Management Policy

[54] The policy specifies that the IT Asset Manager and IT Asset Support Analyst are responsible for patching of the TTC network. This includes scanning the network for vulnerabilities and identifying, categorizing, and prioritizing those patches. This is to be done in accordance with the Patching Standard, discussed in more detail above. These positions are also responsible for remediating zero-day security vulnerabilities via the application of patches, and for obtaining the latest patches from its vendors.

TTC Cybersecurity Training Policy

[55] The purpose of this policy is to provide the TTC workforce with cybersecurity training and awareness. The workforce should be informed about prevalent risks and threats in the cybersecurity domain.

[56] The Information Security Office provides customized cybersecurity training to the workforce based on their job roles and responsibilities. All TTC employees, contractors, and third-party service providers must complete annual cybersecurity training and the content of the training itself is subject to annual review.

[57] The TTC provides this training through its own learning management system, which also tracks whether an employee has completed the training. Some training may be delivered through other methods, such as the Information Security intranet site, corporate notifications, and cybersecurity awareness articles in the TTC's weekly bulletin. The policy also specifies that if an individual does not successfully complete the Cybersecurity Awareness Program by the deadline, their user accounts will be temporarily disabled.

Analysis

[58] This breach occurred because a threat actor was able to use a phishing attack to obtain access to the TTC's systems, and then exploit a known vulnerability that the TTC had failed to patch. In the course of investigating this complaint, it became clear that at the time the incident occurred, the TTC did not have adequate security guidance in place to protect the personal information in its custody or control and, in the case of the vulnerability exploited, failed to apply the guidance it did have in place.

[59] Since that time, the TTC has taken steps to fix the specific vulnerability and address the larger issue of lack of appropriate guidance. The revised Patching Standard clearly sets out the steps that must be taken when the TTC identifies a zero-day vulnerability

and provides timelines for the most critical steps. These require the TTC to put temporary mitigation measures in place, whether those are workarounds, isolating affected systems, or intrusion detection, within 24 hours. The Vulnerability Management Policy clearly states who is responsible for scanning for vulnerabilities, identifying the patches required, and putting those patches in place. This policy also specifies which positions within the TTC are responsible for remediating zero-day security vulnerabilities.

[60] The TTC has also put guidance in place addressing cybersecurity matters more generally. This includes a response plan for cybersecurity incidents and direction on how to identify threats and protect against them.

[61] From my review of the policies, the guidance now in place (and that will be in place imminently) puts the TTC on much better footing to defend itself against future cyber attacks than it had at the time of the incident.

[62] To avoid or minimize the impact of phishing attacks the Fact Sheet recommends the following: segmenting networks containing sensitive data from other networks; using threat intelligence and endpoint protection tools; enabling encryption as the default on documents, devices, and databases containing sensitive information; and conducting regular phishing awareness and training. As noted above, the TTC provided the IPC with specific planned or implemented updates to its security measures. Most have been implemented already, though a few have upcoming completion dates, with the first quarter of 2024 being the latest expected completion date.

[63] These security measures are in line with what is recommended in the Fact Sheet and what is expected of large organizations with access to sensitive data. They are decidedly more comprehensive than the protections in place at the time of the incident. I will not describe these in greater detail due to the security concerns expressed by the TTC, but I do note that they include enhanced monitoring for threats, enhanced end point security protection, and segregation of critical assets.

[64] The one departure from the Fact Sheet is in the TTC's approach to encryption. The TTC's Cybersecurity Awareness Training Course lists "Using Encryption" as one of its topics. The Cybersecurity Policy includes references to established cybersecurity frameworks which include encryption standards. However, that policy also states that these frameworks will only be used as guidance and that the TTC will establish its own controls based on internal direction. I did not find explicit statements that the TTC has enabled encryption as a default as it relates to sensitive information. Given this, I recommend that the TTC put direction in place confirming that it will be enabling encryption as the default on all documents, devices, and databases containing personal information.

[65] I find that the TTC now has reasonable measures in place to protect personal information as required by section 3(1) of Regulation 823 under the *Act*.

CONCLUSION:

Based on the results of my investigation, I have reached the following conclusions:

1. At the time of the incident, the TTC did not have reasonable security measures documented and in place, as required by section 3(1) of Regulation 823 under the *Act*.

2. The TTC now has reasonable measures in place to protect personal information as required by section 3(1) of Regulation 823 under the *Act*.

RECOMMENDATION:

Based on the above conclusions, I recommend that the TTC put direction in place confirming that it will be enabling encryption as the default on all documents, devices, and databases containing personal information.

Within six months of receiving this report, the TTC should provide this office with proof of compliance with this recommendation.

Original Signed By: April 5, 2024

Jennifer Olijnyk
Investigator