For Action
with Confidential Attachment

TTC Status Update – Information and Cybersecurity Strategy

Date: May 13, 2020
To: TTC Board
From: Chief People Officer

Reason for Confidential Information

This report contains information related to the security of the property of the municipality or local board.

Summary

Organizations consistently face the challenge of protecting their digital assets from cybercriminals who continue to exploit security flaws to disrupt the confidentiality, integrity, and availability of information.

Toronto Transit Commission (TTC) is unique in its cybersecurity challenges as it is considered a critical infrastructure organization that consists of a complex computing ecosystem, which includes various mission critical industrial control systems (ICS). The security objective of a typical organization is the protection of its information, whereas an organization with an industrial control system has the additional concern of protecting the integrity of these systems. A successful attack on an ICS could have serious impacts on TTC including service shutdown, financial loss, and health and safety risks.

In the past, ICS were secured by isolating the networks. The modern-day, transit-based Information Technology (IT) infrastructure is highly complex, especially due to the emergence of new technology fueling the need for connected vehicles, connected devices and connected people. The demands of cloud-connected devices and a mobile workforce require industrial control and management systems to have access to the internet and corporate information, leading to the convergence between the corporate and industrial networks. This increases the exposure to threats, hence making these mission and safety critical systems vulnerable to direct and indirect attacks, which will require new and different ways to secure the environment with additional tooling and services.

In order to mitigate these risks and to defend against potential cyberattacks, TTC has developed the Information and Cybersecurity Strategy, and established a program to implement the various initiatives. In addition, the TTC continues to collaborate with the

City of Toronto's cybersecurity team in an effort to align strategies and share information.

This report provides an update on cybersecurity at TTC; the strategy to improve TTC's security posture; and an update on the ongoing activities within the TTC cybersecurity program.

Recommendations

It is recommended that the TTC Board:

1. Endorse the Information and Cybersecurity Strategy as outline in this report.

2. Direct that the information contained in Confidential Attachment remain confidential in its entirety as it contains information related to the security of the property of the municipality or local board.

Implementation Points

Staff will return to the board in the third quarter of 2020 to present a completed enterprise risk assessment of cybersecurity within the TTC.

Financial Summary

TTC's Cybersecurity program is focused on enhancing the security of TTC's IT and industrial control infrastructure. In 2019, TTC focused on investing in key technologies that will enable advanced detection and prevention capabilities.

This report has no additional capital financial impact beyond what has been approved in the 2020-2029 Capital Budget and Plan. The total project cost for the cybersecurity project is approximately $10.3 million. To date, approximately $1.3 million has been invested on stabilizing the network, securing the perimeter, and preparing the scope of services to procure advanced security monitoring, detection and protection, reporting, and incident response capabilities.

The Interim Chief Financial Officer has reviewed this report and agrees with the financial impact information.

Equity/Accessibility Matters

A cornerstone of TTC's Corporate Plan 2018-2022 is accessibility and being a proud leader in providing accessible public transit in the City of Toronto. We are committed to ensuring reliable, safe and inclusive transit services for all our customers. This is supported through the work described in this report to secure all data concerning employees and customers.

Decision History

At the December 13, 2017 meeting of the Audit and Risk Management Committee, staff presented a report providing the Committee members with an understanding of key cybersecurity risks and mitigation strategies associated with the TTC's systems. https://www.ttc.ca/About_the_TTC/Commission_reports_and_information/Committee_meetings/Audit_Risk_Management/2017/December_13/Reports/6_Presentation_Cyber-Security_Risks_%26_Mitigation_Strategies-.pdf

In October 2019, City Council adopted item "Cyber Safety: A Robust Cybersecurity Program Needed to Mitigate Current and Emerging Threats". Through Council's adoption of this item, all Agencies, Boards and Commissions (ABCs), including TTC, were requested to provide a cybersecurity enterprise risk assessment by Q3 2020 to the City's Chief Technology Officer. The City's Chief Technology Officer was also mandated to provide support, oversight and directions on standards, practices and policies to all ABCs; to work with the ABCs to assess regulatory and compliance matters and their impact on moving to a centralized information technology services; and to report on an implementation plan for a centralized model to provide oversight and approval for all technology assets, goods and services purchased by ABCs, including TTC. http://app.toronto.ca/tmmis/viewAgendaItemHistory.do?item=2019.AU4.1

On December 12, 2019, the TTC Board adopted Recommendation 1 of City Council's decision, and supported in principle Recommendations 2, 3 and 4 for the purpose of providing support to the City's Chief Technology Officer in order to respond to City Council's direction. https://www.ttc.ca/About_the_TTC/Commission_reports_and_information/Commission_meetings/2019/December_12/Reports/17_Audit_Risk_Compliance_Emergency_Management_Program_Update.pdf

Issue Background

Over the years, the TTC has implemented various controls and measures to deter cyber threats. Products and services have been implemented with the aim to keep the TTC, its customers, employees, and assets safe.

In January 2018, Metrolinx was attacked by a foreign coordinated virus that infected computers at Ontario's transit agency. In response to that attack, TTC utilized an existing vendor under contract to conduct a security assessment of the IT network to identify vulnerabilities and remediate any high-risk findings to prevent a similar attack.

Subsequently, there was an ongoing, overall audit of TTC being conducted by the American Public Transportation Association (APTA). In specific reference to information and operational technology security, the APTA audit recommended that the TTC should conduct security assessments of its industrial control system networks due to the safety-sensitive risks involved. Accordingly, TTC published a Request for Proposal (RFP) to procure a vendor to conduct this assessment. The contract was awarded to the same vendor that was completing the IT Security assessment and the advancements made on this work are summarized in this report.

Comments

1. Security Assessment

TTC sourced the third-party security assessment to Long View Systems. The vendor has been in business since 1999 and offers a wide range of services, including digital defence, which is used to assess the security posture of an organization.

Long View conducted the Corporate IT security assessment from March 2018 to September 2018, and the Industrial Control Systems (ICS) security assessment from February 2019 to August 2019. The assessment was conducted in accordance with an approved plan agreed upon by Long View and TTC. The goal of the assessment was to conduct an in-depth evaluation of TTC's network configuration and to identify existing risks in the current network.

The assessment methodology followed an industry standard guide for security testing and assessments, which comprised of the use of various testing and validation techniques and interviews with internal stakeholders.

The findings from the assessment were collated, and an action plan was developed to remediate the findings of these assessments. Remediation of findings started immediately alongside with the vendor and the respective support teams of the IT and ICS networks. The TTC team has remediated the majority of the findings, while others have been factored into the TTC's Cybersecurity Strategy. For outstanding items that could not be remediated and which have been rolled into the Cybersecurity program, additional monitoring has been put into place to ensure that the vulnerability identified is not being exploited. In few cases, features have been temporarily disabled or blocked until such time that the mitigating controls are in place. Additional information and details are contained in the confidential attachment to this report.

2. Information and Cybersecurity Strategy

TTC has developed the Information and Cybersecurity Strategy to successfully identify, manage, and mitigate information and cybersecurity risks across diverse TTC environments and information systems through strategic and tactical measures and appropriate controls. The strategy aims to strengthen the cyber resilience of TTC's critical business systems, industrial control networks, other key systems that support transit operations, and their data against an evolving threat environment.

The action plan (i.e. the Cybersecurity Program) focuses on immediately remediating vulnerabilities and implementing recommendations identified as part of TTC's third-party security assessment; and in parallel build a risk-based approach in managing cybersecurity and establishing a robust cybersecurity audit program to continue to identify additional vulnerabilities and exposures.

TTC's Cybersecurity Strategy is structured into four strategic pillars. These four pillars are built upon the core functions (i.e. Identify, Protect, Detect, Respond, and

Recover) within the National Institute of Standards and Technology (NIST) framework for Improving Critical Infrastructure Security. More information on each of the four pillars is listed below.

a. Mature governance and risk management practice

This pillar focuses on establishing the governance requirements and identifying the risk profile that applies to TTC. The objective is to ensure that TTC understands its business operating environment; that it has a good knowledge and understanding of what information and operational technology assets it owns; and what risks, vulnerabilities, and threats exist for these assets.

Cybersecurity Audit Program

TTC conducts various security testing, but in order to improve cybersecurity, TTC will need to put in place a formal and robust cybersecurity audit program that focuses on regular/periodic vulnerability assessments, penetration testing, compliance audits, and overall cybersecurity maturity gap analysis.

Enterprise Risk Management

TTC, through an internal working group, will establish a cybersecurity risk management framework and conduct a detailed enterprise risk assessment. This will allow TTC to make informed decisions about cybersecurity investments based on its risk appetite.

Policies, Principles, Procedures, and Standards

TTC is committed to reviewing all current policies and to establish new policies as required to support the cybersecurity program. This also includes the development of standards to be used in all procurement requirements and as building blocks for technological solution implementations.

b. Strengthen cybersecurity capabilities to enable safe and secure transit operations

This pillar focuses on the development and implementation of appropriate safeguards and capabilities to ensure TTC can deliver safe and secure transit services for its customers.

Corporate and Industrial Control Systems Security

TTC has made significant investments in modernizing the security controls of its corporate and industrial control system network. This initiative continues the procurement and implementation of new capabilities to stay ahead of the threat landscape. It also looks at ensuring industry acceptable controls are applied, such as those set out in the Center for Internet Security (CIS) critical security control benchmarks.

Identity and Access Management

Identity and access management play a pivotal role in security posture. As such, the team is preparing to move to a role-based access and restricted privilege access for critical infrastructure and systems.

Education and Awareness

One of the largest risks to an organization's security systems is human behaviour and their awareness to potential risks and threats. Employee education and awareness helps in driving day-to-day compliance to security controls. TTC will coordinate targeted sessions on topics spanning threats, such as phishing, e-mail, social engineering through the HUB and other channels. Regular mandatory training and awareness engagements will be scheduled for TTC's Leadership staff.

c. Improve cybersecurity resiliency in detecting, responding, and recovering from incident and breaches

This pillar focuses on ensuring that the TTC can expediently detect a cybersecurity attack, take appropriate action to contain the impact of the incident, and restore any business operations with minimal impact.

Forensics and Investigations

Retainer services will be added for forensics, incident response, table-top exercises and any other additional skillsets that may be needed.

Threat Intelligence: Detection and Response

TTC will procure the services of a Managed Security Services Provider (MSSP) that has a strong background with securing an industrial control systems environment to augment existing security operations. This will further strengthen the detection and response process. Additional capabilities will be procured through the MSSP to improve TTC's resiliency.

Disaster Recovery and Business Continuity

TTC will continue to evaluate through "tabletop exercises" its ability to respond to a cyber crisis from both a business and technical perspective. These ongoing efforts will help in maintaining robust and up-to-date emergency response and business continuity plans.

d. Advance overall standing on cybersecurity posture

This pillar focuses on establishing the TTC as a leader and collaborator in the cybersecurity industry, one that is prepared and ahead of evolving threats.

Threat Intelligence and Innovation

Through the use of artificial intelligence and machine learning, it is expected that cyber threats will evolve, revealing new ways of attacking organizations.

The cyber threat will evolve, as it is expected that criminals will use artificial intelligence and machine learning to find new ways to attack organizations. Soon the threat is expected to evolve to cyberattacks through the use of artificial intelligence and machine learning. TTC will need to keep ahead of these new emerging threats through innovation of its cybersecurity defense controls and through intelligence gathering from the global community. TTC's security analysts must continue to undertake research and receive ongoing training in order to support the TTC in its security readiness.

Partnership

TTC works with the City of Toronto and other enforcement agencies to share security requirements and threat intelligence. Also, TTC continues to strengthen ties with security executives in partner transit agencies around the United States and Canada for information sharing sessions.

3. Completed Actions

TTC has implemented several activities to improve the security posture of the organization. The following is a summary of the actions taken to date:

- TTC has invested in cybersecurity insurance. The Insurance safeguards TTC against any Cyber liability to protect the business against the risk of cyber threats.

- TTC continually works on protecting both the Industrial and IT networks. A new perimeter defense has been built around the Industrial control environment. To keep the network resilient against emerging threats TTC performs regular infrastructure vulnerability scans, penetration testing and findings are remediated. To stay ahead of the evolving threat landscape, TTC will always upgrade devices to keep them current and supported.

- End-point devices such as desktops, laptops, tablets, servers, and mobile devices are also a huge exposure for TTC and any organization especially when it comes to mobility and enabling people to work from anywhere. TTC has invested in virus/malware protection for these devices. This ensures the device can detect, contain and report any attack/breach.

- Along with the perimeter and end point protection network, the volume of traffic moving across the TTC network is also important. TTC has invested in devices that can scan traffic movement in order to identify, contain and report any detected anomalies.

- TTC is heavily focused at staying compliant and up to date on its security controls. Therefore, TTC carries out security compliance audits to ensure compliance with all legislative and regulatory requirements. TTC has been actively conducting security testing including vulnerability scanning, web and mobile application testing and penetration testing. Recently, TTC engaged a third party to assess the corporate and industrial networks. All the findings of the assessments that could be remediated with existing controls have been and any gaps have become part of our Cybersecurity Strategy. The goal is to conduct regulatory audits as needed and assessments every two years.

COVID-19 Response

The current COVID-19 pandemic has resulted in many TTC staff working from home for the first time. Working remotely has unique cybersecurity risks, especially as cybercriminals look to exploit the current coronavirus pandemic to target organizations and individuals. The objective during this time is to ensure the security and integrity of TTC and its information and the protection of its employees and customers.

TTC has been mobilizing its workforce over several years to allow end users to work at various TTC sites as well as remotely using TTC issued laptops and tablets. Over half of TTC's computing end users have these devices which ensures that the same security controls and updates are in place as if they were in the office.

For those that do not have a TTC laptop or tablet and are using their personal PCs to connect, we ensure that they connect via the web browser. This helps to ensure the integrity of TTC network as their personal PCs are not directly connected to TTC system.

Lastly, the Information Technology Services Department is conducting regular security education and awareness campaigns. In doing so, it is educating people on best, most secure practices when it comes to e-mails, browsing the web and sharing information. Several corporate communications have been sent reminding people of secure practices when working from home including sharing or printing information, transporting their TTC asset and collaborating via audio or video conference. We continue to send out regular reminders and have centralized all the key points onto an intranet web page that everyone has access to.

4. 2020 Key Focus

In 2020, TTC's primary focus as part of the cybersecurity program will be to award a contract to a successful vendor for the procurement of a Managed Security Services Provider (MSSP) and complete the enterprise risk assessment of TTC's cyber landscape. Additionally, TTC will begin preliminary work within each initiative and continue to procure the required solutions to remediate the findings of the third party security assessment and to enhance our perimeter, endpoint, and network defense capabilities.

Managed Security Service Provider RFP

TTC will engage the services of a Managed Security Services Provider (MSSP) to augment, through an external provider, TTC's security operations and as a vehicle to procure and implement additional capabilities. The RFP was developed and posted on March 5, 2020.

From 2018 to present, TTC has been engaged with the City of Toronto's cybersecurity program team. Upon learning that the City was working on an RFP for a Managed Security Service Provider (MSSP), TTC aspired to piggy-back on the same RFP to leverage the economies of scale. TTC worked with the City's Cybersecurity team to include TTC's requirements in their RFP, but we were not able to include mandatory requirements relating to TTC's industrial control systems. This lead TTC to developing its own RFP, as not including the requirement would have been a risk that the RFP is awarded to a vendor that did not meet our specific and critical requirements. However, TTC's RFP contains provisions for non-exclusivity of products/services under the Supplier, which allows TTC to still piggy-back off the City's award for products where appropriate for a transit organization.

The RFP closes on May 13, 2020.

Enterprise Risk Assessment

Significant work is in progress as part of the cybersecurity program to complete an enterprise risk assessment of TTC's cyber landscape. As per City Council's directive, which was adopted by the TTC Board, the assessment will be forwarded to the City of Toronto's Chief Technology Officer by Q3 2020 and subsequently TTC will submit the risk mitigation plan by Q4 2020.

Contact

Dhaksayan Shanmuganayagam, Head – Information Technology Services
416-393-3922
dhaksayan.shanmuganayagam@ttc.ca

Ronnie Persad, Director – Information Security Office
416-393-4218
ronnie.persad@ttc.ca

Signature

Gemma Piemontese
Chief People Officer

Attachments

Confidential Attachment – Confidential Report and Presentation: TTC Information and Cybersecurity Strategy