Item 8.5

Section III – Items for the Information of the Board

TO: Chair and Members of the Board of Directors
Friday, June 25, 2021 Meeting

FROM: Michael Tolensky, Chief Financial and Operating Officer

RE: **UPDATE ON THE AWARDED CONTRACT FOR MULTI-FACTOR AUTHENTICATION UNDER TRCA'S VENDOR OF RECORD ARRANGEMENT WITH CDW CANADA**

KEY ISSUE

Update on TRCA's upcoming implementation of Multi-Factor Authentication (MFA) security measures.

RECOMMENDATION

WHEREAS Multi-Factor Authentication (MFA) for remote access is a new industry requirement for the renewal of TRCA's optional cyber insurance policy and therefore TRCA is implementing MFA to retain its coverage eligibility;

IT IS RECOMMENDED THAT this report on TRCA's implementation of MFA security measures be received.

BACKGROUND

TRCA's insurers have indicated that there has been a steady increase in cyber related attacks and losses facing the global IT sector. In particular, the industry has seen a 240% increase in ransomware attacks in the last operating year alone, and at the same time, ransomware payments have increased 2300%.

It has become standard for many organizations to finance the risk of cyber-attacks, As a result, TRCA has maintained a standard cyber insurance policy since 2017. This insurance policy provides both first party and third-party liability coverage in the case of a cyber-attack against the organization. TRCA's insurance brokerage, Marsh Canada has informed TRCA that 85% of cyber claims now come from organizations that have not implemented Multi-Factor Authentication (MFA). MFA is a security protocol that requires system users to verify their identity using two or more pieces of independent evidence, usually a combination of something the user knows (e.g., a password), something the user has (e.g., key generator) or biometrics (e.g. a fingerprint).

Because of its effectiveness in protecting against cyber-attacks, MFA has now become a minimum requirement for binding cyber insurance coverage as well as an industry-wide standard security protocol implemented by numerous businesses who require remote access to network services. The implementation of MFA at TRCA will require the installation of software as well as distribution of some hardware across the entire organization. Because of these new additional measures at TRCA, this report is being brought forward in accordance with TRCA's Strategic Business Planning (SBP) Policy, which requires that all potential new projects/programs or proposed modifications to existing initiatives must proceed through the SBP Policy workflow, including reporting to the Board of Directors for informational purposes.

At Authority Meeting #5/17 the Authority passed resolution #A111/17 awarding contract #10003898 for the Vendors of Record for Supply of End-Use Computing Devices and Services to three Ontario Education Collaborative Marketplace (OECM) vendors, including CDW Canada, for the purchase of end user hardware and software. Since that time, TRCA has been using the Vendor of Record arrangement to supply the majority of TRCA's computing and software needs.

RATIONALE

To meet the requirements of TRCA's cyber insurance policy, as well as to further protect TRCA's IT infrastructure, staff have been working diligently to implement MFA as quickly as possible. Given the ongoing success of using TRCA's Vendor of Record program as well as leveraging the OECM cooperative purchasing program, staff have elected to continue to use TRCA's end user computing system VOR to implement a combination of software and hardware systems to meet MFA requirements.

To implement MFA, staff have selected the Okta platform which was first launched in 2009. Otka's time in the market has given it a maturity and depth of integration support not found in other similar systems such as Azure Active Directory. Okta supports legacy systems that do not have integrated support for single sign-on authentication protocols. This will allow TRCA to continue to utilize critical programs such as TRCA's accounting software package as well as its centralized archival and document storage systems.

The use of the Okta platform will also allow for a centralized interface to access multiple applications, allowing for a single point of entry and a simplified and consistent user experience for all staff. In terms of the user experience, TRCA will be rolling out MFA using a combination of physical key generator fobs as well as cellphone applications. When implemented, network users will be requested to enter their username and password as normal but will be further prompted to enter a unique code provided by either their cellphone, or key generator fob before being allowed to login to TRCA's systems.

Relationship to Building the Living City, the TRCA 2013-2022 Strategic Plan

This report supports the following strategy set forth in the TRCA 2013-2022 Strategic Plan:
Strategy 7 – Build partnerships and new business models

FINANCIAL DETAILS

Initial implementation of MFA is estimated to cost approximately $40,000 - $60,000, ongoing costs are estimated at approximately $44,000 and will be allocated to IT capital account 014-01. TRCA has entered into a 3 year arrangement with CDW for the MFA service. The three-year arrangement provides a balance of stability in managing costs, while offering some medium-term flexibility to review the effectiveness of the service in the context of TRCA's evolving operating environment.

DETAILS OF WORK TO BE DONE

Information Technology and Records Management staff have begun implementation of MFA services. Full implementation will require installation of the MFA software platform across TRCA's computer network. Furthermore, MFA key generator fobs will be distributed to staff to enable the generation of unique identifiers to be generated by all staff. In addition to implementing MFA, staff continue to assess cyber security threats against TRCA to ensure its IT system is as resilient as possible to cyber-attack. This includes migration from legacy systems, security audits, and the development of standardized policies and procedures for the use of TRCA's IT network.

Report prepared by: Adam Szaflarski, extension 5596, Chris Moore, extension 5360
Emails: adam.szaflarski@trca.ca; chris.moore@trca.ca
For Information contact: Chris Moore, extension 5360
Emails: chris.moore@trca.ca
Date: June 16, 2021