CITY OF PRINCE GEORGE

STAFF REPORT
TO FINANCE AND AUDIT COMMITTEE

1100 Patricia Blvd. I Prince George, BC, Canada V2L 3V9 I www.princegeorge.ca

DATE: April 16, 2021

TO: STANDING COMMITTEE ON FINANCE AND AUDIT

NAME AND TITLE: Walter Babicz, Acting City Manager

SUBJECT: Options for Cyber Security Risk Review

ATTACHMENT(S): 1. 5-Year Capital Plan for Security Projects
2. 2021 Operating Budget for Security Systems

RECOMMENDATION(S):

That the Standing Committee on Finance and Audit:

1. RECEIVES FOR INFORMATION the report dated April 16, 2021, from the Acting City Manager, titled "Options for Cyber Security Risk Review"; and

2. CONSIDERS the three options to assess the City's cyber security risk, as presented in the report dated April 16, 2021, from the Acting City Manager, titled "Options for Cyber Security Risk Review."

PURPOSE:

This report is in response to the following resolution passed at the February 22, 2021 meeting of the Standing Committee on Finance and Audit:

> *That the Standing Committee on Finance and Audit DIRECTS Administration to report back to the Committee regarding options for an independent review of the City's cyber security risk.*

As the City becomes more reliant on computers, software, networks and data, the risk of a Cyber security incident increases. Cyber-security initiatives are intended to reduce the risk of a cyber-security incident.

Cyber Security refers to the protection of city assets and city staff from cyber threats that include software or communications disruption, data exposure or loss, and targeted social engineering attacks. Protection refers to the prevention, detection and response to cyber-threats and cyber-attacks.

City assets include electronic / digital systems such as financial or payroll software, city communications systems, customer data, and infrastructure such as water and waste control.

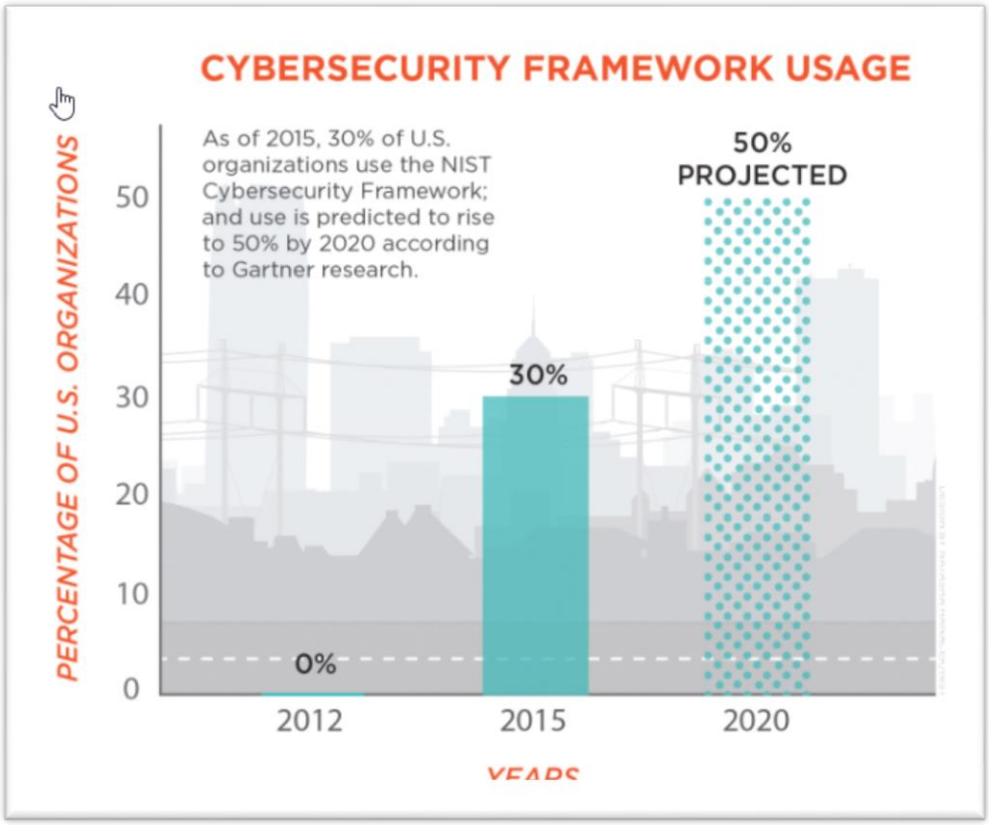
This report is intended to provide the Standing Committee on Finance and Audit, with an overview of the City's cyber security efforts, progress and plans and provide options for an independent review of the City's cyber security risk, as directed by the Committee.

BACKGROUND:

Cyber security is a young industry that has relatively few industry standards or frameworks. Current standards include NIST, ISO 27001 / 27002, HIPPA, GDPR and others.

The City IT Services department generally follows the NIST Cybersecurity framework. Developed by US based private sector organizations, the NIST cybersecurity framework has evolved to include governments, communities and organizations across the globe. See **Image 1** below for forecasted adoption of the NIST Cybersecurity framework.

Image 1



The NIST Cybersecurity Framework is a set of continuous functions intended to achieve specific cybersecurity outcomes. See **Image 2** for a summary of the NIST Framework and functions.

Image 2

IT Services utilizes the NIST Cybersecurity Framework to identify cyber security areas of focus, and to develop actions to address. As cyber threats continually evolve, these areas of focus and related actions change frequently.

The following are options to assess the City's Cyber Security risk.

Option 1 – Maintain Status Quo: No assessment. IT Services continues to follow the NIST Cybersecurity framework going forward, and invest in security technology and services as part of its 5 year capital roadmap.

Option 2 - Perform a Cyber Security Health Check: Conduct an independent Cyber Security assessment to identify key cyber security issues across the City.

Option 3 – Perform Security Tests: Conduct independent penetration tests of city systems including firewalls, networking, applications, databases and accounts. Penetration tests attempt to find exploitable weaknesses in the City's cyber security defenses.

FINANCIAL CONSIDERATIONS:

Option 1 – Maintain Status Quo: In its 5-year capital plan - IT Services has identified over $1.2 million over 5 years, for security related capital projects. See Attachment 1, 5-Year Capital Plan for Security Projects, for more details.

> **Note:** IT Services funds approximately $250k per year on security related hardware, software and services. This is approximately 6% of the total IT Operating budget. See Attachment 2, 2021 Operating Budget for Security Systems, for more details.

Option 2 – Perform a Cyber Security Health Check: The outcome of the Cyber Security Health check will be a report of the security gaps as well as recommendations and actionable items to improve the City's cyber maturity. The estimated cost for a Cyber Security Health Check is $25k - $40k.

Option 3 – Perform Security Tests: The outcome of the penetration tests will identify cyber security risks related to technology and/or technology configurations, and provide specific action items to address these risks. Depending on the scope of the testing, the estimated cost is $12k - $34k

> **Note**: IT Services has recurring security tests in its 5-year capital plan. The next security test will occur in 2022.
>
> **Note**: IT or City staff cannot address all action items. Software or hardware vendors are often responsible for making changes to their systems to address security risks.

SUMMARY AND CONCLUSION:

Cyber Security is complex, expensive and time consuming, but is critical to ensure the safety and integrity of all digital systems and services. While cyber security incidents at the city are relatively rare, security incidents at large organizations reliant on computers, software, networks and data such as the City, are a question of when… not if.

RESPECTFULLY SUBMITTED:

Walter Babicz, Acting City Manager

PREPARED BY: Bill McCloskey, Manager, Information and Technology Services

Meeting Date: May 10, 2021