Item #: BN069

Supplementary Budget – Briefing Note

2022 Budget

3rd Party Cyber Security Municipal Audit

Briefing Note required for:

-items +/- $50,000 or more
-changes in FTE
-Council Priority requests

Dept	Division	Item	Base Supp	Amount	FTE Impact
FBITT	ITT	3rd Party Cyber Security Municipal Audit	B	$55,000	0

Background:

A cyber security audit is an examination done by an unbiased third party to attempt to locate any weaknesses or vulnerabilities in our infrastructure. The third-party will attempt to gain access using the same methodologies and tools as a hacker would and, if successful, will attempt to further penetrate our network and report on any successes with details on how to prevent others from doing the same.

While the ITT team currently utilizes tools to help us identify these weaknesses, having an unbiased set of eyes on the infrastructure can show us areas that our current tools may not be scanning or aware of. It is for this reason, that having a regular audit done is becoming common practice for all organizations and something we expect our service providers to do. A 3rd party audit was also a high-priority recommendation of a recent security strategy workshop done in partnership with InfoTech Research Group.

Elements of the audit may include:

- Security Architecture Review
- Physical Security
- Network Monitoring and Security
- Firewalls
- Authentication and Authorization
- File System Security
- Remote Access Security
- Host Security
- Wireless Security
- Anti-Virus Solutions
- Intrusion Detection and Prevention
- Internet Traffic Analysis
- Social Engineering
- Policy Review

In the past, we have had partial audits completed in partnership with Chatham-Kent Police Services (CKPS). CKPS has an obligation to perform regular audits to ensure a secure infrastructure. Some elements of the municipal infrastructure

Background:

connect with CKPS so we are able to glean some information through this process. However, to obtain a complete picture of municipal infrastructure, we require an audit that covers all the municipal infrastructure.

The deliverable of this audit will be a report containing an executive summary, methodologies used, and a prioritized list of vulnerabilities identified, both internal and external facing, with recommendations on remediation actions that should be taken to correct them and supporting documentation.

Comment:

As Municipal ITT does not have access or knowledge of the PUC SCADA network, this item will not be scanned or assessed. However, any items found in the course of the exercise related to the PUC SCADA network will be passed on to PUC staff for their review and action.