Audit Committee Report

DATE: Monday, May 31, 2021 **WARD(S):** ALL

TITLE: INFORMATION TECHNOLOGY SECURITY AUDIT

FROM:
Kevin Shapiro, Director of Internal Audit

ACTION: FOR INFORMATION

Purpose

To communicate the findings from the Information Technology (IT) Security Audit.

Report Highlights

- The Office of the Chief Information Officer (OCIO) is responsible for managing the effective delivery of technologies and services to achieve the organization's objectives. The Office is responsible for the engineering, architecting, security, maintenance, implementation and support of city-wide technology and communications infrastructure.
- The Facility Management Department is responsible for managing the physical security controls around the computing facilities in the City Hall and the Joint Operations Centre.
- While OCIO has made significant progress on several initiatives over the past number of years, further improvements will be required to ensure risks related to the vulnerabilities and deficiencies uncovered in the audit are mitigated.
- Management has developed action plans which will mitigate the identified risks and address the recommendations outlined in the report.
- Internal Audit will follow up with management and report on the status of management action plans at a future Audit Committee meeting.

Recommendations

1. That the Internal Audit Report on the audit of Information Technology Security be received.

Background

The Office of the Chief Information Officer (OCIO) is responsible for managing the effective delivery of technologies and services to achieve the organization's objectives. The Office is responsible for the engineering, architecting, security, maintenance, implementation and support of city-wide technology and communications infrastructure. OCIO's vision is "Making Vaughan Better for People in our Digital Age". The Facility Management Department is responsible for managing the physical security controls around the computing facilities in the City Hall and the Joint Operations Centre.

Securing computerized data and information is important for several reasons, but principally as a means of keeping information safe. The importance of computer security depends on how harmful it can be if data or information is lost. The City stores a lot of data, some of it very sensitive, including payment information, staff records, e-mails, citizen information and extensive corporate documents, both finished and those in progress.

In addition to security breaches by outsiders, there is also an increasing risk that data and systems can be compromised by staff inside organizations. As part of their daily responsibilities, staff have access to data and information that those outside of the organization typically do not. Although not a risk unique to computerized information, the ease of availability and accessibility to computerized information may increase the likelihood of a security breach.

The objective of the audit is to evaluate the adequacy and effectiveness of the internal controls, processes and procedures in place to mitigate the business risks associated with the management and administration of IT Security.

This audit was co-sourced. Internal Audit worked with iPSS incorporated (iPSS), who were the successful bidder after a competitive procurement process.

Internal Audit assessed that cyber security awareness programs are implemented and operating effectively.

iPSS assisted Internal Audit in assessing that:

- The City's IT network and systems are secure and physical security controls are implemented and operating effectively, through a penetration testing exercise.
- Effective security controls and configuration changes have been put in place to remediate vulnerabilities discovered during penetration testing previously performed by the City.
- The City's computing environment, processes and documentation are compliant with leading industry framework.

- Technology supporting other critical infrastructure is secure and effective.

Previous Reports/Authority

Not applicable.

Analysis and Options

In fulfilment of *RFQ Q20-276-IT Security Testing and Assessment for the City of Vaughan,* iPSS Inc., performed an external and internal network penetration test and red-team exercise, external wireless assessment, physical security assessment, compliance assessment, critical infrastructure assessment and remediation retesting of past results over the course of January 2021 to March 2021.

The results of these activities were captured in a series of reports issued to Internal Audit and OCIO as outlined below.

- Compliance Assessment Report
- Penetration Test and Red Team Exercise Report
- Critical Infrastructure Assessment Report - Wastewater Management SCADA Infrastructure Report
- Remediation Retests Results Report

iPSS has also prepared an executive summary highlighting their key findings and recommendations. It has been provided to the Audit Committee as Confidential Attachment 1, as the information within deals with matters related to the security of the property of the municipality. Management has developed action plans which will mitigate the identified risks and address the recommendations outlined in the report. The action plans have been provided to the Audit Committee as Confidential Attachment 2, as the information within deals with matters related to the security of the property of the municipality.

In addition to the work performed by iPSS, Internal Audit assessed the City's cyber security awareness programs. While conducting the Information Technology Risk Assessment in 2019 and during the early stages of this audit, it was identified that there were opportunities for improvement to enhance the City's cybersecurity awareness programs. An active security awareness program can greatly reduce the risk of cyber related incidences by addressing the behavioral element of security through education and consistent application of awareness techniques.

OCIO has since implemented a formal cyber security awareness and education program during the course of the audit. With proper security awareness training and clear communication of data and device use policies, users can become the first line of defense against cybersecurity incidents.

Financial Impact

There are no direct economic impacts associated with this report.

Broader Regional Impacts/Considerations

Not applicable.

Conclusion

While OCIO has made significant progress on several initiatives over the past number of years, further improvements will be required to ensure risks related to the City's IT security framework are mitigated.

The audit has identified high-risk vulnerabilities, which if not addressed could result in the compromise of the City's information technology environment. Multiple opportunities for remediation and improvement have been highlighted in the confidential report.

Improving security is an ongoing activity that needs to be well planned based on risk and cost. OCIO is currently engaged in this process. Management has developed action plans which will mitigate the identified risks and address the recommendations outlined in the report.

The audit also identified several processes that can be identified as key strengths. These include:

- Strong use of security awareness efforts through social engineering and phishing campaigns.
- Strong overall cyber security tooling capabilities.
- Strong capabilities in the use of central log management for monitoring and use of analytic tools that are scalable and can be automated.
- Strong possibilities to fully leverage security playbook capabilities from Microsoft Azure to augment current teams existing efforts.
- Strong use of tooling for DNS filtering protections against malware and C2 traffic.
- Automated ports scans are performed.
- Backups are regularly performed, and data recovery capabilities are in place to help protect against potential data loss.
- Good use of local administrator credential management on Windows (LAPS).

- Effective WPA2 Enterprise implementation for corporate wireless.

Internal Audit will follow up with management and report on the status of management action plans at a future Audit Committee meeting.

For more information, please contact: Kevin Shapiro, Director of Internal Audit, ext. 8293

Attachments

1. Confidential Attachment 1 – Overall Executive Summary
2. Confidential Attachment 2 – Management Action Plans

Prepared by

Kevin Shapiro, Director of Internal Audit, ext. 8293
Hemingway Wu, Audit Project Manager, ext. 8350

Approved by

Kevin Shapiro, Director of Internal Audit