REPORT
Meeting Date: 2021-11-18
Audit and Risk Committee

For Information

REPORT TITLE: **Information Technology Security Update**

FROM: Sean Baird, Commissioner of Service Excellence and Innovation

OBJECTIVE

To provide update to Audit and Risk Committee on ongoing Cyber Security improvements as these pertain to third-party security assessment that was conducted in 2019.

REPORT HIGHLIGHTS

- The Region of Peel (Region) continues to educate users on the latest Cyber Security threats and overall security safety.
- The remaining areas that need to be addressed as part of the past security assessment are included in the security workplan.
- The Region delivered active Security Score Cards which will provide ongoing, objective measurement of Cyber Security standards, policies, and processes in use at the Region of Peel.
- Application Portfolio Sustainment (Sate of Good Repair) has been funded and process remediation is underway to address legacy applications.
- Third-party security re-assessment will be completed in 2022.

DISCUSSION

1. Background

This report is an update on the cyber security efforts at the Region. The last update was provided in November 2020 and included the results of the third-party security assessment conducted in 2019.

The 2019 assessment was focused on the evaluation of the current cyber security posture of the organization, validating those previous efforts have been completed effectively, and that risks are been managed to maintain confidentiality, integrity, and availability of the systems and information.

The assessment covered a broad area of technologies, controls, and governance items assessed against the CIS Critical Security Controls framework, industry best practices, and industry experience.

The findings identified areas for improvement and remaining activities were added to an existing workplan to remediate or reduce security risks. These remediation activities are ongoing.

Although many changes were made to how the Region deals with threats, threat actors and risks they pose to our information, the Region must not stop delivering innovative ways to protect corporate and personal information entrusted to the Region for delivering its electronic services.

The Application Portfolio Sustainment process was established and funded last year to reduce and modernize applications and their lifecycles which will help Region to enhance overall application security, increase employee productivity and satisfaction as well as decrease the chance of application outages.

2. 2021 Accomplishments

The highlight of this year's Cyber Security accomplishments was the delivery of COVID-19 response activities. IT resources were redeployed to provide technical skills to support Public Health Frontline workers. As a result, certain Cyber Security remediations such as third-party reassessment had to be delayed to 2022.

In addition, the Region worked tirelessly to achieve several milestones. As part of the Application Portfolio Sustainment program, approximately 90 older server operating systems and applications were removed or replaced. This has allowed IT to reduce overall security risks to its systems and applications by 20 per cent.

The adoption of emerging technologies has allowed for the introduction of new tools to discover a threat within minutes, automate its investigation and having security personnel apply countermeasures almost immediately. This is intended to protect both corporate and external client information from unauthorized access or disclosure.

To help educate employees about the dangers of cyber-attacks, new Cyber Security online modules were introduced through its corporate learning management system. The last two releases have increased corporate participation in corporate security training, but overall, it remained below 50 per cent. In addition, approval was obtained to make the training mandatory for all employees. The Cyber Security training practice will be reviewed to find ways to enhance delivery of its content to more employees using mobile device friendly Cyber Security Awareness Training platform.

Simulated email phishing exercises are also continuing with the next exercise scheduled to be completed in November. The target is for 15 per cent or lower of employees who click the phishing link which would constitute a reduction from 19 per cent achieved during the last email phishing exercise.

In 2021, internal Security Score Cards from Microsoft were added. The Score Cards objectively measure how IT applies industry standards, security configuration policies and processes to help secure information and increase maturity of its Cyber Security Program. This is not a substitute for third-party Cyber Security assessment but will provide IT with actionable items to focus on and address in a timely manner. The Security Score Cards are represented as percentages of compliance and provide dynamic day-to-day view and insights for overall improvements. Since the beginning of 2021, Identity Score (employee centric security protection) has increased from 35 per cent to 76 per cent. Overall security score that covers employee, systems and application increased from 38 per cent to 68 per cent. The overall increases can be attributed to modifications that were completed to background Cyber Security systems, processes, and policies.

3. Workplan Activities

The workplan activities includes the items identified in the security assessment as well other activities that will strengthen security and reduce risks. Some activities have been completed are ongoing or planned.

Status Indicators:

√ Completed

√*Scheduled to be completed by end of year

√ Ongoing

√ Not Started

Activities	**2020**	**2021***	**2022**
Deliver continuous Cyber Security awareness training for the organization	√	√	√
Conducted internal email phishing campaign within the organization	√	√*	√
Modernize Security - Enhance security response using cloud machine learning and security audit triggers	√	√	√
Enhance security of mobile devices (smartphones)	√	√*	
Review and update existing security and technology policy statements	√	√	
Application Portfolio Sustainment program is underway to address the legacy applications by retiring, replacing, or upgrading these applications	√	√	√
Enhance regulatory compliance controls	√	√	
(New) Corporate Information Classification and Protection		√	√
New) Establish Operational Security Score Cards		√	

(New) Enhance capabilities of an existing Cyber Security Training platform to reach more employees.			√
Complete follow up IT security assessment (delayed to 2022)			√

Authored By: Arthur Michalec, Advisor, IT Security