Region of Peel
working with you

REPORT
Meeting Date: 2020-09-17
Audit and Risk Committee

For Information

REPORT TITLE: **Information Technology Security Assessment**

FROM: Sean Baird, Commissioner of Digital and Information Services

OBJECTIVE

To inform the Audit and Risk Committee of the security measures that are currently in place and the results of a third-party security assessment that was conducted in 2019.

REPORT HIGHLIGHTS

- There are controls in place to manage the information technology risks.
- Security standards and best practices are used to provide guidance on controls and existing and emerging threats.
- Third-party security assessment was conducted to validate controls and identify areas of improvement to reduce security risk.
- The Region demonstrated a higher level of security maturity in some key areas.
- The findings from the assessment was good however there are areas that need to be addressed which is included in the security workplan
- Remediation work is underway to address the findings including a State of Good Repair program for addressing legacy applications.

DISCUSSION

1. Background

The Region of Peel network consists of large and complex technologies including best of breed cloud technologies; legacy on premise applications and legislated/mandated applications hosted externally. This creates complexity in the environment and the implementation of security measures to ensure the Confidentiality, Integrity and Availability (CIA) of the information entrusted to the Region.

The work of protection is never complete as new threats are introduced daily and threat actors are always one step ahead. This requires constant changes to ensure that vulnerabilities are addressed and that the defenses in place continue to provide the intended mitigation.

To protect the environment, it is prudent to follow well established processes that are most effective in stopping known attacks. These processes are developed in the form of standards and best practices and are a set of well-defined steps to be followed to minimize the security risk in the environment. It is important to note that while the risks related to system or information compromise can be reduced, they cannot be completely eliminated.

Some of the standards and best practices in use are ISO 27000 series, NIST 800 series, Centre for Internet Security's (CIS) 20 Critical Controls and Cloud Security Alliance (CSA) Cloud Controls Matrix.

Along with the standards and best practices, third party security assessments are also conducted to review the environment for the appropriate levels of controls; identify vulnerabilities and areas for improvements. The findings are used as input to the security workplan. Assessments are usually conducted every two to three years to allow time between the assessments for remediation efforts.

2. Current Security Controls

Security controls are safeguards or countermeasures that are implemented to avoid, detect, counteract, or minimize security risks to the information, computer systems, or other assets. The Region of Peel uses a layered approach to security which means that multiple controls are implemented to reduce the risks.

The following controls are currently in place:

Control	Description
Asset Controls	Utilize industry best practices and standards-based system hardening processes, performing threat and privacy assessments based on the level of sensitivity of the information being stored and recommending appropriate remediations to lower the risk to information breaches.
Identity and Access Controls	Two Identity Management platforms are in use to verify user entities before granting them the right level of access to on premise and cloud-based systems and information. Two Factor authentication is also in place as a second layer of security before being granted access.
Endpoint Protection	A suite of products to protect the endpoint devices (computers, laptops etc.) against viruses, malware, drive-by downloads, and other threats that may affect devices or services. The solution applies to both client and servers.
Vulnerability and Advanced Threat Protection	A tool that scans external and internally hosted systems for any vulnerabilities/risks in operating systems, applications, certificates, and the other components.
Security Patch Management	Utilize a tool to deploy operating systems security patches and maintenance patches to affected computers and servers.
Content Filtering	Email and Web content filtering solutions provide protection against delivery of harmful payload through web and emails for mobile and non-mobile platforms i.e. spam emails, malware, objectionable, inappropriate, or illegal content.
Regulatory Controls	A set of tools used to protect sensitive information on laptops, tablets, and servers by encrypting the data.
Virtual Private Network (VPN)	Used to establish a secure remote connection to Region of Peel network resources or devices. It is used by

	employees with a Region of Peel provided device (laptop, tablet, smartphone) or vendors or other third parties.
Firewalls	There are two corporate firewalls in place (one in each Data Centre) used to monitor incoming and outgoing network traffic from the internet and decides whether to allow or block specific traffic based on a defined set of security rules.
. Public Key Infrastructure (PKI)	Provides certificate to all Region of Peel computers and mobile devices to identify as Region devices to provide access to resources.

These controls are reviewed regularly to ensure they are still relevant and additional controls added to address new threats.

3. Security Assessment

As noted above, a good security practice is to compliment the security controls with a security assessment conducted by a third-party assessor. This validates that the controls in place are sufficient, identifies gaps and provides recommendations on how to remediate. A third-party Information Technology Security Assessment was completed between January and April of 2019. The assessment was focused on the evaluation of the current cyber security posture of the organization, validating that previous efforts have been completed effectively, and that risks are being 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 support the development of a workplan to remediate and reduce security risks.

4. Findings

The results from the security assessment validated that protecting the technology environment is never complete and no one is 100 per cent risk free – there is always a need to do more. It did indicate that the Region of Peel demonstrated a higher level of maturity in some key areas in Inventory and Control of Software Assets, Continuous Vulnerability Management as well as Wireless Access Control. Areas identified for improvement include Controlled Access Based on the Need to Know, Limitation and Control of Network Ports, Protocols, and Services, as well as Incident Response and Management.

Multiple critical vulnerabilities were discovered during the internal and external network penetration testing phase of the project. This testing was performed to attempt to exploit identified vulnerabilities to gain access to network devices, applications, accounts, and information in a manner other than intended.

Multiple issues related to missing patches, lack of system build and hardening standards, legacy operating systems and applications as well as outdated software components with vulnerabilities were also identified.

Technical Deficiencies such as weak build standards, lack of centralized log and event management systems, lack of formal incident response program and missing policy statements were also identified.

The workplan activities for the next several years include activities to address the above findings. While remediation of some findings is easier to attain, others such as the legacy applications and outdated software could take several years. This is dependent on the size and function of the application. In some cases, the application meets the need of the program areas and they would like to continue its use, however the inherent risks associated with these applications will force upgrades or replacement. As such a State of Good Repair (SOGR) program has been established to address legacy applications.

A reassessment is planned for 2021 to validate the issues that have been resolved and identify any new issues.

5. 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

√ Ongoing

√ Not Started

Activities	2019	2020	2021
Deliver continuous Cyber Security awareness training for the organization	√	√	√
Conducted internal email phishing campaign within the organization		√	√
Introduced three new technology and security policy statements	√	√	
Implemented Identity Access technology system policies to protect corporate information against unauthorized access		√	
Developed security incident response plan		√	
Implemented next generation endpoint protection solution	√	√	
Implemented Security Incident and Event Management (SIEM) solution to centralize logging of security events	√		

Automated corporate systems build processes	√	√	
Modernized Cyber Security tools to leverage cloud computing, auditing, and analytics	√	√	√
Enhance security of mobile devices (smartphones)		√	√
Review and update existing security and technology policy statements		√	√
SOGR program is underway to address the legacy applications by retiring, replacing, or upgrading the applications	√	√	√
Remediate Technical deficiencies such as missing applications updates	√	√	√
Operationalize Security Incident Response Plan		√	
Enhance regulatory compliance controls		√	√
Improve lower scored areas to increase the security maturity assessment scores	√	√	√
Complete follow up IT security assessment			√

For further information regarding this report, please contact Steve Van de Ven, Director IT Operations, (416) 419-1324, steve.vandeven@peelregion.ca.

Authored By: Janette Myers-Sinclair, Manager IT Service Delivery

Reviewed and/or approved in workflow by:

Department Commissioner and Division Director.

Final approval is by the Chief Administrative Officer.

N. Polsinelli, Interim Chief Administrative Officer