CITY OF VANCOUVER

Internal Audit Summary Report

July 27, 2016

Cyber Security Audit

Background

Cyber Security is consistently identified as one of the top risks in today's organizations as security breaches can have devastating effects on the organization. As cyber criminals have become more sophisticated and attacks are much more prevalent, the potential for serious financial, operational and reputational damage of a cyber-attack is a critical risk that must be managed.

Threat Landscape:

Threats can originate externally, from those seeking financial gain, to make a political point or demonstrate their hacking prowess. Threats can also come from internal sources such as employees or other parties that may have legitimate access to systems.

Attacks are no longer restricted to a company's perimeter defense systems such as firewalls and other intrusion detection systems. Rather, cyber criminals are capable of detecting and exploiting vulnerabilities in the many layers of a company's networks.

Cyber Security's goal

Cyber Security's goal is to protect information and information systems. Cyber security controls include:

- Personnel security
- Physical and environmental security
- Account and password management
- Confidentiality of sensitive data
- Business continuity management
- Security awareness and education
- Incident management
- Access controls
- Asset management
- Change management
- Compliance
- Policy/Privacy
- Systems and data protection
- Insurance

Cyber Security Management at the City

Cyber Security at the City is managed through applications, device management and data management. The IT Security group reports to Finance, Risk and Business Planning and the IT

Security Operations group reports to Human Resources, Digital Strategy & IT. The IT Security group assists with HR related incidents, serves an advisory/governance role, is responsible for IT security related policy development and approves firewall rule creation and modification requests. The IT Security Operations group deals with technical security incidents and IT security incident monitoring, vulnerability scanning, penetration testing and risk assessments.

The IT landscape at the City is set to change drastically over the coming years with initiatives in cloud computing, mobile workforce and engaging citizens through online, mobile and social media channels.

Scope

The objectives of the audit were to assess the current state of cyber security at the City of Vancouver and ensure data is protected by having a proper process and framework in place that meet established standards and procedures. The audit was initiated for the purpose of determining:

- That adequate controls are in place to ensure the integrity of information stored on computer systems;
- That confidentiality of sensitive data is preserved;
- That the continued availability of information systems is ensured; and
- Conformity to applicable laws, regulations and standards.

Conclusion

The audit identified some areas for improvements and discussed them with appropriate management. Work is underway to address them, including:

- Strengthening IT Security governance;
- Establishing an effective cyber security user education and awareness program; and
- Completing a full network penetration test.