CITY OF VANCOUVER
INTERNAL AUDIT REPORT
Cybersecurity

Distribution:	
Audit Committee, KPMG	Leo de Sousa – Director, Enterprise Technology Carolina de Moura – Chief Risk Officer David Polano – Manager, Cybersecurity Josh Scherban – Manager, Cyber Risk James Andrews – Manager, Human Resources Systems and Analytics Sue Goddard – Manager, Human Resources Learning and Strategic Initiatives

EXECUTIVE SUMMARY

January 7, 2021

The objective of the audit was to assess the overall state of the City's cybersecurity program as managed by Technology Services. This did not include the cybersecurity programs at the Vancouver Public Library or the Vancouver Police Department.

In 2020, the Cybersecurity team made progress on improving the City's overall cybersecurity posture, despite additional security challenges brought about by COVID-19 response efforts. Processes for monitoring and responding to cyber threats and incidents have been strengthened. Key cybersecurity functions, such as security patching processes, identified by the NIST Cybersecurity Framework are in place.

However, continued efforts are required to ensure reasonable maturity in all cybersecurity functions as outlined in this report. During the course of this audit, Management had taken a proactive approach in addressing the findings identified. The more significant findings and recommendations include:

E.1 Develop a 3-year roadmap for the cybersecurity program

The Cybersecurity team has plans to implement further improvements in various security related areas in 2021 and onwards to further maturity. A documented roadmap that outlines the work plan and goals for key cybersecurity initiatives for the next 3 years would assist with coordination, prioritizing work, tracking initiatives, and reporting on progress.

E.2 Ensure timely user access removal for leaving employees

A coordinated off-boarding process is important to ensuring that user access is removed for leaving employees to prevent misuse from unauthorized access. However, user access removal is not effective due to a decentralized process on notification of leaving employees. Technology Services and Human Resources have previously identified this risk. Planning is in progress for developing a holistic solution for employee management, including off-boarding. In the meantime, additional controls should be implemented such as periodic reviews, increasing the frequency of the account deactivation process, and improving leaves notification by managers.

E.3 Implement a City-wide cybersecurity awareness program

All employees who use City technologies have a role in ensuring cybersecurity. However, a comprehensive cybersecurity awareness training program is not in place. Technology Services and Risk Management are working on implementing the Cyber Security Awareness Strategy. This strategy should be implemented with training for general, privileged and executive users.

Tony Hui, CPA, CA, CRMA
Chief of Internal Audit

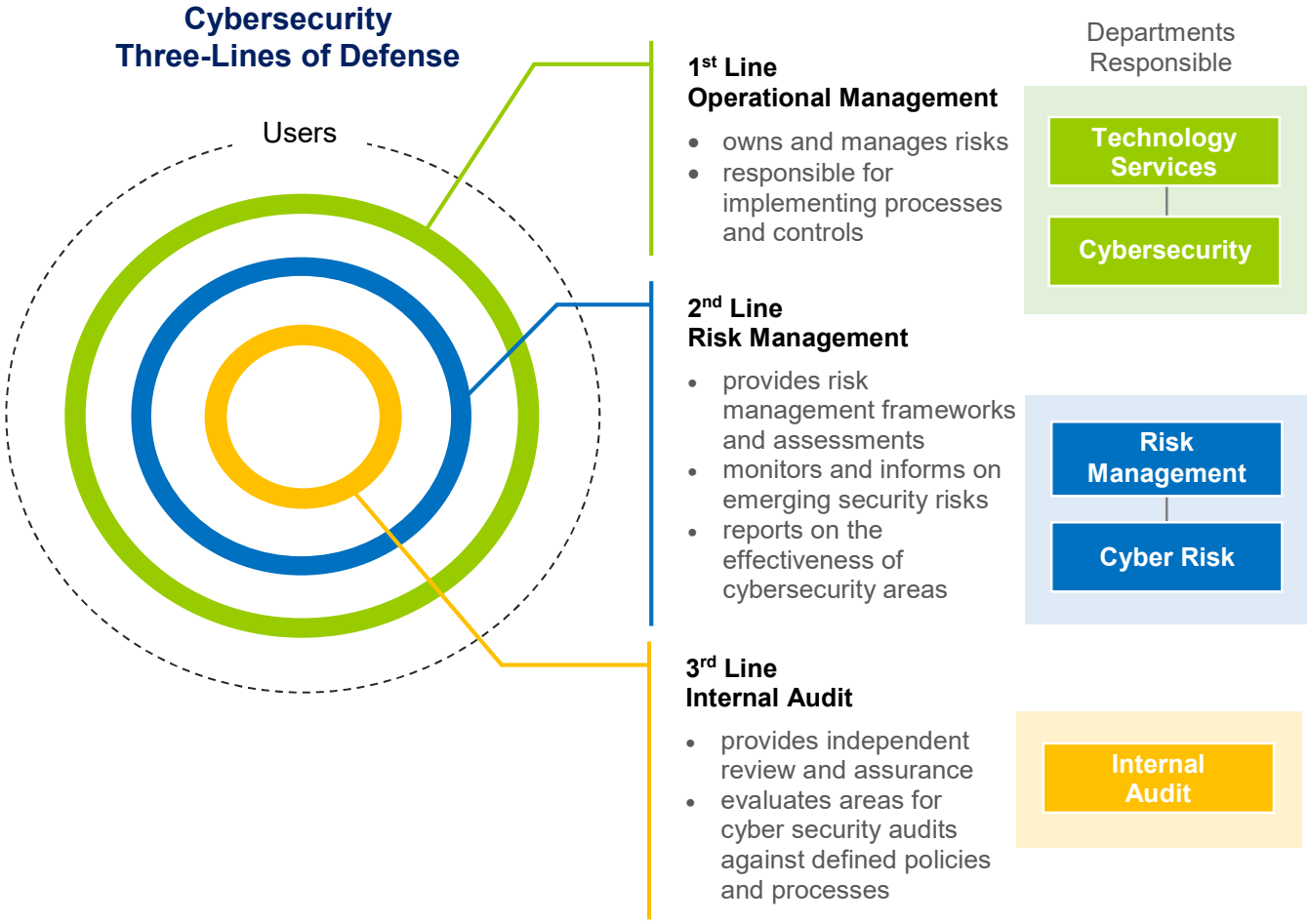
Jenny Lau, CIA, CISA
Senior Internal Audit

A. BACKGROUND

Cybersecurity is the protection of information and technology assets against cyber threats. The City faces increased sophistication of threat actors and increased appetite for digitalization of services by the public it serves. Robust cybersecurity processes are needed to enable the City to deliver services securely and confidently.

Three-Lines of Defense Model

All employees who use City technologies have a role in ensuring cybersecurity. More formally, the City has adopted the three-lines of defense model between Technology Services, Risk Management and Internal Audit for implementing cybersecurity.



Cybersecurity in 2020

In 2020, Technology Services was critical in ensuring the continuation of City operations through a number of COVID-19 response initiatives, including the rapid support of remote work from home. These response efforts introduced a number of new security challenges that were addressed by the Cybersecurity team. Also, the Cybersecurity team on-boarded three new team members in 2020 to its complement of six.

In addition, Technology Services implemented new processes and tools to improve the City's overall cybersecurity posture. Major initiatives included:

- enhancements to threat intelligence and event monitoring tools,
- test of the updated cybersecurity incident response plan, and
- progress on improving overall data and systems redundancy and resiliency.

Going-forward, there are plans to continue to implement processes and tools to further the maturity of the cybersecurity program.

B. SCOPE

The objective of the audit was to provide reasonable independent assurance to assess the overall state of the City's cybersecurity program as managed by Technology Services and supported by Risk Management. The scope of this audit did not include the Vancouver Public Library or the Vancouver Police Department that manage cybersecurity within their respective IT departments.

Our work included interviews with members of the Technology Services and Risk Management teams supported by procedures that included:

- review of policy, planning and procedure documents such as Application Branch Standards, SoP's for security reviews, Enterprise Architecture Requirements and Security Operations Risk Assessment procedures;
- observation of processes through screen demos and walk-throughs of tools such as DevOps testing tools and SIEM applications; and
- sampling of leaving employees to confirm user access.

The audit was not designed to detect fraud. Accordingly, there should be no such reliance.

C. CONCLUSION

Opportunities exist to further develop and mature the cybersecurity program. In 2020, the Cybersecurity team made progress on improving the City's overall cybersecurity posture, despite additional security challenges brought about by COVID-19 response efforts. Processes for monitoring and responding to cyber threats and incidents have been strengthened. Key cybersecurity functions identified by the NIST Cybersecurity Framework are in place. However, continued efforts are required to ensure reasonable maturity in all cybersecurity functions as outlined in this report.

The findings and recommendations identified have been discussed with Management and their responses were incorporated in this report. We thank the Technology Services, Risk Management, and Human Resources teams for their assistance with this audit.

D. RISK ANALYSIS

The potential risks considered if controls were not in place included:

- disruption to systems that support critical City services;
- financial losses from data loss, cyberattack schemes or recovery efforts ;
- reputational harm from loss of trust to the integrity of City systems; and
- regulatory penalties from breach of personal or financial information.

E. AUDIT ISSUES, RECOMMENDATIONS AND MANAGEMENT RESPONSES

E.1 Develop a 3-year roadmap for the cybersecurity program

Progress in 2020
In 2020, the Cybersecurity team implemented a number of tools and processes to improve the City's overall cybersecurity posture. There are plans to introduce further improvements to various areas in 2021 and onwards. Some areas identified include security awareness training, data loss prevention and security, defining cybersecurity KPI's, further improving incident response preparation, and further expansion on use of Splunk security information and event management.

Develop a 3-year roadmap
Given the number of priorities, a documented roadmap that outlines the work plan and goals for key cybersecurity initiatives for the next 3 years would assist with prioritizing work. A roadmap would improve coordination, reporting on progress, and confirming alignment with the City's overall technology strategy for supporting service delivery.

Short-term priority should be allocated to risk areas where maturity is low or require attention. These areas include security awareness training and identity and access management.

Consider formalized framework adoption
In addition, while key functions defined by the NIST (National Institute of Standards and Technology) Cybersecurity Framework are in place, formal adoption a cybersecurity framework, such as the one by NIST, could also be considered. Refer to Appendix 1 for the NIST Cybersecurity Framework.

Recommendation:

E.1.1 The Manager, Cybersecurity should develop a 3-year cybersecurity roadmap that outlines the work plan for key initiatives that would further mature the City's cybersecurity program. The roadmap should also include goals for desired maturity in various cybersecurity areas. This should be completed by June 30, 2021.

Management Response:

Please check one:	Please check one:
☑ Agree with the findings	☑ Agree with the recommendations
☐ Disagree with the findings	☐ Disagree with the recommendations

Management Action Plan:

We agree with finding E.1.1 and will complete a 3-year cybersecurity roadmap by June 30, 2021. Consideration will be given to the NIST Cybersecurity Framework to help shape the roadmap.

E.2 Ensure timely user access removal for leaving employees

A coordinated off-boarding process ensures that user access to City systems and data is removed in a timely manner to prevent unauthorized misuse. However, user account deactivation is not effective due to a decentralized process on notification of leaving employees. Although managers across the City are responsible for notifying Technology Services of leaving employees, this is not done consistently.

To compensate for this, Technology Services relies on a leaving employees report to deactivate user accounts. However, the following were identified:

- User deactivation process is not timely
  For most cases of leaving employees, where notifications were not submitted by departments, Technology Services relies on a leaving employees report to deactivate users. This report is generated weekly. Consequently, leaving employees could have systems access for up to a week after their departure.

- Incomplete report of leaving employees
  The leaving employees report does not capture all employment leaving situations. For example, the report does not capture employees entering retirement and finishing out their vacation banks, or capture situations where the employee's termination date required backdating for payroll purposes.

As a result, 33 employees who left the City between January and November 2020 were identified with active user accounts. Upon identification, Technology Services deactivated the 33 user accounts and no further security issues were identified. In addition, Technology Services began identifying changes to ensure completeness of the leaving employees report.

The security risk of inadequate access and identity management related to employee termination was previously identified by Technology Services and Human Resources. To address this, planning is underway with Human Resources to develop a holistic solution for employee management, including off-boarding notifications. However, to address this risk in the short-term, additional measures should be implemented.

Recommendations:

E.2.1 The Director, Enterprise Technologies should implement a process for periodic review of users to ensure that employees who have left the City do not have systems access. The review should be performed at least every six months. This should be completed by June 30, 2021.

E.2.2 The Director, Enterprise Technologies should review the frequency of the weekly user deactivation process to determine whether user deactivations, in cases where notifications are not submitted by departments, could occur more frequently. This should be completed by June 30, 2021.

Management Response:

Please check one:

☑ Agree with the findings

☐ Disagree with the findings

Please check one:

☑ Agree with the recommendations

☐ Disagree with the recommendations

Management Action Plan:

We agree with the findings and recommendations E.2.1 and E.2.2. The implementation of these recommendations will help reduce the risk in the short-term. However, even if both of these recommendations are fully implemented, some user accounts may still not be disabled in a timely manner. To properly address this risk, an appropriate identity and access management solution is required that automates the onboarding and off boarding of staff/contracts based on established HR triggers.

E.2.3 The Manager, Human Resources Systems and Analytics, in working with the Manager, Compensation and Benefits, should implement methods for reminding managers across the City on the timely use of the eSAF for employee terminations and the completion of the tasks on the "Termination of Employment Checklist", that includes notification to Technology Services to deactivate user accounts. This should be completed by June 30, 2021.

Management Response:

Please check one:	Please check one:
☑ Agree with the findings	☑ Agree with the recommendations
☐ Disagree with the findings	☐ Disagree with the recommendations

Management Action Plan:

An Aha! request has been submitted for TS to add a statement to the bottom of termination ESAFs directing Managers to complete the ESAF in as soon as possible and refers them to the Termination Checklist to ensure that accesses are deactivated for the terminated employee.

The HR leadership will be asked if there is an opportunity to update all City Managers with the same message using the appropriate communication channel.

E.3 Implement a City-wide cybersecurity awareness program

All technology users play a role in security

All employees who use City technologies have a role in ensuring cybersecurity. Improving the cybersecurity practices and digital hygiene of all users helps the City reduce its risk of cybersecurity incidents. However, a comprehensive cybersecurity awareness training program is currently not in place.

Implement the Cyber Security Awareness Strategy

Technology Services and Risk Management are working on implementing the Cyber Security Awareness Strategy that outlines a plan for enhancing cybersecurity competencies across all levels of the City including privileged users and staff in enhanced positions. The goal is to implement City-wide cybersecurity awareness training in 2021.

In the interim, channels such as Citywire Spotlight articles and the cybersecurity awareness month campaign have been used to educate and remind users of good security practices. Also, targeted training was provided to specific groups in roles deemed susceptible to attacks leveraging social engineering techniques.

Recommendations:

E.3.1 The Manager, Cybersecurity should ensure that cybersecurity awareness training is implemented and rolled-out. In addition, targeted training of privileged and executive users should also be included where risk of vulnerability is deemed higher. This should be completed by September 30, 2021.

Management Response:

Please check one:	Please check one:
☑ Agree with the findings	☑ Agree with the recommendations
☐ Disagree with the findings	☐ Disagree with the recommendations

Management Action Plan:

We agree with finding E.3.1 and will deploy a general Cybersecurity Awareness program leveraging the City's Learning Management System by September 30, 2021. Where appropriate the Cybersecurity Awareness program will provided targeted training to specific high-risk groups.

E.3.2 The Manager, Learning and Strategic Initiatives, in working with Manager, Cybersecurity, should ensure that cybersecurity awareness training is required to be taken on a regular, periodic basis by staff who use City technologies. Cybersecurity awareness training should also be incorporated into the new employee onboarding process for staff who use City technologies. This should be completed by March 31, 2022.

Management Response:

Please check one:	Please check one:
☑ Agree with the findings	☑ Agree with the recommendations
☐ Disagree with the findings	☐ Disagree with the recommendations

Management Action Plan:

Agree with the recommendation. HR will work with the Manager, Cybersecurity to implement cybersecurity awareness training into the LMS as part of regular, periodic training and have the training incorporated into the new employee onboarding process.

E.4 Develop a resource plan to retain cybersecurity professionals

The challenges of retaining qualified cybersecurity professionals is an industry-wide issue. To recruit and retain cybersecurity expertise, organizations are having to provide competitive compensation and other incentives.

In 2020, the City's Cybersecurity team had a turnover of 60%. Prior to 2020, there had also been challenges with retaining a full team compliment. The cost of employee turnover not only includes the resources spent on recruiting, onboarding, and training, but also includes the loss of organizational knowledge and continuity to build out longer-term programs.

An alternate resourcing plan could be explored to assist with retaining cybersecurity professionals. The plan may include reviewing the team's structure to include the support of external services firms to provide continuity of knowledge and enable flexibility in allocating job tasks and duties within the team.

Recommendation:

E.4.1 The Manager, Cybersecurity should develop a resource plan for the Cybersecurity team to address the challenges in retaining cybersecurity professionals. The plan may

include a review of the team's structure to explore alternative models and a review of incentives and compensation schemes for assisting with retention. This should be completed by June 30, 2021.

Management Response:

Please check one:	Please check one:
☑ Agree with the findings	☑ Agree with the recommendations
☐ Disagree with the findings	☐ Disagree with the recommendations

Management Action Plan:

We agree with finding E.4.1 and will develop a resource plan for the Cybersecurity team by June 30, 2021.

E.5 Determine the role of VEMA in the event of a major cybersecurity incident

Technology Services updated the Cybersecurity Incident Response Plan and conducted a tabletop exercise in 2020. Technology Services intends to continue to strengthen incident response in 2021 through the creation of incident specific playbooks and performing additional tabletop exercises.

As incident response processes mature, Technology Services should consider the role of the Vancouver Emergency Management Agency (VEMA) in the event of a major cybersecurity incident that affects the ability of the City to deliver core services for a significant period of time.

VEMA is the City's emergency management function responsible for the City's Emergency Program involving both internal departments and external agencies.

Recommendation:

E.5.1 The Director, Enterprise Technologies should work with the Vancouver Emergency Management Agency (VEMA) and Risk Management to determine the criteria for when major cybersecurity incidents would trigger the activation of the City's Emergency Operations Center to enable City-wide coordination, cohesive communication and use of emergency infrastructure and processes. This should be completed by June 30, 2021.

Management Response:

Please check one:	Please check one:
☑ Agree with the findings	☑ Agree with the recommendations
☐ Disagree with the findings	☐ Disagree with the recommendations

Management Action Plan:

We agree with finding E.5.1 and will work with VEMA to define the criteria when a major cybersecurity incident will trigger the activation of the City's Emergency Operations Center.

F. OTHER OBSERVATIONS

F.1 Cyber Risk team on assisting with cybersecurity processes

Given the resource challenges in Technology Services brought about by COVID-19 response efforts in 2020, the Cyber Risk team provided support to the cybersecurity program by assisting with the development of key areas including:

- drafting of the cybersecurity awareness training strategy;
- presenting to the Risk Management Committee on a ransomware scenario; and
- involvement with the updated cybersecurity incident response plan and tabletop exercise.

In the design of the three-lines of defense model for cybersecurity, Cyber Risk provides the second line of defense that has no operational responsibilities and "*is the independent control function (e.g., IT risk, IT compliance) that oversees risk and monitors the first-line-of-defense controls*." [1] However, given the circumstances and risk of delay in the two areas that required attention, the Cyber Risk and the Cybersecurity teams worked together in progressing the two initiatives.

Going-forward, the Cyber Risk team should continue to evaluate and determine whether involvement in design or implementation work could impact the independence and objectivity needed for risk assessment activities.

[1] ISACA, Roles of Three Lines of Defense for Information Security and Governance: Journal 2018, Volume 4

APPENDIX A

NIST Cybersecurity Framework

The NIST (National Institute of Standards and Technology) Cybersecurity Framework in the table below is a set of voluntary standards, guidelines and best practices for managing cybersecurity risk.

Category
Identify (ID)
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.
Protect (PR)
Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.
Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.
Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
Detect (DE)
Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.
Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.

Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.
Respond (RS)
Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.
Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).
Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.
Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.
Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.
Recover (RC)
Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.
Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.
Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).