12.

STAFF REPORT
ACTION REQUIRED

Information Security Policy and Annual Report on IT Security

Date:	December 6, 2021
To:	Toronto Public Library Board
From:	City Librarian

SUMMARY

The purpose of this report is to seek Toronto Public Library Board approval of the *Information Security Policy*, to receive the first annual information report on IT Security, and to direct TPL to participate in the City of Toronto's Cybersecurity Confirmation Program, as per a motion at City Council on November 9, 2021.

The Toronto Public Library (TPL) is committed to achieving a safe and secure IT environment, including a targeted level of protection from internal and external cyber security threats.

TPL has developed for approval an *Information Security Policy* to enable resilient business operations through the protection of staff, suppliers, and customers by maintaining the confidentiality, availability, integrity, and security of TPL's information assets. As per TPL's *Information Security Policy*, an annual report to the Board will be provided on IT Security. The report will outline TPL's efforts in the protection of its data and information assets to ensure business continuity.

RECOMMENDATIONS

The City Librarian recommends that the Toronto Public Library Board:

1. approves the *Information Security Policy*.
2. receives for information the annual report on IT Security.
3. directs TPL to participate in the City of Toronto's Cybersecurity Confirmation Program.

FINANCIAL IMPACT

This report has no financial impact beyond what has been approved in the current year's operating and capital budgets.

The Director, Finance & Treasurer has reviewed this financial impact statement and agrees with it.

ALIGNMENT WITH STRATEGIC PLAN

To enable TPL's Strategic Plan 2020 – 2024, a safe and secure IT environment is essential for both staff and customers. Consequently, the Digital Strategy 2020 – 2024 includes a priority to "adopt a modern security approach to improve cybersecurity and TPL's overall security position".

EQUITY IMPACT STATEMENT

The IT Security, Risk & Governance Program will enable equitable access to technology in a secure manner that protects the privacy and confidentiality of customers and staff. The maturity of TPL's security posture will promote confidence that TPL protects people's identities and activities to participate in the digital world.

DECISION HISTORY

At its October 29 and 30, 2019 meeting, City Council receive one report from the Auditor General on Cyber Safety: A Robust Cybersecurity Program Needed to Mitigate Current and Emerging Threats: Auditor General's Report in Item 2019.AU4.1.

At its meeting on January 25, 2021, the TPL Board approved the Digital Strategy 2020-2024. As identified in the digital strategy action plan 2021, there is a focus on IT Security Advancement.

At its October 25, 2021 meeting, the TPL Board received an update to the Risk Register. IT Security risks are included in this report.

At its April 7 and 8, 2021 meeting, City Council received a report from the Auditor General on Cybersecurity Incidents at the City and its Agencies and Corporations: Integrated Incident Response Plan is Needed: Auditor General's Report in Item 2021.AU8.9

At its meeting on November 9, 2021, City Council made a motion requesting that the Library Board direct TPL to participate in the Cybersecurity Confirmation Program*:* *AU10.4 Auditor General's Cybersecurity Review: Toronto Fire Services Critical System Review.*

ISSUE BACKGROUND

Information Security Policy

An *Information Security Policy* is required to maintain the confidentiality, availability, integrity, and security of the Library's information assets, and enable the Library to operate securely and meet its digital service delivery commitments. The Policy will ensure the provision of reasonable safeguards against accidental or unlawful destruction, loss, alteration or unauthorized disclosure or access to Library data. It will also ensure the application of security frameworks, standards, protective and detective practices and controls to predict, identify and address threats to information security.

Annual IT Security Report

As per the *Information Security Policy,* there will be a report to the Board on a regular basis regarding information security risk and major cyber security incidents. This is the first annual report on IT Security.

City of Toronto Cybersecurity Confirmation Program

A motion at City Council on November 9, 2021*: AU10.4 Auditor General's Cybersecurity Review: Toronto Fire Services Critical System Review* requested the Library Board to direct TPL staff to participate in the City of Toronto's Cybersecurity Confirmation Program. As part of this program, TPL's senior ITS managers would work in consultation with the City of Toronto's Chief Information Security Officer to develop a confirmation program which would identify and report out on rates of compliance, remediation plans and strategies to reduce risk and ensure corporate compliance. The first report would be provided in Q1/2022 and biannually thereafter.

If the Board recommends that TPL participate in the City's cyber security confirmation program, TPL staff will complete the confidential Confirmation Form which will report on the status of key cyber controls at TPL, and return it to the Office of the CISO no later than January 31st, 2022.

COMMENTS

Information Security Policy

The *Information Security Policy* has the follow guiding principles:

- align with the City of Toronto Cyber Security policy;
- use a common industry standards-based approach for enterprise security: National Institute of Standards and Technology (NIST) Cyber Security Framework; and
- align to TPL's enterprise risk management policy.

The *Information Security Policy* formalizes TPL's executive commitment to information security and creates the authority for governance with CIO Office. The Policy also defines a core set of controls, establishes roles and accountabilities, and provides direction on compliance and exceptions.

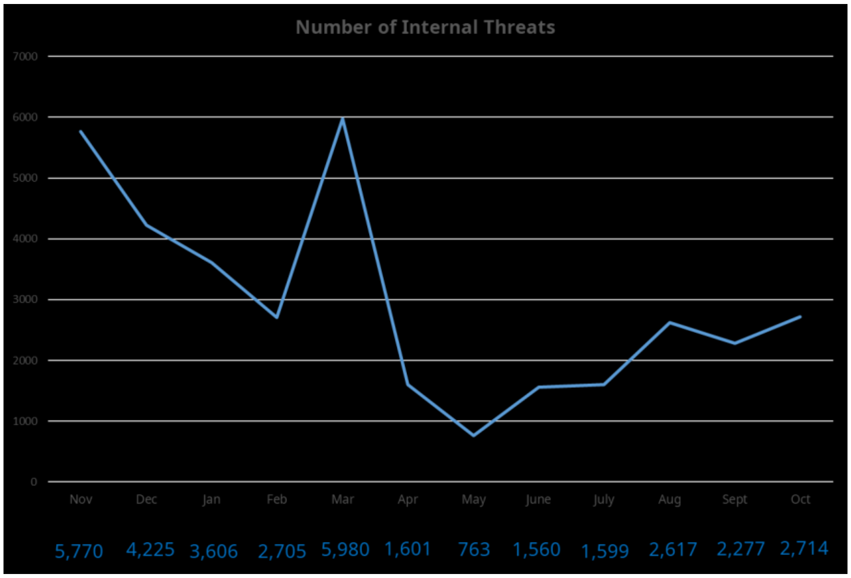
Annual IT Security Report

As a public sector organization, TPL is among the top five organizations targeted for cyber security attacks. A 2021 Data Breach Investigations Report ranked public administration #2 and education #5 for reported security breaches[1]. Despite this, TPL has had no major cyber security incidents since it began reporting on its IT Security Posture in September 2020.

Internal security threats

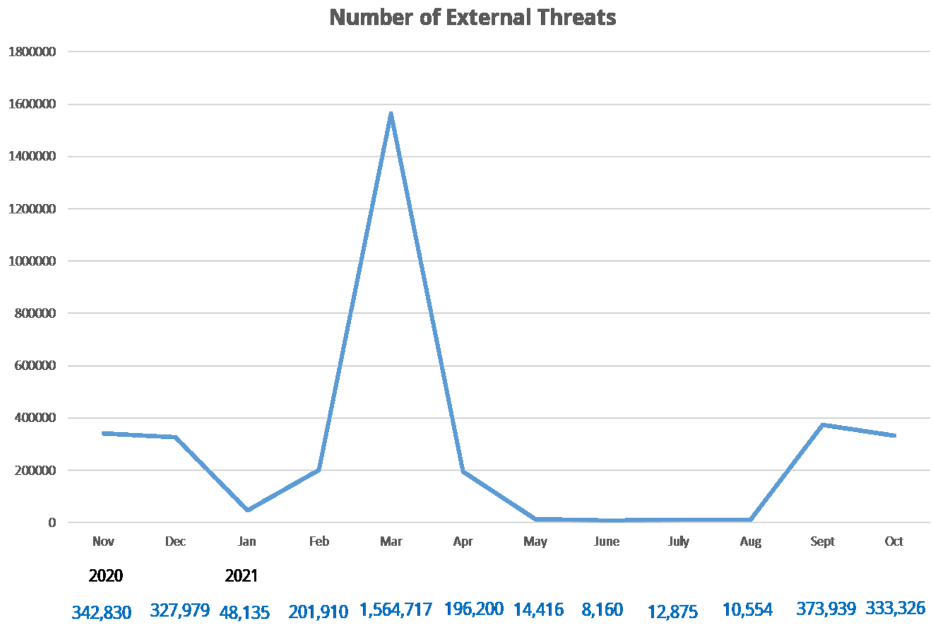
Internal security threats are threats that originate from inside TPL's network. Currently, internal threat reporting is focused on malware. In 2021, the number of internal threats detected correlated to the usage of TPL's public computers. For example, during the stay-at-home lockdown in April, the number of threats decreased significantly, and threats gradually increased as services were reinstated.

[1] 2021 DBIR Master's Guide: https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/.



External security threats

External threats originate outside of the TPL network. During 2021, the number of detected network threats were correlated to overall network activity between the branches.



In all cases where internal and external threats were detected, there were no major cybersecurity incidents. The majority of investigated incidents were phishing attacks or privileged misuse of email.

TPL's IT Security, Risk and Governance Program

In 2020, Gartner performed an independent third party assessment that assessed TPL to be at low maturity in its IT security governance, policies, practices, and security controls. Another third party assessment was performed by Public Safety Canada under the Regional Resiliency Assessment Program. The engagement covered TPL's data centre and overall business resiliency. The results as benchmarked against comparable organizations ranked TPL slightly below the average in resiliency.

As a result of these assessments, a priority was established in TPL's Digital Strategy 2020-2024 to "adopt a modern security approach to improve cybersecurity and TPL's overall security position." Two new roles were hired: Manager, IT Security & Enterprise Architecture (Fall 2020) and IT Security Expert (Spring 2021).

In 2021, an IT Security, Risk & Governance Program was implemented to achieve a safe and secure IT environment, including a targeted level of protection from internal and external cyber security threats. TPL has adopted the National Institute of Standards and Technology (NIST) Cyber Security Framework and risk-based approach.

TPL reports IT risks as part of its Enterprise Risk Management Program, and these risks were presented at the June 17, 2019, September 21, 2020, and October 25, 2021 Board meetings. A number of initiatives are underway to address the risks identified.

To mitigate threats targeted at acquiring identities and passwords, including brute force password guessing, phishing, etc. TPL has created an annual staff cybersecurity awareness program. TPL is also focused on improving identity and access management controls – for example, improved password controls, multi-factor authentication assessment, resetting privileged passwords, etc.; and creating data security standards.

In addition, TPL is enhancing its third party monitoring capabilities by including detection of Internet-based attacks. Currently, TPL uses an Intrusion Detection System to monitor network traffic from the Internet and inspect and report on branch network connections. TPL is also formalizing its cybersecurity incident response and recovery processes.

At the request of the City of Toronto, TPL completed the Information Security Forum assessment for December 1, 2021. TPL will continue to work with the City of Toronto to incorporate recommendations to its IT Security Advancement action plan.

As part of TPL's ongoing cyber security governance, TPL Directors receive quarterly reports on the Library's IT Security Posture and Risks.

CONCLUSION

TPL's IT Security, Governance & Risk Program is based on leading practices to ensure a safe and secure IT environment. By maintaining and improving policy, practices and technology, the risk of internal and external cyber security threats are minimized. The Program is key to achieve the following objectives:

- ensure the protection of TPL's data and information assets;
- establish controls for protecting TPL's information and information systems against theft, abuse, and other forms of harm or loss;
- enable the requirements for confidentiality, privacy, integrity, and availability for TPL's employees, contractors, vendors, and other users;
- ensure business continuity, including the recovery of data and operational capabilities in the event of a security breach;
- motivate administrators and employees to maintain the responsibility for, ownership of, and knowledge about information security;
- ensure that external service providers are made aware of, and comply with, TPL's information security needs and requirements and continuously assess whether they maintain an acceptable security posture;
- balance the need for the above with the investment and policy constraints required to achieve an appropriate level of protection while maintaining business agility; and
- ensure compliance with all applicable laws, regulations, and TPL's policies, controls, standards, and guidelines.

CONTACT

Angela Copeland; Director, Digital Strategy & CIO; 416-393-7104;
acopeland@tpl.ca

Frank Kim, Manager; IT Security & Enterprise Architecture; 416-395-5816;
fkim@tpl.ca

SIGNATURE

____

Vickery Bowles
City Librarian

ATTACHMENTS

Attachment 1:	Information Security Policy

Attachment 1

INFORMATION SECURITY POLICY

POLICY CLASSIFICATION: BOARD POLICY

MOTION# and APPROVAL DATE: (Include the Motion # and date the policy was approved by the Board)

MOTION# and LAST REVISION DATE: (If applicable, include the motion # and date when last revisions were approved):

Effective Date

December 6, 2021

Last Reviewed

Purpose

The Toronto Public Library ("the Library") is committed to achieving a safe and secure IT environment, including a targeted level of protection from internal and external cyber security threats.

This policy outlines the roles and responsibilities for the security of information, including governance, training and awareness, technical security systems and monitoring of the Library's information security program to ensure a safe and secure IT environment that will minimize the risks of cyberattacks. Policies and procedures will be aligned to federal, provincial, and municipal principles. This include adherence to relevant legislation (such as the *Municipal Freedom of Information and Protection of Privacy Act*) and industry best practices.

Accordingly, the library will implement ongoing governance, policies, practices, and security controls that will address the following objectives:

- Ensure the protection of the Library's data and information assets;
- Establish controls for protecting the Library's information and information systems against theft, abuse, and other forms of harm or loss;

- Enable the requirements for confidentiality, privacy, integrity, and availability for the Library's employees, contractors, vendors, and other users;
- Ensure business continuity, including the recovery of data and operational capabilities in the event of a security breach;
- Motivate administrators and employees to maintain the responsibility for, ownership of, and knowledge about information security;
- Ensure that external service providers are made aware of, and comply with, the Library's information security needs and requirements and continuously assess whether they maintain an acceptable security posture;
- Balance the need for the above with the investment and policy constraints required to achieve an appropriate level of protection while maintaining business agility; and

Ensure compliance with all applicable laws, regulations, and the Library's policies, controls, standards and guidelines.

Scope

This Library Information Security Policy applies to:

- All information, information technology assets, including data and facilities owned and managed by the Library (both on premise and offsite);
- All permanent and temporary employees and agents of the Library;
- All contractors and suppliers, including computer software/ hardware/ applications vendors, dependent contractors, professional services, and IT services vendors;
- Other users of the Library's IT assets wherever they may be located; and
- All technology, including free, procured, trial/ promotional, and open source.

The policy covers governance, policies, standards, practices, and controls for information security, including cybersecurity.

Underlying Principles

Information management and protection of the Library's assets is critical to TPL's achievement of its vision, mission, strategic priorities, and digital strategy. TPL's security practices are in alignment with the value of intellectual freedom, and respecting an individual's right to privacy and choice in accessing Library programs and services.

Information is a vital asset to the Library as it relies heavily on it for the delivery of services and management of resources. As such, the Library recognizes the importance of protecting information in its custody from unauthorized access, modification, disclosure or destruction. It also recognizes the urgency to safeguard the library against cyber attackers with the intention to steal, alter, and/or destroy data and/or assets.

Policy Statement

The Library will enable excellent and responsive Library services through the protection of staff, suppliers, and customers by maintaining the confidentiality, availability, integrity, and security of the Library's information assets.

The Library adheres to industry standards and best practice and reasonably provides safeguards against accidental or unlawful destruction, loss, alteration or unauthorized disclosure or access to Library data.

Through an enterprise-wide IT Security, Risk and Governance Program, the Library will apply security frameworks, standards, protective and detective practices and controls to predict, identify and address threats to information security and enable the Library to operate securely and meet its digital service delivery commitments.

The Chief Information Officer (CIO) will provide corporate direction and oversight for developing and implementing the IT Security, Risk and Governance Program.

Compliance to this policy and standards will be monitored. Anyone that observes non-compliance to this policy must immediately report this to both their supervising manager, the Manager of Human Resources, and the Manager, Security and Enterprise Architecture. Any breach of this policy may be a serious offence and will result in the consideration of appropriate sanctions up to and including termination of employment, contract, or legal action. Exceptions to the policy will be assessed between the line of business Director and the CIO. Any permitted exceptions will be assessed for risk and be reviewed on an annual basis.

All employees, agents of the Library, contractors, and customers of the Library IT assets have the duty to take reasonable precautions to protect the Library's information assets and adhere to the policy, standards, practices and controls. Specific directives regarding the following are outlined in this policy:

- Personnel Security
- Physical Security
- Security Operations
- Access and Authorizations to Information Assets

- Computing Devices
- Network Security
- Cloud Security
- Information Encryption
- Information System Procurement
- Risk Management
- Incident Management

Personnel Security

This section identifies security responsibilities and management processes throughout the employment cycle.

Managers and supervisors must ensure:

a) During employment, employees are informed about the information security policies and procedures, information Security roles and responsibilities, and take any relevant training;

b) At the end of employment, employees are reminded of their ongoing confidentiality responsibilities following termination of employment in accordance with the Employee Code of Ethics;

c) Potential or actual information security breaches are investigated and reported, and invoke incident management processes where necessary; and

d) Contractor responsibilities for information security are identified in contractual agreements, which must adhere to the principles and intentions of this Policy

Physical Security

This section identifies operational requirements for protecting facilities to enable IT Security.

The physical security practices will:

a) Design, document and implement security controls for IT facilities based on an assessment of security risks to the facility;

b) Review, and where appropriate test, physical security and environmental control requirements;

c) Establish appropriate entry controls to restrict access to secure areas, and to prevent unauthorized physical access to information and devices;

d) Incorporate physical security controls to protect against natural disasters, malicious attacks or accidents; and

e) Ensure security controls are maintained when computer equipment, information or software is used outside the Library facilities.

Security Operations

This section establishes the requirements to control, monitor, and manage information security changes.

Information & Technology Services (ITS) will:

a) Plan, document and implement change management processes to ensure changes to information systems and information processing facilities are applied correctly and do not compromise the security of information and information systems;

b) Monitor and maintain information systems software throughout the software lifecycle;

c) Define, document, assess, and test backup and recovery processes regularly;

d) Implement processes for monitoring, reporting, logging, analyzing and correcting errors or failures in information systems reported by users and detection systems;

e) Ensure operating procedures and responsibilities for managing information systems and information processing facilities are authorized, documented and reviewed on a regular basis;

f) Establish controls to protect log files from unauthorized modification, access or disposal;

g) Establish processes to identify, assess, and respond to vulnerabilities; and

h) Enable synchronization of computer clocks to ensure integrity of information system logs and accurate reporting.

Access and Authorizations to Information Assets

This section identifies security roles, responsibilities and management processes relating to access and authorization controls for digital information, applications, data, and devices.

Access to digital information, applications, data and devices are granted to individuals based on business requirements and the principles of "least privilege" and "need-to-know."

Information & Technology Services (ITS) will:

a) will support the mechanisms that evaluate the strength of passwords and define the password change frequency for every type of applications, services and devices.

Managers and supervisors must:

a) Ensure the assignment and revocation of access rights follow a formal process; and
b) Regularly, and upon change of employment, review, and update where appropriate, employee access rights to ensure they are up-to-date.

Employees, agents of the Library, contractors, and users of the Library IT assets must:

a) Know and adhere to access and password standards and security practices; and
b) Passwords should be protected and avoid being written down or shared.

Computing Devices

This section defines requirements for secure management of computing devices.

Information & Technology Services (ITS) will:

a) Maintain an inventory of computing devices, including portable storage devices, and mobile devices;
b) Validate the measures taken to protect information systems and devices as part of an enterprise risk management strategy. This includes maintaining, documenting, verifying and valuing asset inventories on a regular basis;
c) Document the return of computing devices in the possession of employees upon termination of their employment;
d) Remove TPL's information from devices that are no longer needed; and
e) Securely dispose of devices in a manner appropriate for the sensitivity of the information the device contained.

Employees, agents of the Library, contractors, and users of the Library IT assets must:

a) must lock and/or secure unattended mobile devices and laptops to prevent unauthorized use or theft; and
b) ensure that information and devices are protected regardless of the type of access or physical location of employees.

Network Security

This section identifies requirements for the protection of sensitive or confidential information on computer networks.

Information & Technology Services (ITS) will:

a) Document network security controls prior to commencement of service delivery;
b) Ensure security features are implemented prior to commencement of service delivery;
c) Document, implement and manage changes to network security controls and security management practices to protect information systems from security threats;
d) Ensure segregation of services, information systems, and users to support business requirements based on the principles of least privilege, management of risk and segregation of duties;
e) Ensure implementation of network controls to prevent unauthorized access or bypassing of security control;
f) Ensure electronic messaging services are protected commensurate to the value and sensitivity of message content; and
g) Ensure information transfers between the Library and external parties are protected using services approved for use.

Cloud Security

The Chief Information Officer provides corporate direction and leadership on the secure use of cloud services by:

a) Establishing policy and providing strategic direction on the use of cloud services;
b) Establishing roles and responsibilities; and
c) Establishing information security requirements for cloud services.

Managers must:

a) Seek approval from the CIO and the Manager of Procurement and Contracts prior to procuring cloud services;

b) Consider existing cloud service offerings provided by ITS prior to procuring new cloud services; and

c) Obtain CIO approval for any exceptions to ITS service offerings and ensure cloud services align with the TPL's architectural principles.

Information Encryption

This section defines encryption methods for improving the protection of information and for reducing the likelihood of compromised sensitive information.

The Chief Information Officer will:

a) Provide direction and leadership in the use of encryption and create an encryption standard that will set corporate direction for the management (generating, storing, archiving, distributing, retiring and destroying) of encryption keys throughout their lifecycle;

b) The use of encryption controls will be commensurate to the information value and security classification; and

c) Employees and contractors will ensure that any relevant encryption mechanisms will be provided or approved by the CIO.

Information System Procurement

This section defines requirements to ensure security controls are included in business and contract requirements for building and information systems, including commercial off the shelf and custom-built software.

Procurements must:

a) Develop, implement and manage the processes and procedures necessary to ensure that information security risks and privacy requirements are taken into account throughout the systems development lifecycle;

b) Assess business requirements and associated risks related to external party access to information and ensure that they are identified, assessed, mitigated and managed;

c) Ensure security controls, service definitions, and delivery levels are identified and included in agreements with external parties prior to using external information and technology services;

d) Ensure security requirements are agreed upon and documented prior to granting external parties access to information, information systems or information processing facilities;

e) Ensure that changes to the provision of services by suppliers take into account the criticality of the information and the assessment of risks;

f) Establish processes to manage and review the information security controls of services delivered by external parties, on a regular basis; and

g) Apply vulnerability scanning, security testing, and system acceptance processes commensurate to the value and risks of the information system.

Risk Management

This section defines the requirements to manage IT security risk, including cyber security.

The Chief Information Officer shall develop and maintain an information security risk management methodology. The methodology will:

a) Align with TPL’s enterprise risk management policy based on probability and impact;

b) Describe TPL’s position with respect to IT security risk;

c) Address the degree of protections with very high security risks being protected with greater security controls than IT assets with a lower risk rating; and

d) Maintain a risk registry that will report on TPL’s IT security risk posture.

IT Incident Management

This section defines the requirements to report, respond, and recover from IT Security Incidents.

The Chief Information Officer shall develop and maintain an incident response and recovery methodology. The methodology will:

e) Describe the process for reporting a suspected IT security breach;

f) Describe the process for preparation, detection and analysis, containment, eradication and recovery;

g) Ensure appropriate escalations and reporting of major incidents;

h) Conduct post-incident assessment and address improvement recommendations; and

i) Maintain an incident log that will report on TPL's IT security risk posture.

Compliance Management

This section defines the requirements to support TPL's compliance requirements.

The methodology will:

a) Align IT security controls with the requirements of TPL's compliance practices; and
b) Address changes to the compliance requirements.

Accountability

The Director, Digital Strategy and Chief Information Officer is responsible for overseeing the implementation of, and adherence, to this Policy.

Chief Information Officer (CIO)

The CIO provides vision and leadership for developing and implementing the IT Security, Risk and Governance Program.

The accountabilities of the CIO include:

- Set strategy for the information security program consistent with the corporate strategic plan, Digital Strategy and IT Strategy;
- Governance over information security program;
- Deliver cyber risk management advice and cyber and digital security solutions
- Align with the Policy, Planning & Performance Management (PPPM) department to ensure that security controls support the Privacy policy;
- Report to the Board on a regular basis regarding information security risk and major cyber security incidents;
- Maintain relationships with local, provincial, and federal law enforcement and other related government agencies; and

- Validate the integrity of the information security program through independent security audits.

Manager, IT Security and Enterprise Architecture

The Manager, Security and Enterprise Architecture develops, implements and administers the IT Security, Risk and Governance Program:

- Information security governance to ensure that controls are functioning;
- Provide security awareness training for the enterprise;
- Develop and maintain enterprise architecture standards, including information security standards;
- Co-ordinate information security risk assessments and audits;
- Lead implementation of the Cybersecurity plan including incident response and recovery;
- Lead in the investigation of information security incidents;
- Support completion of Privacy Impact Assessments for new projects or programs;
- Design security controls for current and new systems;
- Provide security assurance;
- Remain current on information security trends; and
- Continuous improvement and maintenance of the Security program.

Appendices

Relevant Legislation

- Municipal Freedom of Information and Privacy Protection, R.S.O. 1990, c. M.56
- Public Libraries Act, R.S.O. 1990, c. P.44

Relevant Library Policies

- Acceptable Use of IT Resources Policy
- Access to Information and Protection of Privacy
- Employee Code of Ethics
- Financial Control Policy

- Human Rights and Harassment Policy
- Purchasing Policy
- Risk Management Policy
- Signing Authority Policy

Definitions

Agent – A person authorized by a custodian to acts for, or on behalf of, a custodian and not the agent’s own purposes. For example, third party employees, contractors, and volunteers.

Assets – Hardware, software, data, and information owned by the Library. Assets can include, but are not limited to, information in all forms, media, networks, systems, materiel, and IT financial resources.

Audit – An independent examination of an information system and process to detect unauthorized activities.

Availability – The ability of a configuration item or IT service to perform its agreed function when required to ensure information, systems, and data are ready for use when need.

Compromise – Unauthorized disclosure, destruction, removal, modification, interruption or use of assets.

Confidentiality – The protection of sensitive or private information from unauthorized disclosure.

Digital Assets include hardware, software, data, and business processes.

DRP – Disaster Recovery Plan – a documented, structured approach that describes how an organization can quickly resume work after an unplanned incident. A DRP is an essential part of a business continuity plan.

Employee / agent – A Library employee, agent, contractor, volunteer, Board member, or anyone who is authorized to have access to the Library computer environment.

Integrity – The accuracy and completeness of assets, and the authenticity of transactions.

Physical security – Physical safeguards to prevent and delay unauthorized access to assets, detect attempted and actual unauthorized access, and activate appropriate responses.

Risk – The chance of something happening that will have a positive or negative impact on the confidentiality, integrity and availability of information assets.

Risk Assessment – A process that identifies and evaluates risks and their potential impact on an organization in quantitative and qualitative terms.

Security incident – The compromise of an asset, or any act or omission that could result in a compromise. A threat or an act of violence toward employees.

Enquiries

Director, Digital Strategy & CIO
Manager, IT Security & Enterprise Architecture

Annual Update on IT Security

Frank Kim

Manager IT Security & Enterprise Architecture

Angela Copeland

Director, Digital Strategy & CIO

TPL Board
December 2021

toronto public library

agenda

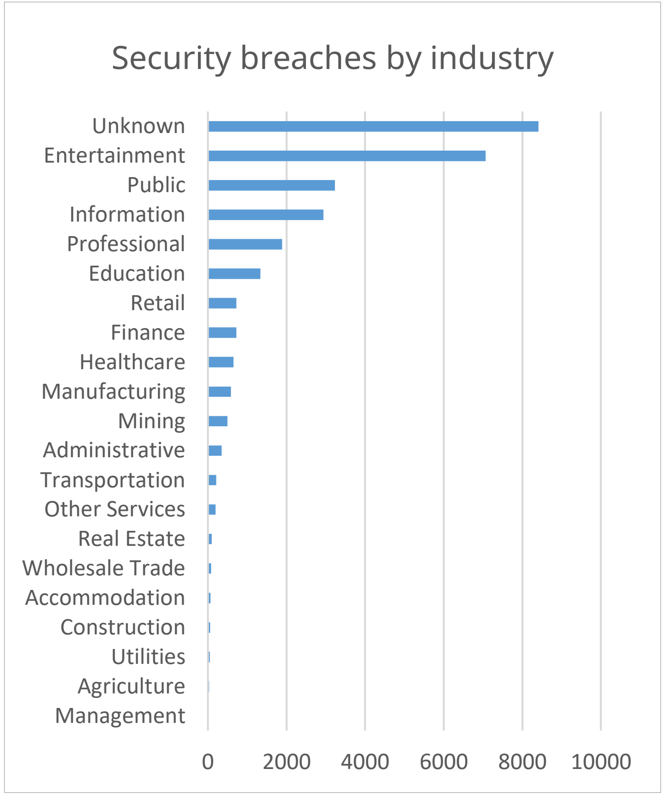
- IT security posture report
- IT security, risk and governance program update

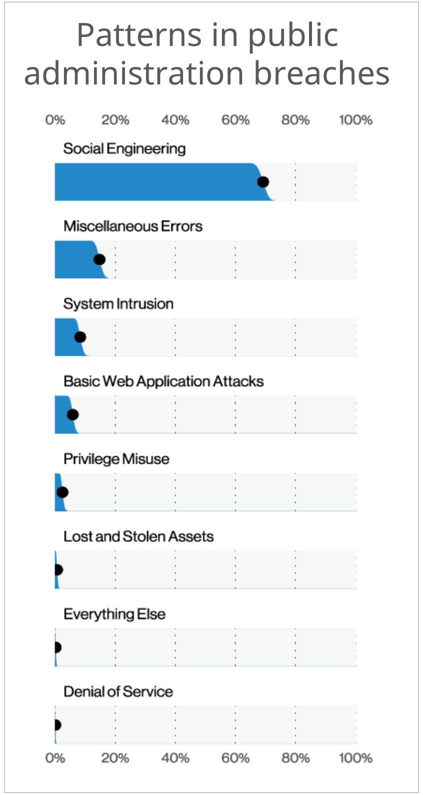
TPL’s IT security posture

global trends 2021

Highlights

- As a public sector organization, TPL is among the top five organizations targeted for cyber security attacks
- Attempts to harvest credentials and internal errors are the top two reported cybersecurity incidents
- TPL has had no major cyber security incidents since it began reporting on its IT Security Posture in September 2020.


Security breaches by industry


Patterns in public administration breaches

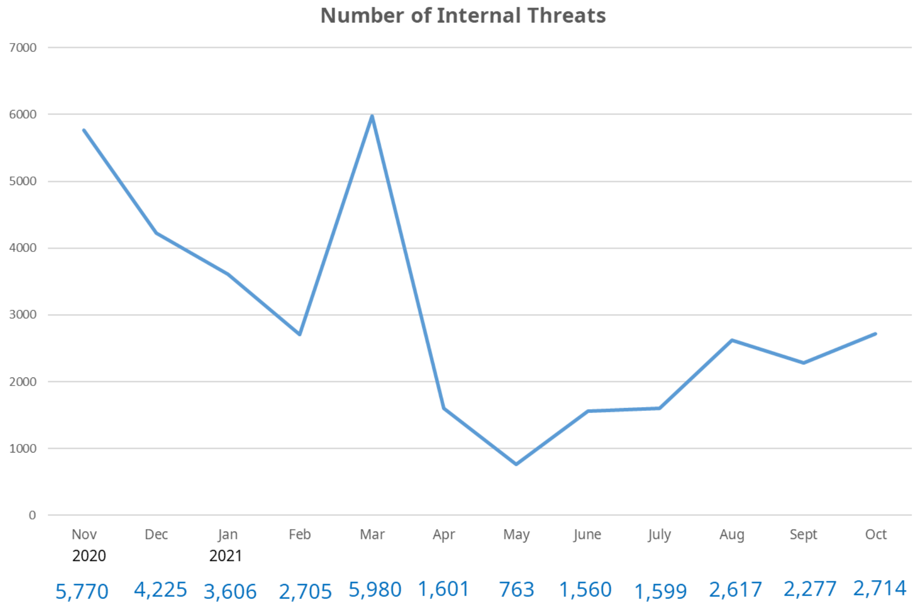
2021 DBIR Master's Guide: https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/

tpl internal threats

Highlights

Internal security threats originate from inside TPL’s network.

- During the stay-at-home lockdown in April, the number of threats decreased significantly, and threats gradually increased as services were reinstated
- There have been no virus outbreaks



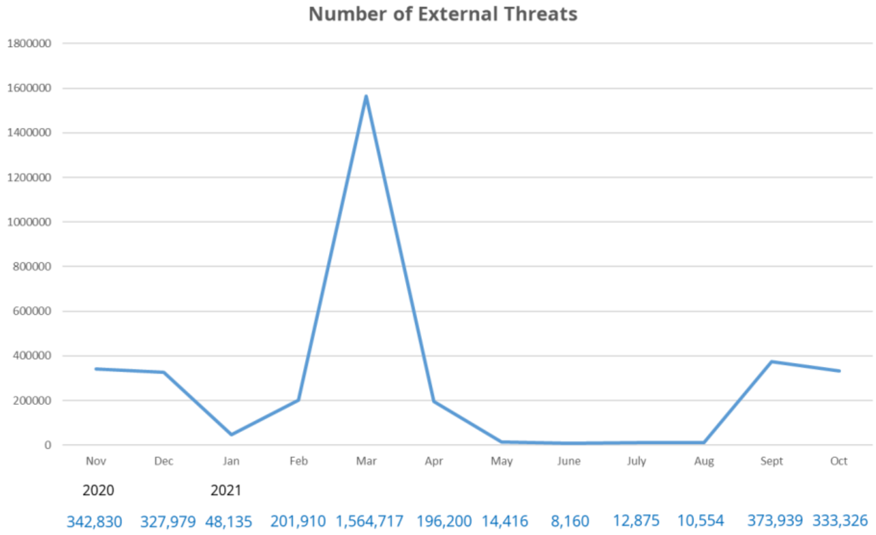
*June – Oct numbers have been adjusted to remove a suspected outlier related to a conflict with McAfee self-protection and Windows update services.

tpl external threats

Highlights

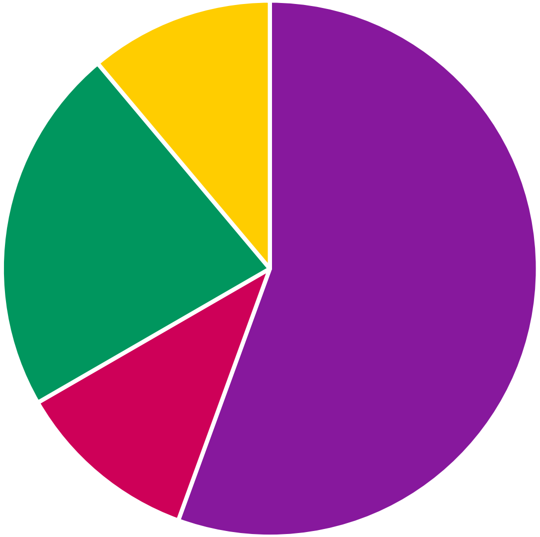
External threats originate outside of the TPL network.

- During March, a peak was observed due to a misconfiguration after a system upgrade
- During the stay-at-home lockdown in April, the number of threats decreased significantly, and threats gradually increased as services were reinstated



*Sept – Oct numbers have been adjusted to remove a false positive resulting from a server change that increased HTTP traffic

escalated security incidents



🟪 **Privileged misuse (5):** misuse of legitimate privileges e.g. insider threats

🟥 **Miscellaneous error (1):** unintentional errors causing a security event e.g. misconfiguration

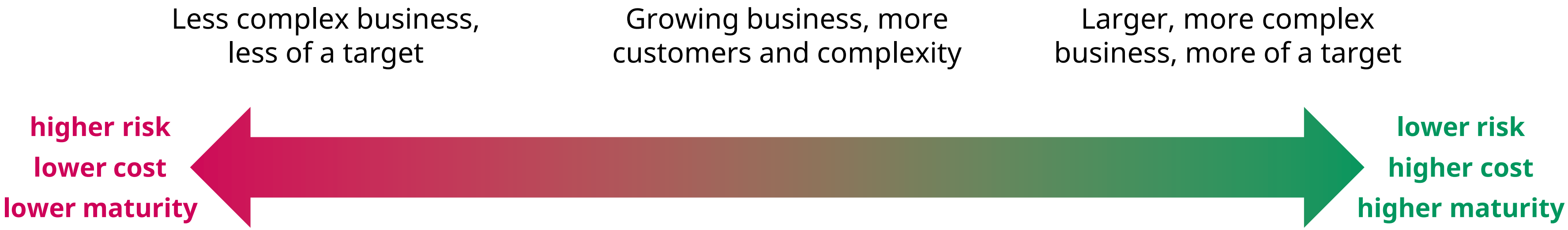
🟩 **Social engineering (2):** psychological coercion to take an action or breach confidentiality e.g. phishing emails

🟨 **Denial of service (1):** compromise of system availability e.g. disruptive flooding of network traffic

The majority of investigated incidents were phishing attacks or privileged misuse of email. There are no major cybersecurity incidents to report.

IT security, risk and governance program update

program goal



Less complex business, less of a target

Growing business, more customers and complexity

Larger, more complex business, more of a target

higher risk
lower cost
lower maturity

lower risk
higher cost
higher maturity

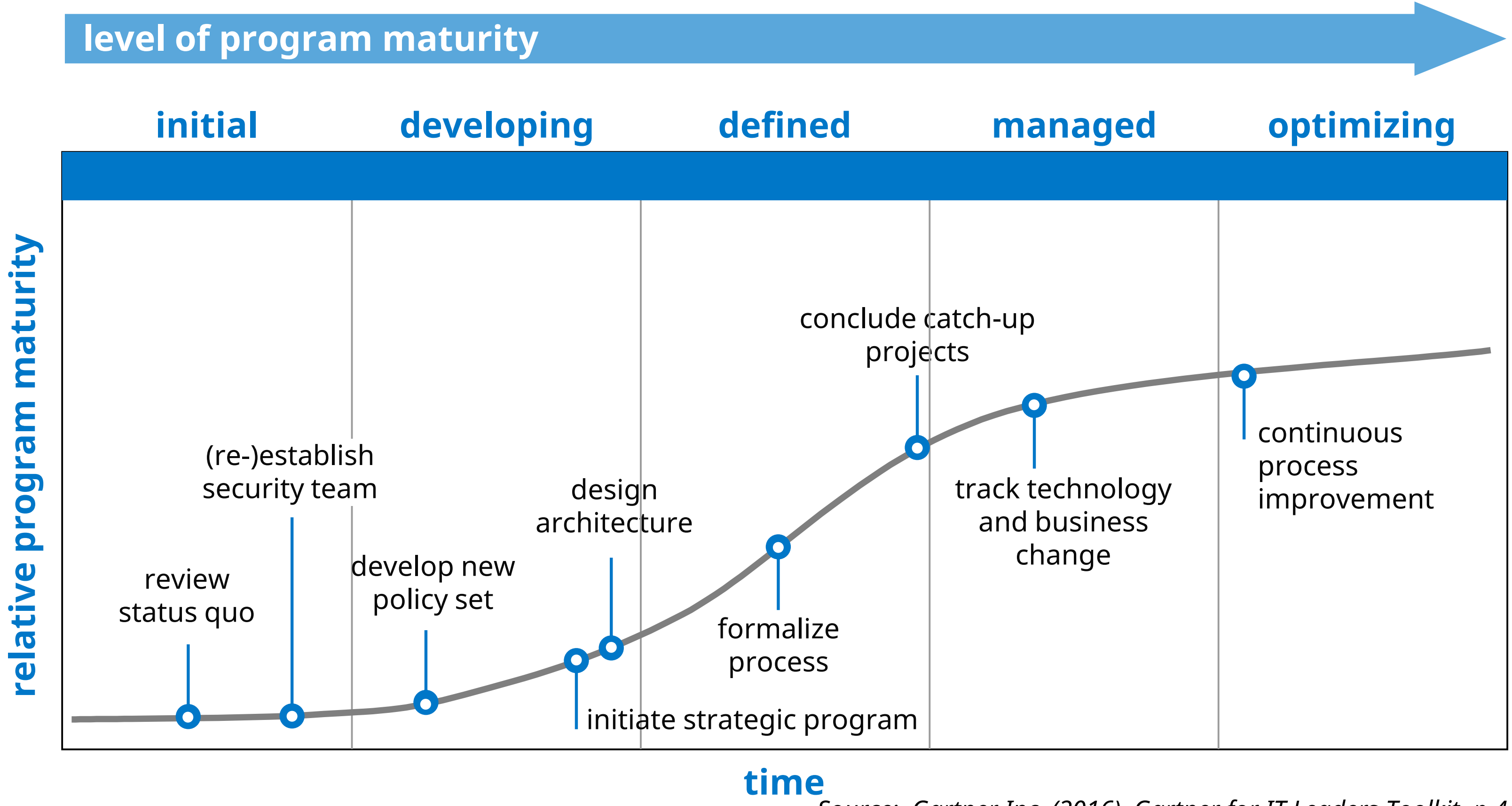
There is no such thing as "perfect protection“

Our goal is to build a sustainable program that balances the need to protect, with the need to run our business.

As our business grows, we have to continually reassess how much risk is appropriate.

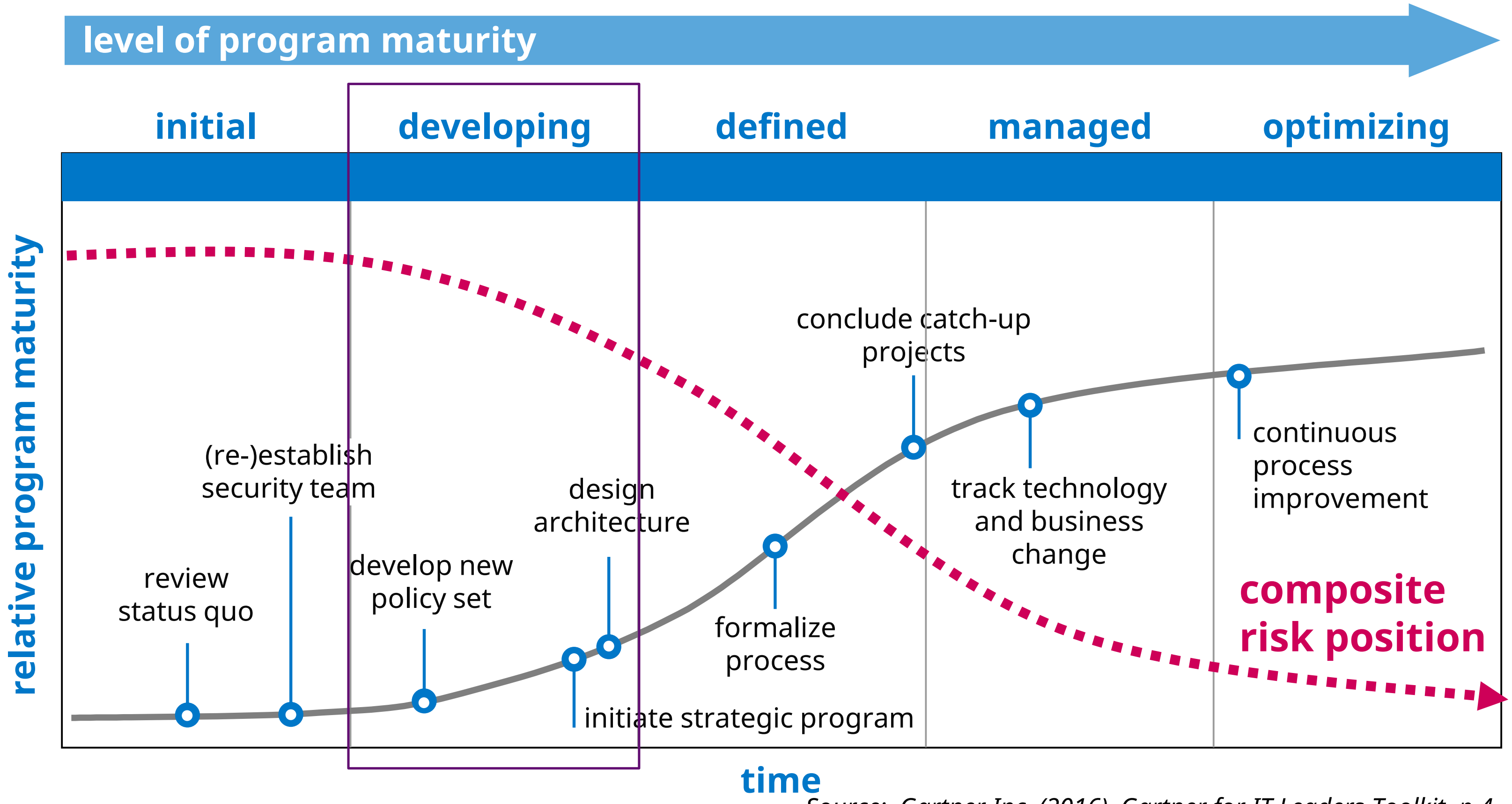
Source: Gartner Inc. (2016). Gartner for IT Leaders Toolkit. p.3.

current program status


level of program maturity
initial
developing
defined
managed
optimizing
relative program maturity
review status quo
(re-)establish security team
develop new policy set
initiate strategic program
design architecture
formalize process
conclude catch-up projects
track technology and business change
continuous process improvement
time

Source: Gartner Inc. (2016). Gartner for IT Leaders Toolkit. p.4.

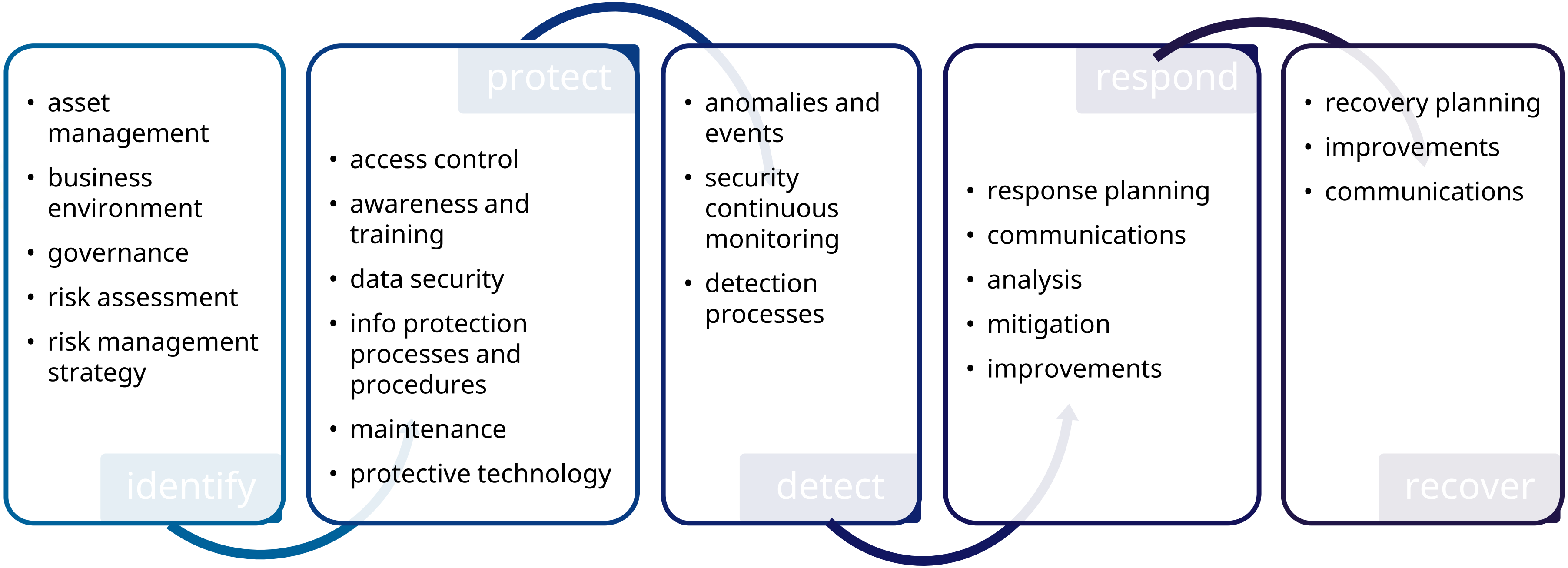
current program status and composite risk



level of program maturity
initial
developing
defined
managed
optimizing
relative program maturity
review status quo
(re-)establish security team
develop new policy set
design architecture
initiate strategic program
formalize process
conclude catch-up projects
track technology and business change
continuous process improvement
composite risk position
time

Source: *Gartner Inc. (2016). Gartner for IT Leaders Toolkit. p.4.*

IT security risk & governance program framework
(based on NIST Cyber Security Framework)



identify

- asset management
- business environment
- governance
- risk assessment
- risk management strategy

protect

- access control
- awareness and training
- data security
- info protection processes and procedures
- maintenance
- protective technology

detect

- anomalies and events
- security continuous monitoring
- detection processes

respond

- response planning
- communications
- analysis
- mitigation
- improvements

recover

- recovery planning
- improvements
- communications

progress to date 1

Business environment

- Public Safety Canada Regional Resiliency Assessment completed in January
- Regular knowledge-sharing with City of Toronto Chief Information Security Officer (CISO) team

Governance

- Monthly reporting reviews by CIO, quarterly by Directors' Committee and annually by the Board of Directors
- Approval of adoption of National Institute Standards and Technology (NIST) Cybersecurity Framework
- Development of an Information Security Policy
- Currently participating in the City of Toronto, Information Security Forum Risk Assessment

Risk assessment

- Monitoring of imminent cyber threats affecting Canada
- Threat risk assessment tasks initiated with enterprise project management methodology

progress to date 2

Identity & access controls

- Password controls
- Privileged account reset including local administrator
- Formalization of improved password standard

Anomalies & events

- Intrusion detection system tuning
- Security Operations Centre (SOC) level 1 (alert collection) services started

Awareness & training

- Implementation of cyber security awareness training (76% compliance)

Information protection processes & procedures

- Vulnerability management program initiated with patch vulnerabilities

progress to date 3

Maintenance

- Resumption of desktop patching

Cybersecurity Incident Response & Recovery

- Security Operations Centre (SOC) level 2 (analysis & triage) services started
- Automated response by blocking threats from Internet
- Automated response by blocking threats from branch network connections

planned activities

Protective controls improvements project

- Cybersecurity awareness and training
- Identity & access management
- Data Security

Detective controls enhancements project

- Internet network detection
- Vulnerability management program

Cyber security incident response and recovery project

- Initiate third party security monitoring
- Assess incident recovery capabilities

thank you

questions