"Cybersecurity is everyone's business"

City of Clarence-Rockland

Cybersecurity Strategic Plan

2019

Michel Cousineau
Chief Information Officer

Contents

Executive Summary

This document represents the City of Clarence-Rockland's first Cybersecurity Strategic Plan. It outlines our approach in ensuring the City's assets are protected to the best of our ability.

The Plan highlights a Framework that addresses for key areas:

- Policies, Processes and Procedures;
- Training and Awareness;
- Physical Security and Business Continuity;
- IT Systems

The result of this plan will be a 3-year Action Plan with initiatives geared at helping us protecting the City's assets. One of the key initial initiatives will be a third-party assessment which will further help to build our Action plan.

Since this is our first plan to address cybersecurity, we will need to review periodically as we will learn from the various initiatives and solidify the plan, as well as our security posture, as we go along.

Although the projects will be managed by the IM/IT Team, every staff member will be involved at some point.

Cost to implement the plan will be approximately **$30,000** for the first year.

NOTE: This document includes a lot of new terminology. Appendix A includes a glossary of common cyber terms.

"Cybersecurity is everyone's Business!"

Challenge

Cybersecurity has become the single largest risk to the world's organizations whether they are all government tiers or businesses of any size. Banks now rank Cyber Risk higher than credit, which is substantial when one considers the credit event of 2008/2009.

Cyber criminals are from every walk of life from young teenagers to organized crime and terrorist groups.

The companies and cities above are just a small example of some of the organizations that have been hacked by various means from ransomware to leaks of personal information.

Some alarming statistics

- Cybercrimes are costing Trillions $ in damages every year (Est. to be $6T/year by 2021);
- Half of damages are to smaller organizations;
- There is an attack every 14 seconds;
- Anyone can become a hacker with an investment of $1 and a little bit of time.

Since Hackers are always a few steps ahead with technology, we cannot only focus on this area.

We must take the approach of focusing on what we can control… Not what the cybercriminal control.

No amount of risk mitigation or investment will Guarantee that no breach will ever occur.

IM/IT Strategic Plan

The Security Strategic Plan would usually be part of a broader IM/IT Strategic plan. Given the current staffing issues on the IM/IT and the fact that Cybersecurity is a significant issue for municipalities, the decision was to prioritize a plan that addresses it specifically.

Cybersecurity Framework

Definition

A Cybersecurity Framework is a set of guidelines by which an organization manages its IT/IM (Cyber) Security. It includes everything from policies to tools and communications. It is critical for any organization to have some kind of framework in place in order to accurately measure its current capacities in protecting its assets as well as have a plan to improve problematic areas. Without a framework, it becomes very difficult to know which areas of focus should be/need to be a priority.

Approach

There are many approaches to creating a framework that range from ad-hoc priority setting to very stringent ISO 90021 certification, with many options in between. The City of Clarence-Rockland will be creating its own Framework for now that aligns as much as possible with the Cybersecurity Framework from the National Institute of Standards and Technology (NIST). It is highly regarded as one of the best standards for Cybersecurity and is flexible enough to allow us to slowly and gradually work towards it with the resources we have.

NIST Cybersecurity Framework

Created in 2014, it has become one of the most adopted standards for managing Cybersecurity. Its core is Broken down into 5 function areas that group the activities to achieve specific cybersecurity outcomes. They are: **Identify, Protect, Detect, Respond, Recover**.

Each of these functions are further broken down into categories, sub-categories and references which are described in Appendix B.

City of Clarence-Rockland (CCR) Cybersecurity Framework

Every Journey starts with some first steps. To simplify our implementation of a solid and modern framework while not confusing everyone with too much NIST nomenclature, we have developed the City's Cybersecurity Framework.

The framework is comprised of four sections as well as two over-arching functions (**Governance and Risk Management**) that are must be a part of all sections.

Below is a description of the framework's sections

Policies, Processes and Procedures

This section deals with the required rules, regulations and check lists to help in managing Cybersecurity for the City.

Training & Awareness

The section is split into two audiences

City Staff

The training (mandatory and optional) that City staff should be taking periodically to ensure they are fulfilling their role in protecting the city's assets and themselves. It also includes the various awareness activities and resources that must be made available to them.

Residents

While there will be no official formal training provided to our community, as a smart city, we owe it to our residents and to ourselves to arm them with as much knowledge as possible to protect their families from potential cyber predators. This will be in many forms such as public presentations and resources on our Web site.

Physical Security and BCP

This section deals with the city's physical security (buildings and other physical assets) and Business Continuity Planning, as well as subsequent Disaster Recovery activities in the event of a significant cyber event. This needs to tie into the broader plan which is managed by the Protective Services Department.

IT Systems

Although many associate Cybersecurity with IT systems only, they are but one part of the equation. With the advancements in technology and tools, it can often be the easier one to manage given the right resources.

Governance

This section is part of every section where it plays key vital roles such as:

- Approval of various policies and procedures;
- Identifying roles, Responsibilities and resources;
- Creating and managing appropriate Committees and Working Groups;
- Communicating the framework to all departments.

Risk Management

Like many organizations, we will be using a solid Risk Management both initially and, on every project, to ensure we are doing the following:

- Creating a Risk Management Process that can be used not only for Cyber Risk but other operational risks as well;
- Identifying all our risks as they pertain to Cybersecurity along with their rating and mitigation activities;
- Creating a formal Risk Registry to track our risks as well as all mitigation activities and statuses.

Detailed Plan

Introduction

This section describes, in detail, all the projects that we will be undertaking over the next several years with the following information:

- A description of the project;
- Who is involved;
- How it aligns with the NIST Framework (for future alignment and auditability)

While this section explains the WHAT, WHY and WHO, it does not go into the WHEN AND WHERE. The tentative timelines for these projects are outlined in the 3-year Action Plan that accompanies this plan. The Action Plan will be revised every year to ensure we are concentrating on the right priorities and ensuring the budget reflects the planned work.

Policies, Processes and Procedures

Policies and Processes would usually be a subset of the Governance function but for the time being, it has its own section is because of the lack of detailed IM/IT Policies that we currently have. Policies help us govern many of the activities within the city, so it is imperative to grow this section substantially in the first year so that we may have a base line of governance to align with.

Approach

The following approach will be taken with all policies & Processes:

- We will use the City's templates and procedures for all policies;
- We will create a Process template that will then be subsequently used for all process documentation;
- Processes must align with policies when applicable.
    - EXAMPLE: It is important to have a fully documented staff onboarding/offboarding process. It is equally important to have a policy that enforces the need to follow the process;
- All Policies will be approved by the Council and communicated to all staff.

- All IM/IT Security Processes will be approved by both the Chief Information officer and Directors who have shared accountability for the process (EX: HR for the Onboarding process);
- As Procedures tend to be operational and very specific. They will be created, reviewed and shared appropriately (EX: Procedure to connect with a VPN).

Current list of Policy, Process and Procedure Deliverables

The following is a list of the documents that are currently part of the plan. *

**Many initiatives will require us to create/modify plans over the next years such as Office365, Smart City Projects, etc.*

Policies

Document	Description	Owner(s)	NIST Activity
IM/IT Acceptable Use Policy	This is a complete revision of the current IT restrictions Policy to ensure it is up to date and reflects current Cybersecurity practices	IM/IT	Protect
Patch Management Policy	This New Policy outlines the requirements to ensure our systems and applications are patched in regular and timely fashion to reduce the chances of them being compromised.	IM/IT	Protect
Change Management Policy	This New Policy outlines the requirements of how change is introduced to our IT Systems environments on premise and in the cloud.	IM/IT	Protect
Cellular & Mobile Computing Policy	This is a complete revision of the Cell phone Policy to ensure it is current and includes other mobile devices as well as remote connectivity	IM/IT	Protect
Cloud Storage Policy	This new Policy outlines the rules and expectations as they pertain to using offsite (cloud) storage for City assets.	IM/IT	Protect
Staff On/Offboarding Policy	This new Policy outlines the requirements for onboarding new employees as well as offboarding employees that are leaving the City.	IM/IT and Human Resources	Protect
Security Training Policy	This new Policy outlines the Requirements as they pertain to staff obligations for training & awareness activities	IM/IT, CAO and All Directors	Protect
Security incident Reporting Policy	This new Policy outlines the requirements to properly report any IM/IT Security incidents that may occur.	IM/IT	Recover
IM/IT Monitoring Policy	This new policy outlines the requirements for tracking specific metrics and Performance Indicators that provide an overview of all IT health, including Cybersecurity.	IM/IT	Identify
Social Networking Policy	This policy addresses use of various Social Media platforms such as Facebook, YouTube, etc..	IM/IT and Comms	Protect

Processes

Document	Description	Owner(s)	NIST Activity
Staff Onboarding Process	This document outlines the detailed process that is followed when new staff members join the City	HR, All departments	Protect
Staff Offboarding Process	This document outlines the detailed process that is followed when a staff member leaves the City (both planned and unplanned)	HR, All departments	Protect
IT Patch Management Process	This document outlines all the system patching occurring and when.	IM/IT	Protect
IT Change Management Process	This document outlines the process followed to introduce change into our production environment.	IM/IT	Protect
IM/IT Engagement Process	This document outlines the process staff need to follow to get IT services including projects, incidents, emergencies, etc..	IM/IT	Identify

Procedures

Document	Description	Owner(s)	NIST Activity
Guidelines for a safe Web experience	This document will outline some general guidelines to navigate and work on the web in a safe way.	IM/IT	Protect

Training and Awareness

Probably the most overlooked area of focus over the last decade even though user behavior accounts for over 90% of cyber incidents because of lack of knowledge and awareness.

Approach

As mentioned in the previous section, this activity will address two different audiences:

- City Staff
- Residents of Clarence-Rockland

City Staff

Since staff share the responsibility of ensuring our assets and have some sort of access to these assets including the network, facilities and data, they are the primary focus of the Training and Awareness Program. This Program will include:

- Mandatory training for all employees of the City whether they are full-time, part-time, City Councillors or any other temporary employee/consultant that can access any of the assets. The delivery of the training will be determined in the fall but will most likely be online;
- Other awareness activities such as information sessions, webinars and presentations that staff will the option to participate in;
- An online Cybersecurity Resource Centre that includes multiple links and information from various expert agencies such as the CSE, OPP and RCMP.

Residents

While the City cannot take responsibility for the online habits of its citizens, we believe that an informed City is a strong City and a SMART City. As such, we will be providing the following activities to residents as part of the program:

- Public Cybersecurity 101 classes in both official languages. The exact content, schedule and frequency of these sessions will be communicated in the fall of 2019.
- Online Cybersecurity resources on our Web site for residents to visit at their convenience.

Current list of Training & Awareness Deliverables

The following are lists of the initiatives are that currently part of the plan. *

Document	Description	Owner(s)	NIST Activity
Cybersecurity Training Plan	A document that outlines the approach the City will take to ensure all staff are properly trained. It will align with the Cybersecurity Training Policy. There will be a special section for IM/IT Staff as their training needs are obviously greater given their mandate to support this plan.	IM/IT	Protect
Cybersecurity 101 Presentations	These presentations will be offered in both languages to our residents. They will include good cyber practices and hygiene as information on resources they can leverage.	IM/IT Comms	Protect
Cybersecurity Resource Centre	A web portal/page dedicated to cybersecurity awareness including information from various agencies and security organizations.	IM/IT Comms	Protect

Physical Security and Business Continuity Planning (BCP)

This area comprises activities that are not completely IM/IT specific and require coordinating with other departments.

- Any activities around physical security require coordinating with building management, protective services and public works;
- Activities around BCP must align with the overall Emergency Management planning and practices.

Approach

Apart some specific projects that have already been approved and funded, the initial projects in this area will comprise of evaluating what the needs and requirements of the City are.
EX: We could invest time and funds into a Disaster Recovery solution only to find out that it does not meet the needs of the business

Current list of Physical Security & BCP Deliverables

The following are lists of the Initiatives that are currently part of the plan. *

Document	Description	Owner(s)	NIST Activity
Cybersecurity Incident Management process	The process that is followed when a cyber incident occurs.	IM/IT	Respond
Cybersecurity Incident Report	The report that is used to document all aspects of a cybersecurity incident including communications, root cause analysis, post mortem, etc..	IM/IT	Respond
Departmental Business Impact Analysis for BCP events	A complete and documented analysis of the needs and potential impacts of every department in the case of a cyber related BCP event. This will be part of an over-arching BCP for the City.	IM/IT Prot. Serv.	Respond
Start yearly BCP tests	These are formal tests of our BCP processes and responses. They are critical to ascertain if the plan and business impacts are aligned. (often done as table top exercise)	IM/IT Prot. Serv.	Respond
Physical Security Architecture	A documented review of the current physical architecture including all door access, cameras and alarms for all the City's assets.	IM/IT Prot. Serv. Building mgt	Identify

IM/IT Systems

This area comprises activities that are related to the actual tools and technologies used for cybersecurity purposes

Approach

This section currently includes some initial initiatives that will help shape the remainder of the Action plan along with the third-party assessment.

Current list of IM/IT Systems Deliverables

The following are lists of the Initiatives that are currently part of the plan. *

Document	Description	Owner(s)	NIST Activity
IT systems Architecture	A revised set of complete system architecture that can be referenced in other initiatives	IM/IT	Identify
Cybersecurity Architecture	A revised set of security architecture specific to cybersecurity	IM/IT	Identify
Vulnerability Assessment	Third-party assessment of the City's security posture	IM/IT	Identify
Full Inventory	A complete inventory of all IT systems	IM/IT	Identify
Review of Monitoring, Metrics and KPIs	A review of the way we monitor our systems as well as the metrics and KPIs we use do to so.	IM/IT	Identify
Review of practices, processes and procedures	A complete review of the various practice in IT that can impact cybersecurity	IM/IT	Identify

3-Year Action Plan

Once the plan is addressed, we will begin the detailed planning of all the activities. Once we perform the third-party Security Assessment, the recommendations that result from it will also feed into the Action Plan.

An initial Action plan will be produced by end of October 2019

Appendix A - Glossary

Taken from the following site:

https://www.globalknowledge.com/ca-en/topics/cybersecurity/glossary-of-terms/

access control — The means and mechanisms of managing access to and use of resources by users. There are three primary forms of access control: DAC, MAC, and RBAC. DAC (Discretionary Access Control) manages access through the use of on-object ACLs (Access Control Lists), which indicate which users have been granted (or denied) specific privileges or permissions on that object. MAC (Mandatory Access Control) restricts access by assigning each subject and object a classification or clearance level label; resource use is then controlled by limiting access to those subjects with equal or superior labels to that of the object. RBAC (Role Base Access Control) controls access through the use of job labels, which have been assigned the permissions and privilege needed to accomplish the related job tasks. (Also known as authorization.)

anti-virus (anti-malware) — A security program designed to monitor a system for malicious software. Once malware is detected, the AV program will attempt to remove the offending item from the system or may simply quarantine the file for further analysis by an administrator. It is important to keep AV software detection databases current in order to have the best chance of detecting known forms of malware.

antivirus software — A software program that monitors a computer system or network communications for known examples of malicious code and then attempts to remove or quarantine the offending items. (Also known as Malware Scanner.) Most anti-virus (AV) products use a pattern recognition or signature matching system to detect the presence of known malicious code. Some AV products have adopted technologies to potentially detect new and unknown malware. These technologies include anomaly detection (i.e. watch for programs which violate specific rules), behavioral detection (i.e. watch for programs that have behaviors that are different from the normal baseline of behavior of the system), and heuristic detection (i.e. watch for programs that exhibit actions which are known to be those of confirmed malware; it is a type of technological profiling).

APT (Advanced Persistent Threat) — A security breach that enables an attacker to gain access or control over a system for an extended period of time usually without the owner of the system being aware of the violation. Often an APT takes advantage of numerous unknown vulnerabilities or zero day attacks, which allow the attacker to maintain access to the target even as some attack vectors are blocked.

asset — Anything that is used in and is necessary to the completion of a business task. Assets include both tangible and intangible items such as equipment, software code, data, facilities, personnel, market value and public opinion.

authentication — The process of proving an individual is a claimed identity. Authentication is the first element of the AAA services concept, which includes Authentication, Authorization, and Accounting. Authentication occurs after the initial step of identification (i.e. claiming an identity). Authentication is accomplished by providing one or more authentication factors—Type 1: something you know (e.g. password, PIN, or combination), Type 2: something you have (e.g. smart card, RSA SecureID FOB, or

USB drive), and Type 3: something you are (e.g. biometrics—fingerprint, iris scan, retina scan, hand geometry, signature verification, voice recognition, and keystroke dynamics).

authorization — The security mechanism determining and enforcing what authenticated users are authorized to do within a computer system. The dominant forms of authorization are DAC, MAC and RBAC. DAC (Discretionary Access Control) manages access using ACL (Access Control Lists) on each resource object where users are listed along with the permissions or privileges granted or denied them. MAC (Mandatory Access Control) manages access using labels of classification or clearance on both subjects and objects, and only those subjects with equal or superior clearance are allowed to access resources. RBAC (Role Based Access Control) manages access using labels of a job role that has been granted the permissions and privileges needed to accomplish a specific job or role.

backing up — Creating a duplicate copy of data onto a separate physical storage device or online/cloud storage solution. A backup is the only insurance against data loss. With a backup, damaged or lost data files can be restored. Backups should be created on a regular, periodic basis such as daily. A common strategy is based on the 3-2-1 rule: you should have three copies of your data - the original and 2 backups; you should use 2 different types of media (such as a physical media (such as a hard drive or tape) and a cloud storage solution); and do not store the three copies of data in 1 plane (i.e. backups should be stored offsite). It is important to store backups for disaster recovery at an offsite location in order to insure they are not damaged by the same event that would damage the primary production location. However, additional onsite backups can be retained for resolving minor issues such as accidental file deletion or hard drive failure.

BCP (Business Continuity Planning) — A business management plan used to resolve issues that threaten core business tasks. (Also known as Business Continuity Management.) The goal of BCP is to prevent the failure of mission critical processes when they have be harmed by a breach or accident. Once core business tasks have been stabilized, BCP dictates the procedure to return the environment back to normal conditions. BCP is used when the normal security policy has failed to prevent harm from occurring, but before the harm has reached the level of fully interrupting mission critical processes, which would trigger the Disaster Recovery Process (DRP).

behavior monitoring — Recording the events and activities of a system and its users. The recorded events are compared against security policy and behavioral baselines to evaluate compliance and/or discover violations. Behavioral monitoring can include the tracking of trends, setting of thresholds and defining responses. Trend tracking can reveal when errors are increasing requiring technical support services, when abnormal load levels occur indicating the presence of malicious code, or when production work levels increase indicating a need to expand capacity. Thresholds are used to define the levels of activity or events above which are of concern and require a response. The levels below the threshold are recorded but do not trigger a response. Responses can be to resolve conflicts, handle violations, prevent downtime or improve capabilities.

blacklist — A security mechanism prohibiting the execution of those programs on a known malicious or undesired list of software. The blacklist is a list of specific files known to be malicious or otherwise are unwanted. Any program on the list is prohibited from executing while any other program, whether benign or malicious, is allowed to execute by default. (See whitelist.)

block cipher — A type of symmetric encryption algorithm that divides data into fixed length sections and then performs the encryption or decryption operation on each block. The action of dividing a data set into blocks enables the algorithm to encrypt data of any size.

botnet — A collection of innocent computers which have been compromised by malicious code to run a remote-control agent granting an attacker the ability to remotely take advantage of the system's resources to perform illicit or criminal actions. These actions include DoS flooding attacks, hosting false Web services, spoofing DNS, transmitting SPAM, eavesdropping on network communications, recording VOIP communications and attempting to crack encryption or password hashes. Botnets can be comprised of dozens to over a million individual computers. The term botnet is a shortened form of robotic network.

bug — An error or mistake in software coding or hardware design or construction. A bug represents a flaw or vulnerability in a system discoverable by attackers and used as point of compromise. Attacks often use fuzzing technique (i.e. randomize testing tools) to locate previously unknown bugs to craft new exploits.

BYOD (Bring Your Own Device) — A company's security policy dictating whether workers can bring in their own devices into the work environment, whether such devices can be connected to the company network and to what extent that connection allows interaction with company resources. A BYOD policy can range from complete prohibition of personal devices being brought into the facility to allowing any device to be connected to the company network with full access to all company resources. Generally, a BYOD policy puts reasonable security limitations on which devices can be used on company property and severely limits access to sensitive company network resources. BYOD should address concerns such as data ownership, asset tracking, geo location, patching and upgrades, security applications (such as malware scanners, firewalls and IDS), storage segmentation, appropriate vs inappropriate applications, on-boarding, off-boarding, repair/replacement due to damage, legal concerns, internal investigations and law enforcement investigations and forensics.

ciphertext — The unintelligible and seeming random form of data that is produced by the cryptographic function of encryption. Ciphertext is produced by a symmetric algorithm when a data set is transformed by the encryption process using a selected key. Ciphertext can converted back into its original form (i.e. plain text) by performing the decryption process using the same symmetric encryption algorithm and the key used during the encryption process. (Also known as cryptogram.)

clickjacking — A malicious technique by which a victim is tricked into clicking on a URL, button or other screen object other than that intended by or perceived by the user. Clickjacking can be performed in many ways; one of which is to load a web page transparently behind another visible page in such a way that the obvious links and objects to click are facades, so clicking on an obvious link causes the hidden page's link to be selected.

cloud computing — A means to offer computing services to the public or for internal use through remote services. Most cloud computing systems are based on remote virtualization where the application or operating environment offered to customers is hosted on the cloud provider's computer hardware. There are a wide range of cloud solutions including software applications (examples include e-mail and document editing), custom code hosting (namely execution platforms and web services) as well as full system replacements (such as remote virtual services to host

databases or file storage). (See SaaS, PaaS, and IaaS.) Most forms of cloud computing are considered public cloud as they are provided by a third party. However, private cloud (internally hosted), community cloud (a group of companies' privately hosted cloud), a hosted private cloud (the cloud servers are owned and managed by a third party but hosted in the facility of the customer) and hybrid cloud (a mixture of public and private) are also options.

CND (Computer Network Defense) — The establishment of a security perimeter and of internal security requirements with the goal of defending a network against cyberattacks, intrusions and other violations. A CND is defined by a security policy and can be stress tested using vulnerability assessment and penetration testing measures.

cracker — The proper term to refer to an unauthorized attacker of computers, networks and technology instead of the misused term “hacker.” However, this term is not as widely used in the media; thus, the term hacker has become more prominent in-spite of the terms misuse. (See hacker.)

critical infrastructure — The physical or virtual systems and assets that are vital to an organization or country. If these systems are compromised, the result would be catastrophic. If an organization's mission critical processes are interrupted, this could result in the organization ceasing to exist. If a country's critical infrastructure is destroyed, it will have severe negative impact on national security, economic stability, citizen safety and health, transportation and communications.

CVE (Common Vulnerabilities and Exposures) — An online database of attacks, exploits and compromises operated by the MITRE organization for the benefit of the public. It includes all attacks and abuses known for any type of computer system or software product. Often new attacks and exploits are documented in a CVE long before a vendor admits to the issue or releases an update or patch to resolve the concern.

cryptography — The application of mathematical processes on data-at-rest and data-in-transit to provide the security benefits of confidentiality, authentication, integrity and non-repudiation. Cryptography includes three primary components: symmetric encryption, asymmetric encryption and hashing. Symmetric encryption is used to provide confidentiality. Asymmetric encryption is used to provide secure symmetric key generation, secure symmetric key exchange (via digital envelopes created using the recipient's public key) verification of source, verification/control of recipient, digital signature (a combination of hashing and use of the sender's private key) and digital certificates (which provides third-party authentication services). Hashing is the cryptographic operation that produces a representational value from an input data set. A before and after hash can be compared to detect protection of or violation of integrity.

cyberattack — Any attempt to violate the security perimeter of a logical environment. An attack can focus on gathering information, damaging business processes, exploiting flaws, monitoring targets, interrupting business tasks, extracting value, causing damage to logical or physical assets or using system resources to support attacks against other targets. Cyberattacks can be initiated through exploitation of a vulnerability in a publicly exposed service, through tricking a user into opening an infectious attachment, or even causing automated installation of exploitation tools through innocent website visits. (Also known as drive-by download.)

cyber ecosystem — The collection of computers, networks, communication pathways, software, data and users that comprise either a local private network or the world-wide Internet. It is the digital environment within which software operates and data is manipulated and exchanged.

cyberespionage — The unethical act of violating the privacy and security of an organization to leak data or disclose internal/private/confidential information. Cyberespionage can be performed by individuals, organization or governments for the direct purpose of causing harm to the violated entity to benefit individuals, organizations or governments.

cybersecurity — The efforts to design, implement, and maintain security for an organization's network, which is connected to the Internet. It is a combination of logical/technical-, physical- and personnel-focused countermeasures, safeguards and security controls. An organization's cybersecurity should be defined in a security policy, verified through evaluation techniques (such as vulnerability assessment and penetration testing) and revised, updated and improved over time as the organization evolves and as new threats are discovered.

cyber teams — Groups of professional or amateur penetration testing specialists who are tasked with evaluating and potentially improving the security stance of an organization. Common cyber teams include the red, blue and purple/white teams. A red team is often used as part of a multi-team penetration test (i.e. security evaluation), which is responsible for attacking the target which is being defended by the blue team. A purple team or white team is either used as a reference between the attack/red and defense/blue teams; or this team can be used as an interpreter of the results and activities of the red and blue teams to maximize their effectiveness in the results.

data breach — The occurrence of disclosure of confidential information, access to confidential information, destruction of data assets or abusive use of a private IT environment. Generally, a data breach results in internal data being made accessible to external entities without authorization.

data integrity — A security benefit that verifies data is unmodified and therefore original, complete and intact. Integrity is verified using cryptographic hashing. A hashing algorithm generates a fixed length output known as a hash value, fingerprint or MAC (Message Authenticating Code), which is derived from the input data, but which does not contain the input data. This makes hashing a one-way operation. A hash is calculated before an event, and another hash is calculated after the event (an event can be a time frame of storage (i.e. data-at-rest) or an occurrence of transmission (i.e. data-in-transit); the two hashes are then compared using an XOR Boolean operation. If the two hashes exactly match (i.e. the XOR result is zero), then the data has retained its integrity. However, if the two hashes do not match exactly (i.e. the XOR result is a non-zero value), then something about the data changed during the event.

data mining — The activity of analyzing and/or searching through data to find items of relevance, significance or value. The results of data mining are known as meta-data. Data mining can be a discovery of individual important data items, a summary or overview of numerous data items or a consolidation or clarification of a collection of data items.

data theft — The act of intentionally stealing data. Data theft can occur via data loss (physical theft) or data leakage (logical theft) event. Data loss occurs when a storage device is lost or stolen. Data leakage occurs when copies of data is possessed by unauthorized entities.

DDoS (Distributed Denial of Service) Attack — An attack which attempts to block access to and use of a resource. It is a violation of availability. DDOS (or DDoS) is a variation of the DoS attack (see DOS) and can include flooding attacks, connection exhaustion, and resource demand. The distinction of

DDOS from DOS is that the attack traffic may originate from numerous sources or is reflected or bounced off numerous intermediary systems. The purpose of a DDoS attack is to significantly amplify the level of the attack beyond that which can be generated by a single attack system to overload larger and more protected victims. DDoS attacks are often waged using botnets. (See botnet.)

decrypt — The act which transforms ciphertext (i.e. the unintelligible and seeming random form of data that is produced by the cryptographic function of encryption) back into its original plaintext or cleartext form. Ciphertext is produced by a symmetric encryption algorithm when a data set is transformed by the encryption process using a selected key. Ciphertext can converted back into its original form (i.e. plaintext) by performing the decryption process using the same symmetric encryption algorithm and the same key used during the encryption process.

digital certificate — A means by which to prove identity or provide authentication commonly by means of a trusted third-party entity known as a certificate authority. A digital certificate is based on the x.509 v3 standard. It is the public key of a subject signed by the private key of a certificate authority with clarifying text information such as issuer, subject identity, date of creation, date of expiration, algorithms, serial number and thumbprint (i.e. hash value).

digital forensics — The means of gathering digital information to be used as evidence in a legal procedure. Digital forensics focuses on gathering, preserving and analyzing the fragile and volatile data from a computer system and/or network. Computer data that is relevant to a security breach and/or criminal action is often intermixed with standard benign data from business functions and personal activities. Thus, digital forensics can be challenging to properly collect relevant evidence while complying with the rules of evidence to ensure that such collected evidence is admissible in court.

DLP (Data Loss Prevention) — A collection of security mechanisms which aim at preventing the occurrence of data loss and/or data leakage. Data loss occurs when a storage device is lost or stolen while data leakage occurs when copies of data is possessed by unauthorized entities. In both cases, data is accessible to those who should not have access. DLP aims at preventing such occurrences through various techniques such as strict access controls on resources, blocking the use of email attachments, preventing network file exchange to external systems, blocking cut-and-paste, disabling use of social networks and encrypting stored data.

DMZ (Demilitarized Zone) — A segment or subnet of a private network where resources are hosted and accessed by the public from the Internet. The DMZ is isolated from the private network using a firewall and is protected from obvious abuses and attacks from the Internet using a firewall. A DMZ can be deployed in two main configurations. One method is the screened subnet configuration, which has the structure of I-F-DMZ-F-LAN (i.e. internet, then firewall, then the DMZ, then another firewall, then the private LAN). A second method is the multi-homed firewall configuration, which has the structure of a single firewall with three interfaces, one connecting to the Internet, a second to the DMZ, and a third to the private LAN.

DOS (Denial of Service) — An attack that attempts to block access to and use of a resource. It is a violation of availability. DOS (or DoS) attacks include flooding attacks, connection exhaustion and resource demand. A flooding attack sends massive amounts of network traffic to the target overloading the ability of network devices and servers to handle the raw load. Connection exhaustion repeatedly makes connection requests to a target to consume all system resources related to

connections, which prevents any other connections from being established or maintained. A resource demand DoS repeatedly requests a resource from a server to keep it too busy to respond to other requests.

drive-by download — A type of web-based attack that automatically occurs based on the simple act of visiting a malicious or compromised/poisoned Web site. A drive-by download is accomplished by taking advantage of the default nature of a Web browser to execute mobile code, most often JavaScript, with little to no security restrictions. A drive-by download can install tracking tools, remote access backdoors, botnet agents, keystroke loggers or other forms of malicious utilities. In most cases, the occurrence of the infection based on the drive-by download is unnoticed by the user/victim.

eavesdropping — The act of listening in on a transaction, communication, data transfer or conversation. Eavesdropping can be used to refer to both data packet capture on a network link (also known as sniffing or packet capture) and to audio recording using a microphone (or listening with ears).

encode — The act which transforms plaintext or cleartext (i.e. the original form of normal standard data) into ciphertext (i.e. the unintelligible and seeming random form of data that is produced by the cryptographic function of encryption). Ciphertext is produced by a symmetric encryption algorithm when a data set is transformed by the encryption process using a selected key (i.e. to encrypt or encode). Ciphertext can converted back into its original form (i.e. plaintext) by performing the decryption process using the same symmetric encryption algorithm and the same key used during the encryption process (i.e. decrypt or decode).

encryption key — The secret number value used by a symmetric encryption algorithm to control the encryption and decryption process. A key is a number defined by its length in binary digits. Generally, the longer the key length, the more security (i.e. defense against confidentiality breaches) it provides. The length of the key also determines the key space, which is the range of values between the binary digits being all zeros and all ones from which the key can be selected.

firewall — A security tool, which may be a hardware or software solution that is used to filter network traffic. A firewall is based on an implicit deny stance where all traffic is blocked by default. Rules, filters or ACLs can be defined to indicate which traffic can cross the firewall. Advanced firewalls can make allow/deny decisions based on user authentication, protocol, header values and even payload contents.

hacker — A person who has knowledge and skill in analyzing program code or a computer system, modifying its functions or operations and altering its abilities and capabilities. A hacker may be ethical and authorized (the original definition) or may be malicious and unauthorized (the altered but current use of the term). Hackers can range from professionals who are skilled programmers to those who have little to no knowledge of the specifics of a system or exploit but who can follow directions; in this instance, they are called script kiddies.

hacktivism — Attackers who hack for a cause or belief rather than some form of personal gain. Hacktivism is often viewed by attackers as a form of protest or fighting for their perceived "right" or "justice." However, it is still an illegal action in most cases when the victim's technology or data is abused, harmed or destroyed.

honeypot — A trap or decoy for attackers. A honeypot is used to distract attackers to prevent them from attacking actual production systems. It is a false system that is configured to look and function as a production system and is positioned where it would be encountered by an unauthorized entity who is seeking out a connection or attack point. A honeypot may contain false data to trick attackers into spending considerable time and effort attacking and exploiting the false system. A honeypot may also be able to discover new attacks or the identity of the attackers.

IaaS (Infrastructure-as-a-Service) — A type of cloud computing service where the provider offers the customer the ability to craft virtual networks within their computing environment. An IaaS solution enables a customer to select which operating systems to install into virtual machines/nodes as well as the structure of the network including use of virtual switches, routers and firewalls. It also provides complete freedom as to the software or custom code run on the virtual machines. An IaaS solution is the most flexible of all the cloud computing services; it allows for significant reduction in hardware by the customer in their own local facility. It is the most expensive form of cloud computing service.

identity cloning — A form of identity theft in which the attacker takes on the identity of a victim and then attempts to live and act as the stolen identity. Identity cloning is often performed to hide the birth country or a criminal record of the attacker to obtain a job, credit or other secured financial instrument.

identity fraud — A form of identity theft in which a transaction, typically financial, is performed using the stolen identity of another individual. The fraud is due to the attacker impersonating someone else.

IDS (Intrusion Detection System) — A security tool that attempts to detect the presence of intruders or the occurrence of security violations to notify administrators, enable more detailed or focused logging or even trigger a response such as disconnecting a session or blocking an IP address. An IDS is considered a more passive security tool as it detects compromises after they are already occurring rather than preventing them from becoming successful.

information security policy — A written account of the security strategy and goals of an organization. A security policy is usually comprised of standards, policies (or SOPs – Standard Operating Procedures) and guidelines. All hardware, software, facilities and personnel must abide by the terms of the security policy of an organization. (Also known as security policy.)

insider threat — The likelihood or potential that an employee or another form of internal personnel may pose a risk to the stability or security of an organization. An insider has both physical access and logical access (through their network logon credentials). These are the two types of access that an outside attacker must first gain before launching malicious attacks whereas an insider already has both forms of access. Thus, an insider is potentially a bigger risk than an outsider if that insider goes rogue or is tricked into causing harm.

IPS (Intrusion Prevention System) — A security tool that attempts to detect the attempt to compromise the security of a target and then prevent that attack from becoming successful. An IPS is considered a more active security tool as it attempts to proactively respond to potential threats. An IPS can block IP addresses, turn off services, block ports and disconnect sessions as well as notify administrators.

ISP (Internet Service Provider) — The organization that provides connectivity to the Internet for individuals or companies. Some ISPs offer additional services above that of just connectivity such as e-mail, web hosting and domain registration.

JBOH (JavaScript-Binding-Over-HTTP) — A form of Android-focused mobile device attack that enables an attacker to be able to initiate the execution of arbitrary code on a compromised device. A JBOH attack often takes place or is facilitated through compromised or malicious apps.

keylogger — Any means by which the keystrokes of a victim are recorded as they are typed into the physical keyboard. A keylogger can be a software solution or a hardware device used to capture anything that a user might type in including passwords, answers to secret questions or details and information form e-mails, chats and documents.

LAN (Local Area Network) — An interconnection of devices (i.e. a network) that is contained within a limited geographic area (typically a single building). For a typical LAN, all the network cables or interconnection media is owned and controlled by the organization unlike a WAN (Wide Area Network) where the interconnection media is owned by a third party.

link jacking — A potentially unethical practice of redirecting a link to a middle-man or aggregator site or location rather than the original site the link seemed to indicate it was directed towards. For example, a news aggregation service may publish links that seem as if they point to the original source of their posted articles, but when a user discovers those links via search or through social networks, the links redirect back to the aggregation site and not the original source of the article.

malware (malicious software) — Any code written for the specific purpose of causing harm, disclosing information or otherwise violating the security or stability of a system. Malware includes a wide range of types of malicious programs including: virus, worm, Trojan horse, logic bomb, backdoor, Remote Access Trojan (RAT), rootkit, ransomware and spyware/adware.

outsider threat — The likelihood or potential that an outside entity, such as an ex-employee, competitor or even an unhappy customer, may pose a risk to the stability or security of an organization. An outsider must often gain logical or physical access to the target before launching malicious attacks.

outsourcing — The action of obtaining services from an external entity. Rather than performing certain tasks and internal functions, outsourcing enables an organization to take advantages of external entities that can provide services for a fee. Outsourcing is often used to obtain best-of-breed level service rather than settling for good-enough internal operations. It can be expensive and increases an organization's security risk due to the exposure of internal information and data to outsiders.

OWASP (Open Web Application Security Project) — An Internet community focused on understanding web technologies and exploitations. Their goal is to help anyone with a website improve the security of their site through defensive programming, design and configuration. Their approach includes understanding attacks to know how to defend against them. OWASP offers numerous tools and utilities related to website vulnerability evaluation and discovery as well as a significant amount of training and reference material related to all thing's web security.

PaaS (Platform-as-a-Service) — A type of cloud computing service where the provider offers the customer the ability to operate custom code or applications. A PaaS operator determines which operating systems or execution environments are offered. A PaaS system does not allow the customer to change operating systems, patch the OS or alter the virtual network space. A PaaS system allows the customer to reduce hardware deployment in their own local facility and to take advantage of on-demand computing (also known as pay as you go).

packet sniffing — The act of collecting frames or packets off a data network communication. This activity allows the evaluation of the header contents as well as the payload of network communications. Packet sniffing requires that the network interface card be placed into promiscuous mode to disable the MAC (Media Access Control) address filter which would otherwise discard any network communications not intended for the specific local network interface. (Also known as sniffing or eavesdropping.)

patch — An update or change or an operating system or application. A patch is often used to repair flaws or bugs in deployed code as well as introduce new features and capabilities. It is good security practice to test all updates and patches before implementation and attempt to stay current on patches to have the latest version of code that has the fewest known flaws and vulnerabilities.

patch management — The management activity related to researching, testing, approving and installing updates and patches to computer systems, which includes firmware, operating systems and applications. A patch is an update, correction, improvement or expansion of an existing software product through the application of new code issued by the vendor. Patch management is an essential part of security management to prevent downtime, minimize vulnerabilities and prevent new untested updates from interfering with productivity.

payment card skimmers — A malicious device used to read the contents of an ATM, debit or credit card when inserted into a POS (Point of Sale) payment system. A skimmer may be an internal component or an external addition. An attacker will attempt to use whatever means to imbed their skimmer into a payment system that will have the highest likelihood of not being detected and thus gather the most amount of financial information from victims. (See POS intrusions.)

pen testing — A means of security evaluation where automated tools and manual exploitations are performed by security and attack experts. This is an advanced form of security assessment that should only be used by environments with a mature security infrastructure. A penetration test will use the same tools, techniques and methodologies as criminal hackers, and thus, it can cause downtime and system damage. However, such evaluations can assist with securing a network by discovering flaws that are not visible to automated tools based on human (i.e. social engineering) or physical attack concepts. (Also known as penetration testing or ethical hacking.)

phishing — A social engineering attack that attempts to collect information from victims. Phishing attacks can take place over e-mail, text messages, through social networks or via smart phone apps. The goal of a phishing attack may be to learn logon credentials, credit card information, system configuration details or other company, network, computer or personal identity information. Phishing attacks are often successful because they mimic legitimate communications from trusted entities or groups such as false emails from a bank or a retail website.

PKI (Public Key Infrastructure) — A security framework (i.e. a recipe) for using cryptographic concepts in support of secure communications, storage and job tasks. A PKI solution is a combination of symmetric encryption, asymmetric encryption, hashing and digital certificate-based authentication.

POS (Point of Sale) intrusions — An attack that gains access to the POS (Point of Sale) devices at a retail outlet enabling an attacker to learn payment card information as well as other customer details. POS intrusions can occur against a traditional brick-and-mortar retail location as well as any online retail websites. (See payment card skimmers.)

ransomware — A form of malware that holds a victim's data hostage on their computer typically through robust encryption. This is followed by a demand for payment in the form of Bitcoin (an untraceable digital currency) to release control of the captured data back to the user.

restore — The process of returning a system back to a state of normalcy. A restore or restoration process may involve formatting the main storage device before re-installing the operating system and applications as well as copying data from backups onto the reconstituted system.

risk assessment — The process of evaluating the state of risk of an organization. Risk assessment is often initiated through taking an inventory of all assets, assigning each asset a value, and then considering any potential threats against each asset. Threats are evaluated for their exposure factor (EF) (i.e. the amount of loss that would be caused by the threat causing harm) and frequency of occurrence (i.e. ARO—Annualized Rate of Occurrence) to calculate a relative risk value known as the ALE (Annualized Loss Expectancy). The largest ALE indicates the biggest concern or risk for the organization.

risk management — The process of performing a risk assessment and evaluating the responses to risk to mitigate or otherwise handle the identified risks. Countermeasures, safeguards or security controls are to be selected that may eliminate or reduce risk, assign or transfer risk to others (i.e. outsourcing or buying insurance) or avoid and deter risk. The goal is to reduce risk down to an acceptable or tolerable level.

SaaS (Software-as-a-Service) — A type of cloud computing service where the provider offers the customer the ability to use a provided application. Examples of a SaaS include online e-mail services or online document editing systems. A user of a SaaS solution is only able to use the offered application and make minor configuration tweaks. The SaaS provider is responsible for maintaining the application.

sandboxing — A means of isolating applications, code or entire operating systems to perform testing or evaluation. The sandbox limits the actions and resources available to the constrained item. This allows for the isolated item to be used for evaluation while preventing any harm or damage to be caused to the host system or related data or storage devices.

SCADA (Supervisory Control and Data Acquisition) — A complex mechanism used to gather data and physical world metrics as well as perform measurement or management actions of the monitored systems for the purposes of automatic large complex real-world processes such as oil refining, nuclear power generation or water filtration. SCADA can provide automated control over very large complex systems whether concentrated in a single physical location or spread across long distances.

security control — Anything used as part of a security response strategy which addresses a threat to reduce risk. (Also known as countermeasure or safeguard.)

security perimeter — The boundary of a network or private environment where specific security policies and rules are enforced. The systems and users within the security boundary are forced into compliance with local security rules while anything outside is not under such restrictions. The security perimeter prevents any interactions between outside entities and internal entities that might violate or threaten the security of the internal systems.

SIEM (Security Information and Event Management) — A formal process by which the security of an organization is monitored and evaluated on a constant basis. SIEM helps to automatically identify systems that are out of compliance with the security policy as well as to notify the IRT (Incident Response Team) of any security violating events.

sniffing — See packet sniffing and eavesdropping.

social engineering — An attack focusing on people rather than technology. This type of attack is psychological and aims to either gain access to information or to a logical or physical environment. A social engineering attack may be used to gain access to a facility by tricking a worker into assisting by holding the door when making a delivery, gaining access into a network by tricking a user into revealing their account credentials to the false technical support staff or gaining copies of data files by encouraging a worker to cut-and-paste confidential materials into an e-mail or social networking post.

SPAM — A form of unwanted or unsolicited messages or communications typically received via e-mail but also occurring through text messaging, social networks or VoIP. Most SPAM is advertising, but some may include malicious code, malicious hyperlinks or malicious attachments.

spear phishing — A form of social engineering attack that is targeted to victims who have an existing digital relationship with an online entity such as a bank or retail website. A spear phishing message is often an e-mail although there are also text message and VoIP spear phishing attacks as well, which looks exactly like a legitimate communication from a trusted entity. The attack tricks the victim into

clicking on a hyperlink to visit a company website only to be re-directed to a false version of the website operated by attackers. The false website will often look and operate similarly to the legitimate site and focus on having the victim provide their logon credentials and potentially other personal identity information such as answers to their security questions, an account number, their social security number, mailing address, email address and/or phone number. The goal of a spear phishing attack is to steal identity information for account takeover or identity theft.

spoof (spoofing) — The act of falsifying the identity of the source of a communication or interaction. It is possible to spoof IP address, MAC address and email address.

spyware — A form of malware that monitors user activities and reports them to an external their party. Spyware can be legitimate in that it is operated by an advertising and marketing agency for gathering customer demographics. However, spyware can also be operated by attackers using the data gathering tool to steal an identity or learn enough about a victim to harm them in other ways.

supply chain — The path of linked organizations involved in the process of transforming original or raw materials into a finished product that is delivered to a customer. An interruption of the supply chain can cause a termination of the production of the final product immediately or this effect might not be noticed until the materials already in transit across the supply chain are exhausted.

threat assessment — The process of evaluating the actions, events and behaviors that can cause harm to an asset or organization. Threat assessment is an element of risk assessment and management. (Also known as threat modeling and threat inventory.)

Trojan Horse (Trojan) — A form of malware where a malicious payload is imbedded inside of a benign host file. The victim is tricked into believing that the only file being retrieved is the viewable benign host. However, when the victim uses the host file, the malicious payload is automatically deposited onto their computer system.

two-factor authentication — The means of proving identity using two authentication factors usually considered stronger than any single factor authentication. A form of multi-factor authentication. Valid factors for authentication include Type 1: Something you know such as passwords and PINs; Type 2: Something you have such as smart cards or OTP (One Time Password) devices; and Type 3: Someone you are such as fingerprints or retina scans (aka biometrics).

two-step authentication — A means of authentication commonly employed on websites as an improvement over single factor authentication but not as robust as two-factor authentication. This form of authentication requires the visitor provide their username (i.e. claim an identity) and password (i.e. the single factor authentication) before performing an additional step. The additional step could be receiving a text message with a code, then typing that code back into the website for confirmation. Alternatives include receiving an e-mail and needing to click on a link in the message for confirmation or viewing a pre-selected image and statement before typing in another password or PIN. Two-step is not as secure as two-factor because the system provides one of the factors to the user at the time of logon rather than requiring that the user provide both.

unauthorized access — Any access or use of a computer system, network or resource which is in violation of the company security policy or when the person or user was not explicitly granted authorization to access or use the resource or system

VPN (Virtual Private Network) — A communication link between systems or networks that is typically encrypted to provide a secured, private, isolate pathway of communications.

virus — A form of malware that often attaches itself to a host file or the MBR (Master Boot Record) as a parasite. When the host file or MBR is accessed, it activates the virus enabling it to infect other objects. Most viruses spread through human activity within and between computers. A virus is typically designed to damage or destroy data, but different viruses implement their attack at different rates, speeds or targets. For example, some viruses attempt to destroy files on a computer as quickly as possible while others may do so slowly over hours or days. Others might only target images or Word documents (.doc/.docx).

vishing — A form of phishing attack which takes place over VoIP. In this attack, the attacker uses VoIP systems to be able to call any phone number with no toll-charge expense. The attacker often falsifies their caller-ID to trick the victim into believing they are receiving a phone call from a legitimate or trustworthy source such as a bank, retail outlet, law enforcement or charity. The victims do not need to be using VoIP themselves to be attacked over their phone system by a vishing attack. (See phishing.)

vulnerability — Any weakness in an asset or security protection which would allow for a threat to cause harm. It may be a flaw in coding, a mistake in configuration, a limitation of scope or capability, an error in architecture, design, or logic or a clever abuse of valid systems and their functions.

whitelist — A security mechanism prohibiting the execution of any program that is not on a pre-approved list of software. The whitelist is often a list of the file name, path, file size and hash value of the approved software. Any code that is not on the list, whether benign or malicious, will not be able to execute on the protected system. (See blacklist.)

Wi-Fi — A means to support network communication using radio waves rather than cables. The current Wi-Fi or wireless networking technologies are based on the IEE 802.11 standard and its numerous amendments, which address speed, frequency, authentication and encryption.

worm — A form of malware that focuses on replication and distribution. A worm is a self-contained malicious program that attempts to duplicate itself and spread to other systems. Generally, the damage caused by a worm is indirect and due to the worm's replication and distribution activities consuming all system resources. A worm can be used to deposit other forms of malware on each system it encounters.

zombie — A term related to the malicious concept of a botnet. The term zombie can be used to refer to the system that is host to the malware agent of the botnet or to the malware agent itself. If the former, the zombie is the system that is blinding performing tasks based on instructions from an

external and remote hacker. If the latter, the zombie is the tool that is performing malicious actions such as DoS flooding, SPAM transmission, eavesdropping on VoIP calls or falsifying DNS resolutions as one member of a botnet.

Appendix B – NIST Detailed Framework

This section is a detailed explanation of the framework, its functions and associated activities.

1. Identify

This section deals with the defining and developing the organization understanding that is required to manage cybersecurity. The categories in this section we will be addressing are:

Category	Description
Business Operating Environment	Understanding the operating environment for every department and they can impact or be impacted by cybersecurity.
Asset Management	Understanding the assets, we are trying to protect as part of this plan.
Governance	Identifying the various roles and responsibilities from council and management to full-time and part-time employees. It also includes the various committees and their mandates.
Risk Management	This includes having an overall strategy to manage risk as well as identifying all cybersecurity risks and potential mitigations.

2. Protect

Probably the function requiring the most attention. It includes all the activities conducted to provide safeguards in protecting our assets. They include

Category	Description
Policies, Processes and Procedure	These are the complete set of policies and processes that guide us in managing cybersecurity. They include: • Acceptable IT use Policy • Mobile Policy • Patch Management Policy • Training & Awareness Policy • Onboarding/Offboarding policies • Various IT System Policies It also includes processes and procedures for tracking issues and reporting incidents.

Training and Awareness	The most important and often overlooked activity. It includes mandatory training for all employees as well as awareness activities and resources for all employees and citizens.
Access Controls	This includes management of access of all City assets from buildings to specific systems and data/information.
Information Protection	This includes all activities to ensure the City's information is properly protected including privacy issues.
Protective Technology	This includes the infrastructure, systems, services and applications used to safeguard our networks, equipment, applications and people
Maintenance & Operations	Includes all the maintenance work required to keep systems and equipment up to date including patching, updates and upgrades.

2. Detect

This function deals with developing the activities required for detecting potential cyber events.

Category	Description
System Monitoring	This deals with the activities required to ensure systems are being monitored appropriately.
Detecting Events	This activity is tied with monitoring and deals with the timely detection of anomalies and potential events
Detection Processes	Deals with what is done when certain events are detected.

Respond

This function deals with the activities that are performed in the event a cyber event has occurred.

Category	Description
Response Planning	Deals with documenting the steps to be taken in the event of a cyber incident.
Communications	Deals with the communications that are required during an event including stakeholders and speaking points. Usually documented in the Response Plan
Analysis	Deals with the work involved in analyzing the problem as well as temporary and longer-term solutions to return to normal operations.

Mitigations	These are the fore mentioned temporary solutions put in place to minimize the impact of the event on staff. Not always required

Recover

This function deals with the steps taken after an incident.

Category	Description
Recovery Planning	Deals with documenting the steps to be taken in the event of a cyber incident. Often coupled with Response planning
Communications	Deals with the communications that are required during an event including stakeholders and speaking points. Usually documented in the Response/Recovery Plan
Post-Mortem Review	This is a complete review of the incidents and recommendations for the future
Incident Reporting	This is the complete report of the incident, including the post-mortem.

Current and target Maturity

To properly align to any framework and/or maximize our investments while minimizing our risks, it is important to look at how we manage cyber risks today vs. how we would like to do tomorrow. The framework identifies these as Tiers and profiles. Although they are not a maturity scale in the strictest definition, they do provide an industry standard approach to measure our capacity to measure cyber risks and practices. We will perform multiple activities to understand where we are and where we want to be. These are identified in the Detailed Plan.