Cybersecurity - Executive Overview

Revised - 2018

This overview provides a summary of the City of Westminster's Cybersecurity program. While not meant to be all inclusive, this document will provide a high-level view of the critical elements the City has included in its Cybersecurity plan and activities, and contains a few examples of current security applications in use. This program is based on industry best practices, and is refined and enhanced as best practices, funding and resources permit.

A periodic assessment and evaluation of risks is essential to any cybersecurity program. On an annual basis, the City conducts two audits of Information Technology systems and controls. The first is a required information technology audit conducted by the City's third party financial auditors. The second, a voluntary and much more comprehensive audit, is conducted by an outside information technology security firm specializing in auditing, penetration testing, vulnerability scanning and social engineering awareness testing. The results of these audits have helped the City establish best practices in many areas of cybersecurity. Elements of the City cybersecurity plan and activities supporting those elements are summarized below.

1) Documentation – including security policies, audit assessment reports and recommendations, and contingency planning
    a. The City has established and implemented a set of security policies and documents covering a broad list of security topics, including backups, offsite storage, disaster recovery, incident handling, and network security. The City has worked extensively to model these policies and documents on the NIST Cybersecurity Framework. This framework, mandated by Presidential Executive Order 13636, provides policy guidance for how organizations can assess and improve their ability to prevent, detect, and respond to cyberattacks. These policies include: management controls, operational controls, and technical controls.
2) Roles and Responsibilities
    a. In 2017 the City authorized the creation of a Cybersecurity Administrator position reporting to the Systems Manager. This position was fully staffed in 2018. An individual serving in this position must possess the skills necessary to help in guiding the organization in the area of systems security and is the City's point person for system security incident handling. Along with the Security Administrator position, the City also authorized a .5 FTE Security Apprentice that will help maintain the City's security infrastructure.
3) Identification and Authentication
    a. The City enforces password policies including aging and account lockout. Additionally, since IT employees have extended permissions and access, they are all assigned two factor authentication, eliminating the risks associated with compromised passwords on accounts with administrator rights.
        i. The City is currently testing applications such as an inline password filter, that will help prevent easily compromised passwords from being used, and to assist the end user in creating a stronger password.

b. Password resets by service desk employees are done only upon verification of the identity of the requesting user.
c. Accounts are locked after a fixed number of invalid login attempts, and an automatic email is generated for IT staff investigations. Reports on failed login attempts and account lockouts are also automatically generated daily and emailed to the appropriate IT staff.
d. In 2017, IT introduced the self-service Password Reset program that allows employees to register their phones to receive text prompts for password resets.

4) Account Management and Access Controls
    a. Active directory accounts are added and deleted automatically as employees are added and removed from the City's human resources/payroll system. This in-house created application insures that active directory accounts are available only for current employees.
    b. The City uses the principle of least privilege when setting up new users, and access is given only to those systems needed to accomplish the functions of that job.
    c. Networks are engineered with the 802.1x protocol and virtual network settings to restrict access based on user privileges.
5) Session Controls
    a. The City enforces password protected screen savers and timed automatic locks on computers.
    b. Internal audits are conducted to insure computers are not left unlocked in unoccupied areas.
6) External Connectivity Controls
    a. The City uses multiple firewalls, DMZs, virtual network configurations, authentication and more to control external access to systems.
        i. Cisco's ASA Firewall and FirePower: This best in class hardware firewall combines firewall functionality with intrusion prevention, advanced malware protection, URL filtering and virtual private network (VPN) capabilities. This technology provides IT with the ability to monitor and control activity on the network and detect and track malware attempts.
        ii. Network Demilitarized Zone (DMZ): The DMZ provides a separate network location for those computers that are public facing, so that they are kept isolated from the private internal network. Any successful cybersecurity attack in the DMZ will not impact the internal network or services. Furthermore, users of public facing applications cannot access the city's internal network and resources. This configuration better protects inside devices from possible attack.
        iii. Internal Network Segmentation: Much like the DMZ, the City also segments networks that need additional security based on requirements. These include SCADA (utility management and control), Public Safety, and Library services. These secure networks are attached through their own separate routing platform and are only available to the Intranet via an additional ASA Firewall. This further elevates protection from unauthorized access to systems and data.

iv. Intranet Security via 802.1x: The City's internal network is available to City owned devices only. Utilizing a special network protocol (802.1x), the City can guarantee that only devices owned by the City and used by an authorized employee can gain access to internal resources. In other words, a terminated employee or outsider is restricted from gaining access to City systems and data through a city owned or personal owned device even when physically connected to a network port.

b. Annual security audits include penetration testing to validate external access controls are configured properly and working as intended.

7) Contingency and backup plans
   a. The City has a disaster recovery hot-site located in a City facility. This site includes backup plans and documentation to reference in the event the disaster recovery data center needs to be brought into production due to a disaster or cyberattack.
   b. Full disaster recovery testing is completed each year to confirm operations of the center and to enhance recovery procedures.
   c. The city also has a recovery site of compressed data backups outside city limits as a tertiary back up.
8) Virus Protection
   a. The City uses multiple antivirus solutions plus an email scanning solution to best protect the City from inbound malicious email and attachments. These solutions provide a layered security approach that has been very effective at minimizing the introduction of viruses into the City.
      i. Google (Postini) Message Security: This application provides filtering services for City email. It protects the city from viruses, malware, ransomware, encrypted emails and executables. Better than 90% of all email bound for City employee inboxes is identified as spam or email containing harmful viruses, malware and ransomware, and is quarantined outside of the City's network.
      ii. Mailsweeper: For email that was not quarantined by Google/Postini, Mailsweeper provides a second layer of filtering services for inbound City email. This service further protects the city from viruses, malware, ransomware, encrypted emails and executables, and has been effective at stopping some "zero-day" viruses that are not quarantined by Google/Postini. This is an on-premise application administered by the IT Department.
      iii. Trend Micro™ Deep Security Anti-virus: Trend Micro™ Deep Security™ provides advanced server security for physical, virtual, and cloud servers. It protects enterprise applications and data from ransomware, breaches, and business disruptions without requiring emergency patching.
      iv. Trend Micro™ OfficeScan: This fourth and final layer of protection provides anti-virus services for the City's desktop and laptop infrastructure. The OfficeScan product provides endpoint antivirus/antimalware, antispyware, antiransomware and threat protection using cloud-based global threat intelligence.
9) Auditing
   a. The City uses several auditing solutions to create logs for IT security staff to use proactively and in review of any incidents.

i. Nessus: The City uses Nessus as a remote security scanning tool, which scans a computer, group of computers or an entire network and raises an alert if the application discovers any vulnerabilities that malicious hackers could use to gain access to city resources.
ii. AD Auditor Plus: The City uses AD Auditor Plus to audit the Active Directory (AD) environment, containing user and computer accounts, users and permissions, password, and other critical information. With this tool, assigned and authorized administrators can determine if unauthorized changes or additions have been made within the AD environment.
iii. Exchange Reporter Plus: The City uses Exchange Reporter Plus to oversee the city's email infrastructure and immediately notify IT administrators of any changes to permissions and security settings.
iv. File Server Resource Manager: This tool allows us to proactively monitor all our file servers for indications of a ransomware attack, and to immediately act to prevent further damage.
v. The City is also investigating tools such as a SIEM (Security Information and Event Management) to aggregate a variety of information sources into one dashboard to be able to more quickly identify anomalies or threats.

10) Maintenance and configuration management
    a. A change management system and team is in place to test and validate updates prior to releasing to production computers.
    b. Development and test environments are separate from production environments.
    c. Timely application of security patches is done for networks and systems. Patch level testing is done internally and during the third party security audit.
    d. Audit reports are used every year to assess and further fortify networks and systems.
11) Media Sanitization and Disposal
    a. Decommissioned PCs are wiped using DOD multiple wipe software prior to donation.
    b. Decommissioned SAN disk drives are securely stored and then shredded onsite by a third-party firm while an IT staff member is present.
    c. Sensitive documents throughout the City are shredded before disposal.
12) Physical Environment
    a. Servers in both the disaster recovery data center and production data center are secured in a locked room with restricted card key access. Systems are also protected from environmental threats such as fires or floods.
    b. Video surveillance is set up in both the disaster recovery data center and production data center with automatic email delivery to multiple IT staff members when motion is detected during periods when the room should be unoccupied.
13) Personnel Security
    a. All prospective employees are required to pass a complete background and criminal history background check prior to employment.
    b. All current and new employees are required to complete Cybersecurity awareness training.

        i. SANS Advanced Cybersecurity Learning Platform (ACLP) training is required in order to reduce the risk of social engineering attacks and to raise awareness in all areas of cybersecurity.
    c. IT Staff along with other personnel are required to take the FBI CJIS (Criminal Justice Information Services) training every other year or as required by their position.
    d. New employee orientation includes discussion of technology related policies ensuring a security focus from the beginning of their employment.
    e. The City has specific policies and requirements for vendor and contractor physical and virtual access to City systems.

14) Software
    a. The City has established software development standards incorporating best practices for building applications that are secure and fortified against cyberattacks.
    b. Vendors providing software solutions to the City are required to provide the City guarantees that their software is void of back doors and other vulnerabilities.
    c. Vendors needing City data to complete software implementations and maintenance are required to sign a non-disclosure agreement protecting the data they receive.