1 North San Antonio Road
Los Altos, California 94022-3087

M E M O R A N D U M

DATE: March 17, 2022

TO: Financial Commission

CC: Jon Maginot, Assistant City Manager

FROM: Andrew Tseng, IT Manager

SUBJECT: CYBERSECURITY

This memo provides an overview of the cybersecurity measures taken by the City to protect the City employees and elected officials who utilize the City's Information Technology resources from cyberthreats. Hardware, software, insurance, and human factors are the four major elements to securing our IT environment. The overall goal is to avoid any unauthorized data access, or any data loss caused by bad actors such as hackers or even inadvertently by our own staff. Although certain information kept by the City's IT systems is subject to PRA requests, we highly value privacy and protect it as permitted by law. The City's IT Division seeks continuous support from City Council for funding and staffing to maintain a balanced workload and continue to modernize our hardware and software resources.

[Hardware]

Firewalls, Backup Appliances, Cloud storage, Message Archiver, VPN Gateway, Door Access Control

Both inbound and outbound network traffic is inspected by firewalls. Most of the malicious attempts to intrude our internal network are filtered and blocked by the firewalls. With an active subscription for security updates and protection services, City firewalls constantly receive complete zero-day protection as well as up-to-date threat emulation and extraction features. Multiple network ports are used by the firewall, creating a barrier to protect certain data from being accessed by unauthorized users.

The City's Backup appliance backups critical servers' images on a regular basis. The images are also sent to a dedicated and secured cloud storage for offsite backup. IT staff have performed actual image recovery from those images to prove the backups are in reliable, working condition.

Message archiver serves as a centralized storage of the City's email communication. A copy of every inbound and outbound email is kept on the local archiver; a second copy is saved in a secured cloud storage for geo-redundancy.

VPN gateway is used for Staff's remote connection. VPN connection software is only used by authorized users and only on City-issued devices. Remote access is made available for contract employees or external partners such as auditors and consultants through a VPN channel separate from internal staff's VPN gateway. Moreover, a separate VPN system different from non-PD users is dedicated for PD's vehicles and personnel.

Door access control systems create another layer of physical control and protection to City staff as well as IT systems. City Hall and Recreation buildings are equipped with door access system. The City is currently expanding door access systems to Police and Maintenance buildings.

The above-mentioned hardware provides a physical layer of protection for staff from cyberattacks. All of these protections require committed funding to maintain, upgrade and operate. Therefore, it is crucial to continually fund these needs.

[Software]

Endpoint protection, Windows Updates, Disk Encryption, Password policy, Multifactor Authentication, System Monitoring, Access Control, Network and Data Protection, Mobile Device Management

We should all acknowledge that there is no perfect computer application or operation system. No system is completely flawless. Therefore, constantly applying updates and security patches is necessary for each end-user device. It is IT's responsibility to make sure antivirus and antimalware software is properly installed before a computer is issued to any users. On the other hand, it is the user's responsibility to setup a password with required length and complexity, and to change it at least every 180 days as per the Electronic Use Policy. Hard drives in all laptops and tablets are encrypted to prevent data loss caused by theft or device loss.

According to NIST (National Institute of Standards and Technology), the definition of MFA (multifactor authentication) is using two or more factors to achieve authentication. Factors are (i) something you know (e.g., password/personal identification number); (ii) something you have (e.g., cryptographic identification device, token); and (iii) something you are (e.g., biometric). MFA is required by City's various critical systems or when the server detects new devices or any anomalies.

Multiple monitoring software systems are used to detect events such as failed logons, server unresponsiveness, mass deletion of files, or member changes in an administrator group. IT receives alerts and responds to these alerts depending on the level of urgency. Besides being backed up, the City's file servers have daily snapshots taken for instant recovery and have a replication partner to keep additional copies in multiple locations, including an air-gapped storage.

MDM (mobile device management) is another powerful tool for IT not only to support users remotely, but also to have the option to execute remote-wipe when a device is lost.

[Insurance]

Business Continuity Service, Cyber Insurance, Routine Penetration Tests

The City has an active cyber insurance policy in place to cover the potential loss due to data breach or cyberattack incidents such as a ransomware attack. Besides, the City also maintains an agreement to have prioritized access to certain IT resources in the event of emergency or datacenter damage. As part of the auditing processes, IT works with external partners to perform routine penetration tests to get real-word results with all protection measures implemented.

[Human Factor]

Password, Shared Accounts, Incident Response, Cybersecurity Awareness Training, IT Staffing

The City has an Electronic Use Policy in place that governs the password complexity and the frequency of changing the password. As mentioned earlier, multi-factor authentication is required for certain systems to strengthen the account security. IT also provides convenient ways for users to open a ticket and report an incident such as suspicious emails, phishing attempts, etc. The use of shared accounts is generally discouraged if individual accounts can be used. If a shared account must be used (due to license constraint, for example), then a strong and complex password is used.

In order to keep users aware of rapidly changing threats, the City uses an external partner to provide cybersecurity awareness training. Staff are required to attend training by watching on-demand video clips to make sure all are aware of different types of threats to our IT environment. In addition, phishing email campaigns are carried out every few months, to keep users alert.

Currently, the IT Division has three full-time employees and one part-time technician. Staffing has been a challenge especially during the pandemic and in the post-COVID19 era. It takes time to interview, hire and train this part-time employee however it's also difficult to retain the technician because of limited work hours and pay. Although IT has tried to automate processes and generate routine reports from various systems, there are still simple needs such as reading and analyzing the reports and responding accordingly. The gaps between the workloads and IT's available resources need to be filled by adding additional headcount. The ideal size of IT organization is to have 4.5 to 5 FTE (full-time equivalent) positions to support all City functions.

Conclusion and Recommendations

By following best practices and keeping hardware and software up-to-date, IT Division's provides and maintains a safe and secure IT environment for staff to work efficiently. Cybersecurity insurance adds another layer of protection to maintain the City's business continuity and peace of mind in the event of cyberattacks at any level. Additionally, the effort to minimize human errors always plays an increasingly important role to maintain cybersecurity, which can be achieved by training (and retraining) our staff regularly.