SFMTA

Cybersecurity Roadmap

William Stuart, Principal Security Manager

July 24th, 2018

Where we are today…

- People
  - Seem to care and are receptive
  - End-user/Admin training missing, gaps in knowledge
- Process
  - Policies need updating
  - Information System lifecycle needs improvement
  - Vendor security review process needs updating
- Technology
  - Some security tools in place
  - Firewall Design should be strengthened
  - IT user creation needs standardization
  - Software patching continues to improve

*Compared to other, similarly situated, organizations…**THIS IS NORMAL!***

Recent Developments...

- COIT Cybersecurity Policy (COIT-CP)
  - Specifies Roles and Responsibilities
  - Includes timelines for completion of certain policy documents, including a department level Cybersecurity Policy and COOP.
  - Recommends NIST Cybersecurity Framework
- AB375–California Consumer Privacy Act (CCPA)
  - Public's right to know what information is shared
  - Public's right to opt-out and to have certain data deleted
  - Public's right to know what the data will be used for
  - Civil and criminal penalties for misuse or mishandling
- Privacy First Amendment (PFA)
  - A framework for future ordinances and regulations about privacy
  - Encourages City Agencies to actively protect the privacy of our residents.
  - Encourages City Agencies to consider privacy when writing contracts or issuing permits.

The way forward...

- Improve Vulnerability Management (CCPA)
  - Run penetration test (completed and remediated)
  - Older servers
    - Retire, upgrade, or remediate (In Progress)
  - Patch Management
    - Create actionable vulnerability reports (In Progress)
    - Centralize patch deployment (Completed)
- Refresh Firewall Design (CCPA)
  - Improve Firewall Architecture
  - Additional Protection for Critical Services
- Email Security (CCPA)
  - Add new detection tools (Completed)
- Identity and Authentication Management (CCPA)
  - Multi-factor authentication (In Progress)
  - Automate user activation/deactivation
  - Improve contactor enrollment process
  - Active Directory Hardening

The way forward...

- Upgrade Endpoint Security (CCPA)
  - Automate local admin password (complete)
  - Next generation malware protection
  - Improved security in Windows 10 image (In Progress)
  - Mobile Device Management enhancements
- Improve Monitoring Tools (CCPA)
  - Expand centralized logging
  - Add Security Information and Event Monitoring (SIEM)
- Update Policies
  - Risk Assessment (COIT-CP/CCPA/PFA)
  - SFMTA Cybersecurity Policy (COIT-CP/CCPA/PFA)
  - COOP/Cybersecurity Incident Management (COIT-CP) (Complete)
  - Assist MTA with permit polices (PFA) (In Progress)
- Additional Training (CCPA)
  - End-user Training
  - Admin Training

Timing...

	Complete	CY-2018	CY-2019
Vulnerability Management	Pen Test Central Patch Mgmt.	Non-MS patches Unsupported S/W	Sustain Upgrade Cycle
Firewall/ Network	Next Gen. Firewalls	Virtual Firewalls New Architecture	Complete Migration
Phishing	New Antiphishing Tools	User Training User Testing	User Training User Testing
IAM	Automate user deactivation	Multifactor Authentication (O365)	Comprehensive Identity Management
Endpoint	Manage Local Admin	Updated Mobile Device Management Win10 Image Advanced Antimalware	Maintain and Monitor
Monitoring	Centralized Logs	Acquire SIEM	Threat Hunting
Policies	COOP	Risk Assessment Cybersecurity Policy	Remediate Processes
Training		Admin/End-user Security Training	Create own training modules