Strategic Plan for the Replacement of Infrastructure

Maintaining a healthy infrastructure for information technology is as important to the functioning of Olathe as maintaining a healthy infrastructure for water delivery and roads. Our technical infrastructure is critical to all roles in the city and important to paving the way for a smarter Olathe 2040.

The Issue

The city utilizes several technologies to provide access to data, applications, Internet and voice services for 900+ employees across 46 facilities. Largely driven by Criminal Justice Information Systems (CJIS) regulations, 2 data centers located within the Police Department building (PDC) and the Johnson County Communications Center (CCC) are utilized to deliver these services.

Underinvestment and delayed maintenance of the city's technical infrastructure, over the course of many years, has left key components outside of their expected lifespan and incapable of supporting growing demands or the use of cloud technologies. At a high level, these components include phone and voicemail systems, data networking, processing and storage.

Detailed list of components:

- Phone and Voicemail Systems
    - The current phone system, used throughout the city, is at capacity with no room for additional extensions. There are 2 voicemail systems in use, each supporting roughly half of the city's employees. The first is hosted onsite and well beyond its expected life. The second is being discontinued by Microsoft, in December of 2019. Acquiring a new Avaya phone system will provide modern, expandable phone and voicemail systems. Because the voicemail system requires replacement by December 2019 this project may be phased to deploy voicemail services prior to the phone system cutover.

- Data Networking
    - PDC Firewalls - The firewalls at the police department are beyond manufacturer support. A failure would leave the Police Department unable to access resources outside the public safety network.

- CCC and PDC Domain Controllers - These servers facilitate the ability for people to log onto the network. The 3 physical servers running Active Directory Domain Services have passed end of life and require replacement.

- Data Processing
  - PDC Primary Processing - The current network appliances have passed the end of life and are due for replacement in 2019
  - CCC Primary Processing - The virtual application delivery servers and software used to present applications is past end of support. Multiple applications serving City departments rely on this architecture for delivery.
  - PDC Physical Servers - The physical servers that support all the currently virtualized servers in the police data center are due for replacement in 2019.

- Data Storage
  - CCC Primary Backup Server - The server and robotic tape library used for backing up all servers to backup tape have passed end of life. The solution provides all backups for all servers and applications residing in the city data center at the CCC.
  - CCC Primary Storage - The storage appliance located at the CCC data center will reach end of the initial three-year prepaid support by the middle of 2019. This is the storage appliance supporting all servers in the CCC facility and is critical to nearly every city-wide application. Extended support for years four and five is available at nearly the cost of replacing the controller and purchasing 3 years of support. In addition, the existing capacity is insufficient to support growing data needs.
  - PDC data storage - One of the two controllers have reached end of life and is no longer supported. This controller is supporting many of the virtual servers at the police department.
  - PDC data storage - The second of two controllers will reach end of life in the middle of 2019. The device is the storage location for all camera footage used in the police department and is at full capacity.
  - PDC Backup Server - The server used for backing up all police servers to backup tape. The server and robotic tape library will reach end of life in 2019. This performs all backups of the servers and data residing in the Police data center.

The Approach

A health check of the existing infrastructure, rating the usability, reliability, obsolescence and cost was completed to assess multiple components of the technical infrastructure and develop a timeline and budget based on priorities. The following table indicates the need to begin replacement of significant portions of our overall infrastructure in 2019.

	CCC					PDC				
Infrastructure System	Meets Need (Usability)	Outage Frequency (Reliability)	Up-to-Date Architecture (Tech Obsolescence)	Cost to Maintain	Health Check Rating	Meets Need (Usability)	Outage Frequency (Reliability)	Up-to-Date Architecture (Tech Obsolescence)	Cost to Maintain	Health Check Rating
Datacenter Network	3	5	4	4	4	1	2	1	3	1.75
Datacenter Primary Storage	4	5	2	2	3.25	1	5	1	1	2
Datacenter Secondary Storage	4	5	5	2	4	1	1	1	1	1
Datacenter Compute	3	5	3	5	4	3	5	1	1	2.5
Wireless Network	5	5	4	4	4.5	5	5	4	4	4.5
Wired Network	4	4	2	1	2.75	4	4	2	1	2.75
Phone System	2	1	1	1	1.25	2	1	1	1	1.25
Voicemail System	1	1	1	1	1	1	1	1	1	1
Enterprise Identity Management	5	5	3	5	4.5	5	5	3	5	4.5
Virtualization Platform	3	5	2	3	3.25	4	5	2	2	3.25
Fiber network	3	3	2	1	2.25	3	3	2	1	2.25
Email	3	5	3	1	3	3	5	3	1	3

Scale	
1.0–3.49	*Needs attention in the next 1–3 years*
3.5–4.49	*Needs attention in the next 3.5–5 years*
4.5–5.0	*Needs attention after 5 years*

Ranked Order of Importance by Component with Estimated Expenditure

Priority Order	Description	Purchase Price	Annual Maint	Line Item Total
1	Datacenter Network	$70,000	$15,000	$85,000
2	Secondary Storage	$275,000	$50,000	$325,000
3	Phone and Voicemail System	$360,000	$90,000	$450,000
4	Firewall	$100,000	$20,000	$120,000
5	Data Storage	$350,000	$65,000	$415,000
6	Data Compute	$275,000	$50,000	$325,000
7	City Network	$100,000	$20,000	$120,000
		$1,530,000	**$310,000**	**$1,840,000**

The Risks and Mitigations

As with any project, risks exist to the successful upgrade of the city's infrastructure; a brief list of those risks and mitigations is included below.

Risk Description	Mitigation
Large scope - Trying to do too much too quickly	Phase projects over a 1.5 to 2-year period allowing time to complete each.
Resource contention	Hire specialized implementation support to supplement current staff
Failure to implement a refresh cycle	Develop funding methods to continue a refresh cycle into the future, adopt SaaS models where possible reducing maintenance
Poor technology selections	Implement proven technologies and shift to the cloud where possible
Out of support products fail before being remedied	Identify priorities and acquire 3rd party support where possible
Taking no action leading to more frequent and severe outages	

The Solution

Ideally the technical infrastructure could be upgraded once and forgotten; however; ongoing refresh and technical needs will continue. The preferred technologies will allow for the modular expansion and upgrade to infrastructure services through on premises or cloud-based systems, reducing the need for a complete refresh in 3 to 5 years. In addition, changes to the funding model for technical infrastructure utilizing a model like the PC replacement fund will be proposed.

Due to the diversity of systems and immediate replacement needs for some, the assessment will guide a phased approach to refreshing the technical infrastructure. An estimated $1.9 million will be required over an 18 to 24-month period. Every effort will be made to reduce the overall expense and timeframe.

Where possible, to extend the life of some components, aftermarket support will be purchased allowing time for the more critical replacements. Cloud based solutions, when appropriate, will be considered in lieu of on premises equipment. In all cases we will strive to reduce overall costs where practical.

Next Steps

Requests for proposal (RFP) have been initiated for the phone/voicemail system as well as secondary storage devices. Existing state contracts are being reviewed to determine best cost for all systems. In the coming weeks, agenda items requesting approval for the highest priorities will be submitted. Requests for subsequent priorities will follow as time and resources allow.

Appendix: The following table includes identified annual expenses eliminated with an infrastructure refresh:

Item	Type	Annual Savings	Description
Iron Mountain	Expens	$ 4,620.00	Storage for all backup tapes held for multiple retention windows based on backup source and purpose.
Tape Management	Labor	$ 13,000.00	Physical management of shuffeling, moving, transporting backup tapes, and performing manual restores of backups.
Cohesity Expansion	Capital	$ 37,800.00	This device would be replaced with this project eliminating the need to acquire another.
Cohesity Support	Expens	$ 11,200.00	Annual support for Cohesity maintenance on existing demo appliance
Firmware & OS Patching	Labor	$ 6,000.00	Time spent on Backup Exec Server (x2), backup storage appliance, tape library (x2), cohesity appliance, File server (x4)
File Server (CHE)	Capital	$ 18,000.00	This device would be replaced with this project eliminating the need to acquire another.
File Server (GIS/AX)	Capital	$ 18,000.00	This device would be replaced with this project eliminating the need to acquire another.
Backup Tapes	Expens	$ 4,500.00	~100 tapes per year, based on current usage and exhaustation rate
Manage Deleted Files	Labor	$ 400.00	Managing Undelete to recover lost files for users. Users will be able to self recover with new technologies.
Equallogic Storage Appliance	Capital	$ 18,000.00	Current appliance is EOL will be EOS next year. Used to hold all video storage at PD. (Highly Critical Appliance)
CoRAID Storage Appliance	Capital	$ 13,500.00	Current appliance is past EOS and no longer servicable. Used to hold roughly 1/4 of virtual servers at PD. (Highly Critical Appliance)
Equallogic Storage Appliance	Capital	$ 27,000.00	Current appliance is EOL and will EOS this year. Used to hold 3/4 of all virtual servers at PD.
		$ 172,020.00	