Town of Southwick, MA

IT Strategic Planning & Business Continuity: Initial Recommendations and Progress to Date

Office of Municipal & School Technology

Executive Office of Technology Services & Security (EOTSS)

Contents

Image: Southwick, MA[1]

Introduction

The Town of Southwick adopted the Business Continuity best practice in April of 2017 as part of a Community Compact agreement signed with the Baker-Polito Administration. Southwick partnered with the State's Office of Municipal and School Technology to evaluate the Town's IT structure, understand the pain points experienced by staff with technology, and work toward a strategic plan to help guide the Town's leadership as they make decisions about technology procurement and staffing.

Community Profile

The Town of Southwick is located in southwestern Massachusetts in Hampden County, with a population of 9,502 residents[2]. Originally, Southwick - the south village or "wick" of Westfield - was set off as a district. In 1775, it became a town. Its proximity to the cities of Springfield, Massachusetts and Hartford, Connecticut via routes 10, 202 and 57 have generated significant demand for new housing. Additionally, the town enjoys its status as a major recreational center because of the Congamond Lakes, Moto Cross 338, and large open space areas. Southwick was also home to the first Rugged Maniac 5k Obstacle Race & Mud Run in 2010. Southwick continues to be home to this popular New England event, and similar events have since spread throughout the US and Canada.

---

[1] Massachusetts Office of Travel and Tourism in Southwick, Massachusetts (April 24, 2012). The Ranch Golf Club, Southwick [Photograph]. *Flickr*. Retrieved from http://bit.ly/2zR6IyE

[2] 2010 Census. *U.S. Census Bureau. American Factfinder*. Retrieved from https://factfinder.census.gov/faces/nav/jsf/pages/community_facts.xhtml?src=bkmk

Project Background

The Town of Southwick has long recognized the importance of technology in performing the functions of local government, but with increasing demand, threats and complexity, they want to become more intentional and take a more enterprise-focused approach to technology. Leveraging the Community Compact program, the Town requested assistance from the State to help them assess their IT practices. In Summer 2017, the Office of Municipal & School Technology (OMST) partnered with Southwick to identify and provide recommendations related to gaps in their IT environment. The OMST coordinated an IT Health Check provided by AKUITY Technologies, and conducted staff interviews to better understand local challenges and provide appropriate recommendations.

AKUITY Technologies Health Check

Before OMST staff met with Town staff, AKUITY Technologies provided a no-cost IT Health Check for the Town. The Health Check provided a high-level overview of Southwick's IT environment, with focus on the following areas: Users, Servers, Network, Backups, Email, and Antivirus. Each category was evaluated using specific criterion (shown in the table below) and ranked. While not unusual in local government, the assessment did reveal that two areas, Users and Servers, contained high risk factors, including the age and grade of equipment and current policies and procedures. [3] This information helped to inform the recommendations made by OMST and enabled the team to have an effective discussion with Town staff around technology.

Office of Municipal & School Technology Engagement

Following the Akuity Health Check, the OMST visited the Town of Southwick to assess the overall technology environment and interview municipal staff. The team held informal interviews with leadership from various departments including: Accounting, Police, Fire, Public Works, Assessor, Treasurer/Collector/Clerk, and Library. The team also discussed the state of IT in the community with the Town's Chief Administrative Officer and Chairman of the Select Board. This process allowed the team to better understand Southwick's technology structure, processes and procedures from the perspective of staff.

[3] The Town is actively working to address the gaps identified in the AKUITY Health Check.

As-Is Observations

Like most organizations, and particularly local government, the technology infrastructure and policies in Southwick have evolved incrementally over time, as needed. The reality is that, while there are a number of opportunities for improvement, for a town with a population of less than 10,000 residents, Southwick has most of the right pieces in place and has demonstrated a relatively strong understanding of their current position and the challenges that organizations in both the public and private sector face as technology demands from the public increase and cyber threats evolve.

Today the Town has one IT staff member, reporting to the Town Accountant, and responsible for technology functions across the Town, with the exceptions of Fire and Police.[4] In speaking with the IT resource and other Town staff, we learned that this role tends to be more reactive than proactive, and the general sentiment of Town staff was that this reality is a function of competing priorities and limited resources.

Technology spending in Southwick happens at the department-level, but while the Town takes a very decentralized approach today, staff feel that technology spending has been consistently identified across departments and this data could be used to better understand technology investments across the Town.

While similar to other organizations, the ability to keep the Town's technology current was a challenge identified in both AKUTIY's IT Health Check and our interviews of Town staff. Over the past 10 years, the number of hardware and software assets in the Town have expanded greatly, however, capacity to maintain that equipment hasn't kept pace. This challenge is noted in many areas, including:

- PC and server hardware running unsupported operating systems
- Hardware that is beyond reasonable life expectancy
- Line of business software in need of updates
- Routine backups that are not periodically verified

[4] Southwick is part of a regional school district, which was beyond the scope of this report.

- A past cyber incident

The somewhat decentralized nature of IT in Southwick also results in challenges that make it difficult to meet current technology expectations. This is a common challenge and moving toward a more intentional enterprise approach would likely help to address some of the challenges highlighted during interviews, which include:

- Underutilized fiber connections between municipal buildings
- Challenges in collaboration between departments
- Inconsistency in hardware replacement cycles
- Disparate network hardware
- Multiple department-based internet connections
- Disparate antivirus/end point protection products

The result is an inconsistent environment, where there are areas of strength and weakness, but potential to elevate the level of service provided to residents and staff in Southwick.

Recommendations

Move from a Reactive to a Proactive and Strategic IT Operation

As noted earlier, like most organizations, the technology infrastructure in Southwick has largely grown and evolved organically as required to meet organizational needs. The result is a technology operation that is less standardized, proactive, secure and strategic than would be optimal. Taking steps that would move the Town toward a more strategic IT operation could result in a more sustainability and security, as well as better end-user experiences for staff across departments.

Technology's place within the organization

In developing sound technology operations in municipal governments, one factor worth considering is the perceived importance of this function among Town staff. The necessity of reliable technology services has become essential to effective government operations across functions. A weak technology operation can lead to staff frustration, but it can also lead to security vulnerabilities and barriers to

productivity for staff across the organization. Over the past 25 years, information technology in government has evolved from a back-office data processing function to integration with all facets of our operations from back-office processing to constituent engagement. This evolution can be seen in organizations of all sizes and types, and is marked by changes from department names like Management Information Services to names like Innovation and Technology or the transition from IT being a function of Administration and Finance to a more central role as an information technology department.

The expectations of municipal IT staff have also evolved greatly in recent years. The evolution of staff across departments having access to computers and email and the public having an expectation of being able to interact with their government over the internet has opened extraordinary opportunity for improved and more efficient service provision. However, with these opportunities come new risks. Increased technology and internet use has also led to a rise in cyber-crime. The timely implementation of security patches, appropriate network configuration and end-user education are now essential components of sound technology operations. Southwick's existing technology position, a Computer Technician, includes many of the critical functions required in municipal government; however, it does not emphasize the importance of software and network security, management of cloud and on-premises technology or the ability to effectively collaborate across departments.

We recommend that over time, the Town consider the possibility of moving technology from being a function of a specific line of business (Accounting) to a central resource – not because of any existing staff deficiency, but to signify and open opportunities to expand the Town's enterprise approach to technology.

We would also recommend that the Town consider changes to their technology staffing model. Today there are gaps leading to security vulnerabilities, inconsistencies across departments and collaboration challenges. The Town's Computer Technician is not well positioned to manage the network, security and end-user demands that continue to grow year over year. This has led to, "…trying to manage expectations…to make sure [staff] know they're not just being ignored". While there is not necessarily a 'right way' to tackle this challenge, one option to consider would be separating core infrastructure

support from end-user and device support. Support of core infrastructure, like network and server maintenance can be handled by staff resources, but there are also vendors who provide server and network monitoring and maintenance services.

Analyze IT Spending

Another important consideration in moving toward an enterprise approach to information technology is the approach to IT procurement and budgeting. One of the challenges identified is that IT investments tend to occur on a department by department basis, however, the fact that Accounting is able to track IT spending at a granular level could help to inform inefficiencies and duplication. Understanding organization-wide IT spend can be helpful in being able to set longer-term IT priorities. Looking at department-level spending can also be useful in identifying unnecessary hardware redundancies across departments, software licensing that could be aggregated to leverage economies of scale or identifying internet circuits that could be aggregated, sometimes with opportunities to leverage higher-quality service at lower cost.

A common practice is to require approval of all IT purchases by a central IT authority. This is generally not meant to be a punitive policy, but one meant to maximize the reach of technology dollars and ensure that staff are aware of relevant resources, standards or initiatives.

We would recommend an analysis of current technology spending to identify any duplication or opportunities to standardize and institute an approval process for IT purchases across the organization. If the Town elects to pursue this recommendation, it is important to take a balanced approach that helps position the Town for long-term success without creating unnecessary barriers to staff performing their day to day duties.

Standards and Consistency

One of the major benefits in moving toward an enterprise approach to technology is that it opens opportunities for more standards and consistency. While poorly implemented standards can result in restrictions that can have a negative impact on productivity, well implemented standards will result in a more secure environment that enables more collaboration and improved end-user support.

Implementing organizational standards for desktop computer refresh cycles, and planning for the operating expenses, can lead to more consistency in the hardware to be supported and ensures that staff are leveraging technology that has not exceeded its anticipated life, which can help to avoid end-user frustration and shift more technology staff time from keeping old equipment running to focusing more on enterprise priorities.

Creating more standards around network infrastructure can also provide significant benefits to the organization, especially when it comes to opening opportunities for collaboration while providing adequate security. Consistency across network hardware over time can help to mitigate any risk of configuration errors, and centralizing oversight and monitoring of the network would likely result in stronger overall security and improvements in the ability to collaborate across departments. As the following video describing the 'One Network' initiative at the Executive Office of Technology Services and Security explains, the notions of 'security by obscurity' and isolated networks are proving to be ineffective in protecting against cybercrime, which continues to grow with our increasing reliance on technology:
https://www.youtube.com/watch?v=BbhV0nlUW5E

Recent network infrastructure investments made at the Southwick Fire Department would serve as an example to be scaled across the community. The wireless infrastructure was implemented with an eye toward allowing for access and collaboration without compromising security. The solution allows for secure network access over the wireless network, while also providing public internet access that is isolated from the municipal network. A solution like this has the potential to be scaled across the organization allowing for consistent network monitoring across the enterprise.

Setting standards for staff can also be an important step in moving toward an enterprise approach to information technology. Policies like 'Acceptable Use' are important, but should also reflect the realities of the organization. One of the concerns raised in the Fire Department was the reality that the nature of their work results in different expectations and challenges than might exist in a department with constant in-office, in-person, interaction with the public. The wireless technology deployed in the Fire

Department can help to address some of these concerns, and an acceptable use policy can help to clarify appropriate behavior over the Town's secure network, reducing the probability of the cyber security incidents that have impacted municipal systems in the past. The Town of Westford has an Acceptable Use Policy that addresses some of the topics that would also be important in Southwick: http://www.westfordlibrary.org/Pages/JVFletcherLibrary_Admin/policies/Information_Technology_Acceptable_Use_Policy.pdf

In recognition of the increasing threat of cybercrime, many communities are now requiring cyber education programs for Town staff. New tools and services make it much easier to pursue employee education, including programs that simulate phishing attempts and provide metrics around staff ability to identify these attempts over time. Cyber threats evolve on a daily basis, and while technology can mitigate the threat, it is unrealistic to expect it to eliminate the threat -- making proactive employees an essential component of protecting the community.

Being Proactive

In moving toward a more mature IT organization, the transition from a reactive to a proactive mindset is important. In this time of increased expectation and threat it is important that network appliances, servers, desktops and software are consistently updated. According to the Multi-State Information Sharing and Analysis Center (MS-ISAC) at least 95% of infections they investigate started with an unpatched vulnerability in an operating system, software or plugin.[5] Said another way, a habit that includes routine maintenance will significantly reduce the probability of a cyber security incident and will likely result in improved end-user satisfaction.

It was noted during the site visit that software updates can be slower to rollout than would be ideal, potentially leading to staff inefficiencies caused by productivity tools that have been superseded or are missing from the current implementation.

[5] Bailey, Kaitlyn. Timely Patching Reduces System Compromises. MS-ISAC. February 2016

Finally, as noted above, proactive employee education can also go a long way in mitigating organizational security risks that may exist.

Determining Where to Make Investments

Determining which services to manage internally versus which to have managed by an external entity has never been more challenging. While the number of options and opportunities available have grown exponentially, so have the complexities in identifying the most appropriate solution. Organizations are struggling to understand the different variants of "The Cloud", the security implications and what it means to be "hybrid". While there is no silver bullet, in this section we hope to highlight some of the factors the Town will want to consider as the technology strategy evolves.

What is the Cloud?

When we talk about "The Cloud" we tend to be talking about one of the following types of cloud services:

Software as a Service (SaaS)

- This is generally a completely managed service over the internet where the end-user software through to the hardware infrastructure is managed by a third party. SaaS eliminates the need for local application infrastructure maintenance and most software maintenance. Examples of SaaS would be online services provided by Microsoft O365, Google GSuite or Tyler Munis (in the case of Southwick).

Platform as a Service (PaaS)

- This is the platform on which software can be developed and deployed. Typically, the service encompasses hardware management, including server and operating system, as well as the software platform on which the business application itself if built. Common examples of PaaS include Heroku, RedHat OpenShift, Google App Engine and Microsoft Azure.

Infrastructure as a Service (Iaas)

- These are the fundamental building blocks of cloud services. IaaS is typically a scalable approach to compute and storage resources. It is often thought about as a virtual data center where compute, storage and network resources can be easily provisioned. Typically the customer is responsible for installing the database, operating system, etc. It is now common practice at the Commonwealth to deploy new servers to an IaaS cloud service provider. Common examples of IaaS include Amazon Web Services, Microsoft Azure and Google Compute Engine.

Pros and Cons of Moving to the Cloud

Pros

- A reputable cloud provider is focused on the service they are providing to you, that generally means very reliable services, more diligence in protecting the systems from cyber threats and more frequent software updates.
- Many cloud providers will include disaster recovery as part of the standard package – meaning if something goes wrong with the system, they are following industry standard processes and should be well equipped to restore your environment.
- Well managed cloud implementations can be very cost effective.

Cons

- Monitoring and deploying cloud solutions requires a different skillset from traditional IT.
- Poorly managed cloud services can be expensive – with an IaaS solution, you are often paying for what you use, so monitoring and optimization are important.
- While the infrastructure tends to be more secure, you must look at different risk factors. The threat revolves more around end-users being prey to phishing emails, and cyber criminals using those credentials over the internet than attacks on the infrastructure itself. The result is more secure infrastructure, with a need for more vigilance in training staff around cyber threats.

Develop an Inventory

The first step in making the right decisions for the organization would be to create an inventory of existing technology assets across the organization to fill any gaps that might exist. The best starting point would likely be an automated inventory. It might be most effective to have a 3rd party perform the automated inventory and provide a network diagram. There will likely be some level of manual inventory work required, but leveraging automated tools can provide a great starting point and can provide software and operating system information that would be very time consuming to collect manually. Be sure that the inventory includes:

- Any desktop computers, laptops and tablets along with details, such as age and operating system
- Servers and Operating Systems
- Peripherals like printers and scanners
- Network hardware and appliances
- Software on PC's, servers or in the cloud

There are different approaches to asset management, ranging from spreadsheets to asset management systems. While their focus is libraries, TechSoup provides templates that provide a sense of the data that should be collected:

http://www.techsoupforlibraries.org/planning-for-success/maintaining-and-sustaining-technology/tools/hardware-and-software-inventory-wor

What Are the Options

Having completed the inventory and having a more complete picture of the as-is state of technology in the community, it should become easier to understand the implications of different strategies. Some of the questions you might want to ask as an organization include:

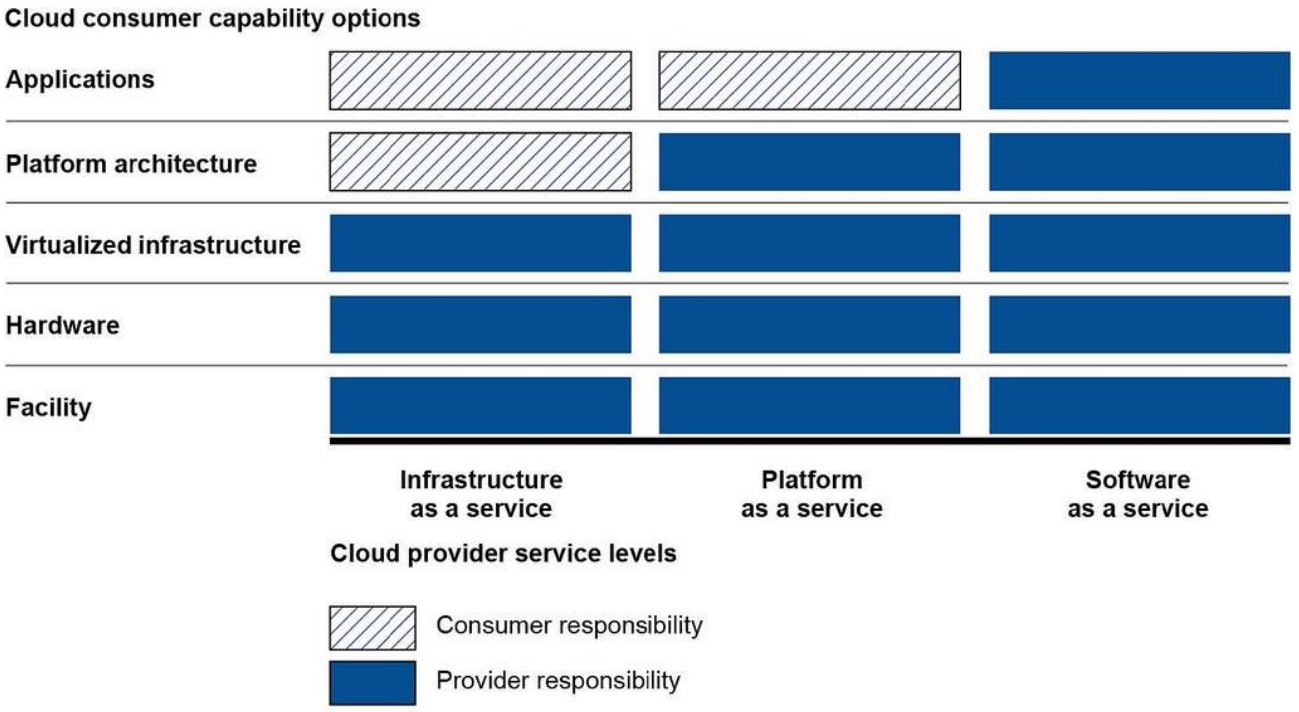
- Is it realistic to move toward a secure town-wide network? This would certainly require technology investments, and more importantly, difficult conversations around staffing and changing roles and responsibilities.
    - If yes, does existing staff have the capacity to effectively manage this function?
        - If no, is there interest in bringing on a new full-time technology resource or might a managed service approach be a better fit? One potential benefit of a managed service approach is that in some cases it can be easier to ensure that the skillset available evolves with changing organizational needs.
    - Could we implement a town-wide end-point protection solution (cyber security)?
- What software are we running on our desktops and servers today and what is the level of effort in maintaining the software?
    - Which of these systems are integrated today and are there existing data/technology silos preventing more effective operations that could be improved?
    - Are there opportunities to move any of these business solutions to a SaaS solution?
        - If yes, will the SaaS solution allow for the integrations necessary?
- How many servers do we maintain today and do we want to continue to house servers locally?
    - If yes, should we consider virtualization?
    - If no or maybe, do we want to consider the possibility of leveraging an IaaS provider?
- How will we approach identity and access management if we move to a hybrid IT environment?
- Who has responsibility for providing end-user support and will support departments in analyzing business processes?

In thinking about these questions, it can be very useful to think about the technology in terms of service models, for instance:

On-Premises IT	Traditional model where infrastructure and software are maintained locally
Shared Datacenter (colocation)	Physical location of servers, their power, air conditioning and racks are outsourced, Town is responsible for maintaining the servers and software.
Infrastructure as a Service (IaaS)	Infrastructure is outsourced with the Town responsible for maintaining the platform and applications.
Platform as a Service (Paas)	Infrastructure and platform are outsourced, the Town is responsible for

	maintaining the applications.
Software as a Service (SaaS)	Infrastructure, platform and software are all outsourced.

The following graphic, developed by the US Government Accountability Office, illustrates responsibilities associated with the various cloud models.



Source: GAO analysis based on National Institute of Standards and Technology. | GAO-14-753

[6]

Note that the goal is not to find a model that meets all needs across the board—the reality is that nearly all organizations will need to take a hybrid approach. You want to look at each of your systems and determine which model is the most appropriate fit, based on factors such as staff capacity, technical requirement and integration priorities.

You will also want to consider how this fits into your staffing plan, specifically whether these services will be managed by Town staff or a managed service provider. By Gartner's definition, "a managed service provider (MSP) delivers network, application, system and e-management services across a network to

[6] U.S. Government Accountability Office. 2014. "CLOUD COMPUTING: Additional Opportunities and Savings Need to Be Pursued." http://www.gao.gov/products/GAO-14-753.

multiple enterprises, using a "pay as you go" pricing model."[7] Any of the models identified above could be outsourced to an MSP, the direction will depend on Town priorities, which will include staffing realities and cost considerations.

Leverage Existing Network Infrastructure and Consolidate Internet Connectivity

The Town of Southwick is very fortunate in that as infrastructure beyond IT has evolved, leaders had the foresight to ensure that conduit were laid, creating opportunities for connectivity between municipal buildings. One of the ways the Town can take advantage of this existing investment is to ensure that there is reliable connectivity between buildings, then look for opportunities to fully leverage the capacity.

Like a lot of evolving organizations, today, each building in Southwick has its own internet connection, generally provided by Comcast over coax. Taking full advantage of the connectivity opportunities provided by the existing conduit could mean the consolidation of multiple internet connections into one centralized connection. There could be cost savings in purchasing one larger connection and maintaining the networking centrally. There are likely security benefits as well, as enterprise equipment would be centrally managed and there would be less risk on consumer grade equipment being deployed at the department-level. In addition, aggregating the internet demand from multiple departments might make internet service over fiber more feasible. While fiber connectivity tends to be significantly more costly than coax, the cost per megabit drops significantly as the size of the connection increases.

While many businesses can operate effectively over a coax connection, there are some compelling benefits in leveraging fiber-based internet services, including:

- Reliability – fiber connectivity tends to be more reliable than coax and is less susceptible to weather-related interruption.
- Symmetrical Speeds – you typically see symmetrical speeds (meaning uploads are the same speed as downloads) when using fiber-based internet service. The benefits of symmetrical service become more apparent as functions move to the cloud.

[7] Gartner, Inc. n.d. Managed Service Provider (MSP). Accessed November 15, 2017. https://www.gartner.com/it-glossary/msp-management-service-provider.

- Latency – fiber connectivity eliminates many of the latency challenges posed by coax connectivity. Latency is the delay in processing data, and while measured in milliseconds, there can be a noticeable different when it comes to the use of VOIP services and cloud-based applications.[8]

As noted earlier, a consistent, centrally managed, and secure network would open opportunities to take an enterprise approach to end-point and network security. Typically, a network managed at the department-level, by staff with differing levels of capacity and technology skill, leads to a complex environment run by different rules and policies, creating challenges in cross-department collaboration and greater risk to the enterprise overall. While at one time network complexity was often viewed as ensuring security, today we understand that this approach tends to provide more points of entry for malicious actors. The simpler your network, and the more you understand it, the easier it will be to monitor and identify unusual activity. Less disparity in equipment throughout the network, fewer interfaces that need to be configured at the edge of each department-based network and more consistent end-point protection can help to simplify management and monitoring. The end result is likely to be a network that provides staff with the ability to collaborate and have access to the resources they need and expect, while also better protecting Town data.

In addition to security, there would also be opportunities for an enterprise approach to backup and recovery. When these efforts are approached on a department by department basis, there are often different systems used, important factors overlooked and a lack of capacity to test backups, which are critical in ensuring the ability to recover if a disaster were to occur.

Progress to Date

The Town of Southwick has made great progress since the initial Health Check was performed and recommendations were made. They have implemented many of the recommendations, and fully leveraged community compact programs to perform and IT Assessment and successfully applied for funding to support the implementation of a converged virtual server infrastructure.

[8] Collins, Tom. 2016. 11 Huge Benefits of Fiber Internet Connectivity. Accessed November 11, 2017. https://www.atlantech.net/blog/11-huge-business-benefits-of-fiber-internet-connectivity.

The Town has made significant progress in enhancing network infrastructure, which allows for an enterprise approach to the provision of technology services, leaving the Town with a much strong cybersecurity posture and allowing for the aggregation of internet connectivity.

The Town has also made significant progress in improving server and storage infrastructure. This will significantly mitigate cybersecurity risk, should simplify ongoing maintenance needs and will leave the Town better positioned to provide services better aligned with staff and public expectations.

Conclusion

The Town of Southwick fully appreciates the importance of technology to ongoing municipal operations, has been diligent in leveraging the opportunities available through the Community Compact Cabinet and has made great progress in addressing many of the recommendations in this report. There are several factors that lead to successful technology transformation and Southwick is fortunate to have leadership with an understanding of the importance of technology and a willingness to make changes and Town staff willing to rethink the status quo. They have committed to continuing this effort in their upcoming fiscal year budget.

We encourage the Town to continue down the current path, continuing to enhance infrastructure and evaluate the approach to end-user support. The continued movement toward a more proactive technology operation will allow staff to focus on performing their business functions and providing the level of service and security residents expect.