Simsbury Technology Task Force
Regular Meeting
March 4, 2019 – 5:30pm
Engineering Conference Room, 933 Hopmeadow Street

Pledge of Allegiance

1. Minutes of February 4, 2019

2. Virtualization Environment – Discussion and Work Plan

3. Study of Shared Services (Town/Board of Education) – Discussion and Work Plan

4. 2016 Blum Shapiro Report

5. Next Steps/Agenda items for next meeting

Adjourn

Town of Simsbury

933 HOPMEADOW STREET SIMSBURY, CONNECTICUT 06070

Technology Task Force
Monday, February 4, 2019, 5:30 p.m.
Engineering Conference Room, Town Hall, 933 Hopmeadow Street

Regular Meeting Minutes - DRAFT

Members Present: Larry DiSciacca, Mark Orenstein, Bill Rucci, Dennis Kearns, Evan Marks, Harald Bender, John Jahne, Liz Peterson, Chris Kelly (Board of Selectmen liaison)

Staff Present: Melissa Appleby, Rick Bazzano

The meeting was called to order at 5:35pm.

1) Minutes of January 7, 2019
The minutes of January 7, 2019 were approved by consensus.

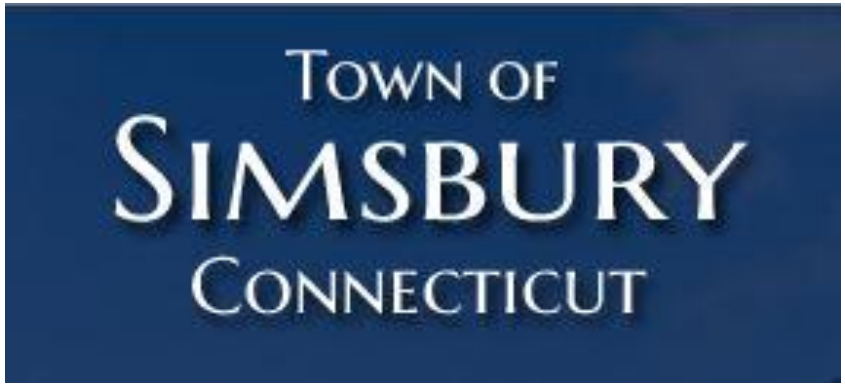
2) Review Social Media and Website Use Policy – Board of Selectmen Referral
Ms. Appleby provided an overview of the draft policy and indicated that the Board of Selectmen is seeking feedback by March 1. Discussion ensued regarding user accountability, consistency in nomenclature, and account recovery. In particular, the group recommended having unique login information that is not shared among staff as well as a process for resetting passwords when employees separate from service with the Town. Under Section V, Part A, the word "edit" should be added to the last sentence to reinforce the fact that the Town Manager has control over account names and other nomenclature used. Members will continue to review the draft policy and will send along additional comments directly to staff.

3) 2019 Planning
Mr. Bazzano described the major trends facing the IT department in the next one to two years. This includes evaluating storage and backup needs. The current platform, Simplivity, will need to be replaced in the next year and a half. In addition, the department is looking at moving to a virtualized environment. Discussion ensued regarding a VM ware solution as compared with Citrix. The group discussed the need to plan ahead for this changing environment, particularly in regards to staffing. Mr. Kelly noted that the concept of shared services between the Town and Board of Education should be explored further. The group discussed other possible upcoming focus areas, including a new financial management system, new payroll system, and website management.

4) Next Steps/Agenda items for next meeting
The group will revisit the 2016 Blum Shapiro report, further explore a study of shared services between the Town and Board of Education, and continue discussion of the virtualization environment.

Adjourn
Mr. DiSciacca made a motion to adjourn at 6:31pm. Mr. Marks seconded the motion. All were in favor and the motion passed unanimously.

Respectfully Submitted,
Melissa Appleby
Deputy Town Manager



Town and School District of Simsbury

IT Operational Assessment

Findings and Recommendations

December 2016

Table of Contents

I. Project Overview

A. Background

The Town and School District of Simsbury (hereafter referred to as "Simsbury") have reached a critical milestone and sought an operational assessment and analysis on the feasibility, benefits or disadvantages of combining or sharing municipal and School district operations related to information technology. Simsbury hired Blum Shapiro Consulting, LLC to conduct this comprehensive evaluation of internal IT operations within the Town and School District departments. Blum Shapiro performed an analysis of the existing operations, including how the IT services are functioning in both areas (Town and School District). Blum Shapiro interviewed 29 individuals as part of the municipal and School district IT operations evaluation. These individuals included personnel from the Town's Finance/Administrative Services Department, Human Resources, Planning, Engineering, Social Services, Public Works, Library, Police, Culture, Parks and Recreation, and Technology/Computer Department; and the School District's Business Office, Superintendent's Office, and District Technology Staff.

The goal of the municipal and School District IT operations assessment was to perform a comprehensive analysis of the existing technology operations, identify any potential operational improvements or enhancements, and any opportunities to reduce or share costs. This assessment focused on three key elements: people, process, and technology.

B. Methodology

The goals and objectives of this municipal and School District technology operations assessment included the following:

- Perform a comprehensive analysis of the existing technology operations in both the Town and School District.
- Evaluate the current IT positions (structure, leadership, staffing).
- Evaluate the way each IT/Technology Department and its respective employees work and provide services.
- Review IT security methods and practices.
- Confirm current technologies and technology acquisitions.
- Develop findings and recommendations for the Town and School District.
- Assess whether the Town and School District are in a position to consider additional formal shared IT service opportunities.

As a result of the aforementioned goals and objectives, the project team focused on the following:

1. Reviewing the current IT strategies, roadmaps and plans, core functions, and support and maintenance processes, including information security practices.
2. Reviewing current IT organizational leadership and staffing, job descriptions, roles and responsibilities.
3. Reviewing methods used to prioritize, schedule, and resource technology projects.
4. Reviewing areas where the Town and School District can realize efficiencies and economies of scale through shared resources or purchasing power.
5. Documenting findings and any gaps observed as part of the discovery efforts.
6. Providing constructive and practical recommendations to achieve potential changes.

The process was participative and consultative. The project team interviewed and consulted with Simsbury's key management and administrative staff, including Town and School District staff. Individual interview sessions were held to gain specific information and perspectives on relevant issues. The entire municipal and School District technology operations assessment methodology was iterative in nature.

C. Acknowledgements

As part of our assessment, BlumShapiro received and reviewed two reports (identified below) and used this information as the basis to develop a going in position for many of our interview sessions.

1. CCAT - IT Assessment Report – January 23, 2015 (Town)
2. The Walker Group – High Level Network Review- May 2013 (BOE)

Blum Shapiro would also like to thank the Town and School District of Simsbury for their participation, support, on-going dialog, and feedback during this project. A list of the project participants is provided in the Appendix.

D. Report Format

We have grouped our findings and recommendations related to the Town and School District technology departments in Section II. For each observation, we discuss the critical issues involved and provide specific recommendations.

E. Commendations

Although this report will identify a number of findings and recommendations as part of the municipal and School District technology operations assessment, there are a number of very positive and successful initiatives that have had a significant positive impact on the overall operations within the Town and School District. Outlined below are some of these initiatives:

1. The Town and School District took a proactive approach to assuring a stable network, and completed fiber installation throughout the Town in June 2016.
2. The School District has completed the implementation of virtual desktop solutions, which significantly simplifies maintenance and reduces PC replacement costs in the long term. The Town has a number of virtual desktop devices in production as well.
3. The School District and Town have proactively unified on a single, financial platform (two databases), SunGard eFinancePlus.
4. The Town and School District have implemented a shared Exchange email system hosted on one Exchange server.
5. Town employees and Department heads generally expressed positively toward Service Levels provided by Town IT Staff.
6. The Town has a volunteer advisory IT Task Force to provide input on strategic technology decisions, purchases and initiatives. School District IT staff often attend Task Force meetings.

Overview of Findings

Generally, the technology support practices for both the Town and School District were sound, but lacked formality and refinement. Blum Shapiro believes that using a maturity model approach to assessing organizational capability across multiple domains of IT service can be beneficial in articulating relative strengths and identifying opportunities to improve. The general progression of maturity levels in a particular practice area or discipline involves five basic levels:

Initial – Processes, procedures, and practices are basic, often disorganized or in a state of evolution, and rely heavily on individual efforts. They are not considered repeatable because they are not sufficiently documented.

Managed – Processes, procedures and practices are organized and repeatable by those who perform the work. Relies largely on individuals or groups collaborating together to achieve results. Basic documentation may be in place, but is largely informal.

Defined – Processes, procedures and practices are organized, formally documented, and repeatable. Independent groups or individuals can easily pick up in an absence of those responsible for the program, project or task.

Measured – Processes, procedures and practices are formally documented and repeatable. The organization has implemented measures and metrics to evaluate the sufficiency of resources and practices, and identified opportunities to improve.

Optimizing – Processes, procedures and practices are measured, managed, monitored, and continuously improved.

Blum Shapiro rated the Town and School District independently based upon our interviews and observations in this assessment. Most practices fell into the Initial and Managed levels. These ratings are provided as a tool to highlight those areas that represent the most opportunity to improve. Generally, most organizations will find it cost-prohibitive to try to achieve an Optimizing level of maturity for all of their processes. For the Town and School District of Simsbury, a reasonable target is to strive for all domains to be in the Defined or Managed levels. For critical domains such as Service Delivery, you should consider striving for a Measured level of maturity.

Summary of Findings

Collectively, the IT environment and operations for Town and School District of Simsbury are not a strong candidate for shared IT services at this time. A Shared Services IT environment can be a great solution when: IT services are significantly strained, staffing levels on one side are disproportionately low given a clearly articulated need, a significant competency or knowledge discrepancy exists, or technology is aging or unsupportable. Based upon our analysis, those conditions do not exist within Simsbury. However, significant improvements and efficiency gains are possible in the delivery of IT strategies and services for the Town and School District of Simsbury by: incrementally maturing practices, introducing formality and structure to processes, investing in IT staff training, and further collaborating with each other in areas where it makes sense. While timing requirements, funding sources, and technology licensing restrictions may be a barrier to collaborating on everything, we believe there is significant opportunity for meaningful collaboration.

Additionally, it is important to note that the method and frequency in which organizations plan for technology and innovation has changed over time. Technology needs and tools are constantly evolving, and traditional IT strategies cannot no longer afford to project out much beyond 3 years. This evolution should require a realignment with the Town and School District's capital improvement project planning.

II. Detailed Findings

Town IT Organization, Infrastructure and Processes

1. The Simsbury Town Computer Department consists of the following:
    a. Computer Manager, overseeing:
        i. An IT Analyst
        ii. One additional funded position
            1. Created in 2015 but not currently filled.
            2. Position is partially being utilized for professional services, partially for budget savings.
            3. Currently, there is not a clear definition for this role, or a date when it will be filled.
                a. Initial Job Description includes duties as a PC/Network Specialist, with lower level PC support duties.
    b. Computer Department is responsible for supporting all Departments located in Town Hall (including Board of Education), Police Station, Library, Social Services/Senior Center, Water Pollution Control, Public Works, Culture, Parks and Recreation, Town Maintenance, Simsbury Housing Authority.
        i. The School District partially funds the two Town IT positions due to the support they provide to the central office of the Board of Education (located in Town Hall).
            1. No formally documented agreement or memorandum of understanding outlines this collaboration.
    c. Generally, no interviewee mentioned issues with respect to timeliness or quality of IT maintenance and support services provided by the Town IT Department.
    d. Employees request services in person, via phone, or email. The Town uses a freeware program called “Bug Tracker” to track IT service tickets.

i. An "open source" program that has been modified by Town IT staff.

ii. Users do not enter service requests, but typically call or email Town IT staff.

iii. Bug Tracker is not always updated with all activity, especially days when staff is busy and many service requests are informal or via phone call.

2. Town IT Leadership, Direction and Strategies

a. Current IT focus is largely on maintaining present systems.

b. The Town Strategic IT Plan has not been updated since 2008, although strategic guidance was provided by CCAT in 2015.

i. Town Department personnel interviewed expressed uncertainty about the strategic direction of technology utilization. While there was not an expressed need for aggressive changes to strategies, general strategic direction was not clear.

ii. During our discussion with the Town's Computer Manager, he articulated a few strategic choices and trends including:

1. Pursuing cloud applications and maintenance contracts whenever possible to reduce the burden on staff resources. Examples include:

a. ESRI (Geographic Information System) in the cloud.

2. Managed service contracts for Town switches and network infrastructure.

3. Choosing "all-in-one" infrastructure solutions, such as the Simplivity servers.

c. Technology acquisition and replacement planning is done as part of the budgeting process.

i. Acquisitions managed centrally by the Computer Manager.

d. The Town has an IT Task Force, composed of Town residents, which serves to advise the Town and Town Computer Manager on IT topics and initiatives.

i. Examples: Suggested the Town pursue server virtualization, suggested a cybersecurity initiative, which resulted in an external vulnerability scan completed in September 2016.

e. Blum Shapiro reviewed the existing position description for the Computer Manager and noted the following:

i. It has not been updated since 1996

ii. The job description did not reflect present technologies, challenges or duties for a head of IT for a Town

iii. Did not specifically reference duties related to IT Strategic Planning

iv. The IT Analyst position description had not been revised since 1999

v. The Computer Manager expressed that more time is needed to be devoted to strategic planning and policy development within the Town.

3. Town IT policies and procedures are not extensive. BlumShapiro was provided with the following:

a. Town of Simsbury Disposal of Electronic Equipment Policy (2016 policy).

b. Document describing Method and Frequency of Backup for Town of Simsbury Servers (current as of 2016).

c. Simsbury Town Disaster Recovery Plan (created approximately 2008).

i. Does not reflect current technologies and has not been recently updated.

d. Town of Simsbury Systems, Email and Internet Use Policy (dated December 2008).

i. Policy was not readily retrievable and content was dated.

4. Town IT Infrastructure and Inventory

a. A formal town IT infrastructure inventory process and method (master inventory list, periodic verification) does not exist.

i. The Town retrieves information from Active Directory for connected devices using a shell script to produce reports.

1. This method provides information about desktops and laptops only.

2. Does not account for other devices, tablets, mobile phones, network infrastructure, and peripherals (copiers and printers).

b. IT Infrastructure primarily consists of:

i. Physical and Virtual Servers

1. Simplivity OmniCubes with VMware

2. Windows 2008 Server

ii. Approximately 200 desktops spread across multiple locations.

1. Most are Windows 7 Pro, with limited Windows XP Pro desktops remaining.

a. The IT Department has tried to virtualize Windows XP to provide an additional security layer.

iii. Cisco Network Switches primarily, with three HP Switches at the Library.

iv. Cisco ASA Firewall / Network Security Appliance.

5. <u>Major Town IT Projects</u>

a. Fiber Connectivity Plan

i. All physical locations on Hopmeadow Street are connected with fiber.

ii. Town Hall connects to the High School with fiber.

iii. Working to ensure quality and redundancy of fiber /network connection with School District.

1. Next step involves building in redundancy in the "loop" with a bidirectional connection to the CEN.

a. Town is presently connected to High School via fiber, adding a connection to Central School will build redundancy.

iv. Water Pollution Control connects through a VPN/internet connection.

b. Virtual Desktop Pilot.

i. Town has several devices in production.

c. Simplivity Server implementation.

i. Completed in 2015 in coordination with a vendor.

ii. Represented a "hyperconverged" architecture, combining many types of network infrastructure into one box.

iii. Backup and recovery functionality was tested extensively during implementation.

6. Town IT training budget is limited.

a. The Computer Manager has utilized the budget for conferencing, with limited training for the IT Analyst position.

b. Generally, both staff have been self-taught and learned technical skills on-the-job.

i. The Computer Manager expressed a need to have training in the following areas:

1. Policy and Strategy Development.
2. Technology Security.
3. Active Directory Network Management.
4. Simplivity Infrastructure Management.

7. Town IT Security Concerns

Some basic security practices are in place to assure many common information security threats are deterred, however, the Town relies largely on obscurity, and may be vulnerable to advanced or targeted attacks. An example of specific areas for concern are noted below.

a. The Town has not undertaken an extensive effort to identify the all locations of sensitive data, which may require additional protection such as encryption. The Town has identified sensitive areas, such as the server for the Financial System, and should seek to encrypt data at-rest and in-use if possible.
    i. Exception: Additional controls are in place over Police Department Systems.

b. Security Policies
    i. Policies and procedures related to security were not in place.
    ii. Basic security is in place, but areas of exposure exist.

c. Physical Security
    i. There are two server rooms at Town Hall, one in the basement and one on the first floor.
        1. Each secured by key entry, however, basic monitoring and detective controls were limited, such as visitor/access logs and a policy designating who has access.
            a. The server rooms have some video monitoring since they are outside the Police Offices.
        2. Server rooms appear to have evolved over time and are lacking general sophistication, given the size of the Town of Simsbury
            a. Basement server room could potentially be exposed to water issues in the event of flooding. There are flood alerts and temperature monitors in place.
            b. First floor server room appears to double as a storage room, and the location is a former office. The exterior window, if broken, would allow direct physical access to critical Town infrastructure.
        3. Physical access to active network ports is possible, due to the public nature of Town facilities.

a. Network ports are not disabled or restricted when not in use, and potentially exposed to an unauthorized person physically connecting to a port and inspecting data.
    i. E.g. A rogue wireless access point could be installed in one of the open ports, allowing a malicious person to access the network from outside the building.
b. The town is not presently using any method to detect unknown devices.

d. Patching Desktops
    i. Although patch management practices described were generally sound, some are manual. We noted that no vulnerability scanning is performed to identify missing patches, or the presence of unnecessary "services."
        1. We asked that Town IT staff run Microsoft Baseline Security Analyzer (a free program that confirms patching and general security) scanning three random desktop devices. We confirmed that patches are not missing and no major areas of exposure were identified.
e. Network User Security
    i. Basic user security settings are in place as of September 2016, to align with Police Department Requirements.
        1. 8 Character Minimum Length
        2. Password complexity requirements
        3. Password History requirements
        4. Password expiration after 90 days, minimum age of 7 days.
        5. Account lockouts after 5 invalid attempts.
f. Network security scanning is generally not performed.
    i. Town IT staff mentioned that they are considering hiring a vendor to perform these scans, and that School District IT have been involved in preliminary discussions.

ii. Some scanning is done by a third party vendor due to payment processing requirements.

g. No web content filtering is done to limit employee access to web sites, which could expose the Town to malware unnecessarily were an employee to visit a compromised site.

i. Anti-malware is installed on desktops and servers, limiting some end point exposure.

h. Barracuda email security devices are in place in two separate environments.

i. Some events are logged and monitored at the server level, but logs are not monitored routinely for adverse events.

8. Miscellaneous Observations

a. In order to allow more time and attention with respect to maturing and advancing IT strategies, IT security, and general processes, additional personnel will likely be required.

i. Per discussion with the Computer Manager, the position that is presently budgeted for but vacant could be filled with a first level technology support person, which could free up some time.

b. Because the Town business continuity / disaster recovery plan is outdated, there is a high likelihood that the Town's various business requirements for backup/recovery points and recovery times have not been defined and may be out of alignment with current recovery methods and respective recovery times.

c. The most common area of need expressed during our interviews with Town Department personnel related to mobile devices and telecommuting.

School District IT Organization, Infrastructure, and Processes

9. The Simsbury School District Technology Department consists of the following employees:
    a. Director of Systems Technology, overseeing:
        i. Network Manager
        ii. Lead Computer Technician
        iii. School Technicians (3)
            1. These positions have experienced some instability and turnover recently.
        iv. Software Specialist (shared with Instructional Technology)
        v. Student Data Systems Coordinator
        vi. Secondary Technology Assistants (2)
        vii. Data Consultant (non-employee)
    b. Director of Instructional Technology, overseeing:
        i. Library Media Specialists
        ii. Library Specialists
        iii. Instructional Coach
        iv. Software Specialist (shared with Systems Technology)
    c. School District IT staff are tasked with supporting IT utilization throughout the district, at each school location including in-class educators, in leveraging advanced technology tools in achieving classroom and curriculum objectives.
        i. Provide nearly 100% of the support for the email server that is shared between the Town and School District
        ii. Provide the majority of Active Directory Administration for the shared domain
        iii. No formal documented agreement or memorandum of understanding exists for these services

d. Employees request IT services in person, via phone, or email. IT recently implemented the School Dude system, which has a component that allows for submission and tracking of service requests. Adoption has been slow to this point for users.

e. The most frequently cited issue with respect to IT support for the School District related to the use of peripheral devices in the classroom, stemming from initial incompatibilities with the Desktop Virtualization project.

    i. Absenteeism and a period of turnover in technician positions, and a lack of technician knowledge of virtual desktops often contribute to service issues. This has been since been mitigated.

f. The School District is considering repurposing a position to focus on IT clerical work, alleviating some of the task work performed by the Director of Systems Technology and the Network Manager.

10. <u>School District IT Leadership, Direction and Strategies</u>

a. School District IT strategies largely focus on supporting the execution of curriculum and teaching activities in the classroom, and administering and operating the schools and district offices.

b. Two Director of Technology positions exist, each reporting up through separate channels.

    i. Director of Systems Technology and his team focus on supporting and maintaining all technologies, providing data analysis services and network infrastructure administration.

    ii. The Director of Instructional Technology and her team focus on enabling technology in the classroom.

    iii. Several interviewees stated that it was less than ideal to have two Directors with separate reporting relationships. It makes discussions about priorities and strategies more cumbersome.

        1. Some noted that many districts are going with two IT Directors, but with a single-reporting structure.

c. A Strategic Technology plan is required to be created due to state education requirements.

    i. Created jointly by the Director of Systems Technology and the Director of Instructional Technology.

        1. Every three years, with separate budgets form classroom equipment and general support infrastructure.

11. School District IT policies are not formally documented.

    a. There are basic computer use policies in the Employee Handbook and Student Handbook.

        i. Based upon Connecticut Association of Boards of Education (CABE) examples.

    b. Other IT procedures are informal, and not likely documented or supported by an overarching policy.

12. School District IT Infrastructure

    a. The School District does have a formal inventory entry process to record and track technology assets.

        i. Network Manager devotes a portion of his time to receiving equipment, confirming purchase orders and packing slips, tagging assets, and recording them in inventory.

        ii. The School Dude system is in the process of being implemented for Inventory tracking.

            1. Previously, there were several spreadsheets and databases that were used to track the various devices, and limited and inconsistent information was available. This approach requires significant manipulation of data.

    b. A program called Lansweeper is used periodically to update the inventory and inspect devices on the network.

    c. Infrastructure consists of:

        i. Physical Servers (Windows 2008), some of which are Domain Controllers.

            1. Many of the physical servers have been decommissioned and replaced with virtual servers.

        ii. Physical Servers with VMware (hosts.)

        iii. Virtual Desktops (Classrooms, Labs, some administrative systems) on “dummy terminals”.

        iv. Physical Desktops and Laptops.

        v. Cisco Switches and Firewalls.

        vi. iPads, Tablets, and Chromebooks.

        vii. Variety of printers, projectors, smartboards and classroom tools.

13. Major School District IT Projects

a. Desktop virtualization project nearly completed (approximately 3-4 year project).
    i. Extends the life of hardware purchases.
    ii. Throughout the project there were unanticipated issues with incompatibilities between virtual desktops and classroom tools and peripherals. Many of the issues have been resolved over the course of the project.
b. The School District is moving toward a 1:1 ratio with Chrome Books at the High School.
c. The School District will be expanding and upgrading the server room located in the High School to account for insufficient space and environmental controls.
d. Network Manager is updating Domain Controllers to Windows Server 2012 from Windows Server 2008.
e. Network Manager has been doing some extensive clean-up work for network and server infrastructure.
    i. Walker group conducted a high-level network review at the beginning of 2013.
        1. This report was provided to Blum Shapiro as part of this review.
        2. Discussed with both the Director of Systems Technology and the Network Manager, who had a number of efforts directed toward resolving the issues.
    ii. The majority of the issues identified in the Walker Group report are now non-applicable.
        1. Desktop Virtualization resolved many of the issues with desktops.
        2. Network and Server recent network an server upgrades resolve many of the issues.
        3. Most of the major remaining issues should be fixed within the next year.

14. Several staff noted that the School District IT training budget is not expansive, as is time allotted to training.

a. Time allotted to cross-training is limited as well.
    i. During the school year most IT staff are busy.

ii. Off-season (during the summer months) is when most of the major projects are completed.

b. Interviewees expressed need in the following areas.

i. Providing support for users with Tablets and iPads.

ii. Providing support and troubleshooting for virtual desktop environment.

c. BlumShapiro also believe the School District could benefit from formal training in the areas of policy development and Information Security.

15. School District IT Security Concerns

a. The School District has not undertaken an effort to identify the location of sensitive data, outside of PowerSchool and SNAP which may require additional protection such as encryption.

b. Some basic security practices are in place to assure many information security threats are deterred, however, the School District, like the Town, relies largely on obscurity, and may be vulnerable to advanced or targeted attacks. Examples of some concerns are listed below:

c. Security Policies

i. Policies and procedures related to security were not in place.

ii. Basic security is in place, but areas of exposure exist.

d. Physical Security

i. The Server Room is at the High School, and is accessible via key entry.

1. Because the room was in a state of transition (will be completed in early 2017), it was difficult to tell what basic security controls were in place.

2. New physical and environmental controls will be in place.

ii. Physical access to active network ports is possible.

1. All ports are active and potentially exposed to an unauthorized person physically connecting to a port and inspecting data.
    a. E.g. A rogue wireless access point could also be installed in one of the open ports, allowing a malicious person to access the network from outside the building.
2. The School District is implementing a tool called Insight, which could allow for auto-discovery of new devices. A tool called "Airewave", that the School District has, could also be used to detect rogue wireless networks.

e. Patching Desktops
    i. Patch management practices described were excellent, especially given the virtual desktop environment.
        1. We noted that the underlying "dummy terminals" in the virtual desktop environment were not required to be patched, because they in essence do not access any resources.
            a. The School District may want to consider performing penetration tests to confirm this is the case.
    ii. We noted that no vulnerability scanning or penetration testing is performed.
f. iPad Security
    i. The Lead Technician mentioned that minimal security is configured for iPads that are in use.
        1. Some could contain ancillary protected personal information.
g. Network User Security
    i. Basic user account security settings are not generally enforced in Active Directory:
        1. No password complexity requirements, password expiration, screensaver lockout, etc.
            a. 6 character minimum password length.
            b. Locked out for 5 minutes after 10 invalid attempts.
h. Network security scanning is generally not performed, but they are considering collaborating with the Town on this.

i. The School District does not have a formally documented Disaster Recovery Plan

i. There are presently sound backup and recovery procedures in place that have undergone recent testing by the Network Manager to verify their effectiveness.

j. Teachers may use cell phones to access school district email.

i. School District does not have a Bring Your Own Device (BYOD) policy.

III. Recommendations

1. Implement an IT Governance / Steering Committee with internal representation from the Town and School District, to provide guidance and direction for mutual IT service and strategy development initiatives.
    a. Consider including the following members at a minimum:
        - Town Finance Director, Town Director of Administrative Services, School District Business Manager, Town IT Manager, School District Director of Systems Technology.
    b. Benefits include:
        - Collaboration opportunities will no longer need to rely only on the Town Computer Manager and School District Director of Systems Technology routinely meeting as deemed necessary by each individual.
        - Where like goals are in mind, strategies can be implemented which may have both hard and soft cost savings.
    c. A Town representative of this Committee may provide updates as necessary to the Town IT Task Force.

2. The Town and School District should collaborate when possible on areas of mutual strategic benefit and cost savings.

    The Town and School District collaborate mostly on an informal basis as opportunities arise. It is largely dependent upon the Town Computer Manager and the School District Director of Systems technology recognizing a joint interest. During this review, Blum Shapiro noted several opportunities where collaboration could benefit each side:

    a. Cloud Technology
        - When considering replacing any systems that are currently hosted locally but have "cloud" licensing options.
        - Backup cloud storage.
        - *Potential Savings:* in joint licensing, and soft costs related to researching and implementing methods.
    b. General Advancement of Information and Cyber Security Practices.

- *Potential Savings:* in purchasing and deploying solutions, and soft costs related to researching and implementing methods.

c. Back-up and Recovery Methods, and Disaster Recovery Plan Development.

- *Potential Savings:* in purchasing and deploying solutions, and soft costs related to researching methods and documenting plans.

d. Infrastructure and "Hyperconvergence" Strategy.

- The Town recently undertook a strategy to implement Simplivity OmniCube architecture, which combines multiple layers of network infrastructure into one box, reducing footprint and increasing integration. This concept is referred to as hyperconvergence.
- The School District is in the process of virtualizing servers, and upgrading architecture.
- *Potential Savings:* cost savings may be realized if the Town and School District are able to standardize purchasing and deployment of similar architecture, as long as licensing restrictions do not exist.

e. Mobile Computing

- The School District deploys tablets and iPads, and there may be some benefit to the Town.
    1. Some interviewees for the Town suggested a need for mobile device technology.
- Potential Savings: soft savings primarily in the form of shared lessons.

f. Server Room Security

- Town Hall has two server rooms that have evolved organically over time. The Library also has a server room.
- The School District is upgrading the server room in the High School.
- The Town should consider sharing server room space.
- *Potential Savings:* cost savings are possible if there is an increase in collaborative space, purchases of systems related to environmental protection (heating/cooling/power).

g. General IT Policy and Procedure development.

- *Potential Savings:* soft costs can be shared if the workload for developing standards and templates is shared.

h. Network, Active Directory and Exchange Server maintenance.

- Collaboration already exists regarding Active Directory and Exchange.
- The School District has some expertise that may benefit the Town IT staff, who expressed a need for Active Directory training.
- *Potential Savings:* a cost avoidance for formal training can be realized if cross-training is possible and beneficial.

i. Virtualization Strategies

i. Desktop environment

- The Town may be able to learn lessons from the School District.
- Mutual strategies can be shared for virtualization.
- *Potential Savings:* soft costs due to lessons learned. Over time, PC replacement savings may be realized.

j. Software and tools related to IT asset inventory and service requests.

- The School District is implementing tools related to School Dude, that could have some benefit if deployed by the Town IT staff.
- *Potential Savings:* shared licensing and implementation costs may be realized if solutions meet mutual needs.

3. <u>Establish a Memorandum of Understanding / Agreement that defines and acknowledges collaborative efforts between the Town and School District</u>

a. There is not presently a documented agreement in place to acknowledge any level of collaboration. Consider including, at a minimum:

- The services provided by Town IT staff to Board of Education technology located in Town Hall.

- The Exchange (email) and Active Directory administration services provided by the School District.
- Collaborative efforts related to the IT Governance / Steering Committee.
- Collaborative policy and strategy development efforts, including those related to Security.
- Collaborative budgeting or purchasing activity.

4. Define and clarify responsibilities for IT Leadership and Strategy-development, while investing in IT governance/ leadership training for those in positions of responsibility.

    a. Three distinctly different IT service areas exist between the Town and School District. The three individuals at manager/director level may be challenged to lead any potential future "shared services" IT environment, or mature the processes and strategies in their respective areas without proper training.

    b. The position description for Town Computer Manager's position does not reflect present duties or expectations for setting strategies. Many of his practices are self-taught, having limited exposure to formal training on leadership or governance frameworks and practices.

    c. The School District has two Directors of IT, each report to different departments. Each has technical strengths that align closely with their respective area of emphasis. A formal framework for IT governance and leadership has not been implemented.

    d. Significant progress can be made toward improving leadership and service delivery by adopting a formal governance framework, training IT Managers/Directors, and "right-sizing" governance for both the Town and the School District. A collaborative approach to choosing a framework will be beneficial.

5. Collaborate on the development of formal IT policies, standards, procedures and plans

    a. Generally, the lack of documentation across the board reflects a relatively low level of IT service/process "maturity." Therefore, it relies on individual manual efforts to ensure practices are consistent.

    b. Basic policies are in place outlining end user responsibilities, otherwise policy documentation is generally informal or outdated, or non-existent.

c. The Town and School District may communicate regularly, but aren't collaborating on the development of standards for common IT service delivery practices such as systems configuration and maintenance, service requests and delivery, security, disaster recovery, incident response, etc.

6. Develop a unified approach to enhance technology security practices within the Town and School District

a. Neither the Town nor the School District had formally documented IT Security Policies, Plans and procedures

b. Security risk assessments are not performed, which would typically drive the implementation of subsequent security controls. Proactive testing of vulnerabilities are not performed to identify exposures.

c. Both the Town and School District each rely largely on a security-through-obscurity approach. Each described sound basic methods used to secure systems components, such as patching, firewalls, anti-virus and anti-malware, email scanning and basic security for provisioning new devices. Alerts are configured where available, and certain security log information is retained to investigate issues that may arise, but it is not proactively monitored. Generally speaking, these practices will deter the majority of cyber threats, however, both are likely exposed to more targeted, focused threats.

d. Each expressed interest in pursuing vulnerability/penetration testing scans. This is a solid best practice.

e. The School District can improve basic user account security (ex. Password complexity and expiration), at a minimum, consider:

- Minimum password length – This should be configured to be no less than 8 characters.
- Password complexity – Configure Active Directory (AD) to require complex passwords to include alpha, upper case, numbers and special characters.
- Password change – This should be configured to require a new password every 120-150 days.
- Password history – AD should be configured to track and store the last 5 passwords so users can't reuse them immediately.
- Password lockout count – A user account should be disabled after 3 unsuccessful login attempts.
- Screen Saver – This policy should be set to 30 minutes or less before a password is required by an authorized user.

f. System backup practices as described are sound and appear sufficiently frequent to assure backup data it is available to recover. Each has recently tested full and file-level restores, although documentation was not available to summarize the results. The Town does have back-up procedures documented, but lacks a useable recovery plan. The School District is presently working on creating documentation for backup and recovery.

g. Physical security for Town server rooms is very basic and unsophisticated. There is a natural opportunity for shared ideas due to upgrades scheduled in the School District server room.

h. Isolating Windows XP machines through segmentation or virtualization.

7. Free up IT Manager and IT Director resources to allow more focus on collaboration, strategies and documentation.

   a. Fill the open IT position at the Town with a Level 1 support position and shift some of the burden for troubleshooting and administrative tasks to from the IT manager to this position, as necessary.

   b. Shift clerical tasks away from the School District Network Manager as appropriate to free up time.

      - At a minimum, consider shifting duties related to asset recording, tagging and inventory.

   c. Implement solutions (ex: School Dude) as appropriate to minimize time required to manipulate data for IT asset inventory.

8. Establish a training plan to ensure IT employees tasked with supporting technologies are sufficiently knowledgeable

   a. Town IT staff have not had recent formal training, relying mostly on self-taught approaches and internet research to learn. They indicated a desire for more formal training on Active Directory Administration, Administering the Simplivity Infrastructure, general information security and training related to policy development.

   b. School District IT staff expressed lesser demand for technology training, although technicians could benefit from training related to supporting and trouble-shooting the virtual desktop environment and iPads. In addition, information security training and policy development training could be beneficial.

   c. The School District's Network Manager should be leveraged, as necessary, to cross-train the Town IT staff on Network / Active Directory administration.

IV. Appendix

A. Acknowledgements

This project relied heavily on information that could only be obtained from the employees of the Town and School District of Simsbury. Our challenge was to accumulate key information and as many viewpoints as possible in a compressed amount of time. A lot of information and viewpoints were identified through individual interviews.

Interview Sessions – 29 individual interview sessions, consisting of representatives from the Town and School District of Simsbury, were conducted over the course of the project. These sessions gave employees from all aspects of the Town and School District the opportunity to share ideas and identify specific needs relevant to their departments.

Administration and staff were asked to consider the following seven questions:

1. What technology or systems are essential to your job? What key information is currently gathered, processed and /or produced within your area?
2. What are the problems/obstacles experienced within your area as it relates to the current systems and technology?
3. How do these problems affect your ability to deliver service? What changes would you make to improve the flow, access and/or retrieval of information within your department?
4. Are there specific technology needs that could make your service delivery more efficient, effective, or convenient?
5. What software capabilities (functions/features) are critical to your needs that are not currently available in your present systems?
6. What software or technology capabilities have been customized to meet your needs?
7. If you presently have a role or responsibility in providing IT Service delivery, what challenges to you face in providing services to your users?

The responses to these questions were evaluated for common themes and specific issues that show how technology is managed within and between the Town and School District.

The following groups were directly involved in providing information for the Simsbury School District and Town IT Operations Assessment. The Blum Shapiro Team thanks all who participated for their time, knowledge and efforts. The individuals that participated included:

Town and School District of Simsbury

Town Staff	
• Rick Bazanno, Computer Manager	• Tom Cooke, Director of Administrative Services
• Brett Marchand, IT Analyst	• Gerry Toner, Director of Culture, Parks and Recreation
• Jeff Shea, Town Engineer	• Taryn Rea, Recreation Supervisor
• Mickey Lecours-Beck, Director of Social Services	• Tina Labrecque, Police Chief's Secretary
• Kathleen Marschall, Senior Center Coordinator	• Laurie Sousa, Payroll Clerk
• Sean Kimball, Interim Director of Finance/Treasurer	• Peter Ingvertsten, Police Chief
• Nick Boulter, Police Captain	• Fred Sifodaskalakis, Police Lieutenant
• Matt Christian, Police Training Sergeant	• James Rabbitt – Director of Planning
• Lisa Karim, Library Director	• Lisa Heavner, First Selectman
• Tom Roy, Director of Public Works	

School District Staff	
• Matt Curtis, Superintendent of Schools	• Brenda Redderoth, Lead Computer Technician
• Erin Murray, Assistant Superintendent	• Jeremy Marin, Software Specialist
• Jason Casey, Director of Systems Technology	• Cindy Heffernan, Student Data Systems Coordinator
• Joncia Lytwynec, Director of Instructional Technology	• Ed Lyman, Data Consultant
• Ray Vernacatola, Network Manager	• Burke LaClair, Business Manager

B. Outline of Selected Policies and Procedures

General Computer Security Policies Outline

A Computer Security Policy document should contain IT security policies that are reviewed and practiced by all managers, supervisors and professional staff that access the organization's systems. This document should provide guidance regarding security policies as they relate to the organization's goals, beliefs, ethics and responsibilities; and identify the security objectives. Minimum elements of computer security policy and formal procedures should include the following:

a. Security Organization

- Confirm and document roles and responsibilities of security
  - Who manages and directs security program
  - Who monitors and reviews security breaches and violations
  - Who participates in the security program
  - Who grants access rights and log-in capabilities
- Document enforcement of security policy and procedures
  - Disciplinary actions and steps
  - Termination actions
  - Outside authority involvement

b. Logical Security

- Confirm the use of PC security
  - Document if software and/or hardware can be implemented on a PC
  - Confirm who grants approval
  - Document what security prevention steps have implemented on the PC
  - Screen saver
  - Other security measures
  - Document how and where files should be stored
- Confirm the use of network security
  - Document usage and protection of passwords
- Confirm the use of application security
  - Document usage and protection of passwords
- Confirm the use of virus protection software
- Confirm the use and protection of firewall security
- Confirm use of remote access capabilities and security surrounding it

c. Managerial Security

- Confirm process by which user ID's and passwords are created, modified and deleted
  - Who performs these tasks and grants network and application access
    - Confirm authorization process
- Confirm how third party vendors can access the system
  - Document security process and procedures for vendors
- Confirm who owns company information
  - Document how information can and should be used
- Develop Password Policies including:
  - Password length and composition
  - User ID lockout policy (after unsuccessful attempts)
  - Password non-disclosure and sharing
  - Periodic password changes
- Termination Policies
  - Confirm employee termination process and disabling system access

d. External Security

- Develop Internet Policies including:
  - Acceptable usage
  - Access to sites
  - Downloading of software
  - Content filtering
  - Monitoring
  - Software licensing

e. Physical Security

- Confirm access to server room
  - Use of key\badge security
  - Locking of server room
  - Sharing of key\badge security
- Confirm the storage and locking of critical documents
- Confirm procedure for removal and return of documents

General Disaster Recovery Recommendations

Create a documented disaster recovery plan to be kept off-site. Although the plan does not need to be overly elaborate, it should include the following elements:

a. Data
- ❑ Confirm and document where backup tapes are stored off-site (i.e. who has them and how are they labeled).

b. Equipment
- ❑ Inventory all critical equipment and identify model numbers, serial numbers and configuration information. In case of a disaster, this will allow for easier purchasing of equipment and filing of insurance claims.
- ❑ Inventory key software applications and identify respective version numbers, operating system information, and identification/activation codes.

c. Facilities/Operations
- ❑ Create a checklist that identifies the appropriate priority and steps/procedures to take in case of an emergency and/or disaster.
- ❑ Confirm how each remote location will be used in case of a disaster. This includes identifying the minimum amount of space and utility requirements (i.e. electrical power, telephone, network wiring, office space and storage space requirements).
- ❑ Develop a list of key contacts and phone numbers (i.e. home phone, cellular, office phone, direct extension number, and pager,) including:
  - Telephone system/equipment vendor
  - Telephone customer service representative
  - Computer/Network services
  - Key employees
  - Insurance agent
- ❑ Document an agreement with your hardware/network vendor that confirms roles, responsibilities and costs for the timely replacement of key hardware/software. Within this agreement, the vendor's response time including hardware/software acquisition and setup should be confirmed.
- ❑ Provide cross training to personnel on the overall network infrastructure and software application. This person(s) should be very familiar with the documented Disaster Recovery plan. Having additional personnel knowledgeable in this area will significantly minimize the overall risk to the organization and help the disaster recovery process.
- ❑ Confirm and test that current backups contain data, programs and operating system information. In addition, on a quarterly basis, test to confirm that the tapes are readable and information can be recovered.
- ❑ Users should be forced to store all of their electronic files and documents on the network. This will significantly help during disaster recovery and provide increased security to all documents and files.