Town of Whately

Strategic Planning Best Practice

Prepared By: The Office of Municipal & School Technology

EOTSS | Executive Office of Technology Services & Security

Image: Whately Town Hall[1]

Introduction

Whately is a town in Franklin County, Massachusetts, that lies along the western banks of the Connecticut River in the Pioneer Valley. Originally incorporated in 1771, the Town now has a population of 1,496 and median household income of $71,927[2]. Whately's rich history, culture, and proximity to employment centers in Hampshire and Franklin counties has given the area a reputation as a good place to live and raise one's family. Town officials have made efforts to retain much of its abundant natural resources, as well as its historic character. With much to protect and preserve, the Town signed a Community Compact agreement on April 27, 2017. Through the Community Compact program, Whately received grant funds to develop a Strategic IT Plan that would provide an analysis of the Town's current IT infrastructure and recommendations for advancement. This report contains a high-level summary of the work the Town completed with Rutter Networking Technologies. Due to the sensitive nature of the original findings report, it will not be available for public consumption.

[1] Taken from the Town's Website.

[2] "Community Facts." United States Census Bureau. *American FactFinder*. Accessed on September 26, 2018. https://factfinder.census.gov/faces/nav/jsf/pages/community_facts.xhtml

Project Process

The Town of Whately became a member of the Community Compact Cabinet in April of 2017. They requested assistance from the State and received grant funding to develop a comprehensive IT strategy and implement the necessary equipment to improve the efficiency of town operations and security of the Town's data. The Town worked with Rutter Networking Technologies to perform a comprehensive assessment of their IT environment, with special emphasis on business continuity, disaster recovery and security processes.

BUSINESS CONTINUITY/DISASTER RECOVERY ASSESSMENT

Business Continuity and Disaster Recovery (BCDR) is an essential element in any IT environment. As part of their overall assessment of Whately's infrastructure, Rutter payed special attention to the Town's current BCDR practices, identified any gaps that were present and provided suggestions for remediation. According to Rutter, "the key to a successful disaster recovery is to have a (emergency plan, disaster recovery plan, and continuity plan) plan well before disaster ever strikes." Organizational contingency plans should address potential disaster scenarios including, but not limited to power outages, IT system crashes, file corruption, and hardware failures.

Rutter conducted a Business Impact Analysis, where they evaluated Whately's business processes using objective measures including financial loss, legal and regulatory issues, and customer impact. Using this objective data, they were able to identify critical applications that support those processes and determine quantifiable DR goals for each. Rutter used the terms Recovery Time Objective (RTO)[3] and Recovery Point Objective (RPO)[4] to identify and document DR standards for each application.

[3] RTO - is the duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in continuity/

[4] RPO - describes the interval of time that might pass during a disruption before the quantity of data lost during that period exceeds the Business Continuity Plan's maximum allowable threshold or "tolerance."

Using the following criteria, Rutter conducted a thorough examination of the Town's BCDR practices. At the end of the engagement, Whately was given a score which rates how well they are performing standard BCDR tasks, a list of recommendations and next steps.

Area	Associated Tasks
Basic Planning	• Confirm participation, sponsorship from Town officials • Ensure/BC/DR is sufficiently funded and included in the budget • Succession team available for refinement and execution of BC/DR plan • Contact information available for succession team (including vendors) • Comprehensive BD/DR plan • Decision hierarchy to prevent delays when a disaster takes place • Identity rally point for the execution of BD/DR plan • Established application SLAs • Keep BC/DR plan available in for accessibility in more than one location • Evaluate current backup and recovery methodology
Communications	• Develop a crisis communication plan for internal and external communications • Include website and social media pertinent to the City • Create an internal list of key individuals who should be contacted in a crisis • Ensure all parties are aware of the decision-making hierarchy • Identity application stake holders per key applications
Continuous Improvement	• Maintains a regular schedule for testing disaster/disruption scenarios • Integrates testing with normal business operations • Identify deficiencies in both planning and procedures • Integrate learnings after each BC/DR test and audit • Review and evolve the BC/DR plan and production changes • Assessing the response capabilities of the recovery team to determine if • additional resources and training are needed • Keep BC/DR on the annual budget to guarantee on-going investment and support • Add redundancies and backups as needed to support the contingency plan

NETWORK ASSESSMENT

In addition to BCDR practices, Rutter also evaluated Whately's network infrastructure focusing on redundancy and throughput. Redundancy was evaluated using the following layers as guidelines. Upon the completion of this activity, the Town was given a score to summarize the state of their network.

Layer 1 – Physical

- Are the devices in use considered enterprise class?
- Are the devices in use under a manufacturers support contract in case of hardware failure?
- For each device interconnect, do they have dual connections between each other?

Layer 2 – Data Link

- Are the devices considered 'managed' network devices?
- Is each device capable of using VLANs for network segmentation?

Layer 3 – Network

- How routing is controlled within the environment?
- Are there multiple paths and redundancy designed within the environment for access to business-critical applications and the internet?

SECURITY ASSESSMENT

Rutter reviewed the Town's security policies and technical controls, as they are critical components to a secure environment. Using the criteria below, they were able to gain insight into Whately's security posture and evaluate the access controls, visibility, and response of the network. Following this exercise, the Town received a score to summarize the state of their network security.

Area	Evaluation Criteria
Inventory of Authorized and Unauthorized Devices	• Does the organization have an actionable inventory of devices on their network? • Does the organization have logging enabled for their DHCP services to provide knowledge of what devices were active on the network at any given time? • Does the organization have a Bring Your Own Device policy and how is it enforced?
Inventory of Authorized and Unauthorized Software	• How is software updating performed? • Does the organization have support contracts for their software (allowing for upgrades and patches)? • Is there an actionable list of authorized software installed on each system? • Can the end user install software on their own workstation without approval?
Secure Configurations of Workstations and Servers	• Are workstations and servers deployed from images? • Are images updated regularly with software updates and patches? • How is patch deployment performed? • What are the procedures for remote administration of workstations and servers?
Vulnerability Scanning	• Are there vulnerability scanning tools in place? • What is the remediation time for vulnerabilities found in systems?
Malware Defenses	• What antimalware tools are in use? • Is central management and reporting in place for the antimalware tools?

	• Are attachments for emails scanned prior to allowing them into the organization?
Wireless	• What method of authorization and encryption is used for internal wireless networks? • What is the method used to provide guest wireless access?
Skills Training	• How often is security awareness training performed for the users within an organization? • How often is technical security training provided for the IT staff within an organization?
Secure Configuration of Network Devices (switches/routers/firewalls)	• What is the organizations firewall policy for permitting and denying traffic to and from the internet? • What method is used to authenticate to all network devices?
Limitation and Control of Network Ports and Services on Each System	• Is a software firewall deployed on workstations and servers? • Is there a process in place for port scanning to determine if any new applications are deployed? • Are there hosted services within the organization that are visible from the internet and how are they secured?
Administrative Privileges	• Are there separate accounts in place for administrator's day-to-day activities from their administrative tasks? • How is password complexity enforced? • Do the users have administrative rights to their own workstations?
Boundary Devices	• Does the organization use a next generation firewall (NGFW)? • How often are the advanced features updated (such as IPS, Antimalware)? • Does the organization have remote access via VPN or other method configured?
Maintenance and Monitoring of Device Logs	• Does the organization use a central logging server for all devices? • What is the current log retention policy for all devices? • Do the devices all have their times synchronized for the purpose of log timestamping?

Controlling Access Based off Need to Know	• Do the organizations critical functions have limited access to only those that require access? • Is there audit logging in place for these functions to know who accessed them, from where and for how long?
Account Monitoring and Control	• Is there a process in place for account creation/modification/deletion? • Are screen locks enabled on all systems? • How often is a review conducted of all active accounts within the organization? • What is the current lockout policy for incorrect logins?
Incident Response Planning	• Is there a documented incident response plan in place? • When was that plan last tested for accuracy?

Conclusion

The Town of Whately has displayed dedication to improving the security and efficiency of their IT environment. After their engagement with Rutter Networking Technologies was complete, Town officials immediately began to implement the recommendations provided in the final assessment report. The Town of Whately has successfully completed their Community Compact objective and are strongly encouraged to continue implementing IT best practices going forward.