Grafton, MA – Business Continuity Best Practice

Prepared by: Allison Poirier & Amelia Percentie

Office of Municipal & School Technology

EOTSS | Executive Office of Technology Services & Security

Image: Grafton Common[1]

Executive Summary

The Town of Grafton adopted a Business Continuity best practice as part of a Community Compact agreement with the Baker-Polito Administration in December 2015. At the time, the Town had recently merged municipal IT services with the School Department, and wanted to ensure seamless recovery in the event of a disaster. Like many cities and towns, Grafton is faced with the challenge of supporting their IT environment with limited resources. They recently migrated their network management from a vendor-supported model to an in-house model, which is now managed by IT staff at the high school. Grafton's Town Administrator, Tim McInerney, and EOTSS partnered to create a strategy that would enhance the Town's business continuity process. This approach included the creation of a documented Business Continuity Plan and a comprehensive IT Assessment performed by Rutter Networking Technologies, which provided Grafton with a snapshot of their current technology environment. The assessment included a gap analysis, and documentation of findings and recommendations.

[1] Flickr user Paul Keleher. "Grafton Common." *Wikimedia Commons*. Creative Commons Attribution 2.0 Generic License. Accessed November 16, 2017. https://commons.wikimedia.org/wiki/File:Grafton_Mass.jpg

Community Profile

Grafton is a semi-rural town located in central Massachusetts. Originally, the Town was called Hassanamisco (place of small stones) by a tribe of indigenous Nipmuc Indians and eventually gained the name "Grafton" in 1735 in honor of Charles Fitzroy, Duke of Grafton, and grandson of Charles the 2nd. The community has a rich history with many examples of the 19th century still present in its mill sites; early American, Greek Revival, and Victorian style homes. According to the 2010 US Census, the Town's population consists of roughly 17,700 residents with a median household income of $88,712. Grafton has 12,364 registered voters and an FY2018 Operating Budget of approximately $50M[2]. Their municipal website offers a multitude of resources including a 'Boards & Committees Information Center' and 'Citizen's Guide to the Budget'. The Town is clearly invested in developing their technology infrastructure to better serve their citizens.

Project Process

Development of Business Continuity and Disaster Recovery Plan

EOTSS partnered with the Town of Grafton to create a documented Business Continuity and Disaster Recovery Plan (BCDR) Plan consisting of a Business Impact Analysis (BIA), Emergency and Disaster Recovery Strategy. They initiated this process by completing a BIA of the Town's current IT environment, essential functions, services, and systems. Grafton has completed the following BIA steps and is currently working on their Emergency and Disaster Recovery strategies.

Step 1 – Identify Essential Functions

Step 2 – Develop Findings for Each Essential Function, and the Applications/Systems that Support Them

Step 3 – Create an Action Plan for Functional Gaps (Based on Findings/Recommendations)

Step 4 – Create a Detailed Remediation Plan

[2] Town of Grafton. "FY18 Municipal Operating Budget." Accessed on November 16, 2017. https://www.grafton-ma.gov/sites/graftonma/files/uploads/fy18_budget_document_gfoa_budget_award.pdf

IT Assessment Overview

To supplement the BCDR work being done in-house, the State provided Grafton with a grant to work with a vendor that would evaluate their IT infrastructure and current BCDR practices. The Town hired Rutter Networking Technologies to perform a comprehensive IT assessment with focus on Business Continuity, Disaster Recovery, Network and Security; and provide recommendations.

BCDR Assessment – Rutter used objective measures such as financial loss, legal and regulatory issues, and customer impact to evaluate Grafton's current business processes and BCDR practices. Using the objective data, they were able to identify critical applications that support those processes and determine quantifiable disaster recovery goals, namely RTO[3] and RPO[4] objectives, for each system. Rutter used the following criteria to identify gaps in the Town's BCDR environment. The results of the evaluation helped to inform Grafton's BIA and overall BCDR Plan.

BCDR Area	*Criteria: Best Practices*
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

[3] *Rutter Definition:* Recovery Time Objective (RTO) – 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] *Rutter Definition:* Recovery Point Objective (RPO) – 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".

	- 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 – To ensure network security and capacity for expansion, Rutter reviewed critical components of Grafton's network infrastructure with focus on redundancy and throughput. Redundancy was assessed from Layer 1 (physical) to Layer 3 (network aka: routing) using the following standards:

Network Component	*Standards: Best Practices*
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 evaluated Grafton's security policies and technical controls to determine how well they respond to malicious behavior. The review provided insight into the Town's security posture, with focus on three major components of their environment (I.e. access controls, visibility, and response), and the fifteen areas listed below that constitute those components.

Area	*Considerations*
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 administrators' 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

Business Continuity and Disaster Recovery is a journey, where incremental improvements are typically made over time and prioritized based on budget constraints. The Town of Grafton should continue to refine their BCDR strategy whenever new funding becomes available and aim to allocate funding to areas of their environment that would maximize impact. Through the Community Compact, Grafton received an IT assessment and completed a Business Impact Analysis, the first stage in Business Continuity planning. The Town is in the process of developing Emergency and Disaster Recovery strategies, which would complete the plan. Grafton has demonstrated a strong commitment to improving their current BCDR processes and is better-positioned to implement business continuity best practices.