Princeton, MA – Business Continuity Best Practice

Prepared by: Allison Poirier & Amelia Percentie

Office of Municipal & School Technology

EOTSS | Executive Office of Technology Services & Security

Image: Princeton, Massachusetts[1]

Executive Summary

In November 2016, the Town of Princeton, Massachusetts selected a Business Continuity best practice as part of a Community Compact agreement with the Baker-Polito Administration. Like many communities, Princeton has been updating their IT infrastructure by making small investments and finding all possible cost savings measures. Their former Principal Assessor, who assisted with IT support, retired in December 2016. In an effort to continue improving Princeton's technology environment, leadership appropriated local funding to upgrade the Town's IT infrastructure and requested assistance from the State. Leveraging state resources, Princeton received a comprehensive IT assessment from Rutter Networking Technologies and completed a Business Impact Analysis to inform new policy around business continuity and disaster recovery.

[1] Pete. "IMG_2295." *Flickr.com*. Creative Commons License. Accessed November 2017. http://bit.ly/2zSvB0H

Community Profile

Princeton is a small town located in central Massachusetts. The Town became an incorporated municipality in April 1759 and is now home to approximately 3,400 residents. Princeton was named after Reverend Thomas Prince, Pastor of the Old South Church in Boston and one of the Town's first residents. Today, the Town is a rural, mostly residential area with a lively agricultural community and picturesque landscapes.

Project Process

IN-HOUSE BUSINESS CONTINUITY WORK

Town leadership partnered with EOTSS to create a business continuity and disaster recovery strategy document that could be referred to in the event of a disaster. Through this partnership, the two parties performed a Business Impact Analysis (BIA) to identify and prioritize essential functions of the Town including their business processes and applications. These essential functions were measured by assessing tangible and intangible impacts that might result should an interruptive event occur. The results of the BIA were documented for future reference.

IT ASSESSMENT OVERVIEW

Princeton received a Community Compact grant from the State to solicit technical assistance from an IT firm. The Town hired Rutter Networking Technologies to perform a comprehensive IT Assessment on their IT environment with focus on Business Continuity and Disaster Recovery; and Network and Security. For security reasons, the final report containing Rutter's findings and recommendations for the Town of Princeton will not be published. However, the following sections summarize the extent of work that was done throughout the engagement.

Section 1 – Business Continuity and Disaster Recovery Assessment (BCDR)

The focus of this assessment was to examine the BCDR practices currently employed at the Town and to provide recommendations for enhancement. A good BCDR strategy should address scenarios including by not limited to: power outages, IT system crashes, file corruption, and hardware failures. Rutter developed a BIA for the Town, which summarized the information in their internal systems. The analysis identified critical applications that support Princeton's essential business functions based on their RTO and RPO.

- *Recovery Time Objective (RTO)* – the duration of time and 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.
- *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 strategy's maximum allowable threshold or "tolerance."

Quantifiable disaster recovery goals were set for each application including but not limited to finance, email, GIS, and tax collector systems. Rutter used the following criteria to determine the current state of Princeton's BCDR practices and identify gaps.

BCDR – Area	BCDR 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 • 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

Section 2 – Network and Security Assessment

Network Assessment – Rutter assessed Princeton's network and provided recommendations to ensure it is stable and has the capacity for growth. Layers 1 – 3, shown below, were used to evaluate redundant connections in the Town's network design.

Network Component	Network Considerations
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 – The following table contains Rutter’s criteria used to measure Princeton’s security posture. The fifteen areas listed below provided high-level insight into the Town’s access controls, visibility and response capabilities.

Area	Security Considerations
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 Princeton has already taken significant steps to improve their technology posture and should continue to prioritize these efforts, particularly around network infrastructure. Princeton has completed their Community Compact best practice initiative with the State and Rutter Networking Technologies. Deliverables include the creation of a Business Impact Analysis and an IT Assessment Findings Report, which can be used in future business continuity planning. Today, Princeton is better-positioned to employ business continuity best practices in Town.