The City of Springfield, MA

Business Continuity Best Practice

Prepared By: The Office of Municipal & School Technology

EOTSS | Executive Office of Technology Services & Security

Image: Springfield City Hall[1]

Introduction

On December 1, 2015, the City of Springfield entered into a Community Compact agreement with the Baker-Polito Administration. In their Compact, the City pledged to implement IT best practices to improve operations. They chose business continuity as their area of focus after witnessing unprecedented natural disasters in the past decade and a natural gas explosion that caused heavy damage to dozens of buildings in the downtown area. Since then, Springfield has progressively been working towards a robust business continuity and disaster recovery (BCDR) strategy, to prevent data loss, and the establishment of a fiber optic loop that would give the City greater resiliency and reliability. Through the Community Compact Program, the City of Springfield received technical assistance from the State to develop living Business Continuity Planning (BCP) documents, and grant funds to perform an IT assessment and create a map of the City's copper and fiber routes. The resulting documentation supports Springfield's goals to build a roadmap and budgeted plan for future fiber connectivity. At a time of crisis, the true character of a city shines through and Springfield remains proud of the resiliency demonstrated by residents and business as well as the many acts of neighbors helping neighbors. This report summarizes the work the City of Springfield has completed to remediate past issues and mitigate risk going forward.

[1] Daderot. "City Hall – Springfield, MA." *Wikipedia Commons*. Creative Commons CC0 1.0 Universal Public Domain Dedication. Accessed on May 15, 2018. https://commons.wikimedia.org/wiki/File:City_Hall_-_Springfield,_MA_-_DSC03295.JPG

COMMUNITY PROFILE

Known as the "City of Homes", Springfield is located in the Western part of Massachusetts in Hampden County. According to the 2010 U.S. Census[2], the population is 153,060 and the median household income is $35,742. Springfield is also known as the birthplace of basketball and is home to the Basketball Hall of Fame, drawing fans from around the world. Additionally, Springfield is known for Theodor Seuss Geisel, better known as Dr. Seuss, a celebrated author and illustrator, who was born and raised in the City. The City continues to offer many attractions, including museums , Forest Park, which is home to the zoo and the popular Bright Nights driving tour in the winter. The City will also be home to the much-anticipated MGM Resorts International casino, set to open in August of 2018.

Business Continuity Initiatives

Springfield has been working to ensure the City's essential systems and functions remain available in the event of disaster. One of their objectives in adopting the business continuity best practice, was to create a BCDR plan that would support future initiatives around fiber connectivity, to increase interoperability between municipal sites. The City partnered with EOTSS/Office of Municipal and School Technology to develop the following multi-pronged approach to address the City's challenges.

- *IT Assessment/Critical Security Controls Review* – A comprehensive review of security controls (performed by a third party), in support of ensuring a complete assessment of the environment, and integration of critical systems and functions.

- *Copper & Fiber Optic Map* – Map the City of Springfield's copper and fiber optic routes (performed by a third party), in support of expanding the routes.

- *Business Continuity Planning* – BCP (performed by EOTSS and Springfield's IT Department), in support of completing the following steps of a Business Impact Analysis: (1) Identify Essential Functions, (2) Develop Findings for Each Essential Function, and the Applications/Systems that Support Them, (3) Create an Action Plan for Functional Gaps Based on Findings/Recommendations, and (4) Create a Detailed Remediation Plan.

[2] "Community Facts." US Census Bureau. American FactFinder. Accessed on May 16, 2018. https://factfinder.census.gov/faces/nav/jsf/pages/community_facts.xhtml

IT ASSESSMENT/CRITICAL SECURITY CONTROLS REVIEW

In April 2017, Rutter Networking Technologies completed a critical security controls review for the City of Springfield and identified several items that required remediation. The following security controls were used as the basis for their findings. Details about each best practice can be found at the Center for Internet Security[3].

#	Critical Security Control	Overview
1	Inventory of Authorized and Unauthorized Devices	Actively manage (inventory, track and correct) all hardware devices on the network so that only authorized devices are given access, and any unauthorized and/or unmanaged devices are found and prevented from gaining access.
2	Inventory of Authorized and Unauthorized Software	Actively manage (inventory, track and correct) all software on the network so that only authorized software is installed and can execute. In addition, all unauthorized and/or unmanaged software is found and prevented from installation or execution.
3	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	Establish, implement and actively manage (track, report on, correct) the security configurations of laptops, servers and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings
4	Continuous Vulnerability Assessment and Remediation	Continuously acquire, assess and take action on new information in order to identify vulnerabilities, remediate and minimize the window of opportunity for attackers.
5	Malware Defenses	Control the installation, spread and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering and corrective action.
6	Application Software Security	Manage the security lifecycle of all in-house developed and acquired software in order to prevent, detect and correct security weaknesses.
7	Wireless Access Control	The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.
8	Data Recovery Capability	The process and tolls used to properly back up critical information with a proven methodology for timely recovery of it.
9	Security Skills Assessment and	For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills and abilities needed to support defense of the

[3] CIS Controls Version 7. *Center for Internet Security: Confidence in the Connected World*. https://www.cisecurity.org/controls/

	Appropriate Training to Fill Gaps	enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.
10	Secure Configurations for Network Devices such as Firewalls, Routers and Switches	Establish, implement and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.
11	Limitation and Control of Network Ports, Protocols and Services	Manage (track/control/correct) the ongoing operation use of ports, protocols and services on networked devices in order to minimize the windows of vulnerability available to attackers.
12	Controlled Use of Administrative Privileges	The processes and tools used to track/control/prevent/correct the use, assignment and configuration of administrative privileges on computers, networks and applications.
13	Boundary Defense	Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.
14	Maintenance, Monitoring and Analysis of Audit Logs	Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack
15	Control Access Based on the Need to Know	The process and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers and applications of a need and right to access these critical assets based on an approved classification
16	Account Monitoring and Control	Actively manage the life-cycle of systems and applications accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them.
17	Data Protection	The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information
18	Incident Response and Management	Protect the organizations' information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.
19	Secure Network Engineering	Make security an inherent attribute of the enterprise by specifying, designing, and building-in features that allow high confidence systems operations while denying or minimizing opportunities for attackers.

20	Penetration Tests and Red Team Exercises	Test the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker

FIBER OPTIC MAP

In November 2017, AccessPlus Communications Inc. was hired to map out Springfield's Fire Alarm copper routes and Focus Springfield's[4] fiber optic routes. As a result of this effort, maps were created and distributed to the City. Additionally, AccessPlus worked with the City GIS manager at the Department of Public Works to merge the newly created maps with existing city maps. The result is a dynamic GIS mapping tool that is maintained by the City and can be upgraded as new routes are added. Finally, they took the various documents that could be found from the Fire Alarm Division and created a database of all the buildings in the City that have (or had) fire alarm cable entrances and pull boxes. As many of these are City owned buildings, this will be valuable route information as the City expands its fiber routes. A dramatic increase in high-speed communications bandwidth is evident with the increase in public safety related traffic (internet, cameras, police radio, telecommunications, etc.).

BUSINESS CONTINUITY PLANNING

Springfield partnered with EOTSS to conduct a BCP - Business Impact Analysis (BIA). During this process, essential functions (EF) were identified and analyzed to determine criticality, and service level requirements. Public Safety essential functions cannot tolerate any down time, or loss of data. The sample below is from the City's BIA document. It shows that the Police Department uses phone and mobile networks to carry out a Mobile Communications function. The RTO (Recovery Time Objective) and RPO (Recovery Point Objective) are both 0, which confirms that this particular system cannot tolerate any outage or data loss.

EF MGMT AREA	DEPTS EF	EF DESCRIPTION	SYSTEM	RTO	RPO
Public Safety	Police Department	Mobile Communications/Cruisers	Phones/Mobile/Network	0	0

With the BIA complete, Springfield is now able to use this living document to ensure any changes are captured on a routine basis. This is a cornerstone of the City's BCP planning. Because it is a living document, it will be updated by the CIO, and tested as part of their IT Disaster Recovery Planning exercises.

[4] Focus Springfield. Community Access Television. http://focusspringfield.com/

Conclusion

Business continuity and disaster recovery is a journey, where incremental improvements are typically made over time and prioritized based on budget constraints. Springfield has implemented changes and made improvements to the City's network and backup capabilities. With two data centers, the City's end-state vision to move to expand fiber connectivity is tangible. This will provide Springfield with the resiliency required to support the essential functions and critical systems that Springfield's constituents depend on.