Town of Stoughton

Cybersecurity Best Practice

Prepared By: The Office of Municipal & School Technology

EOTSS | Executive Office of Technology Services & Security

Image: Stoughton Town Hall[1]

Introduction

Officially incorporated in 1726, the Town of Stoughton was initially an agrarian community known for shoemaking. Today, the Town is a vibrant community with a population of 28,338 and a median household income of $92,757[2]. The Town of Stoughton adopted the Cybersecurity best practice as part of a Community Compact agreement with the Baker-Polito Administration in March of 2017. Leveraging Community Compact funding, the Town retained the services of HUB Technical Services, LLC to conduct a multi-faced cybersecurity risk assessment. Several commonly exploited threat vectors were investigated to gain an understanding of the effectiveness of the security controls in place and to identify actions to minimize risk to the Town. Findings and prioritized recommendations were provided to the Town as an aid to continue improving their IT security posture.

[1] Stoughton Town Hall. Accessed on February 1,2019. https://www.stoughton.org/home/bulletins/town-hall
[2] "Community Facts". United States Census Bureau. American Fact Finder. Accessed on February 1, 2019. https://factfinder.census.gov/faces/nav/jsf/pages/community_facts.xhtml

The Challenge

As cyber threats are ever expanding and evolving, communities must be vigilant in efforts to monitor and prevent incoming threats from compromising systems or accessing sensitive data. To understand the current IT security posture, the Town needed to determine the effectiveness of their existing security controls and determine which areas are most vulnerable.

The Process and Solution

The Town received a Community Compact grant to retain the services of cybersecurity experts to identify technology-based, human, and physical vulnerabilities associated with IT infrastructure, ensuring the confidentiality, integrity, and availability of its IT and electronic data assets. After a thorough assessment, the Town was provided with a prioritized list of practical and detailed steps to eliminate and mitigate risk factors.

The Result

After reviewing how technology is utilized by the Town, HUB Tech focused on assessing commonly exploited threat vectors to determine the effectiveness of controls in place and to gain an understanding of current vulnerabilities related to those controls.

The following threat vectors were assessed:

- Vulnerabilities in publicly accessible systems and susceptibility to attack from the Internet
- Vulnerabilities among internally accessible systems and susceptibility to attack from within the Town's local area network
- Configuration profiles of servers, workstations, and network devices
- Vulnerabilities for wireless network security
- Physical security of core IT infrastructure and access to non-public areas

The deliverable documentation provided valuable insights and actionable steps to reduce existing and potential risk to IT assets the Town relies on to serve the community. Based on the assessment, the Town was provided with a confidential risk summary and, detailed finding documents. Additionally, recommendations based on findings and industry best practices, were provided to support the Town's ongoing efforts to improve cybersecurity posture. Based on the final assessment and recommendations, Stoughton now has a better understanding of how to address cybersecurity risks.