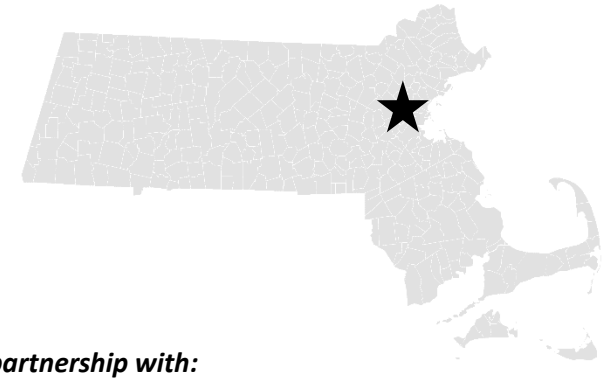
CYBER SECURITY BEST PRACTICE | OCTOBER 2017

Town of
ARLINGTON

Report prepared by: Amelia Percentie, Michael Pineau, and Michael Hamel

EXECUTIVE SUMMARY

The Town of Arlington, Massachusetts adopted the Cyber Security best practice as part of a Community Compact agreement signed with the Baker-Polito Administration in September of 2016. Leveraging Community Compact funding, the Town retained the services of Total Technology Solutions to assess their cyber security via a comprehensive network security audit. In the summer of 2017, Total Technology Solutions completed their assessment and delivered a report to Town leadership detailing their findings and recommendations.



In partnership with:

COMMUNITY PROFILE

The Town of Arlington is located in Middlesex County, just six miles northwest of Boston. Because of its proximity to Boston, Arlington residents are able to enjoy its diverse neighborhoods, active civic life, and good public transportation options. Arlington is more affordable than many of its neighbors and thereby attracts residents who value its geographic location and quality-of-life.

Population is 42,844 residents*
Annual Budget is $37M (FY 2017)
Median Household Income is $93,787*

**US Census Bureau*

Photo Credit: Flickr– Brad Greenlee at Spy Pond in Arlington, Massachusetts

THE CHALLENGE

Arlington has seen an explosive growth of wireless and tablet use and has serious concerns around vulnerabilities to the Town and School IT infrastructure. Arlington experienced a cyber-attack in the past but was able to recover using their backup system. The Town is invested in improving their cyber security standards and requested assistance to complete an assessment of their IT and network environment.

THE SOLUTION

The Community Compact Cabinet provided a grant to Arlington to support their adoption of the Cyber Security best practice. Arlington used this resource to receive technical assistance from Total Technology Solutions to assess the security of their network and make recommendations the Town may want to consider implementing.

THE RESULTS

The Town's network was analyzed over a period of eight days in June of 2017. Both external (public facing) and internal network resources were covered by the assessment. The overall goal of the analysis was to identify any weaknesses in the configuration of the network that could potentially result in a breach of privacy and security.

These findings were placed into a confidential report, which includes a "roadmap" for the Town to follow, with remediation recommendations over the next six months and to the next twelve months. This makes it easy for the Town to understand how to prioritize adjustments to the network. The report also provides additional information about best practices for network configuration which the Town may consider adopting to strengthen their security posture. For example, the report contains this tip about firewalls:

> "*Almost all network based Firewalls have the ability to dynamically protect internal networks from attacks. Services that are common on these Firewalls are Intrusion Protection, Gateway Antivirus, Content Filtering and Application Filtering. Ransomware passes through a gateway Firewall first, so having your firewall identify and/or alert you to this threat is vital to the protection of the internal network.*"

Since this report was delivered to the Town, immediate remediation of the most critical issues has already occurred. Moving forward, this document will help the Town develop long term plans for keeping all network resources secure.

"This project and the Community Compact program have allowed Arlington to immediately and effectively address an issue of significant importance. By maintaining and enhancing our Cyber Security, we are better able to provide consistent public service to both internal and external stakeholders."

Adam Chapdelaine, Arlington Town Manager

Photo Credit: Flickr – C. Hanchey at Robbins Memorial Town Hall in Arlington, Massachusetts