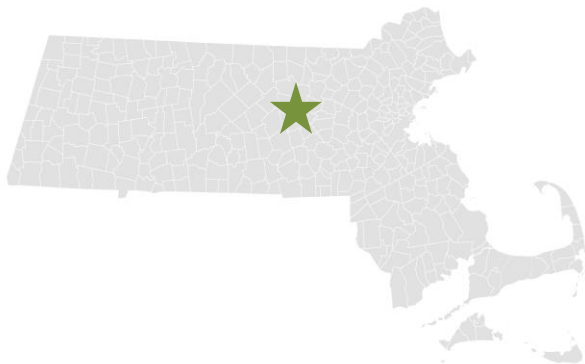# TOWN OF PAXTON

CYBER SECURITY BEST PRACTICE | MAY 2016

EXECUTIVE SUMMARY

The town of Paxton, Massachusetts has recently adopted the Cyber Security best practice as part of a Community Compact agreement signed with the Baker-Polito Administration in October of 2015. The town retained the services of Compass IT Compliance of North Providence, Rhode Island – a technology audit, compliance, and security firm – to perform testing of the town's information technology infrastructure, specifically focusing on information technology security. In March of 2016, Compass completed their audit and made recommendations to Paxton regarding areas that Paxton could improve upon and offered concrete steps it could take to improve security across the entire town's information technology network.

In partnership with:

COMMUNITY PROFILE

The town of Paxton is located in the central part of Massachusetts in Worcester County. The town is home to Anna Maria College and Moore State Park, a 730 acre state park listed on the National Register of Historic Places. Water and electrical services are provided by the town's own municipal departments.

Population is 4,806 residents*
Annual Budget is $12.4M (FY 2016)
Median Household Income is $72,000*

As of 2010 census

Photo Credit: Flickr - Curran Kelleher in Paxton, Massachusetts

THE CHALLENGE

As more and more work is done online, local governments are seeking to interact with citizens in the same digital space. Paxton is no different, but in order for this interaction to be safe and secure for citizens and the town's employees, security must be a leading concern.

Paxton is a small town with limited financial means, so technology in general must be implemented frugally and wisely. The grant provided by the Community Compact allowed Paxton to undertake this important security audit, so the important technology investments are secure.

THE SOLUTION

Compass IT Compliance, in partnership with town leadership in Paxton, used several pieces of security software to analyze Paxton's network and attached devices for any vulnerabilities or other important issues that the town should be aware of. Compass prepared a confidential report for the town detailing their findings.

THE RESULTS

The confidential report from Compass IT Compliance detailed findings in three categories: **zero day vulnerabilities**, for which there are no countermeasures available to mitigate exposure; **confirmed vulnerabilities**, for which prompt remediation is recommended; and **potential vulnerabilities**, for which review is required before categorizing as a confirmed vulnerability. Paxton is evaluating the report currently and is taking immediate steps to implement the recommendations of Compass.

CYBER SECURITY RISKS
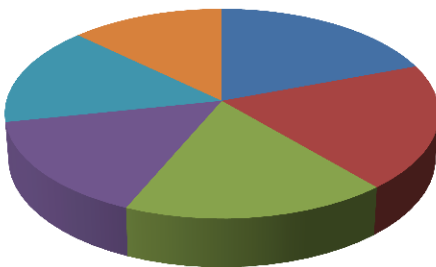
- 24% - Unauthorized Access
- 24% - Infected by Malware
- 22% - Denial of Service
- 19% - Identity Theft
- 19% - Data Stolen
- 16% - No Incidents

Types of significant detected cyber security incidents in municipal networks

73%
of businesses <u>do not</u> perform regular security audits

60%
of businesses have no technology use policies

Source: PwC US State of Cyber Crime - pwc.com/us/en/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf

"The results [of the audit] will certainly enable us to make sound decisions regarding our future IT needs."

- **Carol Riches, Town Administrator**

Photo Credit: Flickr – Pete Banach in Paxton, Massachusetts