Executive Summary (Public)

for

Cybersecurity Vulnerability Assessment and

Security Posture Review

March 11, 2020

Prepared for:
Town of Dudley, Massachusetts

Prepared by:
Dimitrios Hilton, CISSP, Cybersecurity Consultant
Dr. Patrick Johnson, CISSP, Cybersecurity Practice Manager

trueNORTH consulting group

Table of Contents

Executive Summary

Overview

True North Consulting Group was contracted by the Town of Dudley in January of 2020 to perform a Cybersecurity Vulnerability Assessment and Security Posture Review for the Town of Dudley. The approach to the engagement involved a 3-day physical site visit to review the Town facilities and perform data collection regarding current operations, technical systems, and existing security practices inclusive of Town Hall, Fire, Police, Water Departments, and Library operations. The second phase of the engagement involved remote security assessments and audits guided by the National Institute of Standards & Technology (NIST) 800-53r4 and Federal Information systems and Organizations (FISO) for security and privacy controls. The result of both phases met all requirements of the originating request-for-proposal (RFP) and included detailed reports of findings and actionable recommendations as final deliverables to the Town Administrator. The project was completed successfully.

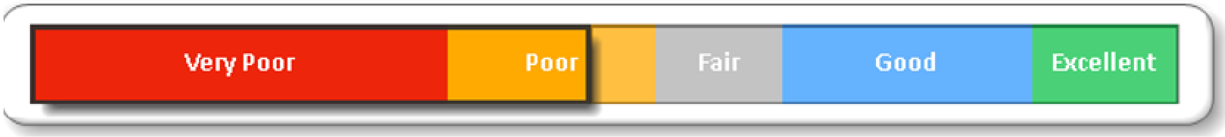
This Project Engagement Period was started on February 11, 2020 and was completed on March 5, 2020.

This Project included but was not limited to the following:

- Site visit and security walk-around of the Town
- Meeting and interviews with selected Town staff
- Custom approach to assessing additional departmental networks
- Depth-in-defense checklist for each Town network
- Internal vulnerability network security scans
- External vulnerability network security scans
- External website application security scans
- Special security review of the Town’s primary website
- Review of critical IT infrastructure and systems
- High level regulatory scoping for PCI, CJIS and HIPAA standards
- Review of current IT policies and procedures
- Review of special security concerns revealed during site visits

Overall Security Posture

The Town of Dudley currently has an overall security posture rating of **VERY POOR/POOR.** This rating is an indicator of how prepared the Town of Dudley is regarding current cybersecurity practices, policies, and operations that would protect the Town from cyber incidents.



The rating is derived from the compiled information attained through the recent security assessment. This security posture rating is the conclusion of the Security Consultant performing the Project and is also based on his experiences completing full quantitative NIST-mapped checklists of similar-sized local government organizations. Several recommendations are provided. Applying the recommendations can improve the overall security posture of the Town.

Top Cybersecurity Risk Items:

The security assessment led to the discovery of several areas of high-risk.

[Redacted for Security Confidentiality]

Risk Ratings Defined

Each security control is assigned a risk rating. Each risk rating considers impact, likelihood, and Information Security Maturity (ISM). Other mitigating controls and relevant risk factors are noted within each rating as described below.

Very Poor	There is limited evidence that controls and safeguards, to include key risk indicator controls, have been designed and implemented to protect organizational assets. Critical vulnerabilities with the presence of applicable threats exist within the environment assessed. A compromise of vulnerabilities is possible and likely based on the current state. A compromise could cause a serious and negative impact to the organization to include substantial financial loss, lack of compliance with regulatory or contractual requirements, and impact to the company brand and reputation. The organization would likely have an impaired ability to operate if the risks were realized.
Poor	There are a limited number of controls and safeguards that have been implemented to protect organizational assets. Vulnerabilities, to include critical, still exist and are in the presence of applicable threats. A compromise of vulnerabilities is possible and would cause a serious impact to the organization to include financial loss, lack of compliance with regulatory or contractual requirements, and impact to the company brand and reputation.
Fair	The majority of the most critical controls and safeguards have been implemented to protect organizational assets. Vulnerabilities still exist and are in the presence of applicable threats. A compromise of these less critical vulnerabilities is possible and would likely be contained to a business unit or division within the organization. Exercised vulnerabilities could cause a negative impact including financial loss.
Good	Critical controls and safeguards have been implemented to protect organizational assets. Non-critical vulnerabilities still exist and are in the presence of applicable threats. A compromise of these less critical vulnerabilities is possible and would likely be contained to a project, business unit, or division. Exercised vulnerabilities would have limited impact, to include financial loss.
Excellent	All critical controls and safeguards have been implemented to protect organizational assets including additional compensating controls. There are no identified vulnerabilities in the presence of applicable threats at this time. Potential impact would be localized to the project level with minimal financial loss.

Summary of Recommendations

Administrative Controls

Administrative Controls form the framework for managing an effective security program and they are sometimes referred to as the “human” part of information security. Administrative Controls inform stakeholders on how organizational leadership expects day-to-day operations to be conducted and they provide guidance on what actions or activities workforce members are expected to perform. Common Administrative Controls include policies, security awareness training, guidelines, standards, and procedures.

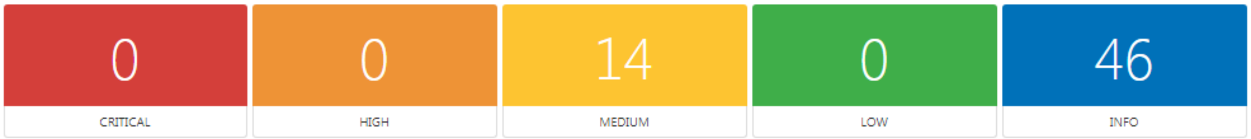
[Redacted for Security Confidentiality]

External Perimeter Technical Controls

External Perimeter Technical Controls are the controls that are technical in nature and used on the perimeter organization's technical domain (the gateways or firewalls). For the purposes of this assessment, switches, intrusion prevention systems, and wireless systems are included.

[Redacted for Security Confidentiality]

External Vulnerability Security Scan Results (SAMPLE):



0	0	14	0	46
CRITICAL	HIGH	MEDIUM	LOW	INFO

Internal Systems Technical Controls

Internal Technical Controls are the controls that are technical in nature and used within your organization's technical domain (inside the gateways or firewalls). Internal technical controls include items such servers, Active Directory authentication, anti-virus software, and mobile device management (MDM).

[Redacted for Security Confidentiality]

Cloud/Vendor Controls

Cloud/Vendor Controls are the controls and accountability necessary when outsourcing a critical application such as a website, email, cloud-based software and storage. These controls also include the accountability, regulatory certification (e.g. PCI, CJIS, PII, HIPAA, SCADA etc.), and vetting of Vendors. This practice is often referred to as Vendor Risk Management. Other external items such as domain names and DNS records are also inclusive to this approach.

[Redacted for Security Confidentiality]

Physical Controls

Physical Controls for information assets cannot be overlooked in an effective information security strategy. Physical Controls are the security controls that protect assets from physical theft, modification, and destruction. Physical Controls can often be touched and provide assurances that information will be safe. Common physical controls include doors, locks, camera surveillance, and alarm systems.

[Redacted for Security Confidentiality]

Conclusion

The Town has taken the best first step by implementing the comprehensive Information Security Assessment. The assessment serves as a guide and indicator for improvements regarding information security. The assessment can help catalyze the implementation of a formal Information Security Program to improve the security posture for the entire organization and all departments. However, actions taken by the organization after that initial report is issued will define the quality and maturity of the way in which it handles security as time moves forward.

Threat actors (hackers) will continue to attack government systems, both targeted and untargeted, while frequency and intensity of attacks will continue to grow with time. The implementation of an information security program will put measures in place to assist the Town moving forward. Systems change and new vulnerabilities will always develop. Implementing and maintaining information security is not a one-time event but an ongoing process. Keeping up with Information Technology is already a challenging task for all IT staff and technology service providers. Keeping up with Information Security is even more challenging and therefore, has evolved into its own profession.

Therefore, the single most important recommendation for the Town of Dudley is the establishment of an ongoing Information Security Program to address current risks and remediations identified in the report and those to come in the future. The implementation should be Town-wide with individual departments executing identified remediations from this report. This approach supports departmental autonomy with an overarching and singular strategy for handling information security for all operations.

The two most important aspects of implementing a formal Information Security Program are to engage a security professional on a regular basis and to have that security professional report directly to the highest levels of administration.