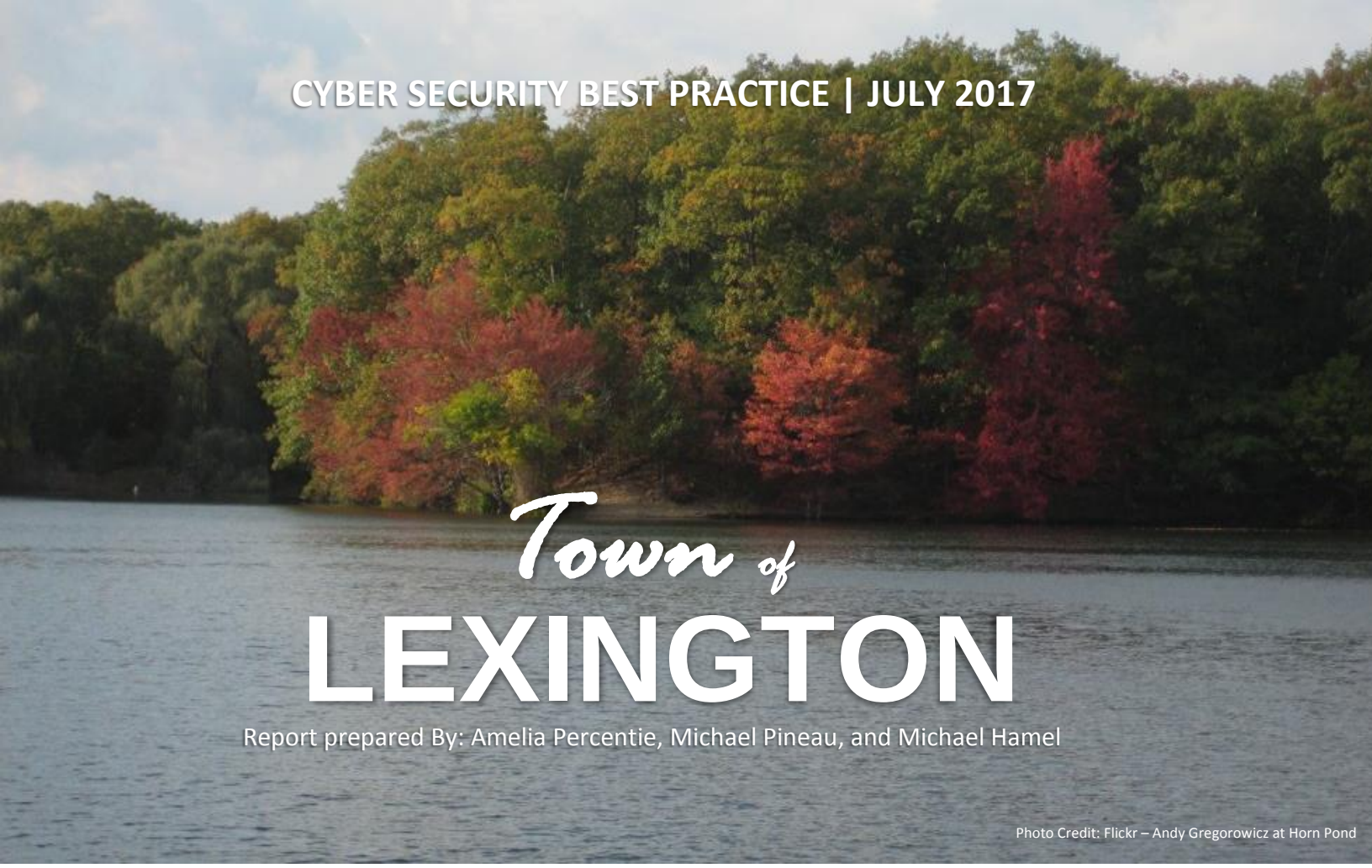


CYBER SECURITY BEST PRACTICE | JULY 2017

Town of LEXINGTON

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

Photo Credit: Flickr – Andy Gregorowicz at Horn Pond

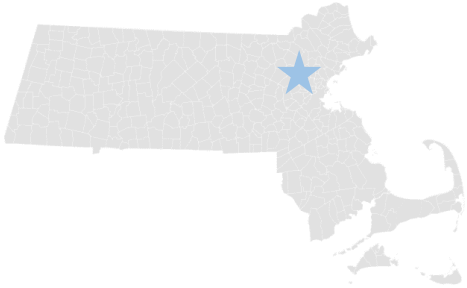
EXECUTIVE SUMMARY

The Town of Lexington adopted the Cyber Security best practice in March of 2016 as part of a Community Compact agreement signed with the Baker-Polito Administration. Lexington's IT Department leveraged a Community Compact grant to retain the services of Advise-X of Burlington, Massachusetts to perform a comprehensive cyber security assessment. The Town chose the Cyber Security best practice in part because of the importance of the shared infrastructure between the municipal and school departments. The Town is currently making many improvements to its technology and the assessment helped validate that the Town's cyber security defenses are keeping pace with these improvements.

Community Profile

The Town of Lexington is located in eastern Massachusetts in Middlesex County. Originally known as a farming community, Lexington has since become historically significant as the site of the first battle of the American Revolution. Today, Lexington is known as a residential community with convienent access to Boston and a nationally-recognized school system.

Population is 32,700 residents*
Annual Budget is $198.5M (FY 2017)
Median Household Income is $149,306*
**U.S. Census Bureau, 2011-2015*



In partnership between:

Office of Municipal and School Technology MassIT


Photo Credit: Flickr – Trevor Huxham

BACKGROUND

Municipal and school technology in Lexington operate on the same shared infrastructure. As the Town makes improvements to the network to keep pace with the growing demands of both municipal and school users, it's important to make sure the network remains secure given the variety of users and information being stored and exchanged on the network on a daily basis. With recent additions of public wifi and upgrades to public safety communications infrastructure, the Town felt it would be a good idea to leverage a Community Compact grant to assess the network and inform Town leadership of any adjustments needed to keep it secure moving forward.

PROJECT PROCESS

The Town used a Community Compact grant to secure the services of Advise-X to perform a comprehensive cyber security assessment of the municipal and school network. The assessment was based on how well Lexington's network was adhering to best practice standards adopted by several industry-leading organizations along with the Commonwealth of Massachusetts. From April to June 2017, testing was performed with the following administrative, technical, and physical controls in scope:

<u>Administrative Controls</u>

- Access Rights Administration
- Authentication
- Disaster Recovery Procedures
- Security Breach Procedures
- Service Provider Oversight
- Security Awareness and Training
- Change Management

Technical Controls Review

- Network Access
- Operating System Access
- DMZ and Firewall
- Email Application Access
- Encryption
- Intrusion Detection and Response
- Logging and Data Collection
- Malicious Code Prevention
- Password Technical Controls
- Remote Access
- Systems Development, Acquisition, and Maintenance
- Wireless LAN

Physical Controls

- Data Center Security

The following table was used to assess risk of each area assessed:

Threat Likelihood	Impact		
	Low	Moderate	High
High	Low	Moderate	High
Moderate	Low	Moderate	Moderate
Low	Low	Low	Low

"Threat likelihood" is a measure of how likely an adverse event is to happen. "Impact" is a measure of the consequences of an adverse event after it happens.

Additional testing was also performed to analyze whether software used by the Town had any known vulnerabilities and exploits that have not been patched. These can allow malicious users the ability to override controls set by the Town to perform a variety of unauthorized activities.

Examples of vulnerabilities include:

- Arbitrary Code Execution
- Buffer Overflow Execution
- Default password (remote command execution or other access)
- Flooding
- Denial of Service
- SSH v1 Weak Cipher Vulnerabilities
- Man-in-the-Middle Attacks
- Cross-Site Scripting
- SQL Injection

Penetration testing was also performed to make sure the public-facing parts of the Town's network are secure against malicious attacks. Town internet resources that could be reached from outside the network had any vulnerabilities classified as either "critical", "high", or "medium" in risk. The Town is actively working to remediate the vulnerabilities discovered.

One area of growing concern in many communities is social engineering, which is the use of deception to trick employees into giving up confidential information like a password. As part of the assessment, Lexington's employees were tested to see if they would volunteer their passwords if solicited by email or telephone. Fourteen employees were contacted but none would volunteer their passwords when requested. Additionally, phishing testing was performed using a fake version of the Town's email page. Sixteen random employees were sent an email containing a link to a web page requesting that they login using the page to "verify new features". Of the sixteen employees, zero logins were successfully phished.

All of Advise-X's findings were delivered in a comprehensive confidential report to the Town in 2017. The report contains a list of 14 issues that the Town should be aware of, ranked in order of risk using the scale referenced earlier: high, moderate, and low. This will allow the Town to prioritize remediation efforts effectively and address all of the concerns in the report.

CONCLUSION

As technology evolves, many municipalities struggle to keep up and some inevitably fall behind due to lack of resources. Lexington's technology environment includes both municipal and school resources, so potentially falling behind would put a large number of users – including students and their data – at risk, making this cyber security assessment and related testing incredibly important. By also testing its users with social engineering and email phishing campaigns, Lexington is making a commitment to stay current with the growing number of threats to municipal and school networks and keep its users secure.