Town of Lunenburg

Business Continuity Best Practice

Prepared By: The Office of Municipal & School Technology

EOTSS | Executive Office of Technology Services & Security

Image: Lunenburg Town Hall[1]

Introduction

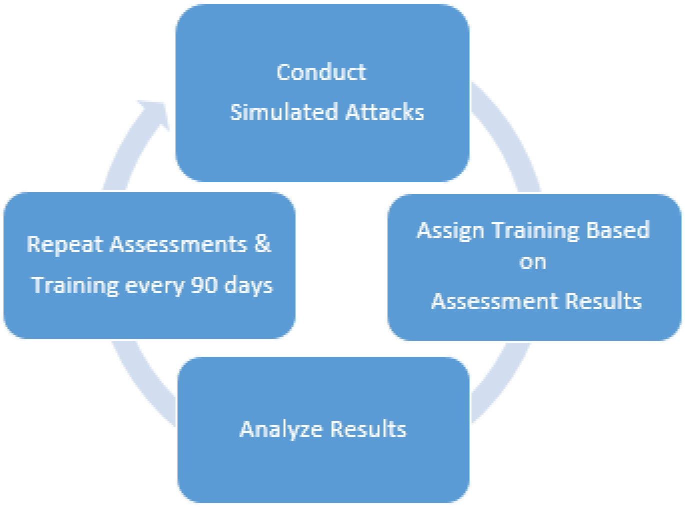
The Town of Lunenburg is located in Worcester Country, Massachusetts. The Town was originally incorporated in 1728 and now has a population of 10,086 and median household income of $89,706[2]. Lunenburg covers approximately 26.4 miles of land, and contains several recreational gems including Lake Shirley, Cowdrey Nature Center, and Hickory Hills Lake. Like many Massachusetts Towns, Lunenburg does their best to keep their infrastructure up-to-date, within budgetary constraints. This dynamic inspired Lunenburg's Town officials to sign a Community Compact agreement, where they would receive assistance to implement business continuity best practices. Through the Community Compact program, Lunenburg leveraged grant funding to perform an anti-phishing campaign. This summary report contains an overview of the work that was done with Wombat Security Technologies, Inc. to prepare the Town for potential cyber security threats.

[1] Doug Kerr. "Lunenburg, Massachusetts." *Flickr.com*. Accessed on November 9, 2018. https://bit.ly/2DcdKTt

[2] "Community Facts." United States Census Bureau. *American FactFinder*. Accessed on November 9, 2018. https://factfinder.census.gov/faces/nav/jsf/pages/community_facts.xhtml

Project Purpose & Process

Town officials chose the business continuity best practice track due to an observed need to assess security risks around the Town's data. Prior to the Community Compact engagement, Lunenburg had completed several audits that identified vulnerability to potential cyber security threats. Officials took serious measures to reduce the risk and contracted a third-party IT firm to assess their IT environment and provide suggestions to make sure the proper safeguards are in place. Lunenburg worked with Wombat to implement a twelve-month Security Awareness program for the Town's employees and end users. The project included the following components, which were repeated every quarter, to ensure completion within one year.


Conduct Simulated Attacks
Assign Training Based on Assessment Results
Analyze Results
Repeat Assessments & Training every 90 days

1. ASSESS KNOWLEDGE AND SUSCEPTIBILITY TO ATTACK

   It is important for organizations to measure security knowledge at the start of a security awareness and training program to establish the baseline level of knowledge. This baseline provided valuable insight into the level of training required and created a benchmark to measure the effectiveness of the ongoing training program as Wombat continued to reassess and train Lunenburg's employees. This initial assessment also provided data to prioritize the plan of attack on any vulnerabilities and weaknesses that were identified.

Simulated Attack Assessment

Wombat's Social Engineering assessment tools established a realistic baseline of Lunenburg's vulnerability against various attack vectors. ThreatSim, one of these social engineering assessment tools, used email to simulate an attack. The number of users that responded to these simulated attempts established a baseline of the Town's vulnerability to phishing attacks. In addition to determining vulnerability, employees who responded experienced a teachable moment where they were provided access to simple instruction to avoid future vulnerability. This motivated employees to take additional training, so they could learn tactics to protect themselves and the organization.

2. ASSIGN IN-DEPTH TRAINING

Wombat assigned training modules to users who responded to ThreatSim attacks. Users had 2 weeks to complete the types of assignments listed below.

- URL Training or Anti-Phishing Phil
- Email Security or Anti-Phishing Phyllis
- Other licensed modules

Wombat also provided assignments for every employee regardless if they responded to a simulated attack. These employees had 30 days in which to complete their Assignments.

3. ANALYZE RESULTS

As users complete the assigned training, Wombat collected data on areas of strength and weakness. They provided reports with status of assignments and each user's training report card. As the training completion deadline approached, Wombat reminded employees of the due date of their training assignment. They gauged employee proficiency and began to plan the next assessments and the next three training module assignments.

Repeat Steps

When the initial assessment and training was completed, Wombat re-assessed, in order to gauge the effectiveness of the training and the users' retention of the training material. Those employees who responded to the phishing attacks were re-assessed within 3 weeks of taking the training with a very similar, but not identical phishing simulation. If they responded again, they were re-assigned training.

Repeat Simulated Attacks

Wombat conducted ongoing simulated attack assessments once a quarter. Once training was completed, the Managed Services representative aided in the selection of attack templates that represent weak areas. Users who fell for simulated attacks were assigned appropriate training as indicated in Step 2 above.

Conclusion

The Town of Lunenburg completed their twelve-month engagement with Wombat Security Technologies, Inc. and received several reports containing the analysis from their anti-phishing test. The analysis results will not be published for security reasons. However, this report contains a direct description of the scope of work provided by Wombat and can serve as an overview of the processes that were executed. The results of the analysis helped to inform Lunenburg around their strengths and vulnerabilities. Today, they are better equipped to prevent potential cyber threats.

Appendix 1 – Project Plan

Initial Planning	
Develop strategy • Assess, Train, Assess • Define Timeline • Engage HR, and IT departments • Plan for possible announcements/notifications to employees	Customer/Wombat
Technical Readiness	
IT Issues • Whitelist IP Address for email server • Spam Filter Testing • Ticket Authentication Method	Customer
Employees	
Define who will be Assessed/Trained Provide the employee list with the following data elements *Email, First Name, Last Name, Department, Group, Location*	Customer
Segment employees based on Assessments and Training requirements and reporting needs	Customer
Format Contact List	Wombat
Upload Contact List	Wombat
Ongoing changes to Contact lists	Customer
Upload changes to Contact lists	Wombat

Assessment/Assignment Process Planning	
Outline how the Assessments & Assignments will be delivered: • ThreatSim Assessment • Training Modules • Follow-Up Campaigns • Training for users who did not fall for simulated attacks	Wombat
Assessment Planning	
Discuss and Determine: • Phishing Template • Teachable Moment • Translations (if applicable)	Customer/Wombat
Approve Preview	Customer
Send Phishing Emails	Wombat
Assignment Planning	
Outline Training Assignment Process • Training Auto-Enrollment	Wombat
Discuss and Edit Notification Templates for new assignments and reminders	Customer/Wombat
Customer Approval	Customer
Create Assignments	Wombat
Send Notifications	Wombat