RECEIVED
By Town Clerk's Office at 8:41 am, Nov 21, 2022

DEPT./BOARD: **Information Systems and Security Advisory Committee**
DATE: 10/**17/2022**
TIME: **7:00 PM**
PLACE: **Virtual via Webex**

Meeting Minutes

Present: Vice Chair David Hughes, Jose DeSousa, Joseph Bongiorno, Phil Pascale, David Miller, Rob Neufeld, Ben Axelrod
Absent: Chair Steve Morin, Bob Cunha, Glen Mills, Michael Wick

Posted Agenda:

1. Public Participation
2. Presentation by CyberForce|Q
3. Adjournment

Public Participation

Wayne Pierce, CyberForce|Q, Advisory Practice Leader

Presentation by CyberForce|Q

CyberForce|Q is a Michigan-based consulting firm with over 25 years of experience in providing cybersecurity assessment services for a wide range of organizations, including municipalities. The company has proposed to assist Burlington town departments in evaluating their readiness to deal with a cyberattack and in developing cybersecurity incident response plans, as described in the Statement of Work dated August 9, 2022, which accompanies these minutes.

There was an extended discussion of the services proposed by CyberForce|Q, and the Q|Frame software application that is used to develop a baseline gap assessment relative to the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Q|Frame creates longitudinal records with trackable cybersecurity events to measure compliance with the NIST control list. As NIST questions are answered, the tool will update credits for other relevant control sets. It will include quarterly sessions with each department, which are expert advisory-led. It's analogous to going to a gym with recognizable milestones, i.e. “where do you want to be a year from now?” Progress depends on users, but the intent is still to get the most traction in the timeframe desired. The tool data are all stored and can be exported at any time.

With a centralized digital notetaking app, different departments can see content others might need to know, which might be easier to maintain. Each department could also contribute pieces to the whole cybersecurity picture across the municipality. It's important to point out that this is a cloud structure but is also self-hosted, so no offsite data center, or no installs.

The work starts with a casual conversation: in other words, tribal knowledge acquisition. The goal is to create action items based on objective information – to create a policy within the tool. It can pull in metrics as proof: is you say you do something, the metrics the tool provides will prove it: with

insurance in a regulatory framework, metrics can prove tracking and effort even in adverse circumstances. These metrics can also quantify improvement of the cybersecurity framework over time.

The privacy of the data contained within the tool is covered by NDA, with exceptions for FOIA for cybersecurity activities.

As far as milestones are concerned, the intent is to teach clients to use the tool efficiently. Therefore, the short-term goal is to get all plans built within four months. Farther out, at the end of 12 months, we should have key topics with a baseline assessment, as well as items that helped during incidents, such as audits to find and manage data. We should also be able to identify things likely to be external issues, such as third-party risks, interagency dependencies, and interagency communication issues.

With these plans in place, cybersecurity becomes something you don't just update once a year. Organizations get in the better habit of injecting cybersecurity thinking at different points in the process: for example, how do you get vendors to commit, or how do you get maintenance to validate incident response? What is the strategic plan, or budget? At this stage of planning, organizations start developing muscle memory, so an incident response plan is created and maintained as part of 2-day operations. It will then be easier for people to build it out with documentation and data capture.

While there are departments that are very non-technical, the important thing for these people to know is where and when to get tech service and escalation – to map out crisis communications, so we know what to say, who says it, and to which audience. To establish this plan, we need to follow the path of power and the path of data.

CyberForce|Q Scope of Work

Motion entertained that Burlington move ahead with scope of work proposed by CyberForce|Q. Motion seconded and adopted, 6-0 in favor.

Adjournment

Meeting adjourned unanimously, 6-0, at 9:38 PM.