RECEIVED
By Town Clerk's Office at 3:13 pm, Sep 03, 2019

TOWN OF BURLINGTON

Meeting Posting

Email Posting to meetings@burlington.org or Bring to the Clerks Office. Thank you
Notice of Public Meeting – (As required by G.L. c. 30 A, c. §18-25)

DEPT./BOARD: Information System Advisory Committee

DATE: September 9, 2019

TIME: 8pm

PLACE: Grand View Farm, Meeting Center and online at:
https://attendee.gotowebinar.com/register/7226018306806556941

AGENDA

Submitted: September 2, 2019

1. Welcome
2. Review and Approval Meeting Notes
3. Action Item Review
4. Discussion
    a. Goals
    b. Methodology
    c. Format for 2020 Report
5. Any Other Business
6. Executive Session – Discussion of current network and systems security architecture

ADJOURN

RECEIVED
By Town Clerk's Office at 11:11 am, Sep 17, 2019

Information System Advisory Committee

Meeting Minutes

09/09/2019

Opening:

The Information System Advisory Committee was called to order at 8:00 PM on Monday, September 9th, 2019 at the Grandview Farms Meeting Center by Gerald Beuchelt.

Present:

Gerald Beuchelt, Chair
Glen Mills, Deputy Chair
David Hughes
David Miller
Larry Warfield
Steven Morin
Robert Chung
Joseph Bongiorno
Philip Pascale
Robert Nevfeld
Daniel McCormack
Kent Moffat
José DeSousa
Robert Cunha
Melinda Beuchelt, Secretary (nonvoting)

Approval of Agenda:

The agenda was unanimously approved as distributed.

Approval of Minutes:

The minutes of the previous meeting were unanimously approved as distributed.

Business from the Previous Meeting:

Other Towns' Framework Usage

No new information regarding other towns' security is available, discussion tabled.

MS ISAC Participation

MS ISAC is open to all local and state governments. In order to join, the town must fill out a short form.

Gartner: Burlington's IT Score

Gartner is busy at the moment, ISAC will hear back later this month.

New Business

Goals

The mission of the committee is to assist the Town of Burlington in cyber threat prevention, protection, response, and recovery and to improve Burlington's overall security posture.

Methodology

Gerald Beuchelt will send a list of high level deliverable goals. Committee members choose the task they would like to complete and Gerald will send updates to inform committee members who will work on what. There will be no discussions about content via email. In this way, the committee will generate content for the 2020 report, which will be discussed in detail at the meetings.

Format for 2020 Report

The 2020 Report will be a long-term, realistic cybersecurity strategy for the Town of Burlington.

Executive Session

At 8:33 PM the committee unanimously voted to go into an executive session to discuss the town's current network and systems security architecture, the security measures currently in place, and the basis for improving the town's security posture.

Additions to the Agenda

Glen Mills Resigns from Deputy Chair Position

The committee voted unanimously (with one abstention) to elect David Hughs as the new Deputy Chair.

Backups

The committee discussed the importance of having backups. See attached notes.

Adjournment:

The meeting was adjourned at 9:56 PM by Gerald Beuchelt. The next meeting will be on Tuesday, October 1st, 2019 at 7:00 PM at the Grandview Farms Meeting Center.

Appendix A - notes on backups as submitted by D Miller

Determine back-up scheduling - when to do incremental, when to do full.

Need to periodically test backup recovery to make sure things work as expected.

Backup devices should not be left connected to network.

Backup devices should be scanned with the best available anti-malware programs.

There should be backups with data only; no OS or Apps.

Identify off-site location(s) for storing backups.

Other

Consideration of retaining a Cyber Security professional consultant to assess the town's risks, needs, and necessary countermeasures. Also can evaluate this committee's recommendations.

Research of cities that were hit by ransome-ware attacks:

(Atlanta) Though it's tempting to say that it's worthwhile to take the easy savings by paying ransoms, experts are reluctant to ever recommend it. Instead, they emphasize that investing in software updates, backups, and network segmentation now can genuinely pay off for institutions later if they are targeted by ransomware.

(Baltimore and Florida) Having back-ups that work, or segmented networks -- built so parts of the network can be cordoned off from the wider network in the event of an attack-- can help, but even these tactics are limited in their effect, Orlando explained.

“On the enterprise side, some equipment is purpose-built to do certain things. Equipment -- especially in health care and manufacturing -- those are not just files that are stored somewhere else that you can replace, like you replace the data you backed up on your cell phone. Back-ups aren’t silver bullets, in terms of time loss and service loss,” Orlando said.

(Atlanta) Brantley credits the ransomware attack with accelerating the city’s migration of many of its critical applications to a hybrid cloud service, which he says has improved the city’s security. He also says the incident has encouraged him to develop the city’s relationships with the state and federal governments.

https://statescoop.com/atlanta-cio-says-city-has-moved-more-systems-to-cloud-since-ransomware-attack/

https://www.wbur.org/hereandnow/2019/08/21/ransomware-attacks-texas-towns

"...sytematic backup and recovery plan that's been tested."

(New Bedford) "After a ransomware attack slapped a hefty payout demand of $5.3 million on New Bedford, Mass., the city announced that it is instead opting to pick up the pieces and restore what it can from backups itself."

(Japanese-POW Website & Listserve) "For those not familiar with our working set-up, the Japanese-POW website and the Listserve email distribution function on servers maintained by west-point.org. On August 1st, those servers suffered a ransomware attack resulting in all files on the servers as well as the backups undergoing encryption. Typically, the owners of the site are required to pay a ransom in order to get a password (decryption key) in order to restore those files and their attendant functionality. Fortunately, the IT staff discovered this activity prior to full file encryption, shutdown the network and the servers. Thus they had full unencrypted backups from which they could restore the site without paying a ransom."