Technology and Communications Commission
August 6, 2024, 7:00 p.m.
Council Chamber, Town Hall
Agenda

- Call to Order
- Establish Quorum
- Pledge of Allegiance
- Approval of Minutes
  - July 2, 2024, Meeting Minutes
- Petitioners
- Old Business
  - Digital Town Hall Technology and Communications Commission Public Input – Update
- New Business
  - IT Accomplishments 2019-2024 Presentation
- Closed Session – Town of Leesburg Incident Response to Global Outage.
- **MOTION**: I move pursuant to § 2.2-3711(A)(19) of the Code of Virginia that the Leesburg Technology and Communications Commission convene in a closed meeting for the purpose of receiving a staff briefing regarding actions taken to respond to specific cybersecurity threats or vulnerabilities to the Town of Leesburg as a result of the recent global outage.
- **MOTION:** In accordance with Section § 2.2-3712 of the Code of Virginia, I move that the Leesburg Technology and Communication Commission certify to the best of each member's knowledge, only public business matters lawfully exempted from open meeting requirements under Virginia Freedom of Information Act and such public business matters for the purpose identified in the motion by which the closed meeting was convened were heard, discussed or considered in the meeting by the Commission Council. (ROLL CALL VOTE)
- Commissioner Comments
- Council Member Comments
- Information Technology Director Comments
- Adjourn

If you require any type of reasonable accommodation as a result of a physical, sensory or mental disability, to attend and/or participate in this meeting, please contact Jakub Jedrzejczak, Director of Information Technology, 703-771-2708. Three days' advance notice is requested.

Technology & Communications Commission
DRAFT MINUTES
July 2, 2024

Commission Members Present: John Binkley (Chair)
Richard Jackson, Vice Chair
Aaron Nadler
Katherine Johnson (Electronic Participation)
Chris Grandjean
Eric Whyne

Commission Member Absent: Brandon Garay

Council Liaison Present: Neil Steinberg

Staff Present: Jakub Jedrzejczak
Peace Hauffe

1. Call to Order 7:00PM
2. Establish Quorum
   Quorum present.
3. Electronic Participation, Motion Jackson to all Katherine Johnson to join us remotely, 2nd Nadler, Motion to allow Katherine Johnson to participate electronically passes 5-0
4. Pledge of Allegiance
5. Approval of Minutes – June 4, 2024
   Motion to approve June 4, 2024 minutes, Whyne, 2nd Jackson Passes 6-0.
6. Petitioners – None
7. Old Business
   Digital Town Hall Technology and Communications Commission Public Input – Update

Mr. Jedrzejczak - did check before the meeting with Town Manager about when the Commission can send this survey and unfortunately when he sent it to the directors for review the Town Manager requested that responses be returned at the end of the week so there is no further update at this time.

CISA Recommendations (Introduced by Chair Binkley

Mr. Binkley asked Mr. Nadler about the email regarding the CISA recommendations
Mr Nadler indicated he created two short statements concerning the Cyber Security Council.
Mr Jedrzejczak indicated Mr. Nadler did recommend that the Commission is in support with the creation of the Cyber Security Council and roles of the council and second that the Commission does support and recognize that the creation of a Chief Information Security Officer(CISO) as a position in the Town. The statement that the creation of a CISO is helpful for the Information Technology Director to recommend to the Town Manager and Council for the creation of the position.
Mr. Binkley requested that the email be sent to the commission for review and further comment.
Mr. Jedrzejczak indicated that he would forward the email to the Commission for review.

8. New Business

Overview of IT Training Program – Presentation

Mr. Jedrzejczak reminded the Commission that about two years ago one of the Technology and Communications Commission meetings was focused on technology training for the Town and that this session would be about what the department does today and where training is going to in the future.

Mr. Jedrzejczak emphasized the importance of IT and cybersecurity training, highlighting both ongoing efforts and future plans to enhance employee education. He described the current online awareness training, which covers cybersecurity and proper internet behavior, required annually for all employees. Acknowledging feedback that repeated training can become monotonous, he noted plans to diversify programs, particularly offering different content for new and existing employees. Specialized training for IT staff on systems like GIS and police systems is also in place.

Mr. Jedrzejczak underscored the value of hands-on training, such as tabletop exercises for ransomware scenarios, and the use of new tools like KnowBe4, which provides short videos and educational games on cybersecurity topics. This system is designed to offer engaging, frequent training to maintain high security awareness. He also discussed plans for a consolidated training calendar, ensuring consistent and accessible sessions for all employees. These will include monthly training on tasks like filling out timesheets and using Microsoft Office tools.

In-person training remains a priority, with a new training room equipped with modern facilities to support these efforts.

Mr. Jedrzejczak expressed pride in the high attendance and positive feedback for these sessions, emphasizing their role in building a robust security culture. He highlighted the support from leadership and the collaborative spirit within the organization, which have been crucial in implementing these training initiatives.

Mr. Jedrzejczak stressed overall that continuous education and practical training are essential for maintaining a secure and knowledgeable workforce, reflecting his belief in the enduring value of comprehensive IT training programs.

Mr. Steinberg asked about receiving a quarantine list of emails and what is the expectations. How do we know that they are legitimate business and how can they be marked?

Mr. Jedrzejczak indicates there is a way to mark the email. Microsoft Office 365 identify's it as an in between email. In this case it could be called legitimate spam. After you receive the email you can right click and make spam. Soon everyone will get a phishing button where you can report it to Information Technology.

Mr. Steinberg since everyone is using Microsoft and they can be hacked, is this a lesson learned for the Town.

Mr. Jedrzejczak highlighted the increasing severity of data breaches, noting that 140 million people's data has been stolen, with financial losses reaching over $10 trillion this year, compared to $3 trillion in previous years. He emphasized the importance of using

robust, standardized security measures from large organizations like Microsoft, which continuously implement new layers of protection.

Mr. Jedrzejczak expressed relief that the town's systems benefit from the same protections as the federal government, citing Microsoft's Office 365 and Department of Defense-specific solutions. He discussed the value of following Azure's evolving security options and acknowledged the ongoing battle against cybersecurity threats, despite progress made by national efforts. He stressed that while current measures are effective, there will always be a need for enhanced security in the future. He pointed out that many localities in Virginia face similar cybersecurity challenges, though these issues are often kept confidential to prevent further crimes.

Mr. Jedrzejczak sought suggestions for improving training from the Commission, emphasizing the critical role of ongoing education in cybersecurity efforts.

Mr. Binkley endorsed the just-in-time training approach, appreciating its modular format. He recommended maintaining thorough records of who completed the training to ensure accountability.

Mr. Binkley emphasized the importance of having a system where personnel can sign off on completed training, making it easier to provide proof during audits or governance reviews. He suggested that, if not already established, a policy should be implemented to ensure everyone in the town receives the necessary training.

Mr. Jedrzejczak explained the rollout of training videos starting in August, which will include a mechanism to track who watches them and ensure engagement through follow-up questions. He emphasized the importance of targeted training, especially for departments like finance, due to the high volume of fraudulent financial requests they encounter. He recounted instances of nearly undetectable fake invoices and emphasized the need for rigorous verification systems.

Mr. Jedrzejczak also highlighted the need for role-based training, particularly for new employees unfamiliar with cybersecurity basics like multi-factor authentication and password management. He underscored the urgency of improving cybersecurity awareness to protect against sophisticated phishing attempts, which are increasingly common and convincing.

Mr. Binkley encourages the department to test phishing emails on a regular basis.

Mr. Jedrzejczak discussed leveraging the system's capability to monitor who completes cybersecurity training, despite concerns about fatigue. He highlighted alarming stories from conferences about paralyzed governments and non-functioning emergency services due to cyber incidents. Following a recommendation from the Cybersecurity and Infrastructure Security Agency (CISA), he initiated the creation of a Server Security Council and established preemptive communication between the town attorney and insurance agency. This proactive approach aims to ensure readiness and coordination before a crisis occurs.

Mr. Jedrzejczak praised the collaborative efforts and ongoing preparations, expressing confidence that these measures enhance their preparedness, even though absolute security cannot be guaranteed.

Ms. Johnson emphasized the benefits of frequent, realistic phishing email tests conducted by her company. She shared that she receives these false phishing emails daily, which she

must report, helping train her brain to recognize and react appropriately to potential threats. Despite her nearly 20 years of experience in the field, she acknowledged the risk of complacency and noted that such regular testing keeps employees vigilant and engaged in cybersecurity practices.

9. Commissioner Comments.
   Mr. Nadler (Inaudible)
10. **Mr. Jackson** highlighted the critical importance of cybersecurity, mentioning that his son-in-law is involved with CISA, the federal government's premier anti-hacking agency. He shared that even CISA recently acknowledged a breach in its systems earlier this year. This incident underscores that even top watchdog agencies are vulnerable, emphasizing the necessity for cybersecurity to be a top priority for anyone involved in technology.
    Mr. Jedrzejczak emphasized the importance of not being the weakest link in cybersecurity. He expressed his determination to ensure that his organization is not the first to be breached in the region, comparing cybersecurity incidents to minor car accidents that serve as learning experiences. He acknowledged the struggles even watchdog agencies face but highlighted the progress made through community collaboration. He stressed that the foundation of success in cybersecurity lies in having key contacts, such as the FBI, CISA, and insurance agencies, to call in an emergency, ensuring he is not alone in managing potential crises.
    Mr. Binkley thanked Mr. Jackson for filling in as Chair while he was out and is happy to be back. Also wish all a happy fourth of July
11. Council Rep Comments - none
12. IT Director Comments
    Mr. Jedrzejczak Thank you to the Commission and thank you to Mr Steinberg for the holiday
13. Adjourn 7:43 PM Motion Jackson, 2nd Nadler Motion Passes 6-0.

Next Meeting, August 6, 2024, 7:00 pm.