Ferguson Township has engaged a third party to serve as a Managed Service Provider (MSP) to remotely service the Information Technology (IT) environment as well as provide on-site service on a biweekly basis. In recognizing the cybersecurity challenges and increasingly growing number of cyber attacks on local governments, Ferguson Township implemented PII Protect as a mandated program in 2019. Additionally, the Township rolled out Multi Factor Authentication (MFA) for all employees. Still, employees and Authorities, Boards, and Commissions (ABC) members were falling victim to phishing attacks through text messaging and emails.

Township Manager Martin engaged a reputable and experienced firm with substantial expertise in cybersecurity to assess the Township's cybersecurity posture at a specific point in time. Hammer Tech, a division of Weidenhammer, performed a Strategic Technology and Vulnerability Assessment to generate a report on the IT vulnerabilities as well as recommendations for remediation. The Strategic Technology and Vulnerability Assessment uncovered many outdated systems exposing a broad range of vulnerabilities and presented significant risk to the Township's IT environment. The assessment and final report provided insight on how the Township should strategize for identifying achievable business and IT goals. Given that technology is fluid, the development of business and technology goals helped identify and align solutions that would yield the biggest impact on productivity, return on investment, and be cost effective based on the holistic needs of the Township.

Business goals were established and consisted of the following:

1. Goal 1 was to enhance the IT service delivery model – to achieve this goal, the Township allocated funds to support a full-time IT Administrator position. This position was filled in November of 2023 and will assist with achieving the established business and IT goals as well as focus on mitigation efforts and critical incident response plans.
2. Goal 2 determined the need to improve IT infrastructure stability – to achieve this goal, the Township upgraded employee email accounts from the outdated, but less expensive, Microsoft licenses to Microsoft 365. Additionally, the Township implemented operating system upgrades to the servers and established future action steps which included the replacement of switches for servers and replacement of outdated servers.
3. Goal 3 emphasized the opportunity to modernize meeting spaces – to achieve this goal, the Township considered solutions after reflecting on complaints on the audio and visual systems and issues with virtual intruders that often disrupted public meetings. The Township invested in Cisco infrastructure for the audio and visual improvement project. The audio and visual equipment upgrades and improvements were completed January 19, 2024.
4. Goal 4 was established to resolve the outages of the regional police records management system (RMS) – to achieve this goal, the Township joined the regional police departments to secure a grant for a consultant to assist with the selection of a secure and functional shared RMS system for the police departments.

5. Goal 5 was identified as the highest vulnerability for the Township and remediation would require the Township to address the instability of the phone system – to achieve this goal, the Township had to first understand the complexities of a vulnerable phone system and how that vulnerability was an opportunity for a savvy cybercriminal to hack the Township's IT system through an outdated phone system that was no longer being patched. It was critical to understand the vulnerabilities and associated risks to justify the expenses associated with upgrading to a highly secure phone system such as Cisco Webex Calling.

   Overall, it was apparent the Township needed to improve its stance on IT security. Goals were established and consisted of the following:

1. To achieve this goal, a thorough review of preventative and maintenance programs had to be reviewed to understand the Township's risk, tolerance to risks, and additional investments that would be suitable and cost effective for the Township. To date, the Township has deployed a modern eXtended Detection and Response (XDR) platform to protect the most vulnerable and potentially damaging assets, the endpoints.
2. Additionally, the Township replaced an obsolete on-premise IP phone system which could not be patched with a modern, highly secure cloud-based system from a reputable vendor with automatic updates to keep the phone system and network from being the cause of a cybersecurity breach.
3. The Township also upgraded employees and Authorities, Boards, and Commissions members to Microsoft 365 licenses which enables the Township to leverage conditional access policies to improve security while also minimizing the inconveniences often associated with enhanced security policies. Previously, some employees had been provided Microsoft Exchange Online licenses which do not support conditional access.
4. In 2023, on a biweekly basis, the Township manager and assistant manager dedicated time to work with the MSP and the party that performed the Strategic Technology and Vulnerability Assessment to review status updates on corrective action taken as part of the remediation plan.

   To conclude, achieving and maintaining security is a journey, not a destination. The Township plans to develop an ongoing vulnerability management program to ensure that new vulnerabilities are identified and remediated as soon as possible. It has become apparent, however, that there are challenges with reallocating resources for a secure and reliable IT environment. Specifically, a common challenge is that personnel are too comfortable operating with a status-quo mindset, and long-tenured staff sometimes resist change that forces employees and stakeholders into more technology environments. It is critical that more education and training is facilitated for a shared understanding of the associated risks of not investing in cybersecurity given that today technology advances operations with increased efficient and effective governance. Generally, it is observed that employees and stakeholders of an agency are also too comfortable with a level of risk associated with not investing in IT security due to the misguided assumption that it is unlikely a cyberattack will happen to their agency.