The Chairman's Corner

by

Matt B. Murell
Matt.Murell@ColumbiacountyNY.com

CYBERSECURITY

4-25-23

Last September, the Suffolk County government was hit with a widespread ransomware attack, reminding everyone yet again that no one is fully inoculated against a cyberattack that could strike any organization at any time. We've all heard similar horror stories.

Here in Columbia County, cybersecurity is an ever-present goal of the Managed Information Systems department.

"Things get trickier and more complex every day," said county Chief Technology Officer Christopher Sweet, who took over as CTO in December 2021. "Cybersecurity occupies quite a bit of the day for the MIS department. And we're improving daily."

The use of multi-factor authentication, workforce training, the use of more complex passwords, and making certain the county workforce is aware of the pitfalls of internet usage are some of the tools deployed in the cybersecurity battle. The MIS department also makes use of resources available from the Multi-State Information Sharing and Analysis Center, which involves input from the FBI, CIA, state agencies, and the like, and the Crowdstrike Endpoint Detection and Response (EDR) system.

As part of its mission, states MS-ISAC, "We offer members incident response and remediation support through our team of security experts and develop tactical, strategic, and operational intelligence, and advisories that offer actionable information for improving cyber maturity."

Crowdstrike "monitors our workstations and alert of us any issues. They can also lock down that workstation if we're not here. That's a real good resource for us to have," said CTO Sweet.

In 2021, said county Director of Emergency Management Services David Harrison, the New York State Division of Homeland Security and Emergency Services (DHSES) came to the county, which it does every three to five years, to conduct a county emergency preparedness assessment.

In addition to a focus on preparedness for a natural disaster, DHSES notes that the number one hazard that the county – and counties across the state -- faces is a cyber-attack. Subsequently, Emergency Management was able to support the county efforts on that front with a $28,000 grant.

Following the DHSES visit, county MIS also fleshed out a continuity of operations plan, which "will allow a county department to continue providing essential services in the event that certain things happen," said Director Harrison. "Should the county informational network go down, how will services be provided? What happens if a building is destroyed?"

"County administration takes this very seriously," he added. "Upcoming this fall we've planned our first-ever cybersecurity tabletop exercise with the DHSES cybersecurity response unit. They'll do an assessment on

where we should increase our efforts. It allows us to test our plans and our information, and what direction we might need to head. It's something we plan to have every few years going forward."

"Things are always evolving," CTO Sweet says. "Policies are always being updated. It's all about how to keep your operation running."