Cyber Incident Summary

The Incident

- On October 28, 2020 Chatham County MIS staff identified a ransomware attack (DoppelPaymer) against our County network
- Chatham MIS staff quickly isolated the affected systems by stopping communication across our network and externally.
- Staff immediately enlisted assistance from state and local agencies with experience with this type of incident.
- Forensic analysis revealed that:
  - Ransomware entered our network through a Phishing email with a malicious attachment.
  - The threat actor acquired data from a limited number of county systems although the data that was acquired could not be specifically determined.

The Impact

- As a result of the incident, we lost the use of computers, internet access, office phones and voicemail.
- We were able to acquire loaner laptops from other counties, towns, and Emergency Management.
- Emergency Management was able to provide temporary internet access points and phones.
- Staff set up temporary email addresses for internal communication and access to the public.

Recovery Efforts

- Chatham Emergency Management helped coordinate daily briefings with stakeholders during the 1st two weeks of the incident.
- MIS staff and agency partners proceeded with full rebuild of our network infrastructure.
- We worked with our existing software vendors to restore our business systems.
- We had to wipe and reimage our servers and over 550 individual staff computers.

Current Status

- The process of restoring business systems, phones, network connection, and getting County computers back to staff is nearly complete
- Full system recovery efforts are estimated to continue through early 2021.
- We have been engaged with staff from the NC Department of Health & Human Services (DHHS) and the NC Attorney General's Office (AG) to ensure we meet the notification/reporting requirements as it relates to disclosures of a breach of protected health information (PHI) and/or personally identifiable information (PII) data.

Breach Notification

- We continue to engage in with our breach counsel, DHHS, and the AG to ensure we respond in the most appropriate manner possible as it relates to the data accessed from our network during the ransomware incident.
- We are going through the files on the server that were impacted to collect the names and addresses of individuals whose PII or PHI may be at risk of exposure.
- Those individuals will be notified of the situation.
- A call center will be available to those individuals to answer any of their questions about this incident.

Improvements

- Along with the extensive mitigation efforts taken by the County during the cyber incident, Chatham MIS also evaluated the existing security protocols in an effort to further build upon the security of our network.
- We are evaluating and implementing additional security measures and reinforcing employee training.
- The threat from outside individuals is constant and Chatham County aims to take all reasonable actions to secure their data and infrastructure.

Improvements

- During this time, we took the opportunity to improve/update some of our software:
  - Office 365 upgrade
  - .gov domain change
  - Changing from CityView to OpenGov software for permitting
  - Northwoods/Laserfiche upgrade at DSS