File #: 21-3692, **Version:** 1

Cyber Incident Report

Action Requested:
Receive the report on the cyber incident

Introduction and Background:
On October 28th. 2020 Chatham County MIS staff identified an ongoing ransomware attack against our county network that resulted in the encryption of much of our county network infrastructure and associated business systems. Chatham County MIS staff acted swiftly to mitigate further propagation by stopping communication across our network and to the outside world once the threat had been identified. MIS contacted the NC Local Government Information Systems Association (NCLGISA) strike team which helped facilitate assistance from various state and local agencies along with the North Carolina National Guard cyber response team. Enlisting the assistance of these valuable outside resources quickly helped our MIS staff understand how to respond to the attack and most effectively mitigate further damage to our network. Throughout the course of two weeks the NCLGISA strike team and National Guard assisted Chatham County MIS staff onsite with the initial steps towards strengthening and recovering our network and associated business systems.

Discussion and Analysis:
The process of restoring business systems, phones, network connection, and getting County computers back to staff is nearly complete but is estimated to continue through early 2021 as we work towards full system recovery. As you know, ransomware incidents are becoming more common. The County had the foresight to mitigate its exposure to such an incident through the procurement of cyber insurance. We are collaboratively working with our cyber insurer on this incident and anticipate that the bulk of the direct costs associated with this incident will be covered. We are thankful for everyone's dedication and efforts to minimize the impact of this incident.

NC Emergency Management provided in-depth forensic analysis of the incident in collaboration with our already existing security monitoring company, SecuLore. Both entities concluded that the threat actor, DoppelPaymer, was able to enter our network using a phishing email with a malicious attachment. Both analyses also concluded that the threat actor acquired data from a limited number of County systems, although the exact data that was acquired could not be determined with specificity. Chatham County staff has 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. We will continue to engage in these conversations 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.

How does this relate to the Comprehensive Plan:

Budgetary Impact: No budgetary Impact

Recommendation: Receive the report