On October 28, 2020 Chatham County MIS staff identified a ransomware attack against our County network that resulted in the encryption of much of our County network infrastructure and associated business systems. In response, Chatham County MIS staff acted swiftly to isolate affected systems by stopping communication across our network and externally. MIS also enlisted assistance from state and local agencies with experience handling ransomware incidents. Enlisting the assistance of these valuable resources helped our MIS staff quickly understand how to respond to the incident and most effectively mitigate any impact to our network. Throughout the course of approximately two weeks, the partner agencies assisted Chatham County MIS staff onsite with strengthening and recovering our network and associated business systems.

Daily briefings were also held with stakeholders during the initial two weeks following the County's discovery of the incident. Ultimately, Chatham County took advice from all resources and proceeded with full system recovery rather than paying the ransom demanded by the ransomware threat actors. Chatham County MIS staff rebuilt our network infrastructure by utilizing existing staff and agency partner resources. These outside resources did not result in additional expenses being incurred by the County and were instrumental in the process of getting us back on our feet as quickly as possible. Chatham County MIS staff also reached out to our existing software vendors to request support under existing contracts as applicable. In some cases, our software vendors were able to provide support under our existing support contracts, but in other instances we needed to contract professional services to restore our business systems to a state in which they were prior to the incident.

Full system recovery meant that we would need to completely wipe and reimage our servers and individual staff computers. Over the next three months, vendors worked to restore our servers and get our business systems operational. During this time, we also decided to move forward with an upgrade to MS Office 365 and change our email domain from chathamnc.org to the more secure chathamcountync.gov.

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.

One of our most important goals is to determine exactly what happened during this incident so that we can do everything possible to prevent it from occurring again in the future. To that end, 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. Currently, 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 and a call center will be available to those individuals to answer any of their questions about this incident.

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.