File #: 20-0157, **Version:** 1

Item:
Durham County Cybersecurity Malware Attack Recovery Update (15mins)

Date of BOCC Meeting: April 27, 2020

Request for Board Action:
On March 6th, 2020, Durham County Government experienced a ransomware attack. Ransomware is a form of malware (malicious software) that encrypts a victim's files. This malware attack was very similar to what hit the City of New Orleans in 2019 where their Mayor declared a State of Emergency due to the impact on the City there. Feedback from our external entities and partners have said, this was an extraordinarily complex cyber-attack on both the City and County of Durham.

The County enlisted resources from the private sector and received assistance from federal and state entities that specialize in complex cyber-attacks and restoration of those operations. This has been an all-hands on deck exercise working 24-hour shifts and weekends to restore IT services here in the County. Restoration of the public facing systems have been the highest priority.

As of today, staff is pleased to report Durham County has made significant progress since the March 6th date. We have now completed many of the IT prerequisites, like reimaging all 2000+ County laptops/desktops, to begin re-enabling public facing services. Further, nearly 300 servers, 800 data bases and over 2 million documents were scanned to ensure systems servers and data was clean. In addition, our communication vehicles are now back online, Email, Phones, Voicemail, and our employee portal, MyDCo. In addition, several critical business applications used by departments like Register of Deeds, Tax, Public Health, DSS, Budget, and Human Resources are back online.

We have made significant enhancements to our IT environment throughout the restoration process and plans are underway to address additional short-term and long-term investments needed to mitigate future attacks. While we cannot prevent such attacks from occurring, the IT security enhancements we are putting in place will help to mitigate and lessen our risk if such an attack happens again.

Staff will keep the Board and public aware of the progress as we work towards maintaining a secure technology infrastructure.

Alignment with Strategic Plan: Goal 5: Accountable, Efficient and Visionary Government.

Resource Persons: Greg Marrow, Chief Information Officer

County Manager's Recommendation: The County Manager recommends that the Board receive the update on the malware attack recovery process.

County Manager: _____