Mayor discusses impact of ransomware attack on New Bedford's computer system

In a press conference at City Hall, Mayor Jon Mitchell briefed the public regarding the impact of a cyberattack on the City's computer system this summer.

On Friday, July 5, 2019, the City of New Bedford's Management Information Systems (MIS) staff identified and disrupted a computer virus attack, known as ransomware, in the early morning hours before City employees began the work day. The MIS staff disconnected the City's computer servers and shut down systems to prevent the virus from gaining a larger foothold across the City's network.

The specific virus was a variant of the RYUK virus, a ransomware virus whose purpose is the financial extortion of a computer network's operator – in this case, the City of New Bedford. RYUK encrypts, or renders inaccessible, the data stored on computer servers and workstations. In order to potentially unlock the encrypted data, the operator must then make a payment to acquire a decryption key from the attacker to access its data. RYUK has been implicated in attacks on government, education, and private sector networks around the nation and the world. These attacks have escalated in their frequency, their technical sophistication, and the size of the ransom demands in exchange for the decryption key.

The attack did not disrupt the City's delivery of services to residents. The City's MIS staff is now addressing the internal impact on city government.

The City's MIS Department has now completely rebuilt the City's server network, restored most software applications,

and replaced all of the computer workstations that were found to be affected; 158 computer workstations, or 4 percent of the total of the City's computers, were found to be affected by the attack.

The encryption, or locking up of data, varied widely across City departments. Several key areas experienced little or no loss of data; other areas experienced significant encryption. The investigation determined that emergency dispatch (911) was completely unaffected, and all Fire Department, Police Department, and EMS units could communicate and deploy as usual. At no time did the attack disrupt public safety departments' ability to respond to calls for assistance. (Several workstations used by the Fire Department for administrative purposes were affected and were temporarily removed form service).

Major municipal services including the New Bedford Public Schools, water and wastewater treatment plants, and trash/recycling services, were unaffected. The City's financial management system was temporarily placed out of service but was quickly brought back online.

The City is taking several actions going forward. Systems will continue to be restored while keeping all essential services operating seamlessly; the City has continued to deliver those services since the attack. The City has also decided to provide public legal notice and put in place appropriate supports related to any personal data exposure, regardless of whether it is legally required to do so. Ransomware attackers typically seek to lock files and hold them for ransom for financial compensation, rather than steal data, and every indication suggests that is the case in New Bedford's attack. Although not all log files were accessible to the City's forensic team, most were – and all of the log files that could be examined showed no evidence of any transfer of personal data. Therefore, the City is acting out of an abundance of caution by providing public legal notice concerning personal

information.

The City will also continue to take measures to prevent any such attacks in the future. The City’s network security has been further enhanced, additional security practices and protocols have been put in place, and the City’s cybersecurity firm will continue to provide further recommendations to the City.

“We live in a world now that is so interconnected that simply pulling up the proverbial drawbridge is unrealistic,” Mayor Mitchell said in his remarks summarizing the ransomware attack. “We will rely on the advice of our experts to guide us, but we must remain constantly vigilant and willing to devote the resources necessary to protect our system from a much more debilitating attack than the one we just experienced. I am committed to making sure our City does just that.”