MEMORANDUM

TO: County Councilmembers

FROM: Howard S. Lazarus, Executive Director
Frank Bilotta, Chief Information Officer

DATE: December 28, 2020

SUBJECT: Security Incident Summary – Cyberattack on County Information Systems

---

PURPOSE: This memorandum provides a summary to support discussion with Council concerning the cyberattack on the County's information systems and the work in progress to protect the County's data and systems from future incidents.

SUMMARY OF EVENT: The initial attack occurred in the form of a *phishing*[1] e-mail to a County employee from an external *threat actor*[2] received on September 10, 2020. The e-mail contained *malware*[3] that was downloaded, and once in the system captured credentials and infiltrated the network. During the period between September 10th and November 21st, the threat actor was most likely stealing credentials, identifying sensitive data, and exfiltrating the information from the County's operating environment.

Sometime between September 10th and November 21st, the threat actor activated a *ransomware*[4] application. On November 21st, a member of the County's IT staff identified abnormalities in the network and promptly notified senior leadership and disconnected all servers and computers. The Executive Director immediately notified the County's elected officials and department directors. The Chief Information Officer notified the Department of Homeland Security and the County's insurance agent. The County's insurance agent provided contacts with a cyber forensics team and outside legal counsel with

---

[1]Phishing is the fraudulent attempt to obtain sensitive information or data, such as usernames, passwords and credit card details, by disguising oneself as a trustworthy entity in an electronic communication. Typically carried out by email spoofing, instant messaging, and text messaging, phishing often directs users to enter personal information at a fake website which matches the look and feel of the legitimate site.

[2] A threat actor or malicious actor is a person or entity responsible for an event or incident that impacts, or has the potential to impact, the safety or security of another entity. Most often, the term is used to describe individuals and groups that perform malicious acts against organizations of various types and sizes.

[3]Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network.

[4] Ransomware is a type of malware that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

expertise in the area of cybersecurity, and the Executive Director authorized the work as an emergency in consultation with County Council.

Working with these resources, the County's IT staff began claiming back the system environment and credentials. The team installed software to protect each computer and to stop the threat actor from communicating into or out from the environment. The focus at this point to contain the intrusion while evaluating the status of data back-ups.

The threat actor early on indicated that its intent was to hold the County's system for ransom, accompanied by a threat to release data, including potential personal information, unless the ransom was paid. Although the County was able to restore its capabilities from its back-up systems, the Executive Director recommended to Council that the ransom payment be made as the County's exposure was limited to the deductible amount ($25,000) on its insurance policy and that working with the threat actor would accelerate system restoration and prevent information from being published. Upon payment of the ransom, the threat actor provided the decryption tool necessary to unlock the County's systems, a list of the files that were exfiltrated, and a general description of how the cyberattack commenced.

ACTIONS SUBSEQUENT TO THE ATTACK: The County's focus since November 22nd has been to restore a secure environment that enabled County services to resume. Working with the Executive Director and County directors, the most impactful systems were prioritized and work-around solutions were developed. As of the date of this memorandum, all key systems have been restored and are available.

WORK PLAN GOING FORWARD: County IT staff is pursuing the following initiatives to provide a more secure environment going forward:

- Rebuild clean versions of the County's server infrastructure.
- Update old versions of operating systems and apply *security patches*[5].
- Remove old hardware and software solutions that are threat vectors.
- Remediate vulnerabilities that outside support agencies have identified.
- Assess whether or not personally identifiable information was compromised and take appropriate steps to comply with all required laws and requirements.

These actions will require continued use of outside resources, including extending the use of the cybersecurity firm, upgrading security software, and engaging third party project management to supplement existing staff. As these actions are taken, the County must also pursue the following measures and provide the resources to ensure the sustainability of its information systems:

- Establish and enforce rigorous and centralized system security and data quality standards for all County systems.
- Move data storage to more secure, off-site environments.
- Systematically upgrade security applications, scheduling system down-time as necessary.
- Continually evaluate the effectiveness of back-up systems.
- Create and integrate an information technology component into the Capital Improvement Program (CIP) to allow for cyclic and systematic upgrade and replacement of computer hardware and software.

[5]A security patch is an adjustment to software and systems that address vulnerabilities cybercriminals might use to gain unauthorized access to devices and data.

- Create a single County domain (to the greatest extent possible) and review access and operating protocols for externally-required systems.

cc: President Judge
Elected Officials
Chief Financial Officer
Chief Personnel Officer
Department Directors