Pottawatomie County, Kansas
Becky Ryan, PIO
785-457-3455
pottcountypio@gmail.com

Est. 1857
POTTAWATOMIE
— COUNTY · KANSAS —

October 1, 2021

POTTAWATOMIE COUNTY OFFICIALS RESOLVING CYBER ATTACK

Westmoreland, Kan. (*October 1, 2021*)-- County officials are making progress in restoring computer systems and machines after a ransomware attack encrypted several servers on September 17, 2021. The Sheriff's Office and emergency response systems were not impacted.

The County initially did not share many details about the attack because that is the right thing to do to protect the County from further attacks under these circumstances, and so as not to compromise the law enforcement investigation. At the same time, County representatives were negotiating with the hackers to reduce the ransom demand.

The resulting resolution was extraordinary, both in terms of the final settlement and the speed at which the County was able to resolve the attack. "The ransom was reduced by more than 90 percent from hackers' original demand, an almost unheard-of outcome, every saved dollar of which is taxpayer revenue the county keeps to serve our citizens," said County Administrator Chad Kinsley. According to cyber experts it can take several weeks to months to resolve a ransomware attack. This negotiation with this threat actor was resolved in just days.

"We are a small county with small resources," Kinsley said. "With the extraordinary demands that the COVID-19 pandemic has placed on local governments like ours, we wanted to make sure that the hackers understood that there was no way we could even come close to meeting their demand," he said. "We were focused on protecting taxpayers and doing everything we could to resolve the issue with as little as possible. We believe we succeeded at that."

The IT team, including expert advisors, has now installed additional sensors on all servers to detect and prevent further attacks and is completing its forensic analysis of how the hackers gained access.

Systems are routinely backed up daily and backup files were readily available to begin rebuilding functionality. The 150 County desktop and laptop computers must be individually imaged for forensics, wiped clean and then software is reloaded. The process can take up to eight hours per PC.

All County offices are open and serving the public. It may take a bit more time to fulfill certain customer requests until computers are fully restored. The only systems that are still down are for email; and driver's licenses, which is not managed by the County. We hope to have them working in the very near future.

###