Dallas approves more than $2 million in IT security as county investigates cyberattack

November 9 2023, by Everton Bailey Jr., The Dallas Morning News

Credit: Pixabay/CC0 Public Domain

The Dallas City Council has approved two agreements totaling nearly $2.7 million to shore up the city's IT security, while Dallas County

officials try to determine if sensitive information stolen by hackers last month has been leaked online.

Both municipal governments have been hit with cyberattacks this year. The latest City Council approval marks at least $9 million in multi-year agreements geared toward information technology security that Dallas city elected officials have signed off on since April.

Of the two deals approved by City Council on Wednesday, the largest is a four-year, almost $2.2 million agreement with technology service provider Netsync Network Solutions to help the city buy equipment for a network security management monitoring and response system. City officials told The Dallas Morning News after the council meeting that the deal is meant for the city to continue using an existing network monitoring tool already in place.

"The security operation team will utilize this technology to assist in detection and prevention of network security breach and destruction from malicious traffic," according to city documents describing the agenda item. "The system ensures the security team shall have adequate security alerts to allow faster response to identified anomalous traffic internally."

The other agreement is a three-year, more than $510,000 deal for new cloud-based security software the city doesn't currently have. That software is meant to "secure online communication, protect websites, and ensure the authenticity and integrity of digital transactions," city documents say.

Dallas has approved at least three other similar purchase agreement deals through Netsync related to IT security, city records show.

On April 12, the council approved the city spending almost $2.2 million

for a backup and recovery system. On April 26, the council greenlit more than $873,000 for threat detection for city servers, employee's computers and other devices. And more than $3.9 million was approved on June 28 for a threat and anomaly detection system.

It's been a little more than a month since a Dallas internal review of the spring cyberattack found hackers used stolen online credentials to get into the city's system and steal files.

Dallas officials say hackers got into the city's system in April, spent about a month going through the city's network, downloaded almost 1.2 terabytes of data, and tripped the city's alert system when a ransomware attack was launched May 3. It took months for Dallas IT workers to restore the city's system after the breach, which impacted city services and led to several servers being taken offline.

City officials reported in August that the addresses, social security numbers and medical information of more than 30,000 people were among sensitive information exposed during the data breach from ransomware group Royal in the spring. The city sent 27,000 letters to people impacted by the data breach informing them of the leak and offering them two years of free credit monitoring.

The City Council in August approved setting aside nearly $8.6 million to pay vendors for hardware, software, incident response and consulting services in response to the ransomware attack.

Dallas County officials revealed Oct. 30 that they detected a cyberattack 11 days earlier. They said Tuesday that an investigation remains ongoing into claims from ransomware group Play that members have made some stolen information available for anyone to download.

"We understand the concerns that such an incident may raise among our

residents, employees, and partners," the county said in a statement on Tuesday. "We want to assure everyone that we are taking this matter seriously. Our top priority is the security and privacy of all individuals associated with Dallas County."

Play says it has demanded a ransom from Dallas County, but as of Wednesday it doesn't appear there's any agreement in place to pay it.

A cybersecurity expert told The News on Tuesday that he found Dallas County arrest records that include dates of birth, arraignments, court orders for mental evaluations and DNA analyses related to court cases on the dark web.

"The attack was real," Murat Kantarcioglu, a computer science professor at the University of Texas at Dallas, said to The News. "I don't know how much they exfiltrated, but these are legitimate files."