Ransomware: Dallas says cyberattack targeted more people than previously disclosed

January 12 2024, by Everton Bailey Jr., The Dallas Morning News

Credit: Pixabay/CC0 Public Domain

Hackers who targeted the city of Dallas had access to the addresses, social security numbers and other personal information of nearly 300 more people than what had been previously disclosed to the public, city officials now say.

Catherine Cuellar, the city's spokesperson, told The Dallas Morning News on Wednesday that further internal investigations into the cyberattack pinpointed an additional 293 people, including residents and employees, whose information may have been accessed by hackers. She said the city has sent letters to notify them.

The disclosure adds to the tally of more than 30,000 people affected by the data breach and comes after the Dallas City Council met in closed session earlier Wednesday to discuss the cyberattack with the city attorney's office. The council's last listed executive session meeting on the topic was in late September.

It's not clear what was discussed during Wednesday's closed meeting, and the council members did not speak about it when they resumed the open meeting in the afternoon.

The City Council voted on Aug. 9 to set aside nearly $8.6 million to pay vendors for hardware, software, incident response and consulting services in response to the ransomware attack. The city has refused to disclose specifically how that money is being spent.

The city appealed a public records request from The News seeking a listing of where the money was going. The attorney general's office approved part of the records to be released, but when the city turned over the information in December, it only provided the contract amounts and censored the name of every vendor and descriptions

"All goods and services were procured between May 3, 2023, and July 31, 2023," the one-page document of ransomware expenditures said. The line items ranged from nearly $7,100 to $4 million.

Cuellar said the city's IT department does not plan to ask the City Council to approve any more spending to address the ransomware attack

beyond the $8.6 million council members had already approved.

The city's refusal to break down any information about the money it has spent is the latest example of how little information the city has disclosed to the public about the May attack, which took some city computers and services offline for weeks.

The city reported the data breach to the U.S. Department of Health and Human Services in August, three months after the city discovered the attack, saying personal information from 30,253 people in Dallas' self-insured group health plans was exposed during the breach.

That same month, the city sent about 27,000 letters, mainly to employees, former employees and their relatives explaining that names, addresses, Social Security numbers, medical information and other details were exposed and possibly downloaded.

They also offered them two years of free credit monitoring. Cuellar said 13% of the people notified had enrolled in credit monitoring as of Tuesday.

Hackers used stolen online credentials to get into the city of Dallas' system last April and steal files during a cyberattack, according to city officials.

The ransomware group Royal connected to a city server and had remote access to the system starting last April. Royal spent about a month going through the city's network, downloaded almost 1.2 terabytes of data through that server, and launched a ransomware attack in May, setting off city alert systems.

City officials told The News last year that the data stolen was equal to roughly 819,000 files stored by the city.

The report said all of the city's more than 40 departments were impacted by the hack. It also lists at least 17 systems that were down at some point during the ransomware attack, including city fax and print services, police surveillance cameras, public safety file sharing, the building permitting system, library management services, fire station alert systems, police and fire mobile data computers, court-ordered warrant management system, and the ePay system for residents to pay their water bills and bills from other departments.

It's not clear how much data was taken from city servers. Royal has threatened to release city-stored information, but Cuellar said the city has found no evidence of any leaked information as of Wednesday.

City officials have cited an ongoing criminal investigation into the hacking as reason to release few details of the incident. They also haven't said if any ransom has been paid to hackers related to the data breach.

An FBI Dallas spokeswoman declined to say if a criminal investigation was still ongoing.

2024 The Dallas Morning News. Distributed by Tribune Content Agency, LLC.