

Del Norte County vs. the cyberattacks

November 19, 2019



It's been a couple of years since Del Norte County's computer systems were targeted by cyberattacks. Luckily, the county's data was backed up on separate file servers and nothing was lost.

But that doesn't mean the threat doesn't remain.

District 5 County Supervisor Bob Berkowitz had heard of recent attacks elsewhere, so he asked Dan McCorkle, the county's information technology director, to update the board of supervisors Nov. 12 on the state of the county's cyber security.

McCorkle reported that ransomware attacks have hit at least 170 county, city or state governmental systems since 2013, and that 22 of those attacks occurred in the first half of 2019.

McCorkle said ransomware encrypts the data on computers or servers, then holds them ransom. "You can't unlock it or decrypt it unless you pay the ransomer money. Like through bitcoin.

"The fact is, there is no way to decrypt the data once it is encrypted. Some agencies have paid the money. The federal government has asked us not to pay the money, because they don't want to encourage this to happen.

“But it has become a multi-billion-dollar industry. The attacks keep happening because governments have the money,” McCorkle said.

He then ran through 2019’s ransomware attacks:

- February, Colorado Department of Transportation, employee computers temporarily shut down by SamSam virus

- March, Atlanta, Georgia.

- March, Jackson County, Georgia paid \$400,000 after the county’s computer system shut down

- March, Albany, New York.

- April, Hackers stole about \$498,000 from the City of Tallahassee.

- April, Augusta, Maine, suffered highly targeted malware attack that froze the city’s entire network and forced the city center to close.

- April, Cleveland Hopkins International Airport.

- May 7, City of Baltimore.

- June 20, Riviera Beach, Florida paid a ransom.

- June 26, Lake City, Florida paid a ransom.

- July 15, City Power, the electric utility for Johannesburg, South Africa.

- August, 22 Texas towns hit in a “cyberassault.”

McCorkle said that when Del Norte County was hit twice about two years ago, employees clicked on links within innocuous-looking emails. “Employees clicked on an email that took them to a site that got something on the computer that locked some stuff on the computer and county network,” he said.

“We were able to retrieve data, because county data is backed up on another network. Nothing was lost and no money was paid.”

McCorkle said the county takes five easy steps to protect its network.

- Maintain up-to-date firewalls and virus protection.

- Keep software up to date.

- Perform daily backups at multiple locations.

- Limit network access.

- Train employees on what to look for.

“Last year, we invested \$70,000, most of which came from state agencies, including the Governor’s Office of Emergency Services, in security routers and appliances to monitor access in and out of our network,” he said.

McCorkle said a big misconception is that cyberattacks come just via the internet. But the county also has many other connections to the state that are vulnerable.

“There might be 10 different connections out there - Health and Human Services, Child Support, Sheriff’s Office, for example - that all have their own individual connections out to the state somehow. Those connections have to be protected.

“We don’t automatically trust them, because they connect to the state. Actually, we see most of the inadvertent activity coming from those state links,” McCorkle said.

Del Norte County has more than 30 servers and 500 computers up to date with the latest security software, he said. This makes it important to regularly install the updates, say, from Microsoft.

“It’s not that they’ve just heard about an attack. That attack probably happened months ago and they’ve finally figured a way to block it,” McCorkle said.

The county utilizes contracting services that monitor all computers and servers, report on all installed software, and track any unauthorized software that the county did not install.

“This year, we contracted for a little over \$30,000 with a vendor with a new backup system to better protect us from ransomware. We’re spending a lot of money to protect us,” McCorkle added.

District 1 Supervisor Roger Gitlin had two quick questions for McCorkle:

“It sounds like the illegal malware industry is growing. Is that your assessment?”

“Yes.”

“So, it’s not a case of if we’re hit, but when?”

“Yes. Anti-virus systems have gotten pretty good. So, the criminals had to find another way. And that was with phishing emails,” McCorkle said. “They’re figuring out where the weak link is.

“There are so many user names and passwords, that’s where attacks are coming from.”