Bond Case Briefs

Municipal Finance Law Since 1971

How Louisiana Responded to Its Recent Ransomware Attacks.

Through quick response and an existing cyberthreat response system, the state managed to stave off what could have been a much more disastrous attack that would have affected twice as many communities.

In July, after a large-scale ransomware attack struck school districts throughout Louisiana, Governor John Bel Edwards issued a first-ever statewide emergency declaration related to a cyberincident.

The attack — which state CIO Dickie Howze describes as a "single, coordinated" one — infected five separate districts and could have brought down more than half a dozen others were it not for officials' quick response.

That response, largely coordinated by the Governor's Office of Homeland Security and Emergency Preparedness (GOHSEP), was something of a first for Louisiana and included the deployment of emergency personnel and resources, as well as coordination with other state, federal and private-sector professionals.

Chief among the constellation of partners making up GOHSEP was the state's IT department, the Office of Technology Services (OTS), which worked alongside other state partners like the National Guard and State Police to pursue solutions during the crisis.

Now, several months after the attacks, the state is still recovering. Speaking with Government Technology, Howze reflected on this tactical outing, revealing that Louisiana's response efforts prevented even more widespread damage that could have taken place.

"A total of 12 districts were targeted," said Howze. "We were successful in preventing encryption — in other words, we found — ransomware in existence in seven other districts. And by following [our] procedure we were able to unplug and clean, therefore preventing those districts from becoming encrypted."

After an initial forensic analysis by the Louisiana State Police fusion center determined that the attacks were, indeed, ransomware, Edwards' emergency declaration specifically authorized OTS and other state agencies and groups to respond and send resources to affected communities, Howze said.

Containment — the act of identifying, isolating and circumventing the downstream spread of malware — is a critical task in cyberevents, experts say. Thus, after the initial confirmation of infection, a critical maneuver for OTS was the development of a containment task list directed at potentially affected systems. This six-phase plan, created in a little more than 24 hours by the state's CISO Dustin Glover, starts with a simple directive: "Unplug your computer," Howze said.

"The way ransomware works, they infiltrate and they don't encrypt until they have crawled the network to gain access to as many devices as they can gain access to and then they flip the switch

and encrypt," Howze said. "So we felt it was in the state's best interest to put this out there and say, 'Hey, immediately do the following, and check yourself out.'"

At the same time that the containment list was being developed, OTS was helping channel people and resources towards the affected communities, while coordinating with partners like the Louisiana National Guard, the FBI, and private-sector helpers like Microsoft. The Guard supplied many of the resources that OTS was authorized to use, while public- and private-sector officials alike helped inspect and analyze affected systems, Howze said.

In large part, such a coordinated response would not have been possible were it not for the prioritization of cybersecurity by the Edwards administration.

Two years ago, Edwards formed the Cybersecurity Commission — a public-private partnership made up of cyberprofessionals dedicated to developing and advancing a statewide defensive posture. The commission, which brings together a wide assortment of academic, professional and government figures, works together with OTS and other state partners in the event of a cyberattack.

At the same time, Edwards also created emergency support function 17 — meant to be deployed in the event of a critical cyberincident — which activates OST and other partners as part of GOHSEP.

So while July's attack was large in scale, the response by state authorities may have helped make it a smaller event than it could have been. A recent report by Moody's Investor Service used the incident as a case study for how statewide emergency declarations are strategic ways to cut down on fallout.

Looking towards the future, the governor has asked Howze and others to survey communities throughout Louisiana in an attempt to identify potential vulnerabilities and work towards improving the state's overall defensive posture. In today's threat environment there's a lot to look out for, Howze said.

"We continue to invest in our environment; we continue to diligently manage and monitor," Howze said. "We deal with millions of attempts a day … For lack of a better term, it's still a full-court press for us."

GOVTECH.COM

BY LUCAS ROPEK / SEPTEMBER 20, 2019