
# NASCIO State IT Recognition Award Submission
# State of Texas
# Texas Department of Information Resources

**Title:** Texas-Sized Attack Gets Texas-Sized Response

**Category:** Cybersecurity

**Contact:** Nancy Rainosek

**Project Initiation:** September 1, 2017

**Project Completion:** August 31, 2019

# Texas-Sized Attack Gets Texas-Sized Response

## Executive Summary

The mission of the Texas Department of Information Resources (DIR) is to serve Texas government by leading the state's technology strategy, protecting state technology infrastructure, and offering innovative and cost-effective solutions for all levels of government. As the State of Texas' technology agency, DIR is charged with many duties by statute, including cybersecurity through the Office of the Chief Information Security Officer of Texas (OCISO). The OCISO works to set state information security policies and standards, publish guidance on best practices, improve incident response preparedness, monitor and analyze incidents, coordinate security services, and promote information sharing throughout the public sector cybersecurity community.

On the morning of August 16, 2019, more than 20 entities in Texas reported what would turn out to be the largest coordinated ransomware attack against local government in US history at the time. Most of these entities were smaller local governments. DIR was well-poised to respond to the August ransomware attack due to the statewide cybersecurity incident response plan, which was the culmination of a two-year long project in response to a legislative mandate issued in 2017. The Texas Emergency Management State Operations Center (SOC) was activated with a day and night shift, with priority placed on response and recovery from the attack. While DIR led the response to the attack, statewide participation, preparation, and cooperation were the keys to the successful Texas response to the August 2019 Ransomware Incident.

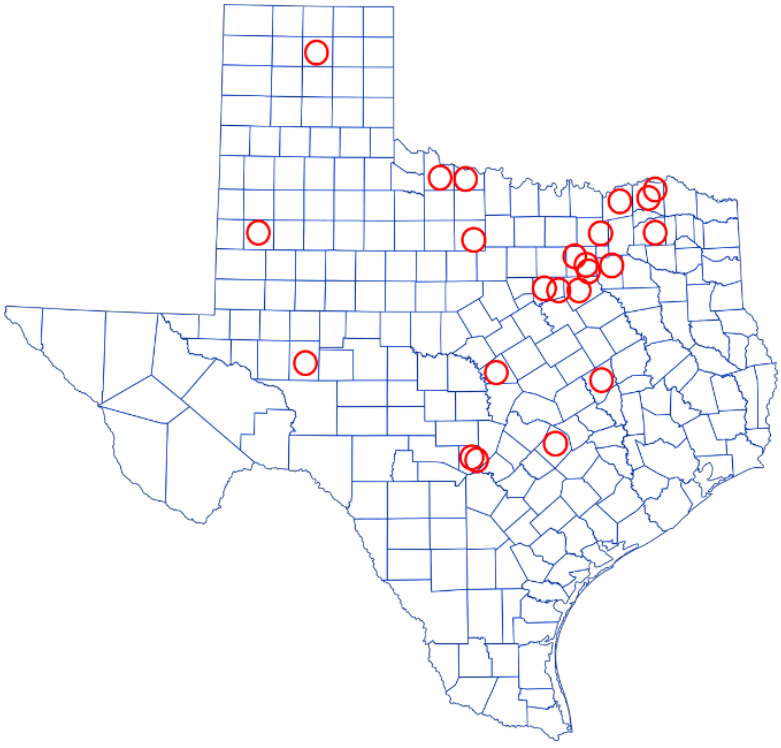

*Figure 1. Approximate locations of the 23 entities impacted by the August 2019 ransomware attack.*

## Project Narrative

**Exemplar:**

On Friday, August 16, 2019, 23 Texas local government entities were simultaneously attacked in the same ransomware event. DIR, through the Office of the Chief Information Security Officer, was called into action to lead the response and assist the impacted entities in their recovery. Managed as a project, preparation and cooperation were the keys to the successful Texas response to the ransomware incident which included support from the following entities:

- Texas Division of Emergency Management (TDEM)
- Texas Military Department (TMD)
- The Texas A&M University System's Security Operations Center and Critical Incident Response Team
- Texas Department of Public Safety (DPS)
- Texas Commission on Environmental Quality (TCEQ)
- Texas Public Utility Commission (PUC)
- Department of Homeland Security (DHS)
- Federal Bureau of Investigation – Cyber (FBI)
- Federal Emergency Management Agency (FEMA)
- Other Federal and Private Sector cybersecurity partners

The ability to bring these entities back online and into the rebuilding phase within one week can be attributed to effective coordination, phenomenal leadership, thorough preparation, and complete cooperation between the responders. All of which were made possible through a two-year long interagency project, led by DIR, to develop a statewide incident plan to respond to enable Texas to effectively respond to an remediate major cyber attacks.

**Concept**

For almost two years the State of Texas developed an incident response plan, utilizing cybersecurity best practices and lessons learned from years of responding to incidents in the event of a large-scale cyber-attack. This plan was put into action on Friday, August 16, 2019. As public servants across the state came to work early that morning and discovered that their

systems had been compromised and held hostage by ransomware, reports began filing into us at DIR. Given the number of entities and systems impacted and the very real public health and safety threat posed by the attack's effects on critical systems, DIR notified the Office of the Governor to discuss the need to issue a disaster declaration. That morning, Texas Governor Greg Abbott issued the State of Texas' *first* statewide disaster declaration for a cyber event.

DIR was well-positioned to respond to the August ransomware attack due to the statewide cybersecurity incident annex, established in response to requirements from the Texas Legislature, effective September 1, 2017. In addition, DIR utilized additional programs and resources:

- **Cybersecurity Incident Annex** - In 2017, the Texas Legislature passed House Bill 8 which called for DIR to create a statewide cybersecurity incident response plan. DIR coordinated the plan's development with the Texas Division of Emergency Management, the Texas Department of Public Safety, and the Texas Military Department. DIR held incident handling training and incident response exercises with response partners to ensure that the state would be well positioned to respond in the event of a large-scale attack. DIR also hosted Certified Incident Handling class for the team through their InfoSec Academy training program which offers industry standard trainings at no cost to agencies.
- **Managed Security Services Contract** - Through DIR's Shared Technology Services program, state and local governments can utilize a pre-negotiated cyber incident response contract with a managed security services vendor with no retainer fee. All contractors under this service are background-checked in advance so they are ready to assist on demand. Through the contract, DIR established competitive pricing as well as service level agreements for guaranteed response times and service quality and delivery.
- **Texas State Operations Center -** Activation and colocation at TDEM's State Operations Center was a critical component to the success. TDEM provides a logistics, communications, and coordination infrastructure and expertise that they use to support response to all manner of disasters, and they are tied into local emergency operation centers and contacts across the state. Additionally, local governments are already accustomed to the communication channels from TDEM.

Collaboration was critical to the success of the state's response to the ransomware attack:

- Utilization of the TDEM SOC was a key driver in Texas' success. TDEM is prepared for communicating with the local entities through their statewide conference call capability, district coordinators, and information sharing tools (Riot and WebEOC) to securely communicate with the incident response field teams.
- Through a Texas A&M agreement, the team was able to deploy end point detection and response software to the impacted entities to detect and prevent any spread or reinfection.
- Through a partnership with the FBI cyber team, the Texas A&M cyber team was empowered to perform much of the forensics and reverse engineering, which significantly improved the timeliness of threat handling at the time of the incident.

- Texas' Department of Public Safety fielded law enforcement units to quickly gather evidence to support criminal investigation and future potential prosecution of the attackers.
- Once the Governor declared a disaster, it opened the door to using another critical component of the plan and the people, skills and resources of the Texas Military Department (TMD) and Texas' guard forces were brought to bear and provided the ability to put boots on the ground and hands to keyboards at each locality by the fourth day of the incident, with one team traveling more than ten hours to get on site.

**Significance**

The interagency cooperation that occurred during this event is a testament to how government agencies at the federal, state, and local level can effectively work together to respond to critical events. No single agency could have responded successfully to the August ransomware incident. Absent these incident responders, the 23 local entities would have had great difficulty responding to the event without either paying the ransom or spending considerable time and resources trying to handle the situation on their own.

Unfortunately, cyberattacks on state and local governments have become our new normal. While the August event was the first statewide cyber disaster declared in Texas, it will likely not be the last. Texas continues to prepare, as a state, for the next event, building and improving on our existing plan and anticipating what the next generation of cyber warfare will look like.

**Impact**

This coordinated state and federal response to a statewide, multi-jurisdictional cybersecurity event was the first of its kind, anywhere, and was a tremendous success.

- No ransom was paid in this event. The current total cost for the state response is approximately one-tenth of the $2.5 million ransom demanded by the criminals responsible for this attack.
- While other attacks have left their victims still struggling to get back to business months and years later, the Texas response enabled every impacted entity to get back to business in just one week.
- Through the dedication and vision of the Office of the Chief Information Security Officer at DIR, a response plan was in place and ready to be put into action immediately.
- Within hours of receiving notice of the event, state and federal teams were executing the plan and in the field at the most critically impacted sites to begin assessing impact to systems and eradicating the malware.
- By day four, response teams had visited all impacted sites and state response work had been completed at more than 25% of those sites.
- One week after the attack began, all sites were operational, open for business, and cleared for recovery to get back to full capacity.

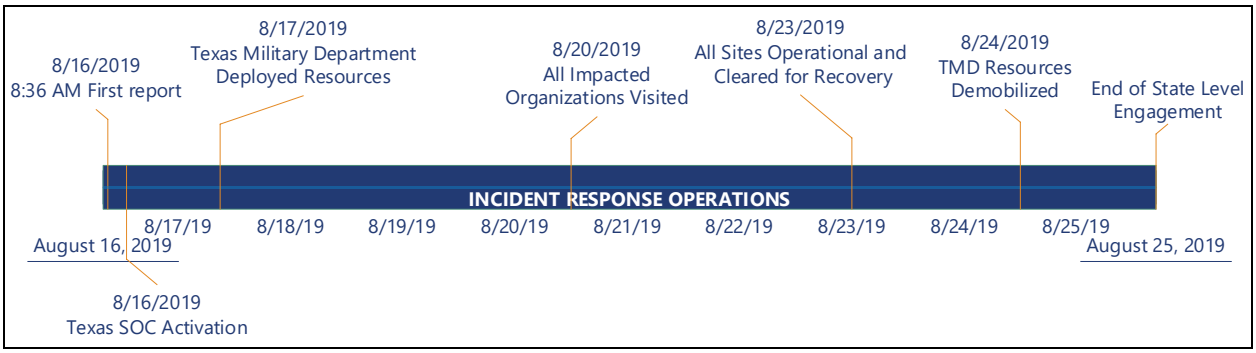


*Figure 2: Ransomware Incident Response Timeline*

The success of this project and the response it enabled was recognized on a national level. In February 2020, DIR's Executive Director Amanda Crawford testified before the United States Senate Committee on Homeland Security and Governmental Affairs in Washington D.C., on the Texas response and what made it such a success.

## Supplemental

Texas Department of Information Resources, Incident Response Planning and Guidance: https://dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=162

"What States, Locals, and the Business Community Should Know and Do: A Roadmap for Effective Cybersecurity." Statement before the United States Senate Committee on Homeland Security and Governmental Affairs, Amanda Crawford, Executive Director Texas Department of Information Resources, February 11, 2020: https://www.hsgac.senate.gov/imo/media/doc/Testimony-Crawford-2020-02-11.pdf

Ransomware- Protective Measures and Response, the Texas Department of Information Resources and the Texas A&M University System Webinar, August 2019: https://www.youtube.com/watch?v=MdXogO-4m4s&t=19s