

Troubling Times: Ransomware Across Texas

**Deputy Chief Information Security Officer – Andy Bennett
2019 Cybersecurity Awareness Month Event
October 22, 2019**



2019 Texas Headlines

Del Rio, Texas ransomware attack knocks city back using to pen and paper | SC Media

SC Magazine · Jan 14



City of Laredo recovering from ransomware attack

Laredo Morning Times · Jun 17

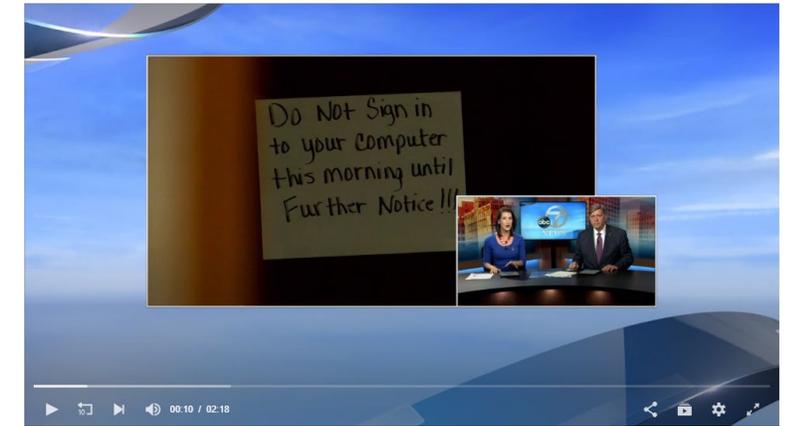
Ransomware Attack Hits 22 Texas Towns, Authorities Say

The state declined to say which towns were affected by the coordinated cyberattack. But one expert said it could signal more such attacks in the future.



Three viruses attack Potter Co. computer system, employees anxious to return to work

by Tiffany Lester | Friday, April 26th 2019



Hackers hold Jackson County computers ransom for undisclosed amount of bitcoin

Victoria Advocate · May 30



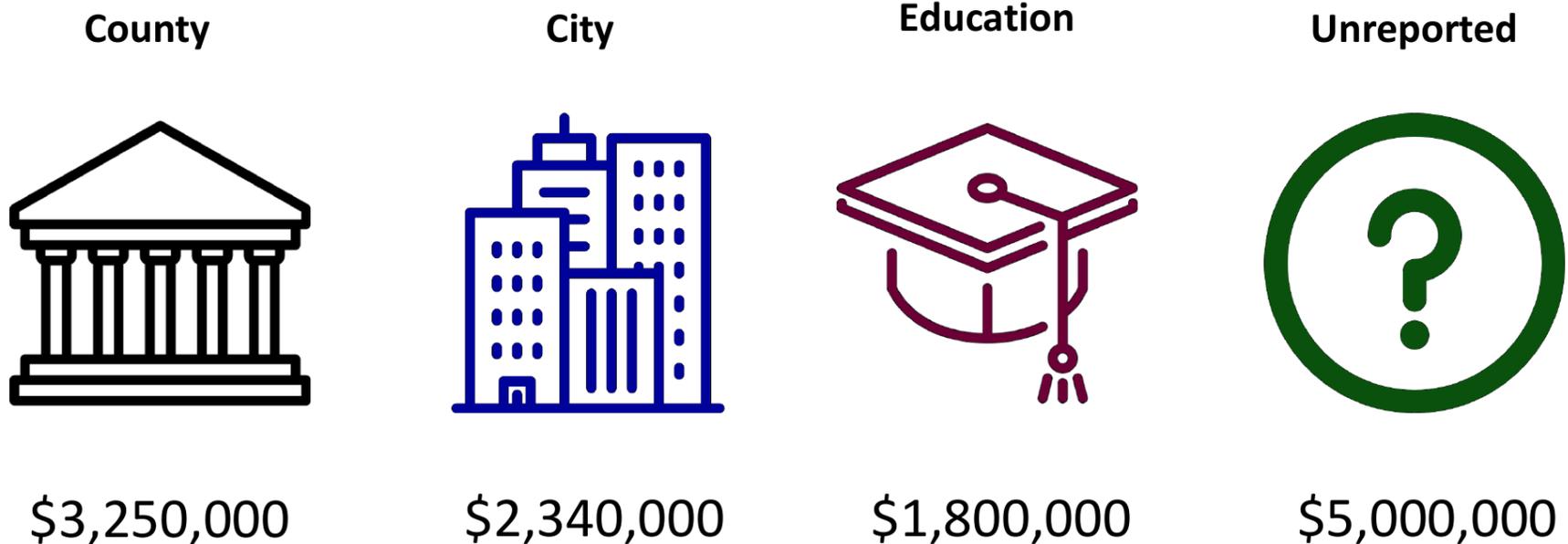
Sul Ross recovering its campus systems from ransomware

Del Rio News Herald · Jun 30



The Texas State Capitol and state offices, where the Texas Department of Information Resources is based. The department is leading the response to the cyberattacks. James Leynse/Corbis, via Getty Images

Estimated Ransomware Costs – Texas 2019



Cyber criminals holding your data and systems hostage



- Increasing # of attacks
 - 200 publicly acknowledged ransomware attacks against SLTT since late 2013
 - Business detection up 363% since 6/18
- Increasing rates of ransom
 - 97% in the past two years
 - MegaCortex - \$20K-\$5.8 million

Concerns:

- Ransom versus the cost to get well
- Image and optics
- Customer/citizen confidence

Preparation is Key: What Texas has done



- **Cybersecurity Annex to the Texas Division of Emergency Management(TDEM) State Response Plan**
 - House Bill 8 (2017) called for DIR to create a statewide incident response plan.
 - The current TDEM annex had not been updated since 2013 and had not been tested.
 - DIR coordinated plan development with TDEM, Department of Public Safety, Texas Military Department
 - Incident handling training (Certified Incident Handling) was included in this effort
 - Held incident response exercise with partners
- **Managed Security Services Contract**
 - Pre-negotiated cyber response contract with managed service vendor with no retainer fee
 - Ticketing System in ServiceNow with MSI
 - All contractors are CJIS background checked
 - Service Level Agreements in place for response times

1. Keep your systems current, hardened, and patched
2. Keep your users and IT staff trained and aware
3. Know where your data is and make sure you have good backups
4. Maintain and practice Incident Response and Business Continuity plans.

RDP

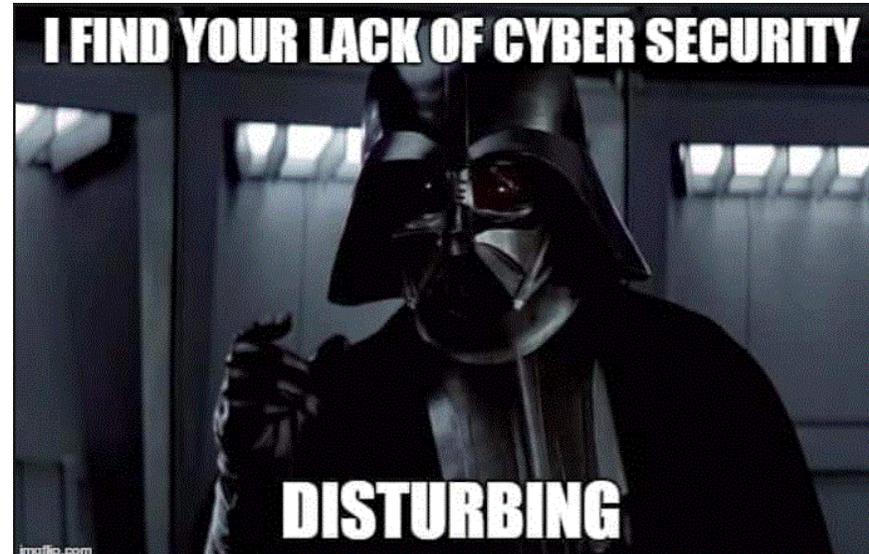
MFA

- Keep accurate inventory and network diagrams
- Know what applications are on your network
- Have security devices that are actively managed and/or serviced
- Pick a cybersecurity framework and use it -Texas CSF, NIST
- Schedule an assessment against the framework
- Build to a baseline – configure and assess systems
- Segment your network
- Use least privilege principle and MFA
- Actively patch and scan your systems for vulnerabilities
- Only use systems and applications that are supportable
- Budget IT and cybersecurity into projects and operations

- Secure Network Design
- Build to a baseline - configure your systems and assess periodically
- Actively scan, patch and log. Keep Anti-Virus up to date
- Use least privilege principle, strong passwords, separate administrator accounts, and MFA
- Only use systems and applications that are supportable

Awareness & Training

- All employees need cybersecurity awareness training. (HB 3834)



- IT staff need to know how to use the tools they have
Are IT and cybersecurity able to quickly respond and isolate?

Third-party risk management

- Know what contracts you have in place
- Vet your service providers
- Have contractual language that covers your requirements
- Be sure the contract has security rule enforcement mechanisms



[This Photo](#) by Unknown Author is licensed under [CC BY-SA](#)

What to do after it happens

Is it real?
Keep Cool



Enact your
Incident Response &
Business Continuity
Plans

- Speed of response upon detection is key to minimizing impact.
- Cyber incidents can have direct and indirect kinetic emergency effects.
- Cyber disaster & public safety – Yes, this IS an emergency

- Can you conduct business without your information systems?
 - How and for how long?
- Can you conduct business without your data?
 - How and for how long?
- What does your staff do if the systems are down?
- What do your customers do if your systems are down?
- How invested is your organization into IT, automation, and services?



Business continuity plan should help guide your decisions.

Cyberinsurance & Pay decisions



Cyberinsurance and pay decisions

Is this simply an informed business decision?

Decisions might be driven by the policy.

Back to square one with the same situation that allowed the ransomware in the first place.

What are the requirements that the cyberinsurance policy establishes for coverage and payout?

Does payment of the ransom put a target on your organization?

Delaying the decision and the window closing.

Case Studies

- Atlanta, GA
- Baltimore, MD
- Colorado Department of Transportation
- Jackson County
- State of Louisiana
- Riviera Beach, Florida - \$600K in ransom payment (\$10K deductible + cyber insurance policy) and \$1million for systems/services to improve their posture going forward



Business Email Compromise (BEC)

\$1.3 billion in 2018 – FBI

\$300 million each month – U.S. Treasury

476% increase from 2017 to 2018

Financially motivated

- Invoices, direct deposit, ...

Low-tech cross checks in processes -
Challenge

Pre-August Ransomware Incidents

- Potter County
 - Entire County infrastructure impacted by ransomware on a Friday.
 - Law Enforcement
 - Commissary
 - Video dashboard cameras
 - Real estate transactions
 - Hired Managed Security Services (MSS) vendor to remediate
 - Potter county did not have good backups so the re-entry cost hundreds of thousand dollars in overtime for re-entry
 - Saturday county election was not impacted due to steps taken after an election security assessment performed by MSS vendor
- Jackson County
 - The first disaster declaration by a county judge due to a cyber event
 - The first execution of the TDEM cyber annex utilizing the Texas Military Department
 - Contracting was the long-pole in the tent. It took almost a week to get the contracts signed between the TMD and the county
 - Jackson County had not had an election security assessment. Had they had it, Trick Bot would have been discovered and they may have avoided this incident.

August 16 Ransomware Incident

- 8:36 am DIR notified about 8 local governments with ransomware
- By 11 am the number had grown to 22
- TDEM Security Operations Center activated by noon through a level two declaration by the governor
- All targets identified and prioritized by noon on Saturday
- All sites visited by Sunday
- By Friday, all sites remediated to the point that state support was no longer required
- The state used the firefighter model. We put out the fire, boarded some windows making the structure usable, but entities had to rebuild their own houses.

Lessons learned

- Utilization of the TDEM SOC was a key driver in our success. They are prepared for communicating with the local entities through their district coordinators and have tools (Riot and WebEOC) to communicate with the field teams
- Prioritization was also important. Knowing which entity to respond to first due to the limited resources available. Complexity and safety was used.
- Due to the federal investigation, we were unable to release information about the incident except to trusted parties under TLP Red designation. We need to expand this list of trusted parties so more information sharing can occur.
- In addition to FBI, we had a Texas A&M cyber team and DHS doing forensics and reverse engineering. We deployed EDR software to the entities to detect any spread or reinfection.
- Don't believe everything you read in the press. 😊

Checklists and Response

- Numerous resources available
- Isolate the affected systems is the common start
- Contact Law Enforcement and insurance company
- Types of recovery – how it was v. how is should be

- DIR - <https://dir.texas.gov/View-About-DIR/Information-Security/Landing.aspx>
- MS-ISAC - <https://www.cisecurity.org/ms-isac/>
- NIST - <https://www.nist.gov/topics/cybersecurity>
- US-CERT - https://www.us-cert.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf

Contact and Questions

Andy Bennett

CISM, CBCP, ITIL

Deputy Chief Information Security Officer

Office of Chief Information Security Officer

Texas Department of Information Resources

DIRSecurity@dir.texas.gov

