Cybersecurity Update

Amanda Crawford

Executive Director and

State of Texas Chief Information Officer

Transforming How Texas Government Serves Texans

Texas Department of Information Resources

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.

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

What We See

Common Cybersecurity Issues

Lack of Knowledge of IT Assets

What is on your network?

- It's probably more than you think.

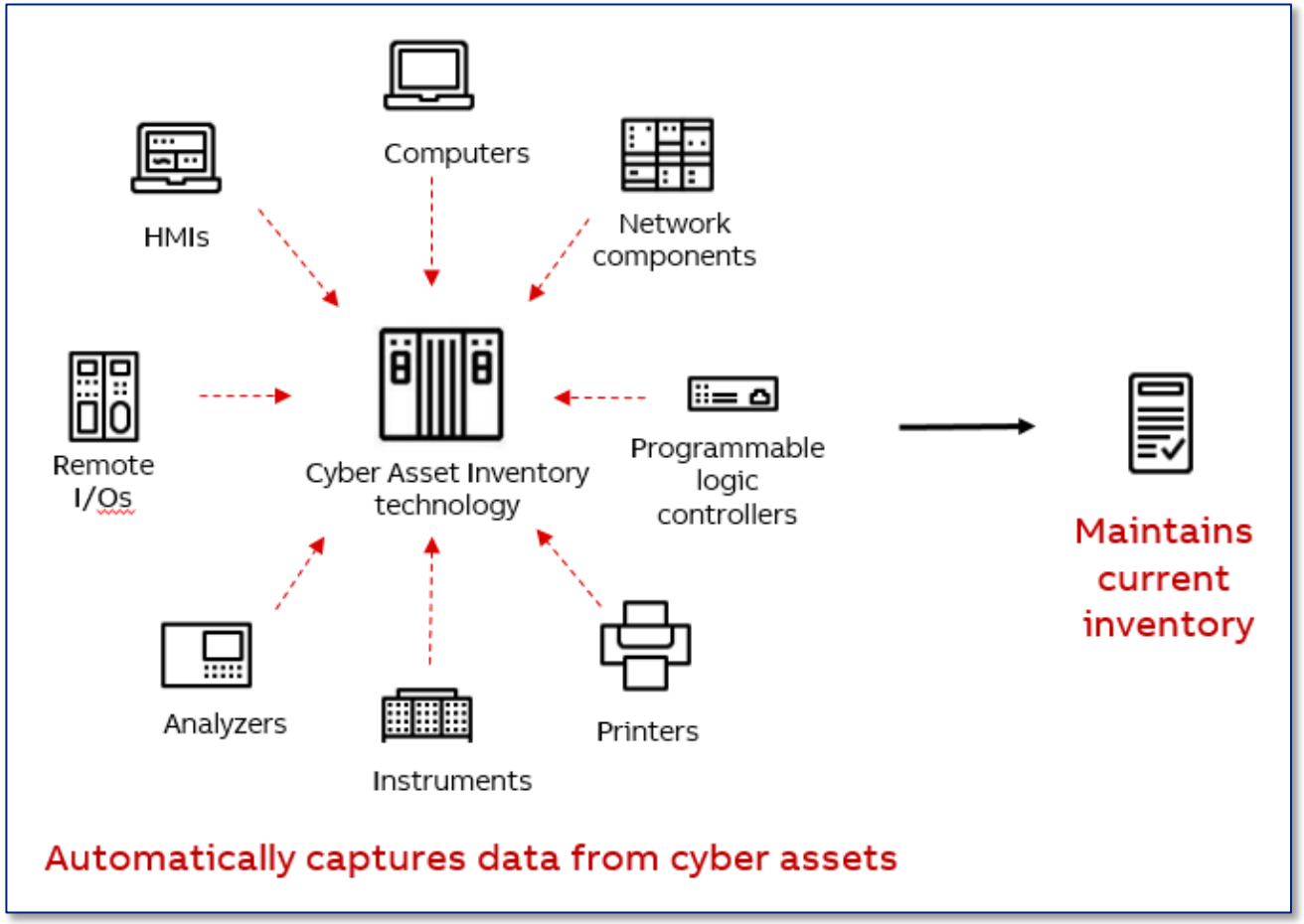
Is your network segmented?

What is running where?

- "We didn't know that system ran off those servers."

Where are your physical resources?

Where are your backups located?



Inventory Your Services

IT teams and service providers are usually not the business experts.

How do your constituents interact with their government?

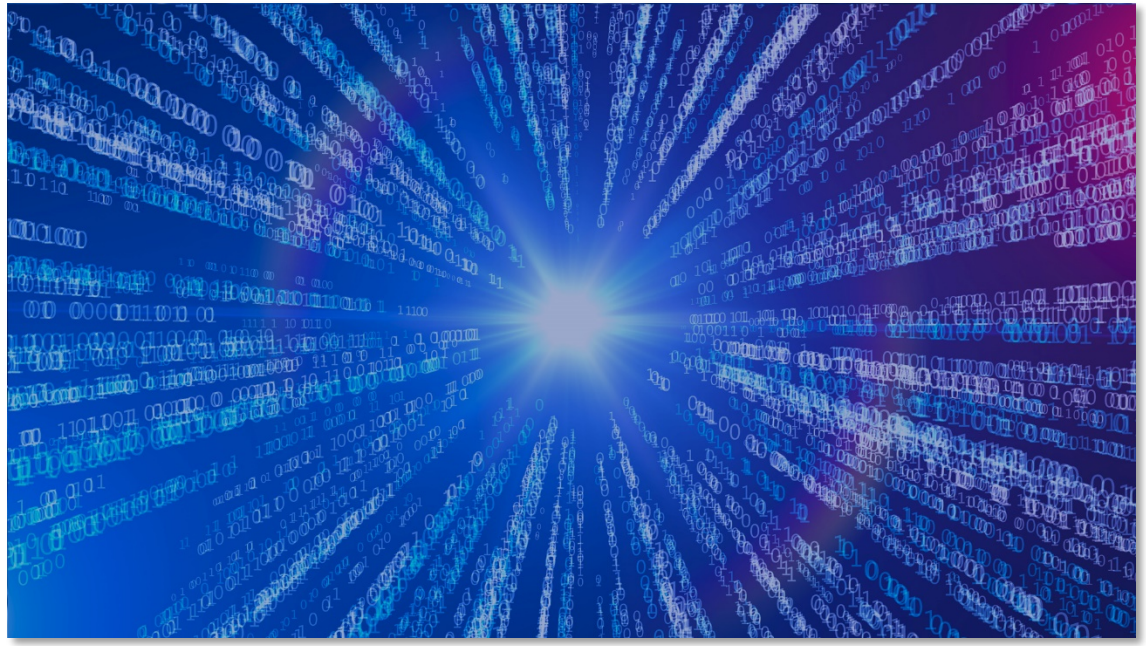
- "We didn't know that application was used so much!"
- Public safety applications
- Billing applications
- "It's always just worked."

What are your critical applications and services?

Inventory Your Data

What is in your databases, email, and file stores?

- Personally identifiable information?
- Criminal investigation information?
- Medical information?
- Billing information?
- PCI data?
- Other regulated data?



When a cybersecurity event happens, who do you have to notify?

- Business requirements
- Legal requirements

Inventory Your Backups

Where are your backups?

- No good if you can't get to them when you need them.

Make sure…

- Your backups are segmented.
- Your backups are tested and usable in case you need them.
- You are backing up what your entity needs.

Offline backups are key in case of corruption.

- One victim only connected their backups to the network one day a month. The hacker figured that out and waited until that day to encrypt the backup.
- Multiple backups that are offline are a great way to ensure you can restore most of your data.

Internet Accessible Administration

Giving your administrators the ability to work remotely helps work/life balance when they answer late night calls, but remote access needs to be secure.

Many breaches happen because:

- Remote access was accessible to the Internet, without requiring VPN, via RDP or SSH.
- Multi-factor authentication was not enabled.
- Administrators use privileged accounts for regular work.
- Default administrative accounts:
  - Not renamed
  - Allowed interactive login
  - Simple passwords
  - No retry lockouts, making them vulnerable to brute force attacks

Third-Party Providers

Third-party providers are a great way to obtain support. They may even feel like part of the family, which can lead to a lack of oversight.

Remember to:

- Audit them to verify security.
- Make sure your contracts have strong cybersecurity and liability protections.
- Work with third-party providers on your response plans.

Lack of Planning

Too often, we hear there was no plan.

- "Not enough time."
- "Didn't know where to start."
- "I wish we had made a plan."

Make your plan flexible.

- Things don't always go according to plan.
- Don't get caught up in details.

Experience is no substitute for having a plan.

- Entities that have no plan despite having been affected before often do not perform as well as entities who have never been affected, but already have a plan in place.

When panic sets in, you need a framework to get everyone on the same page.

- When someone is hurt, it is better to tell one person to go call 911 than it is to yell "someone call 911" to a panicking crowd.

Lack of a Cyber-Aware Culture

Creating a cyber-aware culture starts at the top and sets the expectation for the entire organization.

Remember, cybersecurity is a team sport.

Lack of engagement with management before an incident happens.

- Management "too busy."
- IT staff afraid of management.
- This leads to the blame game.
- Clarify who to contact about what, and when.

Excluding business executives from planning.

- Security and response must be prioritized.

Lack of routine status reports.

Annual and mandatory cybersecurity training for all must be prioritized.

Moving Forward after an Incident

Just because systems are back up and running, that doesn't mean you should go back to the way things were.

- **We have seen entities hit multiple times because they didn't fix the underlying issue.**
- **If the bad guys got in once, make sure the way in is fixed.**
- **Update your plan.**
- **Assess what went right and what went wrong.**

To insure or not to insure? Is it worth it?

How DIR Can Help

DIR Information Security

Office of the Chief Information Security Officer (OCISO)

- Information security leadership, policy, direction, education, awareness, reporting, and statewide initiatives

Cybersecurity Coordination

- Texas Cybersecurity Council

Network Security Operations Center (NSOC)

- Network security monitoring, intrusion prevention services, alerting, incident response guidance, and threat analysis for state agency customers

A Few of DIR's Security Offerings

Offerings	Local Government	State Government	Higher Education
Policy & Security Controls Catalog		✓	✓
InfoSec Academy		✓	✓
End-User Security Awareness Training		✓	✓
Information Security Forum	✓	✓	✓
Vulnerability Scans & Penetration Tests	✓	✓	✓
Security Assessments	✓	✓	✓
Statewide Data Center and Technology Services	✓	✓	✓
Managed Security Services	✓	✓	✓
Network Security Operations Center (NSOC)	✓	✓	✓

Managed Security Services Contract

- Through DIR's Shared Technology Services, local governments can utilize a pre-negotiated cyber incident response contract with a managed security services vendor with no retainer fee.
- All contractors are background checked so they are ready to assist on demand.
- DIR established service level agreements for guaranteed response times.

Eligible Customers

- State of Texas Agencies
- Local County and City
- K-12
- Higher Education
- Special Districts

TEXAS ISAO

The Texas Information Sharing and Analysis Organization (ISAO) provides a mechanism for state and non-state entities in Texas to share actionable and timely information regarding cybersecurity threats, best practices, and remediation strategies, while advancing the cybersecurity capabilities and resilience of the State of Texas.

The Texas ISAO is available to all Texas operations of public, private, and non-profit entities, at no cost.

isao.texas.gov

How the State is Responding

87th Regular and Special Sessions

SB 475 (Nelson/Capriglione)

Relating to state agency and local government information security, including establishment of the state risk and authorization management program and the Texas volunteer incident response team.

A comprehensive data security, data management, and cybersecurity bill that strengthens the state's standards on agencies' data management practices, storage, and Texas' ability to respond to cybersecurity incidents that creates:

- Texas Risk Authorization and Management Program
- State Agency Data Management Advisory Board and Data Management Officers
- Texas Volunteer Incident Response Teams
- Regional Cybersecurity Working Groups
- Regional Security Operation Center

SB 475 also directs state agencies to consider using robotic process automation and prohibits state agencies from collecting biometric identifiers without consent. It also requires agencies to include contractual language requiring vendors to meet security controls proportionate with the risk based on the sensitivity of the data.

Effective immediately, except the state agency prohibition on collecting biometric identifiers becomes effective September 1.

HB 1118 (Capriglione/Paxton)

Relating to state agency and local government compliance with cybersecurity training requirements.

- Require cybersecurity training for elected and appointed officials who have access to the computer system or database and use a computer for at least 25 percent of their required duties.
- Requires local governments to submit written certification of cybersecurity training completion when applying for Governor's Division of Criminal Justice grants.
- Requires non-compliant local governments to pay back Criminal Justice Division grants and makes them ineligible for additional Criminal Justice Division grants for two years.
- Requires agencies to include completion of training certification in their strategic plan.

Effective immediately.

HB 1576 (Parker/Paxton)

Relating to the creation of a work group on blockchain matters concerning this state.

- Creates a legislative working group on block chain policy.

Effective September 1.

HB 4018 (Capriglione/Nelson)

Relating to the creation of the technology improvement and modernization account and the permissible uses of money in the account.

- Creates a legislative oversight committee on agency technology and modernization projects and a dedicated fund for those projects.

☑ **Effective immediately.**

SB 851 (Blanco/Dominguez)

Relating to the composition of the cybersecurity council.

- Adds Secretary of State to the Texas Cybersecurity Council.

☑ **Effective September 1.**

SB 1696 (Paxton/Wilson)

Relating to establishing a system for the sharing of information regarding cyber attacks or other cybersecurity incidents occurring in schools in this state.

- Requires TEA and DIR to establish system for sharing anonymous cybersecurity incidents among schools and the state.

☑ **Effective September 1.**

Cybersecurity Funding in the State Budget

87th Regular and Special Sessions

Cybersecurity Funding in the 87th Regular Session

Around $100 million in funding for cybersecurity projects including:

- **$15.7 million for Endpoint Detection and Response (EDR) technology for state agencies**
  - Allows DIR to purchase EDR technology and implement it at no cost to participating state agencies to better protect them from ransomware and other cyber threats.
- **$6.9 million for Regional Security Operations Centers Pilot**
  - Allows DIR to partner with a public university to establish the security operations center pilot program authorized in SB 475.

Second Called Special - HB 5 Cybersecurity Funding Items

Endpoint Detection and Response	Regional Security Operations Center	Multi-Factor Authentication
• Software for computers and cell phones that detects and blocks threats. This software will better protect state devices and network from cyberattacks.	• Per SB 475, this will provide local partners perimeter security by monitoring incoming network traffic, blocking malicious sites, and protecting against potential attacks.	• Technology that requires several verification factors to gain access to an account or network. • This protects state employees' account security and makes it harder for cyber criminals to gain access to the state's network through stolen passwords.
$6,534,350 and 1 FTEs	$6,909,161and 7 FTEs	$4,000,000 and 1 FTE

Third Called Special – SB 8

Included $200 million of federal funding for DIR to deposit into the Technology Improvement and Modernization Fund

- Before funding projects, DIR must receive approval from the Joint Oversight Committee on Investment in Information Technology Improvement and Modernization Projects established under Section 2054.578, Government Code.

Thank You

dir.texas.gov

#DIRisIT

@TexasDIR

Transforming How
Texas Government
Serves Texans

Texas Department of Information Resources