DIR
Texas Department of Information Resources

Office of the Chief Information Security Officer

THE STATE OF TEXAS GUIDE TO

Cybersecurity Incident Response

Does your municipality or county need state assistance and/or guidance for an active cybersecurity incident?

If you are experiencing a cybersecurity incident and need some help, the state can provide assistance.

Don't hesitate! Call right away.
Disconnect, but don't power down.

When cyber incidents occur, the Texas Department of Information Resources (DIR) can help impacted entities, analyze the potential impact across critical infrastructure, and coordinate the state response to significant cyber incidents.

DIR works in close coordination with other agencies with complementary cyber missions, as well as private sector and other non-state owners and operators of critical infrastructure, and in some cases, the federal government to ensure greater unity of effort and a whole-of-nation response to cyber incidents.

DIR = First Responder

As with any crime, you want both the aid agencies and the police to be present.

State Incident Response assistance led by DIR is like an aid agency. DIR's role is to inhibit the virus from spreading to other systems, help eradicate the virus, help determine how it entered, and advise you on how to lower the chances and damage of any future attacks.

Any law enforcement investigatory response role is to figure out who the perpetrator is and bring them to justice.

State Response – the goal is to help neutralize the threat and enable road to recovery.

At the tactical level, the state can help:

- Find the adversary on its systems;
- Determine how the actor entered;
- Remove the adversary from its systems; and
- Advise on recovery.

At the strategic level, the state will:

- Coordinate the provision of assistance from all resources to the affected entity;
- Share anonymized information about the incident threat indicators as allowable so that others can use it to protect themselves; and
- Identify and alert other entities that may be at risk from this particular incident.

What does state response need to know?

Basic information is needed so we can understand the impact and advise on courses of actions.

In the case of a state cyber response, more details of the layout and situation will be needed before responders arrive on-site so the right people and skills are included.

Costs

Contacting and consulting with the state of Texas for cyber incident assistance has no cost. Depending on the selected incident response, there are both no-cost and priced options.

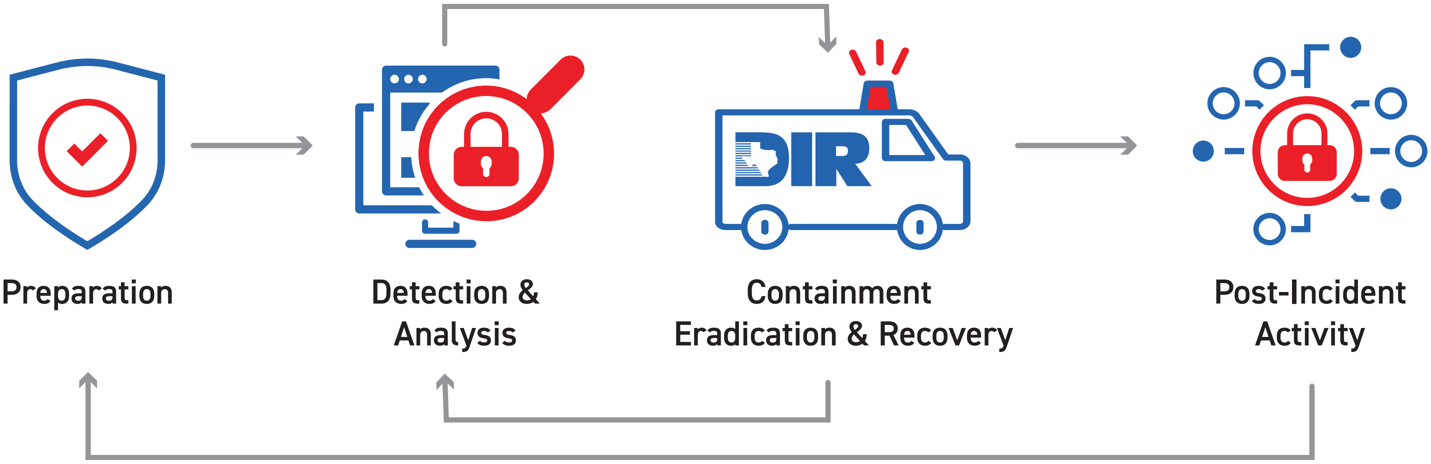
IF YOU NEED ASSISTANCE

Contact your Emergency Management Coordinator or Texas Division of Emergency Management (TDEM) District Coordinator https://tdem.texas.gov/field-response/.
Or, contact DIR Office of the CISO at 1-877-DIR-CISO (1-877-347-2476) or by email at DIRSecurity@dir.texas.gov.

current as of January 2020

continued

Phases of Cyber Incidents



Preparation

Let's get ready for this eventuality and try to lessen the chances and/or impact of it.

Detection & Analysis

Can we quickly know when it happens and quickly start determining what it is?

Containment Eradication & Recovery

Can we trap and eliminate it? Get things back to how they were before the incident and normal operations.

Post-Incident Activity

What happened? What do we need to do? How can we learn from this? How can we lower the chances it happens again and the impact that it would have?

Overarching Guiding Principles

Shared Responsibility: We all have a shared interest and complementary roles and responsibilities in protecting the state and nation from malicious cyber activity and managing cyber incidents and their consequences.

Risk-Based Response: The state government will determine its response actions based on an assessment of the risks posed to an entity, to the state, our national security, the broader economy, public confidence, or public health and safety.

Respecting Affected Entities: State responders will safeguard details of the incident, as well as the affected entity's privacy and sensitive information.

Unity of Governmental Effort: The first state entity aware of a cyber incident will rapidly notify other relevant state agencies to facilitate a unified response.

Enabling Restoration and Recovery: State response activities will facilitate restoration and recovery of an entity that has experienced a cyber incident, balancing investigative and state/national security requirements, public health and safety, and the need to quickly return to normal operations.

HELP

IF YOU NEED ASSISTANCE

Contact your Emergency Management Coordinator or Texas Division of Emergency Management (TDEM) District Coordinator https://tdem.texas.gov/field-response/.
Or, contact DIR Office of the CISO at 1-877-DIR-CISO (1-877-347-2476) or by email at DIRSecurity@dir.texas.gov.

current as of January 2020