State of Texas Cybersecurity Strategic Plan

2024–2029

Table of Contents

From the Desk of the Chief Information Security Officer

The cybersecurity landscape is constantly evolving and can be difficult for Texas government entities to navigate. Texas public entities are alluring targets for cyber threat actors who are using increasingly sophisticated tactics, techniques, and procedures; never-before-seen tools; and exploitative technologies, which can present cybersecurity challenges as dynamic as the cyber threat landscape itself. As we increasingly rely on digital systems and interconnected technologies, the opportunity for attack increases, presenting cyber threat actors with ample opportunity to exploit both known and unprecedented vulnerabilities.

A key challenge facing Texas is the rapid proliferation of technology, ranging from sophisticated hacking tools and techniques—which can be easily accessed on the dark web—to new technologies such as generative Artificial Intelligence (AI) and autonomous vehicles. Access to sophisticated dark web resources enables even the least skilled of cyber threat actors to launch damaging cyberattacks against Texas' government, agencies, and departments. Moreover, the rise of emerging technologies (such as the Internet of Things (IoT) and AI) introduces novel vulnerabilities that demand innovative defensive strategies. As complex security protocols can hinder user experience, balancing usability and convenience with stringent cybersecurity measures poses another challenge for government entities to overcome.

The nationwide shortage of skilled cybersecurity professionals exacerbates these challenges, making it difficult for Texas organizations to effectively deploy, manage, and adapt their security tools to new and evolving threats. This shortage begets outsourcing to third-party vendors, who often face cybersecurity challenges themselves. In this ever-shifting landscape, staying ahead of threat actors requires a proactive approach, continuous learning, strong contracting, and the integration of cutting-edge technologies to fortify digital defenses.

The Texas Department of Information Resources (DIR) prepared the Texas Cybersecurity Strategic Plan to assist organizations with improving their cybersecurity programs. Aligning your organization's cybersecurity efforts with the five goals—risk management, governance, education, resilience, and workforce development—can help your organization be prepared to address the challenges we all face.

While directed at the state level, this plan offers a foundation for strengthening any organization's cybersecurity program. DIR and the Office of the Chief Information Security Officer are here to assist our customers and believe incorporating these goals will advance your cybersecurity initiatives. Cybersecurity is a team sport, and working together, we can create environments to withstand the cybersecurity challenges of today and tomorrow.

Thank you for the privilege of serving you!

Nancy Rainosek

Nancy Rainosek
Chief Information Security Officer
State of Texas

State of Texas Cybersecurity Vision

Texas government entities will form a secure and resilient cybersecurity environment by using their resources efficiently, collaboratively, and effectively to create a risk-aware culture that prioritizes the protection of online government services, critical infrastructure, and Texans' information.

State of Texas Cybersecurity Goals

Our statewide cybersecurity strategy will fortify Texas' cybersecurity landscape by:

Goal 1: Reducing the cyber threat surface through **robust risk management**;

Goal 2: Enhancing the state's **cybersecurity governance capabilities**;

Goal 3: Fostering a prevalent culture of **cybersecurity awareness and education**;

Goal 4: Improving resilient, **uninterrupted business critical operations** during and after cyberattacks; and

Goal 5: Instituting **workforce programs** dedicated to nurturing and advancing cybersecurity professionals.

This comprehensive approach to cybersecurity ensures the protection of Texans' data, the reliability of digital services, and the overall trustworthiness of the state's online infrastructure.

Goal 1: Threat Surface Management

Reduce Texas' cyber threat surface through comprehensive risk management.

Overview

To safeguard digital assets from potential cyber threats, Texas embraces a comprehensive risk management approach that incorporates cutting-edge tools, robust processes, thorough methodologies, and proven governance. By continually monitoring, analyzing, and addressing cyber risks, Texas can proactively identify vulnerabilities and stay one step ahead of cyber threat actors.

Challenge

Texas organizations face an array of cybersecurity challenges. These cybersecurity challenges can be difficult to address due to complicated and evolving factors, such as cyber risk tolerance, social unrest, ever-evolving cyber threats, dynamic landscape of defensive tooling, and vulnerability management practices. To best address these challenges, Texas organizations must first understand their current risks and cybersecurity capabilities. Then, organizations can determine how to securely integrate new and evolving technology into their operations.

Strategies

Texas government entities should:

- Adopt an effective risk-based vulnerability management approach by understanding what must be protected and quantifying the risk of that information being compromised.
- Implement consistent security categorization of systems and data classification.
- Apply zero trust principles where feasible.
- Collaborate and communicate with other Texas entities to support a whole-of-state approach to cybersecurity.

Outcomes

- Increased commitment to data classification and a better understanding of an organization's cyber risks.
- Improved systems protection and threat identification.
- Fully developed risk-based vulnerability management programs.

DIR Initiatives

Texas Risk and Authorization Management Program

Government Code Section 2054.0593 requires DIR to “establish a state risk and authorization management program to provide a standardized approach for security assessment, authorization, and continuous monitoring of cloud computing services that process the data of a state agency.” In support of this legislative initiative, DIR established the Texas Risk and Authorization Management Program (TX-RAMP). This program aims to reduce the risk of using third-party cloud services through assessing the security practices of the cloud service provider.

Endpoint Detection and Response Program

DIR’s endpoint detection and response (EDR) solution provides around-the-clock management of real-time continuous monitoring with rules-based automated response and analysis capabilities. DIR’s EDR solution covers mobile devices, workstations, laptops, and physical and virtual servers. The program is currently monitoring and protecting over 100,000 computing devices and has thwarted nearly 50,000 cyber threats. DIR's EDR solution is available to state agencies at no cost through DIR’s Managed Security Services (MSS).

Assessment Services

DIR funds comprehensive security assessments, penetration tests, and web application vulnerability scans to state agencies, institutions of higher education, and public junior colleges. These services gauge the maturity of an organization’s security programs, providing insights into the strengths and weaknesses that help management prioritize security budgets and resources. DIR shares test results with the assessed organization’s staff to facilitate remediation. Non-state entities may purchase assessment services and other incident response services through MSS.

DIR Initiatives

State and Local Cybersecurity Grant Program

The State and Local Cybersecurity Grant Program (SLCGP) is a component of the federal Infrastructure Investment and Jobs Act, which appropriated $1 billion over four years (fiscal years 2022-2025) to address cybersecurity risks and cybersecurity threats to information systems owned or operated by—or on behalf of—state, local, and tribal governments. Texas was allocated approximately $40 million over four years (excluding a required funding match), which the state will award to local governments to implement one-time cybersecurity services.

74%

74% of breaches involved the human element,
which includes social engineering attacks, errors or misuse.

83%

83% of breaches involved external actors—
with the majority being financially motivated.

Source: verizon.com/dbir

Goal 2: Governance

Strengthen Texas' cybersecurity governance capabilities.

Overview

Effective governance is a crucial facet of any organization, particularly when it comes to cybersecurity. Because it provides a structured framework for managing and mitigating risk, effective governance ensures that Texas' information assets are protected in a consistent and comprehensive manner that aligns with both state and federal regulations. Furthermore, effective governance promotes accountability, transparency, and trust, which are essential for maintaining public confidence. By considering how it governs cybersecurity, Texas can execute strategic decision-making while ensuring cybersecurity initiatives align with the state's overall objectives and priorities. Ultimately, effective governance is key to ensuring the integrity, confidentiality, and availability of Texas' information assets, thereby safeguarding the state's operations, reputation, and public trust.

Challenge

Cybersecurity policies can be complex, challenging to understand, and even harder to accurately interpret. Balancing multiple audit and compliance requirements with daily operations, which often involve intricate and time-consuming processes, can be demanding for Texas organizations. Organizations can address this challenge by engaging—and soliciting feedback from—key stakeholders with mature cybersecurity programs to assist with understanding and developing cybersecurity policies.

Strategies

Texas government entities should:

- Elevate cybersecurity as an essential function of government.
- Identify stakeholders and establish formal governance groups to develop guidance on evolving requirements to better inform and enable effective risk decision making.
- Develop actionable, meaningful, and relevant metrics to effectively monitor progress in improving cybersecurity maturity.
- Ensure executives and business units are accountable for cybersecurity risk.
- Educate data owners on risk, governance, and effective security control implementation and monitoring.
- Contribute expertise and best practices by participating in statewide and national governance initiatives.
- Establish rules and ethical boundaries around the use of emerging technologies, including artificial intelligence (AI) and quantum computing.

Outcomes

- Improved understanding of the given risks of an organization's digital assets and compliance with cybersecurity laws and regulations, leading to an increased level of accountability, ownership, and resource allocation.
- Enhanced collaboration among stakeholders within the information security community.

DIR Initiatives

Statewide Portal for Enterprise Cybersecurity Threat, Risk, and Incident Management

To help tie together the overall state security program, DIR has implemented a governance, risk, and compliance software tool available to all state agencies and institutions of higher education at no cost. The Statewide Portal for Enterprise Cybersecurity Threat, Risk, and Incident Management (SPECTRIM) provides incident management and analysis, policy management, risk assessment analysis, and security plan preparation.

Texas Statewide Information Security Advisory Committee

DIR leads the State Information Security Advisory Committee (SISAC), which includes state and local government information security professionals that collaborate to share ideas and best practices and make recommendations to DIR for more effective information security operations among and within government entities. SISAC provides input regarding the baseline information security standards and statewide policies and guidance. DIR and SISAC members created sub-committees to study and provide guidance on specific topics, including education and communication, policy, and threat intelligence.

Texas Cybersecurity Council

The Texas Legislature created the Texas Cybersecurity Council to develop enduring partnerships between private industry and public sector organizations, ensure that critical infrastructure and sensitive information are protected, facilitate a cybersecurity workforce to protect technology resources from increasing threats, and devise strategies and solutions that ensure that Texas continues to lead in areas of cybersecurity.

DIR Initiatives

InfoSec Academy

The InfoSec Academy provides training for cybersecurity staff from state agencies and institutions of higher education to grant skills for increasing the security of both their respective organizations and the state. Interested participants must receive approval from their organization's CISO/ISO before registration and should be employed in positions related to cybersecurity. DIR also requires that all participants complete the Texas Policy and Assurance course, which is updated every two to three years with the latest security, information technology, and legislative changes. The InfoSec Academy strengthens the state's cybersecurity posture and is an essential function of government.

25%

CISOs are beginning to get the institutional support they need. 25% of state CISOs report they have legislation/statute established and funded for a cybersecurity legislative council or equivalent to do a periodic review and steer the state's cybersecurity posture and allocate funding.

Source: 2022 Deloitte-NASCIO Cybersecurity Study

Goal 3: Education

Build a culture around cybersecurity awareness.

Overview

Embedding cybersecurity into Texas' culture is an ongoing process that requires commitment and engagement from all levels of Texas government. Promoting a shared responsibility for cybersecurity by providing comprehensive policies, protocols, training, and communications will strengthen Texas organizations and improve the security of Texans.

Challenge

Meeting the ongoing and ever-increasing security challenges facing the state will require Texas to equip employees with the skills and knowledge to understand cybersecurity risks, including the best ways to avoid those risks and limit their impact to Texas organizations.

Strategies

Texas government entities should:

- Develop comprehensive cybersecurity policies that outline the acceptable use of technology, password management, data handling, and reporting procedures, making it easy for people to understand security requirements.
- Ensure the organization's leadership is informed of cybersecurity's importance, encourage them to prioritize cybersecurity, and establish channels for communications on cybersecurity-related topics and updates.
- Educate users and the public about cybersecurity awareness through diverse, updated training with various delivery methods.
- Build and develop partnerships with public and private sector entities to encourage customers and employees to stay informed about emerging cyber threats, new security measures, and end-user best practices.
- Find and offer access to relevant training opportunities that include up-to-date and tailored content to meet specific organizational objectives.
- Incorporate a broader variety of training delivery methods such as interactive games, scenario-based learning, simulations, and workshops.
- Regularly assess the effectiveness of cybersecurity awareness programs and training efforts by gathering feedback from customers, conducting surveys, tracking progress, and measuring the impact of training initiatives.

Outcomes

- A well-trained workforce that stays current on best practices in cybersecurity, which, in turn, encourages employees to promptly report potential security breaches without fear of blame or retribution.
- Enhanced statewide cybersecurity awareness, leading to an increased level of security over Texans' data.
- Reduced risk of compromise due to lack of employee awareness or carelessness.

DIR Initiatives

Cybersecurity Awareness and Education

As a statewide leader in information resources security, DIR provides education and support at no cost to state agencies, institutions of higher education, and local governments through a variety of methods, such as offering end-user security awareness training, providing access to technical research and advisory services, hosting educational webinars and events, and organizing Cybersecurity Awareness Month activities.

Information Security Forum

The Information Security Forum (ISF) is an annual educational conference bringing together security and IT professionals from public sector organizations across the state of Texas. This premier conference—which state and local government employees are eligible to attend at no cost—focuses on cybersecurity trends and current issues.

Texas Information Sharing and Analysis Organization

DIR created the Texas Information Sharing and Analysis Organization (TX-ISAO) to provide a forum for Texas entities to share information regarding cybersecurity threats, best practices, and remediation strategies. The TX-ISAO is open at no cost to any organization in Texas, including state agencies, local governments, public and private institutions of higher education, and the private sector. The TX-ISAO provides access to intelligence and educational opportunities and allows members to participate in real-time information sharing.

67%

67% percent of state agency CISOs polled reported security awareness as a "most adopted" security service. In contrast, less than half of CISOs provide cybersecurity training to local government and public higher education staff.

Source: 2022 Deloitte-NASCIO Cybersecurity Study

Goal 4: Resilience

Maintain continuous business critical operations when responding to—and recovering from—cyberattacks.

Overview

As technology increasingly permeates many aspects of modern life and significantly influences the way governments engage with the public, organizational resilience becomes proportionately paramount. Empowering Texas organizations to proactively plan for, recover from, adapt to, and withstand disruptive cybersecurity incidents is essential for Texas' long- and short-term technology and business goals. A comprehensive approach to enhancing cybersecurity response and recovery capabilities will bolster the state's ability to serve Texans and maintain essential services, even in the face of debilitating cyberattacks. Furthermore, adequate planning, training, and relationship management will ensure that Texas organizations are resilient and able to continue business operations when impacted by a cybersecurity incident.

Challenge

Developing contingency plans, including business continuity and disaster recovery plans, can minimize the impact of disruptions and facilitate swift restoration of operations. Government entities must have the ability to continuously deliver services to the public and employees while managing and responding to cybersecurity incidents, making cybersecurity an essential function of government organizations. Additionally, vulnerability management presents a significant challenge.

Two primary challenges inhibit creating a resilient organization. The first is dedicating the time, resources, and effort to develop truly comprehensive, adaptable, and resilient contingency plans that are unique to an organization and work when needed. The second primary challenge is dedicating the time, resources, and effort into ensuring that the business continuity plan remains consistently tested and updated on a regular basis. Additionally, reducing the attack surface through a comprehensive vulnerability management program is necessary to help organizations limit potential attack points and more quickly and effectively identify root causes.

Strategies

Texas government entities should:

- Build resilience by identifying and developing plans to prepare organizations to re-establish essential functions in the event of a cyber disruption.
- Promptly identify the cybersecurity risks of—and subsequently address—cybersecurity vulnerabilities.
- Consistently apply good cybersecurity hygiene practices.
- Emphasize a risk-based approach that optimizes vulnerability management and ensures the highest level of security while prioritizing vulnerabilities based on the potential impact and likelihood of exploitation, ensuring that resources target the most critical threats first.
- Implement corrective actions identified from past cybersecurity incidents and exercises.
- Integrate real-time threat intelligence, understand their organization's unique risk profile, and leverage advanced analytics to make proactive, informed decisions about patching, mitigation, and remediation.
- Utilize third-party risk management strategies and solutions.

Outcomes

- Texas organizations that can proactively manage vulnerabilities and risks while reducing operational costs and ensuring the continuity of critical business operations.
- A tested disaster recovery plan for Texas organizations that ensures business continuity and has established service baselines.
- Identified essential functions of Texas organizations that are resilient during a cyber incident.
- A statewide and cross-functional culture of preparedness that reduces cybersecurity incident impacts and improves response time to address critical cybersecurity incidents.
- Cybersecurity professionals have access to the tools they need to maintain cybersecurity baselines and meet business objectives while successfully mitigating risks.

DIR Initiatives

Third-Party Risk Management Tools

To implement vulnerability management, DIR utilizes specialized third-party tools to enhance proactive identification, assessment, and remediation of potential security vulnerabilities. These tools offer a comprehensive and streamlined approach that facilitates efficient vulnerability detection, risk prioritization, and mitigation strategies.

Texas Volunteer Incident Response Team

The Texas Volunteer Incident Response Team (VIRT) comprises experienced volunteers who can quickly respond to significant cybersecurity incidents and provide support to eligible participating entities, including Texas agencies, institutions of higher education, and local government organizations. Under DIR’s direction, VIRT volunteers provide support to participating entities in coordination with other state level response resources. VIRT volunteers must pass a background check and sign a confidentiality agreement before activation. The VIRT may be activated in response to a Governor-declared disaster for a cybersecurity incident or when multiple participating entities request incident response support.

DIR Initiatives

Cybersecurity Incident Response Team

DIR's Cybersecurity Incident Response Team (CIRT) aims to safeguard critical assets of the state by sharing threat intelligence and providing incident response support to eligible organizations, including onsite and remote security incident management support. The CIRT offers various cybersecurity preparedness activities—such as tabletop exercises and incident response training—to enhance Texas organization readiness. Furthermore, the CIRT offers computer forensics and analysis services to investigate incidents effectively.

Cyber Operations at the Network Security Operations Center

DIR Cyber Operations, based at the Network Security Operations Center (NSOC), offers critical support to state agencies, customers of the state data center, and eligible partners by facilitating internet access through DIR. Operating around-the-clock, DIR Cyber Operations provides a comprehensive range of services, including IP and domain name blocking, vigilant monitoring and prompt alerting for suspicious activities, expert incident response guidance and support, intelligence gathering, and information sharing. Additionally, DIR Cyber Operations oversees Data Center Services security operations and is equipped with distributed denial-of-service (DDoS) attack detection and mitigation capabilities.

Local Government Incident Response Reporting

Local government entities in Texas are now required to report cybersecurity incidents to DIR. After discovering a cybersecurity incident, local government entities have 48 hours to submit an initial incident report to DIR. Within 10 days of recovering from the incident, the impacted entity must report an analysis of the cause of the incident. Reporting incidents to DIR gives the state a more comprehensive view of the cyber threat landscape in Texas. Additionally, DIR continues to share anonymized threat intelligence with members of the TX-ISAO, which can help prevent additional attacks.

DIR Initiatives

Statewide Incident Response Preparedness

DIR maintains the Statewide Cybersecurity Incident Response Plan, which outlines the method and tactics Texas will take to respond to a statewide cybersecurity incident. DIR also leads the Statewide Incident Response Working Group, a collaboration among multiple state agencies that facilitates a whole-of-state approach when responding to significant cybersecurity incidents.

State-Level Cybersecurity Exercises

To maintain a high level of readiness, the state leads and participates in several cybersecurity incident response exercises annually. DIR also participates in national-level cybersecurity exercises, including an internationally sponsored multi-day exercise by the Cybersecurity and Infrastructure Security Agency (CISA) that is conducted in even-numbered years. The primary objective of this CISA-sponsored exercise is to assess the efficacy of existing incident response procedures. In odd-numbered years, DIR develops and conducts state-level exercises that focus on exploring and evaluating novel processes, procedures, and capabilities to enhance the state's cybersecurity readiness.

70%

By 2025, 70% of CEO's will mandate a culture of organizational resilience to survive coinciding threats from cybercrime, severe weather events, civil unrest and political instabilities.

Source: Olyaei, Sam & Isaka, Oscar (2022, December). The Gartner Top Cybersecurity Predictions of 2023 [Webinar]. Gartner, Inc.

Goal 5: Workforce Development

Establish programs to support and develop cybersecurity professionals.

Overview

To ensure a talented, strong, and robust workforce for the future, Texas should have programs in place to identify, train, and develop cybersecurity talent. Partnerships between state and local government organizations, universities, school districts, and junior colleges are key to developing programs that build, retain, and recruit the talent needed for the future.

Challenge

The shortage of qualified and skilled cybersecurity professionals underscores the necessity for programs that attract and retain talent. Effectively addressing these challenges requires focused efforts to enhance recruitment strategies, promote cybersecurity as an appealing career path, and allocate ample resources to cultivate a resilient and proficient cybersecurity workforce.

Strategies

Texas government entities should:

- Dedicate additional funding to cybersecurity positions.
- Partner with K-12 and higher education organizations to develop innovative workforce training and internship opportunities for future cybersecurity professionals.
- Develop programs to upskill existing government employees and fill vacant cybersecurity roles.

Outcomes

- An increase in qualified cybersecurity professionals to fill open positions.
- An increase in training and educational opportunities for potential and existing employees in the cybersecurity workforce.
- An increase in interest in cybersecurity as a career path among Texas students.

DIR Initiatives

Regional Security Operations Center Expansion

DIR established the state's pilot Regional Security Operations Center (RSOC) in April 2022 through a partnership with Angelo State University. To expand its reach and capabilities, DIR will be partnering with the University of Texas at Austin and the University of Texas Rio Grande Valley to establish RSOCs in two new locations. These RSOCs employ, educate, and increase the cybersecurity skills of college students (who work under trained cybersecurity professionals) while providing threat research, monitoring, and mitigation services for customers. DIR, through the RSOCs, can help secure local government entities such as cities, counties, and independent school districts from cyber threat actors while concurrently increasing the quality and quantity of cybersecurity analysts in Texas.

InfoSec Academy

The Texas InfoSec Academy provides industry-standard cybersecurity certification preparation and application developer courses. These industry-standard resources include exam certification vouchers for all courses for information technology staff at no cost to state agencies and public institutions of higher education, including public community colleges. Participant enrollment in a course will require the approval of the registrant's Information Security Officer and is subject to certain limitations. DIR covers the costs of these courses and certifications for the state of Texas. DIR highly encourages staff seeking to expand their skills in protecting the security of the State of Texas and its entities to take advantage of this free resource. In addition to the training offered, DIR created a Texas Policy and Assurance Course, which is designed to prepare security staff to apply state rules regarding information security within state agencies or institutions of higher education.

DIR Initiatives

Internship Program

DIR’s internship program provides college students with experiential learning opportunities for earning college credit and gaining practical experience in a profession related to their college degree plan and career interests. DIR interns learn new skills, get exposure to different work environments, and receive mentorship and guidance from professionals within the agency. DIR’s goal with the internship program is to create a positive learning experience, instill a sense of belonging, and prepare interns for full-time employment, perhaps at DIR or another state agency.

Veteran Hiring

DIR is committed to the successful reentry of military veterans into the civilian workforce and employment. Values instilled in military service members—such as adaptability, courage, teamwork, strong work ethic, emotional intelligence, and reliability—closely align with DIR’s I LEAD Core Values (Innovation, Leadership, Ethical, Accountable, and Delivery). Military service members also possess a wide variety of cross-functional skills, have undergone advanced technical training, and are adept at working with new and emerging technologies. Because of these values, skills, and training, military veterans are highly sought after candidates for DIR positions. Military veterans, therefore, are uniquely qualified to serve the Texas government and help DIR achieve its mission of leading the state’s technology strategy, protecting state technology infrastructure, and transforming how Texas government serves Texans.

50%

50% of state CISOs report inadequate availability of cybersecurity professionals as a top barrier to address cybersecurity challenges.

Source: 2022 Deloitte-NASCIO Cybersecurity Study

Acknowledgements

Texas Cybersecurity Strategic Plan Committee

Daniel Owen, Texas State University

David Boyd, Texas Comptroller of Public Accounts

Melinda Dade, Texas Education Agency

Danny Miller, Texas A&M University System

Dale Harville, Education Service Center, Region 20

Shamika Fehr, Texas Secretary of State

Fernando De Velasco, Prosper Independent School District

Tony Gonzalez, City of New Braunfels

Michael Peters, Panhandle Regional Planning Commission

Kurt French, Texas Department of Public Safety

Texas Department of Information Resources

300 West 15th St., Suite 300, Austin, TX 78701
1-855-ASK-DIR1 | dir.texas.gov | @TexasDIR | #DIRisIT