CYBERSECURITY PROGRAMS AT THE DEPARTMENT OF INFORMATION RESOURCES

AN ISSUE BRIEF FROM LEGISLATIVE BUDGET BOARD STAFF

LEGISLATIVE BUDGET BOARD ID: 7456 NOVEMBER 2024

The Texas Government Code, Chapter 2054, requires the **Department of Information Resources** (DIR) to develop a framework for securing the state's cyberinfrastructure, perform risk assessments, and plan for mitigation activities. Additionally, DIR must maintain a repository for information regarding the protection of state agency information, provide cybersecurity training and assistance to state agencies, and promote public awareness of cybersecurity issues. Historically, DIR's security services primarily involved establishing statewide policy, rules, and guidelines, and providing security for the operation of other services, such as the Texas Agency Network and data center services. In recent years, however, DIR's security-related programs and services have expanded to confront the increasing threat posed by cyber criminals. Appropriations for DIR have increased to facilitate additional programs, and DIR now receives funding for regional security operations centers and direct security services provided for agencies, such as endpoint detection and response and multifactor authentication.

KEY LEGISLATIVE CHANGES

Senate Bill 271, Eighty-eighth Legislature, Regular Session, 2023, establishes consistency among state and local entities regarding the required reporting of security incidents. The legislation requires city and county governments to report to DIR, in the same manner as state entities, a data breach or ransomware attack within 48.0 hours of its occurrence. The legislation also broadens the scope of incidents that must be reported to include cyberattacks in which data is not breached, such as a distributed denial of service attack.

Senate Bill 475, Eighty-seventh Legislature, Regular Session, 2021, fortified the state's standards regarding agencies' data management practices, storage, and Texas' ability to respond to cybersecurity incidents. The legislation also established several programs, including the Texas Risk Authorization and Management Program (TX-RAMP), Texas Volunteer Incident Response Teams (VIRT), regional cybersecurity working groups, and regional security operations centers (RSOC).

ROLES AND RESPONSIBILITIES

The Texas Government Code, 2059.056, specifies that DIR is responsible for network security from external threats, and agencies are responsible for network security management regarding internal threats. Other agency responsibilities include developing and enforcing internal security policies regarding application patches, internal scans, and access control. Agencies also must oversee the building and support of their devices, such as computers and mobile phones. Agencies also are responsible for their own connectivity and isolation of their local area networks. Agencies have ownership of the data stored on the state servers, and DIR does not determine regulatory or security requirements of agency-specific data. Agencies must inform DIR regarding security necessities and confidentiality requirements for medical, criminal, or any other type of personally identifiable information stored on the state data centers or shared cloud environment. DIR then will build the necessary security structures. Additionally, statute requires state and local entities, including agencies, school districts, and institutions of higher education, to report security incidents to DIR and the state's chief information security officer.

DIR and agencies share some responsibilities, including information sharing and training. DIR and the Texas Cybersecurity Council offer several tools and resources, including some at no cost. Agencies are responsible for participating in these offerings and implementing best practices. Agencies may implement their own training materials, such as phishing campaigns that test employees' reactions to high-risk emails. Additionally, all state entities must adhere to state and national standards for policy development pursuant to the Texas Administrative Code, Title 1, Part 10, Chapter 202.

DIR's responsibilities include providing security services directly to customer agencies, institutions of higher education, and certain local government entities. Additionally, DIR maintains the state data centers and protects them from external threats. DIR also assists the Legislature in developing policy intended to mitigate

cybersecurity-related risks and trains and educates state employees and the public regarding cybersecurity best practices.

SECURITY SERVICES

DIR's bill pattern in the Eighty-eighth Legislature, General Appropriations Act (GAA), 2024–25 Biennium, distributes the function of cybersecurity into two strategies. Strategy C.1.2, Security Services, outlines most of DIR's cybersecurity responsibilities and receives 97.0 percent of the total cybersecurity funding, The strategy encompasses the agency's operations and infrastructure related to cybersecurity, including the Network Security Operations Center (NSOC), the RSOCs, multifactor authentication, endpoint detection and response (EDR), and VIRT.

The NSOC provides monitoring, alerts, countermeasures, and incident response for customers using the DIR network and state data centers. Agencies or other data center customers of DIR's Shared Technology Services may receive managed security services, which include cybersecurity operations within three key areas: security monitoring and device management; incident response services; and risk and compliance services. The security monitoring and device management area provides continuous detection and threat blocking and assists agencies to establish or augment their own security operations centers. The incident response services area identifies the causes of attacks and guides customers regarding how to avoid future attacks. During a cyberattack, the service provider coordinates with staff that specialize in legal processes, information technology (IT), business processes, and risk management to provide response services including detection, triage, and containment. The risk and compliance services area provides insights and metrics to help an organization defend itself, identifies vulnerabilities, and recommends practices to mitigate breaches of security.

Senate Bill 475, Eighty-seventh Legislature, Regular Session, 2021, funded new cybersecurity programs and enhancements. The legislation established RSOCs to offer regional infrastructure and support for local governments by installing security operations centers at state universities. The first center was established at San Angelo State University after a ransomware attack affected 23 local governments in August 2019. The 2024–25 GAA appropriates $11.0 million to DIR to establish two centers at the University of Texas (UT) at Austin and UT Rio Grande Valley.

Multifactor authentication is a security enhancement that requires users to provide additional information when logging into a digital resource. This information could include requiring the user to enter a verification code that is sent to a mobile device or to answer a security question correctly.

EDR is a security solution that provides continuous monitoring of end-user devices, including state-owned computers and mobile devices, for incoming indications of a known type of security breach. A breach will initiate an automated response such as logging a user off from a device or sending alerts to a response team.

SECURITY POLICY AND AWARENESS

Another cybersecurity strategy in DIR's bill pattern is C.1.1, Security Policy and Awareness, which encompasses education and outreach and promotes the development of industry standards and policies that help protect organizations across the state.

The Texas Administrative Code, Title 1, Part 10, Chapter 202, establishes minimum information and cybersecurity responsibilities to which all programs or projects at any agency or institution of higher education must adhere. These rules require agencies and institutions to use DIR's Security Control Standards Catalog to implement security controls that align with the U.S. Department of Commerce's National Institute of Standards and Technology. DIR's catalog provides state entities with specific minimum baselines for required information security controls. Each entity may apply additional controls in situations that require enhanced security.

The Texas Government Code, Section 2054.0593, requires DIR to establish a program regarding risk and authorization management to provide a standardized approach for security assessment, authorization, and continuous monitoring of cloud-based computing services that process a state agency's data. The statute also requires DIR to prescribe categories and characteristics of cloud-based services that are subject to the program. Pursuant to this requirement, DIR established TX-RAMP to assess the security strength of these cloud-based products. The Texas Administrative Code, Chapter 202, also requires these products to be certified through TX-RAMP before agencies may contract with the providers. Previously, agencies verified products according to their own standards. TX-RAMP sets criteria for consistent standards across the state. As of October 2024, TX-RAMP had certified 2,060 products.

The Texas Government Code, Section 2054.512, requires the Texas Cybersecurity Council to establish criteria and best practices for addressing security threats, assess the capabilities of the current cybersecurity workforce to address deficiencies and ensure a long-term pool of qualified applicants, and consider establishing an emergency-readiness team to address cyberattacks. The council collaborates with DIR to certify training programs for state employees, government officials, and contractors. These programs are delivered by school districts, universities, state agencies, IT providers, and DIR's InfoSec Academy. DIR's cybersecurity coordinator leads the Texas Information Sharing and Analysis Organization (TxISAO), which was established pursuant to the Texas Government Code, Section 2054.0594, to provide a forum for state and local entities, institutions of higher education, and the private sector to share information regarding cybersecurity threats, best practices, and remediation strategies. TxISAO analyzes trends and makes recommendations, providing more than 1,500 members access to industry-specific cyberintelligence.

FUNDING

DIR's funding differs from that of most state agencies because key programs are funded primarily through administrative fees as cost recovery. General Revenue Funds are appropriated to DIR solely for security services. DIR also may use revenues greater than specified limits from administrative fees assessed for telecommunications services or the Cooperative Contracts program toward cybersecurity activities in lieu of General Revenue Funds. The 2024–25 GAA provides $102.7 million in All Funds to promote efficient security. This amount includes General Revenue Funds allocations of $22.2 million for EDR, $24.8 million for RSOC, and $4.0 million for multifactor authentication. Additionally, the 2024–25 GAA provides $21.7 million in Other Funds for security related to telecommunications services.

CONTACT

Charles Smith Email: IssueBrief@lbb.texas.gov