2022 Cybersecurity Report

November 15, 2022

Texas Department of Information Resources

Transforming How Texas Government Serves Texans

Table of Contents

For the purposes of this report the term cybersecurity event is used interchangeably with the term cybersecurity incident. The National Institute of Standards and Technology (NIST) defines a cybersecurity event as any observable occurrence in a network or system. NIST defines a cybersecurity incident as any action taken using computer networks that results in an actual or potentially adverse effect on an information system and/or the information residing therein. Any cybersecurity incident is a subset of the greater category called a cybersecurity event.

For the purposes of this report, the term "state agency" is generally used to indicate a state agency or a state institution of higher education; and the term "technology" is used to indicate information and communications technologies.

State of Texas Chief Information Security Officer Statement

In 2022, labor and supply chain issues, global conflicts, and economic worries are impacting the cybersecurity risk landscape. In particular, the supply chain issue and labor market tightness mean that organizations often must do more with fewer resources. Over the last two years, Texas faced its own cyber challenges affecting both the public and private sector, such as ransomware attacks and recent nation state cyber threats. During this time when supplier risk and new vulnerabilities are becoming more complex and frequent, security and risk management leaders must focus on balancing adequate protection and business growth.

DIR's 2022 Cybersecurity Report assesses the resources currently available to government entities to respond to cybersecurity incidents, identifies preventive and recovery efforts to improve cybersecurity, evaluates the statewide information security resource sharing program, and provides legislative recommendations for improving cybersecurity.

The 87th Texas Legislature demonstrated a significant interest in improving cybersecurity throughout the state by enacting legislation such as:

- Senate Bill 475, improving cybersecurity standards and data management practices for state agencies and local governments via implementation of certain recommendations and best practices, establishment of a standardized risk and authorization management program, a cybersecurity incident response team, a volunteer incident response team, a regional network security operations center, and prohibition of data usage without written consent;
- Senate Bill 851, requiring the composition of the cybersecurity council to include an employee of the Elections Division of the Office of the Secretary of State;
- Senate Bill 1696, requiring the Texas Education Agency, in coordination with the Texas Department of Information Resources (DIR), to establish and maintain a system to coordinate the anonymous sharing of information concerning cyberattacks or other cybersecurity incidents between participating schools and the state;
- House Bill 1118, requiring local governments applying for law enforcement grants to submit with the grant application a written certification of the local government's compliance with the cybersecurity training required by Government Code 2054.5191, with penalties for noncompliance; and
- House Bill 4018, improving legislative oversight and funding for modernization projects for state agency information resources.

These new laws resulted in several major initiatives for DIR, such as the Texas Risk and Authorization Management Program (TX-RAMP), the DIR Cybersecurity Incident Response Team (CIRT), the statewide Volunteer Incident Response Team (VIRT), and a pilot Regional Security Operations Center (RSOC).

Cybersecurity is everyone's responsibility. As our homes and businesses become more connected, we must all do our part to protect our information resources. By taking the right proactive measures against cyber threats, state government can continue to serve Texans in a reliable, secure, and efficient manner.

-Nancy Rainosek, Texas Chief Information Security Officer
Texas Department of Information Resources

Introduction

Texas Government Code Section 2054.0591 requires the Texas Department of Information Resources (DIR) to produce a report identifying the preventive and recovery efforts the state can undertake to improve cybersecurity.

The considerations presented in this report can be applied to various impacts of cybersecurity risks, threats, and possible incidents. This report, as required by Texas Government Code, includes:

- An assessment of available resources to address the impacts of cybersecurity incidents;
- Recommended preventive and recovery efforts;
- An evaluation of a shared information security resource assistance program;
- A review of existing cybersecurity-related statutes; and
- Legislative recommendations to protect the state against adverse impacts of cybersecurity incidents.

In 2022, cybersecurity incidents across the United States are increasing in volume, velocity, and variety. For example:

- The 2022 Verizon Data Breach Investigation Report found that ransomware remains a dominant threat to systems and data, continuing its upward trend with an almost 13% increase, for a total of 25% of data breaches in 2021 – a rise as big as the last five years combined.
- A 50% increase in live, hands-on intrusion activity was observed year-over-year, according to the Crowdstrike Falcon 2022 Threat Hunting Report.
- Proofpoint's 2022 Social Engineering Report found social engineering to be involved with the overwhelming majority of cyberattacks, with 82% of breaches including the human element in 2021.

Taken together, these statistics show an alarming increase, not only in cybersecurity threats, but also in the rate that these events are increasing every year.

Although the increasing volume of threats poses a substantial challenge, there are many best practices Texas state agencies can implement to lessen the likelihood of successful attacks and mitigate the impact of cybersecurity incidents. For example, by providing employees ongoing security awareness training about attack methods, personnel will be more vigilant, aware, and less likely to open the door for malicious actors. By testing backups and simulating incident response capabilities, agencies can incorporate lessons learned from these simulations into incident response plans and be more prepared for the real thing.

Report Highlights

This report highlights resources and best practices to better prepare the State of Texas for future cyberattacks:

- Having an incident response plan to address the fundamental aspects of roles, responsibilities, and resources is crucial to an expedient and successful response to cyber events; yet of the Texas state agencies that have an incident response plan, 37% do not have a defined exercise schedule to test and potentially improve their incident response capability.
- Educating users and applying protections against cyber threats can help greatly reduce risk, but compliance with statewide cybersecurity awareness training can be improved. The 2022 Verizon Data Breach Investigations Report notes that 82% of breaches included the human element. In FY 2022, 91% of state entities and 33% of local government entities in Texas complied with state mandated cybersecurity awareness training. This is down from 95% of state entities and 36% of local government entities reporting compliance in FY 2021.
- Only 33% of state agencies reported having more than one dedicated information security personnel and 76% of agency designated information security officers have job responsibilities outside of information security, resulting in limited resources and depth of knowledge and skills to build and maintain effective information security programs.
- Local governments often face challenges relating to aging infrastructure, lack of qualified security personnel, and strict budgets that leave their information assets vulnerable. These entities have also been associated with an increasing number of ransomware incidents over the last several years.

Legislative Recommendations

- **Adoption of .gov Domain**: Require government entities to adopt the standardized ".gov" domain suffix before establishing a new domain name to reduce website spoofing.
- **Local Government Incident Reporting**: While state agencies are required to report cybersecurity incidents to the state through DIR, local government entities are not. Requiring local entities to report these incidents to DIR will improve transparency surrounding the threat landscape in Texas and strengthen the state's ability to defend against attacks. DIR recommends that those entities also be required to report these incidents to the state.
- **Cybersecurity Disaster Response:** Currently, the State of Texas Cybersecurity Emergency Support Function (ESF) designates the DIR and TDEM as the primary entities to assist in this planning effort for a cybersecurity disaster. DIR oversees incident response efforts and the Volunteer Incident Response Team (VIRT) for cybersecurity disasters. Codifying the ESF would bring clarity to roles during a cybersecurity disaster particularly as DIR oversees the VIRT and would lead the VIRT's response during a cybersecurity disaster.
- **Prohibit Ransomware Payments:** Cyber criminals use ransomware to encrypt systems and often demand a large financial payment to release those systems. Paying the ransom incentivizes the use of ransomware and funds criminal organizations. Texas should take a stand against ransomware and prohibit public entities from paying or authorizing payments for ransomware.

Resource Assessment

Agency Resources

The State of Texas is an intriguing target for malicious actors due to the sheer number of public sector information assets that house sensitive and confidential information. Over 200 state organizations and thousands of local governments organizations make Texas a target-rich environment.

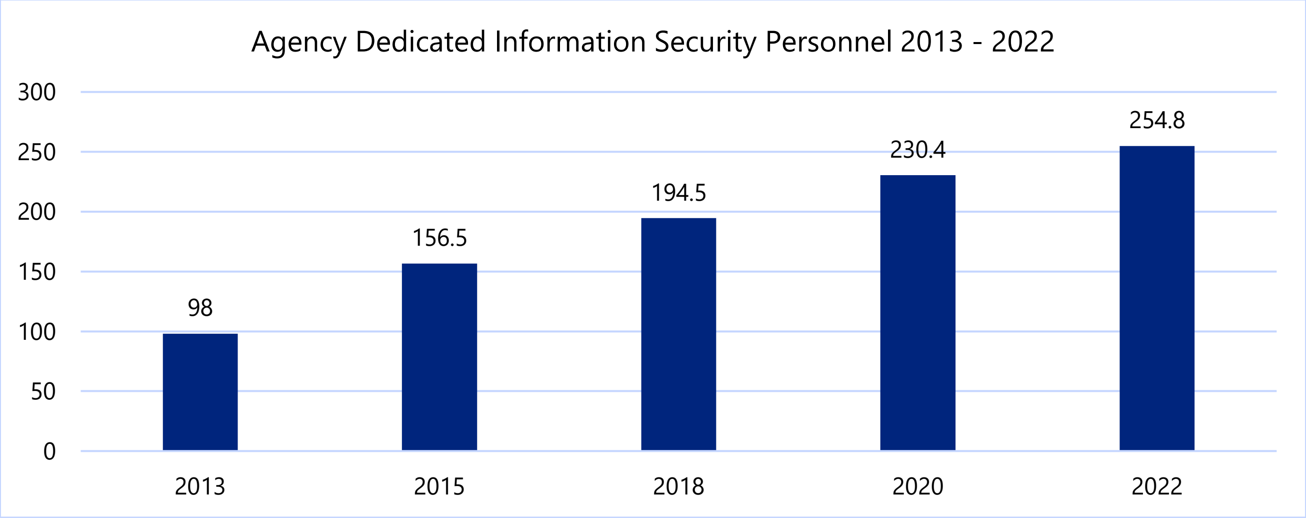
To compound the issue, state entities must balance competing priorities and resources, which can create challenges in sufficiently preparing to address the impacts of cybersecurity incidents. This section provides an overview of how agency personnel and resources support cybersecurity operations across state government.

Agency Cybersecurity Resources

When surveyed, state agencies indicate dedication and commitment to ensuring the security of their information systems. Data show an increase in cybersecurity budgets and personnel year-over-year. As the state's adversaries grow more sophisticated, so does the need for sophisticated defensive capabilities, which require experienced and skilled personnel to operate security tools, investigate suspected issues, and effectively respond to incidents in a timely manner.

The 2022 Information Resources Deployment Review (IRDR), a biennial survey of agency IT implementation, indicated that agencies made cybersecurity a priority as established by the State Strategic Plan for Information Resources Management. The number of fully dedicated security professionals employed by agencies rose 10.6% between 2020 and 2022. While this increase is lower than the 2018 to 2020 change (18.5%), the continued growth suggests an increasing emphasis on information security preparedness and maturity across state agencies.

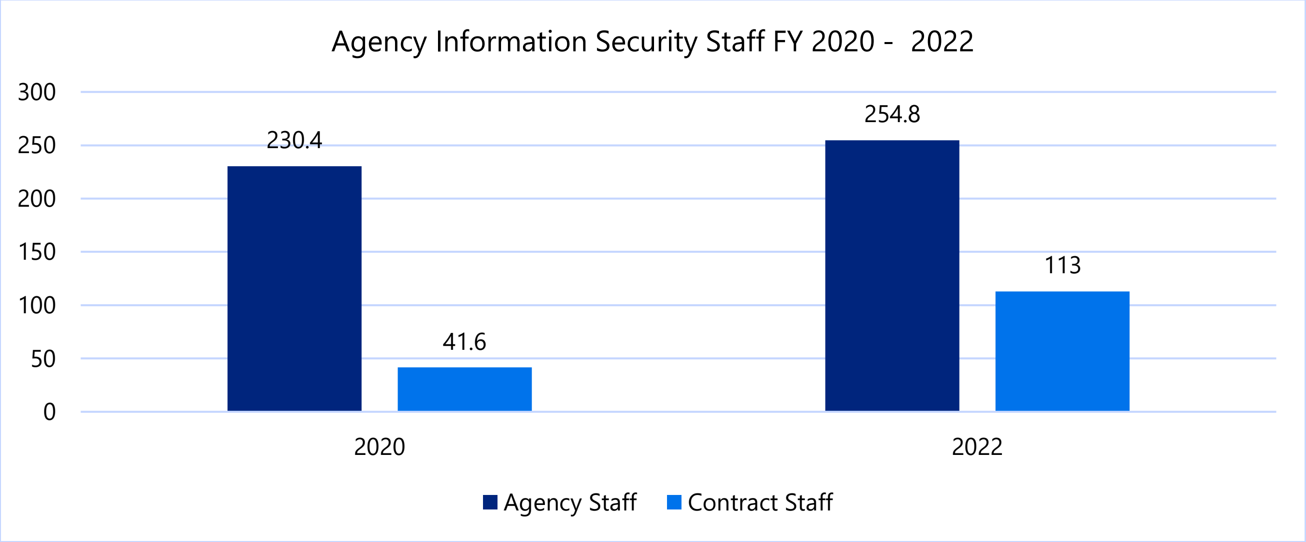
Figure 1: Number of Agency Information Security Personnel 2013-2022



Source: Biennial Information Resources Deployment Review 2013 - 2022

Despite continued growth, the number of agency personnel may not be keeping pace with the growing demand for cybersecurity expertise or resources. In addition to the nearly 255 dedicated agency cybersecurity professionals, agencies reported 113 contractors supporting agency security efforts in 2022.

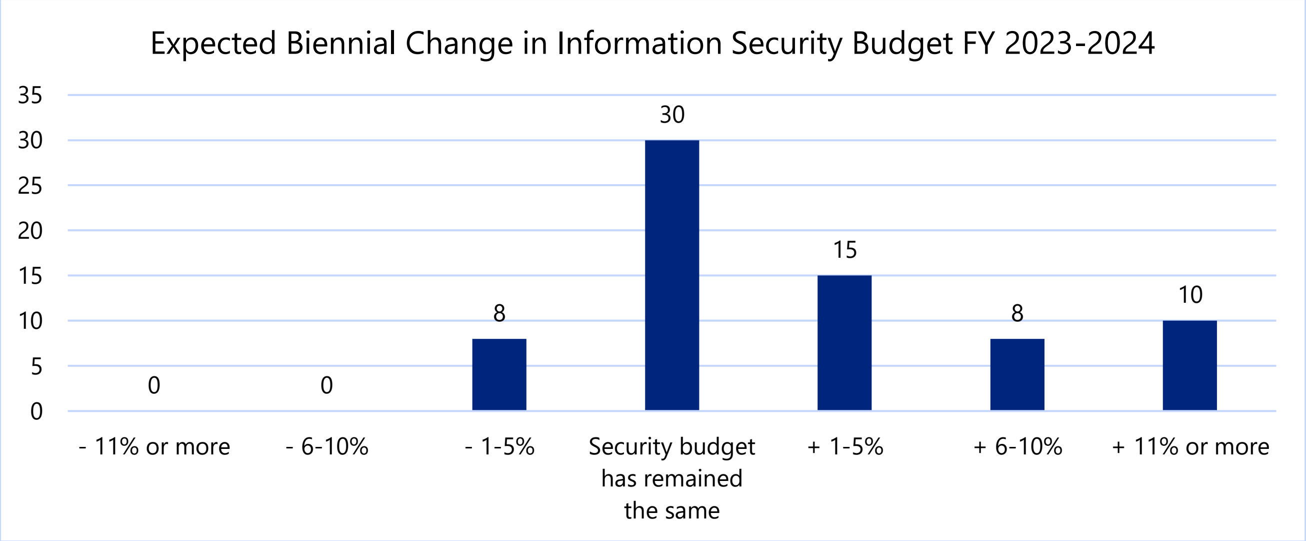
Figure 2: Agency Information Security Staff and Contractors FY 2020-2022



Source: 2022 Information Resources Deployment Review

In addition to an increased number of agency security personnel and contractors, many agencies reported a projected increase in their biennial security budget. In the 2022 IRDR, 33% of agencies plan to increase their security budget from the last biennium. Continued investment in information security is critical to keep pace with the evolving threat landscape.

Figure 3: Expected Biennial Change in Information Security Budget FY 2023-2024



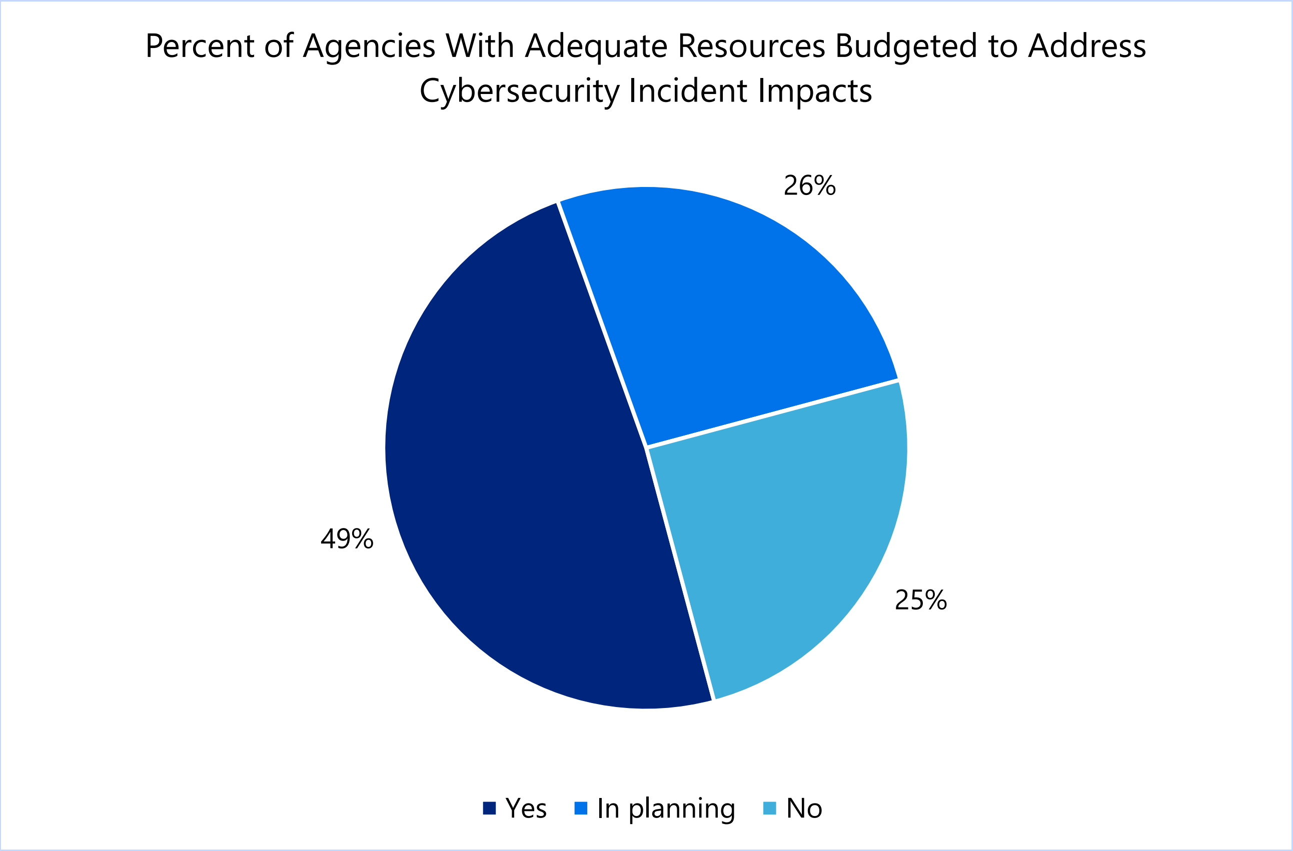
Source: 2022 Information Resources Deployment Review

Agency Cybersecurity Incident Response

In the 2022 IRDR, agencies reported an increased focus on IT security operations, but the majority of agencies report that they do not have adequate resources budgeted to respond effectively to a major cybersecurity incident. Nearly half (49%) of agencies reported specifically budgeting adequate resources to address the operational and financial impacts of a cybersecurity incident. This is an eight percent increase from the 2020 IRDR. Further, 25% of agencies report they do not have adequate resources budgeted, and 26% of agencies are in the planning process to have adequate budgetary resources in place to address a cybersecurity incident.

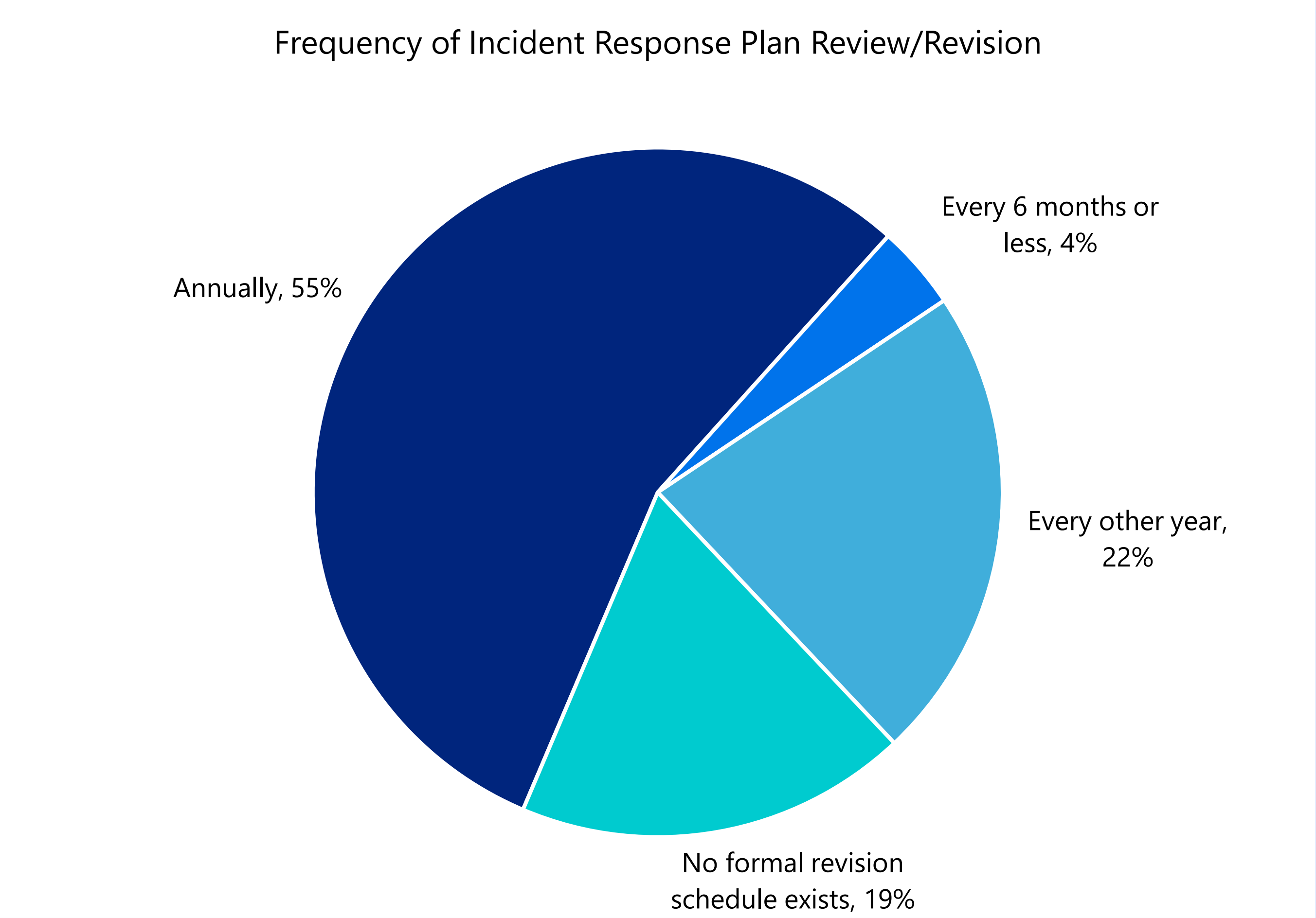
In the 2022 IRDR, agencies reported an increased focus on IT security operations, but most agencies report that they do not have adequate resources budgeted to respond effectively to a major cybersecurity incident. Forty-nine percent (49%) of agencies reported specifically budgeting adequate resources to address the operational and financial impacts of a cybersecurity incident. This is an eight percent increase from the 2020 IRDR. Further, 25% of agencies report they do not have adequate resources budgeted, and 26% of agencies are in the planning process to have adequate budgetary resources in place to address a cybersecurity incident. Incident response planning and review activities are critical to reducing the overall incident costs associated with potential compromises.

Figure 4: Percent of State Agencies with Adequate Resources Budgeted for Cyber Incidents



Source: 2022 Information Resources Deployment Review

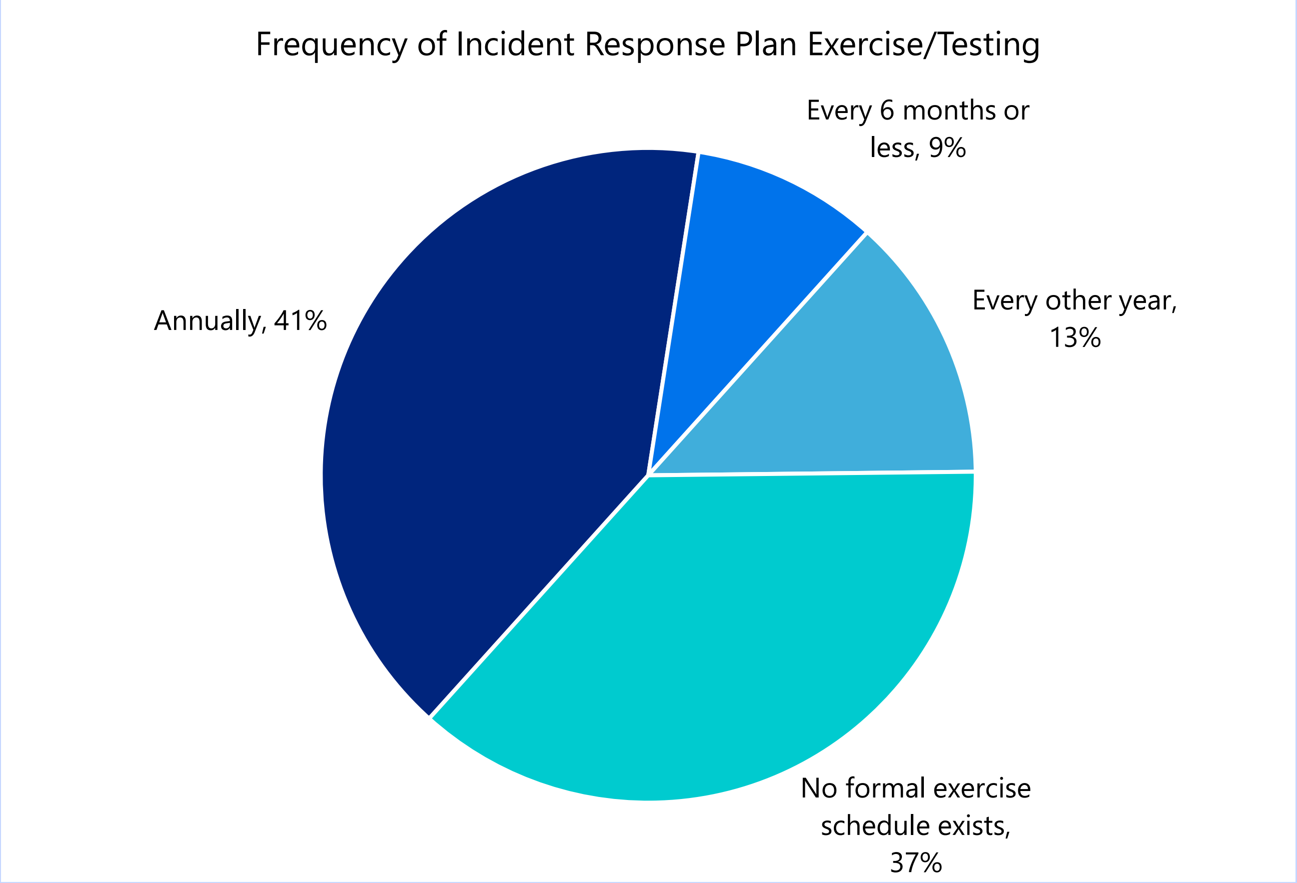
Figure 5: State Agency Incident Response Plan Revision Frequency



Source: 2022 Information Resources Deployment Review

To support a successful response to cybersecurity incidents, agencies need to not only review response plans annually, but agencies also must exercise response plans regularly to realize the full benefits of the planning process. Of the organizations that have an incident response plan, only 63% of agencies reported a defined exercise schedule to test and potentially improve their incident response capability.

Figure 6: State Agency Incident Response Exercise Frequency



Source: 2022 Information Resources Deployment Review

Developing a comprehensive planning, training, and exercise program for each organization's cybersecurity initiatives is a valuable investment to help reduce the impacts of cyber incidents.

State agencies are dedicated to maintaining the security of their information systems. Yet, when incidents do occur, agency resources alone may not be adequate to support incident response activities and agencies may need the assistance of outside resources to support incident response. As noted in *Figure 4: Percent of State Agencies with Adequate Resources Budgeted for Cyber Incidents*, less than half of respondents stated that they had adequate resources budgeted for incident response. DIR, along with other federal and private sector resources, often help fill the gap to support effective and efficient incident response functions.

DIR Resources

DIR provides Texas state and local government organizations access to security resources through multiple programs. These resources enhance the security posture of the state and individual organizations by providing tools and guidance on security topics such as security assessments and testing, incident response, training and education, risk assessments, alerting and monitoring, intelligence gathering, and general best practices. This section provides an overview of the major security resources provided by DIR.

Volunteer Incident Response Team

Government Code 2054.52002 directs DIR to establish the Texas Volunteer Incident Response Team (VIRT) to provide rapid incident response assistance to participating entities impacted by a cybersecurity event.

The Texas VIRT is comprised of volunteers with expertise addressing cybersecurity events that support Texas agencies, institutions of higher education, and local government organizations to respond to significant cybersecurity events. VIRT volunteers serve under the direction of DIR and can use their cybersecurity expertise to support Texas entities throughout the state.

As of October 15, 2022, 68 volunteers have completed the VIRT application and onboarding process including criminal background checks. Incident response practitioners with expertise in addressing cybersecurity incidents may apply for membership on the Texas VIRT by completing the VIRT Volunteer Application and submitting it to DIR for review.

Cybersecurity Incident Response Team

DIR's Cybersecurity Incident Response Team (CIRT) assists state and local governments experiencing a cyber incident through on-site and remote incident response. Additionally, CIRT members disseminate threat intelligence and security bulletins, offer training and tabletop exercises, as well as develop cybersecurity policies and procedures. Since March 2022, the CIRT has responded to 58 total incidents and delivered over 20 tabletop exercises and incident response trainings.

Cybersecurity Operations

DIR Cybersecurity Operations (CyberOps) team provides cybersecurity services for most state agencies and continuously monitors the more than 2.8 million public-facing Internet Protocol (IP) addresses owned by Texas agencies. CyberOps oversees perimeter network security for the state agency network by blocking unwanted traffic, monitoring suspicious traffic, and alerting agencies to malicious activity. CyberOps monitors for Distributed Denial of Service (DDoS) attacks and offers mitigation for the agencies. CyberOps manages data center security operations and security incident response. In addition, CyberOps analyzes suspected phishing emails on behalf of state agencies and takes action to mitigate the phishing emails risks. In fiscal year (FY) 2022, CyberOps analyzed 2,381 suspected phishing emails, and observed notable increases in phishing email submissions, DDoS attacks, intelligence tips shared, and alerts sent to agencies.

DIR Shared Technology Services

DIR's Shared Technology Services (STS) Program provides state agencies, institutions of higher education, K-12 public educational entities, and local governments with managed IT and security services that have the benefit of central management and pre-negotiated volume-based rates. Under STS, eligible public sector entities have access to services including:

- A wide range of proactive and responsive security services through the Managed Security Services (MSS) Program;
- Secure cloud, mainframe, print and mail, and security operation services through the Next Generation Data Center Services Program (DCS); and
- Identity and Access Management (IAM) solutions such as multifactor authentication (MFA) and identity proofing through the Texas Digital Identity Solution (TDIS).

DIR Managed Security Services

The MSS program offers security services at pre-negotiated and competitive industry rates within the categories of risk and compliance, security monitoring and device management, and incident response. All MSS eligible customers have the option of leveraging the incident response offering without having to pay retainer fees. If a cybersecurity incident occurs that requires external assistance, DIR can quickly deploy a team of highly skilled cyber professionals to assist the entity in the incident response process. Since September 1, 2021, 526 organizations have engaged MSS resources 604 times. These requests for service include:

- 20 incident response requests;
- 507 risk and compliance requests; and
- 77 orders for security monitoring and device management.

Table 1: Managed Security Services by Customer and Engagement identifies the number of customers by organization type and the number of requests for MSS services for FY 2021 and 2022.

Table 1: Managed Security Services by Customer and Engagement

Organization Type	Organization Count	Tickets by Organization
State	101	418
Education	94	124
Local Government	248	38
Others	38	14
Total	**526**	**604**

Source: Shared Technology Services Portal

From 2021 to 2022, MSS provided 85 Texas Cybersecurity Framework (TCF) Assessments. The TCF Assessment uses an independent third-party to help organizations identify, assess, and manage cybersecurity risks in their environment.

MSS resources supported the incident response efforts of 20 organizations, providing industry-leading subject matter expertise to mitigate the impacts of cybersecurity incidents and prepare each organization for recovery operations. Accelerated efforts to contain and eradicate cyber threats reduce their potential impact, which may reduce the overall cost of responding to and recovering from cybersecurity incidents.

Data Center Services

The Texas Data Center Services program (DCS) allows state and local governmental entities (customers) to outsource management of technology infrastructure services. Customers receive the benefit of aggregated volume discounts by sharing technology services, while in turn receiving the “best in breed” technology services from competitively procured industry leading vendors. DCS provides secure connectivity to select public and private clouds designed around government security and disaster recovery requirements, and flexible service tiers to meet differing needs and budgets. Joining the program allows customers to delegate infrastructure management while increasing focus on delivering direct, mission-related value to their business users and clients. DCS includes five service towers that collectively provide modern services for Texas government agencies. *Table 2: Shared Technology Services Next-Generation Data Center Towers* identifies the five service towers and how they support the next-generation data center services.

Table 2: Shared Technology Services Next-Generation Data Center Towers

Public Cloud	Private Cloud Management	Technology Solution Services	Print Mail	Security Operation Services
· Infrastructure-as-a-Service · Platform-as-a-Service · Software-as-a-Service	· Texas Private Cloud · Facilities · Computing Services	· Technology Services · Project Delivery · Application Management	· Print and Mail Services · Digitization · Digital Records Storage	· Cybersecurity Policy · Monitoring · Incident Management

The Security Operations Services tower, added in 2020, provides dedicated cybersecurity policies, oversight, and monitoring of the DCS infrastructure.

Cybersecurity policy support helps decrease the risk of a catastrophic cybersecurity incident by dedicating resources to mitigating cyber threats and vulnerabilities. Dedicated monitoring supports early detection of cybersecurity incidents, which is an important factor in containing cybersecurity incidents and reducing potential damage.

In 2022, the DCS program integrated a security operations module into the service management solution, enabling automation and efficiencies to the vulnerability management program and other areas of the security operations of the program.

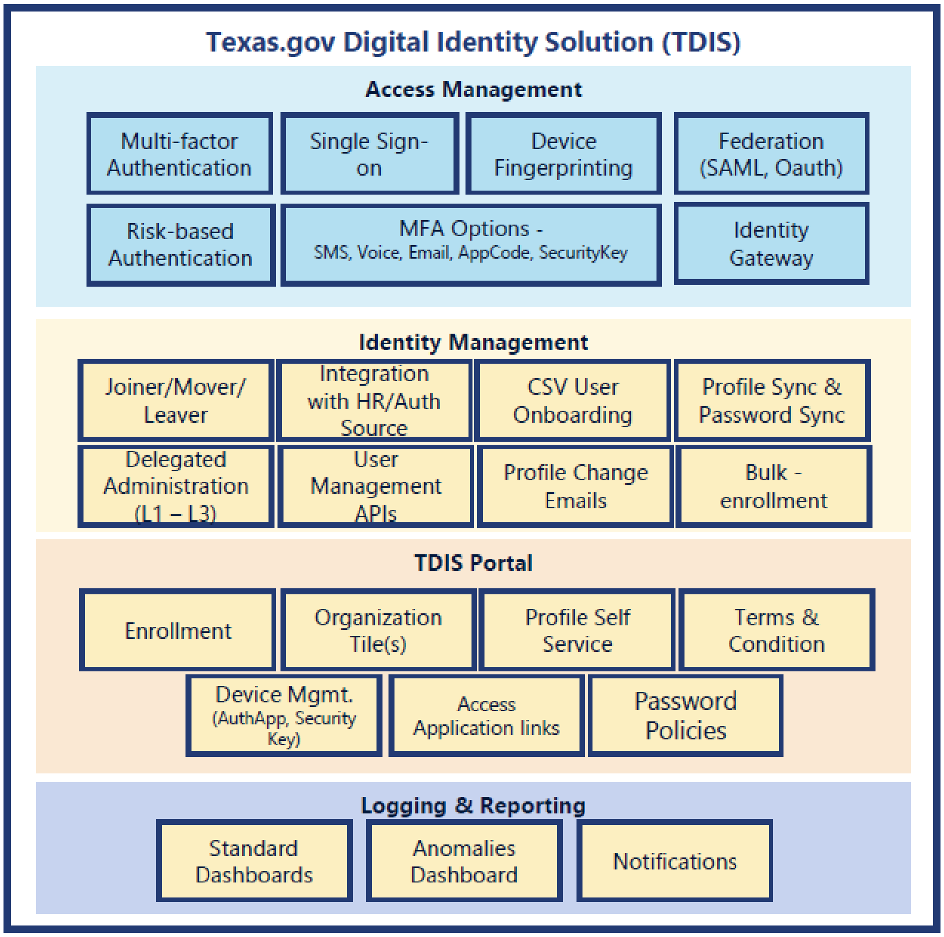
Texas Digital Identity Solution

In the 86th legislative session, DIR received funding to implement a statewide risk-based multi-factor authentication program (MFA) program, called the Texas Digital Identity Solution (TDIS). MFA is the practice of authenticating users attempting to gain access to a system through the verification of two or more authentication factors. MFA provides an additional layer of security that serves as a failsafe if the primary method of authentication, such as a password, were to be compromised by a malicious actor.

With an MFA implementation, attackers can no longer access the target network solely through stolen credentials (e.g., single-authentication username and password). TDIS is a voluntary service available to state agencies and institutions of higher education that has a specific set of identity and access management features. As resources permit, MFA should be applied to high-risk network devices, systems, remote access, and user accounts.

Error! Reference source not found. displays the current TDIS solution capabilities.

Figure 7: Texas Digital Identity Solution Capabilities



Texas.gov Digital Identity Solution (TDIS)

Access Management

Multi-factor Authentication
Single Sign-on
Device Fingerprinting
Federation (SAML, Oauth)
Risk-based Authentication
MFA Options - SMS, Voice, Email, AppCode, SecurityKey
Identity Gateway

Identity Management

Joiner/Mover/ Leaver
Integration with HR/Auth Source
CSV User Onboarding
Profile Sync & Password Sync
Delegated Administration (L1 – L3)
User Management APIs
Profile Change Emails
Bulk - enrollment

TDIS Portal

Enrollment
Organization Tile(s)
Profile Self Service
Terms & Condition
Device Mgmt. (AuthApp, Security Key)
Access Application links
Password Policies

Logging & Reporting

Standard Dashboards
Anomalies Dashboard
Notifications

Texas Cybersecurity Incident Response Plan

In response to increased cybersecurity incident activity, DIR formed the Statewide Incident Response Working Group, initiating a multiyear effort to develop a statewide cybersecurity incident management plan, as required by Government Code Section 2054.518. The Working Group consists of personnel from DIR, the Texas Division of Emergency Management (TDEM), the Texas Military Department (TMD), and the Department of Public Safety (DPS), with supporting members from the Texas Commission on Environmental Quality, the Public Utility Commission, the Texas Railroad Commission, and the Texas Water Development Board. This initiative defined the statewide concept for cybersecurity operations, identification of responsibilities, and coordination strategies to support a successful statewide cybersecurity incident response effort.

The initiative was tested at a previously unprecedented scale slightly two years after initial planning, when a coordinated cyberattack simultaneously impacted 23 local government entities in August 2019. The attack heavily affected local governmental organizations, with some losing the ability to conduct basic business services and even to manage their critical infrastructure systems. Based on the planning efforts, DIR led the response and coordinated with partners including the TMD, TDEM, DPS, Texas A&M University System, MSS resources, and federal and other private sector partners to implement the cybersecurity incident management plan and successfully respond to the cyberattack.

This cyberattack necessitated an activation of the Texas State Operations Center, from which DIR and supporting partner organizations successfully mitigated the active cyber threat, allowing the local government entities to restore operations and begin the recovery process in about a week.

Statewide Incident Response Preparedness

In 2021, TDEM began revisions to the State of Texas Emergency Management Plan Cybersecurity Emergency Support Function (ESF), which outlines the state’s response to a cybersecurity disaster, to include additional resources and coordination mechanisms. This ESF is now undergoing a full revision to reflect Texas’ collaborative approach to responding to cybersecurity incidents across the state and will include additional partners, programs, and resources, such as regional security operation centers, the Texas Volunteer Incident Response Team, and other cybersecurity initiatives. When a cybersecurity incident warrants state involvement, the partner agencies identified in this plan may deploy resources to assist the impacted entity with containment and eradication of the threat and support the organization’s transition to recovery.

DIR maintains a comprehensive Incident Response Redbook template. The Incident Response Redbook provides a foundation for organizations to build their internal incident response capability and response plan. It contains templates, guides, legal references, and additional resources based on industry best practices that can be adopted and tailored to suit the unique needs of individual organizations. In January 2022, DIR revised the Redbook to include foundational steps to building and maintaining a cybersecurity program from the ground up.

DIR uses funding from the Homeland Security Grant Program to support incident response tabletop exercises, training, coordination, and information sharing functions.

Governance, Risk, and Compliance

DIR establishes state information security standards in 1 Texas Administrative Code, Chapter 202 (TAC 202). TAC 202 references the minimum selection of security controls required for state information systems as outlined in the DIR Control Standards Catalog. In 2022, DIR updated the Control Standards Catalog to align with the most recent revision of NIST Special Publication 800-53 (revision 5). DIR developed the Texas Cybersecurity Framework, based off the NIST Framework for Improving Critical Infrastructure Security, as a tool to assist organizations with assessing their information security program maturity across critical information security areas.

The framework is a process-focused approach to assessing information security capabilities, while the control catalog provides the minimum technical and administrative safeguards for state systems. Together, the framework and control catalog offer organizations a standardized scale to measure their overall information security maturity over time. Through the Statewide Portal for Enterprise Cybersecurity Threat, Risk, and Incident Management (SPECTRIM), state organizations can find several tools to automate and conduct information security planning and assessment activities.

Texas Information Sharing and Analysis Organization

Information sharing is crucial in reducing the quantity and impact of cybersecurity attacks on all entities within Texas. Government Code 2054.0594 requires DIR to establish an Information Sharing and Analysis Organization to provide 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.

The Texas Information Sharing and Analysis Organization (TX-ISAO), led by the Texas Cybersecurity Coordinator, acts as a trusted hub for collection and sharing cyber risk information among public and private sector stakeholders. The TX-ISAO is available to all Texas organizations, whether public, private, or non-profit, at no cost to the organization. Members of the TX-ISAO have access to organization and industry-specific cyber intelligence, including information about current cyber threats, attack vectors, indicators of compromise, and other relevant security information. The TX-ISAO also receives cyber threat information from its members, analyzes trends, and issues notifications to improve security awareness. The TX-ISAO hosts monthly meetings to share content and assist members mature their cybersecurity programs.

In 2019, DIR partnered with Texas A&M University (TAMU) and the University of Texas at San Antonio (UTSA) to provide educational services to TX-ISAO members. In 2020, DIR created a multiphase plan for expanding services and information sharing, while concurrently working to build private-public partnerships via the TX-ISAO. The first phase entailed launching a website in 2020 where the public can report a cyber threat and members can enroll infrastructure sector-specific mailing lists to receive cybersecurity information from the TX-ISAO.

In August 2022, DIR implemented an enhanced information sharing portal within SPECTRIM to provide participating TX-ISAO members secure access to more detailed information on cybersecurity threats, best practices, and strategies. In the future, the portal will also include a discussion module for members to share best practices, lessons learned, and insights on how to best defend against evolving cyber threats.

Cybersecurity Education and Outreach

DIR's Office of the Chief Information Security Officer (OCISO) offers many free professional development webinars targeted to state and local governments. On the third week of every month, DIR partners with Gartner to conduct webinars on security topics. On the fourth Thursday of even months, DIR hosts education security webinars presented by third-party vendors sharing hot topics, trends, and information for strategic planning. In addition, the OCISO division holds an annual Information Security Forum (ISF), which is an educational conference for public sector security and IT professionals from across Texas, and an Information Security Officer Summit for officially designated Information Security Officers from state agencies, institutions of higher education, and public community colleges.

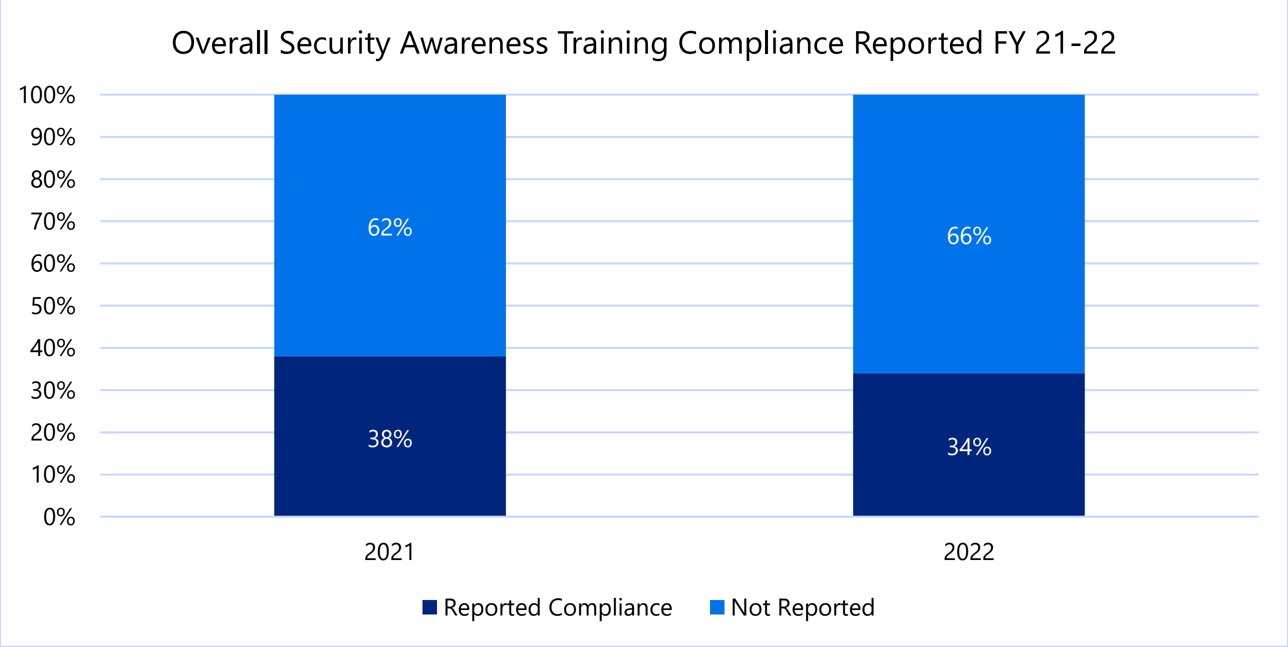
In addition to OCISO's programs, DIR's Texas Infosec Academy offers state agency and higher education information security variety of free professional cybersecurity certifications and trainings to help enhance the cybersecurity capabilities and posture throughout the state. In 2020, DIR added a Secure Developer Foundation certification to the course catalog. In FY 2022, 478 state agency information security personnel attended a course through the InfoSec Academy.

In honor of National Cybersecurity Awareness Month each October, DIR also hosts free in-person events and virtual presentations to raise awareness of cybersecurity issues. DIR also leverages the agency's social media channels to promote Cybersecurity Awareness Month, including posts about DIR's security programs and resources, cyber tips, the DIR High School Cybersecurity Awareness Public Service Announcement (PSA) video competition, and the Multi State-Information Sharing Analysis Center (MS-ISAC) kids' poster contest - in which Texas had two winners for the 2022 calendar. In 2021, more than 5,000 Texas high school students participated in CyberStart (CSA) America, an immersive cybersecurity training game which offers scholarships for high-achieving participants. This year, DIR and the University of Texas Advanced Computing Center (TACC) created the CSA Texas taskforce to expand outreach efforts and support educators and students interested in participating.

Along with free training geared for public sector security staff, DIR oversees the state's security training program required for most state and local employees.

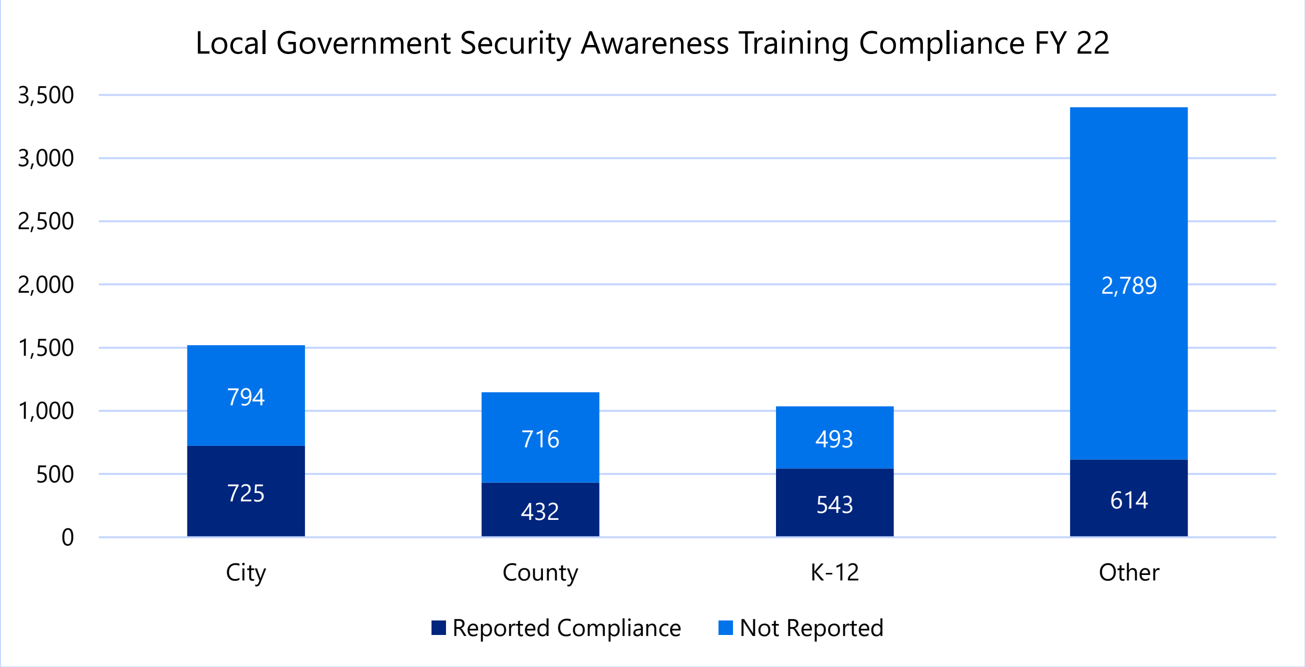
Government Code 2054.519 requires DIR in consultation with the Texas Cybersecurity Council to certify at least five cybersecurity training programs for state and local government employees and requires most state and local government employees to complete a certified training program. For 2022, DIR reviewed and certified 160 training programs. DIR also received 2,505 compliance reports from state and local government entities (34% of the 7,316 state and local government entities).

Figure 8: State and Local Security Awareness Training Reported Compliance



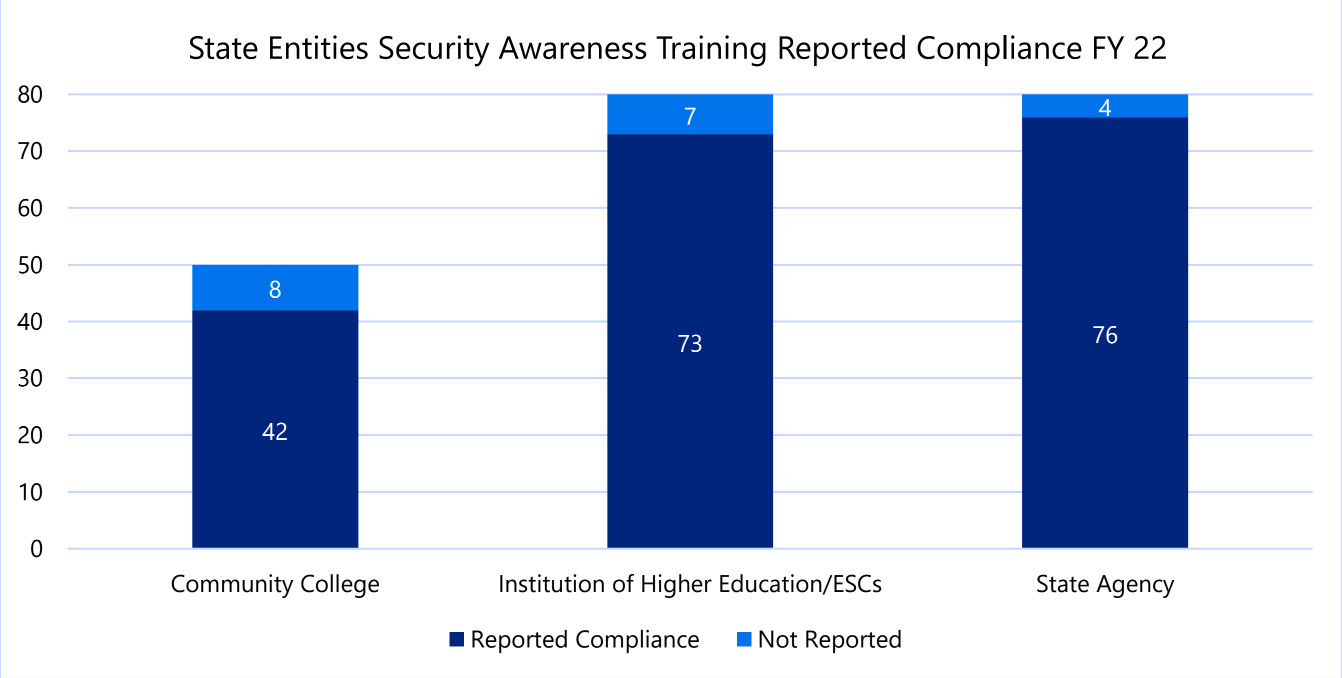
Source: Texas Department of Information Resources Security Awareness Compliance Reporting

Figure 9: Local Government Entity Security Awareness Training Reported Compliance



Source: Texas Department of Information Resources Security Awareness Compliance Reporting

Figure 10: State Government Entities Security Awareness Training Reported Compliance



Source: Texas Department of Information Resources Security Awareness Compliance Reporting

Regional Security Operations Center

Senate Bill 475, passed by the 87th Legislature, authorized DIR to establish a Regional Security Operations Center (RSOC) to provide boots on the ground support close to local governments that need assistance with major cybersecurity incidents. To operate the RSOC, DIR must partner with a Texas public university to give university students hands-on experience and strengthen the cybersecurity workforce of tomorrow. The RSOC may offer network security infrastructure that local governments can utilize and provide real-time network security monitoring; network security alerts; incident response; and cybersecurity educational services. Eligible customers include counties, local governments, school districts, water districts, and hospital districts.

In 2022, Angelo State University partnered with DIR as the pilot RSOC. DIR's vision for the RSOC initiative is to partner with additional public universities and establish RSOCs throughout the state to serve local entities and assist in protecting the state from cyber threats. This vision aligns with a whole-of-state approach to cybersecurity that increases the threat protection and cyber maturity of all of Texas through collaboration and partnerships. DIR is requesting funding from the 88th Legislature to establish two additional RSOCs including one in the Rio Grande Valley and one in central Texas.

Texas Risk and Authorization Management Program

Because cloud computing consists of hosting state data at a site controlled by a vendor, it is important that the state enforce strong security controls surrounding that data. The Texas Risk and Authorization Management Program (TX-RAMP) is a standardized approach to the assessment and evaluation of cloud computing services used by state agencies and institutions of higher education. Government Code 2054.0593 mandates that state agencies, as defined by Government Code 2054.003(13), must only enter into, or renew, contracts to receive cloud computing services that comply with TX-RAMP requirements.

Endpoint Detection and Response

Endpoint detection and response (EDR) technologies are security systems that detect and investigate suspicious activities on endpoints, using automation to allow security teams to quickly identify and respond to threats. EDR goes beyond traditional anti-virus (AV) software, by using not only the signature technologies that are present in AV, but also looks at behaviors and changes in systems to determine that threats exist. The 87th Texas Legislature appropriated funds for DIR to provide EDR services to Texas state agencies at no cost, and other Texas public entities, such as municipalities and counties, can purchase EDR services through DIR's MSS Program. Since 2020, 62 eligible government entities obtained EDR technology from DIR.

Additional Resources

Texas government entities may be eligible to supplement their cybersecurity strategy using the following programs and services.

Texas Municipal League

The Texas Municipal League (TML) is an association that provides resources to and advocates on behalf of local municipal governments in Texas. TML provides a cybersecurity risk pool program to support their members during security incidents.

Texas Association of Counties

Texas Association of Counties (TAC) is an association that offers resources and services to Texas counties. TAC provides members access to the Risk Management Pool to support their members before and after a data breach.

Texas Association of School Boards

The Texas Association of School Boards is an association that offers Texas school districts advocacy, leadership, and services. The association provides members privacy and information security coverage to assist with data breach support and cybersecurity training.

Credit Monitoring Services Available from Texas SmartBuy

The Texas SmartBuy program (formerly called the Cooperative (CO-OP) Purchasing Program) is a cooperative purchasing program operated by the Texas Comptroller of Public Accounts available to state agencies, cities, counties, and school districts. Through contracts available on the SmartBuy Program, organizations impacted by a data breach (where personal information is compromised or stolen) can access services that notify their users of the compromise by mail or by telephone call, and to provide both single- or triple-bureau monitoring services, with available restoration and insurance provisions.

Cybersecurity and Infrastructure Security Agency

The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) coordinates the national effort to understand cyber threats and defend the national infrastructure. CISA in turn funds the Multi-State Information Sharing and Analysis Center (MS-ISAC), an organization that works to improve the overall cybersecurity posture of the nation's State, Local, Tribal, and Territorial (SLTT) governments through focused cyber threat notification, response, and recovery services.

MS-ISAC members may take advantage of federally operated network security monitoring services and free incident response services, including emergency conference calls, forensic and log analyses, mitigation recommendations, and reverse engineering of malicious code.

Preventive And Recovery Efforts

Taking proactive measures to reduce the likelihood of a cyberattack can prevent or minimize potential impacts. The following are initiatives that state and local government entities can take to strengthen cybersecurity defenses and minimize the adverse outcomes of cybersecurity incidents.

Identity Management

Identity management ensures that only authenticated users, whether individuals or devices, are granted access to the specific applications, components, and systems for which they are authorized. Identity theft is an ongoing threat: identity fraud cases are up over 70% since 2020, with losses of an estimated $5.8 billion in 2021 alone, according to the Federal Trade Commission. Implementing identity management, such as the MFA program funded by DIR, can protect entities against unauthorized users gaining access to the system and stealing valuable data.

Inventory Devices, Software, and Data

Before an organization can effectively know what to protect, it must identify what it has. The first step toward a mature information security program is compiling a list of the physical assets possessed by the organization to determine what should and should not be on the network. After inventorying physical devices, an organization can inventory the virtual assets, such as applications, of the enterprise in relation to those physical assets. More mature programs classify the data and information that flows through those programs and the mechanisms used for storage and transmission. Visibility into the systems and devices that send, receive, process, or store sensitive and confidential data can help management make informed decisions about the controls to provide across the network in a cost-efficient manner. Inventory management should be a continuous process to ensure that assets are accounted for on an ongoing basis to minimize the risk of loss.

Ransomware Protection

Ransomware attacks continue to make headlines across the country and in the state of Texas. A ransomware attack uses data encryption to prevent an organization from accessing files and systems. Attackers will often hold the information assets hostage and demand some form of payment in return for restoring system access or providing the decryption key. However, even if an organization agrees to the terms of the ransom, there is no guarantee that the data will ever be returned. The best defense against ransomware are complete backups that are tested routinely and stored physically and logically separate from the production systems. Additionally, ensuring that staff are trained to identify and report suspicious emails can reduce the risk of ransomware, and Endpoint Detection and Response tools provide a good defense. Organizations should have a plan in place specifically to address ransomware from both a proactive and reactive standpoint.

Cybersecurity Training

According to the 2022 Verizon Data Breach Investigations Report, malware used in data breaches were delivered through email in 86% of cases and delivered via the web in seven percent (7%) of cases. Of the malware used in data breaches, 46% were Windows Apps and 17% of an Office document file type. Overall, approximately one-third of data breaches involved some form of social engineering, a type of attack involving the manipulation of a person to complete some action to support an attacker's goal. Educating users and applying protections against these types of threats can help greatly reduce risk.

Executive and IT staff are frequently targeted in carrying out an attack. It is especially important that these individuals receive appropriate training to recognize suspicious communications and react accordingly, as these user accounts typically have the potential for more significant damage if compromised. Executive staff may also be candidates for tailored cybersecurity training. As critical decision-makers, executive management should understand cybersecurity principles and risk to better protect the organization through informed decisions. Finance and purchasing employees have also recently become a preferred target. Attackers have used convincingly designed social engineering attacks to reroute payroll and vendor payments to their own accounts. Organizations should consider implementing an executive-focused or role-based cybersecurity awareness training program to raise awareness of the common attacks a group may experience.

Vulnerability Management and Secure Configuration

The cybersecurity threat landscape and attack methods change rapidly. System or software vulnerabilities are exploited or identified, software patches are issued, remediations are performed, new vulnerabilities are discovered, and the cycle continues. As security defenses improve, so do the complexity of attacks. The demand for adaptability in cybersecurity requires organizations to continuously acquire and act on new information to defend against evolving threats. Organizations benefit from adopting a routine schedule of technical and non-technical assessments of their security posture and prioritize the remediation of identified vulnerabilities and weaknesses based on their unique risk profiles. DIR offers security services such as network and web application penetration testing, mobile application penetration testing, vulnerability scanning, security event and incident monitoring, security assessments, and more.

Cloud Security

In the last 18 months, 79% of companies experienced at least one cloud data breach; even more alarmingly, 43% reported 10 or more breaches in that time, according to Expert Insights. Securing modern cloud workloads requires controls around vulnerabilities, configurations, entitlements, and runtime threat detection. TX-RAMP Cloud Security requirements are derived from NIST Special Publication 800-53, which provides a catalog of security and privacy controls for all U.S. federal information systems except those related to national security. These controls ensure that all outstanding compliance issues and vulnerabilities are identified, documented, tested, and resolved within a timely manner.

Improve Boundary Defense and Visibility

Texas government entities would greatly benefit from advanced boundary defenses and the ability to have more visibility into the network and the Internet. The Center for Internet Security states that the purpose of boundary defense is to detect, prevent, and correct the flow of information transferring networks of different trust levels with a focus on security-damaging data. In accordance with the DIR security control catalog, each information system should be defined within a system security plan, which is derived from internal and external risk assessments.

Using a standardized, well-documented process allows an organization to know all their system interconnections, whether internally owned, or to an external network of systems. Creating a defined internal and external network, system, and data boundaries provides an easier means to determine possible risks. Implemented security controls, approved communications such as interconnection agreements, and applicable contract language grant business partners a better means to verify the legitimacy of transmitted confidential or sensitive information over secure channels (i.e., encrypted ports). Organizations that adopt this process and implement strong boundary defense will have greater ability to identify, protect, detect, respond, and recover from real world risks and threats.

The ability to block suspicious and malicious communications is key to protecting state assets. Boundary defenses are defined as technical security controls (hardware and software) that contribute to the protection and segregation of the disparate networks. The network will have systems and applications that have varying degrees of trust, such as impact levels: high, medium, or low; and sensitivity levels: confidential, sensitive, or public. Organizations can further consider differing levels of security compliance and existing vulnerabilities to identify the need for multiple and redundant defensive measures to counter security control failures and/or vulnerability exploitation.

Secure Application Development and Testing

It is important to develop applications with security in mind throughout the software development life cycle and to perform comprehensive testing prior to moving an application into production. There are some fundamental coding practices that can reduce application vulnerabilities and remediation costs such as input validation, least privilege access, or ensuring appropriate error messages. Malicious code injection, broken authentication and session management, sensitive data exposure, leveraging existing vulnerable code, and other critical security risks are easier to address during development than after deployment. Organizations may benefit from sending application developers through a secure coding training or having a member of the application development team designated as a cybersecurity subject matter expert on development projects. DIR provides secure coding courses through its InfoSec Academy for developers at state agencies and institutions of higher education though funding provided by the legislature.

Incident Response Planning and Exercises

The difficulty of predicting the details of a cyberattack makes it challenging to fully prepare to respond to an incident when the time comes. When, where, and how a cyberattack will occur are primarily determined by factors outside of an organization's control. Having a general plan of action to address the fundamental aspects of roles, responsibilities, and resources is crucial to an expedient and successful response. Each organization should have an incident response plan that is routinely updated and exercised in as near a real-world simulation environment as possible.

Third-Party Information Security

Whether using a managed service, moving applications to the cloud, or procuring off-the-shelf software, there is a growing reliance on third-party organizations and products when delivering information services. Organizations should obtain information security assurances and liability protections to the greatest extent feasible when entrusting sensitive and confidential information to a third-party service provider. Integrating standard security language and artifacts such as data use agreements, acceptable use agreements, background checks, and required security training for contractors may help promote these assurances. Additionally, when incorporating third-party applications, code, or other information system components in internal systems, a risk assessment of the security implications should be performed, documented, and approved by personnel with the appropriate level of authority.

Shared Information Security Resource Program

Overview

Government Code 2054.0591(4) requires DIR to include in the cybersecurity report "an evaluation of a program that provides an information security officer to assist small state agencies and local governments who are unable to justify hiring a full-time information security officer."

State agencies, public institutions of higher education, and community colleges, are required by Government Code 2054.136 to designate an Information Security Officer (ISO) who:

(1) reports to the agency's executive-level management;

(2) has authority over information security for the entire agency;

(3) possesses training and experience required to perform the duties required by department rules; and

(4) to the extent feasible, has information security duties as the officer's primary duties.

The ISO's responsibilities are set by rule 1 TAC 202.21 and include:

(1) developing and maintaining an agency-wide information security plan as required by Government Code Section 2054.133;

(2) developing and maintaining information security policies and procedures that address the requirements of this chapter and the agency's information security risks;

(3) working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of this chapter and the agency's information security risks;

(4) providing for training and direction of personnel with significant responsibilities for information security with respect to such responsibilities;

(5) providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities as set by 1 TAC 202.22;

(6) ensuring that:

(A) risk assessments are performed by the information owners and supported by the information-custodians at least biennially for systems containing confidential data and periodically for systems containing agency sensitive or public data; and

(B) security assessments are conducted biennially for systems containing confidential data and periodically for systems containing agency sensitive or public data;

(7) reviewing the agency's inventory of information systems and related ownership and responsibilities;

(8) recommending and collaborating to establish policies, procedures, and practices, in cooperation with the agency Information Resources Manager, information-owners, and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, access, exposure, or disclosure;

(9) coordinating the review of security requirements and specifications, and verifying that security requirements are identified and risk mitigation plans are developed and contractually agreed and obligated prior to the acquisition of new information systems and/or related services and applications;

(10) verifying that security requirements are identified and risk mitigation plans are developed and implemented prior to the deployment of internally-developed information systems and/or related applications or services;

(11) reporting, at least annually, directly to the agency head the status and effectiveness of the security program and its controls;

(12) informing any relevant parties in the event of noncompliance with this chapter and/or with the state agency's information security policies; and

(13) all other duties required by Government Code 2054.136.

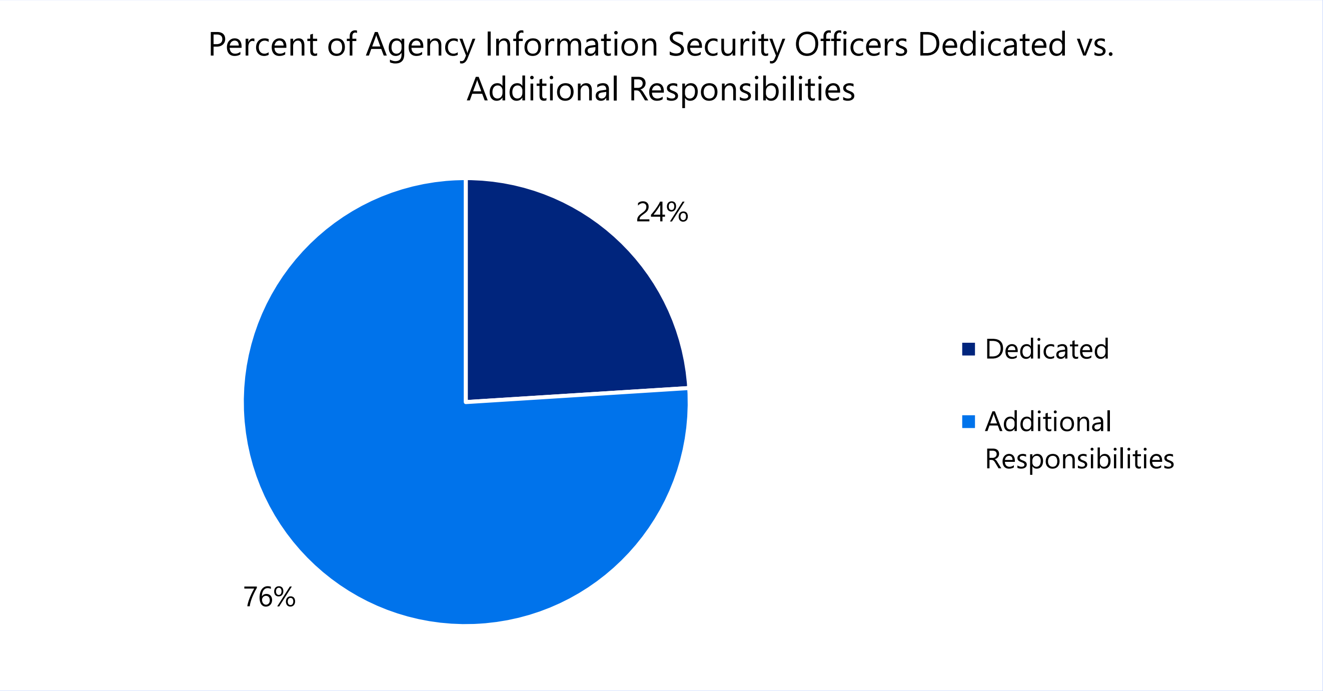
State Information Security Workforce and Challenges

There are nearly 200 state agencies and universities of higher education in Texas, and while each state organization is required to have a designated ISO, some agencies may not be able to dedicate an employee solely to information security-related duties as their primary function.

Particularly in smaller agencies where IT budgets and personnel are limited, an agency ISO often may also serve in other official roles. Therefore, some ISOs my not have a strong familiarity of IT, security best practices, or the depth of knowledge and skills to build and maintain effective information security programs.

In the 2022 IRDR, 76% percent of state agencies reported that their information security officer had additional responsibilities outside of information security.

Figure 11: Percent of Information Security Officers with Additional Responsibilities

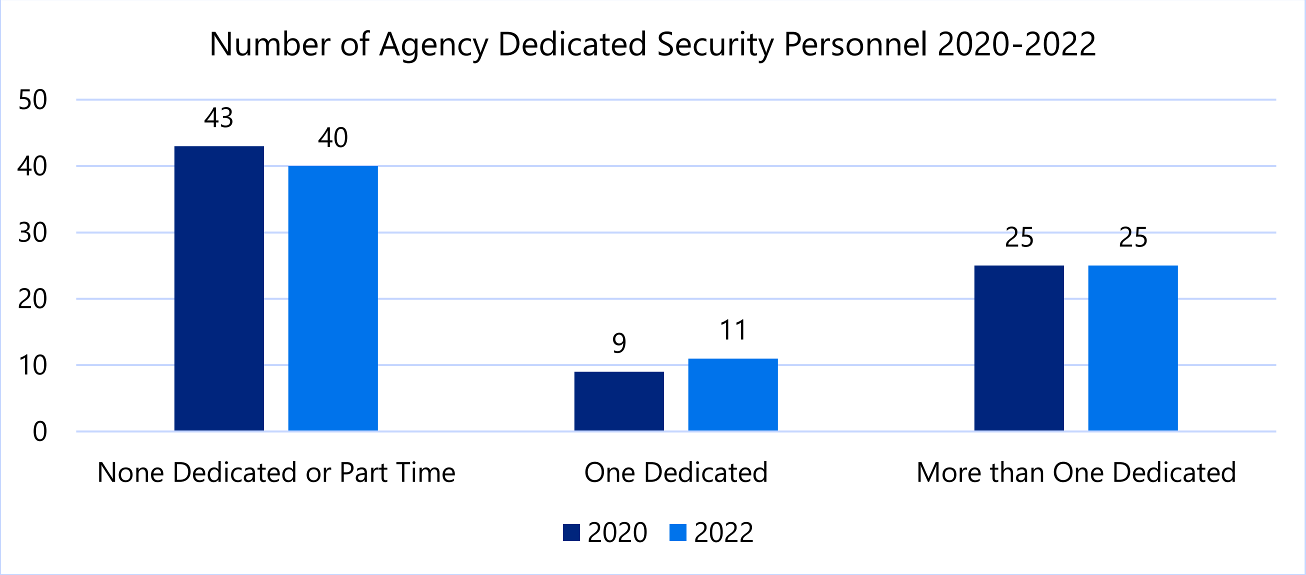


Source: 2022 Information Resources Deployment Review

According to the 2022 IRDR, only 31% of state agencies reported having more than one dedicated information security personnel. Additionally, 40 agencies reported having fewer than one dedicated (part-time only or none) agency security personnel within their organizations.

While the number of overall information state security personnel increased consistently over the last several years, smaller and mid-sized organizations continue to report challenges in staffing and retaining qualified information security professionals. *Figure 12: Number of State Agency Dedicated Information Security Personnel 2020-2022* shows the number of information security personnel for state agencies as reported in the 2020 and 2022 IRDR.

Figure 12: Number of State Agency Dedicated Information Security Personnel 2020-2022



Source: 2022 Information Resources Deployment Review

As reported in the 2022 IRDR, the largest barriers agency face concerning information security are increasing sophistication of threats, lack of sufficient funding, and inadequate availability of security professionals.

Sharing a common resource for managing IT or information security has existed in state government for several years. Currently, some small state agencies and judicial organizations share a single information security officer. However, this arrangement is typically determined directly by the participating organizations with the designated information security officer employed by a single entity. This arrangement creates barriers for other entities that are interested in entering similar agreements due to lack of standardization and clarity in roles and responsibilities.

Given these challenges, an information security resource sharing program could provide cost-effective assistance and allow existing overcommitted resources to focus on other initiatives to reduce risk. State agencies participate in other state-provided resource sharing programs and have expressed interest in utilizing information security resources.

Local Government Participation

Local governments are frequently targets of cyberattacks. Since 2019, local governments experienced an average of 32 security incidents per year that required assistance or guidance from the state. Local governments often face challenges relating to aging infrastructure, lack of qualified security personnel, and strict budgets that leave their information assets vulnerable.

Currently, local government entities are not required to follow the security standards that DIR sets in TAC 202. While public school districts are required to designate a cybersecurity coordinator with the Texas Education Agency, other local government entities, such as cities and counties, do not have to designate an ISO or a point of contact for information security to the state. Assuming the same challenges faced by small and mid-sized agencies exist across local governments, a resource sharing program among local entities could potentially fill the knowledge and skill gaps of the workforce.

Conclusion

The primary goal of an information security resource sharing program is to reduce risk. Legislative consideration of a resource sharing program at both the state and local level may help reduce staffing challenges and improve information security capabilities. Potential benefits include:

- Shorter response time to information security program risks;
- Improved availability (quantity and quality) of security professionals;
- Increased agency's information security maturity; and
- Support for small and medium-sized agencies with resource challenges.

As of 2021, the U.S. Bureau of Labor Statistics reports 163,000 security analyst positions with a 35% projected rate of employment change. This is higher than the average for all occupations and could be indicative of frequent moves between employers. Competition with the private sector for high-demand skillsets is particularly difficult for smaller government entities that already struggle to justify a full-time information security position due to resource limitations.

Costs and potential savings from a resource sharing program depend on a multitude of factors such as:

- Ratios of organizations to program resources;
- Level of workload and workload complexity;
- Level of agency-provided assistance;
- Knowledge, skills, abilities, and experience of shared resources;
- Employment/contractor replacement/displacement;
- Length of engagements;
- Existing technologies; and
- Number of participating organizations.

Shared resource programs distribute the costs of skilled professionals across multiple entities, allowing access to expertise that would otherwise be cost-prohibitive.

Legislative Recommendations

Adoption of .gov Domain

Cyber criminals attempt to defraud users into handing over sensitive personal and financial information by creating domains that imitate government websites. For example, someone trying to trick users into handing over sensitive information may register a government entity's name with a .com address and purport to be offering services that require registering personal details. However, the .gov domain is administered by CISA and any issuance of the .gov domain is vetted for authenticity. Use of .gov can increase confidence and assurance that the site belongs to the entity it claims to be. DIR recommends the Legislature consider requiring government entities to adopt the verified .gov domain before establishing a new domain name or for certain websites that collect personal or financial information.

Local Government Incident Reporting

While state agencies are required to report cybersecurity incidents to the state through DIR, local government entities are not. Requiring local entities to report these incidents to DIR will improve transparency surrounding the threat landscape in Texas and strengthen the state's ability to defend against attacks. DIR recommends that those entities also be required to report these incidents to the state. Emergency Management and Cybersecurity Incident Response

Currently, the State of Texas Cybersecurity Emergency Support Function (ESF) designates the DIR and TDEM as the primary entities to assist in this planning effort for a cybersecurity disaster. DIR oversees the incident response efforts and Volunteer Incident Response Team (VIRT) for cybersecurity disasters. Codifying the ESF would bring clarity to roles during a cybersecurity disaster particularly as DIR oversees the VIRT and would lead the VIRT's response during a cybersecurity disaster.

Prohibit Ransomware Payments

Cyber criminals use ransomware to encrypt systems and often demand a large financial payment to release those systems. Paying the ransom incentivizes the use of ransomware and funds criminal organizations. Texas should take a stand against ransomware and prohibit public entities from paying or authorizing payments for ransomware.

List of Tables

List of Figures

References

Crowdstrike. (2022). *Falcon Overwatch Threat Hunting Report.*

Expert Insights. (2022, March 28). *50 Cloud Security Stats You Should Know in 2022*. Retrieved from Expert Insights: https://expertinsights.com/insights/50-cloud-security-stats-you-should-know/

Federal Trade Commission. (2021). *Consumer Sentinel Network Data Book.*

National Council on Identity Theft Protection. (n.d.). *2022 Identity Theft Facts and Statistics*. Retrieved from identitytheft.org: https://identitytheft.org/statistics/

Proofpoint. (2022). *Social Engineering Report.*

Verizon. (2022). *2022 Data Breach Investigations Report.*