# 2020 Cybersecurity Report

November 15, 2020

**Texas Department of Information Resources**

Transforming How Texas Government Serves Texans

## Table of Contents



*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 cybersecurity event is used interchangeably with the term cybersecurity incident.*

*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

The 86th Texas Legislature demonstrated a significant interest in improving cybersecurity throughout Texas with legislation such as:

- Senate Bill 64, requiring a report on the strategies to incentivize institutions of higher education to develop cybersecurity degree programs, codifying the prioritization of cybersecurity and legacy modernization projects, and expanding state information security requirements to public junior colleges.
- Senate Bill 820, requiring that a school district adopt a cybersecurity policy to determine risks and implement mitigation planning and to report any cybersecurity breach to the Texas Education Agency.
- Senate Bill 936 and SB 475, requiring the Public Utility Commission and Electric Reliability Council of Texas to monitor cybersecurity and establishing the Texas Electric Grid Security Council.
- House Bill 1421, requiring the Secretary of State to develop best practices to securing and transmitting election data, election officials to request cybersecurity assessments as recommended by the Secretary of State, and immediate notification of a breach of election data to the Secretary of State.
- House Bill 3834, requiring government entities at all levels to ensure the delivery of certified end user security awareness training for staff and contractors.
- House Bill 4390, establishing the Texas Privacy Protection Advisory Council to study privacy laws and updating data breach reporting requirements to the Office of the Attorney General.

Texas has faced many cybersecurity challenges over the past two years – ransomware, web defacements, and denial-of-service attacks – all compounded by the mass remote access necessitated by COVID-19. These and other recent high-profile cybersecurity incidents within the public sector have shown potential for catastrophic impact to public safety and government resources.

The State of Texas has recognized the critical role cybersecurity plays in fulfilling the mission of serving Texans. The Texas Department of Information Resources will continue to elevate the visibility of cybersecurity across the state. It is imperative that Texas stands ready to meet future cyber challenges.

The 2020 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.

Cybersecurity is everyone's responsibility. As the world becomes more connected, we must all do our part to protect our information resources. By taking the right proactive measures, we can continue to serve Texans in a reliable, secure, and efficient manner.

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

## Introduction

Section 2054.0591, Government Code, requires the Texas Department of Information Resources (DIR) to produce a report on 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 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 against adverse impacts of cybersecurity incidents.

**Ransomware (61%) is by far the most common malware category.**

Modern cybersecurity incidents continue to be relentless in volume, velocity and in variety. The 2020 Verizon Data Breach Investigation Report states that 21.4% (6,943) of the global incidents reviewed for last year were in the public sector. Further, of those attacks, 8.8.% (346) were breaches. Ransomware (61%) is by far the most common malware category. A large-scale phishing campaign could infect thousands of government computers with malware or compromise the credentials of its victims. Then a ransomware attack will hold critical data hostage until a payment is delivered, with the threat that years' worth of data will be destroyed. Another risk is that a data breach could make millions of Texans' personal data public and increase the risk of identity theft. Further, a Denial-of-Service attack could render an important web application unusable limiting service availability for citizens and state personnel for an extended period.

**Misconfigurations contribute to 30% of breaches when compared to all security incidents. This is especially evident where organizations are responsible for cloud application security configurations.**

There is more than one way to address incidents and reduce the likelihood of successful attacks. This report provides information on better preparing the state for future cyberattacks. For example, the success of a ransomware attack can be effectively reduced through ongoing security awareness training that informs personnel about the types of attacks and their prevention. Other means would involve ensuring data backups are routinely stored and tested according to organizational specifications and physically or logically separated from the production environment. Misconfigurations contribute to 30% of breaches when compared to all security incidents. This is especially evident where organizations are responsible for cloud application security configurations. This drives the need for continual verification of network devices, servers, applications, and data repository configurations no matter their location.

## Report Highlights

- Security related budgets and the number of agency staff focused on cybersecurity may not be keeping pace with the growing demand for cybersecurity expertise or resources and the sophistication of cyber threats.
- Having an incidence 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 organizations that have an incident response plan, only 52% of Texas state agencies reported a defined exercise schedule to test and potentially improve their incident response capability.
- Educating users and applying protections against cyber threats help greatly reduce risk but compliance with statewide cybersecurity awareness can be improved; 93% of state entities met compliance and 46% of local government entities complied with state mandated cybersecurity awareness training.
- Only 31% of state agencies reported having more than one dedicated information security personnel, resulting in limited 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; they have also had an increasing number of cyber-attacks, including 50 security incidents in 2019.

## Legislative Recommendations

Recommendation 1: Create Security Operations Centers Across Texas

Recommendation 2: Establish a Texas Cybersecurity Incident Response Team

Recommendation 3: Enable a Volunteer Based Incident Response Team

Recommendation 4: Pilot a Shared Information Security Resource Program

Recommendation 5: Establish Mandatory Use of .gov and .edu Domains

Recommendation 6: Establish a Mechanism for Tracking Security Incidents at all Levels of Government

Recommendation 7: Strengthen Security Awareness Training

Recommendation 8: Require Agencies to Include "Authority to Connect" Clauses in Vendor Contracts

Recommendation 9: Establish a Risk and Authorization Management Program (RAMP) for Texas State Agencies and Institutions of Higher Education

# Resource Assessment

## Agency Resources

The State of Texas is a large cybersecurity target due to the sheer number of public sector resources that house sensitive and confidential information. Over 200 state organizations and thousands of local governments organizations make the state a target rich environment. Texas has the potential for many unauthorized connections to access or extract data from the considerable number of organizations' access points.

The state also faces competing priorities and limited resources, which challenges organizations' abilities to prioritize security and adequately prepare for potential adverse impacts from exploitation of information systems. This section provides an overview of how agency personnel support security operations across state government.

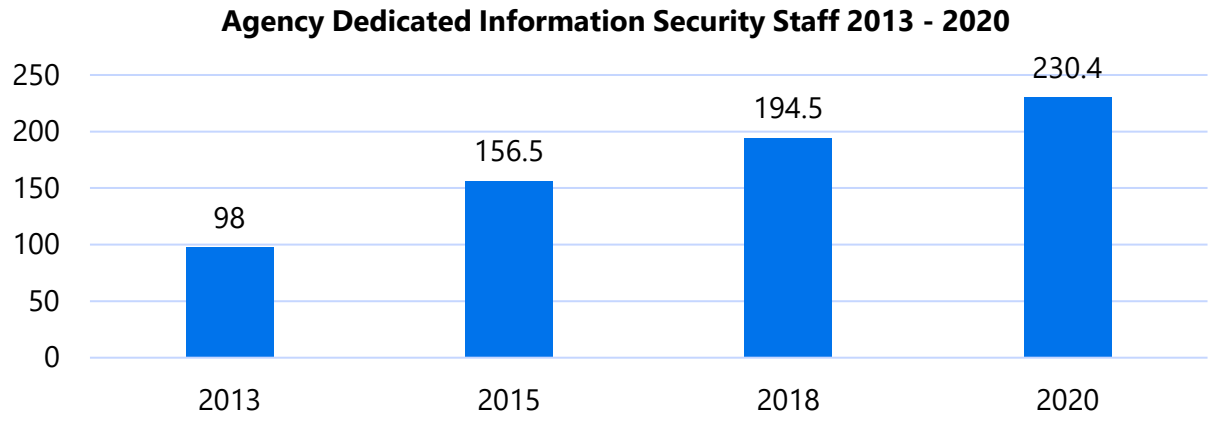
## Agency Cybersecurity Resources

When surveyed, state agencies indicate dedication and commitment to ensuring the security of their information systems. Data shows an increase in security related budgets and the number of agency staff focused on cybersecurity. In addition to increasingly sophisticated threats, the monitoring and detection systems are becoming more sophisticated and require skilled and trained staff to operate, investigate, and remediate potential and identified threats.

In the 2020 Information Resources Deployment Review (IRDR), a biennial technology self-assessment survey, agencies indicated that they continue to make 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 18.2% between the 2018 and 2020. This continued growth indicates an increasing emphasis on information security preparedness and maturity throughout state agencies.

**The number of fully dedicated security professionals employed by agencies rose 18.2% between the 2018 and 2020.**

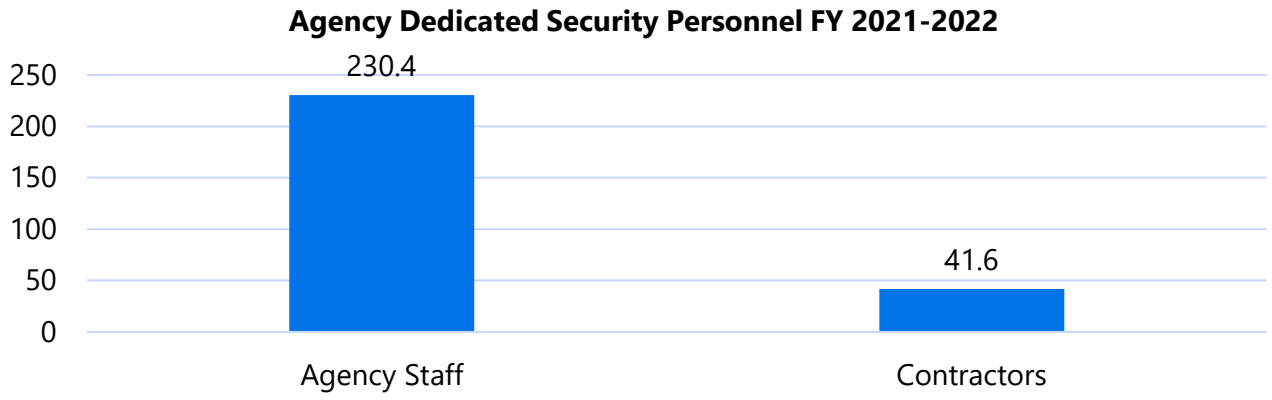
**Figure 1: Number of Agency Information Security Personnel 2013-2020**




Source: 2020 Information Resources Deployment Review

Despite this continued growth, agency staff may not be keeping pace with the growing demand for cybersecurity expertise or resources. In addition to the approximately 230 dedicated cybersecurity professionals, over 41 contractors support state agencies with information security activities. These contracted staff resources may have specific technical skillsets, but are temporary resources assigned to compensate for vacant positions.

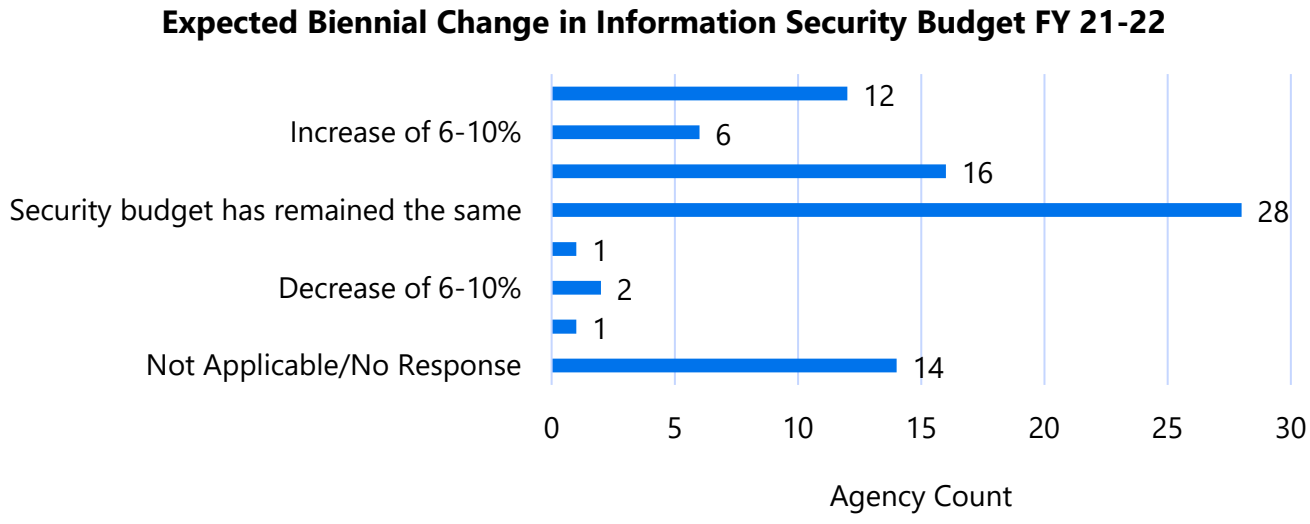
**Figure 2: Agency Information Security Staff and Contractors FY 2021-2022**




Source: 2020 Information Resources Deployment Review

In addition to an increased number of agency security staff and contractors, many agencies report increases in their biennial security budget. In in the 2020 IRDR, 44% of agencies plan to increase their security budget from the last biennium. Continued investment in information security is critical to keep pace with the continually evolving threat landscape.

**Figure 3: Expected Biennial Change in Information Security Budget FY 2021-2022**




Source: 2020 Information Resources Deployment Review

Although security staff resources continue to grow, there is a national trend of state government organizations continuing to rely on outside resources to support their daily operations and their

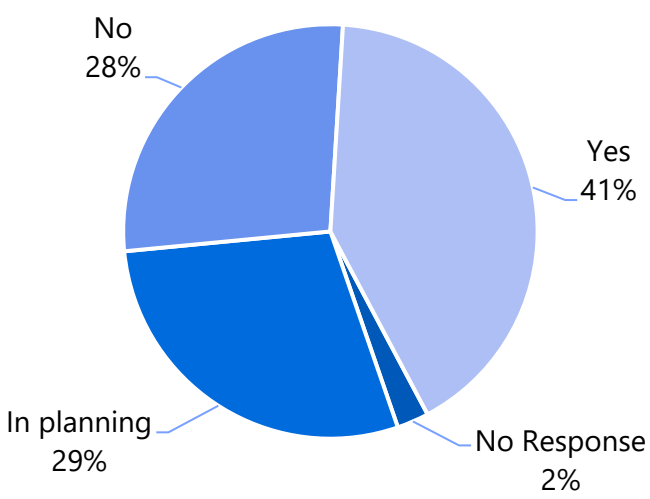
response to major security incidents. The 2019 NASCIO State Chief Information Officer Survey further identified that 53% of the nationwide state government CIOs use brokered services to fill the gap of cybersecurity skills and roles. This trend is generally reflected in the 2020 IRDR. Organizations that experience a major cybersecurity incident, including ransomware, data breach, or other attacks still generally rely on external incident response and recovery resources.

## Agency Cybersecurity Incident Response

In the 2020 IRDR, agencies reported an increase in focus on IT security operations, but most agencies report that they still do not have adequate resources budgeted to respond effectively to a major cybersecurity incident.

The 2020 IRDR indicates 41% of agencies specifically budget adequate resources to address the operational and financial impacts of a cybersecurity incident. This is a three percent increase from the 2018 IRDR findings. Further, 28% of agencies report they do not have adequate resources budgeted, and 29% of agencies are in the planning process to have adequate budgetary resources in place to address a cybersecurity incident.

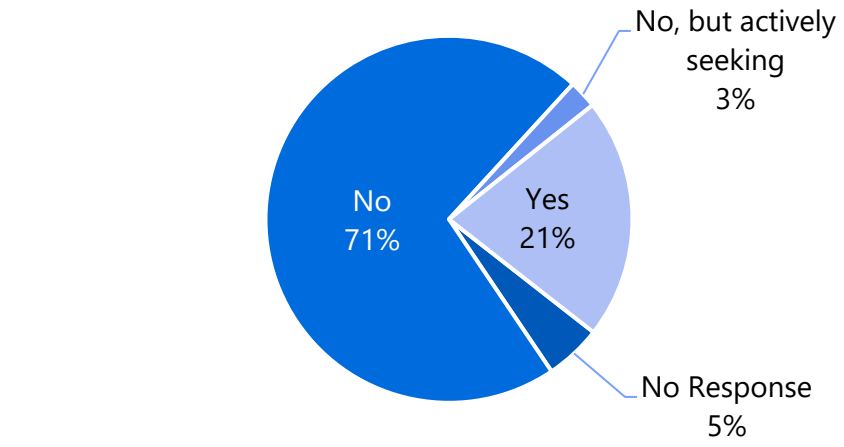
**Figure 4: Percent of State Agencies with Adequate Resources Budgeted for Cyber Incidents**




Source: 2020 Information Resources Deployment Review

In addition to a limited number of organizations reporting adequate resources budgeted to address cybersecurity incidents, 71% of agencies do not have cybersecurity insurance policies, which may help offset the potential costs of cybersecurity incidents in certain situations.

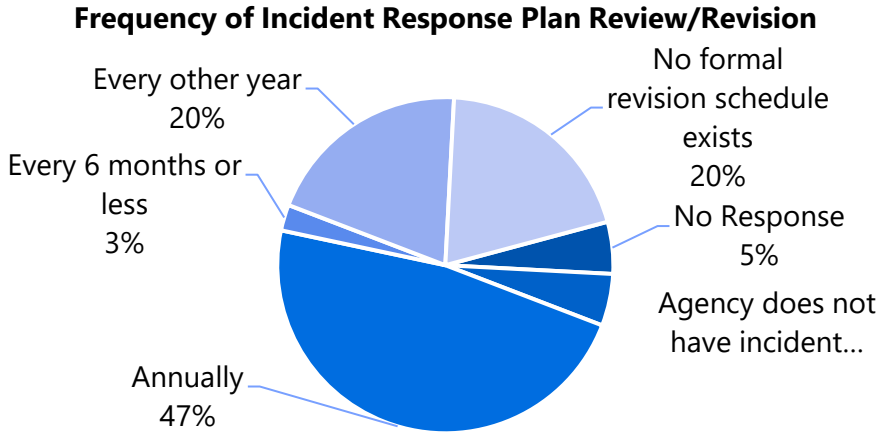
**Figure 5: Percent of State Agencies with Cybersecurity Insurance**




Source: 2020 Information Resources Deployment Review

Incident response planning and review activities are critical to reducing the overall incident costs associated with potential compromises. The 2019 Verizon Data Breach Investigations Report specifically identifies, "Having documented, understood, and tested incident response plans to the real thing will allow the containment process to begin during that first hour to limit the effectiveness and impact through quick identification."

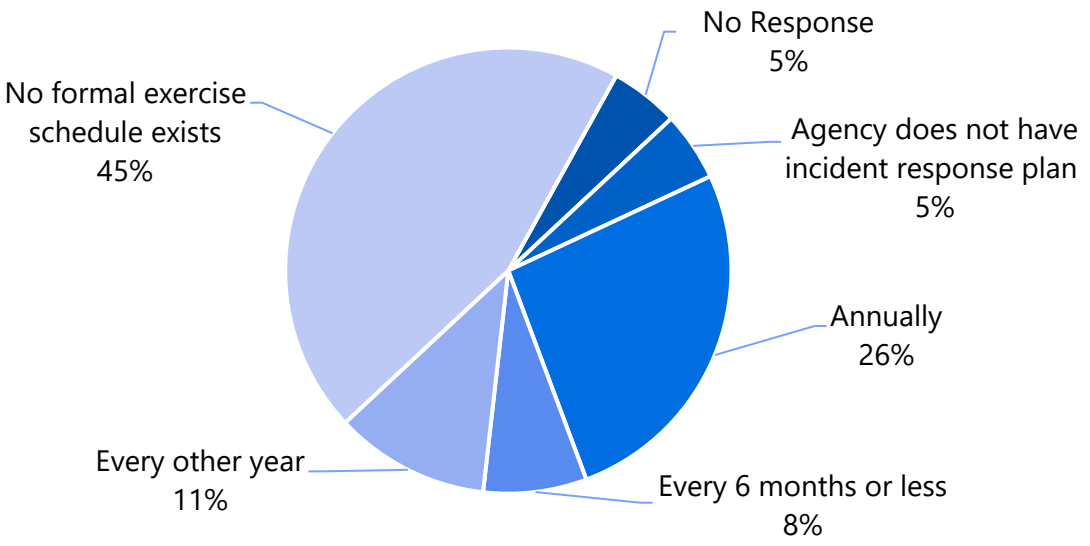
**Figure 6: State Agency Incident Response Plan Revision Frequency**




Source: 2020 Information Resources Deployment Review

Reviewing an incident response plan annually is not enough to support a successful response to cybersecurity incidents. Each incident response plan must be communicated and exercised regularly to realize the full benefits of the planning process. Of the organizations that have an incident response plan, only 45% of agencies reported a defined exercise schedule to test and potentially improve their incident response capability.

**Figure 7: State Agency Incident Response Exercise Frequency**




Source: 2020 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 agency staff resources are fully dedicated to maintaining the safety and security of their information systems. Yet, when cyber-incidents do occur, state agency resources 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*, 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.

### Network Security Operations Center

The DIR Network Security Operations Center (NSOC) provides security services and network monitoring for most state agencies. The NSOC routinely blocks over one billion malicious communication attempts per month. In additional to blocking malicious communications, the NSOC reviews suspected phishing emails and will take appropriate action to help mitigate the email's risk. In calendar year 2019, the NSOC received and reviewed 1,303 suspected or actual email phishing attempts. In addition to baseline security threats, 2020 also saw increases in Advanced Persistent Threat activity, denial of service attacks, ransomware, COVID-19 themed pretexting and other phishing, webpage defacements, and malware.

**In calendar year 2019, the NSOC received and reviewed 1,303 suspected or actual email phishing attempts.**

### DIR Shared Technology Services

DIR's Shared Technology Services (STS) Program provides organizations access to managed IT and security services, which allow program participants to access services with the benefit of central management and pre-negotiated volume-based rates. The Managed Security Services program provides public sector entities with a wide range of proactive and responsive security services. The Next Generation Data Center provides secure cloud, mainframe, print and mail, and security operation services to state organizations. The Texas.gov Digital Identity Solution provides Identity and Access Management solutions such as multifactor authentication and identity proofing for state organizations.

### DIR Managed Security Services

State agencies, institutions of higher education, independent school districts, and local governmental entities may obtain Managed Security Services (MSS) through DIR's Shared Technology Services program. The MSS program offers security services within the categories of risk and compliance, security monitoring and device management, and incident response at pre-negotiated and competitive industry rates. All MSS customers have the option of leveraging the Incident Response offering without having to pay retainer fees. If a cybersecurity incident that requires external assistance were to occur, the agency could quickly deploy a team of highly skilled cyber professionals to assist in the incident response process.

In 2019 and 2020, 373 organizations participated in the MSS program and have engaged MSS resources 617 times since September 1, 2018. These requests for service include:

- 30 incident response requests

- 310 risk and compliance requests
- 254 election security assessments
- 23 orders for security monitoring and device management

Table 1 below identifies the number of customers at each organizational level and the number of requests for MSS services for fiscal years 2019 and 2020.

**Table 1: Managed Security Services by Customer and Engagement**

| Organization Type | Organization Count | Tickets by Organization |
|---|---|---|
| State Agencies | 63 | 251 |
| Higher Education | 28 | 54 |
| Local Government | 259 | 271 |
| K-12 School Districts | 2 | 3 |
| Others | 1 | 1 |
| **Total** | **353** | **580** |

MSS resources have supported the incident response efforts of more than 24 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.

## Next-generation Data Center Services

Six contracts began September 1, 2020 as part of the DIR portfolio of Shared Technology Services for government. These contracts constitute five service towers which collectively provide modern services for Texas government agencies. *Table 2* below 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<br>• Platform-as-a-Service<br>• Software-as-a-Service | • Texas Private Cloud<br>• Facilities<br>• Computing Services | • Technology Services<br>• Project Delivery<br>• Application Management | • Print and Mail Services<br>• Digitization<br>• Digital Records Storage | • Cybersecurity Policy<br>• Monitoring<br>• Incident Management |

The transition to next-generation data center services adds a fourth tower of service offerings. The Security Operations Services tower provides dedicated cybersecurity policies, oversight, and monitoring of the Data Center Services 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.

## Texas.gov Digital Identity Solution

As a result of the 86th legislative session, DIR received funding to implement a Statewide Risk-Based Multifactor Authentication (MFA) program. This program, known as the Digital Identity Solution (DIS), provides a voluntary service that has a specific set of Identity Access Management (IAM) features. The service is available to state agencies and institutions of higher education. As resources permit, MFA should be applied to the high-risk network devices, systems, remote access, and user accounts.

According to the 2019 Verizon Data Breach Investigations Report, exploited system administrator accounts are a top target for threat actors. System administrator or privileged accounts are prime targets for hackers, as those accounts allow threat actors to gain system and network access to carry out successful cyberattacks, often going undetected for weeks or months. MFA is among the best practices to prevent this type of unauthorized access.

**MFA is the practice of authenticating users through the verification of two or more authentication factors.**

MFA is the practice of authenticating users through the verification of two or more authentication factors. This provides an additional layer of security that serves as a failsafe if the primary method of authentication were to be compromised by a malicious actor. MFA prompts users attempting to login with a username and password to authenticate with a second step. This second step can be a push notification of a registered cell phone using a security app, or by entering a code received via test, voice call, or email.

MFA products tend to come with additional capabilities to secure the network and systems, which may include Single Sign-On (SSO) and other security features. Within an MFA implementation, attackers can no longer access the target network through stolen credentials (e.g. single-authentication username and password).

The Digital Identity Solution suite of capabilities include:

- User identity and access management
- Identity gateway for custom system integration
- Centralized employee portal
- Security event logging and reporting
- Secure configuration based on state information security requirements

As of May 2020, state agencies and institutions of higher education may request the Digital Identity Solution, which provides adaptive MFA, SSO capabilities, and resides within a FedRAMP[1] authorized private government cloud for high impact security controls.

[1] https://www.fedramp.gov/

## Texas Cybersecurity Incident Annex

In response to increased cybersecurity incident activity, DIR initiated a multiyear planning effort to develop a statewide cybersecurity incident annex. Started in late 2017, this initiative addressed the statewide concept of operations, assignment of responsibilities, and direction and control methods to coordinate a statewide cybersecurity incident response.

The initiative was tested at an unprecedented scale barely two years after initial planning, when 23 local government entities were simultaneously impacted by a coordinated cyberattack. These local governmental organizations were heavily impacted, losing the ability to conduct basic business services and even to manage their critical infrastructure systems. Based on the planning efforts, DIR was able to coordinate with response partners including the Texas Military Department, Texas Division of Emergency Management, Texas A&M University System, MSS resources, and federal and other private sector partners to implement the cybersecurity incident annex 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.

## Statewide Incident Response Preparedness

The state's incident response plan and state cyber annex was reviewed and revised in 2018. In the past two years, the plan has been executed twice. When a cybersecurity incident warrants the state involvement, the partner agencies identified in the plan can deploy resources and highly skilled teams to contain the situation. In the last statewide cyber incident, the Texas Military Department successfully provided Cyber Protection Mission Ready Package to perform response for impacted government entities. In addition to support, these units conduct in-depth reviews of Texas government cyber programs and make recommendations for strengthening cybersecurity capabilities.

DIR maintains a comprehensive Incident Response Redbook template. This Redbook provides a foundation for organizations to build their internal incident response capability and develop their internal incident 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. The Redbook was revised in coordination with members of the Statewide Incident Response Working Group and the update was published in August 2020.

The Homeland Security Grant Program (HSGP) assists the state with funding to assist in the implementation of the National Preparedness System. Texas utilized HSGP funding for their incident response tabletop exercises, including the 2020 cybersecurity incident response tabletop exercise workshop. Approximately 100 participants from local and state level organizations participated in the March 2020 workshop, where subject matter experts facilitated a ransomware impact scenario. This facilitated discussion highlighted to importance of developing an incident response plan, incorporating senior management, elected officials, legal representatives, and communications staff

into incident response to successfully support an organization wide response to cybersecurity incidents.

## Governance, Risk, and Compliance

State information security standards are set by Texas Administrative Code, Chapter 202 (TAC 202). TAC 202 references the minimum-security controls required for state information systems as outlined in the DIR Control Standards Catalog. 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 provides 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 can provide organizations with a standardized scale to measure their overall information security maturity over time. The Statewide Portal for Enterprise Cybersecurity Threat, Risk, and Incident Management provides state organizations with 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. Section 2054.0594, Government Code, 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 (TxISAO), led by the Texas Cybersecurity Coordinator, acts as a trusted hub for collection and sharing cyber risk information among public and private sector stakeholders. Members of the TxISAO 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 TxISAO also receives cyber threat information from its members, analyzes trends, and issues notifications to improve security awareness. The TxISAO is available to all Texas organizations, whether public, private, or non-profit, at no cost to the organization.

In 2019, DIR partnered with Texas A&M University (TAMU) and the University of Texas at San Antonio (UTSA) to provide Security Operations Center (SOC) services, as well as educational services to TxISAO members. In 2020 DIR created a multiphase plan for expanding services and information sharing, while concurrently working to build private/public partnerships via the TxISAO.

The TxISAO launched a website in 2020 as part of its first development phase. The website contains an informational overview of the TxISAO functions, a public cyber threat reporting form, and a sign-up form for infrastructure sector specific mailing lists so the TxISAO can share cybersecurity information with members. The TxISAO hosts monthly meetings to share content to assist members mature their cybersecurity.

Future initiatives include creating an enhanced information sharing portal to provide participating members easy access to more detailed information on cybersecurity threats, best practices, strategies, and services offered by TxISAO partners. Partnerships with universities are expected to expand to at least three additional universities, making their services available to all entities in the state.

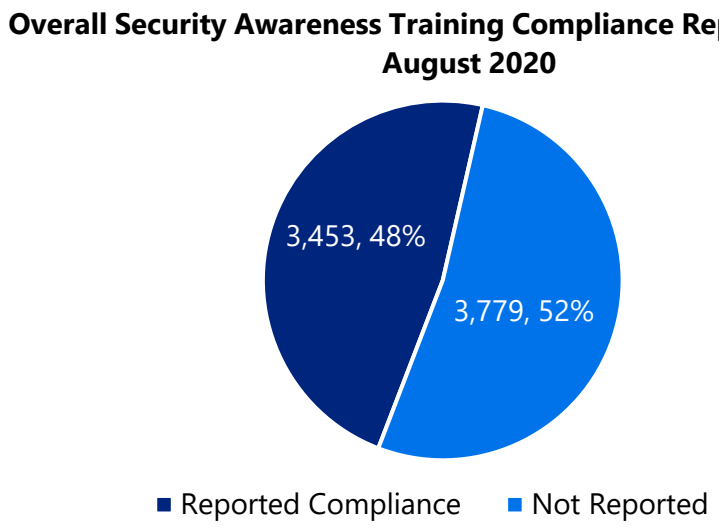
## Cybersecurity Education and Outreach

State agency and higher education information security staff can obtain cybersecurity certification training courses through the DIR provided Texas InfoSec Academy. These courses are provided at no cost to the organization and help enhance the cybersecurity capabilities throughout the state. In April of 2020, DIR added security training for computer software developers to the Texas InfoSec Academy's offerings to train developers in security best practices for application development.

Throughout the month of October, cybersecurity awareness events and presentations are hosted to raise awareness of cybersecurity issues. DIR works with K-12 organizations to host a cybersecurity public service announcement competition and encourage participation in K-12 cybersecurity skill competitions for students. DIR also works with the SANS Institute to encourage high school students to consider cybersecurity as a future career path. In 2020, three Texas students placed second, third, and fourth in the SANS sponsored national competition.

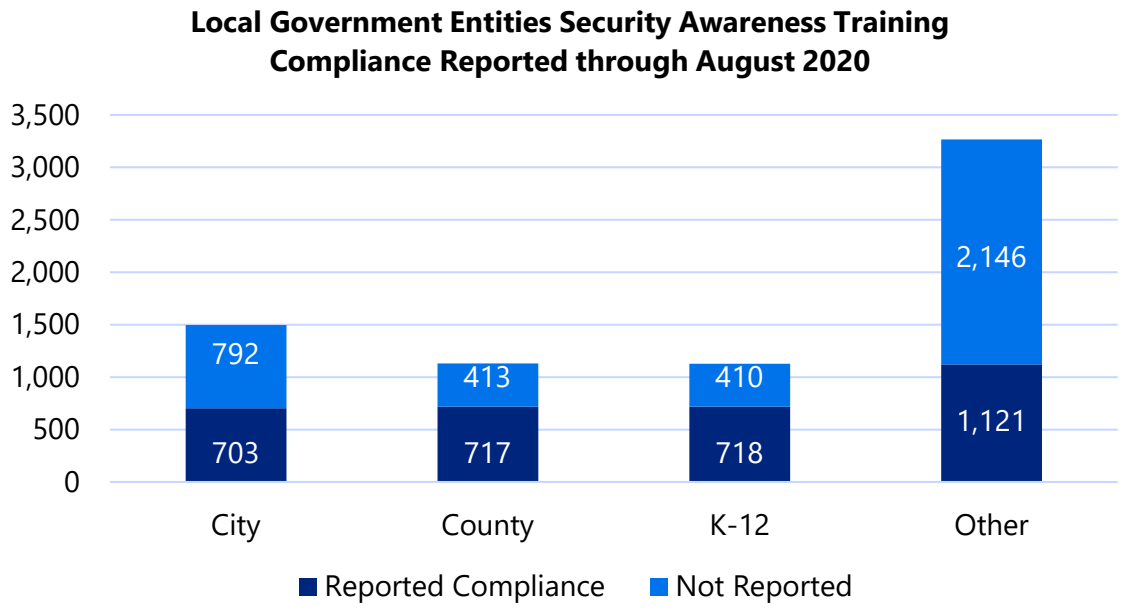
Section 2054.519, Government Code, requires DIR in consultation with the Texas Cybersecurity Council to certify at least five cybersecurity training programs for state and local government employees and requires state and local government employees to complete a certified training program. In 2019, DIR reviewed and certified 125 training programs. DIR also received 3,453 compliance reports from state and local government entities (48% of the 7,232 state and local government entities. *Figure 8, Figure 9,* and *Figure 10* show the compliance reported with training requirements by organization type as of August 2020.

**Figure 8: State and Local Security Awareness Training Reported Compliance**



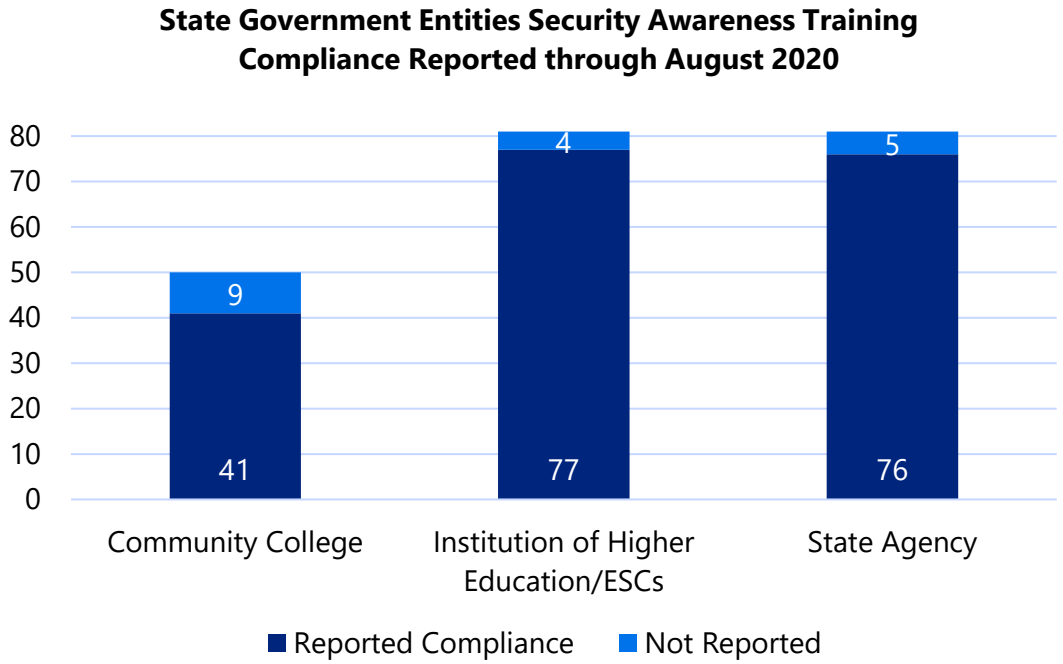

Source: Texas Department of Resources Security Awareness Compliance Reporting

**Figure 9: Local Government Entity Security Awareness Training Reported Compliance**




Source: Texas Department of Resources Security Awareness Compliance Reporting

**Figure 10: State Government Entities Security Awareness Training Reported Compliance**




Source: Texas Department of Resources Security Awareness Compliance Reporting

## Additional Resources

There are several organizations and programs available to public sector entities regarding cybersecurity. Texas governmental organizations may be eligible to supplement their cybersecurity strategy using the following programs and services.

### Texas Municipal League

The Texas Municipal League (TML) is a municipal association that provides resources to and advocates on behalf of local municipal governments in Texas. TML provides a cybersecurity risk pool program to support pre and post breach services to their members.

### Texas Association of Counties

Texas Association of Counties (TAC) is an association that provides resources and services to Texas counties. TAC provides members access to the Risk Management Pool to support pre and post breach services to their members.

### Texas Association of School Boards

The Texas Association of School Boards (TASB) is an association which supports Texas schoolchildren with advocacy, visionary leadership, and high-quality services to school districts. The association provides privacy and information security coverage to their members to assist with breach support and cybersecurity training.

### Credit Monitoring Services Available from Texas SMARTBUY

Members of the Texas SmartBuy program have access to purchase from State of Texas contracts. Membership is available to state agencies, cities, counties, and school districts. The contract provides a mechanism for organizations impacted by a data breach (where personal information is compromised or stolen) to notify their users of the compromise by mail or by telephone call, and to provide both single or triple – bureau monitoring services with restoration and insurance.

### Multi-state Information Sharing and Analysis Organization

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is 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 also take advantage of additional network security monitoring services and their computer emergency response team can provide free incident response services to member organizations including emergency conference calls, forensic and log analyses, mitigation recommendations, and reverse engineering of malicious code.

### Other Federal Resources

The Federal Bureau of Investigation's (FBI) Internet Crime Compliance Center (IC3), Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), the National

Institute for Standards and Technology (NIST), and other Federal agencies may provide additional assistance to governmental entities depending on the nature of the incident.

## Preventive and Recovery Efforts

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

### 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.

### Ransomware Protection

**Dwell Time – 3 Days. In most cases, at least 3 days passed between the first evidence of malicious activity and the ransomware deployment.** Source: FireEye

Ransomware attacks continues to make headlines across the country, and the state of Texas. A ransomware attack uses data encryption to prevent and organization from access 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. Also, Endpoint Detection and Response (EDR) tools are a good defense against ransomware. Organizations should have a plan in place specifically to address ransomware from both a proactive and reactive standpoint.

### Cybersecurity Training

According to the 2019 Verizon Data Breach Investigations Report, malware used in data breaches were delivered through email in 94% of cases. Of the malware used in data breaches, 45% were 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 risks 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 & 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.

The 2020 Verizon Data Breach Investigations Report noted cloud assets were involved in about 24% of breaches, while on-premises assets were involved in 70% of reported breaches. Cloud best practices 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. That standard specifies that cloud solutions should only be placed in a FedRAMP authorized government cloud (GovCloud). These types of environments ensure that all outstanding compliance issues and vulnerabilities are identified, documented, tested, and resolved within a timely manner.

## Improve Boundary Defense & 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 (SSP), 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 & 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 86$^{th}$ legislative session.

## 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

In accordance with Texas Administrative Code (TAC) 202 and Section 2054.0591, Government Code, each state organization (state agencies, public institutions higher education, and community colleges) must designate an Information Security Officer (ISO). This is 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.

In general, the ISO is the individual responsible for the organization's information security program. It is important for an ISO to remain current on relevant information security requirements, applicable risks, threats, and vulnerabilities that pertain to the organization. An ISO has many expected duties, functions, and responsibilities that may include, but are not limited to:

- Develop and maintain agency-wide information security plan
- Develop and maintain information security policies and procedures that address information security requirements and risks
- Work with business and technical resources to ensure that controls are utilized to address all applicable information security requirements and risks
- Provide security awareness and role-based training and direction to personnel with significant information security responsibilities
- Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users
- Ensure that annual security risk assessments are performed, documented, and remediated
- Review the agency's inventory of information systems and related ownership and responsibilities
- Develop and recommend policies and establish 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, or disclosure
- Coordinate the review of data security requirements, specifications, and, if applicable, third-party risk assessment of any new or major computer application change or services that receive, maintain, and/or share confidential and sensitive data
- Verify that security requirements are identified
- Develop risk mitigation plans
- For high impact computer technology and obligate security requirements prior to the purchase of information technology hardware, software, and systems development services that send, receive, maintain, process, and/or share sensitive and confidential data
- Report, at least annually, to the state agency head the status and effectiveness of security controls and vulnerabilities

- Inform designated parties in the event of a security control noncompliance and vulnerability exploitation as per the organization's information security policies, plans, and procedures

## State Information Security Workforce & Challenges

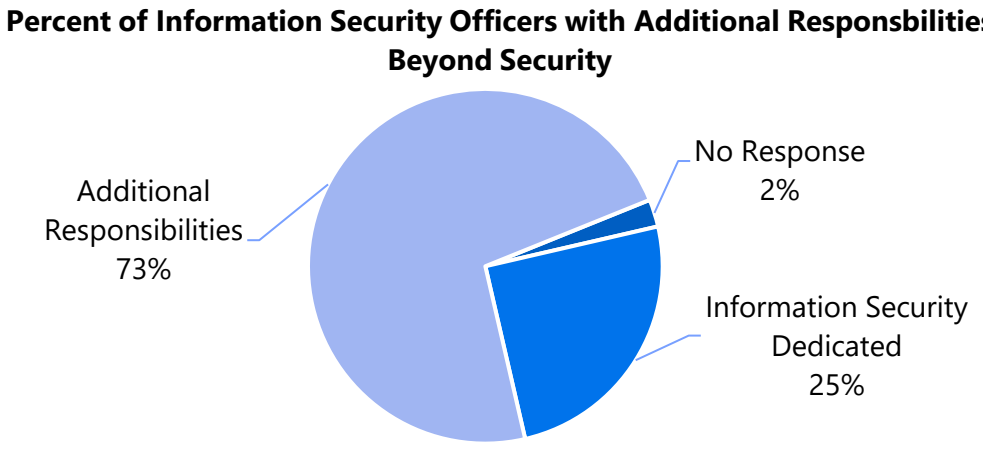
Presently, over 200 state organizations are required to have a designated ISO. While each state organization is required to have a designated ISO, it is not always feasible that the designated individual have information security related duties as their sole or primary function.

The individual designated as ISO for an agency may often serve in other official roles, particularly in smaller agencies where IT budgets and personnel may be limited. This may result in an individual serving in complex roles because it is statutorily required but without the strong familiarity of IT, security best practices, or depth of knowledge and skills to build and maintain effective information security programs. Leveraging an experienced and qualified resource on-demand for planning and risk assessment purposes provides valuable insight for agency decision-makers regarding the often-complex challenges associated with securing information assets.

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.

While each state organization is required to designate an ISO, the person assigned to the role may often have other responsibilities in the organization. In the 2020 IRDR, 73% percent of state agencies reported their Information Security Officer had additional responsibilities outside of information security.

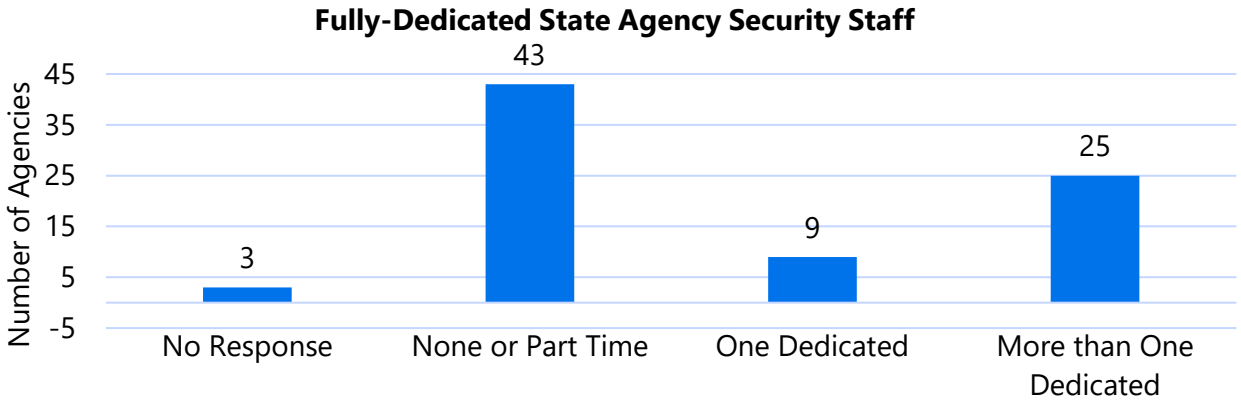
**Figure 11: Percent of State Agency Information Security Officers with Additional Responsibilities**




Source: 2020 Information Resources Deployment Review

According to the 2020 IRDR, only 31% of state agencies reported having more than one dedicated information security personnel. Additionally, 43 agencies reported having fewer than one dedicated (part-time only or none) agency security personnel within their organizations. While the number of overall information security personnel has risen 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* shows the number of information security personnel for state agencies as reported in the 2020 IRDR.

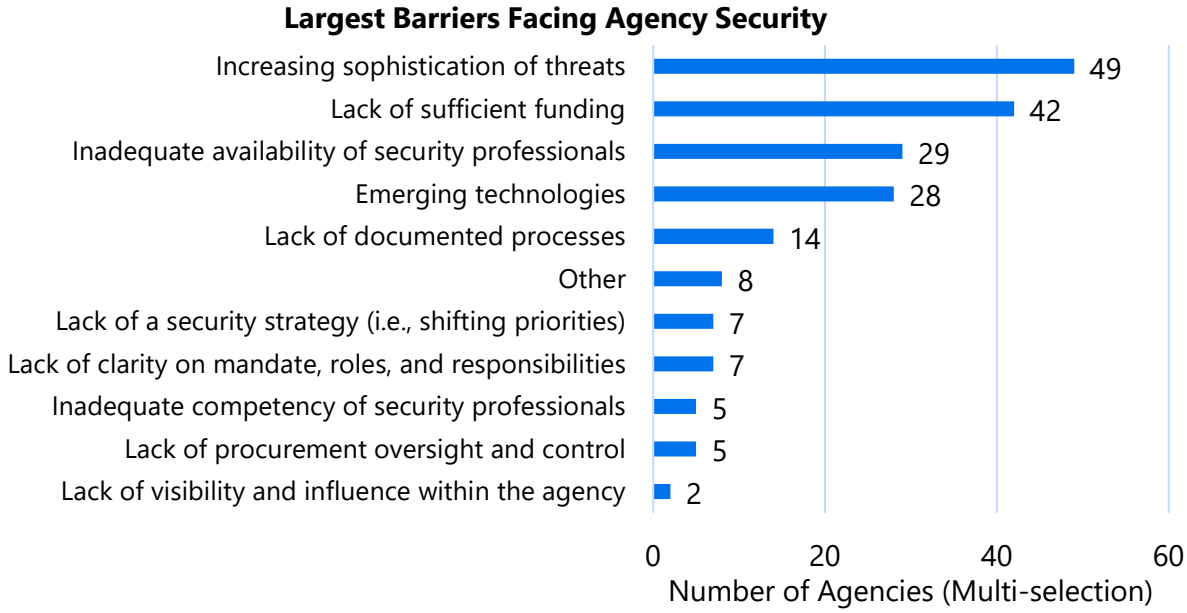
**Figure 12: Number of State Agency Dedicated Information Security Personnel**




Source: 2020 Information Resources Deployment Review

*Figure 13* displays the largest barriers agency face concerning information security as reported in the 2020 IRDR. *Lack of sufficient funding* and *inadequate availability of security professionals* near the top of reported barriers, with only *increasing sophistication of threats* receiving more responses.

**Figure 13: Largest Barriers Facing State Agency Information Security**




Source: 2020 Information Resources Deployment Review

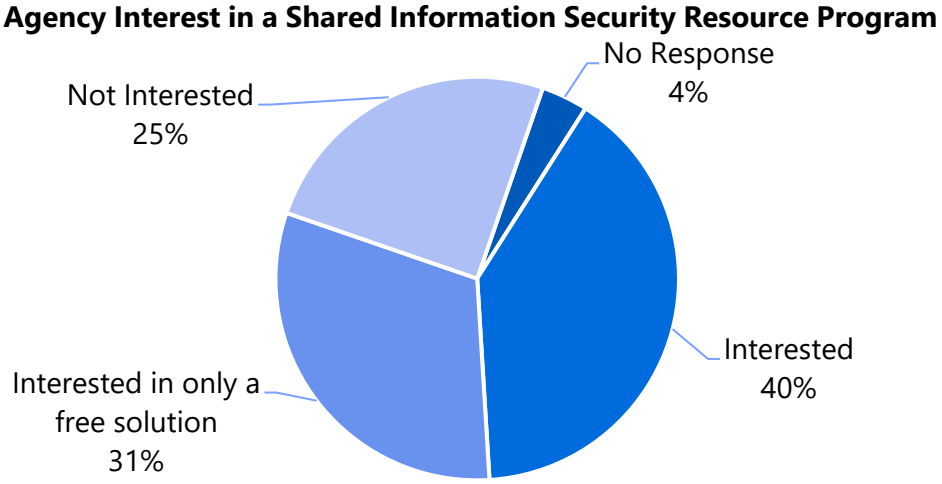
State agencies and higher education organizations may additionally have some, or all, of the following information security program challenges:

- Limited resources or funding
- Cybersecurity knowledge gaps
- Legacy and/or emerging technology skills
- Shortage of information security and cybersecurity staff
- Insufficient role-based security training
- Complying with regulations
- Planning and reporting requirements

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 have responded well to other state-provided resource sharing programs and have expressed interest in an information security resource sharing program. *Figure 14* shows 40% of agencies surveyed in the 2020 IRDR would be interested in a such a program, with an additional 31% interested in a solution if provided at no cost to their organization.

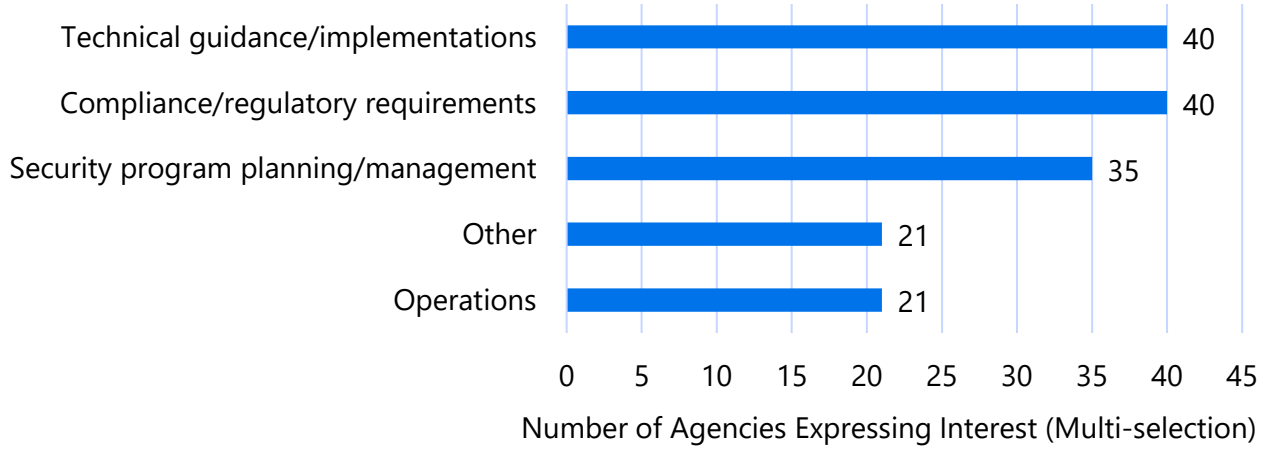
**Figure 14: Agency Interested in Shared ISO Program**




Source: 2020 Information Resources Deployment Review

*Figure 15* displays the areas of support agencies are most interested in obtaining through a shared Information Security Officer or assistance program, with *technical guidance/implementation and compliance/regulatory requirements* as the most desired areas of support.

**Figure 15: Shared Information Security Officer Program Areas of Interest**




Source: 2020 Information Resources Deployment Review

## Local Government Participation

Over the past few years local governments have had an increasing number of cyber-attacks. In 2019, local governments experienced over 50 security incidents 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. With limited resources and without assistance, jurisdictions can become overwhelmed in trying to respond to these attacks. Rather than expending time and resources to better investigate the intrusion methods, impacted entities may simply and rebuild their systems, potentially leaving the existing vulnerability in their systems. Some cities and counties do well to address the growing challenges of security, modernization, innovation, and lending edge applications. However, some are operating with serious security deficiencies; both known and unknown.

Currently, local government entities are not required to follow TAC 202 or to designate an official Information Security Officer. 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 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 could potentially fill the knowledge and skill gaps of the workforce.

## Program Support & Activities

The sharing program would use state information security standards and organization-specific regulations to determine the best practices to be used as guiding principles. Program goals would

focus on facilitating the implementation of information security controls and improving information security maturity.

The provided resources would be technical security leaders that are able to engage and communicate with agency personnel through technology and/or face-to-face meetings to foster the best balance between trust and control within an agency's information security programs. This program would support agency information security strategy, guidance, compliance, and general support within a specified time frame.

The shared resources program staff could also provide the following types of support:

- Brief the current IT threat landscape for state agencies and higher education organizations.
- Verify alignment and compliance with applicable standards, frameworks, laws, and regulations.
- Complete mandatory reporting requirements.
- Review lessons learned report and tracking the after actions of post investigations of incidents.
- Translate knowledge into identifiable risks and create actionable plans to protect information assets.
- Make recommendations to improve identity and access management.
- Review and revise information security policies and procedures.
- Develop and implement a cybersecurity awareness training program.
- Assist with creating and revising cybersecurity strategy.
- Communicate best practices and risks to all parts of the organization.

Participating organizations would continue to hold the ultimate responsibility for their information security and their decisions for that information security program. The provided resource would be accountable to the participating organization but serve in an advisory capacity for the organization's decision-makers.

## Conclusions

The primary goal of an information security resource sharing program is to reduce risk. Legislative consideration of a resource sharing program may help reduce staffing challenges and improve information security capabilities throughout state agencies. The program could provide potential benefits in the form of:

- Improved response time to information security program risks
- Improved availability (quantity and quality) of security professionals
- Minimized short term information security staffing gaps
- Increased agency's information security maturity
- Support for small and medium-sized agencies with resource challenges

The U.S. Bureau of Labor Statistics reports 112,300 security analyst positions as of 2018, with a projected employment change must faster than the average for all occupations at 32%. Competition with the private sector for high-demand skillsets limits the ability to obtain qualified information security staff, and this is particularly difficult for smaller organizations. Smaller government entities may not be able 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
- Number of participating organizations

This shared resource program would allow organizations to distribute the costs of skilled professionals across multiple agencies, which would allow access to expertise that would otherwise be cost-prohibitive.

## Legislative Recommendations

### Recommendation 1: Create Security Operations Centers Across Texas

Create regional Security Operations Centers (SOCs) located at universities or with other governmental entities in different geographically regions across Texas. This would allow for "boots on the ground" close to local governments that may need assistance with major cybersecurity incidents in each region, as well as network security infrastructure that regional governments can utilize. It also contemplates the use of student workers, thereby offsetting staffing costs and simultaneously providing real world training for the needed cybersecurity professionals of the future.

### Recommendation 2: Establish a Texas Cybersecurity Incident Response Team

A statewide Cybersecurity Incident Response Team (CIRT) would receive standardized training and opportunities to assist organizations impacted by cybersecurity incidents. The CIRT would be comprised of information security professionals with the knowledge and capabilities required to contain and resolve security incidents. A CIRT can provide critical services expediently to mitigate the damage during incident scenarios.

### Recommendation 3: Enable a Volunteer-Based Incident Response Team

Government entities may lack the capability or workforce capacity to respond to a cybersecurity incident or budgeted resources to bring in paid third parties.

Amend Subsection 2054.0594 (b), Government Code, to require DIR to consider creating an incident response team of vetted volunteers to assist with responding to cybersecurity events. DIR would also create a framework for Regional Cybersecurity Working Groups (CWG) along with Mutual Aid

Agreements (MAA). These CWGs should be based on the existing Council of Government regions. The incident response teams, CWG, and MAA framework would create a shared talent pool to assist with responding to events across Texas. Public entities could then share resources to assist in recovery processes.

## Recommendation 4: Pilot a Shared Information Security Resource Program

Small agencies and local governments could benefit from the expertise and cost-effectiveness of a resource sharing program. A limited initial implementation of the program would help identify demand, determine optimal staffing ratios, and plan common initiatives to improve workload efficiency. The pilot outcomes could further help define a plan for a large-scale implementation.

## Recommendation 5: Establish Mandatory use of .gov and .edu Domains for Local Government and K-12 School District Websites

During the past year, DIR has discovered several websites that have been set up to mimic local government websites across Texas. The ability to do this is made easier because many local governments and independent school districts do not use the regulated .gov and .edu internet domains. It would make it more difficult to trick citizens to go to a fake website for anything from submitting payments to viewing informal election results by requiring these governmental entities to use the .gov and .edu domains.

## Recommendation 6: Establish a Mechanism for Tracking Cybersecurity Incidents at all Levels of Texas government

Texas Election Code Chapter 279.003 requires that if a county election officer becomes aware of a breach of cybersecurity that impacts election data, the officer shall immediately notify the secretary of state. Texas Education Code Chapter 11.175 requires that the district 's cybersecurity coordinator report to the Texas Education Agency to the agency any cyber-attack or other cybersecurity incident against the district cyberinfrastructure that constitutes a breach of system security as soon as practicable after the discovery of the attack or incident.

This fragmented approach does not enable the state to have knowledge of the overall cybersecurity attack landscape, and therefore leaves Texas unable to fully prepare for cyberattacks across the state. To enable the state to understand the attack landscape and enable pattern tracking, all Texas political subdivisions should be required to report ransomware and other critical incidents to DIR.

## Recommendation 7: Strengthen Security Awareness Training

House Bill 3834 (86R) established statewide security training for all state and local government entities. This legislation differentiated between state and local entities and can be enhanced to further provide training to help improve the security posture of the state and improve the

workforce. This alignment would help ensure that all entities working on public resources, both local and state-wise, have security training.

Amend Subsection 2054.519, Government Code, to align the requirements of state agencies and local governments to:

- Require the training of all contracted entities that access an IT resource, including at a local level.
- Remove the minimum 25% usage requirement placed upon state agencies so that all state employees are trained.
- Remove the cybersecurity coordinator exception for local entities so that DIR verifies that all training programs meet the minimum requirements.
- Require reporting completion of training of all governmental entities.
- Require training of all employees, elected officials, and appointed officials at both state and local entities.
- Stipulate a mechanism to either encourage participation, or to hold agencies, local governments, and their elected and appointed officials that do not comply with legislation accountable.

## Recommendation 8: Require Agencies to Include "Authority to Connect" Clauses in Vendor Contracts

Several major US cybersecurity incidents have been the result of connecting to vendors with poor security controls. Not setting minimum security requirements for contracted entities allows for those entities to have weaker security than the agencies they support, increasing the risk to the state. This proposal includes amending Texas Government Code 2054 to require state agencies to have their contracted entities that access, transmit, utilize, or store state data include clauses that the contracted entity also meet, at minimum, agency defined security controls commensurate to the amount of risk to the agency based on the sensitivity of the data. Additionally, it would require agencies to require entities that access, transmit, utilize, or store state data to periodically provide evidence to the agencies that they are meeting the defined security requirements. Agencies should review this evidence and determine if the contracted entities are issued an authority to connect, granting that entity permission to access, transmit, utilize, or store the state data as per the contract they are executing. Entities that fail to provide sufficient evidence should be required to remediate any shortcomings or lose their authority to connect.

## Recommendation 9: Establish a Risk and Authorization Management Program (RAMP) for Texas State Agencies and Institutions of Higher Education

As more agencies move to the cloud, it is important that cloud vendors have security controls in place to protect Texas' data. DIR is proposing a RAMP program that provides standardized approaches to security assessment, authorization, and continuous monitoring for cloud products and services for those vendors providing services for Texas agencies. While Texas can currently use FedRAMP (federal government's cloud framework), it requires vendors to go through a lengthy expensive process to get certified, adding controls and costs that are not always required based on the value of the data and risk of exposure.

DIR is proposing a RAMP program for Texas to assist state and local government organizations to move to the cloud more securely. This program would require vendors to provide documentation of predetermined controls prior to bidding on or contracting with an agency for cloud services. DIR proposes partnering with other states, possibly through the StateRAMP program, to enable this process. Reciprocity agreements would enable Texas to provide further assertions of cloud security controls while not bearing the full cost of developing and implementing such a program. StateRAMP is an independent not-for-profit organization, with the goal of providing an efficient and cost-effective solution for verifying cyber security of cloud service providers for state and local government. Their goal is to:

- Enable state and local procurement officials to confidently contract with secure third–party cloud service providers in a manner that will not jeopardize government and citizen data,
- Provide a strong framework that saves state and local governments time, money, and personnel from conducting redundant cloud security assessments,
- Make it easier for third–party cloud service providers to work with governments through a clear framework and transferable certification process, and
- Help State and local government cost effectively avoid unnecessary cyber risks.

# Appendix

## List of Tables



## List of Figures



## References

National Association of State Chief Information Officers. (2019). *State CIO Survey.* Retrieved from https://www.nascio.org/wp-content/uploads/2019/11/2019StateCIOSurvey.pdf

Texas Department of Information Resources. (2019). *2020-2024 State Strategic Plan for Information Resources Management.* Retrieved from https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/2020-2024%20State%20Strategic%20Plan%20for%20Information%20Resources%20Management.pdf

Verizon. (2019). *Data Breach Investigations Report.* Retrieved from https://enterprise.verizon.com/resources/reports/dbir/

Verizon. (2020). *Data Breach Investigations Report.* Retrieved from https://www.verizon.com/about/news/verizon-2020-data-breach-investigations-report