2018 CYBERSECURITY REPORT

S.B. 1910, 85R

Texas Department of Information Resources
November 15, 2018

TABLE OF CONTENTS

LETTER FROM THE STATE OF TEXAS CHIEF INFORMATION SECURITY OFFICER

The 85th Texas Legislature demonstrated a significant interest in improving cybersecurity throughout Texas with legislation such as House Bill 8 (Texas Cybersecurity Act), Senate Bill 532, and Senate Bill 1910. Elevating the visibility of cybersecurity and increasing the dialogue with agencies will go a long way to improving the security of state data and systems. Communication and collaboration are imperative to ensuring the state is adequately prepared to meet future cyber challenges, and the State of Texas has recognized the critical role cybersecurity plays in fulfilling our missions.

The progression of technological advancement has increased efficiency in both our work and personal lives, but that same progress comes with new challenges. Cybercriminals and their attacks are becoming more organized and sophisticated every day. To defend and protect state information assets, we need to continually assess and improve our capabilities. Recent high-profile cybersecurity incidents within the public sector have shown potential for catastrophic impact to our safety and resources. Increasing connectedness and reliance on information technology to support society requires effective protections to ensure the systems and information we use for our benefit are not used against us.

The 2018 Cybersecurity Report assesses current resources available for agencies to respond to cybersecurity incidents, identifies preventive and recovery efforts to improve cybersecurity, evaluates tertiary disaster recovery options, evaluates the costs and benefits of cybersecurity insurance, and provides legislative recommendations for improving cybersecurity.

Cybersecurity is our shared responsibility, from the end user to the executive management. As we become more connected it will become even more important that we all do our part to protect our information resources. The future of our state is digital. By taking the right proactive measures, we can help to ensure that we can continue to fulfill our mission to serve the citizens of Texas in a reliable, secure, and efficient manner.

Nancy Rainosek
Chief Information Security Officer
Texas Department of Information Resources

INTRODUCTION

Senate Bill 1910 (85R), requires the Texas Department of Information Resources (DIR) to produce a Cybersecurity Report on the preventive and recovery efforts the state can take to improve cybersecurity. In accordance with this legislation, this report includes:

- An assessment of the resources available to address the operational and financial impacts of a cybersecurity event;
- A review of existing cybersecurity statutes;
- Recommendations for legislative action to protect against the adverse impacts of a cybersecurity event;
- An evaluation of the costs and benefits of cybersecurity insurance; and
- An evaluation of tertiary disaster recovery options.

CYBERSECURITY EVENTS

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 through the use of computer networks that results in an actual or potentially adverse effect on an information system and/or the information residing therein. For the purposes of this report the term *cybersecurity event* will be used interchangeably with the term *cybersecurity incident*.

Cybersecurity incidents can manifest in many ways with varying levels of severity. For example, a Denial-of-Service (DoS) attack could render an important public-facing web application unusable limiting service availability for citizens in need for an extended period. A successful ransomware attack could hold critical data hostage until a payment is delivered. Code injected through an insecure web form could provide an attacker with sensitive or confidential personal information. A large-scale phishing campaign could infect thousands of government computers with malware or compromise the credentials of its victims.

These are just a few of the common cyberattacks governments and businesses face daily, and each case presents unique challenges and concerns. The fiscal impacts of a cyberattack can vary greatly as well, ranging from a few hundred to billions of dollars. The *2018 Cost of a Data Breach Report*[1] determined that the average total cost of a data breach across all industry sectors to be $3.86 million with an average cost of $148 per stolen record. The public sector cost of a breach is the lowest identified at $75 per record, with the health sector having the highest costs at $408 per record.

$75

PUBLIC SECTOR AVERAGE PER RECORD BREACH COST

Regardless of the varying costs across industries, the government has an obligation to protect the information entrusted to it. While data breaches are of great concern, they should not be the only type of cybersecurity incident considered. Denial-of-Service, cryptojacking, ransomware, and other attacks can strain resources without necessarily compromising data. The considerations presented in this report can be applied to various impacts of cybersecurity incidents.

$3.86 Million

Average Cost of a Data Breach Across All Sectors

[1] 2018 Cost of a Data Breach Study, Ponemon Institute.

RESOURCE ASSESSMENT

AGENCY RESOURCES

The state of Texas is a particularly large target for cyberattacks due to the nature of the public sector and sheer volume of its resources and information. The DIR Network Security Operations Center (NSOC) routinely blocks billions of malicious communications attempts every month. With an attack surface this large, and facing competing priorities and limited resources, it can be a challenge for organizations to adequately budget and prepare for the potential adverse impacts of a successful exploitation of an information system. Of the state agencies surveyed in the biennial Information Resources Deployment Review (IRDR), only 36% responded that they specifically budget adequate resources to address the operational and financial impacts of a cybersecurity incident.

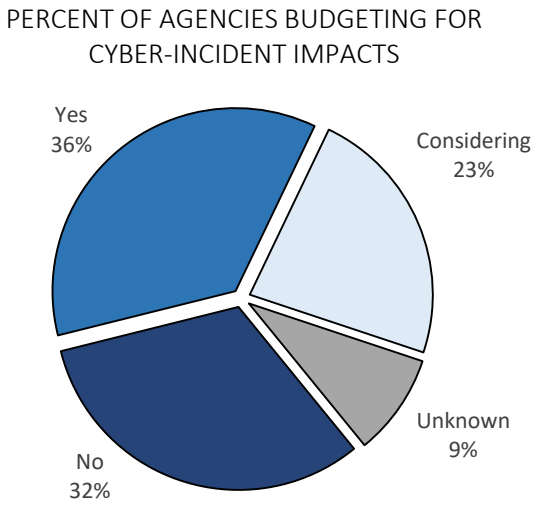


FIGURE 1: PERCENT OF AGENCIES THAT BUDGET FOR INCIDENT IMPACTS

However, the same 2018 IRDR survey indicates that agencies are focusing more on cybersecurity than in years past. The number of fully-dedicated security professionals employed by agencies has risen 24% from 2015 to 2018, and nearly three quarters of agencies claim to set funding by analyzing risks. These figures indicate an increasing emphasis on information security preparedness and maturity throughout state agencies. Agencies identified security awareness and training, risk assessments, data protection/loss prevention, and disaster recovery/continuity of operations planning as the top security initiatives over the next biennium. Agencies reported increasing sophistication of threats, lack of sufficient funding, inadequate availability of security professionals, and emerging technologies as the largest barriers to addressing cybersecurity.

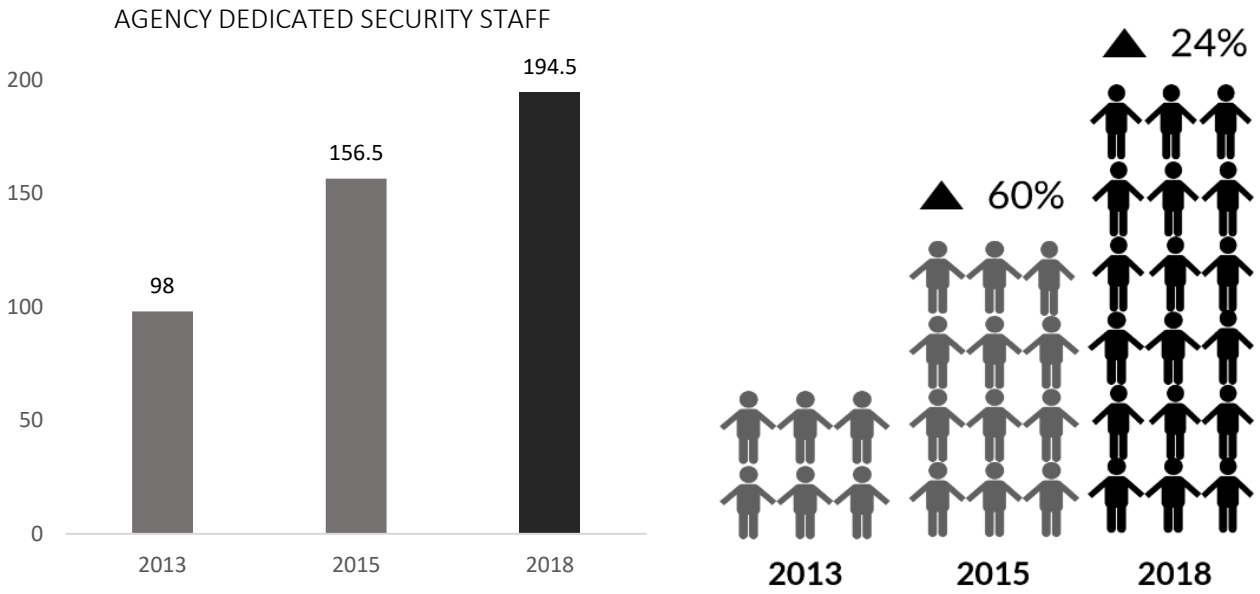


FIGURE 2: COUNT OF AGENCY FULL-TIME INFORMATION SECURITY STAFF

Additional Resources

There are several organizations and programs available to public sector entities regarding cybersecurity in addition to their individual resources and capabilities. Texas governmental organizations may elect to supplement their cybersecurity strategy using the following programs and services.

DIR Managed Security Services

As of March 1, 2018, state agencies, institutions of higher education, and local governmental entities can obtain Managed Security Services (MSS) through DIR's Shared Technology Services program. The MSS program offers a wide range of 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 were to occur that requires external assistance, the agency could quickly deploy a team of highly skilled cyber professionals to assist in the incident response process.

Statewide Portal for Enterprise Threat, Risk, and Incident Management

The Statewide Portal for Enterprise Threat, Risk, and Incident Management (SPECTRIM) is DIR's governance, risk, and compliance system available to state agencies and institutions of higher education. The SPECTRIM portal offers incident management and tracking capabilities that allow users to monitor and collaborate on incident response workflows from identification to eradication.

Incident Response Preparedness Resources and Training

In 2018, DIR published a comprehensive *Incident Response Redbook* that provides a foundation for organizations to develop their internal incident response plans. The Incident Response Redbook contains templates, guides, and additional resources based on industry best practices that can be adopted and tailored to suit the unique needs of individual organizations.

State agency and institutions of higher education information security staff can obtain cybersecurity certification training courses through the Texas InfoSec Academy. These courses are provided at no cost to the organization by DIR and help enhance the cybersecurity capabilities throughout the state.

Additionally, the Information Security Working Group comprised of Texas state government security staff meet monthly to review tabletop security and incident response scenarios.

Cybersecurity Emergency Funding

In 2017, the Texas Legislature authorized DIR to request that the governor or the Legislative Budget Board make a proposal to provide funding to manage the operational and financial impacts if a cybersecurity event creates a need for emergency funding. Should an agency's cybersecurity event rise to the level of emergency, this fund source may be used to help address and remediate the adverse effects of a widespread catastrophe.

DIR SHARED TECHNOLOGY SERVICES

DIR manages the IT infrastructure for many state agency customers through the Shared Technology Services program. The Texas Consolidated Data Center offers secure connectivity to multiple public and government clouds. The two state data centers offer storage, disaster recovery, and redundancy in fully-managed, 24x7x365 facilities that include redundant power, networking, business continuity, and enhanced physical security. These services are backed up with a fully redundant data center along with detailed business continuity and disaster recovery plans.

STATEWIDE INCIDENT RESPONSE

DIR has partnered with the Texas Military Department (TMD) and the Texas Department of Public Safety to develop a statewide approach to handling cybersecurity incidents. If a cybersecurity incident warrants an intervention, the partner agencies can readily deploy resources and highly skilled teams to contain the situation. TMD can also provide Cyber Protection Team assessments for government entities. These units conduct in-depth reviews of Texas government cyber programs and make recommendations for strengthening cybersecurity capabilities.

INCIDENT RESPONSE GUIDANCE

The DIR Office of the Chief Information Security Officer (OCISO) and NSOC work with targeted customer agencies in a coordinated response to resolve cyber incidents. Agencies must report major cyber incidents to DIR within 48-hours of discovering a suspected or actual breach. The OCISO and NSOC can provide agencies with guidance and work with affected agencies to assist in incident resolution.

TEXAS INFORMATION SHARING AND ANALYSIS ORGANIZATION

House Bill 8 (85R), requires DIR to establish an information sharing and analysis center to provide a forum for state agencies to share information regarding cybersecurity threats, best practices, and remediation strategies. DIR's Texas Cybersecurity Coordinator is leading the development of the organization, which is expected to be operational in 2019.

MULTI-STATE INFORMATION SHARING AND ANALYSIS CENTER

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 prevention, protection, response and recovery. Governmental members of the MS-ISAC can take advantage of additional network security monitoring services, industry news, and advisory publications. The MS-ISAC Computer Emergency Response Team can provide free incident response services to SLTT organizations including emergency conference calls, forensic and log analyses, mitigation recommendations, and reverse engineering.

MS-ISAC
Multi-State Information Sharing & Analysis Center

FEDERAL RESOURCES

The Federal Bureau of Investigation's Internet Crime Compliance Center (IC3), Department of Homeland Security's National Cybersecurity Communications Integration Center (NCCIC) and U.S.-Computer Emergency Readiness Team (US-CERT), 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. Resources specifically identified for SLTT governments can be found on the US-CERT website.

PREVENTIVE AND RECOVERY EFFORTS

OVERVIEW

While the ability to address the impacts of a cyberattack is critically important, taking precautions to reduce the likelihood of a successful cyberattack and proactively minimizing potential damage helps prevent the need to address the impacts of a cyberattack in the first place. The following are a few initiatives the state or individual organizations can undertake 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 know 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 applications and software 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. This insight into the systems and devices that process and store sensitive and confidential data can help management make informed decisions about the controls to provide across the network in a cost-efficient manner.

RISK-BASED MULTI-FACTOR AUTHENTICATION

Multi-factor authentication (MFA) is the practice of authenticating users through the verification of at least two of the following types of authentication factors: knowledge factors, such as a password; possession factors, such as a hardware or software token; or inherence factors, such as a fingerprint. Implementing MFA means that attackers attempting to leverage stolen credentials face significantly more difficulty than if they were to obtain a single-authentication username and password. The *Verizon 2018 Data Breach Investigations Report*[2] (DBIR) identified system administrators as the top type of internal actors involved in breaches in 2018. These privileged accounts are prime targets for hackers, as gaining this level of access often permits behavior necessary to execute a successful cyberattack. Multi-factor authentication is a best practice across enterprises, however as resources permit, MFA should be applied to the systems and user accounts that would most substantially reduce risk.

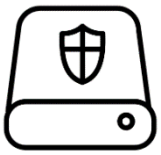
ROUTINE BACKUPS AND TESTING

Ransomware attacks continues to make headlines across the country. A ransomware attack involves an organization's data being encrypted or stolen and subsequently held hostage by an attacker, who then requires some form of payment or action in return for the data or decryption key. Additionally, 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 separately from the live systems.

[2] Verizon 2018 Data Breach Investigations Report

FULL DISK ENCRYPTION

With the rise of mobile computing, it is inevitable that laptops and other devices will be stolen or misplaced. While storing sensitive or confidential information on the local drive of these devices is generally discouraged, completely encrypting the local drives of machines that store sensitive or confidential information can prevent unauthorized access to the data should the computer be lost or stolen.



EFFECTIVE CYBERSECURITY TRAINING

According to the 2018 DBIR, phishing and pretexting (e.g. misrepresentation of identity to obtain trust or compliance) represent 90% of social engineering incidents and 93% of breaches, with email continuing to be the most common vector (96%). Additionally, the public sector tops the list of industries when it comes to breaches attributed to social engineering. Although common belief holds that no amount of training can fully eliminate successful phishing attacks, educating users and applying protections against these types of threats can help greatly reduce risk and attack surface. Frequently targeted groups such as executives and IT staff should not be overlooked. It is especially important that these individuals receive appropriate training and become primed 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. Consider implementing an executive-focused cybersecurity awareness training course or program.

CONTINUOUS VULNERABILITY MANAGEMENT

The cybersecurity threat landscape and attack vectors change rapidly. System or software vulnerabilities are exploited or identified, remediations are performed, new vulnerabilities are exposed, 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 should seek to adopt 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. Eligible customers may qualify for certain services at DIR's cost through DIR's MSS program.

SECURE APPLICATION DEVELOPMENT AND TESTING

It is important to develop applications with security in mind throughout the software development life cycle and perform comprehensive testing prior to moving the application into production. While not every developer can be an information security expert, 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.

INCIDENT RESPONSE PLANNING AND EXERCISES

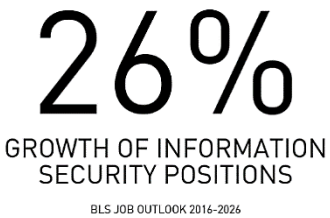
The difficulty of predicting the details of a cyberattack makes it challenging to fully prepare to respond to an incident when the time comes. When, where, and how a cyberattack will occur are primarily determined by factors outside of an organization's control. Having a general plan of action to address 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 ASSURANCE

Whether using a managed service, moving applications to the cloud, or procuring off-the-shelf software, there is a growing reliance on other 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, and acceptable use agreements 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 and documented.

CYBERSECURITY COMPENSATION AND CLASSIFICATION JOB ANALYSES

The Bureau of Labor Statistics (BLS) cites the 2016-2026 job outlook for Information Security Analysts as growing much faster than average at an increase of 26%[3]. In May of 2017, the BLS indicated the national median salary for Information Security Analysts was $95,510 per year, while the Texas State Auditor's Electronic Classification Analysis System indicates the median pay for comparable job classifications (Cybersecurity Analysts and IT Security Analysts) for FY17 was $84,600 per year. To ensure the state remains competitive with a rapidly expanding demand for competent security professionals, a review of the current workforce capabilities and anticipated future demands for cybersecurity knowledge, skills, and abilities should be conducted with recommendations for ensuring the state of Texas can attract and retain an elite cybersecurity workforce over the next decade.



INDEPENDENT CYBERSECURITY EXPENDITURE TRACKING

Currently, the state's budgeting and expense tracking processes do not fully differentiate between information technology purchases and cybersecurity purchases. While there is a degree of overlap between the two categories, it can be difficult to determine the state's return on investment for cybersecurity purchases without the ability to separate technology purchases into a more discrete cybersecurity category.

EVALUATION OF EMERGING TECHNOLOGIES

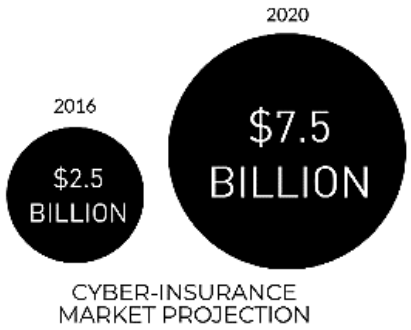
With better protection, monitoring, and alerting, an agency is better able to respond quickly and efficiently to cyber threats. Artificial intelligence, machine learning, network forensic tools, and other technologies are innovative approaches that offer potential benefits that, if implemented appropriately, may greatly improve an agency's security program effectiveness. However, different tools have their own strengths and weaknesses. To obtain the most comprehensive view of the threats facing an organization, multiple tools and strategies must be evaluated and understood before implementation.

[3] 2016-2020 Job Outlook Report, Bureau of Labor Statistics.

COSTS AND BENEFITS OF CYBERSECURITY INSURANCE

OVERVIEW

Traditional commercial general liability policies typically exclude cybersecurity risks from their terms, leading to the emergence of cybersecurity insurance as a stand-alone line of coverage. Cybersecurity insurance (cyber-insurance) is designed to mitigate losses from the impacts of various cyber incidents, such as data breaches, business interruptions, and network damage. The National Association of Insurance Commissioners stated in a 2017 report that the overall U.S. market for cyber-insurance was roughly $2.49 billion, with substantial potential for growth up to $7.5 billion projected by the end of the decade[4]. With projections like this, the cyber-insurance market is garnering the attention of insurance and technology professionals alike worldwide.



CYBER-INSURANCE MARKET PROJECTION

Cyber-insurance has evolved in recent years to take on many forms and continues to mature as adoption becomes more widespread. Offerings can take the form of privacy and data breach coverage, business interruption and restoration costs, network security claims, media liability, regulatory costs coverage, cyber extortion, crisis communication, hacker theft, consultant services, e-payments, regulatory fines, notification costs, response costs, and more.

In many cases, cyber-insurance can be thought of in the same light as most other forms of insurance. An organization pays a premium which maintains agreed upon terms of coverage that are often subject to an annual aggregate limit and deductible. A key difference between cyber-insurance and other forms of insurance is the degree of variability in policies between providers. Whereas more established forms of insurance have gravitated towards standardization, cyber-insurance policies have mainly been underwritten uniquely for organizations seeking coverage.

Some of the most common types of coverage in cybersecurity liability insurance policies include:

- ***Business Interruption Coverage*** – provides coverage for lost business experienced during and immediately following a data breach.
- ***Breach Response Coverage*** – covers the costs for legal consultation with breach response experts, digital forensics expenses, public relations consulting, notification costs, credit monitoring, and other breach-related incurrences.
- ***Cyber Extortion/Ransomware Coverage*** – allows funds to pay for the ransom or extortion demand and related expenses such as the fee for a negotiator or expert to attempt to regain control.
- ***Data Breach and Privacy Crisis Management*** – includes expenses for general incident management such as investigation, remediation, notification, and, credit monitoring and alerting.

[4] 2017 NAIC Report on the Cybersecurity Insurance Coverage Supplement.

- ***Fiduciary Liability Coverage*** – protects in the event a data breach requires expedient notification or carries strict penalties for violation of a law.
- ***Media Liability Coverage*** – provides coverage for legal defense costs arising out of claims alleging libel, slander, or infringement of intellectual property.
- ***Professional Liability Coverage*** – provides coverage for legal defense costs arising out of negligence claims in providing a professional service such as consulting or software development.

38%
OF STATES HAVE CYBER-INSURANCE POLICIES

Some states have adopted policies for cyber-insurance to assist in reducing the risk not directly under the control of the agency that owns the data, such as the case in contracting with a cloud-provider that cannot provide assurance of meeting a certain level of data protection. In the case provided, minimum cyber insurance liability coverage was determined based on the number of protected records associated with the service. Other states have held more global statewide policies covering multiple agencies for several years. The National Association of State Chief Information Officers (NASCIO) *2017 State CIO Survey* reports that the amount of states with cybersecurity insurance policies is on the rise. The survey shows a 18% increase in cyber insurance across states, with 20% of states having cyber insurance in 2015 and 38% in 2017[5]. Although there is little information about the effectiveness of cyber-insurance policies within the public sector due to the relatively recent emergence of offerings, a few states specifically mentioned the following potential benefits that Texas should explore:

- ***Immediacy of response*** – Cyber insurance companies have contracts in place to quickly stand up a call center or provide identity theft protection in the event of a significant breach. Standing up these services quickly could prove to be difficult in a public sector environment, and a slower response could ultimately mean a costlier breach.
- ***Determination of culpability*** – When two drivers have a collision, auto insurance companies will investigate to determine who is culpable for the accident. Similarly, cyber-insurance companies will perform due diligence to determine who is culpable or responsible for a breach. Having an insurance policy in place could save the state the burden of determining fault and potential litigation costs in the event of a breach at a vendor facility, particularly when there are multiple service providers involved.
- ***Unbudgeted expenditures*** – Due to the nature of the public sector it can be challenging to secure the funds to handle the aftereffects of a cyber incident in an expedient manner. A single incident has the potential to demand an entire biennium's worth of budgeted funds. Insurance policies may help mitigate the potential of drained resources due to an incident.

Texas agencies and institutions of higher education have shown little activity regarding cyber-insurance. An August 2018 informal survey of Information Security Officers found that roughly two-thirds of respondents were not considering a cybersecurity insurance policy at this time. Of the respondents who have or are considering a cyber-insurance policy, the most sought category of coverage included breach response and extortion/ransomware coverage with liability amounts ranging from $50,000 to more than $10 million. Responding agencies also raised concerns about burdensome underwriting,

[5] NASCIO 2017 State CIO Survey

existence of policy loopholes, challenges of decentralized organizational structures, and the relative immaturity of the cyber-insurance market.

While the frequency in which a cybersecurity incident results in a confirmed data breach is low relative to the total number of incidents recorded, the financial and operational impacts of a breach have the potential to be enormous and persistent. Agencies should weigh the costs and benefits in conjunction with their unique characteristics to make the determination as to whether cyber-insurance is the right choice.

Costs & Considerations

Premiums for cyber-insurance vary depending on the size of the organization, the type of information it possesses, industry, maturity of security programs, and other factors. As someone with a good driving record may be offered a lower premium for similar coverage, so may an organization that has a more mature cybersecurity program.

Insurance policies are often written narrowly, so it is important to understand the parameters of the policy including what is and what is not covered, partial-coverage, or the factors or circumstances that could negate the coverage entirely (such as policy holder negligence or *force majeure* clauses). It may also be beneficial to work with an independent underwriter to ensure the policy is clearly understood and aligned with the organization's cybersecurity strategy. Consider pursuing a manuscript policy in lieu of the standard policy offerings. Manuscript policies are specifically written to include coverage or conditions not included in a standard policy and may be more tailored to the organization's needs. These policies can also introduce confusion, so it is important to have the appropriate expertise involved in the development and implementation of such a policy.

Although less significant than the policy itself, there may be reputational concerns to weigh when evaluating cyber-insurance options. When a breach occurs, people may question whether preventative measures against the breach would have been more beneficial than buying insurance and writing off losses. Alternatively, cyber-insurance may be perceived as something deployed by a more mature security program that understands where the risks are and can demonstrate a level of security competency that allow for an affordable cyber-insurance policy. Clearly communicating how cybersecurity insurance adds value to the organization can help preempt negative reactions from outside the organization.

Organizations should also consider which divisions and budget categories would be responsible for funding cyber-insurance. Information technology and security budgets are already constrained, and some may see cyber-insurance as a luxury that allocates money to uncertainty and draws limited resources away from real and present issues. Allocating funds to cyber-insurance and away from improving internal capabilities may also be perceived as merely transferring risk, rather than addressing it and doing the most to protect sensitive and confidential information.

Depending on the complexity and magnitude of the coverage, cyber-insurance may require the organization to hire additional staff or reallocate current staff to the management and administration of the insurance policies. While cyber-insurance may not warrant the addition of an entire full-time equivalent employee, it is likely that there will be some administrative requirements to ensure the policies maintain the intended level of coverage.

From a statewide perspective, the variability in individual agency security maturity, applicable regulations, and types of data may result in a higher premium than the industry average. A statewide or multiple-agency policy may result in cost savings through volume discounts, but the uncertainty of covering various agencies with differing needs may increase premiums and outweigh potential savings.

BENEFITS

Whether cyber-insurance will be beneficial to an organization is largely dependent on the characteristics of the organization, the terms of the policy, and the probability of adverse incident outcomes. The impacts of a cyber incident or data breach vary from case to case, which makes generalizing the benefits of cyber-insurance difficult. However, existing research provides industry-level average costs per breached record, although true costs may vary significantly from industry averages.

The *2018 Cost of a Data Breach Report* identified 22 factors that contribute to the per capita cost of a data breach. Factors were determined to be either cost-additive factors (meaning presence of that factor typically increased the per capita cost of the breach) or cost-savings factors (meaning presence of that factor typically decreased the per capita cost of the breach).

The study found that having an *incident response team* and *using encryption* resulted in the greatest amount of cost savings associated with breach costs. On average, presence of the *incident response team* factor was associated with a decrease of $14 per capita and the presence of the *encryption* factor was associated with a decrease of $13 per capita. This means that using the average $148 per capita cost as a starting point, an organization with a strong incident response team could expect to experience lower per capita breach costs with an average of $134 per record prior to accounting for any additional factors.

When looking at the cost-additive factors, *third-party involvement* and *extensive cloud migration* were associated with $13 and $12 increases to the per capita cost of a data breach respectively. In this case with all other factors being equal, *third party involvement* would be associated with an increase from the average per capita cost of $148 to $161.

The factor *insurance protection* fell into the cost-savings category, with a relatively small impact on the per capita cost of a data breach. Insurance protection reduced the per capita cost by $4.80 on average, which may not be as significant as other cost savings factors such as having an effective incident response team but can go a long way when the number of records compromised is large.

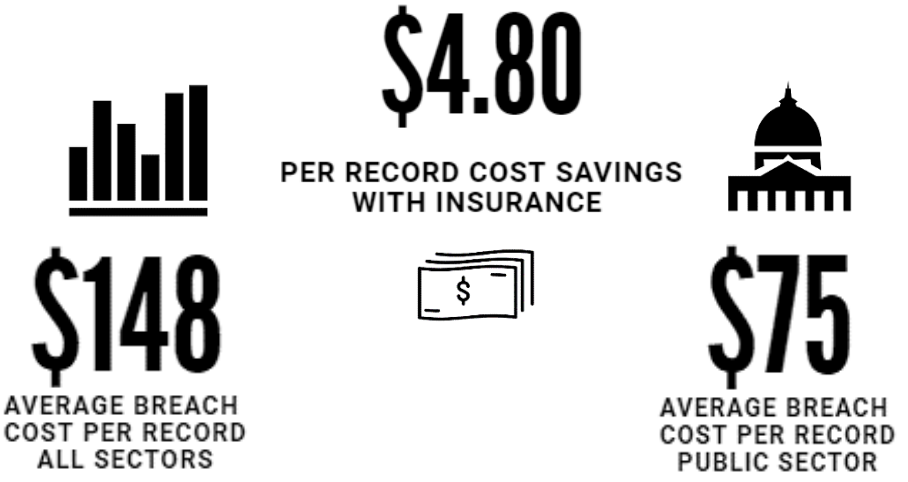


Table 1 illustrates a high-level comparison of the costs of a data breach using the data provided in the *2018 Cost of a Data Breach Report*. The difference in average total costs compared to total costs adjusted for insurance highlights the impact of a relatively small cost savings factor as the number of records increases.

TABLE 1: PER CAPITA COSTS OF A DATA BREACH, ADJUSTED FOR INSURANCE (ROUNDED)

NUMBER OF RECORDS	AVERAGE COST PER RECORD	RECORD COST, ADJUSTING FOR INSURANCE	TOTAL BREACH COST	BREACH COST, ADJUSTING FOR INSURANCE	BREACH COST DIFFERENCE
1,000	$75	$70.20	$75,000	$70,200	$4,800
5,000	$75	$70.20	$375,000	$351,000	$24,000
10,000	$75	$70.20	$750,000	$702,000	$48,000
50,000	$75	$70.20	$3,750,000	$3,510,000	$240,000
100,000	$75	$70.20	$7,500,000	$7,020,000	$480,000
500,000	$75	$70.20	$37,500,000	$35,100,000	$2,400,000
1,000,000	$75	$70.20	$75,000,000	$70,200,000	$4,800,000
10,000,000	$75	$70.20	$750,000,000	$702,000,000	$48,000,000

While these figures may illustrate the effects of certain factors on average, the reality of a breach cost is more complicated. Some breach-related expenses will be incurred regardless of breach size. A single breached record is likely to cost much more than the per capita cost presented due to standard breach-related activities such as incident response, investigation, or remediation. Similarly, a million breached records will not be directly proportional to the cost presented. There may also be compounded effects between the factors where no factor individually has the same effect when observed in the presence of additional factors. However, these figures generally illustrate the magnitude of potential savings when considering the number of affected records in a breach.

When it comes to determining what the costs for cyber-insurance will be, firms typically look to a mix of quantitative and qualitative data about the client and their practices. Texas agencies and institutions of higher education may benefit from having a standard framework upon which quantitative metrics are derived to demonstrate a level of cybersecurity maturity. Agencies seeking cyber-insurance policies should keep in mind any Texas Cybersecurity Framework assessments or other security program evaluations that might help result in lower premiums or better coverage.

The example illustrated in *Table 1* only considers a generalized view of the relationship between the cyber-insurance factor and the per capita cost of a data breach. To determine if a cyber-insurance policy is likely to benefit an individual organization, the details of a policy and the potential impact expenses need to be compared. While data breach frequency varies by organization, framing the investment over an extended period reveals how cyber-insurance coverage may ultimately prove to be a beneficial investment strategy despite experiencing years where the costs outweigh the benefits.

CYBER-INSURANCE EVALUATION

Consider an organization who obtains a cyber-insurance policy with data breach coverage. The policy terms include a $200k annual premium, $250k annual deductible, $2.5 million in maximum coverage, and a 1% annual premium increase. Over the course of six years, the organization experiences four data breaches of confidential information: 200 records in year one, zero records in the second year, 1,100 records in the third year, 20,000 records in the fourth year, zero records in the fifth year, and 2,500 records in the sixth year. Using the public sector average per capita cost ($75) the organization, the total breach costs can be determined for each year (*Table 2)*.

TABLE 2: BREACH COVERAGE SCENARIO 1

COMPONENT	YEAR 1	YEAR 2	YEAR 3	YEAR 4	YEAR 5	YEAR 6
Premium	$200,000	$202,000	$204,020	$206,060	$208,121	$210,202
Records Breached	200	-	1,100	20,000	-	2,500
Breach Cost	$15,000	$0	$82,500	$1,500,000	$0	$187,500
Deductible	$250,000	$250,000	$250,000	$250,000	$250,000	$250,000
Coverage Max	$2,500,000	$2,500,000	$2,500,000	$2,500,000	$2,500,000	$2,500,000
Without insurance	$15,000	$0	$82,500	$1,500,000	$0	$187,500
With Insurance	$200,000	$202,000	$204,020	$456,060	$208,121	$210,202
Insurance Savings	($185,000)	($202,000)	($121,520)	$1,043,940	($208,121)	($22,702)

In this scenario, the aggregate cost of absorbing the estimated breach impact costs outweighs the cost of maintain the cyber-insurance policy over time. Although some years have the opposite outcome, when taking into consideration the unpredictability of a large-scale data breach, this scenario benefits from maintaining the coverage (*Table 3*).

TABLE 3: SCENARIO 1 AGGREGATE COSTS

SCENARIO 1 AGGREGATE COSTS	
6 Year Cost	$1,785,000
6 Year Cost w/ Insurance	$1,480,403
6 Year Insurance Savings	**$304,597**

If the original scenario is adjusted to reduce the amount of records breached during year four to a figure like the other breaches, the decision to maintain a policy with the specifications becomes costlier than absorbing the breach costs directly.

TABLE 4: BREACH COVERAGE SCENARIO 2

COMPONENT	YEAR 1	YEAR 2	YEAR 3	YEAR 4	YEAR 5	YEAR 6
Premium	$200,000	$202,000	$204,020	$206,060	$208,121	$210,202
Records Breached	200	-	1,100	2,000	-	2,500
Breach Cost	$15,000	$0	$82,500	$150,000	$0	$187,500
Deductible	$250,000	$250,000	$250,000	$250,000	$250,000	$250,000
Coverage Max	$2,500,000	$2,500,000	$2,500,000	$2,500,000	$2,500,000	$2,500,000
Without insurance	$15,000	$0	$82,500	$150,000	$0	$187,500
With Insurance	$200,000	$202,000	$204,020	$206,060	$208,121	$210,202
Insurance Savings	($185,000)	($202,000)	($121,520)	($56,060)	($208,121)	($22,702)

Scenario two results in a significant difference between absorbing the costs and maintaining an insurance policy (*Table 5*). For a cyber-insurance policy to make financial sense in this scenario, the policy terms would need to be adjusted to reflect the appropriate level of coverage for the risk of the organization.

TABLE 5: SCENARIO 2 AGGREGATE COSTS

SCENARIO 2 AGGREGATE COSTS	
6 Year Cost	$435,000
6 Year Cost w/ Insurance	$1,230,403
6 Year Insurance Savings	**-$795,403**

The previous examples are but two of an endless possibility of combinations to illustrate the effects of determining the appropriate policy terms for an organization's risk in terms of breach probability and frequency. For example, if an organization has at maximum 50,000 sensitive and confidential records and is a consistent attack target going through a major transition phase, then the probability of a breach would be elevated, and insurance coverage is more likely to benefit provided the policy terms are appropriate for the expected level of damage. Replacing the same year with a worst-case scenario breach of 50,000 records yields a much different result in terms of six-year savings (*Table 6)*.

TABLE 6: SCENARIO 3 AGGREGATE COSTS

SCENARIO 3 AGGREGATE COSTS	
6 Year Cost	$4,035,000
6 Year Cost w/ Insurance	$1,818,283
6 Year Insurance Savings	**$2,216,717**

To frame a potential real-world scenario, consider a 2012 public sector entity breach responsible for disclosing approximately 3.3 million citizens' bank account information. If this volume were to be extrapolated based on the affected state's population and the population of Texas, we would see a volume of approximately 18.5 million sensitive records. Using the same policy described earlier ($250k premium, $300k deductible, $10m maximum coverage) and the public sector average record cost ($75/record), the state would be positioned to save approximately nine-million dollars over a period of six years. Although the per capita cost of a breach is likely to decrease with increasing breach scale, the overall cost is likely to grow regardless. Therefore, the total breach cost based on the $75 per capita may be inflated when considering breaches of massive scale. *Table 7* illustrates the overall costs for this scenario.

TABLE 7: SCENARIO 4 AGGREGATE COSTS

SCENARIO 4 AGGREGATE COSTS	
6 Year Cost	$1,387,500,000
6 Year Cost w/ Insurance	$1,378,238,004
6 Year Insurance Savings	**$9,261,996**

CONCLUSIONS

Modern cybercriminals are incredibly sophisticated and adaptive. Just as the most experienced driver is not immune to an accident, an organization can implement every industry best practice but may still fall victim if faced with an opportunistic opponent. This reason alone may be compelling enough to explore cyber-insurance options.

It is important for organizations to understand their own risk profiles before pursuing a cyber-insurance policy. As someone who does not own a vehicle would not have a direct need for auto insurance, an organization may not benefit from a certain coverage area as it may not apply to their risk profile. Those exploring the option should perform cost benefit analysis based on probability and risk to determine whether the coverage is appropriate and cyber-insurance is a beneficial decision.

The market for cyber-insurance is still evolving with coverage varying from policy to policy. As the market for cybersecurity insurance policies continues to develop, standardized practices and policies may become more common. The maturation of offerings will allow organizations to more readily compare coverage and premiums to make more informed decisions. Near-term policy seekers should consider leveraging cyber-insurance subject matter experts or an independent underwriter to ensure that policies meet the expected needs of the organization. Manuscript policies may be costlier in terms of policy development but could ultimately prove more useful in reducing risk and mitigating the adverse effects of an incident or breach. Supplementing less mature areas of an information security program rather than all facets with cyber-insurance can reduce risk without expensive premiums. Agencies should explore coverage areas which address the most risk for minimal cost.

Cyber insurance companies have contracts in place to quickly stand up a call center or provide identity theft protection in the event of a significant breach. Standing up these services quickly could prove to be difficult in a public sector environment, and a slower response could ultimately mean a costlier breach.

When two or more drivers have a collision, auto insurance companies will investigate to determine who is culpable for the accident. Similarly, cyber-insurance companies will perform due diligence to determine who is culpable or responsible for a breach. Having an insurance policy in place could save the state the burden of determining fault and potential litigation costs in the event of a breach at a vendor facility.

Cyber-insurance should not be used as a safeguard for a weak information security program. Only the most expensive cyber-insurance policies would cover all related information security risks and impacts. A weak information security program would likely result in cost-prohibitive premiums or non-insurability altogether. Ultimately, whether cyber-insurance is beneficial will be determined by the organization seeking the coverage. A risk-averse agency that processes millions of sensitive and confidential records may find data breach coverage extremely valuable, while a risk-tolerant agency that has fewer protected records may see cyber-insurance as an unnecessary expense on a limited budget.

The State Office of Risk Management is uniquely suited to provide expertise and guidance regarding cybersecurity insurance to state entities. As the cyber-insurance market continues to evolve, additional guidance and resources can help agencies make informed decisions about cyber-insurance policies and coverage.

TERTIARY DISASTER RECOVERY OPTIONS

OVERVIEW

88%

PERCENT OF AGENCIES HAVE WRITTEN COOP PLANS

Disaster recovery refers to the process of recovering and restoring operations, data, and IT infrastructure following the disruptive impacts of a disaster. Disaster recovery planning is an integral component of any continuity of operations plan. The 2018 IRDR responses indicate that most agencies (88%) have written continuity of operations plans. However, fewer report to have revised the plan in the last 12 months (82%) and even fewer report having tested the plan within the same time frame (63%). Although these figures indicate a relatively mature approach to disaster recovery, additional recovery options may further improve statewide preparedness and resilience.

Disaster recovery planning is a comprehensive activity with many facets, but a major component of disaster recovery involves creating redundant system storage backups in separate virtual or physical environments to assist the organization in recovering information and functionality after a disruptive event. A backup site can be another data center location operated by the organization or contracted via a company that specializes in disaster recovery services. In some cases, organizations with similar IT infrastructure needs may also have a reciprocal agreement with another organization to set up backup sites at each of their data centers, which could be utilized by the affected party during a disaster.

Ideally the backup location is geographically diverse and logically separated enough as not to be affected by the same event (e.g. flood, DoS attack, etc.). However, in recent years there have been cases where the secondary backups are also affected by the cyberattack. For instance, attackers have successfully been able to encrypt both the primary and secondary backups of organizations in cases of ransomware. In fact, ransomware attacks are much more likely to target both production and backup systems because it gives the attackers the leverage to demand extortion. While the risk of both the primary and secondary options being compromised can be reduced by proper segmentation, adding a tertiary recovery option for critical information may be a suitable strategy to reduce risk.

TERTIARY DISASTER RECOVERY

Tertiary disaster recovery options refer to the strategies and technologies implemented beyond the secondary failsafe mechanisms in place for an organizations information systems and data. A tertiary recovery option could come in many forms – an additional datacenter location, distributed storage solutions such as cloud, physical tapes, Disaster Recovery-as-a-Service, a warm site, or anything outside of the existing approach that assist with restoration of data or systems. Perhaps the most commonly referenced tertiary disaster recovery option are cloud-based solutions.
Cloud services provide several advantages over on-premise or alternate backup site strategies but may also serve to supplement current practices.

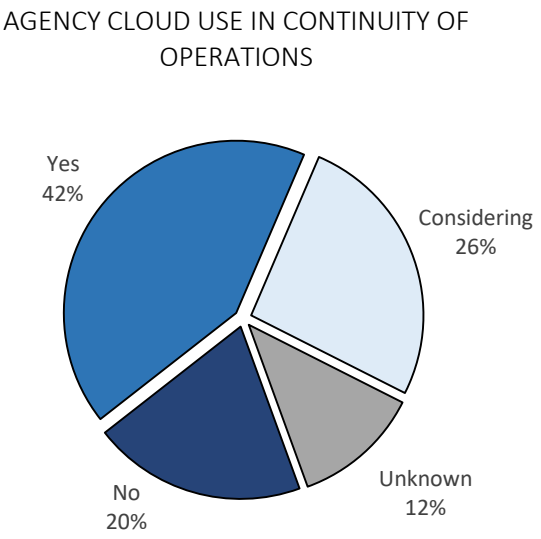


FIGURE 3: AGENCIES USING CLOUD IN RECOVERY PLANNING

Generally, organizations do not need to incur the expenses of additional facilities, infrastructure, hardware, or software with cloud. Instead cloud services are billed by usage based on the volume, architecture, security, or other characteristics of the data and infrastructure required. Cloud can virtually eliminate any geographically-based disaster risks such as both the primary and secondary locations being affected by a single event. Overall, agency survey responses, as shown in figure 3, show that there may be growing interest in the use of cloud services as part of their disaster recovery strategies.

While cloud solutions offer some advantages over traditional approaches, there are also some trade-offs that should be taken into consideration. Organizations may be reluctant to give up the level of control over their data, particularly if the data has regulatory requirements. There may also be concerns about who has access to the data at any given time and how data is stored with other organizations. As cloud becomes more prevalent, agencies should consider the use cases to decide if their cybersecurity and service delivery could benefit from a cloud implementation. The cost effectiveness of a cloud strategy for disaster recovery can also depend on how frequently the backup data needs to be accessed. Cloud storage solutions for data that rarely needs to be accessed can be extremely affordable, even with high volumes of data. However, if there is a need for the data to be continually or frequently accessed, the costs can add up quickly. *Table 8* provides a high-level summary of the pros and cons of common disaster recovery backup options.

Disaster Recovery Options

Table 8: Common Disaster Recovery Options

OPTION	SUMMARY	PROS	CONS
Onsite backup	Data is stored via onsite storage media separated from production environment.	· Readily available · Agency controlled	· Susceptible to loss · Single point of failure
Cold Site	Disconnected physical location without infrastructure.	· Less expensive than warm or hot site	· Requires physical access · Requires additional infrastructure
Warm Site	Partially connected, may contain some infrastructure.	· Tradeoff between expense and response time	· Moderately expensive · Requires additional configuration
Hot Site	Near duplicate of original site, typically synchronized with production environment.	· Fast and complete recovery · Allows for system replication	· Expensive to operate · Requires technical administration
Cloud Solution	Data is stored in a distributed fashion across many devices and accessible via the internet.	· Geographically independent · Utility-based · Fast and complete recovery	· Potential compatibility issues · Potentially expensive · Privacy, security, or legal concerns
Reciprocal Agreements	Warm site agreement between one or more organizations.	· Varies based on agreement. · Expenses may only occur if activated.	· Legal barriers · Potential compatibility issues · May require similar infrastructure · Complications in testing

A comprehensive disaster recovery plan will rely on no single option for its critical data and systems, but the appropriate combination recovery options should be determined through an evaluation of risk and available resources. A multi-option disaster recovery strategy has the potential to be both effective and affordable if based on the needs of the organization and designed efficiently.

REVIEW OF CYBERSECURITY LEGISLATION

OVERVIEW

Early cybersecurity legislation in Texas centered around criminal justice relating to cybercrime and computer-based offenses. Recent focus has been on state cybersecurity preparedness and the ability to defend against and recover from the impacts of cyberattacks. The Texas Cybersecurity Act (House Bill 8, 85(R)) brought significant attention to information security management within state government. In a review of cybersecurity legislation, the following recommendations are proposed for the purposes of consistency, clarity, and efficiency within statute.

SEC. 2054.077 – VULNERABILITY REPORTS.

- Change responsibility of preparing reports from the Information Resources Manager to the Information Security Officer and add the Information Resources Manager to the list of recipients.

SEC. 2054.516-7 – DATA SECURITY PLANS.

- Consolidate the separate sections for agencies and institutions, aligning language with the section applicable to state agencies.

SEC. 2054.0591 – CYBERSECURITY REPORT.

- Remove the requirements to evaluate tertiary disaster recovery options and cyber-insurance as part of the recurring report.

SEC. 1702.104 – INVESTIGATIONS COMPANY.

- Add language to exempt digital forensics companies performing services for non-criminal from Private Investigator licensing requirements.

CHAPTER 552 AND 2054, GOVERNMENT CODE.

- Review and consolidate disparate information security exemptions to the Public Information Act.

LEGISLATIVE RECOMMENDATIONS FOR IMPROVING CYBERSECURITY

In addition to the preventive and recovery efforts outlined earlier in this report, certain legislative actions can help enable and facilitate the advancement of cybersecurity throughout the state. The following recommendations were developed with input from the state information security community, advisory groups, and stakeholders throughout state agencies and institutions of higher education.

RISK-BASED MULTI-FACTOR AUTHENTICATION

Multi-factor authentication is the practice of verifying authenticity through at least two types of authentication factors (knowledge, possession, or inherence). Compromised accounts are a major contributor to data breaches and cyber events. Implementing multi-factor authentication can mitigate the damage that can be done from stolen user credentials.

With funds appropriated through the General Appropriations Act, authorize DIR to deploy multi-factor authentication for certain agency staff to have when accessing state systems.

SHARED POOL OF INFORMATION SECURITY PROFESSIONALS

Cybersecurity maturity takes dedicated staff and resources to stay up to date with the current threats and vulnerabilities. Smaller agencies, with staff who may already have competing priorities and responsibilities, do not have the time or resources to become experts in cybersecurity but also may not need a fully-dedicated resource to meet statutory obligations and agency needs.

Amend Government Code, Chapter 2054, to authorize a statewide shared pool of Information Security Officers and resources for state agencies.

CYBERSECURITY INSURANCE OFFERINGS AND GUIDANCE

The State Office of Risk Management is uniquely suited to provide expertise and guidance regarding cybersecurity insurance to state entities. As the cyber-insurance market continues to evolve, additional guidance and resources can help agencies make informed decisions about cyber-insurance policies and coverage.

Direct the State Office of Risk Management to investigate offering cybersecurity liability insurance policies to state agencies and develop guidance based on best practices for making cybersecurity insurance decisions, including the decision whether to self-insure or insure through a third party. Policy details and coverage amounts shall be considered exempt under Section 552.139, Government Code. The Texas Department of Information Resources should review the offerings and guidance identified as a strategy for protecting the statewide technology center.

Statewide Phishing Simulation

Email continues to be the number one attack vector for delivering malware. New phishing simulation technology can allow security departments to develop custom or templated phishing campaigns to deploy across the enterprise. The reporting capabilities of these tools can pinpoint the areas of weakness observed to tailor training for the organization. Iterative testing and training of phishing scenarios show great promise for improving the ability of users to recognize and report phishing attempts.

Authorize DIR to conduct a statewide phishing simulation, analyze the results, and investigate efforts and make recommendations to improve the cybersecurity awareness of state employees.

Texas Cyber Range

A cyber range is a virtual environment that is used for interactive cyberwarfare and cybertechnology training. It provides tools that help strengthen the stability, security, and performance of cyberinfrastructure and information systems used by government and military agencies. These virtual environments give participants a hands-on training experience that can simulate real-world cyber-attack scenarios.

Authorize DIR or other appropriate entity to create a Cyber Range to improve the skills and abilities of cybersecurity staff within the public sector.

APPENDIX

LIST OF TABLES

LIST OF FIGURES

REFERENCES

Bureau of Labor Statistics. "2016-2020 Job Outlook." May 2017. *Occupational Employment Statistics.* <https://www.bls.gov/oes/current/oes151122.htm>.

National Association of Insurance Commissioners. "Report on the Cybersecurity Insurance Coverage Supplement." August 2017. <https://www.naic.org/documents/cmte_ex_cybersecurity_tf_rpt_cyber_ins_coverage_supplument.pdf>.

Officers, National Association of State Chief Information. October 2017. *https://www.nascio.org.* <https://www.nascio.org/Portals/0/Publications/Documents/2017/NASCIO_2017_State_CIO_Survey.pdf?ver=2017-10-25-174540-510 >.

Ponemon Institute. "2018 Cost of a Data Breach Study." 2018. *<https://www.ibm.com/security/data-breach>.*

Verizon. *2018 Verizon Data Breach Investigations Report*. April 2018. <https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf >.

Texas Department of Information Resources

www.dir.texas.gov
300 West 15th St. Suite 1300
Austin, TX 78701
1-855-ASK-DIR1