Senate Select Committee on Cybersecurity

Interim Report

October 2018

October 30, 2018

The Honorable Dan Patrick
Lieutenant Governor of the State of Texas
Capitol Building, Room 2E.13
Austin, Texas 78701

The Senate Select Committee on Cybersecurity submits this report in response to the charges laid out in House Bill 8 85R. This report examines the state of cybersecurity in Texas, offers a brief legislative history, answers keys questions for legislators, and offers recommendations to mitigate cybersecurity threats facing the state. Texas is well positioned to become a leader on cybersecurity policy, and we hope this report furthers our goal to protect valuable state data and ensure that vital services are provided without interruption.

Respectfully submitted,

Senator Jane Nelson, Chair

Senator Konni Burton

Senator Donna Campbell

Senator Brian Hughes

Senator Boris Miles

The Senate Select Committee on Cybersecurity
Report to the 86th Texas Legislature

Preface

House Bill 8 85R required the Lieutenant Governor and Speaker of the House to establish select committees on cybersecurity to study cybersecurity issues, review state agency security plans, and make legislative recommendations.[1] On October 2, 2017 the Lieutenant Governor appointed the Senate Select Committee on Cybersecurity, making Texas the sixth state in the nation to appoint a legislative committee with specific jurisdiction over cybersecurity issues. With the establishment of the House Select Committee on Cybersecurity on April 5, 2018, Texas became the first state with two legislative committees with jurisdiction over cybersecurity.

The Senate Select Committee on Cybersecurity met on December 6, 2017 and March 21, 2018. Information regarding witnesses and testimony can be found at: https://senate.texas.gov/cmte.php?c=515.

Legislative History of Cybersecurity in Texas

Cybersecurity is a critical, yet relatively new, core function of state government. In fact, the first reference to cybersecurity was added to statute in 2011 when Senate Bill 988 established the Cybersecurity, Education, and Economic Development Council. Realizing the need for better coordination and focus on cybersecurity, the Legislature tasked the Council with facilitating relationships between members of governmental agencies, businesses, and institutions of higher education. The Council's mission was to advance cybersecurity initiatives while providing research for the improvement of the state's cybersecurity infrastructure.

Building upon the work of the Council, the Legislature passed three key pieces of cybersecurity legislation in 2013. With the passage of Senate Bill 1134, the Legislature formally vested state cybersecurity oversight with the Department of Information Resources (DIR), including the direction to develop a framework to protect the state's cyberinfrastructure. Senate Bill 1102 established the role of the State Cybersecurity Coordinator within DIR. The purpose is to cultivate partnerships between public and private entities, and implement any or all recommendations made by the Council. Finally, Senate Bill 1597 directed each state agency to develop an information security plan to protect the agency's information. These bills established the federated system of information security in place today where DIR provides guidance and direction to agencies which in turn are responsible for their own cybersecurity.

Key Bills of the 85th Legislature

The 85th Legislature moved Texas even further into the age of cybersecurity with several key pieces of legislation.

House Bill 8 (Capriglione/Nelson)

Known as the Texas Cybersecurity Act, HB 8 made sweeping statutory changes to minimize Texas' vulnerability to cyber attacks by assessing risk at state agencies, better securing state data,

[1] H.B. 8, 2015 Leg., 85th Reg. Sess. (Tex. 2017).

promoting collaboration of leaders in information technology, and ensuring best practices for cybersecurity.

Senate Bill 532 (Nelson/Capriglione)
Senate Bill 532 made further strides toward protecting state data by requiring agencies to: consider the security costs and benefits of cloud computing, report the inventory of information resource infrastructure, and keep cybersecurity information confidential.[2]

Senate Bill 1910 (Zaffirini/Capriglione)
Senate Bill 1910 instructed DIR to submit a biennial cybersecurity report to the Legislature and requires agencies to designate an information security officer.[3]

The State of Cybersecurity in Texas

At its December hearing, the Senate Select Committee on Cybersecurity heard testimony from Doug Robinson, Executive Director of the National Association of State Chief Information Security Officers (NASCIO) [4]. After a robust presentation outlining state risks of cybersecurity, Robinson closed with seven key questions for state leaders (See Appendix A) which are addressed throughout this report to describe Texas' state of cybersecurity.

Culture of Information Security

Texas took a giant leap toward developing a culture of information security with the passage of House Bill 8 in 2017 by establishing a governance structure of state leadership and stakeholders to study cybersecurity. Among its many accomplishments, the bill: increased the membership of the Cybersecurity Council and broadened its mission; established select committees on cybersecurity in the Senate and House of Representatives; and required agency cybersecurity assessments during Sunset reviews.

Cybersecurity Council
Until HB 8, the Cybersecurity Council, known as the Private Industry- Government Council was an authorized entity housed at DIR without specified membership or a clear mission. HB 8 structured the Cybersecurity Council by appointing the state's cybersecurity coordinator to lead it, and it specified the membership to include a representative of the Governor's office, a member of each legislative chamber, representatives of institutions of higher education, and leaders in the private sector. The Cybersecurity Council is a now a blend of public and private sector stakeholders whose required duties now include: considering establishing a computer emergency readiness team to address cyber attacks, addressing cybersecurity threats to critical state installations, assisting state agencies in understanding and implementing cybersecurity measures that are most beneficial to the state, and assessing the state's information technology and cybersecurity workforce. The Council is required to provide recommendations to the Legislature to implement cybersecurity best practices and remediation strategies.

[2] S.B. 532, 2015 Leg., 85th Reg. Sess. (Tex. 2017).
[3] S.B. 1910, 2015 Leg., 85th Reg. Sess. (Tex. 2017).
[4] Hearing Before the S. Select Comm. on Cybersecurity, 2018 Leg., 85th Interim (Tex. 2017) (written testimony of Doug Robinson, National Association of State Chief Information Security Officers).

Sunset

HB 8 also directs the Sunset Commission to assess a state agency's cybersecurity practices as part of their scheduled Sunset review. By including these issues in Sunset reviews, the Legislature has increased oversight of whether agencies are in compliance with the Texas Cybersecurity Act.

Texas Cybersecurity Framework

Per its statutory obligation, DIR has promulgated Texas Administrative Code 202 (TAC 202) that sets a minimum baseline for cybersecurity standards for state agencies and institutions of higher education (IHE). First established in 2003, the code is continually reviewed and updated to keep pace with technology. Since its inception, it has been amended to address wireless technology, firewalls, encryption, and incident management. It outlines: the responsibilities of agency heads, chief information security officers, and agency staff; the development of information security programs and reporting; and security risk management.[5]

Underlying TAC 202 are the Security Control Standards which are based on the National Institute of Standards and Technology (NIST) special publication 800-53. This consists of the selection of a primary set of baseline security controls including incident response, access control, ability for disaster recovery and business continuity. The Control Standards are divided into five core functions: identify, protect, detect, respond, and recover.[6] In turn, each function is divided into forty security controls that specify the minimum information security requirements that state organizations must use to provide the appropriate levels of information security according to risk levels. The control catalog specifies the purpose, levels of risk, implementation overview, and implementation examples for each control activity. These controls align with the NIST Cybersecurity Framework in accordance with industry best practices.[7]

Per Texas Government Code, 2054.133, each state agency is required to develop, and periodically update, an information security plan for protecting the security of the agency's information. In 2014 DIR adopted the Control Standards into the Texas Cybersecurity Framework which serves as a template for agencies to report their plans, which are due on October 15 of odd numbered years. Through DIR's Statewide Portal for Enterprise Cybersecurity Threat, Risk and Incident Management (SPECTRIM) portal, agencies self-report their maturity level for each of the forty controls on an ascending scale of 0-5: zero being nonexistent and five being optimized. DIR aggregates the data and produces a statewide cybersecurity maturity level for each control, compares agencies against one another, and identifies maturity trends. That data is submitted in a report to the governor, the lieutenant governor, and the Legislature in January of odd numbered years and provides a basis for legislative recommendations.[8] Additionally, per HB 8, state agencies implementing an internet website or mobile application that processes any sensitive personally identifiable or confidential

[5] TEX. ADMIN. CODE § 202.
[6] Nicole Keller, CYBERSECURITY FRAMEWORK NIST(2018), https://www.nist.gov/cyberframework (identifying main elements of NIST framework, identify, protect, detect, and recover).
[7] OFFICE OF THE CHIEF INFORMATION SECURITY OFFICER, SECURITY CONTROL STANDARDS CATALOG (2016).
[8] TEX. GOV'T. CODE § 2054.133.

information must submit a biennial data security plan to DIR, subject the website or application to a vulnerability and penetration test, and address any vulnerability identified in the test.[9]

Critical Controls

In his testimony, Doug Robinson of NASCIO indicated that the first six of what are commonly known as the "Top Twenty Critical Controls" can mitigate approximately 80-90% of all security breaches.[10] These controls were established by the non-profit Center for Internet Security and are not mutually exclusive of the NIST Framework; in fact these controls can be mapped onto most NIST controls. The top six (known as Basic Controls) are:

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
4. Continuous Vulnerability Assessment and Remediation
5. Controlled Use of Administrative Privileges
6. Maintenance, Monitoring, and Analysis of Audit Logs

The Legislature has recognized the value of these controls which have influenced recent legislation For example, SB 532 85R (Nelson/Capriglione) directs agencies to submit to DIR an inventory of servers, mainframes, cloud services, and other information technology equipment per Critical Control 1. Additionally, the legislation requires DIR to use that information to evaluate each agency's operational risks and requires agencies at higher risks to assess remediation options for associated risks and vulnerabilities per Critical Control 4. While the state has not formalized a framework based on the Critical Controls, they can provide valuable guidance to prioritize controls within the Texas Cybersecurity Framework.

Training

Statute requires DIR to develop and provide training to state agencies on cybersecurity measures and awareness.[11] HB 8 further required DIR to provide mandatory guidelines to state agencies regarding the continuing education requirements for cybersecurity training that must be completed by all information resources employees. For employees who handle sensitive information, including financial, medical, personnel, or student data, statute requires agencies to develop and update a data use agreement that is to be distributed to and signed by those employees.[12] There are no specific requirements for other employees.

DIR develops and administers several programs as part of its charge to train employees and provides security training and certification exams for information security staff. The training is designed to educate end users in any organization about security awareness and compliance. This is a resource that bolsters Texas public sector information security awareness through curriculum designed by the SANS (SysAdmin, Audit, Network and Security) Institute, a nationally

[9] H.B. 8, 2015 Leg., 85th Reg. Sess. (Tex. 2017).
[10] Hearing Before the S. Select Comm. on Cybersecurity, 2018 Leg., 85th Interim (Tex. 2017) (written testimony of Doug Robinson, National Association of State Chief Information Security Officers).
[11] TEX. ADMIN. CODE § 202.
[12] TEX. ADMIN. CODE § 202.

recognized cybersecurity training program. Additionally, DIR launched the InfoSec Academy in 2014 which provides industry standard cybersecurity certification prep courses and exam vouchers completely funded by DIR for agency and IHE security staff. It also disseminates relevant cybersecurity information to state agencies though its weekly Cybersecurity Insights Newsletter.

Some agencies have taken the initiative to engage in dynamic cyber training. For example, the Health and Human Services Commission hosts a Cyber Fair in October to coincide with Cybersecurity Month to raise awareness and provide the resources needed for employees to stay secure on the state's network. The fair is available via webinar for those who cannot attend, and staff who attend in person can receive continuing education credit.

While training is a critical component of cybersecurity, limited resources constrain the amount of training available to every state employee. To augment training, Dr. Greg White of UT-San Antonio testified that the state should create a culture where employees take responsibility for their own cybersecurity. As an example, he discussed how in the 1980s the public service campaign "Only You Can Prevent Forest Fires" by the U.S. Forest Service featuring Smokey the Bear shifted the responsibility of preventing forest fires onto individuals by compelling them to change their behavior. He suggests a similar model for state cybersecurity.

Risk Assessments, Data Classification, and Metrics

Risk Assessments

House Bill 8 required each state agency to conduct a biennial security assessment of the agency's information resources systems, network systems, digital data storage systems, digital data security measures, and information resources vulnerabilities. Agencies may conduct their own risk assessments or contract with a third party through DIR. Additionally, DIR makes available to all state agencies and institutions of higher education (IHE) a voluntary governance, risk, and compliance software tool. SPECTRIM provides incident management and analysis, risk assessment analysis, and agency security plan template preparation. This portal was launched in April 2016 to help tie together the overall state security program. The use of the portal is not mandated, but is an option for agencies and IHEs to use. SPECTRIM assessments gauge the health of the organization, and provides lists of strengths and weaknesses to management, along with a roadmap and suggested plans to improve the security position for the organization. The assessments also show the organization's security posture compared to other state organizations.

Data Classification

Data classification is the process of categorizing data into various types, forms, sensitivity level, or any other grouping of similar characteristics. DIR has developed a guide that classifies data according to the Texas Public Information Act and applicable federal standards.[13] Data classification is the basis for identifying an initial baseline set of security controls for information and information systems, which makes security decisions more efficient because it instantly identifies and communicates the level of protection required for any piece of data and who can access it.

[13] TEX. ADMIN. CODE § 202.

DIR's proposed classification scheme for agencies uses four categories of data that require increasing levels of protection: public, sensitive, confidential, and regulated.[14] Each category must be protected by certain security controls. For example, confidential information that is transmitted over a public network must be encrypted. Appropriate data classification can also enable a more efficient use of IT capital. Specifically, data that has been categorized at a level requiring more protection can provide an objective justification for certain capital expenditures to help protect that data.

Metrics

DIR tracks several metrics such as number of security incidents reported to DIR by state agencies per month, amount of known bad traffic blocked, top targeted agencies, etc. Other metrics include system maturity scores according to the Texas Cybersecurity Framework. Metrics aid DIR in determining what is working, and helps to identify areas for improvement.

Threat Management and Analytics

DIR operates the Network Security Operations Center (NSOC) which delivers security information management and vulnerability assessment services to Texas agencies, local governments, and IHEs. As the state's internet service provider, the NSOC sees all traffic going to and from agencies through the internet. Perimeter tools provide continuous blocking based on reputation and targeted block lists. All traffic that pass though the NSOC is monitored by in house security experts as well as trusted third parties, and alerts are distributed for any malicious traffic observed. Additionally, the agencies and IHEs have the ability to procure vulnerability detection and advanced threat analytics through managed security services or cooperative contracts.

Statute requires each state agency and IHE to provide timely reporting of certain types of security incidents to DIR, which depending on the threat or level of risk to the state, could mean emergency reporting.[15] Timely reporting is required (preferably within 24 hours) for incidents that may: propagate to other state systems (emergency reporting); result in criminal violations that shall be reported to law enforcement; and involve the unauthorized disclosure or modification of confidential information, e.g., sensitive personal information. There is no standard requirement for agencies to analyze the cause of or report identified system breaches.

Cyber Disruption and Communication Plans

HB 8 required DIR to develop a plan to address cybersecurity risks and incidents by incorporating cybersecurity risk and incident prevention and response methods into existing state emergency plans, including continuity of operation plans and incident response plans. DIR is currently developing a statewide comprehensive plan, however each state agency is required to develop one that can be executed individually. Additionally, DIR is developing a crisis communication plan for cybersecurity incidents.

[14] TEX. ADMIN. CODE § 202 (classifying data as public, sensitive, confidential, or regulated).
[15] TEX. ADMIN. CODE § 202.

Critical Infrastructure

The Department of Homeland Security (DHS) defines critical infrastructures as assets, systems, and networks so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, public health or safety.[16] Two major energy sectors that comprise our state's critical infrastructure include electric providers and oil and gas companies, however the state exercises limited authority over the cybersecurity of these industries.

The electric industry has received the most scrutiny recently due to reports by DHS that Russian hackers have gained electronic access to power plant control rooms across the country. The North American Electric Reliability Corporation (NERC) is the federally designated entity whose purpose is to protect the reliability and security of the grid by developing Critical Infrastructure Protection (CIP) Security Compliance Standards which include cybersecurity regulations. In turn, NERC is subject to oversight by the Federal Energy Regulatory Commission (FERC).

All electric generators and transmission companies in Texas with a direct connection to the state's electric grid fall under CIP Standards with the exception of small electric cooperatives with no direct connection to the grid.[17] The Public Utility Commission expressed concerns that developing state specific standards for the electric industry could be duplicative of federal standards and burden electric companies while providing no extra benefit. However, DHS and the FBI indicate that breaches have occurred by first penetrating suppliers and third party vendors, entities which are not covered by CIP standards and may be the weak links in electric grid's cybersecurity.

While the oil and gas industry is a driving force behind Texas' economic success, the state does not regulate the cybersecurity of its associated companies, despite the potential threats. Sixty-eight percent of oil and gas companies have suffered at least one security compromise involving the loss of confidential information or the disruption of their operations in the past year.[18] Pipelines could be particularly vulnerable to nation states who seek to hold oil and gas assets hostage or disrupt service to customers. Recently, the chairman of the Federal Energy Regulatory Commission has suggested that Congress should vest the Commission with the statutory authority and resources to implement mandatory cybersecurity standards for gas pipelines much like it does for the electric grid.[19]

Cybersecurity threats extend further into state government critical infrastructure including highway systems, bridges, dams, water, and defense. Threats to these systems range from manipulating the control of mechanical systems, to obtaining classified geographic information,

---

[16] Critical Infrastructure Sectors, DEPARTMENT OF HOMELAND SECURITY(2018), https://www.dhs.gov/critical-infrastructure-sectors (last visited Sep 7, 2018).
[17] Hearing Before the S. Select Comm. on Cybersecurity, 2018 Leg., 85th Interim (Tex. 2018) (testimony of Commissioner Brandy Marty Marquez, Public Utility Commission).
[18] Charles Cooper, WHAT'S FUELING CYBERSECURITY CONCERNS IN THE OIL AND GAS INDUSTRY?5 EASY WAYS TO IMPROVE YOUR CYBERSECURITY | AT&T BUSINESS, https://www.business.att.com/learn/secure-networking/whats-fueling-cybersecurity-concerns-in-the-oil-and-gas-industry.html (last visited Sep 7, 2018).
[19] Neil Chatterjee & Richard Glick, CYBER SECURITY RULES NEEDED FOR PIPELINES: FERC COMMISSIONERS HOUSTON CHRONICLE (2018), https://www.chron.com/business/energy/article/Cyber-security-rules-needed-for-pipelines-FERC-13002008.php (last visited Sep 7, 2018).

or detecting weaknesses for exploitation. Unlike the private sector, the state does regulate the cybersecurity of agencies responsible for maintaining these systems, and the Sunset Commission will assess their cybersecurity efforts during its review of agencies.

Local Governments

While the state has made tremendous strides in recognizing the need for adequate cybersecurity protections for itself, it does not provide oversight of or support to local cybersecurity efforts. Cities and counties are an attractive target for cyber attacks, due to the data they store, and they are often connected to larger systems and networks.[20] In 2018 Atlanta was the victim of a ransomware attack that impacted services for almost a week.[21] The hackers demanded $51,000 in Bitcoin to decrypt the data. Baltimore was also a victim when their dispatch systems were interrupted for more than seventeen hours, seriously impacting public safety. In a survey conducted in 2016 by the International City/County Management Association (ICMA), almost forty percent of local governments reported cyber attacks in the last year.[22]

DIR has launched a comprehensive Managed Security Services (MSS) contract that gives state agencies, local governments, school districts and other public entities access to resources to help manage their data. The MSS consists of three major offerings: security monitoring and device management, incident response, and risk and compliance. The program is voluntary for entities that choose to purhase services.

Workforce Development

The cybersecurity workforce pipeline is a challenge for governments looking to hire experts to protect state information systems: the demand for talent far outstrips supply. And the shortage isn't unique to governments. Some estimates predict a 1.5 million global shortage of cybersecurity professionals by 2020.[23] Recognizing the need for a well trained workforce, the Legislature passed House Bill 3593 in 2017 to allow public school districts to offer cybersecurity courses for credit and to create language credits for coding courses.

Additionally, in 2018, the Texas Education Agency, DIR, and SANS Institute partnered on Girls Go CyberStart, created to get more young women involved in the growing field of cybersecurity. The Girls Go CyberStart is an extracurricular learning competition for high school girls designed to encourage interest in the cybersecurity field through a national cyber competition.

Texas universities have become important centers for cybersecurity research as well as training grounds for the state's cybersecurity workforce. UT San Antonio is home to a premier cybersecurity program spanning three colleges - Business, Engineering, and Sciences - and

---

[20] Ted Newcombe, SMALL TOWNS CONFRONT BIG CYBER-RISKS GOVERNMENT TECHNOLOGY: STATE & LOCAL GOVERNMENT NEWS ARTICLES(2017), http://www.govtech.com/security/GT-OctoberNovember-2017-Small-Towns-Confront-Big-Cyber-Risks.html (last visited Oct 3, 2018).

[21] Donald Norris et al., LOCAL GOVERNMENTS' CYBERSECURITY CRISIS IN 8 CHARTSGOVERNMENT TECHNOLOGY: STATE & LOCAL GOVERNMENT NEWS ARTICLES(2018), http://www.govtech.com/security/Local-Governments-Cybersecurity-Crisis-in-8-Charts.html (last visited Oct 3, 2018).

[22] Ted Newcombe, SMALL TOWNS CONFRONT BIG CYBER-RISKS GOVERNMENT TECHNOLOGY: STATE & LOCAL GOVERNMENT NEWS ARTICLES(2017), http://www.govtech.com/security/GT-OctoberNovember-2017-Small-Towns-Confront-Big-Cyber-Risks.html (last visited Oct 3, 2018).

[23] Jeff Kauflin, *The Fast-Growing Job With A Huge Skills Gap: Cyber Security*, FORBES, 2017.

houses three research centers aimed at combatting global security challenges encountered by individuals, industry, government and the military. Students can earn a variety of degrees and certificates in cybersecurity from bachelor to doctoral programs. Similarly, the Texas A&M University Cybersecurity Center offers minor fields of study and a masters degree in cybersecurity engineering. The University has also started a boot camp for high school teachers to teach the basics of the industry and to raise awareness of career opportunities for students. [24]

Budget

Cybersecurity is not a specified item in the Texas budget, rather it is included within appropriations for related strategies, projects, and programs.[25] Figure 1 shows estimated biennial cybersecurity expenditures according to the Legislative Budget Board.

Figure 1

Estimated Cybersecurity Spending for '18-'19 Biennium (in millions)	
Department of Information Resources	$21.5
Cybersecurity Employees	$16
PCLS Projects	$24
Agency Daily Operations	$25.7
Data Center Services	$24.7 - $49.3
Total State Cybersecurity Spending	**$111.9-$136.5**

For the current biennium, DIR was appropriated $21.5 million in All Funds to address security policy, assurance, education, and awareness programs; and to assist state entities with identifying security vulnerabilities.[26] This amount also includes $3 million for HB 8 security assessments and penetration tests. The Legislative Budget Board (LBB) estimates that $16.0 million is expended biennially on 180 agency employees whose responsibilities are primarily related to cybersecurity. LBB also estimates agencies will spend $25.7 million in daily operations for cybersecurity efforts this biennium along with $24.7 - $49.3 million on cybersecurity costs in DIR's Data Center Services program.

Finally, certain cybersecurity projects are specifically identified in the budget via agency riders. Article IX, Section 9.10 of SB 1directs DIR to submit to the LBB a prioritization of state agencies' cybersecurity projects and projects to modernize or replace legacy systems known as the Prioritization of Cybersecurity and Legacy Systems (PCLS) Projects Report.[27] Legacy systems operate with old, obsolete, unsecured, or inefficient hardware or software and are more

[24] About Us, TEXAS AM CYBERSECURITY CENTER, https://cybersecurity.tamu.edu/about-us/ (last visited Oct 3, 2018).
[25] Hearing Before the S. Select Comm. on Cybersecurity, 2018 Leg., 85th Interim (Tex. 2018) (written testimony of Richard Corbell, Legislative Budget Board).
[26] Hearing Before the S. Select Comm. on Cybersecurity, 2018 Leg., 85th Interim (Tex. 2018) (written testimony of Richard Corbell, Legislative Budget Board).
[27] Hearing Before the S. Select Comm. on Cybersecurity, 2018 Leg., 85th Interim (Tex. 2018) (written testimony of Richard Corbell, Legislative Budget Board).

difficult and costly to maintain, less resilient, and carry a higher degree of security risk. Ultimately, the Legislature decides which, if any, projects to fund based on total risk which are paid for with General Revenue via rider in each receiving agencies' budget. However, there is no dedicated funding mechanism or line item to track expenditures.

Agency cybersecurity expenditures are heavily influenced by unplanned system breaches and data losses. In Texas, the fiscal impact to the state for security breaches has been costly. For example, in FY13 the Health and Human Services Commission reported $2.3 million for staffing costs to respond to and recover from 1,948 security incidents. In FY 2016, the Department of State Health Services reported an estimated cost of $1.9 million from security incidents. Other areas of concern for potential impacts and losses include: physical loss of devices or media containing data; incidents affecting IT infrastructure hosted by a third party; electronic leakage of data; personal data exposure; inappropriate IT resource use by employees; and viruses and malware.

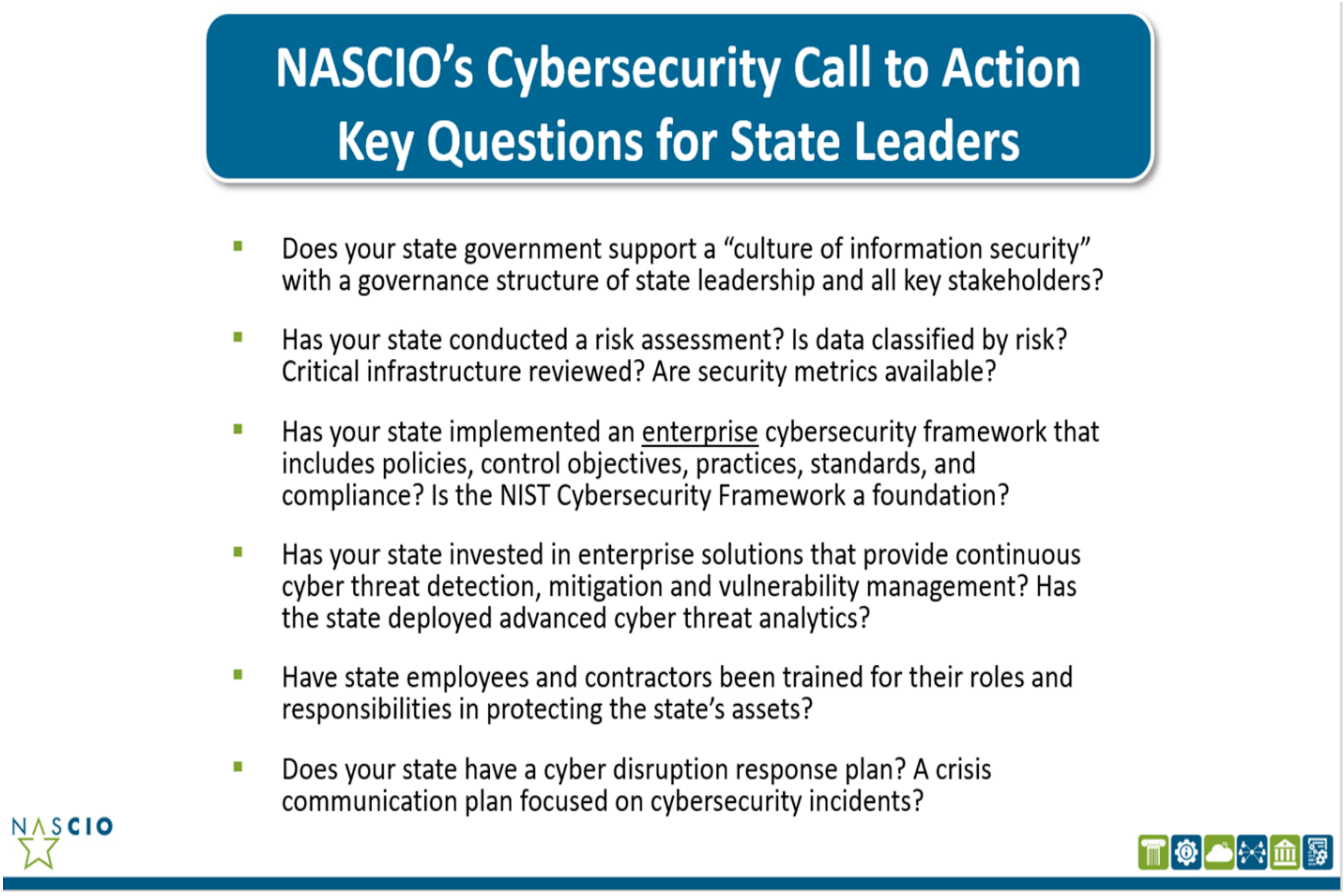
Conclusion

By all measures, Texas is well positioned to confront cybersecurity challenges and protect itself against malicious cyber attacks. The state has benefited from strong leadership in both the executive and legislative branches which have set forth frameworks, policies, and strategies based on nationally accepted best practices. However, the state should continually assess its cybersecurity threats and vulnerabilities so it can adapt to an ever evolving cyber landscape across the entire enterprise of agencies, entities, and subdivisions.

Recommendations

1. The state should continue evaluating cybersecurity threats and vulnerabilities and support agency cybersecurity maturity.
2. The state should support efforts to bolster cybersecurity for local entities.
3. The state should foster the cybersecurity workforce pipeline.
4. The state should continue evaluating legacy systems and their impact on cybersecurity.
5. The state should ensure the electric grid is protected from cyber attacks.
6. Legislative agencies should adopt cybersecurity best practices.
7. DIR should expand its Texas Cybersecurity Framework by adding controls prioritized by the CIS Top 20 Critical Controls.
8. DIR should create an innovative campaign to foster a culture of cybersecurity among state employees.

Appendix A



Hearing Before the S. Select Comm. on Cybersecurity, 2018 Leg., 85th Interim (Tex. 2017) (written testimony of Doug Robinson, NASCIO)