INTERIM REPORT

to the 86th Texas Legislature

HOUSE SELECT COMMITTEE ON CYBERSECURITY

January 2019

HOUSE COMMITTEE ON CYBERSECURITY, SELECT
TEXAS HOUSE OF REPRESENTATIVES
INTERIM REPORT 2018

A REPORT TO THE
HOUSE OF REPRESENTATIVES
86TH TEXAS LEGISLATURE

GIOVANNI CAPRIGLIONE
CHAIRMAN

COMMITTEE DIRECTOR
KATY ALDREDGE

Committee On
Cybersecurity, Select

January 31, 2019

Rep. Giovanni Capriglione   P.O. Box 2910
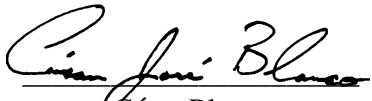Chairman   Austin, Texas 78768-2910

The Honorable Joe Straus
Speaker, Texas House of Representatives
Members of the Texas House of Representatives
Texas State Capitol, Rm. 2W.13
Austin, Texas 78701
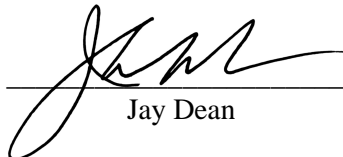
Dear Mr. Speaker and Fellow Members:

The Committee on Cybersecurity, Select of the Eighty-fifth Legislature hereby submits its interim report including recommendations and drafted legislation for consideration by the Eighty-sixth Legislature.

Respectfully submitted,

_____
Giovanni Capriglione, Chairman

_____   _____
César Blanco   Tony Dale

_____   _____
Jay Dean   Ina Minjarez

<div align="center">

TABLE OF CONTENTS

</div>

INTRODUCTION

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. On April 5, 2018, the Honorable Joe Straus, Speaker of the Texas House of Representatives appointed five members to the House Select Committee on Cybersecurity (the Committee). The Committee's membership consisted of the following five members: Chairman Giovanni Capriglione, César Blanco, Tony Dale, Jay Dean, and Ina Minjarez.

INTERIM STUDIES

House Bill 8 (85R) required the study of:
1. Cybersecurity in this state;
2. The information security plans of each state agency; and
3. The risks and vulnerabilities of state agency cybersecurity.

The Committee also studied:
1. Cybersecurity education, curriculum, training, workforce, and outreach to increase interest in the technology career field;
2. The Jack Voltaic 2 Cybersecurity Exercise; and
3. Funding provided to specific state agencies.

ANALYSIS

The Committee studied the assigned issues in a series of two hearings held in May and September 2018. Both of these hearings were open to invited witnesses and public witnesses. This report includes a background on, discussion of, and recommendations for each issue based on the Committee's proceedings.

ISSUE #1: CYBERSECURITY IN THIS STATE.

Background

The Committee met on Wednesday, May 16, 2018 at 1:00 PM on the campus of the University of Texas at San Antonio in the Student Union Retama Auditorium (Room 2.02.02 on the 2nd floor) in San Antonio, Texas. The committee took invited testimony and public testimony from the following stakeholders:

1. Gregg Cannon (Grimes County)
2. Brigadier General Greg Chaney (Texas Military Department)
3. Colonel Theresa Cogswell (Texas Military Department)
4. Will Garrett (San Antonio Chamber of Commerce/Cyber Security SA)
5. Sid Hudson (City of McKinney, TML, TAGITM)
6. Todd Kimbriel (Department of Information Resources)
7. Lieutenant Colonel Kristy Leasman (Texas Military Department)
8. James Perschbach (Port Authority of San Antonio)

Discussion

State Government - Department of Information Resources

The Department of Information Resources (DIR) offers numerous services to state government, institutions of higher education, and local government (see Figure 1). Though DIR does provide support for local government entities, those entities are generally only guided by Federal and Texas law, while DIR has jurisdiction over Texas Administrative Code (TAC) 202, Information Security Standards, guiding both state agencies and higher education.

Figure 1:

LOCAL GOV	STATE GOV	HIGHER EDUC		LOCAL GOV	STATE GOV	HIGHER EDUC	
	✓	✓	Policy/Security Controls Catalog	*	✓	✓	Statewide Portal for Enterprise Cybersecurity Threat, Risk, & Incident Management (SPECTRIM)
	✓	✓	InfoSec Academy				
	✓	✓	End-User Security Awareness Training		✓	✓	Decision Support Services
✓	✓	✓	Information Security Forum (ISF)	✓	✓		Network Security Operations Center (NSOC)
✓	✓	✓	Vulnerability Scans/ Penetration Tests	✓	✓	✓	Statewide Data Center and Technology Services (DCS)
✓	✓	✓	Security Assessments		✓		Legacy Modernization
✓	✓	✓	Managed Security Services	✓	✓	✓	Texas Cybersecurity Council

* Planned

2

Through the Network Security Operations Center (NSOC), DIR collects the data on what kind of threats are aimed at state and local governments. 41% are suspicious activity, 26% are ransomware, 12% are InfoStealer, 11% are other, 6% are downloader/backdoor, and 4% are miners[1]. Of the active threats, fraud and organized crime are a high threat of phishing, Nation/States are a high advanced persistent threat, and hacktivists are a low threat. DIR currently blocks billions of intrusion attempts every month with the typical country of origin being Russia and China.

All state agencies and institutions of higher education are required to submit their Agency Security Plans to DIR in October of even numbered years, which DIR then evaluates and compiles into their Biennial Security Report and is submitted to the Legislature in January of odd numbered years. This report gives a comprehensive overview of the cybersecurity health in Texas. Through this process, DIR then adds any new legislation that spurs new rules and regulations and works with the agencies on improving their overall cybersecurity capabilities.

Texas cybersecurity rules, TAC 202, give a framework that all agencies are required to follow. These rules are based on the National Institute of Standards and Technology (NIST) and include a customized list of 40 control objectives to help agencies identify, protect, detect, respond, and recover. Having a set of cybersecurity standards that are consistent across state agencies and institutions of higher education is important when identifying issues from normalized data and finding improvements. Texas is unique in having such a robust and comprehensive control from a cybersecurity perspective, particularly because the state has a non-cabinet style gubernatorial leadership. Texas Administrative Code also requires all state employees to participate in security training at least once every two years. While DIR provides guidance and optional tools, it is up to each agency to determine the scope and the effectiveness of their training.

DIR participates in the Multi-State Information Sharing and Analysis Center utilizing their forensic services and network monitoring services. This group has access to certain intelligence not available to states. For example, they can identify a new threat vector coming from a specific geolocation or IP address, and knowing it is bad and malicious traffic, can share the threat with the participating states for the traffic to be blocked. This is important so the State of Texas can be up-to-date on the latest threats. House Bill 8 (85R) required the creation of a Texas Information Sharing and Analysis Organization, which will cover many of the blank spaces in Figure 1.

State Government - Texas Military Department

The Texas Military Department (TMD) is made up of 24,000 members, 80% of whom are Texans, and provides the Governor and President with ready cyber forces in support of state and federal authorities at home and abroad. TMD's cybersecurity components are divided into a defense element that defends the networks within the TMD, and the Air National Guard and the Army National Guard who have the mission of defending the Department of Defense networks.

The Defense Cyber Operations Element of the Texas State Guard cyber teams defend TMD's constellation networks. All of these teams can be leveraged to conduct training and provide support to mission partners in Texas to detect and analyze the cause of cyber attacks, provide an active network defense, conduct vulnerability assessments, and conduct remediation. As with all

requests of TMD, for the cyber teams to deploy, there must be a request from the Governor.

Because the Air and Army National Guards support federal missions, TMD cannot always rely on those personnel to be available for assistance in State cyber incidences. For this reason, developing the Texas State Guard's capacity is important for long-term reliability.

Local Government - Port San Antonio

Port San Antonio, the largest air field in the region, is home to Boeing's largest services sight in the world and one of the largest engine aircraft complexes in the world. Nearby to the Port is the headquarters of the 25th Air Force, providing multisource intelligence, surveillance, and reconnaissance products, applications, capabilities and resources, to include cyber and geospatial forces and expertise. On the other side of the Port is the headquarters of the 24th Air Force, the operational warfighting organization that establishes, operates, maintains and defends Air Force networks to ensure warfighters can maintain the information advantage as U.S. forces prosecute military operations around the world.

The Port is surrounded by two neighborhoods, and views itself as part of the community. On the Port's property is the San Antonio Museum of Science and Technology. In early 2018, the Port started a program to reach out into the community and bring students to the museum to participate in a 4 hour cybersecurity program taught by industry experts. In the first two months of the program, more than 750 students had been through the pilot program. Several of the students who have gone through have been matched with industry professionals as mentors, creating a pipeline to programs like Cyber Patriot and to education programs at local community colleges, the University of Texas at San Antonio, and the Texas A&M System.

With not only all the technology experts at Port San Antonio, but also throughout the San Antonio region, the availability of expertise makes for a center for innovation. Port San Antonio combines integration, collaboration, and innovation with their professionals in defense, logistics, education, aerospace, cybersecurity, and manufacturing, connecting all of these industries to be a port of technology.[2]

Texas should be leveraging its assets to show its value proposition for the IT and cybersecurity industry. If the state does that, it could be seen as the place where cyber and advanced technologies are being integrated into mature industries. Being successful in this pursuit would make Texas the home of protecting all of the aforementioned industries and the home of data analytics.

Local Government - San Antonio Chamber of Commerce

Launched in 2015, Cybersecurity San Antonio is a public private partnership with the San Antonio Chamber of Commerce, City of San Antonio, and Bexar County. San Antonio's technology industry grew from the establishment of the U.S. Air Force Security Service in the 1940's into what would be information technology, electronic warfare, and eventually intelligence surveillance and reconnaissance. The location of roughly 40 other federal agencies in San Antonio, some operating on the defense side, some engaging with the commercial and public sectors, and some engaging municipal and state governments, this has put San Antonio on the map as a hub for

cybersecurity.

Cybersecurity San Antonio is focused around five core areas:
- ➢ The Organization - How do we as a city and a part of Texas develop a sustainable organization to be globally competitive;
- ➢ Military and Government Partners
- ➢ Workforce and Talent
- ➢ Innovation and Economic Development
- ➢ Global Engagement

Cybersecurity San Antonio has put together a consortium between the municipally owned and operated entities. The CIOs, CISOs, and Data Coordinators from the City of San Antonio, CPS Energy, San Antonio Water System, VIA Metropolitan Transit, explore and build collaborative arrangements that would see shared data, shared threat intelligence, and ultimately lead to a municipal collaborative security operations center. This consortium can then tap into the federal assets like the FBI, Air Force, NSA.

Traditionally, expansion of operations and commercial security recruitment of firms has happened on the east and west coasts in Washington D.C., Boston, New York, and Silicon Valley. Talent is the number one differentiator for Texas[3]. Texas has a less hyper-competitive environment than on the coasts and the price point for this talent, while expensive, is very competitive. Other states have state-funded programs to attract companies with tax credits which keeps the talent and the funding outside of Texas.

Local Government - City of McKinney

At the municipal level, education is the front line defense against cyber attacks. They help users become skilled in identifying social threats to the network via email, phone calls, social media, and others. Getting an education program started in every municipality to educate users is imperative. The City of McKinney provides quarterly education for its employees through an educational video that includes a test at the end.

Another imperative action for municipalities to take is to implement standard best practices. However, a majority of small to medium municipalities do not have the dedicated security staff within their IT departments to implement these standards. In most cases, network firewalls are the shortest line of defense.

In addition, the level of sharing about certain threats or attacks incurred by municipalities needs to be greatly increased so everyone can be more aware of what to look out for. An umbrella organization, such as the Texas Municipal League or DIR, would be helpful in gathering and disseminating intelligence on cyber threats including what the attack or threat was, how it was mitigated, and technical details.

One of the biggest barriers to increasing IT awareness for municipalities is funding. While security assessments like vulnerability scans and penetration testing may be available through other governmental entities, such as DIR, the municipalities don't have the funding to take advantage of

those services. IT needs come secondary to police and fire departments, and building communities. However, it is important to keep in mind that the cost of not assessing security risks could be much greater.

There is also a growing demand for IT professionals who want to work for governmental entities. Attached to the issue of municipal funding is the fact that private sector technology jobs can pay a great deal more than salaries available in local governments. It is imperative for city managers to understand the importance of growing technological threats and the need to have skilled staff at the ready. The state could provide matching grants, similar to what's provided to police and fire departments, to hire security staff to help protect against cyber attacks, and help municipalities to procure the software and hardware needed to protect their networks and data.

Local Government - Grimes County

Whether a county is big or small, they all face the same cybersecurity threats. Counties are seeing an increase in PHISHING attacks via email and endure a constant barrage of attacks against individual office firewalls, many from foreign countries. To counter cyber threats, counties can work with agencies like the CIRA (County Information Resources Agency) a division of the Texas Association of Counties, to learn about new Federal, State and local legislation, grant programs and security threats.[4]

The weakest point in the government's cyber armor is going to be the small to medium cities, counties, and school districts who can't afford to keep IT staff on payroll. Having a pool of talent available to these smaller entities through regional collaborations could help alleviate the financial burden while providing much needed expertise.

Recommendations

> - Greater training for all state employees on cyber hygiene.
> - Continue developing the Texas State Guard's cyber response capacity.
> - Increase funding for the Defense Cyber Operations Element of the Texas State Guard.
> - Study the current state statutes and standards to increase cybersecurity cohesiveness with federal partners.
> - Encourage government entities to share data and threat intelligence amongst themselves.
> - Require government entities to create regional Information Sharing and Analysis Centers.
> - Require all government entities to follow the state's 48-hour breach notification requirement.
> - Create a matching grant program to help local government entities upgrade cybersecurity posture.
> - Instruct DIR to create a cybersecurity threat assessment for local governments as a best practice for preventing cybersecurity attacks.

ISSUE #2: CYBERSECURITY EDUCATION, CURRICULUM, TRAINING, WORKFORCE, AND OUTREACH TO INCREASE INTEREST IN THE TECHNOLOGY CAREER FIELD.

Background

The Committee met on Wednesday, May 16, 2018 at 1:00 PM on the campus of the University of Texas at San Antonio in the Student Union Retama Auditorium (Room 2.02.02 on the 2nd floor) in San Antonio, Texas. The committee took invited testimony and public testimony from the following stakeholders:

1. David Abarca (Texas Cybersecurity Council)
2. Joe Sanchez (CyberTexas Foundation)
3. Gregory White (UTSA/CIAS)

Discussion

According to Dr. Gregory White, Texas is doing a good job compared to other states when it comes to increasing the cybersecurity workforce. We have a number of colleges that have cybersecurity programs, many NSA/DHS recognized Centers of Excellence, however we have to do better at filling the pipeline starting early. There are many great programs, including CyberPatriot, which introduces the cybersecurity field in middle school and high school. Thanks to programs like this, many students are so interested in the field that they work towards and receive industry certifications by the time they graduate high school. Having robust cybersecurity paths at universities is important, but because a secondary degree is not the right path for everyone, encouraging certification options is key. There is also a vast differential between the numbers of men and women in the cybersecurity field. Girls' interest in the field drops off as they reach high school, so outreach programs are increasing their focus on the high school level. Outreach programs are also trying to overcome this stigma and encourage girls to continue their cybersecurity interests.

Over the last 16 years, 25 community college districts and individual Institutions and Technical Colleges scaled up courses to offer certificates and degrees in Network Administration, which is the entry-level workforce field of study that leads to many Information Security career opportunities. Del Mar College was one of the first Community Colleges to recognize and address the need for a well-prepared workforce in the cybersecurity field. Through a series of National Science Foundation grants, they developed a small consortium of institutions to create a curriculum and new field of study to address the emerging need. While an associates degree will nearly guarantee a job, it is important for students to add to their degree with various certifications. Many community college programs will include those certification programs with the associates degree curriculum to better prepare students for the industry.

San Antonio is home to the second largest cybersecurity workforce concentration in the U.S., second only to the National Capitol Region including major federal cybersecurity elements. The area also has five NSA/DHS designated Centers of Academic Excellence in Information

Assurance Education including UT San Antonio, Our Lady of the Lake University, Texas A&M University - San Antonio, San Antonio College, and St. Philip's College. The CyberTexas Foundation provides scholarships, through industry support, and internship opportunities. With the vast industry expertise available in Texas, the CyberTexas foundation is able to find mentoring opportunities to students interested in the field, and those who participate in the Air Force Association's CyberPatriot competition.

One of the CyberTexas Foundation's focuses is on opportunities for area youth to learn and experience cybersecurity, including through the CyberPatriot cyber defense competition. CyberPatriot has a Center of Excellence in the area to increase middle school and high school interest in the Cybersecurity field. CyberPatriot is a competition that puts teams of high school and middle school students in the position of newly hired IT professionals tasked with managing the network of a small company. In the rounds of competition, teams are given a set of virtual images that represent operating systems and are tasked with finding cybersecurity vulnerabilities within the images and hardening the system while maintaining critical services. Teams compete for the top placement within their state and region, and the top teams in the nation earn trips to Baltimore, MD for the National Finals Competition where they can earn national recognition and scholarship money. San Antonio fielded 309 teams during the 2017-2018 season, more than any other city in the U.S. The greatest growth was in the middle schools with more than 70 teams competing. San Antonio has sent 13 teams to the finals in the last seven years, including being national champions in 2012. The CyberTexas Foundation also worked with Southwest ISD to develop a TEA-approved innovative course called the Principles of Cybersecurity that is available for free to any middle school or high school across the State of Texas.

Recommendations

➢ Encourage 2- and 4- year institutions to develop security programs.
➢ Develop a Texas program to fund scholarships similar to the National Science Foundation (NSF) Scholarship for Service (SFS) program that could help increase interest in the career field and fill needed cybersecurity positions at the state and community levels.
➢ Encourage middle and high schools to develop classes in computer science and cybersecurity.
➢ Ensure all middle and high schools know they have access to a free TEA-approved cybersecurity course and curriculum.

ISSUE #3: INDUSTRY PERSPECTIVE ON CYBERSECURITY INNOVATION, EDUCATION, AND CERTIFICATION.

Background

The Committee met on Wednesday, May 16, 2018 at 1:00 PM on the campus of the University of Texas at San Antonio in the Student Union Retama Auditorium (Room 2.02.02 on the 2nd floor) in San Antonio, Texas. The committee took invited testimony and public testimony from the following stakeholders:

1. Bob Butler (Self)
2. Chris Humphreys (Self)
3. Sarah Matz (CompTIA)
4. Michael Wyatt (Texas Business Leadership Council)

Discussion

The U.S. technology sector is one of the largest industries in the U.S. economy. According to CompTIA's annual Cyberstates Report[5], the technology sector market is $3.7 trillion globally and $1 trillion in the U.S., employing approximately 5.7 million Americans. To give perspective, the gross output of the technology sector exceeds the legal services industry, the automotive industry, the airline industry, the motion picture industry, the hospitality industry, the agriculture industry, and the restaurant industry. In Texas, the technology sector is responsible for an estimated 8.7% of the overall state economy, and is home to over 37,000 technology businesses. Texas saw a 41.4% increase from 2016 to 2017 in the number of job postings related to emerging technologies, such as the Internet of Things, smart cities, drones, artificial intelligence, machine learning, and virtual and augmented reality. Overall, employment in the technology industry grew by over 7,600 jobs in 2017, and the industry contributed over $125 billion to the state's economy. With nearly one million workers, Texas ranks second among the 50 states and the District of Columbia in net technology employment. The Texas technology workforce makes up 7.2 percent of the state's total workforce.

Currently, there is a gap between how important cybersecurity issues are and the amount of involvement in those issues by senior leaders in the private and public sectors. This disjuncture is a direct result of the "knowledge gap" between most executives and cybersecurity professionals. Corporate leaders and state agency heads typically have considerable managerial experience and business acumen, rather than narrow, technical expertise. Most do not have the requisite knowledge to properly analyze the technical information given by cybersecurity professionals. Similarly, cybersecurity professionals often lack knowledge about risk management, corporate governance, and strategic planning, which makes it difficult for them to communicate effectively with senior leaders. Thus, the "knowledge gap" can also quickly become a "communications gap."

However, to manage a complex challenge like cybersecurity, an organization must be able to collaborate across disparate functional areas—including defense, prevention, detection, remediation, and incident response. Such coordination requires that company and state agency

leaders openly share their expertise, agree upon priorities, and ensure that security efforts are aligned with objectives.

Security can no longer be isolated as a technical problem with a technical solution; it must be prioritized as a critical business concern. The greatest weakness in most companies' or agency security is not their technology, but their people and processes. 97% of attacks attempt to trick a user to unwittingly hand over valuable data or information. Defending against these kinds of attacks requires more than just the latest patch or upgrade. Instead, the culture must emphasize and value cybersecurity. Senior executives should lead this change by providing adequate resources and using cybersecurity metrics as key performance indicators within state agencies.

We often think of cybercriminals who attack networks from faraway locations, however, the greatest threats typically come from within an organization. In the 2016 Cyber Security Intelligence Index[6], IBM found that 60% of all attacks were carried out by insiders. Of these attacks, three-quarters involved malicious intent, and one-quarter involved unknowing accomplices. In Sarah Matz's testimony[7], citing a Vanson Bourne survey, IT employees were actually more likely than average to engage in risky cyber behaviors, such as opening attachments, downloading third-party apps without authorization, and clicking on links in social media sites. Training makes a difference, if it is done right. To develop effective training programs, state agencies should consider the different levels of need across the organization.

Public sector organizations are attractive targets for bad actors due to the treasure trove of valuable data that can be used for monetary gain. In addition, espionage is a common objective with governmental attacks focusing not only on military secrets, but also political information. Given the various missions of government entities, "hacktivism" is a concern. In the Verizon 2018 Data Breach Investigations Report[8], over 53,000 incidents, with 2,200 confirmed breaches, provides insight into the criticality of addressing cybersecurity posture. Worth noting, cybercriminals have success using techniques around for many years, which shows the lack of cybersecurity posture in general. From the insider threat perspective, human error accounted for one in five breaches. For example, even with training for not clicking on unknown links, 4% of employees and contractors will always click.

Additionally, the Verizon Report finds that ransomware is on the rise, accounting for 40% of malware in organizations. When ransomware attacks a life and safety entity, it's no longer a risk of data, it is a risk of human life. 87% of compromises take an average of 16 minutes from attack to compromise. And, 68% of detections take months, if not longer. There has been a focus on prevention, but prevention does not always work.

According to 2016 Deloitte-NASCIO Cybersecurity Study[9], the commercial sector spends roughly 7%-9% of total information technology budgets on cybersecurity. However, compare that to state government, where over 50% of the states invest zero to 3% of information technology spending on cybersecurity, with another 20% in the 3-5% range. With limited budgets in government entities, not everything has to be done through general appropriations. Entities can take advantage of grants from the Department of Homeland Security, and creating cross agency collaborations can help scale and be a force multiplier on funds already appropriated.

Across industries, but especially in the public sector, the cyber talent gap exists, and will remain a challenge for the foreseeable future. By 2022, the global shortfall in the information security workforce is projected to exceed 1.8 million[10], and an astounding 313,000 cybersecurity jobs in the U.S. remained unfilled as of December 2018[11]. As technology trends evolve and demand for a cyber workforce increases, training opportunities are failing to meet the need for specialized cyber talent. The National Initiative for Cybersecurity Education (NICE) framework provides guidance on cybersecurity education and workforce development, and is recommended to be utilized by any institution looking to develop and increase talent for cybersecurity personnel. While it is important for entities to purchase advanced technology for cybersecurity purposes, it is just as important to establish and validate cyber policies and procedures. Entities need to conduct risk assessments to determine a hierarchy of protection within their organization.

Also, it is important to remember that additional regulatory mandates for cybersecurity are not sustainable to proactively address the cyber threat. The challenge with over-regulating the cyber threat is that by the time the bureaucratic standards development process has finished a regulation or standard, the cyber threat to be mitigated from that new standard or regulation has evolved. As a result, the standards development process is never-ending – it is constantly trying to catch up with the latest iteration of the targeted threat. Meanwhile, the security risk is neglected while organizations wait for the new standard. Also, organizations are able to use the plausible deniability defense if a security compromise occurs because they can point to the fact they are "compliant." The only way to sustain cyber threat and balance regulatory expectations is to adopt a risk-based model that incorporates the numerous already well-established security best-practices where compliance is a proactive byproduct of being secure instead of simply reacting to a new regulation.

Since the Texas Cybersecurity, Education, and Economic Development Council (TCEEDC, the council preceding the Texas Cybersecurity Council) released their report[12] in 2012, the State of Texas has made great strides in improving its cybersecurity posture. However, there are many improvements recommended in the report that could be implemented today. Among those recommendations, TCEEDC felt the state needed sustainable public-private partnerships to scale best-practices developed in the cybersecurity industry for use in government, implement a "Cyber Star" resiliency program, increase workforce development initiatives across the state, and implement a comprehensive state-wide education approach to cybersecurity.

Investment in these areas brings multi-faceted enhancements to the State. Providing guidance to smaller businesses or organizations helps them grow and enhances the stability of the smallest units of the Texas economy and increases entry-level cybersecurity jobs. Fostering more cybersecurity operations at the entry level has the cascading effect of improving the entire cybersecurity workforce and ecosystem. Private companies in more security-aware industries such as critical infrastructure may rely less on guidance provided by the state, but are nonetheless made more effective and resilient through increased state collaboration.

In addition, Texas has a relatively new and unique partnership with the Army Cyber Institute (ACI) which is spurring greater collaborative action for the state in the area of cyber incident response improvements. In 2016, the ACI initiated an experimentation and cyber research program, known as Jack Voltaic (JV), to assess and learn from local community response to cyber incidents. The

first experiment took place in New York City, and was orchestrated by a partnership between ACI and Citigroup. In 2018, ACI and corporate partners partnered with the City of Houston, Harris County and the state of Texas to simulate a combined natural disaster and cyberattack which impacts multiple critical infrastructure sectors in the City of Houston. JV 2.0 will demonstrated the challenges of responding to two incidents simultaneously and assessing the impact of physical infrastructure degradation on an interconnected, networked environment and vice versa. Specifically, JV2 assessed the City of Houston's initial response capability, the communication between public and private partners, the integration of military forces, and the military's coordination with regional and state authorities. This was the first time Texas exercised a combined cyber/physical incident response, leveraging all of the capabilities of public-private sector partners. Exercises like this set a foundation for developing state-wide incident response programs and campaigns. Key takeaways from the JV 2.0 exercise are:

- In terms of emergency response, Texas must train in a "bottom up" manner. First responders must be trained to deal with cyber and physical threats because there is no time to wait for a federal response.
- The State is very prepared for physical threats, but lacks the infrastructure necessary to combat cyber threats.
- The State should create a public-private partnership campaign for rapid response training exercises on a regular basis to better protect critical infrastructure.
- The State must develop methodologies that are repeatable from city to city and must find a way to better integrate frameworks. Modeling technologies can be used to simulate threats and better prepare first responders.
- The Texas Military Department needs authorization and a play book so they can more readily exercise cyber security responses.

Recommendations

➤ Ensure employees with different responsibilities and knowledge get the right type of IT training:
  o For cybersecurity professionals: go beyond routine training and focus on ongoing education
  o For non-IT employees: training should be frequent, engaging, and relatively short
  o For executives and directors: remember they too need training, even in "basic" security protocols
➤ Prioritize governmental entity spending on threat detection technology.
➤ Encourage state agency executive teams to participate in cybersecurity threat simulations with IT staff.
➤ Encourage government entities to adopt risk-based cybersecurity standards incorporating security best-practices instead of regulating by reacting to attacks.
➤ Implement a "Cyber Star" program to foster improvement of cyber resiliency in public infrastructures across the state and increase public trust by establishing a baseline for responsible cyber operations.

ISSUE #4: STATE AGENCY CYBERSECURITY AND DATA PRIVACY PRACTICES, AND H.B. 8 (85R) IMPLEMENTATION.

Background

The Committee met on Wednesday, September 26, 2018 at 1:00 PM in Room E2.016 of the Texas Capitol. The committee took invited testimony and public testimony from the following stakeholders:

1. Invited Testimony
    - Darran Anderson (Texas Department of Transportation)
    - Ernesto Ballesteros (Department of Information Resources)
    - Allison Benz (Texas State Board of Pharmacy)
    - Steve Buche (Texas Health and Human Services)
    - W. Boyd Bush (Texas State Board of Dental Examiners)
    - Seth Christensen (Texas Juvenile Justice Department)
    - Shirley Erp (Texas Health and Human Services)
    - Mark Havens (Texas General Land Office)
    - Skylor Hearn (Texas Department of Public Safety)
    - Mike Higginbotham (Texas Department of Motor Vehicles)
    - Melvin Neely (Texas Department of Criminal Justice)
    - Melody Parrish (Texas Education Agency)
    - John Raff (Texas Facilities Commission)
    - Brandon Rogers (Texas General Land Office)
    - Zhenzhen Sun (Texas Higher Education Coordinating Board)
2. Public Testimony
    - Alex Meed (Self)

Discussion

Department of Information Resources

In laying out the current cybersecurity threat landscape, Mr. Ballesteros said there is an increased and growing threat whether it is from individual actors or nation states, and their capabilities are growing faster than the State's ability to contend with them. The state cannot deal with the threat of cyber attacks alone, and the issue must be addressed by collaborating with the public/private sectors and institutions of higher education. The Texas Cybersecurity Council plays an important role in this collaborative effort. The council is made up of state government, higher education, and private industries. These three communities can help provide unique perspectives on cybersecurity threats that affect all of us, and the council aims to use these perspectives and insight to make policy recommendations. The council works on implementation strategies using subject-matter experts who can provide insight on how to approach and solve problems. These deliverable are then reviewed and recommended to the legislature for consideration if appropriate.

One of Mr. Ballesteros' top priorities leading up to the next legislative session is to continue

exploring viable options for standing up a state level information sharing and analysis organization that can be a vehicle to foster coordination with the public and private industries.

Health and Human Services Commission

The Health and Human Services Commission (HHSC) has over 38,000 full-time employees, operates 70 offices, administers more than 500 programs, serves more than 5 million clients, manages over 115,000 computer devices, is responsible for 1.6 million network addresses, and faces more than 94 million cyber attacks annually[13]. HHSC adheres to many state and federal requirements so it takes a very diligent effort to keep up with these arduous standards.

HHSC has both proactive and reactive cybersecurity measures. There are employees scanning screens looking for threats along with recently purchased technology that automatically stops threats. However, there is still the problem of stopping individuals from clicking on links. In implementing H.B. 8, HHSC has been redacting confidential information from websites and working with their contracting department to remediate websites.

State Board of Dental Examiners

The State Board of Dental Examiners has over 90,000 licenses with valuable information to protect[14]. In the 2018-19 biennium, the legislative appropriated funding for AWS cloud services, firewall services, and Microsoft 365 as remote access for workers. The agency is currently in the process of moving everything to the cloud, and is exploring options for cloud vendors. The agency saved money by selecting a more cost efficient firewall provider. While the agency will be switching over to Microsoft 365, they are currently researching which direction they want to take with file processing software as most platforms and templates use Google. Currently, though, the agency already has a virtual private network (VPN) so their employees can utilize remote access.

State Board of Pharmacy

The State Board of Pharmacy had requested $340,000 for information technology funding in the 2018-19 biennium, and ended up being appropriated $229,000. They used this funding to bring their network up to data protection standards and enable field inspectors to digitally upload pharmacy inspection reports to improve efficiency and reduce errors. The agency had also requested funding for a voice over internet protocol (VoIP) phone system, which was funded separately and implemented.

Texas Department of Transportation

The Texas Department of Transportation (TxDOT) has implemented many provisions of H.B. 8 as required by state agencies, including continuing education for cybersecurity, anti-phishing campaigns relative to emails, and information vulnerability assessments. Currently, they are implementing best practices for cybersecurity in day-to-day operations and traffic management operations.

Last session, $10 million was appropriated from the state highway fund, which has enabled

TxDOT to meet some of their security objectives. TxDOT currently uses the MATURE Program, an acronym aimed to summarize security objectives:

- **M**anage our risk, patches, software and hardware to limit exposure to threats;
- **A**utomate detection, response, and recovery efforts in a much more extensive manner across the department to allow for personal acting upon those automated detections;
- Op**T**imize the teaching of our employees in a greater manner and advance the employee training that we already conduct;
- **U**se advance analytics to enable our business operations both internally as well as in the cloud environment in a much more extensive manner than we currently do;
- **R**enewing our independent verification and validation efforts that look at the security capabilities provided by our outsourced IT provider and validating those securing activities as a separate step when we conduct operations;
- **E**xtend our encryption capabilities across the department from what the current capabilities currently are.

Increasing technology, such as internet connections and connected vehicles, requires a more sophisticated traffic management network that will also need a mature cybersecurity network. The traffic system is made up of endpoints, such as traffic lights and sensors, that all need managers to detect anomalies and cyber threats and to respond quickly. TxDOT continually assesses and improves the information security maturity level and capabilities, and has steadily improved its overall posture.

TxDOT also learns from other states' experiences. For instance, when there was a recent attack on the Colorado tollway system, a TxDOT officer traveled to Colorado to learn about how the state responded and handled the threat. There is information sharing between states in regards to these matters. TxDOT did have an incident where W2 and account information was compromised. The agency worked with their employees, the IRS, and the FBI to flag the affected accounts so there could be no false filing of tax returns. They contained the situation and no financial consequences were absorbed by the employees. Phishing risks have been mitigated since the incident with updates to the security system and protection protocols.

Department of Motor Vehicles

The Texas Department of Motor Vehicles (DMV) holds millions of motor vehicle records and has a high priority to protect them with active cybersecurity measures. DMV covers all aspects of cybersecurity: user training, network security, physical security controls, and resiliency programs. Their short term cybersecurity goals are:

- Procure a security, information, and event management system
- Conduct a biennial Texas cyber security framework assessment
- Execute application vulnerability assessments and penetration tests for all TX DMV internet facing applications that process confidential and sensitive information
- Implement an application security scanning and code quality and analysis service to conduct advance software analysis and application security scans

- Implement image and place tools to facilitate the rapid response and quick turnaround of individual workstation malware remediation
- Implement advanced threat protection email security cloud service to validate that email links and attachments are free of malware
- Procure cloud services to centrally manage certificates for encrypting communication with internal and external systems
- Implement a centralized internet protocol security management solution to integrate the management of three key address services into a single console allowing simple management and a more agile network change management process
- Implement mechanisms and procedures to simplify motor vehicle records and safeguard their integrity

Looking ahead, DMV will continue to work towards its short term goals, but will also pursue additional initiatives to advance their security posture. These initiatives include two-factor authentication, end point data loss prevention, and access management automation.

Texas Facilities Commission

The Texas Facilities Commission requested funds in the 2018-19 biennium for cybersecurity employment purposes, which enabled them to hire an Information Security Officer. The Commission will not be able to utilize the DIR-established program to complete another security assessment, establish an agency-wide security council with representation from every division, establish an ongoing process to educate all personnel about security threats and implement security initiatives agency-wide, increase integration of building controls and IT function to shift the primary function of partnership from connectivity to security, provide guidance to collection of logging and monitoring security system alerts and alarms, move quickly to address threats, and implement best practices and recommended security improvements more fully in a shorter timeframe while applying appropriate security to business practices.

Moving forward, the Commission will look to build off its success through additional funding requests. The Commission will be requesting approximately $400,000 for the 2020-21 biennium.

Department of Criminal Justice

The Texas Department of Criminal Justice's (TDCJ) information security program is governed by three main policies:
- Texas Administrative Code 202 - Establishes a baseline of security standards for Texas state agencies;
- Internal Information Resources Security Program - Establishes information security criteria for information systems that support the operations of the organization. This specifies how much security is needed relative to the level of risk and informs employees their level of responsibility in maintain TDCJ's information;
- Agency Directives - Provides guidance on information resources areas.

Information resources policy establishes the guidelines for maintenance, expansions, and use of network infrastructure. Areas such as auto logging, procedures for firewall, and other primary systems are covered. Education, virus protection, and endpoint protection are the most important things TDCJ does to prevent cyber attacks and threats. The agency trains all information resources/security employees to the best of their ability, uses Malwarebytes to detect malware and viruses, has implemented intrusion detection and prevention devices, reviews and tests code before it is put into production, and stays current on patching, which is always tested and reviewed before being implemented.

While staying apprised of the latest cybersecurity risks and implementations help, TDCJ is facing a crisis if their Offender Management System is not replaced soon. The system currently in use is 40 years old and written in COBOL, a programming language so old it is no longer being taught in college. The vast majority of programmers who are educated in how to run this system are in the Baby Boomer generation, and are aging out of the workforce at an increasing rate, while programmers entering the workforce are not educated in the language. As of September 2018, TDCJ had not been able to hire new programmers educated in COBOL in 46 months even though they have positions to fill. A system that is written in a newer language is needed so TDCJ can hire programmers from a much wider pool of applicants. The agency will have a $24 million legislative appropriation request for the 2020-21 biennium to cover the cost of the new system. An additional $10 million will be requested in the 2022-23 biennium to finish out the project.

Juvenile Justice Department

In the 2018-18 biennium, the Texas Juvenile Justice Department (TJJD) was appropriated $6.8 million for an infrastructure refresh and $715,606 for cybersecurity improvements. As of September 2018, TJJD had procured $5.9 million in new hardware, software, and equipment for its refresh and cyber improvements. While not funded by the legislature, the agency's youth case management system desperately needed an update. TJJD's executive director requested and received approval from the Legislative Budget Board and the Governor's office to transfer appropriations for the funding of this system. TJJD has also encumbered nearly $33,000 of the cybersecurity improvement dollars appropriated to hire an information security analyst who is responsible for monitoring and maintaining infrastructure to protect information systems from unauthorized use.

Going forward, the agency has plans to improve IT and cybersecurity functions. In 2019, they plan to use $915,000 for network and storage replacements, core network fiber upgrades, and modernizing voice systems for compatibility with a new incident response call center. They will also use $617,000 for software to manage and monitor file share permissions, implement software to consolidate and streamline account management for systems/applications, and to fund an information security analyst.

Department of Public Safety

The Texas Department of Public Safety (DPS) is on its way to developing a strong cybersecurity system. DPS is aggressively maturing its policies to meet the statutory requirements of H.B. 8, including:
- ➤ Adopting the state agency plan assessment to provide continuous maturing level monitoring improvement;
- ➤ Bolstering staff with an IT auditor;
- ➤ Seeking third party auditing of systems every five years;
- ➤ Adopting NIST security framework and risk management framework to be implemented by 2020.

DPS received $5 million in cybersecurity funding through the cybersecurity amendment. $1.8 million was invested in data loss prevention, $2.1 million was invested in intrusion prevention systems such as malware protection, firewalls, email security, and network monitoring, and $960,000 in security vulnerability management systems.

In the 2020-21 biennium, DPS will be requesting $11.1 million for seven additional FTEs, four cybersecurity analysts for incident response, and one cybersecurity analyst for governance and compliance with security risk tools.

Texas statute has provided for the disclosure of driver record information in certain circumstances since 1959. In 1975, an Attorney General decision stated the open records law mandated the disclosure of driver record information in certain circumstances and required the Department to provide a large volume of driver record information to a requestor. The Driver's Privacy Protection Act of 1994 (DPPA) provided nationwide standards for disclosure, however Texas' Motor Vehicle Records Disclosure Act of 1997 is more restrictive than the federal laws. Fees collected from the purchase of driver records are deposited in the Texas Mobility Fund. There are 2,797 vendors that obtain records from DPS, and on average these amount to 1.2 to 1.3 million records per month. Fees range from $4 to $20, and in 2017 the agency collected $67,173,002.

Texas Education Agency

The Texas Education Agency (TEA) commissioned Gartner, a research and IT firm, to conduct a study to assess TEA's cybersecurity risk. The study had 40 controls and was scored on a scale between 0-5 with 5 being the lowest risk level. It was determined that 3.25 was a satisfactory due diligence level for TEA. 36 of 40 controls scored 3.25 or higher with the remaining 4 scoring lower. To increase those unsatisfactory scores, TEA consolidated all servers so that all security patches could be applied easily, but other upgrades and work need funding. The agency asked for funding for the 2018-19 biennium, but only received a partial funding, which is currently being used to fix the identified problems.

TEA also received funding for the Texas Student Data System (TSDS), which contains 3.4 billion

records. The TSDS allows student data to be collected more efficiently and to consolidate data into one system to take the burden off the school districts. $968,000 was allocated for the biennium to incorporate in-house applications. S.B. 2080 allocated funding for a residential facility tracker, requiring the tracking of children with disabilities who reside in residential facilities, and will be remediated and incorporated in the TSDS.

Higher Education Coordinating Board

As a source for higher education data and as a provider of student loans in Texas, the Texas Higher Education Coordinating Board receives millions of records each quarter. Due to the magnitude and value of the records held, the agency views cybersecurity as one if its top priorities. The core mission of the agency's cyber security framework is to assess and improve the agency's ability to detect, prevent and respond to cyber incidents. The framework uses business drivers to guide cyber security activities and considers cyber security as part of the agency's risk management processes.

The Board's security initiatives implementation roadmap is published at the beginning of each fiscal year to help prioritize the agency's security progress initiatives and to help secure resources. H.B. 8 and DIR publications were used as guidelines. The Board works closely with its security governance committee to understand their business priorities and determine acceptable levels of risk. The goal of this roadmap is to support the Board's mission, support the state higher strategic plan, and to help improve the maturity level of security control objectives.

With implementing H.B. 8, the Board established a continuing cybersecurity training program giving IT staff access to an online learning platform to seek help when needed, a computer security incident response team was established to respond to cyber threats, and a security governance committee was established to set priorities and drive initiative related to information security and privacy issues. During 2019, the Board will be working with the information security officer to continue to lead efforts to enhance their cybersecurity framework and to improve maturity levels of security control objectives.

In the 85th session, the Board was allocated $430,000 for security initiatives. A portion was used to identify and access management initiatives and to implement a cloud-based solution to protect data and privacy. The rest supported the security incident and event management initiative. Infrastructure was improved and more technical controls were introduced.

The Board is planning to request two exceptional items for the 2020-21 biennium. First, they would like to introduce a service-oriented architectural design and to consolidate existing applications. This would assist in legacy system modernization. Second, they would like funding to create a permanent privacy officer position that is responsible for the development of privacy practices and polices.

Prior to January 2015, the General Land Office (GLO) had no formal information security program in place. In the summer of 2015, it was discovered that the GLO did not have the infrastructure in place to meet the coming requirements. To address these concerns, the GLO established the office of information security.

The GLO operates eight long-term nursing care facilities for veterans which need to protect large quantities of personal and medical information. The loan program operated by the agency requires the storage of sensitive and private financial documents. The agency also handles crucial documents relating to disaster recovery, like personal information on those who lost their housing during Hurricane Harvey and applied for short term housing relief. Since creating the office of information security, the GLO has expanded their cybersecurity staff from two to seven with the primary goals of remediating security control gaps and to mature their information security program.

In 2017, the office of information security spent $1.2 million in finishing the protection of records. The office is budgeted just over $1 million for 2019. The GLO also had $80,000 appropriated for data loss prevention and vulnerability management as required in H.B. 8. The GLO is continuing to enhance standards to prepare for future cyber threats and looks to maintain competent and capable staff.

Recommendations

- ➢ Continue to appropriate funding for legacy system replacements.
- ➢ Ensure state agencies continue maturing their cyber policies.
- ➢ Encourage migration of state agency applications and data to cloud-based services.
- ➢ Require all new state IT procurements to be cloud-ready.
- ➢ Require DIR, in conjunction with institutions of higher education, to provide and promote a centralized repository of cybersecurity education and training available to all government entities in Texas.
- ➢ Empower state agencies and government entities to utilize next-generation technologies such as cryptocurrency, block chain, and artificial intelligence.
- ➢ Review state policies and procedures on collecting, storing, deletion, and sale of citizen data from 1984 to today.

ISSUE #5: THE STATE OF ELECTION SECURITY IN TEXAS.

Background

The Committee met on Wednesday, September 26, 2018 at 1:00 PM in Room E2.016 of the Texas Capitol. The committee took invited testimony and public testimony from the following stakeholders:

1. Dana DeBeauvoir (Self)
2. Keith Ingram (Texas Secretary of State, elections division)

Discussion

H.B. 8 required the Secretary of State (SOS) to conduct a study on vulnerabilities and risks of cyber attacks against Texas' election systems. As of September 2018, there have been no documented cyber attacks on voting systems, voting registration systems, or election infrastructure.

When it comes to election infrastructure, there are four main components: public facing websites, management of election night returns, the statewide voter registration database, and the voting equipment:

➢ Public Facing Websites - There is no confidential information housed on these websites. It is important they remain available and provide election information to the voters throughout the election process.

➢ Management of Election Night Returns - These are managed in-house. The SOS is currently in the process of implementing multifactor authentication. The systems are currently secure, but they are segmented from one another in different programs. The goal is the use federal funding o upgrade to one sustainable, secure, end-to-end system from candidate filing through the canvass of the general election. The SOS has also upgraded security on the reporting website where citizens can look up their registration status and polling locations. A more robust protection against denial of service attacks has been established to keep the website up and running.

➢ Statewide Voter Registration Database - This database contains personal information of Texas residents, including social security numbers. By virtue of the information it contains and the fact that it is connected to the internet, the database is a more enticing target to hackers. However, as of September 2018, there have been no attempted or successful attacks on this database. Texas is one of the first states to obtain a federal funded Albert sensor on the voter registration database to monitor traffic. 38 states now use Albert sensors and information is shared between states on attempted attacks so other states can take appropriate measures.

➢ Voting Equipment - Computers that program the machines and tabulate the results are never connected to the internet and are kept under strict security in-between elections. Equipment cannot be used for an election unless it has scored a 100% on the tabulation

tests. The SOS elections division has visited many elections offices across the state and have not found anyone who is not following the election security guidelines. The division will request, as an exceptional item, funding for four new employees whose job will be to visit counties across the state to ensure security procedures are being followed. They will train anyone who is not following procedures properly to do a better job.

Election security is an on-going and never finished race, but the recently appropriated $24.5 million in federal Helping America Vote Act (HAVA) dollars will aid the state and counties tremendously in protecting elections. The SOS is confident that every citizen can trust the election results and that the integrity of elections is not compromised.

In Travis County, the elections clerk of 31 years, Dana DeBeauvoir, began studying how to improve the security and efficiency of electronic voting systems in 2005. She had been trying to make incremental changes to existing electronic voting systems in order to anticipate and confront immerging threats. Electronic voting systems became mainstream after the 2000 presidential election. States began buying these systems to avoid paper issues. But elections administrators can only buy systems that are certified by the State.

Paper trails were added to electronic voting in the early 2000s. They were initially poorly designed and did not work very well. No one liked them, so they were rejected by the marketplace. However, paper trail voting systems have greatly improved and immerged back on the market in 2016. With the growing threat of cyber attacks, the development of a new electronic voting system that has a paper trail, is secure, and can thwart cyber security attacks when needed. Ms. DeBeauvoir began meeting with cybersecurity experts, statisticians, and programmers from top institutions. They worked together to design an encrypted electronic voting system with a paper trail to ensure that results can be verified by elections officials and third parties. Travis County issued a request for procurement (RFP), known as STAR-vote, to build the designed system, but no one who responded was able to do a full build out and develop the system because the RFP went against the grain of what was widely built and used in the marketplace.

Travis County then returned to the normal marketplace to purchase a new voting system, but wanted something as close to STAR-Vote as possible with standards they believe should be universal:
  ➢ Do not buy a system unless it offers a voter verified paper audit trail to be used for recount purposes.
  ➢ The paper trail has to offer better security and must support risk limiting audits. Risk limiting audits are the first step to being able to offer end-to-end verification.
      o End-to-end verification - When a paper trail is introduced, the ideal situation is to have a voter with an unambiguous ballot, print off their selections from the electronic submitted ballot. The voter then verifies that the paper is correct and inserts it into a separate machine to make a electronic copy of the paper copy. An audit would ensure that the electronic copies match the submitted ballots. This

constitutes a voter verified paper audit trail because the voter has to confirm that the paper copy is correct before submitting the electronic ballot.

While there has never been a successful hack or attack of elections systems in Texas, that is not to say there haven't been attempts. Thinking about an attack in the form of a home invasion, when a home invader tests the door to see if it's unlocked, that is not technically an attack, just an attempt. While cyber criminals have attempted to enter elections system, the cyber "doors" have always stayed closed and locked.

Recommendations

➢ Ensure the Secretary of State's office continues to assist counties in procuring new voting equipment.
➢ Continue to provide adequate funding for security systems around the state's voter registration database.

ENDNOTES

[1] Hearing Before the H. Select Comm. on Cybersecurity, 2018 Leg., 85th Interim (Tex. 2018) (written testimony of Todd Kimbriel, Department of Information Resources).

[2] Hearing Before the H. Select Comm. on Cybersecurity, 2018 Leg., 85th Interim (Tex. 2018) (written testimony of Jim Perschbach, Port San Antonio).

[3] Hearing Before the H. Select Comm. on Cybersecurity, 2018 Leg., 85th Interim (Tex. 2018) (testimony of Will Garrett, San Antonio Chamber of Commerce).

[4] Hearing Before the H. Select Comm. on Cybersecurity, 2018 Leg., 85th Interim (Tex. 2018) (testimony of Gregg Cannon, Grimes County).

[5] (The Computing Technology Industry Association (CompTIA), 2018)

[6] (IBM Corporation, 2016)

[7] Hearing Before the H. Select Comm. on Cybersecurity, 2018 Leg., 85th Interim (Tex. 2018) (testimony of Sarah Matz, CompTIA).

[8] (Verizon, 2018)

[9] (Robinson & Subramanian, 2016)

[10] (Frost & Sullivan, 2017)

[11] (CyberSeek, 2018)

[12] (Texas Cybersecurity, 2012)

[13] Hearing Before the H. Select Comm. on Cybersecurity, 2018 Leg., 85th Interim (Tex. 2018) (testimony of Steve Buche, Health and Human Services Commission).

[14] Hearing Before the H. Select Comm. on Cybersecurity, 2018 Leg., 85th Interim (Tex. 2018) (testimony of W. Boyd Bush, State Board of Dental Examiners).