Chairman Darby and members:

My name is Andy Bennett and I serve as the State Deputy Chief Information Security Officer at the Texas Department of Information Resources ("DIR"). Thank you for allowing me to testify before the House Select Committee on Mass Violence Prevention and Community Safety. I am here to address Charge Number Four: "Evaluate the ongoing and long-term workforce needs of the state related to cybersecurity, mental health, law enforcement, and related professionals." Prior to joining DIR, I worked in an array of industries and sectors from oil and gas, to banking and finance, retail, applied research, law enforcement, higher education, and government. While my experiences over the last two plus decades have shown me that there are incredibly talented and dedicated people working to support the secure delivery of technology services to customers and constituents alike, there are simply not enough of them to meet the demand. The current global deficit of cybersecurity professionals is estimated at over 4 million.[1]

Although this problem is not unique to government, government is uniquely positioned to feel the long-term negative effects of this shortfall.[2]

It is easy to dismiss the outrageous numbers being thrown around as they are so large that they seem unreal. Go to any conference where they talk about such things and you are likely to hear that cybersecurity is one of the few professions with negative unemployment[3] even in these turbulent times. While this is true, and has been for quite some time now, it is far from the whole story.

To better understand the whole story, we need to skip to the end. By now, everyone almost certainly knows about the devastating impacts that cyber-attacks can have on business and governments of all levels and sizes. In August of 2019, twenty-three Texas local government entities were subjected to a coordinated attack that saw their systems and operations crippled by ransomware. In May of this year, the Texas Department of Transportation (TXDoT) and the Office of Court Administration (OCA) were both attacked, and again it was ransomware. These attacks threaten critical infrastructure and government functions.[4] They threaten the continuity of our water supply, the stability of our power grid, the safety of our roads, and even the operations of an entire constitutional branch of Texas government.

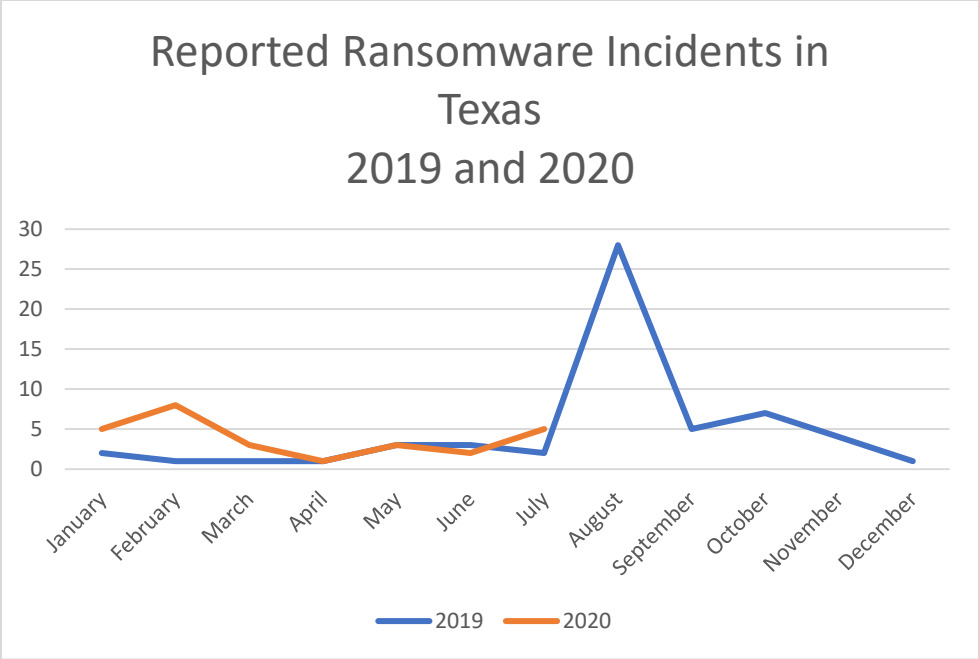
---

[1] (ISC)2 CYBERSECURITY WORKFORCE STUDY, 2019 - https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482

[2] U.S. DHS CyberSkills Task Force Report Fall 2012 https://www.dhs.gov/sites/default/files/publications/HSAC%20CyberSkills%20Report%20-%20Final_0.pdf

[3] Texas Comptroller "Texas' Cybersecurity Industry" Exhibit 4: https://comptroller.texas.gov/economy/economic-data/cybersecurity/texas.php

[4] It is Time to Get Serious About Securing Our Nation's Critical Infrastructure: https://www.cisecurity.org/blog/it-is-time-to-get-serious-about-securing-our-nations-critical-infrastructure/



Unfortunately, this is a story that repeated itself many more times across Texas. Texas has already seen at least 27 additional ransomware attacks this year, and our adversaries show no signs of stopping or even slowing down.[5] While ransomware is certainly recognizable and a constant threat to Texas government, it is by no means the only type of attack cybersecurity professionals face on a daily basis. Texas is the tenth largest economy[6] in the world, and it faces nation-state level threats every day, often with small town resources.

Texas government cybersecurity professionals defend against denial of service[7] attacks, detect phishing[8] campaigns and whaling[9] attempts, watch for the downstream effects of watering hole attacks[10], guard against the exploitation of unpatchable vulnerabilities[11] in legacy systems[12] found throughout government, and face advanced persistent threats[13] from nation states. They keep vigil watch over the integrity of our election systems, investigate events, remediate malware[14], identify risks, respond to incidents, report to executives, and sometimes even testify to the legislature. They are constantly pulled in many different directions, often recruited from other functions to be the go-to security experts in their organizations, as there is no solid pipeline and supply of well-qualified professionals waiting to be hired.

I can relate to this story as I only got into cybersecurity by accident. I got my start as a cybersecurity professional by simply being at work the day my employer had a security incident. I was a field technician and had been working in IT for 7 years when I was assigned to take charge of the response. I

---

[5] https://www.infosecurity-magazine.com/news/cyberattacks-up-37-over-past-month/
[6] Putting America's enormous $19.4T economy into perspective by comparing US state GDPs to entire countries- https://www.aei.org/carpe-diem/putting-americas-enormous-19-4t-economy-into-perspective-by-comparing-us-state-gdps-to-entire-countries/
[7] https://csrc.nist.gov/glossary/term/denial_of_service
[8] https://csrc.nist.gov/glossary/term/phishing
[9] https://csrc.nist.gov/glossary/term/whaling
[10] https://csrc.nist.gov/glossary/term/watering_hole_attack
[11] https://csrc.nist.gov/glossary/term/vulnerability
[12] https://csrc.nist.gov/glossary/term/Legacy_Environment
[13] https://csrc.nist.gov/glossary/term/advanced_persistent_threat
[14] https://csrc.nist.gov/glossary/term/malware

was completely unqualified and had almost no resources but managed to successfully respond to the incident and resolve it quickly. From that day on, this history magjor was now "the security guy."

My story has a happy ending, but it provides a lens through which we can examine the larger problem we face today. The organization that I worked for at that time lacked sufficient security staff to be able to assign a qualified responder to manage the case. While this proved to be a valuable opportunity , it highlights the deficit in the cybersecurity workforce going back nearly two decades.

When we look at the data, we begin to put some color to the picture. We find this shortfall has been recognized and discussed for more than a decade, but little progress has been made. We have already heard that the predicted global shortfall of cyber professionals is in the many millions of people globally. Closer to home, the (ISC)[2] 2019 Cybersecurity Workforce Study[15] estimates the cybersecurity workforce gap in the United States is already nearly 500,000 workers. This includes both the public and private sectors. Further, the cybersecurity workforce needs to grow at a rate of 62% to keep up with current demand. The job outlook for cybersecurity professionals shows the overall growth in demand for professionals is 32%.[16] This means that, if left unchecked, the cybersecurity deficit will double every two and a half years. By 2023, we could be looking at as many as a million unfilled cyber vacancies in the US alone.

In June of 2012, the U.S. Department of Homeland Security (DHS) announced it was forming the Task Force on CyberSkills, a two part initiative. First the task force sought to identify the best ways DHS can foster growth and development of the national security workforce; and, second, it sought to outline how DHS can improve recruitment and retention of cybersecurity talent within DHS itself. At the same time, the National Institute for Standards and Technology (NIST) developed the National Initiative for Cybersecurity Education (NICE) and an associated framework for building educational curricula that would raise cybersecurity awareness nationally and help train new cybersecurity professionals.[17] Both programs recognize the need for developing the national cybersecurity workforce and provide valuable resources for educators and employers. Unfortunately, neither has proven to be a silver bullet for bridging the gap.

Almost two million students a year graduate with a bachelor's degree, across all fields, nationwide. Studies indicate that only three percent of those students (about 65,000) come out of college with cyber-relevant skills, and only a fraction of them will choose to "answer the call."[18] There are many fields competing for these students.

Rapid growth is placing high demands on the available pool of both experienced and entry-level cybersecurity professionals. This high demand and low supply have led to a highly competitive market, with increasing compensations for even entry-level positions. Candidates with only an associate degree

---

[15] (ISC)2 CYBERSECURITY WORKFORCE STUDY, 2019 - https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482

[16] U.S. Bureau of Labor Statistics, Occupational Outlook Handbook: https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-1

[17] NICE and Our Community, What is NICE: https://www.nist.gov/itl/applied-cybersecurity/nice/about/frequently-asked-questions

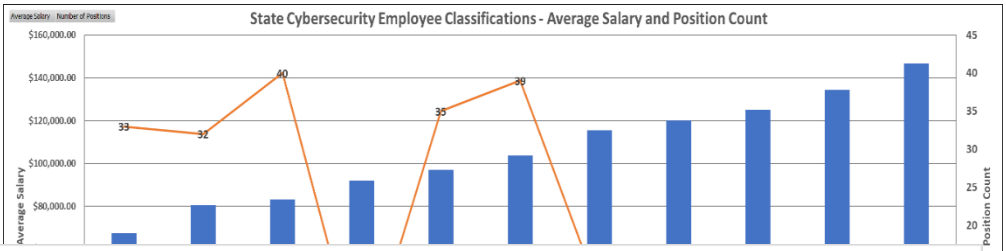
[18] https://cybersecurityventures.com/only-3-percent-of-u-s-bachelors-degree-grads-have-cybersecurity-related-skills/#:~:text=Of%20those%20graduates%2C%2064%2C405%20students,all%20will%20answer%20the%20call.

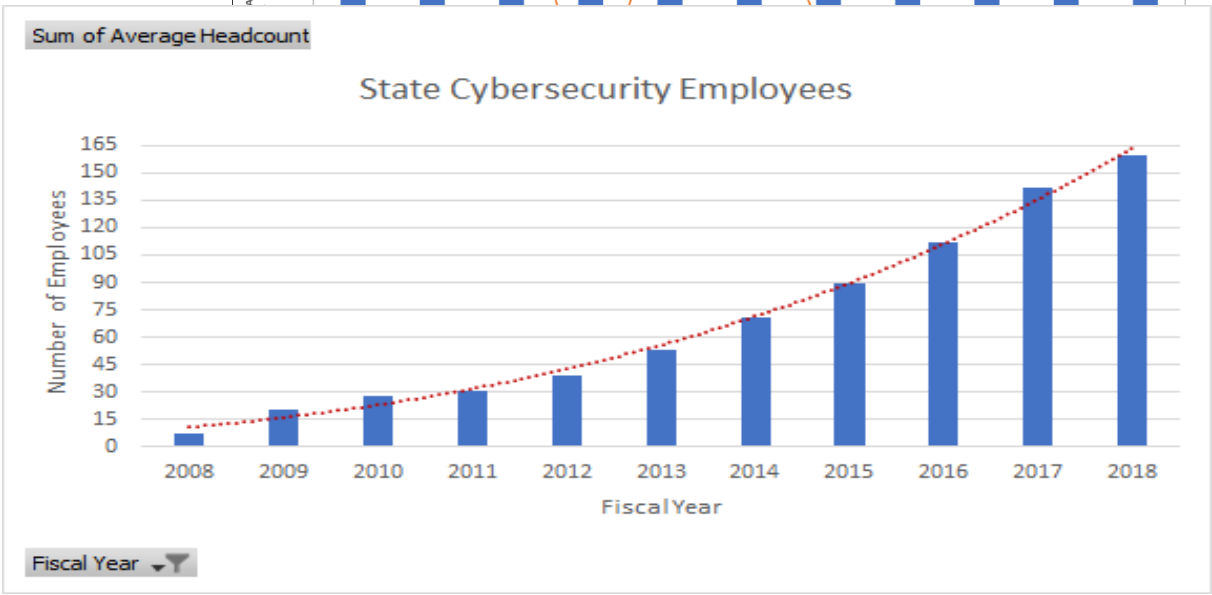
are commanding salaries of more than $95,000 per year.[19] This salary naturally increases with experience and credentials, and some senior technical cybersecurity positions are bringing in high six-figure salaries.[20]

According to the Texas Comptroller's office, there were at least 9,029 cybersecurity professionals employed in Texas as of 2018. During the past five years, the state added 1,338 jobs in this occupation, and is expected to add 3,757 more during the next ten years. All told, that is a growth rate of 41.6 percent.[21] This rate significantly outpaces the previously referenced national growth rate of 32% per year. This creates additional pressure on the labor pool and will likely make hiring for these professionals an increasingly expensive proposition. As demand drives salaries up in the private sector, it is likely the state will struggle even more to meet its own recruiting and retention needs.

Though currently under review by the State Auditor's office, there are six general state job classifications specific to cybersecurity and information security. They are the Information Technology Security Analyst (I-III) position series and the Cybersecurity Analyst (I-III) series. There are also a few additional positions used by a small number of agencies to fill security leadership positions (Cybersecurity Officer, Chief Cybersecurity Officer, Information Security Officer, and Chief Information Security Officer).

Pay scales for the general positions range from B23 to B29, with salary midpoints of $72,789 through





[19] Strategies to Incentivize Institutions of Higher Education to Develop Degree Programs in Cybersecurity, Executive Summary: http://reportcenter.highered.texas.gov/meeting/committee-supporting-documents/v-i-strategies-to-incentivize-ihes-to-develop-degree-programs-in-cybersecurity-a-report-to-the-texas-legislature-07-22-20/

[20] https://www.salary.com/research/salary/listing/senior-cloud-security-architect-salary

[21] https://comptroller.texas.gov/economy/economic-data/cybersecurity/texas.php

$123,000. The total range of salaries for those positions is $55,184 to $156,256[22]. While the upper end of this salary range would seem sufficient, only about 50 of the more than 160 cybersecurity FTEs are categorized in such higher paying cybersecurity analyst and leadership roles.[23] It is also worth noting that this does not account for the many FTEs across the state who perform cybersecurity functions for their agencies on an "other duties as assigned" basis. I am classified as a Director IV and would not show up on this report. Though the classification is appropriate to my general duties, it does demonstrate where we are likely to find holes in our data.

Our available data does readily show that the hiring needs of the state are directly tracking the needs and growth rates of Texas as a whole. The growth rate illustrated in the above graph comes out to a little more than 42%, while the Comptroller's figures for the state as a whole were 41.6%. Unfortunately, while salaries are increasing in the private sector, we in state government do not have the same flexibility with regard to starting salaries, career laddering, and salary growth. The result is that the state finds itself at a disadvantage not only in recruitment, but in retention as well. The Bureau of Labor and Statistics tells us that a junior security analyst with less than 5 years of experience can expect an average salary of $112,300[24], which is already above the midpoint for the most senior Information Technology Security Analyst (III) position working for the state. The net impact, should the status quo remain, is that state agencies will continue to struggle and potentially be unable to hire qualified security professionals. Even if agencies hire less experienced personnel and train them, they run the risk of losing them through attrition to the higher paying private sector, as they gain experience and credentials.I do not have all the answers; however, I know Texas has excellent people working to solve this problem. DIR recently worked with the Texas Higher Education Coordinating Board in support of their report to the legislature on developing curricula to build the cyber workforce. Texas has universities around the state building out security degree programs, providing vocational programs, and gaining national recognition for their cybersecurity programs. We also have several universities recognized as National Security Agency (NSA) certified Centers of Academic Excellence (CAE), giving them access to additional federal resources and grant funding to further develop their cyber research and education programs. For example, the University of Texas at San Antonio is established as the national standards body for Information Sharing and Analysis Organizations (ISAOs), and the Texas A&M University System's cybersecurity apprenticeship program is producing experienced cyber professionals. Sam Houston State University has the world's first Ph.D. in Digital and Cyber Forensic Science, and the University of Texas at Dallas' Cyber Security Research and Education Institute is working with the private sector to find solutions to pressing cybersecurity issues. And that is just to name a few.

All across Texas, efforts are being made to bridge the gap, and those efforts are beginning to pay dividends. There is still a need for action and innovation to encourage professionals to "answer the call" and join the cybersecurity workforce. If this issue is left unaddressed, the risk is simple: Texas government will fall behind in capability and capacity to respond to and protect against cybersecurity threats.

---

[22] http://www.hr.sao.texas.gov/CompensationSystem/ScheduleAB?scheduleType=2020B

[23] http://www.hr.sao.texas.gov/Reports/Category/CompensationAndClassification/

[24] U.S. Bureau of Labor Statistics, Occupational Outlook Handbook: https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-1

While I have certainly sought to establish a sense of urgency, my role here is not one of advocacy. Rather, it is my goal and my intent to offer the Select Committee and its members some of the information it needs to understand a growing problem facing all levels of Texas government. There is a shortage of qualified personnel to defend our systems and the critical, personal data they contain. The people of Texas and its leaders are all in this together, because it is our data, our identities, and potentially even our safety at stake.