A REVIEW OF THE TEXAS ECONOMY FROM THE OFFICE OF **GLENN HEGAR**, TEXAS COMPTROLLER OF PUBLIC ACCOUNTS

MARCH 2019

FISCAL NOTES

ALSO INSIDE THIS ISSUE:

Texas Cybersecurity: Protecting Data Systems

By Courtney King

TEXANS LOSE BIG TO CYBERCRIME

Cybercrime — the use of computer technology or the internet to gain unauthorized access to information for exploitative or malicious purposes — is a growing threat to private companies, governments and individual consumers alike.

The internet, arguably one of our most important technologies, wasn't designed to cope with today's sheer volume of connectivity. Due to the rise of mobile and "smart" devices as well as wireless technologies, huge amounts of confidential information are regularly transmitted across inadequately defended networks with an ever-increasing number of access points available for attack. To compound matters further, many information security and data protection measures, such as firewalls and anti-virus software, are becoming ineffective against sophisticated criminal tactics.

Crime on the internet is soaring, and the reasons are simple. The theft of confidential information or intellectual property is relatively easy and can be highly lucrative; furthermore, it's largely risk-free — most cybercriminals are never caught or prosecuted. And there's a constantly growing number of targets, as new internet and mobile users log on worldwide each day.

Yet just as a body's immune system fights back against disease, economic threats breed economic countermeasures — in this case, the young but burgeoning cybersecurity industry, which already employs thousands of Texans.

THE COST OF CYBERCRIME

It only takes one ill-fated click for an individual or organization to fall prey to a devastating cyberattack. The security software company McAfee estimates that of the more than 2 billion people online worldwide, *two-thirds* have had their personal information stolen

CONTINUED ON PAGE 3

A Message from the Comptroller

We live in a world increasingly bound together with lines of computer code. In just two decades, computers and mobile devices connected by the internet have become ubiquitous and essential to governments, businesses and individuals alike. Billions of dollars' worth of economic activity hums along cables and through wireless connections each day.

Unfortunately, this new world has created a new breed of criminal, the cyberthieves and fraudsters who use technology to prey on others. This new type of crime, in turn, has spurred the creation of new countermeasures — the rapidly growing field of cybersecurity.

In this issue of *Fiscal Notes*, we take a look at this industry, one so new that federal statistics haven't even defined it yet. Our research, however, indicates that nearly 8,200 Texans worked as information security analysts in 2017 — and we expect that number to rise by nearly 40 percent in the next decade, the fastest growth rate among the nation's largest states. Demand is outpacing supply for these specialists, as our educational institutions simply can't turn them out fast enough.

We also look at state government's own efforts at cybersecurity, which received a major boost in the last legislative session with the passage of two major pieces of legislation — the Texas Cybersecurity Act and the Texas Cybercrime Act. The former greatly strengthened the state's information security requirements, with new risk assessments and new tools and planning to reduce the incidence of security breaches involving state data. The Cybercrime Act, in turn, modernizes Texas criminal law, creating new penalties for various types of cybercrime. We've talked with the author about the need for this legislation.

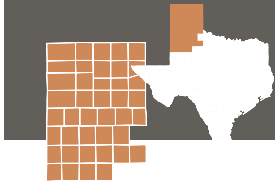
As always, I hope you enjoy this issue!

Hegar

GLENN HEGAR

Texas Comptroller of Public Accounts

REGIONAL SNAPSHOT



HIGH PLAINS REGION

POPULATION GROWTH

The High Plains Region's estimated total population in 2017 was 873,000, or more than 3 percent of the state's total population. This is an increase of about 4 percent (more than 33,000 people) since the 2010 census.

POPULATION GROWTH, HIGH PLAINS REGION VS. TEXAS AND U.S., 2010-2017

REGION 3.9%

TEXAS 12.6%

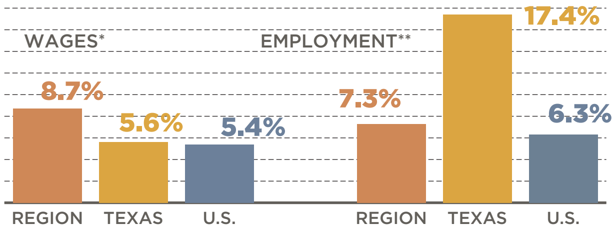
U.S. 5.5%

Source: U.S. Census Bureau

JOBS AND WAGES

In 2017, the High Plains Region accounted for more than 3 percent of the state's total employment.

GROWTH, HIGH PLAINS REGION VS. TEXAS AND U.S., 2007-2017



* Real rate of change

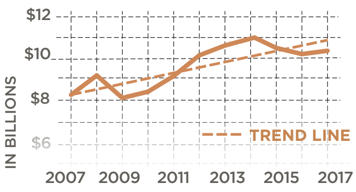
**Figures include private and public-sector employees with the exception of active-duty military personnel, railroad employees, religious institution employees and the self-employed.

Sources: JobsEQ and U.S. Bureau of Labor Statistics

ECONOMY

Sales receipts subject to state sales tax directly attributable to the High Plains Region trended upward in the past decade.

REGIONAL RECEIPTS SUBJECT TO SALES TAX 2007-2017



Source: Texas Comptroller of Public Accounts

CONCLUSION

The High Plains Region's median age is on par with that of Texas, but Lubbock County – the region's most populous – is significantly younger than the state as a whole. The region's high school graduation rate is above the state average. Individual wages in the region are below the state average, but wages are increasing at a faster pace. The High Plains economy peaked in 2014, falling off since. But sales subject to state sales tax in 2017 indicate the local economy is moving upward again. These factors, combined with agriculture's large footprint, distinguish the High Plains regional economy.

THE HIGH PLAINS REGION IS ONE OF THE COMPTROLLER'S 12 ECONOMIC REGIONS.

To see a complete list of these regions, plus more in-depth county-by-county data, visit: comptroller.texas.gov/economy/economic-data/regions/

If you would like to receive paper copies of *Fiscal Notes*, contact us at **fiscal.notes@cpa.texas.gov**

CONTINUED FROM PAGE 1

or compromised. A 2017 global study by consulting firm Accenture found an average of 130 security breaches per company each year.

Based on more than 21,000 interviews with representatives of 254 companies in seven nations, Accenture estimates that cybercrime costs each of these organizations an average of $11.7 million annually. This average includes not only the initial costs incurred from damages — which can range from loss of assets to disruption of business continuity — but the money organizations have to spend to recover from damages and protect themselves against the constant deluge of cyberthreats.

Unsurprisingly, banks are the top targets of cybercriminals. The financial services industry has the highest average cybercrime costs, at nearly $18.3 million per organization (**Exhibit 1**).

The Federal Bureau of Investigation's Internet Crime Complaint Center receives more than 800 complaints of criminal activity per day. In 2017, U.S. victims reported losses totaling $1.42 billion.

Given Texas' population, it's unsurprising that the state ranks third nationally in its number of cybercrime victims (**Exhibit 2**). Texas victims reported about $115.7 million in losses in 2017.

Cyberattacks are becoming more common and costlier. In response, organizations are investing in information security capabilities and staff on an unprecedented scale. Inevitably, cybersecurity has become one of the largest and fastest-growing technology needs.

EXHIBIT 2

TOP 10 STATES BY NUMBER OF CYBERCRIME VICTIMS AND FINANCIAL LOSSES, 2017

VICTIMS			FINANCIAL LOSSES		
RANK	STATE	VICTIMS	RANK	STATE	LOSSES
1	CALIFORNIA	41,974	1	CALIFORNIA	$214,217,307
2	FLORIDA	21,887	**2**	**TEXAS**	**115,680,902**
3	**TEXAS**	**21,852**	3	FLORIDA	110,620,330
4	NEW YORK	17,622	4	NEW YORK	88,633,788
5	PENNSYLVANIA	11,348	5	ARIZONA	59,366,635
6	VIRGINIA	9,436	6	WASHINGTON	42,991,213
7	ILLINOIS	9,381	7	ILLINOIS	42,894,106
8	OHIO	8,157	8	NEW JERSEY	40,441,739
9	COLORADO	7,909	9	COLORADO	39,935,041
10	NEW JERSEY	7,757	10	MASSACHUSETTS	38,962,867

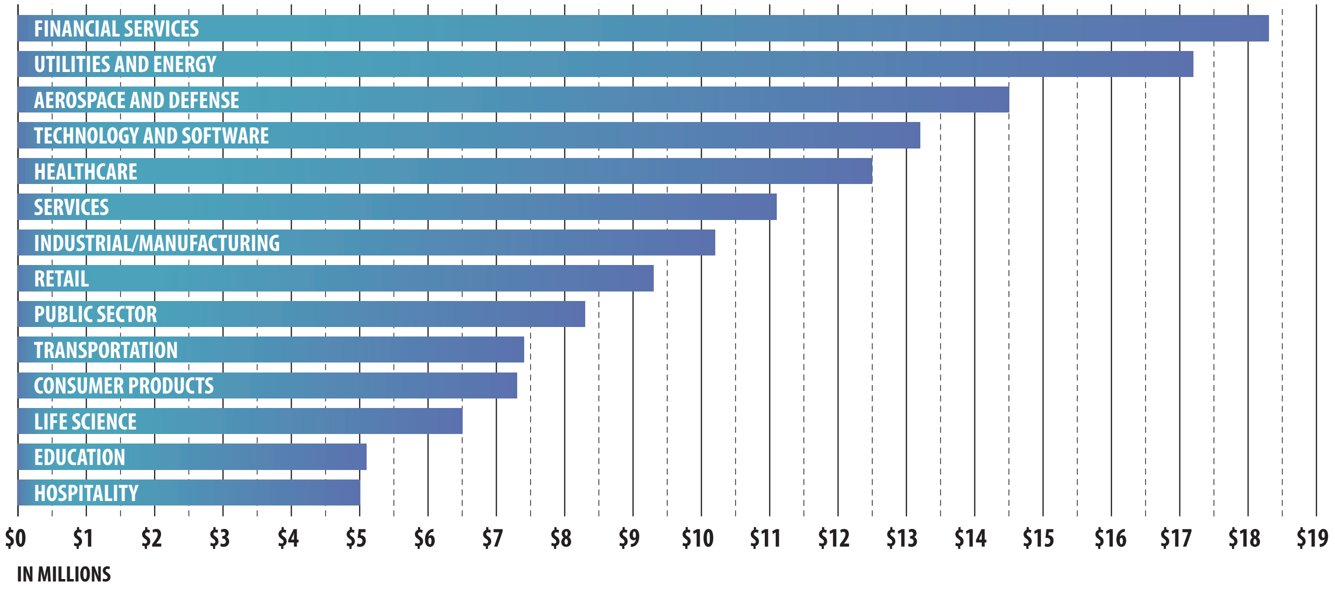
NOTE: Information based on the total number of complaints in which the complainant provided state information.
Source: Federal Bureau of Investigation

CYBERSECURITY IN TEXAS

Cybersecurity is a relatively new field — so new it hasn't yet been defined as an industry by the federal government's North American Industry Classification System, the standard federal agencies use to collect, analyze and publish statistical data related to the business economy.

EXHIBIT 1

AVERAGE ANNUALIZED COST OF CYBERCRIME BY INDUSTRY SECTOR, PER ORGANIZATION, AUGUST 2017



Source: Accenture and Ponemon Institute LLC

> **Today, the information security analyst occupation has a near-zero unemployment rate.**

Even differentiating cybersecurity *jobs* from other information technology (IT) positions can be difficult. The Department of Homeland Security recently noted inconsistencies in the way employers define and use the term, which can include a wide range of job functions requiring different qualifications and skillsets. Job descriptions and titles for the same job vary from employer to employer. Some researchers and industry practitioners contend that *every* IT job is involved in cybersecurity to some extent.

The Comptroller's office has examined employment statistics for *information security analysts*, defined by the federal Standard Occupational Classification (SOC) system as workers who "plan, implement, upgrade, or monitor security measures for the protection of computer networks and information … and respond to computer security breaches and viruses."

In 2017, 8,165 Texans worked as information security analysts in various sectors of the state economy. The largest numbers were employed in *professional, scientific and technical services* and *finance and insurance*, with 3,091 and 1,471 jobs, respectively (**Exhibit 3**). Emsi, a company that provides labor market statistics, expects robust job growth in this field in multiple sectors.

Texas' job count in this occupation is expected to grow by more than 39 percent from 2017 to 2027 — the largest projected percentage increase among the nation's five most populous states, and considerably faster growth than in the nation as a whole (**Exhibit 4**).

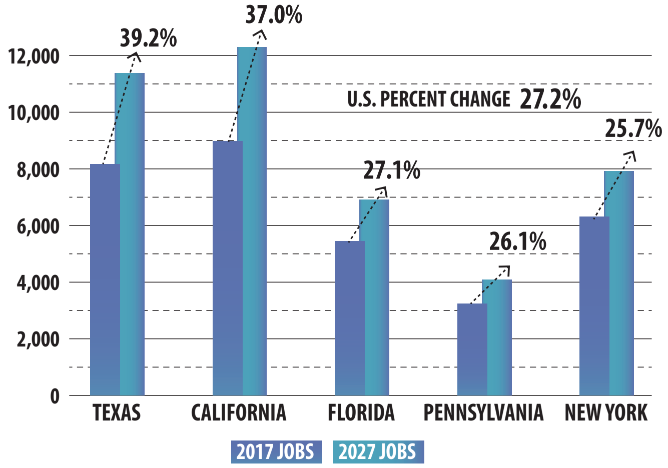
Today, the information security analyst occupation has a near-zero unemployment rate.

DEMAND OUTPACES SUPPLY

A qualified and well-trained cybersecurity workforce is essential to mitigating and responding to cyberthreats. Demand, however, is outpacing supply, resulting in a global shortage of information security workers.

EXHIBIT 4

INFORMATION SECURITY ANALYSTS: PROJECTED JOB GROWTH IN THE FIVE MOST POPULOUS STATES



Source: Emsi

EXHIBIT 3

TOP 10 INDUSTRY SECTORS* EMPLOYING INFORMATION SECURITY ANALYSTS IN TEXAS, 2017-2027

INDUSTRY SECTOR*	JOBS IN INDUSTRY, 2017	OCCUPATION SHARE BY INDUSTRY, 2017	PROJECTED JOBS IN INDUSTRY, 2027	PROJECTED JOB COUNT CHANGE, 2017 - 2027
PROFESSIONAL, SCIENTIFIC AND TECHNICAL SERVICES	3,091	37.9%	4,931	59.5%
FINANCE AND INSURANCE	1,471	18.0	2,010	36.6
GOVERNMENT	676	8.3	744	10.1
INFORMATION	659	8.1	804	22.0
ADMINISTRATIVE AND SUPPORT AND WASTE MANAGEMENT AND REMEDIATION SERVICES	528	6.5	628	18.9
MANAGEMENT OF COMPANIES AND ENTERPRISES	509	6.2	822	61.5
MANUFACTURING	341	4.2	328	-3.8
WHOLESALE TRADE	284	3.5	317	11.6
HEALTHCARE AND SOCIAL ASSISTANCE	157	1.9	210	33.8
MINING, QUARRYING AND OIL AND GAS EXTRACTION	124	1.5	193	55.6

* As defined by the federal North American Industry Classification System.
Source: Emsi

SAN ANTONIO — A NATIONAL LEADER

San Antonio, a nationally recognized hub for cybersecurity, hosts several colleges and universities recognized as National Centers of Academic Excellence in Cyber Defense Education — most notably the University of Texas at San Antonio (UTSA). UTSA is home to three cybersecurity centers and research institutes and has the nation's top-ranked cybersecurity education program. Program graduates earn average starting salaries of $60,000 to $80,000 annually.

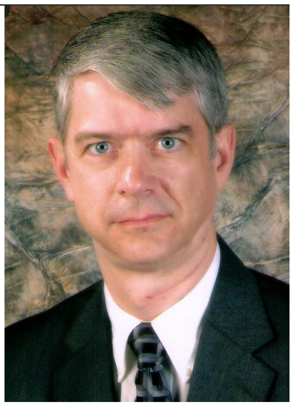
Superior training and education, combined with close proximity to cybersecurity offices and installations of the National Security Agency, the Federal Bureau of Investigation, the Department of Homeland Security and the U.S. Air Force, have helped the San Antonio area amass the highest concentration of cybersecurity professionals outside of Washington, D.C.

The research company Cybersecurity Ventures estimates there are more than 1 million vacant cybersecurity positions worldwide. If current trends continue, the number of unfilled cybersecurity jobs will reach 3.5 million by 2021.

Emsi tracked more than 96,000 job postings for information security analysts in Texas from September 2016 to December 2017 alone.

Employers have cited a number of difficulties filling open positions, including a low number of prospects and training shortages. While academic institutions around the nation are developing talented professionals, their programs often are still small and evolving.

According to Dr. Gregory White, professor of computer science and director of the University of Texas at San Antonio's (UTSA's) Center for Infrastructure Assurance and Security, the cybersecurity field faces a bottleneck; the nation simply can't train enough people to fill all open positions and keep up with growing demand. "We could double the number of people in school now and still not fill all open positions," White says.



DR. GREGORY WHITE

DIRECTOR,
UTSA CENTER FOR
INFRASTRUCTURE
ASSURANCE AND SECURITY

WORKING AROUND THE LABOR SHORTAGE

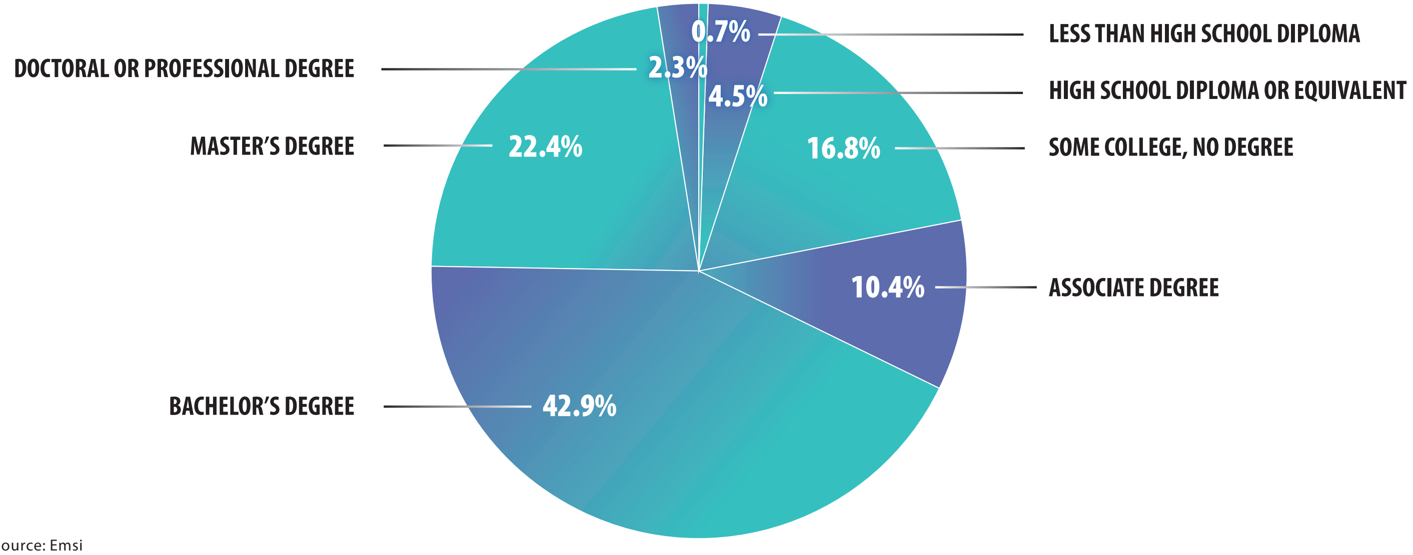
"Organizations need to truly ask themselves if their positions require a [four-year IT] degree," White says. "I would guess that a number of vacant positions can be filled by people without a degree."

In fact, many cybersecurity professionals learned the necessary skills through certificate programs and on-the-job training rather than a degree program. "There are students in the San Antonio area that are obtaining two or three certifications in high school and getting job offers after graduation," White says.

In 2017, nearly a third of information security analysts employed in Texas held less than a four-year degree (**Exhibit 5**).

EXHIBIT 5

EDUCATIONAL LEVELS OF INFORMATION SECURITY ANALYSTS, 2017



Source: Emsi

As with other technology fields, there's a gender gap in cybersecurity.

According to the 2017 Global Information Security Workforce Study, many workers enter information security from related fields, most commonly computer science or engineering. Others enter from non-technical careers including the military and defense-related work.

As with other technology fields, there's a gender gap in cybersecurity. In 2017, only about a fifth of Texas' information security analysts were women (**Exhibit 6**). Attracting and retaining a more diverse pool of labor could help improve the labor shortage.

SHARED RESPONSIBILITIES

Technical measures alone aren't enough to counter cyberthreats effectively. Cybersecurity requires *all* employees to be aware and vigilant.

"In addition to focusing on building the cybersecurity workforce, we also need to work on cybersecurity *in* the workforce," says White. Many data breaches have occurred because technology users failed to take the most basic protective measures.

"If we can instill a culture of security in our workforce, it would go a long way to help the minimal number of cybersecurity professionals we have go further," White says. "It's not just the professionals' job to protect the systems. Anyone who touches a keyboard has a responsibility at some level."

White is also director of the Information Sharing and Analysis Organization Standards Organization (ISAO SO), which works to identify standards, guidelines and best practices for information sharing and analysis related to cybersecurity risks and incidents.

White notes that it was once common for financial institutions not to share cybersecurity information, particularly concerning data breaches, for fear of legal consequences or of losing a competitive advantage. Banks now understand, however, that on this topic, quick, efficient and regular information-sharing is critical. Organizations in other sectors are beginning to do the same thing.

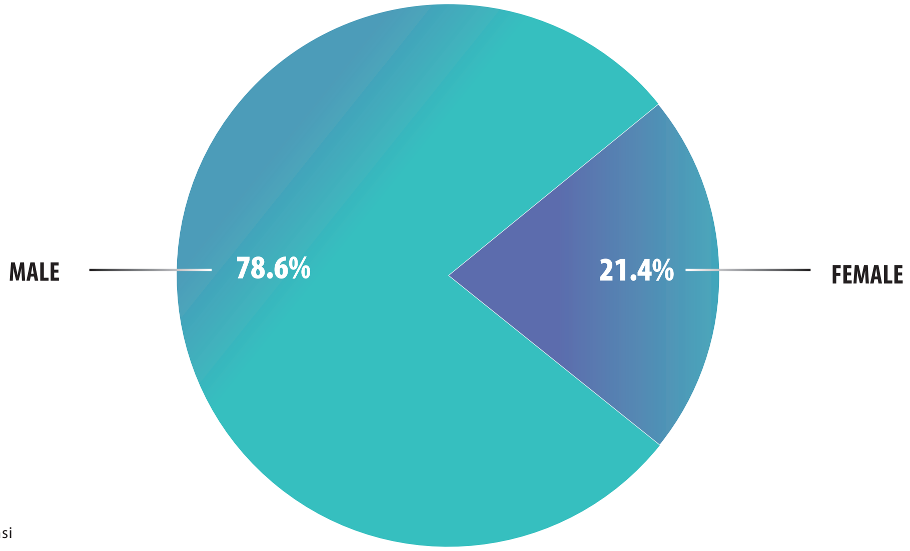
"From a security standpoint, it isn't one bank versus another bank — it should be both banks versus the attackers," White says. "Institutions should be teammates in cybersecurity and not competitors."

Currently, White and the ISAO SO are working to increase cyberthreat information sharing everywhere, in hopes of elevating information security not only in Texas but in the nation as well. **FN**

For more on cybersecurity efforts in Texas, see our online Line Items *feature at FiscalNotes.org.*

EXHIBIT 6

GENDER BREAKDOWN OF INFORMATION SECURITY ANALYSTS IN TEXAS, 2017



Source: Emsi

Cyberdefense for Texas State Government

By Jackie Benton

PUBLIC DATA SYSTEMS, INFRASTRUCTURE UNDER ATTACK

While the 2017 regular legislative session wrestled with many contentious issues, from sanctuary cities to plastic bag bans, members from both sides of the aisle united to pass cybersecurity legislation for Texas state agencies and institutions of higher education.

The need for tougher cybersecurity measures for state systems was obvious, says Texas Rep. Giovanni Capriglione, noting the state's reliance on legacy hardware and software systems dating back to the 1980s.

"As the use of technology increases in our daily lives, it's more important than ever that private citizen data held by the state is protected," Capriglione says.

Governmental agencies, increasingly reliant on aging computer systems and the internet, are prime targets for cybercrime; a 2018 national survey of state chief information officers noted dozens of security breaches in the preceding 12 months (**Exhibit 1**). And more than the agencies themselves are at risk. Government systems store confidential personal and business data including Social Security numbers, federal tax IDs, employer identification numbers and more — all cybercriminals need to commit identity theft and credit fraud.

EXHIBIT 1

RECENT SECURITY BREACHES REPORTED BY STATE CHIEF INFORMATION OFFICERS, 2018

WEB APPLICATIONS	30
MALICIOUS CODE (E.G., VIRUSES/WORMS/ SPYWARE/MALWARE/RANSOMWARE)	28
ELECTRONIC ATTACK (HACKING)	16
PHYSICAL ATTACK (E.G., STOLEN COMPUTER SYSTEMS)	14

Source: 2018 Deloitte-NASCIO Cybersecurity Study

2017 CYBERSECURITY LEGISLATION

After becoming aware of the need to upgrade Texas' cybersecurity systems, Capriglione filed House Bill (HB) 8 and HB 9 in the 2017 regular legislative session and saw both become law.

HB 8, the Texas Cybersecurity Act, provides specific measures to protect sensitive and confidential data and maintain cyberattack readiness. HB 9, the Texas Cybercrime Act, updates the Texas Penal Code to recognize several new types of cybercrime and their

REP. GIOVANNI CAPRIGLIONE

TEXAS HOUSE OF REPRESENTATIVES

punishments. Both acts took effect on Sept. 1, 2017. Together, they're intended to deliver a one-two punch against cybercrime.

"HB 8 and HB 9 were both born through discussions with technology industry experts from my district and stakeholders in Austin," Capriglione says. "We ended up having input from more than 50 different individuals, trade organizations, private companies, cities, counties, universities and law enforcement."

According to Capriglione's office, the 2017 Legislature also budgeted $30.6 million for system upgrades at state agencies to protect against the loss of sensitive data due to cyberattacks (**Exhibit 2**). While he's pleased with this support, he notes Texas government still has much work to do to keep up with cyber threats.

The Department of Information Resources' (DIR's) Network Security Operations Center "blocked 2.46 billion communication attempts from known bad actors against state agencies in just a matter of a few months," he says. "It's no secret that technology in government doesn't progress as quickly as the business world around us, but for the state to still be operating systems on 'green screens' and computer systems that truly don't exist anymore today is mindboggling."

The Texas Cybersecurity Act provided Texas state agencies and institutions with a wide array of new tools.

TOUGHER CYBERSECURITY REQUIREMENTS

The Texas Cybersecurity Act provided Texas state agencies and higher education institutions with a wide array of new tools to help them ready themselves for cyberattack. DIR plays a pivotal role in implementing the act.

To meet its requirements, the agency was required to provide guidelines for cybersecurity training and continuing education for all state employees who deal with information resources. A guidebook,

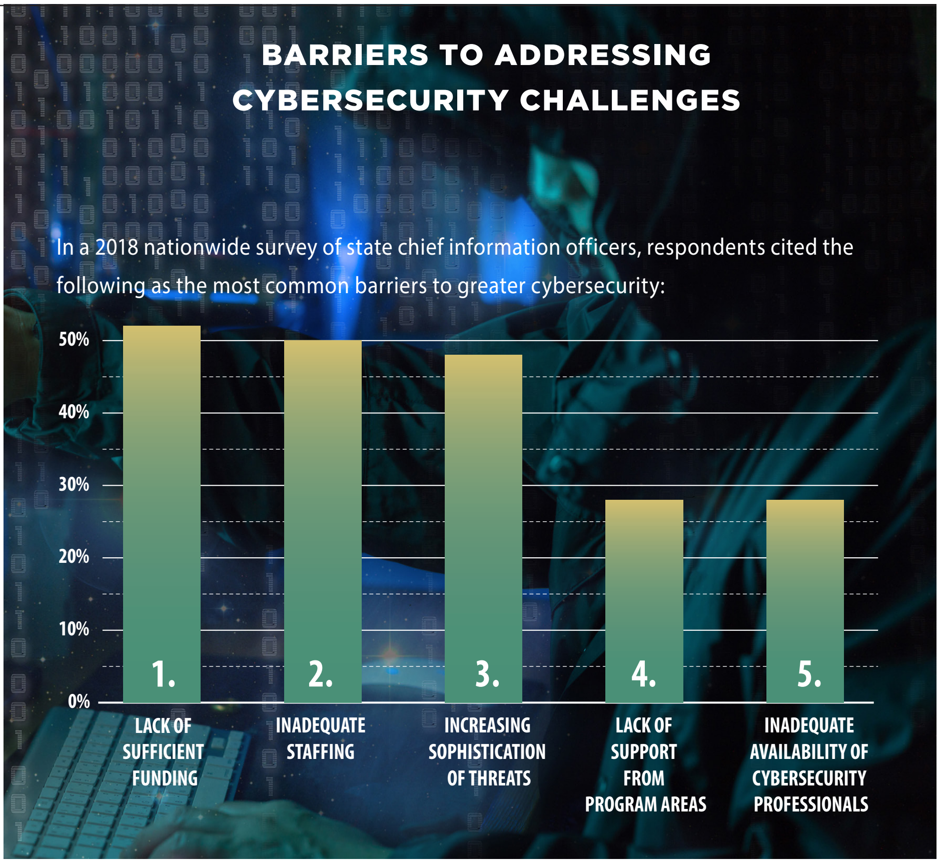
EXHIBIT 2

CYBERSECURITY APPROPRIATIONS IN THE 2018-2019 TEXAS STATE BUDGET

AGENCY	AMOUNT	PURPOSE
TEXAS ETHICS COMMISSION	$45,780	Disclosure Database System
TEXAS FACILITIES COMMISSION	187,900	Information Security Officer
TEXAS EDUCATION AGENCY	5,968,000	Implementation of the Texas Student Data System (TSDS) and Ensuring Student and Teacher Data Privacy
HIGHER EDUCATION COORDINATING BOARD	215,000	Security Upgrades to the Agency's Identity and Access Management Services
	225,000	Cybersecurity Improvements
JUVENILE JUSTICE DEPARTMENT	6,821,007	Infrastructure Refresh
	715,606	Cybersecurity Improvements
DEPARTMENT OF PUBLIC SAFETY	2,240,000	Data Loss Prevention System
	2,200,000	Intrusion Prevention System
	1,216,000	Security System Vulnerability Management System
GENERAL LAND OFFICE	40,000	Data Loss Prevention System
	40,000	Vulnerability Management
DEPARTMENT OF MOTOR VEHICLES	400,000	Management Systems Security Provider
TXDOT	10,000,000	Cybersecurity Initiatives
STATE BOARD OF DENTAL EXAMINERS	50,000	Information Technology
STATE BOARD OF PHARMACY	200,000	Acquisition of Information Technology
TOTAL	**$30,564,293**	

Source: Office of Texas Rep. Giovanni Capriglione

Information Resources Employees Continuing Education Guidelines for Cybersecurity, was made available to state agencies in July 2018.



BARRIERS TO ADDRESSING CYBERSECURITY CHALLENGES

In a 2018 nationwide survey of state chief information officers, respondents cited the following as the most common barriers to greater cybersecurity:

Source: 2018 Deloitte-NASCIO Cybersecurity Study

DIR also has established requirements for a biennial information security assessment and report to be completed by all state agencies. DIR compiled the results of the first round of these assessments into a report submitted to the Legislature on Jan. 11, 2019.

In addition, state agencies and institutions of higher education now must perform vulnerability and penetration testing of their websites and any mobile applications that process confidential information.

Before the Texas Cybersecurity Act, state agencies were required only to generally identify data security issues and create a broad plan to reduce risk. Now, agencies must develop and implement specific procedures, analyses and strategies into these plans. The act also requires state agencies that experience a breach or suspected breach of confidential information to notify DIR officials and, if election data have been compromised, the Texas Secretary of State, within 48 hours.

Yet another new provision requires an agency's cybersecurity assessments and related data to be considered in the Sunset Review process. The Texas Sunset Advisory Commission works with DIR to determine the criteria and information to be collected and ascertain whether the agency under review is complying with best cybersecurity practices.

Under the act, DIR also developed a plan addressing state cybersecurity risks and incidents that was implemented during fiscal 2018. The plan included cybersecurity certification testing for state security personnel through the agency's InfoSec Academy, which provides industry-standard certification courses; online end-user training to state agencies; monthly exercises for agency security staff; and updates to the statewide cybersecurity portion of the state's emergency plan.

State agencies that experience a breach or suspected breach of confidential information must notify DIR officials within 48 hours.

Finally, DIR has completed a comprehensive managed security services (MSS) contract with AT&T, giving state agencies, local governments and other public entities cost-effective access to security monitoring, device management, network and web application firewalls and intrusion detection and prevention. To access these services, agencies go to the DIR portal, identify their needs and place an order. DIR also vets and monitors vendor performance and ensures contract compliance.

BEYOND DIR

To keep state security strategies confidential, the Texas Cybersecurity Act made some key changes to the Texas Open Meetings Act and Public Information Act. Governmental bodies are no longer required to hold open meetings to deliberate information security assessments or deployments, network security information or the deployment of security personnel, critical infrastructure or security devices. Also, prior to posting information regarding contracts for the purchase of goods and services on the internet, state

The Texas Cybersecurity Act and the Texas Cybercrime Act work together to give Texas government and law enforcement a much-needed boost in providing cybersecurity.

agencies now must redact information related to computer network security deemed confidential under HB 8.

The act also created select committees on cybersecurity in both the Texas House and Senate. These committees were directed to either jointly or separately study state agency cybersecurity plans and cybersecurity issues and report their findings and jointly adopted recommendations to the Legislature by Jan. 13, 2019. Both House and Senate reports have been submitted and are currently under review.

The Texas Secretary of State was tasked with conducting a study on election cyberattacks to preserve election integrity, including the investigation of vulnerabilities such as attempted cyberattacks on voting machines and registered voter lists. The study assessed the security procedures of several counties in central Texas that use a variety of voting systems. It concluded "the statewide electronic voter registration database is as secure as currently possible," but recommended additional funding be allocated to support it in providing additional on-site assistance and advice to county election officials regarding security measures.

The Cybersecurity Act also affected the responsibilities of the Texas Cybersecurity Council, a group of private- and public-sector leaders who collaborate to develop strategies to protect critical infrastructure and sensitive information. Thanks to the act, the council's duties now include a cost-benefit analysis of potential ways in which to mitigate and respond to cyberthreats. The first of these reports has been submitted to the council leadership, and a committee chaired by Capriglione is preparing legislative recommendations.

THE TEXAS CYBERCRIME ACT

The other half of the 2017 cybersecurity package, the Texas Cybercrime Act, provides Texas law enforcement agencies with more robust tools for fighting cybercrimes. The act was a first step toward modernizing the Texas legal system to keep up with today's high-tech criminal, says Capriglione.

The act amends the Texas Penal Code to include the third-degree felony offense of "electronic access interference," in which a person intentionally interrupts or suspends access to a computer system or network without the owner's consent. It also adds the offense of "electronic data tampering," the intentional alteration of computer data and the introduction of malicious code such as ransomware, and "unlawful decryption," covering the intentional decryption of encrypted private information. Penalties for both offenses (including enhancements) range from a Class C misdemeanor to a first-degree felony, depending on the aggregate dollar amount involved and whether a client or patient of a victim suffered bodily injury or death attributable to the offense.

Legitimate law enforcement and business activities, such as "white hat" internal network testing operations, are not targeted by the Texas Cybercrime Act. Capriglione says the new law is designed to encourage more law enforcement agencies, particularly at the state level, to pursue cybercrime investigations.

MORE HELP ON THE WAY?

The Texas Cybersecurity Act and the Texas Cybercrime Act work together to give Texas government and law enforcement a much-needed boost in providing cybersecurity. As an example of how much more needs to be accomplished, Capriglione points to a malicious hacking incident of a Texas county emergency system that had serious repercussions.

"Tarrant County's 911 system was hacked in October 2016, when an 18-year-old college student posted a Twitter link that, when clicked on, caused users to dial into the 911 network," Capriglione says. "The Tarrant County 911 District estimates it had at least 850 hang-up calls during the attack, severely crippling response times for those who were having an actual emergency.

"While we've been focused on our state cybersecurity, I have been working with cities and counties to provide assistance to our local government entities and provide resources for making sure data is protected at all levels of government, like requiring local government entities to participate in regional Information Sharing and Analysis Centers to communicate with other local entities about similar cyber threats they are facing," he says.

More legislation to further improve cybersecurity is being considered in the 2019 session. **FN**

Look for our Fiscal Notes Legislative Wrap-Up Issue *later this year to stay up to date about new laws that will affect state government and the Texas economy.*

State Revenue Watch

This table presents data on net state revenue collections by source. It includes most recent monthly collections, year-to-date (YTD) totals for the current fiscal year and a comparison of current YTD totals with those in the equivalent period of the previous fiscal year.

These numbers were current at press time. For the most current data as well as downloadable files, visit **comptroller.texas.gov/transparency.**

Note: Texas' fiscal year begins on Sept. 1 and ends on Aug. 31.

NET STATE REVENUE — All Funds Excluding Trust

(AMOUNTS IN THOUSANDS)

Monthly and Year-to-Date Collections: Percent Change From Previous Year

Tax Collections by Major Tax	FEBRUARY 2019	YEAR TO DATE: TOTAL	YEAR TO DATE: CHANGE FROM PREVIOUS YEAR
SALES TAX	$2,795,612	$16,843,656	7.77%
PERCENT CHANGE FROM FEBRUARY 2018	7.02%		
MOTOR VEHICLE SALES AND RENTAL TAXES	420,255	2,486,793	-1.11%
PERCENT CHANGE FROM FEBRUARY 2018	-0.36%		
MOTOR FUEL TAXES	299,318	1,853,134	1.93%
PERCENT CHANGE FROM FEBRUARY 2018	0.86%		
FRANCHISE TAX	20,621	-185,287	-40.03%
PERCENT CHANGE FROM FEBRUARY 2018	252.10%		
OIL PRODUCTION TAX	268,549	1,867,529	26.67%
PERCENT CHANGE FROM FEBRUARY 2018	-12.56%		
INSURANCE TAXES	837,695	944,600	1.67%
PERCENT CHANGE FROM FEBRUARY 2018	3.48%		
CIGARETTE AND TOBACCO TAXES	104,293	655,302	9.22%
PERCENT CHANGE FROM FEBRUARY 2018	3.27%		
NATURAL GAS PRODUCTION TAX	163,751	927,398	31.27%
PERCENT CHANGE FROM FEBRUARY 2018	22.21%		
ALCOHOLIC BEVERAGES TAXES	103,696	665,325	7.60%
PERCENT CHANGE FROM FEBRUARY 2018	8.06%		
HOTEL OCCUPANCY TAX	47,307	289,147	6.02%
PERCENT CHANGE FROM FEBRUARY 2018	5.92%		
UTILITY TAXES[1]	10,602	221,734	10.54%
PERCENT CHANGE FROM FEBRUARY 2018	21.60%		
OTHER TAXES[2]	18,730	136,827	15.59%
PERCENT CHANGE FROM FEBRUARY 2018	8.48%		
TOTAL TAX COLLECTIONS	**$5,090,430**	**$26,706,158**	**8.68%**
PERCENT CHANGE FROM FEBRUARY 2018	**4.85%**		

Revenue By Source	FEBRUARY 2019	YEAR TO DATE: TOTAL	YEAR TO DATE: CHANGE FROM PREVIOUS YEAR
TOTAL TAX COLLECTIONS	$5,090,430	$26,706,158	8.68%
PERCENT CHANGE FROM FEBRUARY 2018	4.85%		
FEDERAL INCOME	3,916,559	21,379,419	1.59%
PERCENT CHANGE FROM FEBRUARY 2018	7.46%		
LICENSES, FEES, FINES AND PENALTIES	522,979	3,448,427	2.75%
PERCENT CHANGE FROM FEBRUARY 2018	0.26%		
STATE HEALTH SERVICE FEES AND REBATES[3]	543,639	3,884,280	-13.88%
PERCENT CHANGE FROM FEBRUARY 2018	-28.44%		
NET LOTTERY PROCEEDS[4]	189,208	1,304,015	20.54%
PERCENT CHANGE FROM FEBRUARY 2018	7.43%		
LAND INCOME	161,727	1,212,690	29.30%
PERCENT CHANGE FROM FEBRUARY 2018	8.93%		
INTEREST AND INVESTMENT INCOME	86,786	1,063,762	51.48%
PERCENT CHANGE FROM FEBRUARY 2018	-16.83%		
SETTLEMENTS OF CLAIMS	5,958	485,868	0.54%
PERCENT CHANGE FROM FEBRUARY 2018	29.91%		
ESCHEATED ESTATES	4,241	109,269	36.87%
PERCENT CHANGE FROM FEBRUARY 2018	36.51%		
SALES OF GOODS AND SERVICES	22,602	131,749	-5.18%
PERCENT CHANGE FROM FEBRUARY 2018	8.55%		
OTHER REVENUE	462,322	914,442	-0.59%
PERCENT CHANGE FROM FEBRUARY 2018	21.64%		
TOTAL NET REVENUE	**$11,006,449**	**$60,640,078**	**4.86%**
PERCENT CHANGE FROM FEBRUARY 2018	**3.65%**		

[1] Includes public utility gross receipts assessment, gas, electric and water utility tax and gas utility pipeline tax.

[2] Includes taxes not separately listed, such as taxes on oil well services, coin-operated amusement machines, cement and combative sports admissions as well as refunds to employers of certain welfare recipients.

[3] Includes various health-related service fees and rebates that were previously in "license, fees, fines and penalties" or in other non-tax revenue categories.

[4] Gross sales less retailer commission and the smaller prizes paid by retailers.

Notes: Totals may not add due to rounding.

Excludes local funds and deposits by certain semi-independent agencies.

Includes certain state revenues that are deposited in the State Treasury but not appropriated.

FISCAL NOTES

Texas Comptroller of Public Accounts
Communications and Information Services Division
111 E. 17th St., Suite 301, Austin, TX 78774-0100

GLENN HEGAR

Texas Comptroller of Public Accounts

Fiscal Notes is one of the ways the Comptroller's office strives to assist taxpayers and the people of Texas. The newsletter is a by-product of the Comptroller's constitutional responsibilities to monitor the state's economy and to estimate state government revenues.

Fiscal Notes also provides a periodic summary of the financial statements for the state of Texas.

Articles and analysis appearing in *Fiscal Notes* do not necessarily represent the policy or endorsement of the Texas Comptroller of Public Accounts. Space is devoted to a wide variety of topics of Texas interest and general government concern.

Fiscal Notes is not copyrighted and may be reproduced. The Texas Comptroller of Public Accounts would appreciate credit for material used and a copy of the reprint.

FIELD OFFICES

Find a list of all Comptroller field offices at comptroller.texas.gov/about/contact/locations.php.

ONLINE SUBSCRIPTIONS, RENEWALS OR CANCELLATIONS

of *Fiscal Notes* may be entered at
comptroller.texas.gov/economy/fiscal-notes
Send questions or comments to fiscal.notes@cpa.texas.gov

HOW TO REACH US

Contact the Communications and Information Services Division at
800-252-5555 (VOICE),
512-463-4226 (FAX).

OR WRITE *Fiscal Notes,* Texas Comptroller of Public Accounts
Communications and Information Services Division
111 E. 17th St., Suite 301, Austin, TX 78774-0100

In compliance with the Americans with Disabilities Act, this document is available in a reader-friendly format at comptroller.texas.gov/economy/fiscal-notes.

Texas Comptroller of Public Accounts
Publication #96-369,

MARCH 2019