Cybersecurity and IT Modernization

by Jorge Barro

center for
PUBLIC FINANCE
Rice University's Baker Institute for Public Policy

Commissioned by **Texas 2036**

center for
PUBLIC FINANCE
Rice University's Baker Institute for Public Policy

The Center for Public Finance (CPF) at Rice University's Baker Institute focuses on the economic effects of major U.S. fiscal policies. Given the complexity of the U.S. tax system and the unsustainable nature of current U.S. tax and spending policies, the center examines the potential effects of various fiscal reforms on economic growth and the distribution of income in an effort to inform policymakers, stakeholders and the general public. In addition, CPF examines the challenges facing the country if policymakers continue to delay implementing solutions to these critical issues. CPF scholars actively participate in the policymaking process by advising various national government agencies, state and international governments, and multilateral development institutions, as well as various key individual policymakers. CPF scholars routinely present their work at CPF sponsored events, other public and private events, and in testimony before federal and state government committees.

bakerinstitute.org

TEXAS 2036

Texas 2036 is a non-profit organization building long-term, data-driven strategies to secure Texas' continued prosperity for years to come. We engage Texans and their leaders in an honest conversation about our future, focusing on the big challenges. We offer non-partisan ideas and modern solutions that are grounded in research and data to break through the gridlock on issues that matter most to all Texans. Smart strategies and systematic changes are critical to prepare Texas for the future.

texas2036.org

Jorge Barro, Ph.D., is a fellow in public finance at Rice University's Baker Institute of Public Policy. His research involves the development of dynamic macroeconomic models to evaluate the impact of state and federal fiscal policy. Before joining the Baker Institute, Barro was an economist at the Wharton School at the University of Pennsylvania, where he developed a large-scale macroeconomic model of the United States and helped launch the nonpartisan Penn Wharton Budget Model. Barro received his Ph.D. in economics from the University of Texas at Austin.

With sizable state and federal appropriations for technology upgrades in consideration, this report studies several challenges and opportunities for Texas state government officials, including optimal cybersecurity financing, identifying unique risks, allocating limited resources among competing priorities, and coordinating efforts with internal and external stakeholders. By understanding the value of cybersecurity and information technology (IT) investments, government officials are provided a broad perspective to evaluate certain tradeoffs, improve allocations, and consider other actions to better serve their constituents.

Cybersecurity

Over the past several decades, an increasing dependence on information systems has introduced an ever-growing threat of cyber-attacks. Mitigating this risk involves several measures, including identifying vulnerabilities, maintaining updated hardware and software, hiring expert personnel, and providing proper cybersecurity training to all employees. Even when these measures are clear, the limited resources of the state government must be allocated in the most efficient way, requiring prioritization of alternative measures.

The aftermath of the COVID-19 pandemic highlighted information system deficiencies and expedited the need for technological improvements in response to heightened demand for government services, remote work capabilities, and a global surge in cyberattacks. Moreover, governments around the world are undergoing a process of digitization, where several services are converting to digital format, increasing the efficiency of government provisions. This transition reflects a fundamental technological restructuring of the government where ongoing technological advances were accelerated and new technological challenges were presented. Ensuring proper cybersecurity standards would allow the state government to realize the full potential of technological advancement.

National Trends in Cybersecurity

Cyberattacks have been rising over the last decade, with escalation in recent years. Data from the FBI's Internet Crime Complaint Center indicated exponential growth in its complaints over the past five years, experiencing a 69.4 percent surge in 2020 over 2019.[1] A study of data breaches in over 500 organizations suggested that the costs associated with each breach also rose 10 percent over the previous year.[2] Research also suggests that cybercriminals have become more sophisticated in their attacks, making them harder to detect and becoming more prolific in their ability to circumvent cybersecurity efforts.[3] Increases in the frequency, average costs, and sophistication of cyberattacks highlight the importance of enhanced cybersecurity standards.

In many ways, the COVID-19 pandemic exacerbated growing issues in cybersecurity by introducing new vulnerabilities and amplifying existing ones. According to a recent survey, 81 percent of executives admitted that adjustments at the onset of the COVID-19 pandemic forced

[1] https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

[2] https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic

[3] https://blogs.microsoft.com/on-the-issues/2020/09/29/microsoft-digital-defense-report-cyber-threats/

their organization to bypass cybersecurity processes and controls.[4] Of all the respondents in the survey, 77 percent saw a clear rise in cyberattacks in 2021, compared to a 59 percent rise the previous year. Another recent study attributes the post-pandemic rise in cybersecurity risk to three factors—the shift to remote work, expanding software supply chains, and migrating to the cloud-based technology.[5] Understanding the threats corresponding to these factors can provide insights into the allocation of government resources across competing methods of cybersecurity risk mitigation.

An adverse consequence of the transition to remote work at the start of the pandemic was a dramatic rise in cyberattacks. In the early months of the pandemic, the FBI's Cyber Division reported an increase in daily cybersecurity complaints from around 1,000 per day to around 3,000-4,000 daily complaints.[6] To make matters worse, the average cost of a data breach increases by over $1 million when remote work is a factor, relative to all other breaches.[7] Despite a clear rise in these cyberattacks, many of them could have been avoided by employees following proper policies and procedures. An estimated 95 percent of all cybersecurity issues can be traced to human error.[8] A recent study explored the causes of workforce cybersecurity breaches and found that they mostly stemmed from non-malicious reasons, including stress, job demands, and the prohibitive burdens of cybersecurity policies themselves.[9] These findings illustrate the opportunities for organizations, including governments' internal operations, to create an environment that facilitates cybersecurity compliance.

Advances in IT have allowed for enhanced provision of government services through a broad technological supply chain, including hardware, software, service providers, managed third-party vendors, and other contractors.[10] This reliance on external technological resources within the government's supply chain adds a dimension of complexity in mitigating cyberattacks. Because these technological supply chains can introduce obscurities in cybersecurity mitigation efforts, cyberattacks on supply chains are expected to escalate over time by an order of magnitude and increase in sophistication.[11] As a result, agencies should dedicate considerable attention to ensuring the integrity of their technological supply chains.

Growing data storage and computational demand has prompted growth in cloud services. The COVID-19 pandemic accelerated the transition to cloud services, as governments experienced an escalation in digital transformation to enhance services and meet the needs of their constituents.[12] While the growth in cloud-based operations can enhance the efficiency of government services, the costs associated with cloud-based breaches also tend to be higher. In 2021, companies with

[4] https://www.ey.com/en_us/cybersecurity/cybersecurity-how-do-you-rise-above-the-waves-of-a-perfect-storm

[5] https://www.tenable.com/press-releases/seventy-four-percent-of-organizations-attribute-damaging-cyberattacks-to

[6] https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic

[7] https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic

[8] https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

[9] https://hbr.org/2022/01/research-why-employees-violate-cybersecurity-policies

[10] https://www.cisa.gov/supply-chain

[11] https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks

[12] https://www2.deloitte.com/us/en/insights/industry/public-sector/government-digital-transformation-strategy.html

higher rates of cloud migration had an average breach cost of $5.12 million, while companies with lower levels of cloud migration had an average breach cost of $3.46 million.[13] In the notable case of SolarWinds—a software company headquartered in Austin, Texas, Russian hackers accessed cloud-based services, affecting at least 100 large companies, state governments, and several U.S. federal agencies, including the Treasury, Energy, Justice, and Homeland Security departments.[14] In this case, as in several cloud-based cyberattacks, hackers established credentials and infiltrated organizational data and communications. This example highlights the importance of cybersecurity in cloud-based operations and technological supply chains in general.

State-level Cybersecurity

With a rise in cyberattacks, several states recently passed legislation to enhance cybersecurity and combat cybercriminals. In Texas, over the past few legislative sessions, lawmakers have significantly increased funds and passed other legislation to improve cybersecurity and modernize information systems. These state funds, along with federal stimulus and infrastructure funds, have prompted efforts to prioritize the dedicated funds in ways that optimally mitigate broad risks to society and promote efficiency through improvements in information systems.

According to the Texas Legislative Budget Board, cybersecurity in the state budget is manifested in several ways, including state agency staff, data center services, centralized accounting and payroll/personnel systems, capital budgets, ongoing maintenance, and major information resources projects.[15] A large share of this is appropriated to the Department of Information Resources (DIR) for ongoing cybersecurity services and new cybersecurity projects and initiatives. Through these administrative allocations, Texas officials must draw from national trends and assess existing vulnerabilities to prioritize investments in cybersecurity and information system modernization.

Risk and Optimal Mitigation

One approach to measuring the adequacy of state cybersecurity measures is to compare resource allocations to private sector institutions. Private sector businesses have direct financial incentives to protecting their assets from cyberattacks, making their decisions indicative of the value of cybersecurity efforts. Relative to private sector institutions, state governments have historically underemployed cybersecurity professionals. In 2018, for example, the average state IT security office employed 6-15 cybersecurity professionals, while financial service firms, for example, of similar size employed over 100 cybersecurity professionals, on average.[16]

While state government cybersecurity teams may historically maintain fewer cybersecurity professionals relative to private sector institutions of the same size (with respect to employees), several factors differentiate the value of mitigating cyberattacks. First, costs incurred by the

[13] https://www.ibm.com/downloads/cas/JDALZGKJ

[14] https://foreignpolicy.com/2021/05/24/cybersecurity-cyberattack-russia-hackers-cloud-sunburst-microsoft-office-365-data-leak/

[15] https://www.lbb.texas.gov/Documents/Publications/Presentation/5196_Cybersecurity_SFC_Mar_21.pdf

[16] https://www.nascio.org/wp-content/uploads/2019/11/2018DeloitteNASCIOCybersecurityStudyfinal.pdf

private sector reflect a dollar-for-dollar tradeoff, while the costs incurred by the government include the excess burden caused by distortionary taxation. In that regard, an otherwise equal cost-benefit analysis would account for the relative underinvestment of government resources allocated to mitigation efforts. The benefits of state-level mitigation efforts also generally differ significantly from private sector benefits. For comparison, JPMorgan Chase & Co—one of the largest financial institutions in the U.S.—had $279 billion in equity ($3.4 trillion in assets) in 2020, while Texas had a $51 billion net asset position ($228 billion in assets).[17,18] From that perspective, larger private sector resources allocated to cybersecurity would seem more appropriate. Such an approach to validating state cybersecurity resources, however, understates the value that cybersecurity enhancement efforts would create. For example, measures of state assets significantly understate the broader impact on households, businesses, and other potential beneficiaries, like local governments.

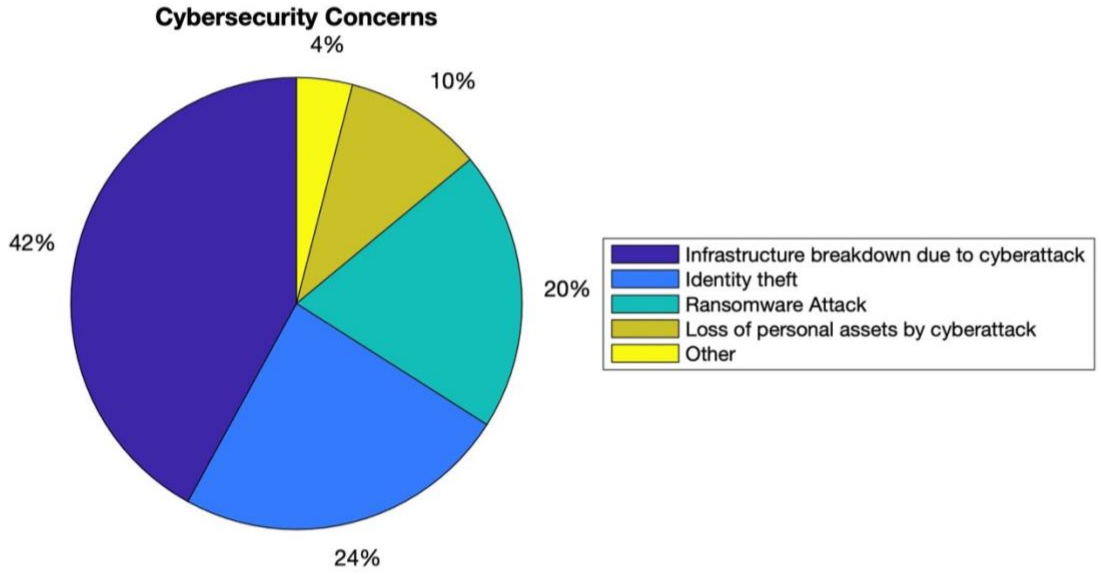
Determining the optimal allocation of state funds and design of mitigation efforts involves a complicated abstract framework that identifies internal and external stakeholders, assesses the corresponding value protected by state cybersecurity mitigation, and quantifies risks of cyberattacks. The state's internal assets, stakeholders, and value at risk may be easier to identify because of its direct oversight of its own resources. To understand the broader social benefit of the state's cybersecurity mitigation efforts, however, the state must also identify stakeholders outside of its direct supervision but still within its regulatory jurisdiction or scope of influence. For example, Texas has over 1,200 incorporated cities—many which may not have the resources to invest in appropriate cybersecurity mitigation.[19] By leveraging its size, the state can exploit economies of scale to provide cybersecurity assistance to local governments and enhance the wellbeing of its constituents.

Another challenge in measuring the proper allocation of state resources involves understanding the risks incurred by each of the respective stakeholders. Quantifying risk involves determining the frequency of successful cyberattacks and the corresponding losses associated with an attack. The attacks and corresponding losses can come in several forms, including confiscation of assets, ransoms paid, and information theft. In a survey of cybersecurity leaders across the world, 42 percent found an infrastructure breakdown due to cyberattacks to be the greatest concern, followed by identity theft at 24 percent, ransomware attack at 20 percent, and loss of assets by cyberattack at 10 percent. These responses reflect expectations over future cyberattacks and can serve as inference to the corresponding risk associated with different types of cyberattacks.

[17] https://www.wsj.com/market-data/quotes/JPM/financials/annual/balance-sheet

[18] https://comptroller.texas.gov/transparency/reports/comprehensive-annual-financial/2020/

[19] https://comptroller.texas.gov/transparency/local/cities.php



The specific concerns of cybersecurity leaders can provide some guidance to governments seeking to mitigate the impact of cyberattacks. For example, given the extensive scope of the Texas state government infrastructure—including regulatory authority over private providers—concerns over infrastructure breakdown indicate that critical infrastructure protection against cyberattacks should be prioritized. Additional concerns over identity theft highlight the need to protect state-held constituents' data, including any driver's license information and taxpayer data. Exposure of individual data could lead to identity theft, causing victims to incur significant direct financial losses. Similarly, exposure of any private business data could give significant advantages to the competitors of Texas-based corporations, diminishing the value of Texas residency. Ransomware attacks are particularly concerning to smaller resource-constrained entities, including local governments, who are generally more susceptible to cyberattacks. Finally, direct loss of assets could be a bigger concern for private institutions that hold financial assets or intellectual property, but as mentioned above, the state of Texas maintains $228 billion in assets, requiring assessment and protection from cyberattacks.

Potential Vulnerabilities

State governments across the US are facing several challenges in addressing cybersecurity. In a recent survey of state-level chief information security officers, 57 percent identified ransomware attacks as the greatest cybersecurity risk pertaining to the continuity of government.[20] Other risks included compromises to the software supply chain, agency use of shadow IT solutions or products, and stolen identities/fraudulent claims for benefits. Texas has confronted several of these challenges faced by other states, while also incurring several extraordinary risks. This section identifies and evaluates several of these risks.

[20] https://www.nascio.org/wp-content/uploads/2021/10/2021-State-CIO-Survey.pdf

Critical Infrastructure

Although cyberattacks can come in several different forms, the occurrence of ransomware attacks has grown in recent years. Notably, on May 7, 2021, hackers accessed Colonial Pipeline Company's computer system and installed malware, causing the company to shut off its entire network.[21] The 5,500-mile system of pipeline, which runs from Texas all the way up the East Coast to New York, became effectively locked until a ransom of $5 million was paid to Russian-based cybercriminals the next day.[22] The potential harm caused by these disruptions makes private and public infrastructure a key target for cyberattacks. In another alarming case, on February 5, 2021, a hacker tried to poison the water supply of 15,000 people in Oldsmar, Florida by increasing sodium hydroxide levels.[23] These cyberattacks show how critical infrastructure, serving millions of people, could become impaired without maintaining strict cybersecurity standards.

Because of its prevalence in energy production and other industrial sectors, Texas has an extensive network of industrial infrastructure, including the nation's largest pipeline network. According to data from the U.S. Department of Transportation, Texas leads the nation in natural gas distribution with 15.9 percent of the total natural gas pipeline and approximately one-third of nation's hazardous liquid pipeline.[24] The vast extent of infrastructure within the state highlights the exceptional risks associated with potential cyberattacks in Texas.

Damages in Texas associated with Winter Storm Uri indicate the potential losses from a disruption in the state's energy infrastructure stemming from a cyberattack. The value of uninterrupted power supply to households and businesses is measured by a metric known as *value of lost load* (VOLL). During Winter Storm Uri, the load shed duration was 70.5 hours, with an average load shed of 14,000 MW, leading to an estimated VOLL of $4.3 billion in 2019 dollars, or roughly $61 million per hour.[25] As the Texas population grows and energy needs of the state continue to expand, the potential losses will rise with it, highlighting the importance of protecting the state's critical infrastructure from cyberattacks.

Although much of the state's energy and industrial infrastructure is privately managed, the existence of large externalities presents incentives for underinvestment in cybersecurity measures, relative to socially optimal levels. As a result, the electric grid infrastructure and other critical infrastructures have heightened susceptibility to cyberattacks. Although much of the Texas electric grid operates in an autonomously regulated environment through the Electric Reliability Council of Texas (ERCOT) and the Public Utility Commission of Texas (PUCT), certain federal regulations still apply in the maintenance of security standards.[26] Specifically, the North American Electric Reliability Corporation (NERC) provides regulatory standards known as Critical Infrastructure Protection (CIP)—a set of security standards, including cybersecurity,

[21] https://www.npr.org/2021/05/08/995040240/cybersecurity-attack-shuts-down-a-top-u-s-gasoline-pipeline

[22] https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html

[23] https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2021/03/10/florida-hack-exposes-danger-to-water-systems

[24] https://www.phmsa.dot.gov/data-and-statistics/pipeline/pipeline-mileage-and-facilities

[25] https://www.dallasfed.org/research/economics/2021/0415.aspx

[26] https://www.ercot.com/mktrules/compliance

applicable to certain components of the nation's electric grid. While these enforceable standards can mitigate underinvestment in cybersecurity resources, two factors limit the extent of its impact. First, NERC's regulatory authority is limited to utilities that generate more than 300 MW of electricity, which excludes 84 percent of all Texas utility companies.[27] Second, NERC's regulatory authority is limited to the transmission, but not the distribution of electricity, where many of the documented cases of cyberattacks have happened.[28] The limitation of the federal regulatory authority over these entities creates an opportunity for the state to promote cybersecurity standards through regulation or guidance.

A recent study evaluated potential cybersecurity weaknesses in Texas' electrical grid and offered solutions for Texas policymakers to protect unregulated sections from cyberattacks. The recommendations were based on a public-private partnership that enhances communications between utilities and state regulatory agencies and allows for increased flexibility in resolving individual issues. The improvement in communication would include guidance from the state agencies on best practices and provide a clearinghouse for cooperation and coordination in response to incidents. The study also recommended three options for specific actions to reduce cybersecurity risks in the electrical grid. First, the state could promote CIP compliance and offset its costs, either through a grant program or other subsidies. This would be aimed primarily at cooperatives and municipal governments who may lack the scale in financial resources to maintain proper cybersecurity standards. Second, the state could simplify complicated aspects of CIP standards and streamline an audit process to improve compliance. This could reduce the costs of implementation and improve the efficiency of audits. Finally, the state could mandate or otherwise promote cyber insurance policies. In addition to pooling risk, insurance companies in this market have taken on the additional roles of protecting and preventing breaches and aiding in compliance. In this more market-based approach, individual entities might benefit from lower insurance premiums by having higher cybersecurity standards. Moreover, the role of insurance companies in mitigating cyberattacks could align the incentives within the private market to promote effective and efficient methods of implementing cybersecurity standards.

While most electric companies and other utility providers implement cybersecurity standards corresponding to their specific service, other entities might be involved in a broad set of services, causing them to fall outside of the scope of specific guidelines for a given utility. For example, the Lower Colorado River Authority (LCRA) provides services that span multiple utility categories, such as water and electric power supply.[29] As a result, the cybersecurity standards pertaining to electricity, for example, might not have the flexibility to serve the broader needs of the organization. Instead, the LCRA adopted the NIST's Cybersecurity Framework (CSF) that provided LCRA with this needed organization-level flexibility.[30] The CSF provides voluntary guidance, based on existing standards to effectively manage cybersecurity risk. Organizations implementing CSF span a range of categories, including governments, academic institutions, and critical infrastructure providers. The success of the LCRA in implementing CSF standards indicates the value that adoption might have for other entities in Texas. As a result, PUCT might benefit from working with utility companies under its supervision to adopt and implement the

[27] https://onlinelibrary.wiley.com/doi/abs/10.1002/rhc3.12241
[28] https://www.osti.gov/servlets/purl/1337873
[29] https://www.lcra.org/about/overview/
[30] https://www.nist.gov/cyberframework/success-stories/lower-colorado-river-authority

CSF. Moreover, given the flexibility of the CSF, other organizations throughout the state government and throughout the scope of influence of the state government might also benefit from adopting the CSF.

Technological Supply Chains

As mentioned earlier, technological supply chains span a broad range of categories, including hardware, software, service providers, and third-party vendors. Although many of these private suppliers implement industry-leading cybersecurity standards, the state is ultimately responsible for ensuring the integrity of its cybersecurity. Moreover, some suppliers might not practice ideal cybersecurity standards, exposing the state's data and resources to cybercriminals. In one case, a cybersecurity breach of Vertafore's database exposed information of 27.7 million Texas drivers, including their driver's license numbers, names, dates of birth, addresses, and vehicle registration histories.[31] Although Vertafore's relationship with the state is unclear, the prospect of a company maintaining private government data highlights the risks involved with technological supply chains.[32]

Part of most states' technological supply chains includes cloud services. The role of cloud-based services, including storage and web-based applications, in the ongoing digital transformation by state governments condenses data in large digital storage units, increasing the value of a breach to cybercriminals. As a result, a notable increase in recent breaches have been cybercriminals accessing cloud-based services. In response to this increased reliance on cloud-based services and the corresponding surge in cyberattacks on cloud-based resources, the state should prioritize cybersecurity of any cloud-based operations.

The Texas Risk Authorization Management Program within the DIR currently provides a framework for ensuring the cybersecurity compliance of cloud services. The framework also applies to several peripheral technologies and certain software within the state government's supply chain. Ensuring the sufficiency of resources dedicated to the program can expedite broad compliance and facilitate ongoing transitions to cloud-based operations.

Local Governments

Compliance with modern cybersecurity standards can be prohibitively expensive for small entities, including local governments. This persistent underinvestment in cybersecurity combined with extensive amounts of personal information and, in many cases, management of critical infrastructure makes local governments prime targets for cyberattacks.[33] For example, in 2020, 44 percent of the global ransomware attacks targeted municipalities.[34] In August of 2019, local government cybersecurity vulnerabilities were exposed when 22 Texas towns were hit by a ransomware attack. The cybercriminals accessed the towns' internal systems through their

[31] https://www.zdnet.com/article/info-of-27-7-million-texas-drivers-exposed-in-vertafore-data-breach/
[32] https://www.txdmv.gov/vertafore
[33] https://icma.org/articles/pm-magazine/look-local-government-cybersecurity-2020
[34] https://www.infosecurity-magazine.com/news/local-government-targeted

supply chain by infiltrating a software used by several municipal governments.[35] This attack created irreparable damage to local governments and their constituents and prompted a lengthy recovery process.

The Texas Municipal League maintains a cybersecurity clearinghouse to disseminate information and provide resources to encourage local governments to implement best practices in cybersecurity.[36] Through the organization, municipal governments can also access an intergovernmental risk pool that insures against losses associated with cyberattacks.[37] In a recent national survey of local governments' IT executives, 90 percent indicated that their local government organization had insurance in 2021, relative to 78 percent the previous year.[38] Despite this growth in insurance take-up rates among local governments, the survey also indicated increased complexity and stringent procedures associated with the policies, as only 23 percent of local government IT executives expressed confidence in their understanding of insurance policy requirements and procedures following an incident. This may present an opportunity for the state government to work with municipal governments to improve their compliance with cyber insurance policies. This could lead to an improved relationship between the state and local governments in addressing cybersecurity, as the survey found that 44 percent of local IT executives' organizations had a fair relationship with the state's IT organization, while 25 percent indicated the relationship was poor. Finally, the state might also consider subsidizing local cybersecurity efforts, as 57 percent found their corresponding budgets to be inadequate. Part of the financial strains experienced by local governments are the result of rising insurance costs, as 69 percent of respondents confirmed an increase in cyber insurance premiums since the last renewal date.

At the state level, the Texas Cybersecurity Council establishes a partnership between private industry and public sector organizations to provide resources, including information, assessment, and best practices.[39] Moreover, the state requires cybersecurity training for all employees of state and local governments.[40] In addition to these resources, the state might benefit from expanding its role as a general cybersecurity consultant to local governments. By leveraging its scale, the state government could enhance its assistance to local governments, much like it does with its broader technological procurement procedures.[41]

Identity Theft

Although identity theft is often associated with financial losses to households—a category that falls largely within the scope and jurisdiction of federal law enforcement—state governments can also incur significant losses resulting from identity theft. In 2020, fraudulent government benefits

[35] https://www.usatoday.com/story/tech/news/2021/07/26/texas-ransomware-attack-impact-cyberattack-cybersecurity-small-town-america/8090316002/

[36] https://www.tml.org/199/Cybersecurity-Clearinghouse

[37] https://www.tmlirp.org/risk-management/cyber-liability/

[38] https://comptiacdn.azureedge.net/webcontent/docs/default-source/research-reports/pti-2021-cybersecurity-report-final.pdf?sfvrsn=fbe93818_2

[39] https://dir.texas.gov/information-security/texas-cybersecurity-council

[40] https://dir.texas.gov/information-security/statewide-cybersecurity-awareness-training

[41] https://dir.texas.gov/it-solutions-and-services/local-government

comprised the largest share of identity theft (32 percent), followed by credit card fraud (30 percent) and miscellaneous identity theft (23 percent).[42] Across the U.S., a notable surge in fraudulent and improper unemployment insurance claims associated with pandemic-related job losses amounted to an estimated $87 billion in losses of federal resources. A report from the Department of Labor attributed deficiencies in improper unemployment insurance payment detection to states' IT systems not being modernized and insufficient staffing resources.[43]

In Texas, losses associated with pandemic-related fraudulent unemployment insurance claims reached an alarming $2.5 billion.[44] Although Texas fares better than other states in terms of shares of fraudulent claims paid, enhancements in information systems and cybersecurity could generate large returns to taxpayers. These enhancements could involve both internal enhancements to state-level technology and cybersecurity mitigation efforts, as well as any efforts to improve constituents' identity protection.

Possible Actions

This section presents some potential considerations in the prioritization of state spending and the implementation of cybersecurity standards within the state's scope of influence. Any policy resolution addressing state cybersecurity must recognize that certain available funds—particularly transfers from the federal government—may not be available in the future. As a result, the funding structure itself must be considered in prioritizing spending alternatives. This may be particularly relevant for certain outlays, such as staffing decisions.

With the heightened risk to critical infrastructure, expanding the capacity of the PUCT to ensure cybersecurity standards of entities within its jurisdiction could result in more resilient utility provision. Events over the past few years that immobilized utility and resource provision highlighted the importance of its continuity. By implementing heightened cybersecurity standards, the PUCT might also resolve underinvestment because of a misalignment between private and public returns in these markets.

Policy resolutions addressing state cybersecurity must recognize the regulatory burden imposed onto any organization, including state agencies. A recurring theme in the implementation of cybersecurity standards, whether internal to organizations or external through government regulations, is that compliance can create an overwhelming responsibility to cybersecurity officials and staffs. For example, roughly half of information security officers identify compliance as the most stressful part of their jobs, and 57 percent of them anticipate that regulation will become more onerous in the years to come.[45] Although this should not be interpreted as motivation for reducing standards, it does highlight the importance of implementing standards designed to facilitate compliance. Otherwise, the limited resources of

[42] https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20theft%20and%20fraud%20complaints

[43] https://www.oig.dol.gov/doloiguioversightwork.htm

[44] https://www.kvue.com/article/news/local/texas/texas-unemployment-fraud-pandemic/269-bef17d2a-07d9-4520-a7b6-1ff63ed34d91

[45] https://www.ey.com/en_us/cybersecurity/cybersecurity-how-do-you-rise-above-the-waves-of-a-perfect-storm

any entity or agency might be dedicated to circumventing compliance instead of enhancing cybersecurity.

The cases of overlapping utility services showed why cybersecurity standards must be flexible enough to meet the needs of heterogeneous organizations, rather than standards specific to an industry. The standards achieved by LCRA also showed how state officials might approach cybersecurity of critical infrastructure through flexible guidance instead of regulation. That approach might involve the DIR or state agencies working with entities within their jurisdiction to implement standards in a way that facilitates and encourages compliance.

Given the cybersecurity issues associated with remote work, the state should consider security enhancements to remote work environments. This priority could be an ideal candidate for allocating one-time money since it reflects a surge in cybersecurity standards. Certain specific actions could include revisions to remote work policies, establishing heightened connection standards (i.e., network security), regulating personal devices, and securing communications.[46]

In a survey of state chief information officers, lack of sufficient cybersecurity budget and inadequate cybersecurity staffing were the top barriers to overcome cybersecurity challenges.[47] To overcome these challenges, state officials might consider taking steps to enhance cybersecurity workforces by providing financial resources to recruit and retain qualified staff. This might include specific measures like improving pay scales, providing better training opportunities, and expanding workforce competencies.[48]

Another specific action that the state can take is continuous vulnerability assessment. Vulnerability management tools and methods can be used to assess state resources to help cybersecurity professionals identify risk exposure and prioritize mitigation efforts.[49] As with many other cybersecurity priorities, meeting goals may also involve increased staffing. The National Initiative for Cybersecurity Careers and Studies identifies a specific area of specialization for vulnerability assessment analysts and provides recruiting guidance for management.[50]

Finally, the state should take every effort to secure its broad technological supply chain and any cloud-based resources, including data storage, migration, and operations (including web applications). Much of the existing literature on cybersecurity—particularly in the aftermath of the pandemic—identifies an increase in security threats to supply chains and cloud-based operations as a result of accelerated digital transformation. By taking steps to ensure the cybersecurity of these resources as early as possible, state officials can lay the foundations for secured digitization to enhance the delivery of government services. The NIST offers standards

[46] https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/how-to-maintain-cybersecurity-for-your-remote-workers.aspx
[47] https://www.nascio.org/wp-content/uploads/2020/10/2020-Deloitte-NASCIO-Cybersecurity-Study-1.pdf
[48] https://www.nascio.org/wp-content/uploads/2021/04/NASCIO_ResilientWorkforce_3.2021.pdf
[49] https://hbr.org/2021/09/the-sec-is-serious-about-cybersecurity-is-your-company
[50] https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework/vulnerability-assessment-and-management

and guidelines for cyber supply chain risk management that may serve as a model for state government resources.[51]

IT Modernization

A key step in optimizing productivity and ensuring the integrity of state information systems involves modernizing hardware and other technology. By maintaining its technology, the state government can improve the efficiency and stability of its operations and enhance cybersecurity standards. Modernizing obsolete information systems can often lead to heightened returns on investment that maximize employee productivity and provide government services at scale.

Technological Returns on Investment

Because government agencies are generally operating from established budgets, rather than driven by profit incentives, fiscal limitations often prevent managers from updating obsolete technology. While such efforts may limit spending over shorter time horizons, it can also lead to growing inefficiencies over time. For example, one study by the Texas Legislative Budget Board found that keeping personal computers more than 4 to 4.5 years led to compounding inefficiencies, including costing 59 percent more to support, taking 50 percent longer to perform tasks, having 53 percent more security breaches, taking 50 percent more energy, and often being out of warranty.[52] Given the growing costs of obsolescence over time, the state might eventually save money on certain systems by modernizing its IT.

In 2017, the Texas Comptroller of Public Accounts reviewed the state's legacy systems and summarized several concerning trends.[53] For example, nearly two-thirds of critical business applications in Texas governments relied on unsupported legacy components. Moreover, the rising costs of maintaining legacy systems reduce the shares of agencies' budgets remaining to update existing systems, compounding the problem. Finally, the persistence of legacy systems causes skilled worker shortages, as the veteran personnel qualified to operate the outdated technology retire or resign.

An increasingly common piece of legacy hardware is the mainframe computer. Although mainframes are still produced and can serve productive business roles, some of the outdated systems might be prime candidates for deprecation. In addition to running slower, the systems often require scarce qualified operators and often cost more than cloud-based services.[54] Outdated mainframes also create lags in processes that require immediate adjustments. For example, in the immediate aftermath of the pandemic, state employees worked on green screens to modify mainframe computer code to expand unemployment insurance from the typical 13

[51] https://csrc.nist.gov/CSRC/media/Projects/cyber-supply-chain-risk-management/documents/C-SCRM_Fact_Sheet_Draft_May_25.pdf

[52] https://www.lbb.texas.gov/Documents/Publications/Issue_Briefs/257_IT%20Replacement%20Schedule.pdf

[53] https://comptroller.texas.gov/economy/fiscal-notes/2017/dec-jan/legacy-it.php

[54] https://www.wsj.com/articles/state-agencies-clinging-to-mainframe-computers-1536163666

weeks.[55] Complexities and inefficiencies corresponding to the existing technology caused massive backlogs and errors at a time when government services needed an escalation of efficiency. Although the systems were nearing replacement at the time, all of the state's taxpayer and unemployment insurance data had been stored on two IBM mainframes that were installed sometime in the early 1990's. This example highlights the importance and urgency in maintaining modernized technology throughout state government.

Texas is not alone in updating its technology. The onset of the COVID-19 pandemic prompted several states to readdress legacy system modernization efforts, partly in response to stimulus and infrastructure funding. According to recent survey results, 60 percent of state information officers indicated an accelerated deployment of legacy modernization strategies, and nearly as many placed a greater emphasis on online services.[56] Other measures included a greater focus on software-as-a-service (commonly known as SaaS) and outsourcing, as well as expanded influence of state-level information offices. Over the next two years, 75 percent of respondents indicated a significant capital investment for legacy modernization in their public service provisions. More than half of respondents also expected significant capital expenditures in labor and employment, health services, and administration/finance/workforce systems.

Adjusting for a Post-pandemic Labor Market

Modernized and enhanced technology could generate significant efficiency improvements, particularly as many employees shift to remote work and as labor markets become increasingly tight. While many employees have returned to in-person work, the state cannot ignore the ongoing transition in labor markets. Growing labor scarcities coupled with increasing competition from outside employers offering remote work opportunities will pressure the state government to consider altering its existing labor policies.

Although competitive labor market pressures will prompt reconsideration of state labor policies, remote work with proper technology could yield several benefits to both the state government and its employees. Regarding benefits to the state government, one study found that widespread adoption of work-from-home technology during the pandemic increased the productivity of working at home by 34 percent, relative to the productivity of working in the office.[57] Given the sharp rise in Austin's cost of living and mounting traffic issues, transition to remote work could also translate into sizable labor cost savings.[58] For example, one study of U.S. workers found that 65 percent of surveyed respondents were willing to take a pay cut to work remotely.[59]

Remote work also has several benefits to employees. With regards to their finances, one study found that 40 percent of remote workers reported saving $5,000 annually, while 20 percent

[55] https://www.kxan.com/investigations/twc-was-1-month-away-from-hiring-firm-to-replace-computer-servers-before-pandemic-hit/
[56] https://www.nascio.org/wp-content/uploads/2021/10/2021-State-CIO-Survey.pdf
[57] https://voxeu.org/article/work-home-technology-boon
[58] https://www.kvue.com/article/money/economy/boomtown-2040/austin-cost-of-living-increase-filterbuy/269-de1d7216-fdcb-4c12-b858-081be5869712
[59] https://www.shrm.org/resourcesandtools/hr-topics/compensation/pages/most-employers-lack-a-pay-strategy-for-remote-workers.aspx

indicated saving up to $10,000 annually.[60] A survey of professionals who worked remotely in the past year also revealed health benefits, as 59 percent of respondents reported making health a priority.[61] Not all employees prefer remote work, however, as 18 percent of those surveyed wanted to return to the office full-time.

An expanding transition to remote work would require restructuring or reconfiguration of state agencies' technological resources. For example, remote work may require portable devices, such as laptops, or possibly home desktops. Creating a remote work environment might also require additional investments in collaborative software. Storage, access to software, and computational resources for remote workers could be facilitated through an expedited transition to cloud-based operations. Finally, increasing prevalence of remote work would also require enhanced cybersecurity infrastructure, including virtual private networks, authentication protocol, and device security. By investing in these technologies, the state government could enable the secure transition to remote work and potentially generate significant fiscal returns over time.

Automation in Government Services

Inherently tight labor markets in the aftermath of the pandemic combined with the ongoing retirement of the baby boom generation will contribute to diminished labor supply over foreseeable future. At the same time, technological advancements have introduced software that can manage several business operations, allowing a technological expansion for tasks previously handled directly by employees. In many cases, these technologies can even generate superior results, relative to employees handling the task directly. Automation through artificial intelligence in customer interaction, for example, has been shown to improve the delivery of government services and generate heightened customer satisfaction.[62] This may involve automated phone services or so-called "chatbots" on agency websites. Significant growth in the Texas population will continue generating a corresponding growth in demand for government services that can be met with scalable automation.

Although automation can resolve several problems and enhance the delivery of government services, government officials may need to overcome several obstacles in its widespread implementation. A survey of state information officers found that adoption and implementation of automation faced four persistent challenges—creating a strategic vision, overcoming a skills gap, having incompatible legacy technology, and establishing policy clarity.[63] This observation highlights recurring problems across information service agencies, including the scarcity of qualified staff and the restrictive consequences of legacy technology. As a result, state officials would benefit from creating a broad strategic vision that addresses several overlapping issues, including workforce development, IT infrastructure modernization, cybersecurity, and automation.

[60] https://www.wsj.com/articles/does-working-from-home-have-to-mean-a-lower-salary-11635699600
[61] https://online.hbs.edu/Documents/work_from_home_infographic.pdf
[62] https://www.mckinsey.com/industries/public-and-social-sector/our-insights/automation-in-government-harnessing-technology-to-transform-customer-experience
[63] https://www.nascio.org/wp-content/uploads/2021/10/NASCIO-CDG-IBM-AI-Meets-the-Moment-2021.pdf

Conclusion

Texas state officials have a unique opportunity to restructure the foundations of state government by securing and modernizing its technological infrastructure. In response to an escalation in the frequency and sophistication of cyberattacks, state officials should deliver corresponding effort to heighten cybersecurity, mitigate risk, and protect state resources and constituents' privacy. By thinking beyond its own agencies, the state government can also improve resource reliability by helping to insulate critical infrastructure and local governments from cyberattacks.

State officials might also consider adjusting policies and spending priorities to match the evolving technological landscape of government services and changes in the labor market. By safely transitioning to cloud-based services and adopting automation, government officials can enhance services and accommodate a remote working environment. Moreover, the state government will be able to soften the impact of several ongoing developments, including population growth, tight labor markets, and an increase in cyberattacks. Making these technological investments and policy adjustments today will help ensure the state's continued success.