BETTER TECH FOR TOMORROW

MODERNIZING TEXAS' WATER INFRASTRUCTURE CYBERSECURITY

WRITTEN BY
David Dunmoyer
May 2024

TABLE OF CONTENTS

MODERNIZING TEXAS' WATER INFRASTRUCTURE CYBERSECURITY

WRITTEN BY **David Dunmoyer**

KEY POINTS

- **Recent cyber attacks** on water infrastructure systems throughout the nation demonstrate the frailty and inadequacy of existing defenses.
- **As state water systems** become more digitalized, the attack vectors are growing without commensurate growth in cyber security and preparedness.
- **The history of public policy** for critical infrastructure cybersecurity is punctuated by a reactionary, fragmented system of governance.
- **The Texas Legislature** should consider seven policy recommendations in the 89th Legislature to position the state as a national leader in water infrastructure cybersecurity.

EXECUTIVE SUMMARY

This paper examines prominent areas of Texas' critical infrastructure and reports on best practices and cybersecurity management procedures that have worked well in other industries and argues that such policies ought to apply to water. Following an analysis of the policy, workforce, and technological needs for critical water infrastructure, this paper proposes seven concrete recommendations that the Texas Legislature and relevant state agencies should consider to equip stakeholders with the tools and resources necessary to lead proactively.

INTRODUCTION

In January of 2024, three small towns in the Texas panhandle were hit with a virulent series of cyberattacks, believed to be levied by a Russian hacktivist group. One such Texas town, Muleshoe, was overwhelmed by the cyber infiltration of their water systems, resulting in their water tank overflowing. This event ultimately forced the city to take their systems offline and revert to manual operations (Lyngaas, 2024). In Hale Center, Texas, authorities noted 37,000 unique attacks in a series of four days, each one attempting to inflict harm on the water supply for this small community of 2,000 residents (Miller, 2024). While these recent attacks highlight the vulnerability of water systems throughout Texas—particularly those in more rural regions of the state—an older and well-documented incident in the state of Florida provides more context for the nature of cyber warfare launched by nefarious actors.

Over the last decade, Oldsmar, Florida, has modernized its water infrastructure, including the use of digital technologies available to water treatment facilities to improve efficiency, accuracy, and economics. Renovation reduced wastewater pollutants and improved the delivery of clean water to its approximately 15,000 residents. However, it created a new threat vector for cyberattacks, as the facility did not include the IT systems, knowledge, or tools

leaving it vulnerable. In February 2021, Oldsmar's water treatment facility was hacked by criminals who adjusted the levels of sodium hydroxide to a toxic concentration (Greenberg, 2021). Were it not for a vigilant employee who spotted the intrusion as it was happening, this could have proved fatal for an unthinkable share of its residents.

The Oldsmar incident was not merely the consequence of failure to prepare. This is just one example of such an attack, propelling numerous cybersecurity experts to sound the alarm. Municipal water systems can be easy targets for hackers because a local government's computer infrastructure is often underfunded and ill-prepared (The Detroit News, 2021). While cybersecurity challenges persist throughout the entire utility sector, the water industry is emerging as the bigger target, with threats to its security and safety increasing daily (Segal, 2022).

The Federal Energy Regulation Commission and the North American Electric Reliability Corporation have had a long-term goal of securing the electric grid against cyber criminals. Both organizations have codified cybersecurity rules that are applicable to each electric utility provider.

For its part, the oil and gas industry adopted a more reactive approach, tightening cybersecurity after the 2021 Colonial Pipeline attack (Jones, 2022). However, "there are no set standards or enforced guidelines for the cybersecurity standards in the water and wastewater sector. This has been mostly governed through the [Cybersecurity and Infrastructure Security Agency] CISA and [the National Institute of Standards and Technology] NIST" (D. Wallace, personal communication, March 1, 2022).

At the federal level, a finer point was placed on the urgency to modernize water infrastructure cybersecurity preparedness in a letter warning state governors from the Environmental Protection Agency Administrator Michael Regan and National Security Advisor Jake Sullivan. The letter underscored the rise in threat from attackers—namely the Iranian Government Islamic Revolutionary Guard Corps—exploiting water facilities that neglect to change default passwords as well as state-sponsored attacks from the People's Republic of China that indicate a pre-positioning to wreak destructive havoc on water infrastructure in the event of military conflicts (The White House, 2024). The letter goes on to encourage governors to take immediate action to ensure cybersecurity best practices and consider advancing policy and practices that will better fortify their critical water infrastructure systems.

This paper serves as a resource to accomplish these very goals and position Texas as a national leader in critical water infrastructure cybersecurity.

THE WATER INFRASTRUCTURE CYBERSECURITY PROBLEM

Densely populated cities across the world are capitalizing on emerging technologies to improve service delivery and management. Such cities are eagerly adopting the title "smart city" which is characterized as a municipality that leverages information and communication technologies (ICT) to enhance the efficiency of operations and management, while improving information sharing for the purpose of benefitting citizen welfare and government services (digi.city, n.d.). As the world population increasingly shifts from rural to urban areas, smart city features are seen as a necessity to effectively manage scarce resources with ever-growing communities and urban footprints.

While there is no concrete threshold for what makes a city "smart," numerous cities throughout Texas have publicly committed to incorporating smart city tenets and technology into their respective ecosystems, including, Austin, Houston, Dallas, San Antonio, and Fort Worth, among others. Each city has taken steps to define an actionable vision of what their smart city future could become, with robust goals over time to leverage data and emerging technology to benefit citizens. While it will certainly be some time before these cities adopt all manner of smart city capabilities, there is an important reality at play that introduces an unavoidable tension: the reality that technology moves faster than policy.

Table 1

Smart city water management examples

1	Computers and software can be used to assess water composition, determine the amount of chemicals needed to treat water, the delivery ofchemicals to treat water, and other routine water system actions.
2	Modeling, simulation, and predictive analysis can be used in critical water infrastructure to develop more sustainable water distribution networks, water collection systems, and flood protection systems.
3	Smart water meters can improve user and technician convenience as well as autonomously collect information to instantaneously generate error reports when consumption anomalies are detected.
4	Automated alarm mechanisms can report malfunctions as soon as they occur, potentially stopping the flow through any given network to avoid wasted water in the event of broken pressurized pipes.
5	Detection systems can monitor and analyze pollutants even prior to reaching a treatment plant, ensuring that the contents and concentrations of the water will be known before it even reaches the plant.

Note. Data from https://www.sae.org/blog/sae-j3016-update

Consider the city of Austin. In December 2015, the U.S. Department of Transportation (USDOT) launched its Smart City Challenge for cities to "develop ideas for an integrated, first-of-its-kind smart transportation system that would use data, applications, and technology to help people and goods move more quickly, cheaply, and efficiently" (U.S. Department of Transportation, 2017). Seventy-eight cities entered the challenge, submitting plans that outlined problems specific to their city and proposed solutions if awarded the $40 million winning prize. While Austin did not win the challenge, it was one of seven finalists. Following this competition, stakeholders throughout Austin committed to operationalizing some of the goals outlined in the plan. Given the tremendous resources, stakeholder time and expertise, and vision-casting that went into this plan, then-mayor Steve Adler and the Austin City Council codified many elements of this plan into their strategic planning and vision documents. Such elements include automation, connected vehicles, smart grids, enmeshed ICT, and more. Despite the exhaustive detail incorporated into the 70-page proposal, there is only one mention of cybersecurity—an aside that Austin will base its security practices off NIST Cybersecurity and Risk Management Frameworks (Letter from Austin Mayor Steve Adler to Secretary Foxx, 2016). As mentioned previously, there are no robust NIST cybersecurity standards or enforced guidelines for the water and wastewater sector. Naturally, this reveals a significant gap in the consideration of resiliency and safeguards for just one of Texas' major cities with a commitment to becoming a smart city. Unfortunately, this gap in Austin's preparation against a cyberattack on its water infrastructure exists across the urban centers of Texas and the nation.

These five examples are just some of the water sector's smart city components either already underway or being considered by cities throughout Texas. And as a recent Polaris Research report notes, the global smart water management market was a $13.73 billion industry in 2021, and is expected to grow to $31.73 billion by 2030 (Kite-Powell, 2022). As computing power has increased and the cost of processing power, memory, and batteries have

decreased, the tangible and digital worlds are melding into one. Digital devices that are on the edge of critical infrastructure are most commonly linked to the core IT networks that are in turn connected to the wider internet. This means that, as physical infrastructure becomes enmeshed with the digital realm, almost every piece and facet of our water infrastructure may introduce a new cybersecurity threat vector that motivated criminals can exploit .

The Rural Problem

While rural regions of the state are less inclined to fully embrace the "smart city" revolution, they face unique challenges that put their water infrastructure at risk of cyberattack. As noted by the United States Agency for International Development (USAID), "[rural] government institutions frequently lack the budgets, technical capacity, and professional management capabilities" to deliver on the types of services needed for robust critical infrastructure security (United States Agency for International Development, 2022, p. 14). Thus, many rural systems suffer from outdated technology, inadequate cybersecurity expertise and education, funding constraints on prioritizing physical security, and a limited awareness of cybersecurity relative to larger, urban systems and teams.

THE CHALLENGE

There are 7,000 public water systems in Texas. Each system is vulnerable to cybersecurity risks, challenges, and opportunities for enhanced security (Carver & Salhorta, 2023). The problems are broad in number, with Texas being home to various urban, suburban, and rural environments with different needs, regions with a shortage of a cybersecurity workforce, and divergent technological infrastructure and capabilities.

Despite the vastness and diverseness of Texas, the state's water infrastructure cybersecurity needs largely reflect that of the United States at-large. As revealed by a survey conducted by the Water Sector Coordinating Council (WSCC)[1], the utility industry identified four key needs:

1. Water sector specific training and education,
2. Technical assistance, assessments, and tools,
3. Cybersecurity threat information, and
4. Federal loans and grants (2021, p. 5).

The WSCC survey asked respondents to identify the frequency of organizational risk assessments, which include threat and vulnerability analyses, downsides to information processing, and risk mitigation stemming from security and privacy controls. Of the 606 water and wastewater utilities that responded, 27% of utilities conduct threat evaluations less frequently than annually, 24% annually, 17% don't conduct them, and 16% don't know. Further, 71% of respondents noted they have 0 – 2 full-time employees (including contractors and municipal or county staff) dedicated to Information Technology (IT) cybersecurity, and 73% noted 0 – 2 full-time employees dedicated to Operational Technology (OT) cybersecurity. The WSCC survey identified a finding of great consequence: fully 67% of water utilities report that cybersecurity is either not a priority or a low priority (Water Sector Coordinating Council, 2021).

Texas has an agency tasked with overseeing critical infrastructure cybersecurity: the Texas Department of Information Resources (DIR). In 2013, the Texas Legislature passed Senate Bill 1102 to create the Texas Cybersecurity Council, a program overseen by DIR, which facilitates partnerships between private industry and public sector organizations to safeguard the cybersecurity of Texas' critical infrastructure (2013). In 2020, DIR adopted the Texas Cybersecurity Framework, based on the NIST Framework for Improving Critical Infrastructure Security. DIR published a report in 2020, acknowledging current shortfalls in Texas' cybersecurity preparedness. The DIR report provides information on tips and tools across the entire critical infrastructure ecosystem,

1 The Water Sector Coordinating Council is a "policy, strategy and coordination mechanism for the US Water and Wastewater Systems Sector in interactions with the government and other sectors on critical infrastructure security and resilience issues…[it] coordinates and collaborates with EPA, the Department of Homeland Security, state primacy administrators and other government agencies" (NACWA, 2022).

but without a direct mention of water infrastructure. The DIR report concludes with a lengthy list of legislative recommendations, suggesting new laws to address the direct concerns and needs of water infrastructure across the state (Texas Department of Information Resources, 2020).

Immediately, this reveals the more quantifiable challenge of water infrastructure security. Water utility providers acknowledge specific needs to improve the security of their systems, but they lack the resources, knowledge, workforce, or drive to make action a priority. While the trade associations might declare that cybersecurity is a top priority for the water and wastewater sector, this has yet to translate into needed policy or substantive downstream change (Germano, 2019). Considering the potential human and financial toll of sluggish target hardening and cybersecurity enhancements, it has become evident that the clock is ticking to ensure state lawmakers make security the state water infrastructure a priority.

Cyberattacks constantly evolve to identify new vectors, vulnerabilities, and tactics to disrupt water infrastructure systems and wreak dangerous and costly havoc. As an abstract example, chemotherapy is accepted as an effective means of fighting cancer. But what would happen if cancer cells learned to adapt to evade chemotherapy and attack its host more virulently, rendering chemotherapy ineffective? This is how cyber criminals operate. While a security system might have been effective in defending against a common cyberattack levied in 2022, criminals constantly identify new security systems, evaluate bugs or gaps to penetrate, adapt, and find new methods to exploit vulnerabilities, necessitating constant reevaluation of cyber defense processes and systems (Burt, 2023).

The water and wastewater sector remains a soft target for cyber criminals. It has been under a barrage of attacks in the last decade, ranging from ransomware attacks, tampering with industrial control systems, manipulative valve and flow operations, chemical treatment formulations, and efforts to destroy operations and inflict monetary and human life damages. Attacks attempting to contaminate water supply, bring system operations offline, or induce outages can have devastating effects, including casualties, delays in emergency response by healthcare, police, or firefighters, hamstringing transportation systems, and affecting food supply (Germano, 2019).

Identity theft is also a real concern. Much of the water sector store highly sensitive information—for both customers and employees—ranging from billing information, personal identifying information, and sensitive employee information. In 2018, the Federal Bureau of Investigation (FBI) and the U.S. Department of Homeland Security (DHS) made clear that Russian state-sponsored cyber attackers are specifically targeting the U.S. water sector due to its vulnerabilities and the opportunity to inflict cataclysmic harm (Cybersecurity & Infrastructure Security Agency, 2018). Further, in 2024, FBI Director Christopher Wray testified that China's targeting of critical American infrastructure—including water—was happening at an unprecedented scale, with the PRC inserting "offensive weapons within our critical infrastructure poised to attack whenever Beijing decides the time is right" (Parkinson & Hinshaw, 2024).

Despite these dangers, the water sector remains vulnerable and underprepared for this era of digital warfare. As noted by the DHS and the FBI, in many of the successful Russian attacks on the water sector, penetration occurred in networks where multi-factor authentication was not used (Cybersecurity & Infrastructure Security Agency, 2018). Single factor authentication, which remains a common practice across the sector, is a susceptible vulnerability that rogue criminals will continue to exploit. The American Water Works Association (AWWA) identified some underlying inefficiencies in cybersecurity preparedness that increase the risks of attack as illustrated in **Table 2**.

Table 2

Existing inefficiencies in cybersecurity preparedness for water infrastructure

1	Insufficient antivirus, integrity-maintenance, and other security tools, particularly for network devices used by small businesses and operating on residential-class routers.
2	Manufacturers build and distribute the devices with exploitable services to make them easier to install, operate, and maintain.
3	Failure to change vendor default settings, enhance security, and regularly patch systems and software.
4	Failure to remove or update antiquated or outdated equipment that is no longer being supported by the manufacturer or vendor.
5	Overlooking network devices when assessing risk or recovering from a cyber intrusion.

Note. Information from *Cybersecurity Risk & Responsibility in the Water Sector*, American Water Works Association, 2019 (https://www.awwa.org/Portals/0/AWWA/Government/AWWACybersecurityRiskandResponsibility.pdf).

The Texas Commission on Environmental Quality (TCEQ)—in conjunction with the Environmental Protection Agency (EPA) and the Water Information Sharing and Analysis Center—notified public water systems across Texas that cyberattacks are a critical threat that continue to increase due to the Russian-Ukrainian conflict (Betts, 2022). This TCEQ notice came on the heels of the EPA announcement of its Industrial Control Systems Cybersecurity Initiative—Water and Wastewater Sector Action Plan (Action Plan). The Action Plan was directly associated with President Biden's Industrial Control Systems Initiative, which established a joint effort between the critical infrastructure sector and the federal government to streamline the utilization of technologies created to increase the visibility, indicators, detections, and warnings associated with cyber threats (Evironmental Protection Agency, 2022). Unfortunately, the Action Plan lacks adequate funding, enforcement, or strong, actionable goals that are needed to drive the critical water infrastructure sector to a position of strength and compliance. Indeed, the Action Plan creates a task force of water sector leaders, introduces pilot projects for incident monitoring, seeks to improve information sharing, and looks to find ways to provide technical support to water systems. However, it does not provide training, federal loans and grants, or additional tools that AWWA and its members have requested. While reasonable minds can differ on the most prudent and beneficial investments to make in target hardening for critical infrastructure, the bipartisan nature of federal cybersecurity proposals highlights the reality that domestic security and the general welfare of Americans—vis-à-vis cybersecurity—is an apolitical priority.

Cost remains a key animating challenge shared by water infrastructure operators, leaders in Texas, and agencies and elected officials in Washington. During a Congressional hearing in the House Committee on Homeland Security in late 2022, members concluded that fortifying cybersecurity protocols and technology for water infrastructure was a top issue facing critical infrastructure nationwide (Kelley, 2022). Witnesses from municipal water districts were quick to point out that while cybersecurity is no longer optional in the

water sector, budget challenges mean the only way they can make moderate improvements is through increasing utility costs. This practice may be resisted by utility customers. For states with large rural areas like Texas, many districts do not have the money or the means for raising funds for basic technology (Mulverhill, 2019). While witnesses at the hearing pleaded for more federal money, the only response thus far has been the Infrastructure Investment and Jobs Act (IIJA), which authorized $1 billion in funding for a state and local cybersecurity grant program for critical infrastructure (U.S. Department of Homeland Security, 2022). Texas was allocated approximately $40 million through the State and Local Government Cybersecurity Grant Program, and at the time of this publication, the request for applications for year one is closed and awaiting review. It has yet to be seen what priority state and local governments will place on critical water infrastructure over other critical infrastructure through this program (Texas Department of Information Resources, n.d.).

OTHER CRITICAL INFRASTRUCTURE

Cyber threats to critical infrastructure are not new. In 1996, President Bill Clinton issued Executive Order 13010 (1996) which both defined critical infrastructure and established the National Commission on Critical Infrastructure and issued protections (Mariani et al., 2022). Since then, there have been both broad national efforts to address critical infrastructure, as well as sector-specific efforts to harden targets. Given the rate at which technology has progressed since 1996, and the glacial pace of policy related to the same, many of the industry-specific efforts have been in response to crises.

Take for example the success of the 2021 Colonial Pipeline attack attributed largely to lack of preparation. Cyber criminals hacked into the system using ransomware, shutting the entire 5,500-mile system down for five days (Government Technology, 2021). The China-based criminals rendered the pipeline inoperable, stopping the flow of gasoline and jet fuel to customers across the country. Due to the severe damage caused by the security breach and an inability to expeditiously bring systems back online, Colonial opted to pay a $5 million ransom to the criminal group (Wilkie, 2021). This successful blackmail prompted change for the cybersecurity of critical oil and gas infrastructure in the U.S. The White House issued an executive order (2021a) and a national security memo (2021b) which mandated better disclosures of cyber incidents, created a federal playbook for incidents, required the upgrade of cybersecurity technology, established a review board, and promoted a system of cyber-intelligence sharing between government agencies and the private sector (Anscombe, 2022). In addition, DHS established new regulations that require the following: pipelines must designate a "cybersecurity coordinator" who is always available to report cybersecurity threats to the Transportation Security Administration (TSA) and CISA; pipelines must review cybersecurity practices and address new risks and submit monthly reports on these reviews to TSA and CISA; and what were once voluntary guidelines became mandatory, with violations subject to considerable fines (Hendricks & Sessler, 2021). The same vulnerabilities that allowed criminal enterprise to succeed in attacking the largest pipeline system for refined oil products in the U.S. plagues much of America's critical infrastructure and its staff, particularly our water systems.

Electric grids represent another example where the cybersecurity of critical infrastructure was enhanced in the U.S. in reaction to a catastrophic attack. While there have yet to be any successfully executed cataclysmic attacks on America's grid, the 2015 Russian attack on Ukraine's electric grid captivated the attention of leaders across the world. Amidst conflict between the two nations, a Russian threat actor took Ukraine by surprise when a hacker successfully utilized malware to remotely compromise the information systems of three large energy distribution companies. Without any warning, more than 230,000 Ukrainian customers were left without power for hours in the blisteringly cold month of December (Council on Foreign Relations, 2015).

The successful attack in Ukraine demonstrated a tangible threat to America, catalyzing the federal

government into action to harden the cybersecurity preparedness for electric grids. Electric utility grids have adopted numerous cybersecurity improvements over the last decade. The North American Electric Reliability Corporation (NERC) introduced robust cybersecurity standards that have become new requirements on all U.S. electric utilities, including risk assessments, incident reporting, and security controls. In addition, as the U.S. Department of Energy (DOE) acknowledged that the electric grid was developed decades ago using outdated technology that posed cybersecurity risks, electric utilities were required to implement advanced technologies such as intrusion detection systems, firewalls, and security information and event management systems to better defend against cyber threats (U.S. Department of Energy, 2021). The U.S. government now conducts regular simulated cyberattack exercises as a means of testing system readiness. The U.S. government also stepped up to lead efforts in information sharing and public-private partnerships to provide accountability, synergy in adopting best practices, and real-time, industry-wide threat sharing.

These examples illustrate two important realities related to cybersecurity efforts for critical infrastructure systems in the U.S. First, improvements have largely been reactionary. While one could make the case that industry lobbying and advocacy efforts from the electric and oil and gas industries has resulted in securing improvements for their industries over water, their case is made more compelling and urgent because they can point to demonstrable harm, with critical infrastructure cybersecurity measures largely reactive in nature.

Second, it underscores the reality that the U.S.—and states like Texas—address cybersecurity through a sector-specific regulatory scheme. For example, at the federal level, cybersecurity regulations with actual teeth are created and enforced by an agency germane to that industry. The DOE oversees the electric grid and power plants, DHS imposes requirements on pipelines, and EPA is the body responsible for regulating water plants. Consequently, substantive changes to cybersecurity for critical infrastructure are both siloed and driven largely by the fears following a costly attack.

POLICY RECOMMENDATIONS

Federal action can motivate cybersecurity preparedness for water infrastructure in the short term, but ultimately industry stakeholders must adopt similar requirements and mandates that have been imposed by DHS and DOE on the pipeline and electric grid infrastructure, respectively. However, the State of Texas should take the lead and not wait for the federal government or a national water infrastructure cyber crisis to begin adopting policies that will position this key component of Texas' critical infrastructure ready to withstand the digital threats of the 21st century. Below are the policy recommendations that the 89th Texas Legislature should strongly consider adopting if it is to protect our most critical resource.

Create Requisite Statewide Cybersecurity Standards under the Texas Department of Information Resources

DHS implemented two critical steps to standardize cybersecurity requirements that could be emulated in Texas for its water infrastructure. First, the Texas DIR cybersecurity standards and best practices that are currently voluntarily imposed on water infrastructure must be mandated by law, with financial penalties for noncompliant actors. These standards include everything from basic cybersecurity hygiene—such as multi-factor authentication—to certified training programs for specific employees. Second, DHS imposed its cybersecurity standards by clearly defining itself as the chief water infrastructure cybersecurity authority in a parallel manner to how DHS regulates pipeline cybersecurity. DIR could also create a new department with the sole responsibility of overseeing water infrastructure cybersecurity. This will establish a more active relationship between stakeholders in the water space and gives DIR both the stick of enforcement and the carrot of aid —with aid provided both informationally and financially where appropriate. Importantly, while DIR would oversee these standards, they should continue to

partner with the private sector, the Texas Legislature, the Texas Commission on Environmental Quality, and other key stakeholders to make revisions and updates to these standards when necessary.

Prudent Investments in Career Technical Education

Texas must raise the number and quality of IT and OT professionals at water infrastructure sites across the state in order to increase cybersecurity readiness. Unfortunately, there is a looming workforce shortage of these highly sought out professionals. Initially, there was a 41.3% increase in Texas' cybersecurity industry employment from 2013 to 2018, with an expected 35% growth rate over the next decade (Texas Comptroller, n.d.). However, alongside this growth and demand has been a decrease in supply: there is a global shortage of 3.4 million workers in the field of cybersecurity, with more than 700,000 unfilled cybersecurity jobs in America (Lake, 2022). Texas alone has approximately 36,000 cybersecurity job openings that remain unfilled (CyberSeek, n.d.).

The Texas Legislature must invest in comprehensive IT career and technical education opportunities. Texas could develop a policy that better aligns the incentives of CTE funding with outcomes, so programs throughout the state are incentivized to provide more IT programs that can generate high-paying jobs for graduates. If the Texas Legislature passes a law that allocates existing state funding to programs in a weighted fashion—i.e., more money for programs that generate high-paying jobs for CTE students and less for those with lower earnings and outcomes—the market of CTE programs will provide more opportunities for students to earn higher income as cybersecurity professionals for an education that is a fraction of the cost of a four-year college degree.

The benefit to this workforce investment would have a two-fold benefit to the security of the state's critical water infrastructure. Initially, there would be a positive spillover effect. With more IT and cybersecurity professionals in Texas, there would be better cyber standards developed for water infrastructure, better

There is a global shortage of 3.4 million workers in the field of cybersecurity, with more than 700,000 unfilled cybersecurity jobs in America. Texas alone has approximately 36,000 cybersecurity job openings that remain unfilled.

educational cybersecurity training and content for staff working in the industry, and a larger pool of talent to fill IT and OT staffing shortages. An additional benefit is wage normalization for cybersecurity professionals. By creating more employees who can fill the shortage of cybersecurity jobs in Texas, the average salary level will gradually normalize across the board, making the currently noncompetitive salary offered by water infrastructure facilities much more competitive.

Require that Each Water District in Texas Have a Qualified Cybersecurity Manager

The Texas Legislature considered several bills in the 88th Legislature that would have required one person at each Independent School District (ISD) to serve as the point person for instituting the required cybersecurity plan and liaising with Texas' chief ISD cybersecurity officer. A similar model should be applied to water districts throughout the state.

In practice, each water district would designate either an existing full-time employee (FTE) or a new FTE as the manager of DIR-issued cybersecurity standards. These managers would be required to complete additional cybersecurity training (on top of the quarterly training outlined below) and monitor their facility to ensure cyber standards and hygiene are adhered to. Managers would be the party responsible for reporting any cybersecurity threats or attacks made on their facility. Overseeing these "cybersecurity managers" would be DIR, a natural candidate for a central reporting agency that could review, oversee, and respond to cyber reports.

With repeated studies showing that almost 90% of all data breaches and cybersecurity attacks are caused by an employee mistake, human error continues to be a main vulnerability for all sectors at high risk for cyberattacks.

Of important note, this would be a herculean lift for each of the approximately 400 water districts—as well as more than 950 municipal utility districts—to each have their own experts. To avoid one expert overseeing a very small water operation, legislation could be considered that assigns one cybersecurity expert to a collection of water districts based on a set population count.

Increase Cybersecurity Training and Educational Opportunities for Water Districts in Texas

DIR currently requires an annual statewide cybersecurity awareness training for employees at all government entities. While this is an important start, the training infrequency minimizes the efficacy of this program. To increase individual awareness and education of cybersecurity hygiene for employees working in water infrastructure, the frequency of this training should be conducted quarterly. Extensive studies show that employees tend to forget their training after six months, with cybersecurity experts agreeing that employees should receive quarterly training to maximize the cybersecurity benefits. With repeated studies showing that almost 90% of all data breaches and cybersecurity attacks are caused by an employee mistake, human error continues to be a main vulnerability for all sectors at high risk for cyberattacks (Sjouwerman, 2020). Incorporating such training mitigates against the risks that social engineering, ransomware, malware, phishing, and other similar attacks will be successful in water utilities throughout Texas. While the cybersecurity manager will play an important role in creating a culture of cyber hygiene at their water districts, offering expertly crafted, complimentary required trainings from DIR will address a significant oversight currently persisting in Texas.

Conduct Regular Critical Water Infrastructure Cybersecurity Audits

Each water district, at the leadership of its cybersecurity manager, should be required to conduct a cybersecurity audit twice annually. The specifics of the audit's requirements would be issued by DIR, whom the cybersecurity manager would then submit for approval. This would accomplish several important goals. First, required audits would create a mechanism of transparency to ensure that each water district throughout Texas adheres to the uniform DIR standard. Second, audits generate more buy-in from water districts to take the standards and requirements issued by the cybersecurity manager seriously, as they would run the risk of penalties associated with noncompliance. Audits could be a valuable tool for DIR to obtain data on the cybersecurity needs of the entirety of Texas' critical water infrastructure, as well as needs associated with water districts located in specific regions or of certain sizes. Moreover, this could inform state policy and appropriations by identifying targets for Texas to focus its cybersecurity investments for maximum impact, while helping to identify emerging themes on threats, system vulnerabilities, or underdeveloped technologies that DIR should prioritize for training, education, and technological investments.

Ensure Procured Technology Comes Equipped with the Strongest Cybersecurity Options

DIR should develop standard procurement contract language to ensure that in all vendor agreements and technology procurement contracts, strong security filters, storage, and software are incorporated as a default. Many cybersecurity incidents across America are caused by government bodies working with vendors that employ weak security controls (Keating, 2022). By ensuring all vendor agreements are adopted conditioned upon DIR-imposed security standards, the threat of vulnerabilities for systems, information, or data stored with third parties would be greatly mitigated. Language that requires any purchased technology from a vendor for a water

district to come equipped with the strongest security options will increase uptake of readily accessible software designed to protect critical systems. Standard contractual terms represent a simple change that could be readily adopted and provide a strong safety benefit for all critical infrastructure in Texas.

Create a Grant Program or Financing Mechanism for Broader Cybersecurity Improvements

Costs have been the barrier to substantive change to cybersecurity. Yet as this paper lays out, the status quo requires the assumption of significant risk, in the form of extensive human and economic devastation. There is no easy way to estimate the cost of cybersecurity unpreparedness for Texas' water infrastructure. But were one to imagine the consequence of a successful remote poisoning of treated water flowing into the homes of Austin residents, tens, if not thousands, of Austinites could die within minutes of such an attack. Imagine the cost and consequence if the largest dam in Texas—the Mansfield Dam in Austin—were to be hacked and the floodgates left open in this dam that impounds the 369-billion-gallon Lake Travis. There would be incredible damage to the homes, businesses, and infrastructure of the surrounding area, and we would have squandered a precious, scarce, and large resource that all of Texas relies upon.

The Texas Legislature should evaluate the availability of existing state and federal funding for the purpose of operationalizing the cybersecurity policies outlined above. Any additional state funding should be based on verifiable, demonstrated need, and be targeted, prudent, and cost-effective investments. From this fund, low- or no-interest loans should be made available to eligible water districts throughout Texas. Water districts would be required to make repayments into the fund, ensuring that this serves as a resource to fund cybersecurity improvements in critical water infrastructure in perpetuity.

CONCLUSION

Fortunately, Texas has yet to suffer the extensive damage caused by a successful cyberattack on its water infrastructure, but it is carrying the risk. Texas should lead, rather than wait for economic or political heat to take action to make this critical infrastructure more secure. The Legislature should heed the warning calls and pleas from water infrastructure professionals to provide the assistance to fill existing gaps. The call to action can be summed up as follows: the water sector needs more cybersecurity professionals, funding, expert support and guidelines, and standardization to keep their essential services running smoothly and safely. To effectively accomplish this, Texas can pass an omnibus critical water infrastructure cybersecurity bill in the 89th Legislative Session to address this in a manner that is appropriately proactive, protective of this critical resource, and dynamic and long-term oriented to stay abreast of new threats in this sector. ■

REFERENCES

Almar Water Solutions. (n.d.). *Water management in smart cities*. Retrieved April 11, 2024, from https://almarwater.com/water-management-in-smart-cities/

Anscombe, T. (2022, December 6). *What will it take to secure critical infrastructure?* DARK Reading. https://www.darkreading.com/ics-ot-security/what-will-it-take-to-secure-critical-infrastructure

Betts, E. (2022, February 23). *TCEQ and EPA emphasize cybersecurity for water and wastewater utilities*. Texas Rural Water Association. https://www.trwa.org/blogpost/1539239/450385/TCEQ-and-EPA-Emphasize-Cybersecurity-for-Water-and-Wastewater-Utilities

Burt, A. (2023, May 16). The digital world is changing rapidly. Your cybersecurity needs to keep up. *Harvard Business Review*. https://hbr.org/2023/05/the-digital-world-is-changing-rapidly-your-cybersecurity-needs-to-keep-up

Carver, J., & Salhorta, P. (2023, May 3). Everything you need to know about Texas' beleaguered water systems. *The Texas Tribune*. https://www.texastribune.org/2023/05/03/texas-water-infrastructure-broken-explained/

Council on Foreign Relations. (2015). *Compromise of a power grid in eastern Ukraine*. https://www.cfr.org/cyber-operations/compromise-power-grid-eastern-ukraine

Cybersecurity & Infrastructure Security Agency. (2018, April 20). *Russian state-sponsored cyber actors targeting network infrastructure devices*. https://www.cisa.gov/news-events/alerts/2018/04/16/russian-state-sponsored-cyber-actors-targeting-network-infrastructure

CyberSeek. (n.d.). *Cybersecurity supply/demand heat map*. Retrieved April 11, 2024, from https://www.cyberseek.org/heatmap.html

digi.city. (n.d.). *Smart city definitions*. Retrieved April 11, 2024, from https://www.digi.city/smart-city-definitions

Environmental Protection Agency. (2022, January 27). *EPA announces action plan to accelerate cyber-resilience for the water sector* [Press release]. https://www.epa.gov/newsreleases/epa-announces-action-plan-accelerate-cyber-resilience-water-sector

Exec. Order No. 13010, 61 Fed. Reg. 37,347 (July 15, 1996). https://www.govinfo.gov/content/pkg/FR-1996-07-17/pdf/96-18351.pdf

Germano, J. (2019). *Cybersecurity risk & responsibility in the water sector.* American Water Works Association. https://www.awwa.org/Portals/0/AWWA/Government/AWWACybersecurityRiskandResponsibility.pdf

Goddard, W. (2021, August 2). *What are the features of a smart city to look for?* IT Chronicles. https://itchronicles.com/smart-city/what-are-the-features-of-a-smart-city-to-look-for/

Government Technology. (2021, July 8). *Back to basics: A deeper look at the Colonial Pipeline hack*. https://www.govtech.com/sponsored/back-to-basics-a-deeper-look-at-the-colonial-pipeline-hack

Greenberg, A. (2021, February 8). A hacker tried to poison a Florida city's water supply, officials say. *Wired*. https://www.wired.com/story/oldsmar-florida-water-utility-hack/

Hendricks, A., & Sessler, J. (2021, May 31). New cybersecurity rules for pipelines are good. Now let's secure all the other critical infrastructure. *The Dallas Morning News*. https://www.dallasnews.com/opinion/commentary/2021/05/31/new-cybersecurity-rules-for-pipelines-are-good-now-lets-secure-all-the-other-critical-infrastructure/

Jones, D. (2022, May 17). *How the Colonial Pipeline attack instilled urgency in cybersecurity.* Cybersecurity Dive. https://www.cybersecuritydive.com/news/post-colonial-pipeline-attack/623859/

Keating, M. (2022, August 23). *Local governments stay vigilant to cyber threats when acquiring technology*. American City & County. https://www.americancityandcounty.com/2022/08/23/local-governments-stay-vigilant-to-cyber-threats-when-acquiring-technology/

Kelley, A. (2022, September 21). *Federal cyber mandates for water infrastructure are too costly to implement, experts say*. Nextgov. https://www.nextgov.com/cybersecurity/2022/09/federal-cyber-mandates-water-infrastructure-are-too-costly-implement-experts-say/377474/

Kite-Powell, J. (2022, November 27). How technology can mitigate flooding and secure water infrastructure. *Forbes*. https://www.forbes.com/sites/jenniferhicks/2022/11/27/how-technology-can-mitigate-flooding-and-secure-water-infrastructure/?sh=418509875d88

Lake, S. (2022, October 20). The cybersecurity industry is short 3.4 million workers—that's good news for cyber wages. *Fortune*. https://fortune.com/education/articles/the-cybersecurity-industry-is-short-3-4-million-workers-thats-good-news-for-cyber-wages/

Letter from Austin Mayor Steve Adler to Secretary Foxx. (2016, May 20). https://www.transportation.gov/sites/dot.gov/files/docs/Austin-SCC-Technical-Application.pdf

Lyngaas, S. (2024, April 17). *Russia-linked hacking group suspected of carrying out cyberattack on Texas water facility, cybersecurity firm says.* CNN. https://www.cnn.com/2024/04/17/politics/russia-hacking-group-suspected-texas-water-cyberattack/index.html

Mariani, J., Li, T., Weggeman, C., & Kishani, P. (2022, March 8). *Incentives are key to breaking the cycle of cyberattacks on critical infrastructure*. Deloitte Insights. https://www2.deloitte.com/us/en/insights/industry/public-sector/cyberattack-critical-infrastructure-cybersecurity.html

Miller, K. (2024, April 18). *Rural Texas towns report cyberattacks that caused one water system to overflow.* Associated Press. https://apnews.com/article/texas-muleshoe-water-systems-cyberattacks-russia-5f388bf0d581fc8eb94b1190a7f29c3a

Mulverhill, L. (2019). *Texas' digital divide*. Texas Comptroller. https://comptroller.texas.gov/economy/fiscal-notes/archive/2019/oct/divide.php

NACWA. (2022, May 26). *Water sector coordinating council discusses cybersecurity with EPA, DHS*. https://www.nacwa.org/news-publications/news-detail/2022/05/26/water-sector-coordinating-council-discusses-cybersecurity-with-epa-dhs

Parkinson, J., & Hinshaw, D. (2024, February 18). FBI Director says China cyberattacks on U.S. infrastructure now at unprecedented scale. *The Wall Street Journal*. https://www.wsj.com/politics/national-security/fbi-director-says-china-cyberattacks-on-u-s-infrastructure-now-at-unprecedented-scale-c8de5983

SB 1102. Enrolled. 83rd Texas Legislature. Regular. (2013). https://capitol.texas.gov/tlodocs/83R/billtext/pdf/SB01102F.pdf#navpanes=0

Segal, E. (2022, February 13). Biden administration seeks to bolster defenses against cyberattacks on water systems. *Forbes*. https://www.forbes.com/sites/edwardsegal/2022/02/13/bidden-administration-seeks-to-bolster-defenses-against-cyberattacks-on-water-systems/?sh=6a0498491ff9

Sjouwerman, S. (2020, March 4). *Stanford research: 88% of data breaches are caused by human error.* KnowBe4. https://blog.knowbe4.com/88-percent-of-data-breaches-are-caused-by-human-error

Texas Comptroller. (n.d.). *Cybersecurity: Statewide overview*. Retrieved April 11, 2024, from https://comptroller.texas.gov/economy/economic-data/cybersecurity/texas.php

Texas Department of Information Resources. (2020, November 15). *2020 cybersecurity report*. https://dir.texas.gov/sites/default/files/2021-03/2020%20DIR%20Cybersecurity%20Report_0.pdf

Texas Department of Information Resources. (n.d.). *State and Local Government Cybersecurity Grant Program (SLGCP)*. https://dir.texas.gov/information-security/state-and-local-cybersecurity-grant-program-slcgp

The White House. (2021a). *FACT SHEET: President signs executive order charting new course to improve the nation's cybersecurity and protect federal government networks*. https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/

The White House. (2021b). *National security memorandum on improving cybersecurity for critical infrastructure control systems*. https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/

The White House. (2024, March 18). *Environmental Protection Agency and National Security Affairs letter to governors*. https://www.epa.gov/system/files/documents/2024-03/epa-apnsa-letter-to-governors_03182024.pdf

The Detroit News. (2021, February 8). *In Florida city, a hacker tried to poison the drinking water.* https://www.detroitnews.com/story/news/nation/2021/02/08/florida-water-treatment-hack-lye/115453008/

United States Agency for International Development. (2022). *Technological innovations for rural water supply in low-resource settings*. https://www.globalwaters.org/sites/default/files/4dec_technological_innovations.pdf

U.S. Department of Energy. (2021). *Spotlight: Advancing cybersecurity to strengthen the modern grid*. https://www.energy.gov/sites/default/files/2021/01/f82/OTT-Spotlight-on-Cybersecurity-final-01-21.pdf

U.S. Department of Homeland Security. (2022, September 16). *Biden-Harris administration announces $1 billion in funding for first-ever state and local cybersecurity grant program*. https://www.dhs.gov/news/2022/09/16/biden-harris-administration-announces-1-billion-funding-first-ever-state-and-local

U.S. Department of Transportation. (2017, June 29). *Smart city challenge*. https://www.transportation.gov/smartcity

Water Sector Coordinating Council. (2021). *Water and wastewater systems: Cybersecurity 2021 state of the sector*. https://www.waterisac.org/system/files/articles/FINAL_2021_WaterSectorCoordinatingCouncil_Cybersecurity_State_of_the_Industry-17-JUN-2021.pdf

Wilkie, C. (2021, June 9). *Colonial Pipeline paid $5 million ransom one day after cyberattack, CEO tells Senate.* CNBC. https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html

ABOUT THE AUTHOR

David Dunmoyer is the campaign director for Better Tech for Tomorrow at the Texas Public Policy Foundation. In this role, he publishes research and commentary, provides expert testimony, and advocates for responsible technology policy in the Texas legislature. His portfolio includes data privacy, cybersecurity, kids' online safety, AI, broadband, and other emerging technology issues. Prior to this role, he served as Chief of Staff to the executive team at TPPF after spending several years working in public affairs and digital marketing. David received undergraduate degrees at Texas Christian University and graduated with a Master of Public Affairs from the University of Texas at Austin's LBJ School of Public Affairs.

Texas Public
POLICY FOUNDATION

901 Congress Avenue | Austin, Texas 78701 | (512) 472-2700 | www.TexasPolicy.com