Texas Public POLICY FOUNDATION

TESTIMONY BEFORE THE HOUSE SELECT COMMITTEE ON SECURING TEXAS FROM HOSTILE FOREIGN ORGANIZATIONS

BY **David Dunmoyer,** Texas Public Policy Foundation
SEPTEMBER 10, 2024

Dear Chair Hefner and Committee Members:

My name is David Dunmoyer, and I am the campaign director for Better Tech for Tomorrow, an initiative of the Texas Public Policy Foundation. I am grateful for the opportunity to testify before you today and to submit this written testimony.

This committee's work, and today's topic in particular, is critically important to ensuring privacy, safety, security, economic stability, and human flourishing in Texas. Hostile foreign entities present grave threats to Texas' economy, security, intellectual property, critical infrastructure, values, and way of life. These threats are more pronounced and scalable with the increased digitalization of our economy and society. For example, recent cyberattacks 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. Furthermore, the explosion in artificial intelligence makes this challenge even more difficult. Unfortunately, the history of public policy for critical infrastructure cybersecurity is punctuated by a reactionary, fragmented system of governance.

This testimony will frame the problem, survey the challenges posed to critical infrastructure in the age of digitalization and artificial intelligence (AI), highlight state and federal responses, and, ultimately, provide concrete policy recommendations to help Texas meet these challenges and be a national leader on critical infrastructure cybersecurity.

THE CHALLENGES POSED TO CRITICAL INFRASTRUCTURE IN THE AGE OF DIGITALIZATION

The realm of critical infrastructure presents tremendous opportunities and threats in the age of digitalization and the application of emerging technologies such as AI. As noted by the Cybersecurity and Infrastructure Security Agency (CISA), there are 16 infrastructure sectors that our economic security, public health and safety, and national security are so dependent on as to be deemed critical. These sectors include communications, emergency services, financial services, energy, water and wastewater systems, nuclear, and more (CISA, n.d.). And while these critical infrastructure subsets have existed for decades, the digital transformation taking place is a newer phenomenon. In fact, only in the last decade

continued

have operators of critical infrastructure needed to worry about rogue state-sponsored actors and terrorists digitally infiltrating their systems. There are myriad catalysts for this, ranging from urban regions of the country digitalizing public services in pursuit of becoming a "smart city," to the increased desire of employees to remotely access critical infrastructure systems hastened by the post-COVID-19 world of remote work (Tufts, 2023). Prior to this push for digitalization, much of the critical infrastructure ecosystem was air gapped—meaning it was not all centrally connected through the internet (Tufts, 2023). Thus, the consequence of rapidly digitalizing our critical infrastructure without commensurate investments in cybersecurity has introduced a gaping vector for cyberterrorists and nefarious actors to exploit. As noted by the Department of Homeland Security (DHS) (n.d.):

> [n]ation-states and their proxies, transactional criminal organizations, and cyber criminals use sophisticated and malicious tactics to undermine critical infrastructure, steal intellectual property and innovation, engage in espionage, and threaten our democratic institutions. … As innovation, hyper-connectivity, and digital dependencies all outpace cybersecurity defenses, the warning signs are all present for a potential "cyber 9/11" on the horizon. (para. 2)

Recent surveys and the data demonstrate the marked jump in cybersecurity attacks on American critical infrastructure in the last few years. Initially, of the 2,825 ransomware attacks that organizations reported to the Federal Bureau of Investigation in 2023, more than 40% afflicted critical infrastructure organizations—an increase over the one-third of attacks impacting critical infrastructure sectors in 2022 (Kapko, 2024; FBI, 2023, p. 13). And it is a fair assumption that these reports are only the tip of the iceberg, as the FBI noted from its successful 2023 infiltration of a well-known ransomware group's infrastructure that only 20% of its victims reported attacks to law enforcement. These attacks are overwhelmingly perpetrated by rogue nations, with nearly 60% of critical infrastructure cyberattacks led by state-affiliated actors (Security Magazine, 2023). The types of attacks being deployed by cybercriminals have severe implications for the application of AI in critical infrastructure. As revealed by 2022 assessments, valid accounts represent 54% of successful attempts to hack into critical infrastructure.[1] The second most common attack method was spearphishing, with these attacks being successful 33% of the time (CISA & USCG, 2023).[2]

Foreign adversaries are increasing the frequency and sophistication of their cyberattacks against our critical infrastructure. In conjunction with the overall increase in number of attacks, the share of attacks coming from foreign adversaries is growing: per 2023 data, 60% of CI cyberattacks came from state-affiliated actors, namely China, Russia, North Korea, and Iran (Security Magazine, 2023). For example, nation-states are targeting critical infrastructure to collect information, gain access to industrial control systems, conduct espionage, steal intellectual property, and establish a foundation for future offensive operations. The increased frequency is attributed to a number of concerning trends. First, the increase in victims of ransomware attacks that end up paying the ransom to cyber terrorists. Second, the rise of AI and its enablement of cybercrimes. Third, cyberterrorism training: foreign actors are attacking rural ISDs, water providers, and the like, not just for immediate damage. They are assessing weak points and leveraging gaps in defenses to refine their tactics.

---

1 Valid accounts refer to former employee accounts that were never fully removed by the organization after the termination of an employee, or simply default administrator accounts that were never equipped with needed cybersecurity safeguards.

2 Spearphishing is a form of social engineering whereby threat actors pose as a boss, colleague, client, or associated organization, duping a victim into providing sensitive information or network access through digital communications.

For example, a recent Texas story highlights this growing concern of foreign nations digitally invading our critical infrastructure. On January 18, 2024, officials in Muleshoe, Texas, received notice that a water tower of theirs was overflowing, losing tens of thousands of gallons of water. Thankfully, Muleshoe was able to unplug its systems and resume operations remotely. The next day, they received a call from CISA, asking if their water system had been attacked, as they received reports indicating their systems may have been breached. Indeed, a cyberattack was levied by Russian cyberterrorists. CyberArmy posted videos on the dark web laying claim to these attacks on behalf of Russia. They used a remote login system to hack into the Supervisory Control and Data Acquisition (SCADA) system, which is a network that allows operators to remotely monitor and control water infrastructure.

This was one of at least three Texas cities that were attacked (Miller, 2024). Another Texas town, Hale Center, was hit with approximately 37,000 attempts to infiltrate the city's firewall. These types of attacks should be seen as a pre-positioning: it was Russia flaunting its strength and capabilities for disrupting Texas' critical infrastructure. While the water supply was not poisoned in Muleshoe or the other Texas cities, we can't yet see the full extent of the damage done, as Russia may have gleaned valuable insight on vulnerabilities and refined its TTPs (Tactics, Techniques, and Procedures) for subsequent attacks. Naturally, this attack rattled the community. The city responded by changing all the default passwords to stronger, unique passwords and implemented multi-factor authentication (MFA) for access to the OT network. Nevertheless, more needs to be done to counter this persistent and potentially fatal threat.

THE CHALLENGES POSED TO CRITICAL INFRASTRUCTURE IN THE AGE OF AI

The threats posed to cybersecurity in the age of digitalization are only magnified by the use and scale of AI.

For example, Reuters notes that "worries mount that U.S. adversaries could use the [AI] models, which mine vast amounts of text and images to summarize information and generate content, to wage aggressive cyber attacks or even create potent biological weapons" (Reuters, 2024, para. 3). Furthermore, according to the DHS Homeland Threat Assessment 2024, "cyber actors use AI to develop new tools and accesses that allow them to compromise more victims and enable larger-scale, faster, efficient, and more evasive cyber attacks" (DHS, 2023, p. v). For example, these threats, from hostile nation-states, terrorists, and other non-state actors, are driven by "AI-developed malware and AI-assisted software development—technologies that have the potential to enable larger scale, faster, efficient, and more evasive cyber attacks—against targets, including pipelines, railways, and other U.S. critical infrastructure" (DHS, 2023, p. 18).

Given the stark realities America is currently facing with the ability of rogue actors to hack into a water treatment system and poison a city's water supply, AI can be deployed as a tool to worsen an already bleak situation. For cyber attackers, three ingredients are always present in a successful attack: capability, motivation, and opportunity. Opportunity has already been addressed, as evinced by the increasing opportunities to infiltrate critical systems due to the digitalization of critical infrastructure. As for motivation, most attacks are motivated by money, but there is a growing share of attacks stemming from political motivation, with nation-states, terrorists, and other rogue actors wreaking havoc and straining systems as part of escalating conflict. Finally, attackers need to possess the capability. Without proper guardrails, generative artificial intelligence (GAI) introduces tremendously accessible new tools for sophisticated and non-sophisticated attackers alike to hit their victims with greater frequency, precision, and disruption.

Professor Drew Hamilton of the Texas A&M Cybersecurity Center testified before the Texas House Select Committee on Artificial Intelligence & Emerging Technology and outlined numerous use cases for AI supporting cyber offense. These uses include adver-

sarial machine learning, automated exploitation and vulnerability discovery, AI-enhanced social engineering, deepfake detection and attribution evasion, AI-driven cyber-physical attacks, AI-enabled malware analysis and evasion, AI-powered botnet resilience, and more (House Committee on Artificial Intelligence & Emerging Technologies, 2024, p. 41). This list is certainly not exhaustive but illustrates a continued threat and trend of cybersecurity for critical infrastructure: attackers are remarkably adaptive to new technologies and increase their success rates year-over-year because they are highly motivated to stay ahead of cyber defense systems.

To illustrate how lucrative a tool AI can be for cyber attackers, take spearphishing, the second most common attack method for the critical infrastructure sector. Like most attackers, spearphishers seek to obtain sensitive information or system access to a specific organization. These attackers will target a particular individual, using digital forms of communication like email to dupe them into thinking the attacker is a trusted ally. This is accomplished through what is called social engineering, where the attacker uses information specific to the victim or the victim's organization to convince them that they are credible, and that urgent action is necessary. That "urgent action" tends to be directing the victim to open a malicious attachment or link that compromises the security of the host. AI can assist this process in numerous ways. Initially, as previously mentioned, the majority of cybersecurity attacks come from foreign actors where English may be a second language. GAI can dramatically speed up the process of foreign actors translating spearphishing emails into different languages, while simultaneously increasing the accuracy over human translators. Furthermore, it is a common technique for spearphishers to pose as a friend of the victim. GAI can be trained on the voice of specific persons through social media posts and other public information, allowing the attacker to craft an email that is in the voice and style of the person they purport to be. Finally, one of the greatest barriers to entry for spearphishing attacks is the amount of time it can take to draft attack emails. With minimal prompt engineering, unsophisticated actors can use GAI products like ChatGPT and Gemini to rapidly churn out socially engineered emails specific to the victim, their organization, and what will motivate them to act on clicking a malicious link.

Deepfakes also introduce pressing concerns for cybersecurity broadly that scammers are wielding with great effect. For example, in early 2024, an employee at a multinational corporation was contacted by a scammer posing as the chief financial officer. The purported "CFO" asked to set up a video call to discuss the need for a secretive transaction. While the employee was dubious, he agreed to the call and almost immediately had his concerns assuaged. Not only was the voice, cadence, physical depiction, and intonation of the "CFO" a near perfect replica, but the scammers incorporated deepfake video and audio of other employees onto the video call, affirming the "realness" of the situation by having the employee's peers go along with the "CFO's" request. Consequently, the employee remitted a total of $25.6 million, falling prey to the perpetrators deception (Chen & Magramo, 2024).

Scores of similar stories have recently emerged, and stateside, Americans lost $2.6 billion in imposter scams in 2022 (Karimi, 2023). Given all a threat actor needs are a minute or two of a person's voice and a no- or low-cost subscription to an audio cloning service, it is a real possibility that nefarious actors can use AI-powered cloning technologies to finagle their way into gaining access to critical infrastructure systems.

USING AI AS A PROACTIVE AND REACTIVE TOOL IN CYBERSECURITY FOR CRITICAL INFRASTRUCTURE

Pursuant to Executive Order 14110 (2023), the Department of Homeland Security published its initial "Guidelines and Report to Secure Critical Infrastructure and Weapons of Mass Destruction from AI-Related Threats" in April 2024. While it is devoid of much substance, DHS articulated a key threat vector: new cybersecurity vulnerabilities stemming

from AI design and implementation in critical infrastructure systems. Given the historic mismatch between enhanced digitalization and cybersecurity improvements in critical infrastructure, this point bears repeating. DHS (2024) warns of "[d]eficiencies or inadequacies in the planning, structure, implementation, or execution of an AI tool or system leading to malfunctions or other unintended consequences that affect critical infrastructure operations" ("Guidelines to Mitigate AI Risks to Critical Infrastructure" section). These guidelines emphasize that critical infrastructure and cybersecurity policy should reflect not only a response to existing threats, but aid in proactively defending our most precious systems from threats posed by AI.

While cyber attackers are quickly adding AI tools to their toolkit, there are also promising applications for the defense of our most critical infrastructure. One major application in the space of nuclear energy and technology is with video surveillance. The International Atomic Energy Agency (IAEA) operates more than 1,300 surveillance cameras across the world, running 365 days-per-year to provide continuity of knowledge for nuclear material monitoring and for verification that no unauthorized access is given to specific materials or locations in a facility. Each nuclear site tends to have multiple cameras, and it has historically been incumbent upon inspectors to monitor and review these huge swaths of camera data. This is an important task, but one that is prone to human error and is highly time consuming. IAEA notes that "AI provides the basis for the next generation of surveillance review software that allows for the efficient analysis of these data. … AI and ML can strengthen the collection, integration, and analysis of multiple information sources (Wagman & Nicula-Golovei, 2022, "Artificial Intelligence and Machine Learning" section). Another closely related example for the water sector would be utilizing AI to monitor the treatment of water. AI systems could flag enigmatic readings—more lye than desired, for example—before chemicals are mixed into water and certainly well before a toxic supply of water is administered to a customer base. This AI-enhanced safeguard strategy can be applied across the critical infrastructure spectrum.

In addition to AI tools fostering more proactivity in cyber defenses, there are promising applications for reactive measures as well. While cybersecurity attacks make headlines when outages or document leaks ensue, the reality is that infiltration of a critical system and palpable damages are two different metrics. According to Yehoshua (2023), data breaches take on average 322 days for an organization to detect and contain them. For example, it was recently revealed that amidst a hacking campaign launched by the Chinese to infiltrate transportation hubs and critical American infrastructure, the cybercriminals had successfully maintained access to their victim's networks for "at least five years" (Lyngaas, 2024, para. 1). Considering such harrowing examples, there is great promise to utilizing AI for pattern detection to more quickly ascertain whether data has been compromised by ransomware or similar cyberattacks. For example, machine learning and data analytics can be employed to monitor network traffic to identify unusual patterns or anomalies that are often unseen by the human eye, recognizing signs of hacking and malware infections amidst gargantuan sums of data. Early applications of such AI-supported security tools have already reduced data breach detection and containment from 322 days to 214 days—a significant improvement when considering the daily costs of system outages and breaches of personal information (Yehoshua, 2023).

AI-powered tools can also enable faster recovery times for all sectors post-cyberattack. Consider that nearly half of the victims of ransomware attacks pay cyberterrorists the demanded ransom (Blinder & Perlroth, 2018). While there are many factors contributing to this, a big motivating factor is the time it takes for system operators to bring their systems back online. For Independent School Districts or critical infrastructure systems, some opt to pay because they cannot bear the cost of extended system outages—both monetarily and in providing essential services. AI-powered systems can give

decision-makers better visibility into the minutiae of the compromise, providing valuable, actionable information on how to manage the crisis. In addition to assessing the scope of the damage, such AI-powered systems can automate a significant portion of recovery management, shifting the anachronistic "reactive" response model into one that is much more adaptive (Bovbjerg, 2023). For rural critical infrastructure system providers in particular, tools like this on a limited budget can make a dramatic difference in their cybersecurity preparedness and response.

POLICY RECOMMENDATIONS

Ultimately, 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 policy recommendations that the 89th Texas Legislature should strongly consider adopting to protect our most critical resources.

First, create requisite statewide cybersecurity standards under a centralized entity such as the Texas Department of Information Resources (DIR). For example, the Texas DIR cybersecurity standards and best practices that are currently voluntarily imposed on water infrastructure should 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, make prudent investments in Career and Technical Education (CTE). 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. 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.), despite the fact that there is an expected 35% growth rate in Texas' cybersecurity industry over the next decade (Texas Comptroller, n.d.). The Texas Legislature should invest in comprehensive IT Career and Technical Education opportunities. For example, Texas could develop a policy that better aligns the incentives of CTE funding with outcomes, so that programs throughout the state are incentivized to provide more IT programs that can generate high-paying jobs for graduates.

Third, require that each water district in Texas have a qualified cybersecurity manager, or at least one manager for a region of small towns or counties. Each water district or region would designate one full-time employee (FTE) as the manager of DIR-issued cybersecurity standards. These managers would be required to complete additional cybersecurity training 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.

Fourth, increase cybersecurity training and educational opportunities for water districts in Texas. 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). While DIR currently requires an annual statewide cybersecurity awareness training for employees at all government entities, the frequency of dedicated training for employees at a critical infrastructure facility should be conducted quarterly.

Fifth, conduct regular critical water infrastructure cybersecurity audits. Each water district, under the leadership of its cybersecurity manager, should be required to conduct a cybersecurity audit twice annually. This would accomplish several important goals, including transparency, accountability, statewide datasets, and more. Ultimately, 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.

Sixth, ensure procured technology comes equipped with the strongest cybersecurity options. Unfortunately, many cybersecurity incidents across America are caused by government bodies working with vendors that employ weak security controls (Keating, 2022). Accordingly, 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.

Seventh, create a grant program or financing mechanism for broader cybersecurity improvements. Indeed, costs have been the barrier to substantive change to cybersecurity. While there is no easy way to estimate the cost of cybersecurity unpreparedness for Texas' water infrastructure, it is important for lawmakers to 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. A revolving loan fund model is ideal, through which low- or no-interest loans could 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.

Finally, the Legislature must consider the impact of AI and other emerging technologies in critical infrastructure.[3] TPPF has heavily engaged in these conversations through interim testimony, forthcoming research, published articles, events, and numerous video and audio products. Ultimately, the Foundation argues that industry and legislators must balance technological innovation with utmost respect for human dignity, privacy, transparency, and accountability. Light-touch, values-driven, state-based, legislative guardrails for AI, built upon a risk-based framework, are necessary to propel humanity forward.

CONCLUSION

Thank you, again, for the opportunity to testify. The Foundation looks forward to working with the chair, this committee, and the rest your colleagues to ensure robust protections for critical infrastructure are in place. Moreover, the Foundation is eager to assist with the broader charge of this crucially important select committee wherever our research might be valuable.

David Dunmoyer
Campaign Director
ddunmoyer@texaspolicy.com

The Honorable Zach Whiting
Senior Fellow and Policy Director
zwhiting@texaspolicy.com

Better Tech for Tomorrow
Texas Public Policy Foundation

3 Indeed, there are numerous committees, councils, and stakeholder working groups studying AI in the lead up to the 2025 session, including the AI Advisory Council pursuant to HB 2060 (2023), House Select Committee on Artificial Intelligence & Emerging Technologies, Senate interim charges in three committees, and several AI stakeholder groups. The work of these groups will produce not only a comprehensive AI bill but also several targeted AI bills, underscoring the thoughtful process through which Texas lawmakers will act.

REFERENCES

Blinder, A. & Perlroth, N. (2018, March 29). Hard choice for cities under cyberattack: Whether to pay ransom. *The New York Times*. https://www.nytimes.com/2018/03/29/us/atlanta-cyberattack-ransom.html

Bovbjerg, M. (2023, May 24). *How AI can help organizations adapt and recover from cyberattacks*. Dark Reading. https://www.darkreading.com/cyber-risk/how-ai-can-help-organizations-adapt-and-recover-from-cyberattacks

Chen, H. & Magramo, K. (2024, February 4). *Finance worker pays out $25 million after video call with deepfake 'chief financial officer'*. CNN. https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html

CISA & USCG. (2023). *CISA analysis: Fiscal year 2022 risk and vulnerability assessments*. https://www.cisa.gov/sites/default/files/2023-07/FY22-RVA-Analysis%20-%20Final_508c.pdf

CISA. (n.d.). *Critical infrastructure sectors*. Retrieved August 26, 2024, from https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

CyberSeek. (n.d.). *Cybersecurity supply/demand heat map*. Retrieved August 26, 2024, from https://www.cyberseek.org/heatmap.html

DHS. (2024, April 29). *DHS publishes guidelines and report to secure critical infrastructure and weapons of mass destruction from AI-related threats*. https://www.dhs.gov/news/2024/04/29/dhs-publishes-guidelines-and-report-secure-critical-infrastructure-and-weapons-mass

DHS. (2023). *Homeland threat assessment 2024*. https://www.dhs.gov/sites/default/files/2023-09/23_0913_ia_23-333-ia_u_homeland-threat-assessment-2024_508C_V6_13Sep23.pdf

DHS. (n.d.). *Secure cyberspace and critical infrastructure*. Retrieved August 26, 2024, from https://www.dhs.gov/secure-cyberspace-and-critical-infrastructure

Exec. Order No. 14110, 88 Fed. Reg. 75191 (2023, November 1). https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence

FBI. (2023). *2023 Internet crime report*. https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

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/

HB 2060. Enrolled. 88th Texas Legislature. Regular. (2023). https://capitol.texas.gov/tlodocs/88R/billtext/pdf/HB02060F.pdf

House Committee on Artificial Intelligence & Emerging Technologies, Select. (2024). *Interim report to the eighty-ninth Texas Legislature*. Texas House of Representatives. https://www.house.texas.gov/pdfs/committees/reports/interim/88interim/House-Select-Committee-on-Artificial-Intelligence-Emerging-Technologies.pdf

Kapko, M. (2024, March 11). *Ransomware attacks are hitting critical infrastructure more often, FBI says*. Cybersecurity Dive. https://www.cybersecuritydive.com/news/ransomware-hitting-critical-infrastructure-fbi/709814/

Karimi, F. (2023, April 29). *'Mom, these bad men have me': She believes scammers cloned her daughter's voice in a fake kidnapping*. CNN. https://www.cnn.com/2023/04/29/us/ai-scam-calls-kidnapping-cec/index.html

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/

Lyngaas, S. (2024, February 7). *Chinese hackers have lurked in some US infrastructure systems for 'at least five years'*. CNN. https://www.cnn.com/2024/02/07/politics/china-hacking-us-agencies-report/index.html

Miller, K. (2024, April 19). *Rural Texas towns report cyberattacks that caused one water system to overflow*. The Texas Tribune. https://www.texastribune.org/2024/04/19/texas-cyberattacks-russia/

Reuters. (2024, May 9). *US lawmakers unveil bill to make it easier to restrict exports of AI models*. https://www.reuters.com/technology/us-lawmakers-unveil-bill-make-it-easier-restrict-exports-ai-models-2024-05-10/

Security Magazine. (2023, September 19). *Energy sector faces 39% of critical infrastructure attacks*. https://www.securitymagazine.com/articles/99915-energy-sector-faces-39-of-critical-infrastructure-attacks

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 August 26, 2024, from https://comptroller.texas.gov/economy/economic-data/cybersecurity/texas.php

Tufts, S. (2023, July 6). *Critical infrastructure attacks are ramping up*. Security. https://www.securitymagazine.com/articles/99597-critical-infrastructure-attacks-are-ramping-up

Wagman, J. & Nicula-Golovei, T. (2022). The evolution of safeguards technology. *IAEA Bulletin 63*(3). https://www.iaea.org/bulletin/the-evolution-of-safeguards-technology

Yehoshua, R. (2023, August 14). *Why detection and response technology won't solve all ransomware attacks*. SC Magazine. https://www.scmagazine.com/perspective/why-detection-and-response-technology-wont-solve-all-ransomware-attacks

ABOUT THE AUTHORS

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.

The Honorable Zach Whiting is Policy Director and Senior Fellow for Better Tech for Tomorrow at the Texas Public Policy Foundation.

Prior to joining the Foundation, he served as a state senator in his native state of Iowa. He served as Assistant Majority Leader, chair of the Labor and Business Relations Committee, and vice chair of the Administrative Rules Review Committee. Prior to the senate, Zach worked as a Legislative Assistant and Policy Advisor to a member of Congress. He graduated summa cum laude with a B.A. in political science from Stetson University and earned a J.D. from the Regent University School of Law.

Texas Public
POLICY FOUNDATION

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