CENTER FOR
CYBERSECURITY
POLICY AND LAW

WHITEPAPER

BUILDING TEXAS CYBER RESILIENCE

Turning Policy into Operational Capability

JULY 2026
Version 2.07.28.26

Cover photo: Texas State Capitol by LoneStarMike (CC BY 2.0); cyber overlay added

Building Texas Cyber Resilience

> *At a recent convening at the University of Texas at Austin's Strauss Center, state and municipal leaders, higher education institutions, cybersecurity practitioners, and the Texas Cyber Command (TXCC) gathered around a shared challenge. Texas understands cyber risk. The open question is how to convert that awareness into statewide capability.*

For years, cybersecurity policy has emphasized executive awareness, user education, and public warnings. Those efforts remain important, but they no longer suffice on their own. Small and midsized cities, counties, school districts, colleges, and public utilities take cybersecurity seriously. They struggle because they must defend increasingly complex environments without the staffing, tools, or response structures that mature security programs require.

Created through House Bill 150 and passed by the 89th Texas Legislature, the TXCC is positioned to help close that gap. Its mission is to prevent and respond to cyberattacks against the public and private entities Texans depend on, drawing on the expertise and resources of state, local, and federal partners. The event, described by its hosts as a “collaboration from academia, the private sector, and the public sector to work on how we better build cyber resilience across the state of Texas,” examined how the command can become more than a signal of priority. Speakers agreed that resilience cannot depend on every entity building a mature program in isolation. The state's opportunity lies in shared capacity: workforce development, threat visibility, incident response coordination, shared services, and the trusted relationships that hold all of it together.

Cybersecurity Is a Leadership Problem, Not Just an IT Problem

Speakers repeatedly framed cybersecurity as a matter of community leadership, operations, and public safety rather than a narrow technical discipline. “Cybersecurity is a team activity. It takes all of us to do this,” said Bart Lauwers, Deputy Chief of the TXCC. Incidents reach well beyond servers and networks. They can disrupt emergency response and erode trust in local institutions such as schools.

Demetra Koelling, General Counsel for ON2IT Cybersecurity and a co-host of the event, observed that “none of your [organizations'] main goals will happen if you get breached.” The most effective organizations have stopped treating cyber as an IT function and begun treating it as a resilience function. Deron McElroy, with the Alamo ISSA, offered the executive framing: “I would want the leaders of Texas to understand that cybersecurity is not primarily a technical domain. It's a risk management domain. You're managing risk to your organization.”

The framing has budget consequences. Treated as a technical problem, cybersecurity gets delegated downward in staffing and funding. Treated as risk management, it becomes part of executive budgeting, workforce planning, and senior accountability. A breach at a large agency draws headlines, but an incident at a school district, small city, or utility can disrupt daily life just as severely.

Uvalde Consolidated Independent School District offers a recent example. In September 2025, the district closed campuses for several days after ransomware disrupted phones, air-conditioning controls, security camera monitoring, visitor management, and payroll. School safety operations were

affected, and bus drivers, maintenance staff, and custodians faced the prospect of delayed paychecks. As Jeremy Carter of the UT Austin Regional Security Operations Center put it, cybersecurity "encompasses everyone, [it is] not just the IT folks that are responsible. It's the everyday, average citizen that needs to be aware of cybersecurity risks."

A Capability Gap, Not an Awareness Gap

Most Texas public entities already know that ransomware, phishing, and data breaches can cause serious harm. Knowing what should be done is different from having the ability to do it consistently. Leaders need expertise, funding, and a clear support pathway before an incident occurs, not only after. The problem is most acute for small and midsized entities that deliver critical services, hold sensitive data, and run aging systems with small IT teams and little or no dedicated security staff.

The consequences become tangible when an event reaches essential services. In January 2024, cyberattacks against rural towns in the Texas Panhandle were linked to a Russian hacktivist group. Officials said the attackers caused Muleshoe's water system to overflow before local staff shut it down and ran it manually. The public was never endangered, but the episode shows how quickly a network intrusion can cross into physical infrastructure in a small community.

Smaller entities are attacked precisely because limited resources, aging systems, and operationally important services make them both vulnerable and valuable, particularly when they serve as dependencies for larger targets like power and water facilities. "In this day, where small entities are targeted... it's really important for communication to be primary," Koelling said. Nor can technology alone close the gap. Lauwers cautioned that "technologies like endpoint detection and response are really good, but unfortunately there's no such thing as a silver bullet, and there is not a technology you can deploy that will make you safe from any threat actors."

Part of the answer is simply connecting entities to help that already exists. "There are a lot of resources that the state has that are either unknown or unavailable because somebody is just unaware," Koelling noted. Shane McDaniel, CIO for the City of Seguin, described the new command as a "one stop shop," a way for the state to gather available resources and communicate them to entities so they know how to use them, which he called "invaluable." The state need not replace every local capability. It can clarify support pathways and give each entity access to capabilities it could never build alone, which is the premise of the TXCC itself. Public descriptions of the command's planned functions point to cyber threat intelligence, incident response, digital forensics, and coordination as core elements. The open question is how those functions reach the organizations with the greatest need.

The Rise of Shared Cyber Defense

The strongest path forward for Texas is a shared cyber defense ecosystem rather than any single tool or program.

Texas Cyber Command The TXCC can coordinate statewide priorities, threat intelligence, incident response, and resource visibility.	**Regional Security Operations Centers** Regional Security Operations Centers (RSOCs) extend operational services and security monitoring to public entities across the state.
Universities and community colleges Universities and community colleges train students, support clinics, and build workforce pathways.	**Private-sector partners** Private-sector partners contribute technical expertise and operational experience.

Convenings such as the one at UT Austin are themselves part of the model, building trust before a crisis arrives.

Francesca Lockhart, Assistant Director of the Strauss Center, described the missing element today, "we lack some of that connective tissue around bringing in academia and rethinking bringing in private sector partners, and ensuring that the right information and the right intelligence is getting into the right hands." Shared defense, in this view, is less a roster of organizations than a means of moving information, expertise, and support to where they reduce risk. Carter framed the RSOC role in practical terms, stressing the importance of communicating "the metrics, the services that we provide to various public entities across the state."

Speakers identified concrete support areas for smaller entities, including:

- Shared SOC services
- Vulnerability scanning
- Incident response assistance
- Training
- Threat-feed consolidation
- Vendor assessment
- Standards for service providers

> *"A huge difference could and will be made through the Texas Cyber Command standing up their cyber threat intelligence sharing center and apparatus, and expanding upon some of those information sharing efforts that are already ongoing. Getting those right partners into that communication and into that fold," is a huge role for groups like the Strauss Center, said Lockhart.*

Coordination Requires Trust as Much as Technology

Speakers returned again and again to coordination, communication, and trust. Who do you call during an incident? Who is responsible for what? How do local, state, federal, academic, and private partners operate together under pressure? "Every leader in the state of Texas needs to understand that

coordination is going to be key," said Robert Glover of Houston Community College, adding that when incidents happen, "that information has got to be passed."

Texas has already proven the value of coordinated response to cyber catastrophes. In August 2019, more than 20 Texas entities, most of them smaller local governments, reported ransomware attacks in a statewide, multi-jurisdictional incident. The Texas Department of Information Resources led the response, the State Operations Center was activated, and state, federal, and academic partners were brought in. Within a week, every affected entity had moved from response and assessment to remediation and recovery, with business-critical services restored. A later DIR submission described it as the largest coordinated ransomware attack against local government in U.S. history at the time, crediting statewide preparation and cooperation for the outcome.

The lesson is that cyber response needs the clarity leaders expect in physical emergencies. When roles, escalation paths, and relationships are defined in advance, support moves quickly. When they are not, local entities lose critical time determining whom to call and what to share. Francisco Sanchez of the University of Houston connected cyber response to emergency management, arguing that it should not be "just focused on the world of ones and zeroes" but should include "the incident command structure, the response and the consequence management." A cyber incident is a potential operational crisis involving public communications, legal decisions, insurance, vendors, and affected residents. Relationships built only on the day of the incident will slow the response.

AI Raises the Stakes for Human Capability

AI featured prominently, particularly in the higher education panel, where it is reshaping both the threat landscape and the workforce conversation. Attackers and defenders alike are accelerating their existing integration of the technology into their workflows. AI can help defenders move faster by summarizing data, assisting analysts, and supporting triage, but it can also create false confidence, amplify low-quality work, and let attackers scale their operations. Elizabeth McGee of Houston City College presented the people-centered view of the challenge with AI, "We need to invest in the awareness, the training, and education, so that we can combat the threat together."

The relevant question is whether an organization's people have the fluency to use AI responsibly and the judgment to evaluate its output. The fundamentals of cyber defense still matter, from phishing resistance and identity security to patching, backups, and incident planning. The real test is whether organizations can execute them consistently as AI increases the speed and complexity of the environment. AI changes how cyber work is performed. It raises rather than reduces the value of people who combine technical fluency with sound judgment.

Workforce Development Is a Security Strategy

Cyber resilience is built with people as much as technology, and Texas has an opportunity to align its cybersecurity strategy with its education and workforce strategy. Lockhart emphasized higher education's role in "reaching into our colleges and universities like UT Austin to mentor and equip students with the skills that will make them competitive in the cybersecurity workforce." She also addressed a persistent myth head-on, saying, "You don't have to be a computer science major to be successful in cybersecurity." The field needs risk managers, policy thinkers, educators, investigators, and most importantly, leaders.

Glover connected workforce development to early career pathways, saying, “we have to have the methodologies and the systems in place to make those educational experiences and those workforce experiences valid for what we want to do, not only in Texas, but across the entire United States.” Applied learning, apprenticeships, clinics, community college pathways, and RSOC-based training all help students move from classroom knowledge to operational readiness. They also help local governments by expanding the pool of people who understand both cyber risk and public-sector realities. Viewed this way, workforce development is a security strategy in its own right.

From Convening to Action

One of the clearest lessons from the event was that trust must exist before an incident, not be improvised during one. A statewide resilience model cannot be built through memos, portals, or policies alone. It depends on local entities knowing who is involved, what support exists, what data may be shared, and how participation strengthens rather than erodes local authority. Convenings create space for that candid conversation before a crisis. Koelling noted that by partnering with institutions like the Strauss Center and the Center for Cybersecurity Policy and Law, conveners “become a help and support for conversations that are really important.”

Convening cannot be the end goal, however. McElroy warned against collaboration without outcomes, stressing the need to define what partners are trying to accomplish and then take concrete steps toward it. Carter echoed the point, calling for, “communication with a goal, like an end state” rather than “a meeting to have a meeting,” and for measures and lines of effort “so that they will follow through and follow up.” In practice, that means clearer incident response pathways, shared threat intelligence, training programs, and pilot deployments with local entities that establish what works before scaling statewide.

What Success Looks Like

A resilient Texas five years from now does not mean every incident is prevented. It means communities detect, respond, and recover faster. Threat intelligence moves quickly, smaller entities know where to turn, and local governments draw on shared resources. A school district does not have to interpret every alert without context and a community college student sees a clear pathway from education into public service.

There was confidence evident among the speakers that these goals could be achieved with the support of the TXCC. “I have confidence in the state of Texas in our cyber resiliency, because we are a state that does hard things. We take on challenges and we are an incredible actor on the world stage,” McGee said. Lauwers agreed, “I'm confident about the future of cybersecurity in the state of Texas because Texas is doing what is right. They're paying attention to it. They're prioritizing cybersecurity.” Sustaining that confidence through execution will be the test as the TXCC's priorities roll out over the next several years.

Texas has the ingredients for a national model that includes political leadership focus, academic involvement, private-sector expertise, regional operational capacity, and a sense of shared responsibility. The TXCC's long-term success depends on whether it closes the capability gap for the entities that need help most. Koelling suggested that a state-level cyber command prioritizing “communication, resource availability, and capacity building” could make one of the biggest impacts in the state. **Texas does not need more warnings. It needs practical capability, and if the state succeeds, its most important cybersecurity advantage may prove to be neither a tool nor a program, but the ability to connect people, institutions, and resources before the next crisis arrives.**