Strengthening Cyber Resilience Across Illinois Transit Agencies

Project 2562
December 2025

Scott Belcher, Terri Belcher, & Andy Souders

In 2025, the Mineta Transportation Institute released its most recent transit cybersecurity study on transit entitled *Does the Transit Industry Understand the Risk of Cybersecurity and are the Risks Being Appropriately Prioritized?*[1] (the 2025 MTI Study). The 2025 MTI study was a follow-up survey-based project to an earlier report MTI released in 2020.[2] Both studies concluded that many transit agencies lacked basic cybersecurity hygiene and that, without dedicated funding and a mandate, were unlikely to implement cybersecurity best practices. After the release of the 2025 MTI Study, MTI and the Federal Transit Administration (FTA) challenged the authors to identify an alternative approach to addressing the impediments to adoption.

Pilot Overview

The 2025 MTI study authors, with technical collaboration from Cybrbase, and early support from MTI, worked with the Illinois Department of Transportation (IDOT) to launch a Cyber Resilience Pilot (the Pilot) to bolster the cybersecurity posture of small, rural, and mid-sized transit agencies across Illinois. This innovative Pilot engaged IDOT and six of their partner transit agencies, focusing on a collaborative, group-based assessment model aligned with the U.S. Department of Homeland Security (DHS) Cyber Resilience Review (CRR) and the National Institute for Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0.[3] The participating agencies have completed one baseline cybersecurity assessment, facilitated by cybersecurity professionals, with follow-up assessments scheduled for November 2025. Despite the loss of external funding mid-project, the Pilot continued through personal investment, ensuring momentum was not lost and participating agencies could continue improving their cybersecurity preparedness.

Delivered Value to Date

- **Baseline Cybersecurity Assessments:** Through the Pilot, six transit agencies completed NIST CSF 2.0-based assessments, establishing a clear baseline of each agency's cybersecurity risks and maturity. Each agency's individual responses were kept confidential while the entire cohort participated in the discussion.

---

1. Mineta Transportation Institute, Does the Transit Industry Understand the Risk of Cybersecurity and are the Risks Being Appropriately Prioritized? https://transweb.sjsu.edu/research/2405-Transit-Industry-Cybersecurity-Risks, 2025.
2. Mineta Transportation Institute, Is the Transit industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness, https://transweb.sjsu.edu/research/1939-Transit-Industry-Cyber-Preparedness, 2020.
3. Illinois Department of Transportation and Cybrbase. "Illinois DOT and Cybrbase Launch Cost-Effective Cybersecurity Pilot." ITS International (online), accessed 2025. https://www.itsinternational.com/news/illinois-dot-and-cybrbase-collaborate-lower-cost-cybersecurity

- **Expert-Guided Action Plans:** Each agency received a tailored 90-day action plan to address critical gaps. These plans, developed and guided by cybersecurity experts, provided step-by-step guidance to enhance resilience in areas such as incident response, backup/recovery, and access control. Follow-up assessments are planned to measure progress against the identified gaps in November 2025.

- **Peer Collaboration Workshops:** The Pilot convened periodic workshops for agencies to share best practices, discuss challenges, and learn from each other's experiences. This peer learning approach accelerated the adoption of cybersecurity measures and drove consistency across agencies. For example, smaller agencies benefited from mentorship and policy templates shared by a mid-sized peers fostering a supportive community of practice.

- **Notable Outcomes:** The collaborative model delivered tangible improvements. One participating agency increased its cybersecurity insurance coverage from $1 million to $3 million for the same premium after going through the Pilot and addressing some low-hanging items. Across all agencies, cybersecurity awareness and executive attention to cybersecurity have measurably increased as evidenced by new policies and staff training initiatives. Each agency also established six core cybersecurity policies where none existed before.

Interim Findings – Vulnerabilities and Lessons Learned

Common Vulnerabilities: The initial assessments revealed a set of recurring cybersecurity weaknesses across the transit agencies:

- **Informal or Ad-hoc Risk Management:** Agencies lacked standardized processes to identify and analyze cybersecurity risks to critical services (e.g., dispatch, scheduling, payroll) and had not prioritized mitigating those risks.

- **Incident Response:** Agencies lacked formal incident response plans and communication protocols. Most agencies did not have a documented plan for how to handle a cybersecurity incident or how to notify stakeholders, which would severely hinder their response to a serious breach. Moreover, most agencies were unaware of their state and federal reporting obligations.

- **Service Continuity:** Agencies generally lacked formal business continuity and disaster recovery planning. Most had not documented or tested backup and restoration procedures for critical services whether those disruptions are caused by a cybersecurity event, a facilities issue (e.g., depot fire or power loss), operational workforce disruption, or an information technology (IT) outage.

- **Training and Awareness:** Agency staff had limited cybersecurity awareness. Phishing vulnerability was high because employees had not been regularly trained to recognize suspicious emails or follow basic cybersecurity hygiene practices.

> ***Phishing*** refers to deceptive emails or messages designed to trick a person into clicking a malicious link, opening an infected attachment, or providing credentials or sensitive information. This pattern is consistent with industry research across public sector agencies.[4]

- **Access Controls:** Agencies generally had weak controls for authentication and system access. Several agencies relied on shared accounts, and many did not have meaningful password policies, if any existed at all. User privileges were not consistently reviewed or updated, and access was not always revoked when staff left the agency. These practices significantly increase the risk of unauthorized access or insider threats.

Key Lessons Learned: Simply identifying operational and system vulnerabilities was not sufficient. How agencies respond is crucial:

- **Cybersecurity Assessments Alone Are Insufficient**: Without leadership commitment and dedicated resources – including personnel and funding, agencies will struggle to close the gaps identified. For a cybersecurity assessment to translate into real risk reduction, management must treat the findings as actionable tasks and allocate time, budget, and expertise to address them. In the Pilot, progress was uneven; agencies that had resources to address the gaps were able to make improvements while others simply did not have the bandwidth or budget. This aligns with broader transit industry findings that many agency leaders do not yet appreciate the cybersecurity risks they face or know how their teams are addressing them.[5]

> **Executive leadership and their Boards have a fiduciary responsibility** to be aware of their organization's cyber vulnerabilities and to ensure plans are in place to manage those risks.[6] Without high-level ownership, even well-documented vulnerabilities are likely to go unmitigated.

- **Leadership Engagement is Critical:** Perhaps most importantly, the Pilot reinforced that cybersecurity must be treated as an enterprise risk management issue, not merely an IT issue. Agency executives and board members need to actively champion cybersecurity initiatives. In the Pilot, when agency leadership was briefed on the stakes of a cybersecurity attack (e.g., the potential for service disruptions, ransom demand, public disclosure of customer of employee data, or safety incidents from a cybersecurity attack), they became more supportive of investing in protections, where that was possible. This finding echoes guidance from the Transportation Security Administration (TSA), FTA, trade associations, and MTI that transit agencies' top executives should designate a cybersecurity coordinator, establish an incident response plan, and conduct regular vulnerability assessments as

4. Abnormal.ai, "Threats in Transit: Cyberattacks Disrupting the Transportation Industry", accessed 2025. https://abnormal.ai/blog/transportation-industry-email-attack-trends
5. Progressive Railroading (2025). "Report: Transit industry unprepared for more cybersecurity threats." News article, May 14, 2025 – Summary of the 2025 MTI report, noting no significant improvement since 2020 and urging coordinated efforts.
6. Ibid., 2

part of basic governance.[7] Cybersecurity threats pose not only technical problems but also strategic, financial, and reputational risks. Leadership involvement is essential to ensure cybersecurity policies are documented, practiced, and kept up to date.[8] Agency leaders must also ensure compliance with any federal or state cybersecurity requirements (e.g., TSA's 2021 security directives for surface transportation) and confirm that the agency carries cybersecurity insurance or has the means to self-insure against the costs of recovering from a cyber incident event.[9] In short, executive and board engagement is a prerequisite for sustained cybersecurity resilience improvements at transit agencies.

- **Support and Coaching Drive Action:** Agencies benefited significantly from hands-on guidance in executing their 90-day action plans. The Pilot found value in providing a coordinating "coach" or facilitator who could check in regularly, answer questions, and help resolve obstacles. This kind of support helped agencies implement improvements (e.g., enabling multi-factor authentication or documenting and instituting regularly scheduled data backups) that they might not have tackled on their own. An important takeaway is that building cyber resilience in resource-constrained transit agencies often requires an external catalyst or ongoing mentorship – a cyber-resilience "quarterback," meaning a dedicated coordinator or guide – not just one-time recommendations.

- **Preparation Matters – Start with a Pre-Assessment and Policy Foundation:** Starting "cold" with the formal assessment created unnecessary frustration and artificially low scores. While facilitators worked diligently to interpret the industry-agnostic Cyber Resilience Review (CRR) in transit-specific terms, many agencies lacked even a baseline understanding of cyber resilience or any documented cybersecurity policies. Several participants commented that having a brief pre-assessment survey and access to basic policy and plan templates would have made them far better prepared for the full review. This feedback led to a refinement of the model: beginning with a simplified pre-assessment, followed by a focused policies-and-procedures workshop to help agencies establish foundational artifacts before conducting the comprehensive assessment.

> *"Starting with the policies and risk management workshop will really help the agencies feel more prepared and confident, instead of feeling weighed down by so many low-scoring areas."* — Greg Meldrum, Systems Administrator, QC METROLINK, Cohort Participant

- **Collaboration Strengthens Resilience:** The group-based, in-person assessment sessions sparked meaningful discussion and peer learning. By comparing results, sharing implementation progress, and talking through challenges in real time, agencies built confidence and a shared sense of purpose. Because transit agencies do not compete, the environment encouraged openness and collaboration, allowing participants to align on policy templates, training approaches, and even shared solutions. The result was stronger engagement, faster progress, and a collective step forward in building cybersecurity resilience across the transit community.

7. Ibid.
8. Ibid.
9. Ibid.

> A "stronger-together" approach is especially effective for smaller transit agencies, a point underscored by MTI's finding that smaller operators continue to lag far behind larger peers in cybersecurity readiness.[10] This aligns with a broader principle articulated by MIT Sloan: "Cyber should be seen as a noncompetitive domain where organizations, even those in the same industry, work together to achieve greater levels of resilience…"[11]

National Context and Comparative Approaches

Transit agencies in Illinois are not alone in facing these challenges. Other states have begun pursuing statewide or "whole-of-state" cybersecurity Pilots that offer support to local governments and transit operators, providing useful models and context for Illinois' efforts:

- **Ohio – CyberOhio Initiative:** Ohio recently enacted a sweeping cybersecurity mandate for local governments (effective September 2025) led by the state's CyberOhio program. Under this initiative, every local government must implement a basic cybersecurity program aligned to best practices (such as the NIST Cybersecurity Framework or CIS Controls), provide cybersecurity training for all employees annually, and report any cyber incidents to state authorities.[12] CyberOhio, established in 2016 as a state-level cyber coordination hub, provides guidance and free resources to help municipalities comply. For example, Ohio's Persistent Cyber Improvement (O-PCI) program offers free training courses to local government staff to meet the new requirements.[13] The CyberOhio office coordinates statewide cyber capabilities, develops standards, and serves as a centralized point to assist local entities – essentially treating local cyber preparedness as a shared responsibility with state government. This approach has positioned Ohio as a leader in mandating and facilitating cybersecurity readiness at the local level.

- **Texas – Statewide Cyber Command:** Texas has invested heavily in a centralized cybersecurity command structure. In June 2025, Texas established the Texas Cyber Command via House Bill 150, with a $135 million state investment to create the nation's largest state-run cybersecurity center.[14] Headquartered in San Antonio, this new Cyber Command will coordinate cyber defense efforts across state agencies and local governments, acting as a state-level "mission control" for cybersecurity. It is tasked with launching a cyber threat intelligence center and partnering with local, state, and federal entities to streamline responses to cybersecurity attacks.[15] Texas' initiative recognizes that many municipalities lack sufficient cyber resources; the state Cyber Command is designed to fill those gaps by

10. Ibid.
11. MIT Sloan Management Review, The CEO's Cyber Resilience Playbook, accessed 2025. https://sloanreview.mit.edu/article/the-ceos-cyber-resilience-playbook
12. WLWT5 – Ohio, "Ohio to roll out new cybersecurity standards for local governments", accessed 2025. https://www.wlwt.com/article/ohio-new-cybersecurity-standards-local-governments/68030862#
13. CyberOhio (2025). Ohio's Local Government Cybersecurity Standards (HB 96) – State initiative requiring NIST/CIS-aligned cyber programs, annual training, and incident reporting for all local governments. CyberOhio provides free training (O-PCI) and coordination.
14. TX Office of the Governor (2025). Texas Cyber Command Announcement – House Bill 150 (2025) established a Texas Cyber Command Center in San Antonio with $135 million funding to coordinate statewide cybersecurity and develop a threat intelligence center.
15. Ibid.

providing expertise, rapid incident response support, and a unified strategy. The substantial funding underscores the priority placed on cybersecurity coordination as critical state infrastructure. Texas' model illustrates how dedicating state funding and organizational capacity can elevate cybersecurity across all levels of government.

> National attention to cybersecurity in transportation rose significantly following several cyber incidents involving transportation infrastructure, including the widely reported breach at the Texas Department of Transportation (TxDOT), which exposed sensitive data for more than 423,000 individuals.[16] These incidents highlighted that uncoordinated local response models often leave individual agencies struggling to manage incident response alone.

- **New Jersey – New Jersey Cybersecurity & Communications Integration Cell (NJCCIC) Cyber Fusion Center:** New Jersey operates one of the earliest and most robust state-level cybersecurity programs through its NJCCIC. Established in 2015 as part of the New Jersey Office of Homeland Security and Preparedness, NJCCIC functions as a 24/7 cybersecurity fusion center and information sharing hub[17]. It serves as the state's one-stop shop for cybersecurity threat intelligence, real-time monitoring, incident reporting, and technical assistance. NJCCIC analysts continuously monitor threats to New Jersey's public agencies and critical infrastructure; the center disseminates cybersecurity alerts, best practice advisories, and weekly threat bulletins to stakeholders statewide.[18] Importantly, NJCCIC provides direct support to local governments and school districts – including free network vulnerability scanning, risk assessments, and an incident response hotline staffed around the clock.[19] This "local enablement" mission has helped even small towns in New Jersey access sophisticated cybersecurity tools and expertise that they could not afford on their own. By combining centralized threat intelligence with on-call local support, New Jersey's model shows the impact of a well-resourced state cybersecurity team acting as a force multiplier for municipal and transit agency cybersecurity.

- **North Dakota – Whole-of-State Shared Services:** North Dakota has pioneered a "whole-of-state" cybersecurity approach, moving beyond the traditional siloed model. The state legislature authorized a unified cybersecurity strategy in 2019, enabling the central IT department to extend its services and standards to all state agencies and political subdivisions.[20] As a result, virtually all public entities in North Dakota (state agencies, counties, cities, K-12 schools, public universities, and public transit operators) operate on a common secure network (the STAGEnet network) and leverage shared cybersecurity services. This centralized architecture means that threat monitoring and defenses are

16. Hoplon InfoSec. "Texas DOT Data Breach: What Happened, Who Was Affected." Hoplon InfoSec (online), accessed 2025. https://hoploninfosec.com/texas-dot-data-breach-what-happened
17. New Jersey Cybersecurity & Communications Integration Cell "About the NJCCIC" Cyber New Jersey (online), accessed 2025. https://www.cyber.nj.gov/connect/about-the-njccic
18. New Jersey State League of Municipalities "Cybersecurity Resources", accessed 2025. https://www.njlm.org/1276 Cybersecurity-Resources
19. Ibid.
20. Government Technology "North Dakota CISO Highlight Whole-of-State Security Approach", accessed 2025. https://www.govtech.com/security/north-dakota-ciso-highlights-whole-of-state-security-approach

managed in a coordinated way rather than fragmented across hundreds of local networks.[21] North Dakota's Information Technology Department provides local governments with a suite of cybersecurity tools as shared services – for example, endpoint protection software, managed vulnerability scanning, security awareness training programs, and even cybersecurity maturity assessments are offered statewide.[22] Smaller entities that lack IT staff can opt into these services, immediately raising their security baseline. The whole-of-state model yields efficiencies of scale and ensures consistent protection: any improvements to the central defenses benefit every connected local entity. North Dakota's experience shows that having all jurisdictions on a unified network with centralized cybersecurity operations can significantly enhance the overall security posture and enable faster, more uniform responses to threats across the state.

Each of these state programs reinforces a common theme: improving cybersecurity resilience for transit agencies (and local governments generally) often requires state-level leadership, funding, and coordination. The Pilot collaborative approach is very much in spirit with these models, focusing on shared knowledge, common standards, and resource pooling, albeit executed on a smaller scale to date. Interim results from Illinois further highlight issues such as lack of formal policies and executive awareness that national studies have found prevalent in transit systems nationwide,[23] underscoring that solutions will likely require the kind of comprehensive, multi-level efforts exemplified by the programs above. Perhaps the most important finding is that group-based participation reduces the cost while accelerating cybersecurity resilience. The Pilot's coordinators are actively pursuing similar cohort-based approaches in Ohio and Michigan.

Next Steps and Opportunities

Broad Knowledge Sharing: A critical next step is to disseminate the findings and lessons from the Pilot to a broader audience of transit operators, policymakers, and government officials. This White Paper is one such vehicle. Additional knowledge-sharing efforts are already under way, including recent presentations to the Ohio Transit Risk Pool, Michigan DOT, and the Transit Association of Maryland as well as upcoming conference presentations hosted by New Mexico DOT, IDOT, and MTI. These forums will share practice guidance, implementation strategies, and templates that other transit agencies can adopt and adapt.

By sharing these interim lessons now, the Pilot hopes to accelerate replication elsewhere, especially among small and mid-sized transit agencies facing similar challenges. The "tear-out" guidance included in the 2025 MTI Study for transit leadership, which stressed board-level engagement and concrete cybersecurity steps for agencies,[24] will be incorporated into these outreach materials to drive home the urgency for action at the management level. Building a culture of cybersecurity across the transit sector requires evangelizing not just IT fixes, but governance and policy changes as well. Illinois' experience can inform those conversations nationally.

---

21. Ibid., 5.
22. Ibid.
23. Mineta Transportation Institute, "Cybersecurity Still Not On Track", accessed 2025. https://transweb.sjsu.edu/press/Cybersecurity-Transit-Still-Not-Track
24. Ibid., 2.

Pilot Expansion and Services: There is interest in Illinois in evolving the cohort-based model into a sustained, recurring initiative that could support additional transit agencies and, potentially, other local government units. A future iteration could include annual cohorts that progress through a structured pathway of assessments, remediation planning, peer workshops, and periodic monitoring.

As the Pilot matures, participating agencies could also access optional shared services, for example: statewide security awareness training, fractional Chief Information Security Officer (CISO) support (pooled cybersecurity expertise for agencies that cannot fund an internal role), and mutual-aid agreements for incident response so that, in the event of an attack, peer agencies and state experts could rapidly mobilize to assist.

Unlike traditional consulting models, which are slow and siloed, this approach is faster, more cost-effective, and scalable. By leveraging a shared platform, agencies avoid starting from scratch: instead, they build from common templates, adopt proven best practices, and benefit from structured peer support. This allows smaller systems to make measurable progress without the cost or delay of bespoke consulting. IDOT paved the way.

Other states, Ohio, Maryland, Virginia, and Michigan, are exploring similar models. But with each effort operating independently, a significant gap remains: there is no national body overseeing coordination, replication, or transit-specific governance for cybersecurity. Without a unified approach, momentum risks being lost to duplication and inefficiency. Addressing this gap is key to national resilience.

Funding Support: None of this progress is sustainable without dedicated funding. The Pilot has demonstrated clear benefits in risk reduction and capacity-building. To sustain this momentum, additional funding support is critical. Initial support came from MTI, and subsequent direct funding from Cybrbase enabled the Pilot to continue.

Looking ahead, the Pilot's coordinators continue to explore additional funding sources at both the state and federal level to support ongoing assessments and implementation of security upgrades, while also looking to expand the model to Ohio, Maryland, Virginia, and Michigan under existing state funding. A potential source of funding at the Federal level was the State and Local Cybersecurity Grant Program (SLCGP), a federal initiative created to help jurisdictions strengthen cybersecurity defenses. While the SLCGP's statutory authority expired at the end of Fiscal Year 2025 and no new grants are currently available, bipartisan efforts to reauthorize the program remain active in Congress.[25] Should that funding resume, states such as Illinois, Ohio, Maryland, Virginia, Michigan, and many others could be well-positioned to pursue collaborative, multi-entity proposals.

In parallel, agencies are also exploring support through state homeland security offices, academic research partnerships, insurance risk pools, trade associations, and infrastructure grants from private or philanthropic sources. Sustained investment is necessary to advance resilience from planning to execution, and to ensure that transit systems remain both secure and operational in the face of evolving cybersecurity threats.

---

25. National Association of Counties, "Support Reauthorization of the State and Local Cybersecurity Grant Program, accessed 2025.https://www.naco.org/resource/support-reauthorization-state-and-local-cybersecurity-grant-program#

Conclusion

The IDOT Cyber Resilience Pilot clearly demonstrated, on a small scale, the positive impact that a structured, collaborative approach can have on improving cybersecurity in the transit sector. In six months, six Illinois transit agencies moved from minimal cyber preparedness to taking concrete steps that reduce their vulnerability to attack, such as establishing incident response plans, training staff, and implementing essential technical safeguards. Just as importantly, the Pilot fostered a culture change: agencies are now sharing cybersecurity strategies, and transit leadership is beginning to view cybersecurity as core to operational continuity and public safety.

The work is far from complete. As national research and the Pilot's own findings confirm, transit agencies, especially smaller ones, remain attractive targets for cybersecurity threats, and sector-wide readiness is still nascent.[26] The Illinois Pilot offers a compelling blueprint for closing this gap: peer-driven, executive-supported (at the DOT level), and cost-efficient, with measurable outcomes delivered faster than traditional one-off consulting engagements. The model's speed and scalability are enhanced by shared platforms, which allow for the reuse and sharing of policies, procedures, and training content across participants.

Despite growing interest in this approach, there is currently no national coordinating body responsible for standardizing and scaling it. The FTA provides eligible funding for cybersecurity activities through both formula and discretionary grants, and many discretionary programs explicitly expect applicants to demonstrate an established cybersecurity posture. However, FTA has not yet assumed a national organizing role in convening states, curating shared playbooks, or driving a common implementation model across jurisdictions. This leaves a gap.

Institutions such as MTI, with their research mission and convening capacity, help bridge that gap by studying early models, translating lessons into standards, and aligning state-level efforts into a coherent framework. The model now emerging in Illinois, and echoed in other states, offers a scalable pathway that could raise the cyber baseline across U.S. transit systems in a repeatable way.

The coming months will include follow-up assessments and additional workshops for IDOT participants, that will offer new insights into the Pilot's effectiveness and where refinements are needed. These lessons will feed into its continuous improvement. In summary, the IDOT Cyber Resilience Pilot marks a proactive step toward modernizing cybersecurity in public transportation. It demonstrates that even with limited budgets, strategic collaboration can yield substantial dividends in resilience and risk reduction. By refining, expanding, and replicating this approach, Illinois, and others, can help ensure that cybersecurity becomes embedded in the operational fabric of transit, ultimately protecting millions of riders and the critical systems on which they depend.

26. Progressive Railroading, "Report: Transit industry unprepared for more cybersecurity threats", accessed 2025.https://www.progressiverailroading.com/security/news/Report-Transit-industry-unprepared-for-more-cybersecurity-threats--74530#

Acknowledgment

The authors thank Lisa Rose for editorial services, as well as MTI staff Project Assistant Cameron Simons and Graphic Designer Michael Virtudazo.

About the Authors

Scott Belcher is the President and CEO of SFB Consulting, LLC, where he specializes in transportation, transportation technology, the internet of things, smart cities, the environment, and cybersecurity. Mr. Belcher is a Mineta Transportation Institute (MTI) Research Associate and has written several white papers and two MTI studies on cybersecurity in transportation.

Terri Belcher is a writer and analyst who has worked in Washington, D.C. for the past 35 years. Ms. Belcher has 25 years of experience working for the federal government, federal contractors, and a number of non-profits.

Andy Souders is a technology executive with over 35 years of experience in digital innovation and organizational transformation across industries such as Cloud, Cybersecurity, and Smart Cities.

This report can be accessed at **transweb.sjsu.edu/research/2562.**

The Mineta Transportation Institute (MTI) is a university transportation center located within the Lucas Graduate School of Business at San José State University. MTI supports the advancement of safe, efficient, and innovative surface transportation through research, education, workforce development, and technology transfer.