

Article

Strengthening the Transportation Cybersecurity Workforce: A Mixed-Methods Analysis of Workforce Development, Organizational Preparedness and Cross-Sector Collaboration

Amjad Ali ^{1,2,*}, Larry Liu ³, Blessing Ojeme ² , Chidozie Anadozie ², Fremah Agyemang ² , Satish Ukkusuri ⁴, Eunhan Ka ⁴  and Shagun Mittal ⁴ 

¹ National Transportation Center, Morgan State University, Baltimore, MD 21251, USA

² Department of Computer Science, Morgan State University, Baltimore, MD 21251, USA

³ Department of Sociology & Anthropology, Morgan State University, Baltimore, MD 21251, USA

⁴ Lyles School of Civil Engineering, Purdue University, West Lafayette, IN 47906, USA

* Correspondence: amjad.ali@morgan.edu

Abstract

The rapid digitalization of transportation systems has expanded the cyberattack surface of critical infrastructure while exposing significant shortages in transportation-specific cybersecurity workforce capacity. Existing workforce studies rarely integrate transportation-sector workforce development, organizational preparedness, operational technology (OT) challenges, and interdisciplinary collaboration within a unified analytical framework. In response to this gap, this study employs a mixed-methods approach that integrates Term Frequency–Inverse Document Frequency (TF-IDF) text analysis of publicly available workforce development documents, qualitative interviews with academics, policymakers, and transportation cybersecurity professionals, and organizational survey analysis to examine workforce development challenges across transportation subsectors. The findings reveal persistent information technology (IT) and operational technology (OT) competency gaps, curriculum–industry misalignment, organizational staffing shortages, disparities in cybersecurity preparedness, and the critical importance of experiential learning and dedicated cybersecurity staffing. The study further emphasizes the need for interdisciplinary education, organizational capacity building, and sustained collaboration among academia, government, and industry to strengthen the transportation cybersecurity workforce’s readiness and resilience. Collectively, the findings position transportation cybersecurity workforce development as a systems-coordination challenge that requires long-term strategic investment, cross-sector collaboration, and workforce innovation to enhance the security, resilience, and operational continuity of transportation systems.

Keywords: transportation cybersecurity; cybersecurity workforce development; transportation systems; cybersecurity skills gap; organizational preparedness; operational technology security; interdisciplinary collaboration; critical infrastructure protection; transportation workforce resilience



Academic Editor: Zhibin Chen

Received: 13 May 2026

Revised: 20 June 2026

Accepted: 26 June 2026

Published: 30 June 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

This study examines the shortage of cybersecurity talent in the transportation systems sector and the broader challenges of developing a sustainable workforce capable of protecting the United States’ transportation infrastructure. Modern transportation relies heavily on operational technology (OT), Internet of Things (IoT) devices, connected/autonomous

vehicles, traffic management systems, signaling, and vehicle-to-everything (V2X) communications. Legacy systems are being integrated with digital controls, expanding the attack surface significantly. Greater interconnectivity, combined with remote access points and IT/OT convergence, amplifies risks to critical infrastructure. Cyber threats to ports, rail, aviation, and road systems can cause operational disruptions, safety hazards, and cascading effects on public safety and the economy. General cybersecurity talent is already in short supply globally, with many unfilled positions [1], but transportation demands specialized knowledge in areas like autonomous technologies, supply chain logistics, and safety-critical environments that blend cyber and physical risks. This niche expertise is even scarcer, exacerbating the pipeline challenge.

Developing a qualified transportation cybersecurity workforce is therefore critical to safeguarding the security, resilience, operational continuity, and public safety of the nation's transportation systems. General cybersecurity talent shortages are acute, but transportation requires specialized expertise in OT security, safety-critical systems, and domain-specific regulations. Without dedicated professionals who understand both cyber and transportation contexts, agencies and industries struggle to implement effective defenses, incident response, and resilience measures. In response to this growing need, this study investigates and analyzes barriers to developing a steady pipeline of qualified cybersecurity talent and identifies strategic and innovative approaches for strengthening workforce development across academia, industry, and government. The study further emphasizes the importance of interdisciplinary and cross-institutional collaboration in preparing cybersecurity professionals with the technical, operational, and sector-specific competencies needed to address the evolving cybersecurity challenges of modern transportation systems while ensuring the safety and trust of the traveling public.

Addressing transportation cybersecurity workforce challenges requires coordinated efforts among academia, industry, and government. Universities play a critical role in developing future talent through education, research, and experiential learning opportunities. Industry contributes operational expertise, workforce demand signals, internships, apprenticeships, and professional development pathways. Government agencies support workforce development through policy frameworks, funding initiatives, standards development, and critical infrastructure protection programs. Collaboration among these sectors is essential for developing a skilled cybersecurity workforce capable of strengthening the security, resilience, and operational continuity of modern transportation systems. While academia–industry–government collaboration is well established in public management, cybersecurity, and engineering education literature, limited research has examined how workforce development, organizational preparedness, operational technology (OT) competency requirements, and cross-sector collaboration can be integrated within a unified transportation cybersecurity workforce framework.

To identify the strategies for strengthening the workforce development pipeline in the transportation sector, this interdisciplinary research uses a combination of document text analysis, interviews with cybersecurity experts and leaders in transportation companies, U.S. Department of Transportation officials in the government and cybersecurity faculty in universities in the United States, and an analysis of the Mineta Transportation Institute (MTI) 2020 and 2024 surveys [2,3] on cybersecurity workforce development.

The key research questions (RQs) in this research paper are:

- RQ1: What does the academic, industry, and government literature reveal about the challenges associated with training the cybersecurity workforce in the transportation systems sector (text analysis)?

- RQ2: How can universities best develop curriculum, mentorship, and awareness programs to better prepare students for the cybersecurity workforce in the transportation sector (interview)?
- RQ3: How can transportation-related government agencies design effective programs and sustainable funding streams that would help universities prepare workforce-ready cybersecurity talent and assist employers in the transportation sector (interview)?
- RQ4: How can the transportation industry develop effective recruitment programs for cybersecurity-related roles through scholarships, workshops/conferences, internships, or co-op opportunities (qualitative interview)?
- RQ5: How can academia, government, and industry collaborate effectively to strengthen the cybersecurity talent pipeline for transportation systems (qualitative interview)?
- RQ6: To what extent does self-assessed cybersecurity preparedness align with the adoption of formal cybersecurity practices among U.S. public transit agencies (survey)?
- RQ7: To what extent are organizational characteristics, specifically agency size, cybersecurity staffing, and leadership structure, associated with the level of formal cybersecurity practice adoption (survey)?

The security of the United States' transportation systems is increasingly dependent on the resilience of its digital infrastructure [4]. As transportation networks from aviation to freight rail to public transit become more reliant on interconnected systems, they also become more vulnerable to cyberattacks. In this context, the shortage of skilled cybersecurity professionals represents not just a labor market challenge but a pressing national security concern. Ensuring that a well-trained, adaptable, and adequately sized cybersecurity workforce is in place is essential to protecting the nation's transportation systems from cyber threats that could disrupt commerce, compromise safety and erode public trust.

Unlike prior workforce studies that focus primarily on generalized cybersecurity labor shortages, this study integrates transportation-sector workforce development, organizational preparedness, operational technology challenges, and interdisciplinary collaboration into a unified analytical framework. The study further provides organizational-level evidence on the link between cybersecurity staffing capacity and the adoption of formal cybersecurity practices among U.S. transit agencies.

Addressing this workforce gap requires more than simply expanding the number of graduates in cybersecurity fields. It demands that education and training programs align closely with the rapidly evolving needs of industry and government. Existing academic pathways often fail to prepare graduates with both the technical skills and the sector-specific knowledge needed to secure transportation infrastructure. For example, traditional degree programs may not emphasize offensive and defensive cyber operations, or they may address information technology (IT) systems without adequately covering operational technology (OT) components that are critical to transportation operations. Closing these gaps requires a coordinated effort among universities, industry, and government to define workforce competencies, standardize training approaches, and create pipelines that begin before students even enter college.

The study findings highlight several major themes for building a stronger transportation cybersecurity workforce: aligning academic programs with industry needs, hiring faculty with industry expertise, increasing government investment in collaborative research and training while building on alum networks, creating uniform IT/OT standards and targeted training, elevating cybersecurity as a core business priority for transportation companies, making workforce development a key performance indicator, expanding internships that expose students to experiential learning, harnessing the resources of professional associations and developing outreach initiatives to attract high school students

to cybersecurity careers in the transportation sector. Survey results indicate that 41% of transportation agencies report a low level of perceived preparedness to defend against cybersecurity threats. In contrast, large agency budgets and having full-time cybersecurity staff are associated with higher preparedness levels.

The literature review addresses existing gaps in transportation cybersecurity workforce development research, particularly the limited integration of organizational preparedness, operational technology challenges, interdisciplinary education, and cross-sector collaboration.

This study contributes to the transportation cybersecurity literature in three primary ways (Table 1). First, it develops an integrated transportation cybersecurity workforce framework that brings together workforce development, organizational preparedness, operational technology challenges, and interdisciplinary collaboration within a unified analytical perspective. Second, it combines text analysis, qualitative interviews, and organizational survey analysis to provide empirical evidence across multiple transportation subsectors. Third, it provides practical workforce-development recommendations for academia, industry, and government to strengthen resilience in transportation cybersecurity.

Table 1. Key Contributions of the Study.

Contribution	Description
Integrated Transportation Cybersecurity Workforce Framework	Integrates workforce development, organizational preparedness, operational technology (OT) competency requirements, and cross-sector collaboration into a unified framework for transportation cybersecurity workforce development and resilience.
Multi-Method Empirical Analysis	Combines computational text analysis of 44 documents, expert interviews, and transportation-sector survey data to identify workforce-development challenges, skills gaps, organizational preparedness issues, and barriers to building a sustainable transportation cybersecurity talent pipeline.
Practical Workforce Development Recommendations	Provides actionable recommendations for strengthening the transportation cybersecurity workforce through interdisciplinary education, experiential learning, industry partnerships, workforce-development initiatives, and transportation-specific cybersecurity training.

2. Literature Review

2.1. Transportation Cybersecurity as a National Problem

Cybersecurity in the transportation sector plays a vital role in the well-being of citizens and riders. Transportation systems are becoming increasingly dependent on technology, as 82% of logistics companies have formulated their plans to further increase their technology investments [5]. These increased investments in transportation technology and digitalization will unlock significant economic value through shorter, simpler, and faster supply chains. Increasing transparency in transportation enables better forecasting, decision-making and resource optimization. Transportation technology also reduces costs and increases the efficiency and competitiveness of the national economy [6]. However, the increased digitalization of the transportation sector comes with cybersecurity vulnerabilities. Ransomware attacks on cargo ships have increased by 200% between 2021 and 2023. Cybercrime is expected to reach \$10.5 trillion globally, posing a significant risk to global logistics [7].

2.2. The Transportation Cybersecurity Workforce Shortage

As a result, there is significant demand for cybersecurity professionals who can protect transportation systems from rapidly evolving cyber threats [8]. The Bureau of Labor Statistics estimates that the cybersecurity workforce (information security analysts) will grow by 33% between 2022 and 2032 [9]. The significant growth in the demand for cybersecurity workers implies a severe shortage of qualified cybersecurity talent, posing a significant risk to the resilience of the U.S. transportation sector. The rising demand for cybersecurity workers is not matched by sufficient availability of cybersecurity talent, indicating a significant need to train more cybersecurity professionals [1].

Gig economy platforms have been heralded as a possible way for companies to find suitable cybersecurity talent [10]. However, such platforms do not account for the need to provide initial cybersecurity training. Providing cybersecurity training at universities and training institutes is vital to developing talent for cybersecurity companies in the transportation sector [11]. However, students may obtain certifications that are less relevant to industry needs [12].

Current workers in the industry often lack awareness of cybersecurity risks as well [13]. Workforce development must co-occur with evolving policy frameworks, technological advancements and operational requirements [14]. Like other professional fields, cybersecurity requires competency-based frameworks to identify the precise knowledge, skills, and abilities needed by its workforce [15]. Recent literature further suggests that transportation cybersecurity workforce development extends beyond technical training and certifications. The increasing convergence of information technology (IT) and operational technology (OT) in transportation systems requires professionals with interdisciplinary competencies spanning cybersecurity, transportation operations, critical infrastructure protection, industrial control systems, and cyber–physical systems security. In addition, workforce-development efforts must be supported by organizational preparedness, leadership commitment, and collaboration among academia, industry, and government to ensure that workforce capabilities remain aligned with evolving technological, operational, and regulatory requirements. Studies have highlighted the growing need for expertise in OT environments, cybersecurity governance, risk management, and organizational resilience [16–18]. Collectively, these findings highlight the need for a more comprehensive and coordinated approach to transportation cybersecurity workforce development that integrates technical competencies, organizational preparedness, transportation-specific operational requirements, and cross-sector collaboration to address emerging cybersecurity challenges. The key themes in the literature review are covered in Table 2.

Table 2. Key Themes from the Literature Review.

Theme	Sources
Transportation Digitalization and Economic Benefits	[5,6]
Transportation Cybersecurity Threats and Risks	[7]
Cybersecurity Workforce Demand and Talent Shortages	[1,8,9]
Alternative Talent Development Pathways	[10]
Education, Training, and Competency Gaps	[11–13]
Workforce Development Requirements and Competency Frameworks	[14,15]
Interdisciplinary and Collaborative Workforce Development	[11,14,15]
Organizational Preparedness and Cybersecurity Capacity	[2,3]
IT/OT Integration and Operational Technology Security	[16–18]

2.3. Literature Gap: Cross-Institutional Collaborative Approach

This research identifies several gaps in the transportation cybersecurity workforce literature. Existing studies have primarily focused on workforce shortages, education, training, certifications, and talent development while providing comparatively less attention to the integration of workforce development, organizational preparedness, operational technology (OT) competency requirements, transportation-specific cybersecurity resilience, and cross-sector collaboration within a unified analytical framework. In addition, relatively little research has examined the interdisciplinary competencies required to secure increasingly interconnected transportation systems that span both information technology (IT) and OT environments. Furthermore, relatively few studies in the transportation sector have examined the relationship between cybersecurity workforce capacity and organizational preparedness. In response to these gaps, this research investigates barriers to developing a sustainable pipeline of qualified transportation cybersecurity professionals and explores strategies to strengthen workforce development, organizational preparedness, and cross-sector collaboration.

3. Research Methodology

This study employs a mixed-methods research design that integrates targeted web scraping, computational text analysis, qualitative interviews, and organizational survey analysis to examine transportation cybersecurity workforce development challenges, organizational preparedness, and cross-sector collaboration needs. The mixed-methods approach enables triangulation across multiple data sources and provides both technical and organizational perspectives on workforce shortages, skills gaps, institutional preparedness, and collaborative workforce-development strategies within the transportation sector.

3.1. Web Scraping and Computational Text Analysis

The study employed targeted web scraping and computational text analysis to collect and analyze publicly available documents on transportation cybersecurity workforce development, transportation systems security, operational technology (OT) security, organizational preparedness, and interdisciplinary workforce development challenges.

3.1.1. Web Scraping

Given the data-centric and interdisciplinary nature of transportation cybersecurity workforce research, web scraping enabled the collection and analysis of a broad range of academic, industry, and government sources, extending beyond traditional manual literature review approaches.

The web-scraping process was implemented using the Python Scrapy framework (version 2.11.2) due to its scalability, support for multiple data formats, and effectiveness in handling unstructured web documents and large-scale corpus collection. Scrapy also provides mechanisms to address common web-scraping challenges, including variability in document structure, data quality, and the automated extraction of publicly accessible online content.

Documents were collected from publicly accessible academic databases, government repositories, transportation-security publications, and cybersecurity workforce-development sources, including IEEE Xplore, ACM Digital Library, Springer, U.S. Department of Transportation (USDOT) publications, Department of Homeland Security (DHS) resources, National Institute of Standards and Technology (NIST) documents, and industry reports from organizations such as ISC2 and the SANS Institute. Additional practitioner-oriented documents were collected from transportation and cybersecurity news outlets and from publicly available policy and workforce development reports.

Search terms included combinations of “transportation cybersecurity,” “cybersecurity workforce development,” “transportation systems security,” “critical infrastructure cybersecurity,” “operational technology (OT) security,” “industrial control systems (ICS) security,” “IT/OT integration,” “transportation cybersecurity workforce,” “cybersecurity skills gaps,” “transportation infrastructure protection,” and “cross-sector cybersecurity collaboration.”

The collected documents were screened using predefined inclusion criteria requiring explicit discussion of workforce-development challenges, cybersecurity education and training, organizational preparedness, transportation-system security, interdisciplinary workforce competencies, recruitment, retention, or collaboration among academia, government, and industry. Technical cybersecurity papers without workforce-development implications were excluded from the final corpus. The resulting corpus comprised documents published predominantly between 2020 and 2025, reflecting the contemporary nature of transportation cybersecurity workforce research.

The final text corpus consisted of 44 publicly available documents spanning academic research, federal agency reports, transportation security publications and practitioner-oriented workforce development studies. The diversity of sources enabled the study to capture both theoretical and operational perspectives on transportation cybersecurity workforce development.

3.1.2. Computational Text Analysis

All collected documents were preprocessed prior to analysis to improve consistency and reduce analytical noise. Preprocessing steps included duplicate removal, lowercasing, punctuation removal, stop-word removal, and lemmatization to reduce words to their base forms. These preprocessing procedures improved text standardization and enhanced the reliability of downstream computational analysis.

To identify dominant thematic structures within the corpus, the study employed unsupervised machine-learning techniques. Term Frequency–Inverse Document Frequency (TF-IDF) was selected as the primary vectorization method because it effectively identifies terms that are both frequent within specific documents and distinctive across the entire corpus, thereby highlighting domain-specific and contextually important concepts rather than generic or ubiquitous terms. Unlike simple term frequency counts, TF-IDF down-weights commonly occurring words (e.g., “transportation” or “cybersecurity”) while elevating more informative, discriminative terms, which is particularly valuable when analyzing a specialized corpus of policy, industry, and academic documents. This approach produces meaningful numerical feature vectors that better capture the relative importance of terms [19].

Following TF-IDF vectorization, K-means clustering was applied to group documents with similar semantic content. The optimal number of clusters was determined empirically using silhouette analysis, which evaluates cluster cohesion and separation, yielding seven clusters. This data-driven approach enabled thematic identification without imposing predefined categories on the corpus. The resulting clusters were interpreted by examining high-weight terms, representative documents, and recurring thematic relationships within each cluster. Cluster validity was assessed through manual inspection of document groupings and thematic consistency, ensuring that each cluster represented a coherent and interpretable topic.

While clustering identified structural groupings within the corpus, domain-informed interpretation was applied to contextualize clusters within transportation subsectors and workforce development challenges. The thematic interpretation focused on recurring concepts related to transportation cybersecurity workforce development, including sector-specific training, interdisciplinary skill requirements, IT/OT integration, experiential learn-

ing, organizational preparedness, staffing shortages, and industry-aligned education. These computationally derived themes were then compared with findings from the qualitative interviews and organizational survey analysis to assess convergence, complementarity, and thematic gaps across data sources.

The triangulation of computational text analysis, interviews, and survey findings strengthened the study's validity by integrating multiple forms of evidence from academic, industry, and government perspectives. This mixed-methods integration supports more robust conclusions regarding transportation cybersecurity workforce development challenges and organizational preparedness needs.

3.2. Qualitative Interviews

This study employed a semi-structured qualitative interview methodology to obtain expert perspectives on transportation cybersecurity workforce development challenges, organizational preparedness, interdisciplinary skill requirements, and collaborative workforce development strategies across academia, government, and industry. The interviews were designed to provide contextual and experiential insights that complement the computational text analysis and organizational survey findings.

Participants were selected using purposive expert sampling based on demonstrated expertise and professional experience in cybersecurity, transportation systems, workforce education, operational technology (OT) security, critical infrastructure protection, and transportation cybersecurity workforce development. Academic participants were identified from universities offering cybersecurity, transportation systems, engineering, and related interdisciplinary programs, particularly institutions affiliated with National Transportation Centers funded through the U.S. Department of Transportation (USDOT). Government participants were identified through transportation-related agencies and cybersecurity organizations, including the Federal Transit Administration (FTA), the U.S. Department of Homeland Security (DHS), and the Cybersecurity and Infrastructure Security Agency (CISA). Industry participants were identified through professional referrals, industry partnerships, and transportation cybersecurity networks.

Participants were recruited through institutional websites, professional networks, and publicly available organizational contact information. In total, 64 individuals were contacted, 16 completed expert interviews representing academia, government, transportation agencies, engineering, and cybersecurity sectors in the United States. Interviews ranged from approximately 30 to 60 min in duration. A list of participant occupational categories is provided in Appendix A.

The interview protocol covered multiple dimensions of transportation cybersecurity workforce development, including workforce shortages, interdisciplinary curriculum development, experiential learning opportunities, IT/OT competency gaps, organizational cybersecurity preparedness, recruitment and retention challenges, industry-aligned workforce training, and opportunities for collaboration among academia, government, and industry. Interviews continued until sufficient thematic saturation was achieved across the major workforce-development and organizational preparedness themes. The semi-structured interview format enabled participants to provide detailed perspectives on emerging workforce challenges, organizational needs, and long-term strategies for strengthening transportation cybersecurity workforce resilience.

Because the research involved human subjects, Institutional Review Board (IRB) approval was obtained on 18 February 2025, from the IRB at Morgan State University (IRB #25/02-0034) prior to conducting interviews.

The interview data were analyzed using thematic analysis following the approach outlined by Braun and Clarke [20]. The analysis involved systematic coding of participants'

responses to identify recurring patterns, organizational challenges, workforce development needs, interdisciplinary skill requirements, and collaborative strategies across transportation cybersecurity contexts. The analysis incorporated both deductive coding based on predefined research themes and inductive coding to allow emergent themes to develop directly from participant responses. This analytical approach aligns with grounded-theory principles, in which conceptual themes emerge iteratively from the data rather than being imposed entirely *a priori* [21].

To enhance methodological rigor and data validation, this study incorporated several trustworthiness measures [22]: (1) member checking, whereby interview summaries were shared with selected participants for verification and clarification; (2) peer debriefing among the research team during analysis; and (3) detailed audit trail documentation of all analytical decisions.

3.3. Survey Analysis

To establish an empirical baseline of organizational cybersecurity governance, formal cybersecurity practices, and workforce capacity within the U.S. public transit sector, this study conducted a secondary analysis of publicly available survey datasets published by the Mineta Transportation Institute (MTI). The survey analysis provides demand-side evidence of the workforce-development challenges identified through computational text analysis and qualitative interviews and contextualizes the organizational and workforce needs examined throughout this study.

All data used in the analysis were publicly available and de-identified. No additional IRB approval was required for the secondary analysis of these datasets.

3.3.1. Data Sources for the Survey Analysis

The analysis drew upon two publicly available Mineta Transportation Institute (MTI) cybersecurity survey datasets and accompanying reports.

The first dataset originated from MTI Project 1939 (2020 survey) [2], in which MTI researchers distributed a 26-item digital survey to 312 U.S.-based public transit executives affiliated with the American Public Transportation Association (APTA). The survey addressed cybersecurity staffing, certifications, policy adoption, incident response, training practices, cybersecurity preparedness, and organizational governance. After removal of incomplete responses, duplicates, and non-U.S. operators, the original study retained 90 usable responses. The publicly available dataset contains 103 de-identified records and 28 variables.

The second dataset originated from MTI Project 2405 (2024 survey) [3], which expanded the earlier instrument into a 54-item survey distributed to approximately 300 transportation executives through APTA, the American Association of State Highway and Transportation Officials (AASHTO), and the Community Transportation Association of America (CTAA). The expanded survey addressed cybersecurity staffing, leadership structure, IT and cybersecurity budgets, cybersecurity assessment practices, tabletop exercises, disaster recovery planning, differentiated training, cyber insurance, and organizational preparedness. After removing duplicate and non-U.S. responses, the final sample included 78 transit organizations.

Both surveys targeted organizational leaders responsible for or knowledgeable about cybersecurity practices within their transit agencies. Because the surveys did not employ probability sampling, the findings should be interpreted as evidence from the achieved samples rather than as nationally representative estimates for all U.S. transit agencies.

Survey items from both years were recoded as binary indicators to facilitate cross-year comparisons and harmonization between the two datasets. “Do not know” responses were

coded conservatively as practice absence for operational-practice indicators, based on the rationale that an inability to confirm the existence of a cybersecurity practice may itself reflect limitations in organizational preparedness.

3.3.2. Core Practice Index

To operationalize the adoption of organizational cybersecurity practices, the study developed a six-item Core Practice Index (CPI). The CPI included the following foundational cybersecurity practices: (1) documented cybersecurity policy, (2) documented cybersecurity incident response plan, (3) audit or accountability mechanisms, (4) cybersecurity clauses in vendor contracts, (5) long-term network log retention, and (6) annual or more frequent cybersecurity training.

Each item was coded as binary and aggregated into a standardized 0–100 scale that represents the proportion of practices adopted. Agencies with fewer than four non-missing items were excluded from CPI-based analyses.

The selected practices represent observable, operationally significant governance practices drawn from the NIST Cybersecurity Framework and the CISA Cross-Sector Cybersecurity Performance Goals, and were measured consistently in both MTI instruments. The CPI is constructed as a formative index rather than a reflective scale: each item captures a distinct and non-redundant practice that contributes to overall adoption rather than reflecting a single latent trait. Therefore, reflective-scale internal-consistency criteria are not used for item retention [23,24].

3.3.3. Sample Description and Index Characteristics

Of the 78 responding agencies in the 2024 sample, 28 (36%) reported annual operating budgets below \$5 million, 20 (26%) between \$5 million and \$50 million, and 29 (37%) above \$50 million; one agency did not report a budget. The most common transit modes represented in the sample were bus (72%), on-demand services (65%), and para-transit (53%). Forty agencies (54%) reported employing at least one full-time equivalent (FTE) dedicated to cybersecurity, while 34 agencies (46%) reported having no dedicated cybersecurity personnel.

Internal consistency and item statistics are reported here for transparency (Kuder-Richardson 20 = 0.827, $n = 74$ complete cases; corrected item-total correlations from 0.288 for network log retention to 0.796 for documented incident response plans, with five of six items exceeding 0.45). Consistent with the formative specification, the lower item-total correlation for log retention reflects its relative independence from the other practices, as it was the only practice without a size-based differential. The mean CPI score was 47.2 (SD = 36.3; median = 50.0) on a 0–100 scale ($N = 75$).

The CPI distribution revealed substantial variation in the adoption of organizational cybersecurity practices across transit agencies. Seventeen agencies (23% of complete cases) reported adopting none of the six foundational cybersecurity practices, while 18 agencies (24%) adopted five practices and 8 agencies (11%) adopted all six. This polarized distribution suggests that cybersecurity preparedness across the transit sector is not distributed along a gradual maturity continuum but rather reflects a divide between low-adoption and high-adoption organizational groups.

3.3.4. Statistical Methods

Descriptive statistics, nonparametric analyses, correlation analyses, and regression modeling were used to evaluate relationships among organizational preparedness, cybersecurity staffing, agency size, leadership structure, and formal adoption of cybersecurity practices.

Spearman's rank correlation was used to assess relationships between self-assessed cybersecurity preparedness and formal cybersecurity-practice adoption. Kruskal–Wallis and Mann–Whitney U tests were used to examine differences in cybersecurity practice adoption across organizational categories and workforce characteristics. Fisher's exact tests with false discovery rate correction were used to compare adoption rates of individual cybersecurity practices across agency groups.

Regression modeling was used to examine the association between organizational characteristics and the adoption of cybersecurity practices. Additional robustness and sensitivity analyses were conducted to evaluate the consistency of findings across datasets and organizational groupings.

Collectively, the survey analysis complements the computational text analysis and qualitative interview findings by providing organizational-level evidence regarding cybersecurity workforce capacity, preparedness disparities, staffing limitations, and cybersecurity governance practices within the transportation sector.

4. Results and Analysis

4.1. RQ1: What Does the Academic, Industry, and Government Literature Reveal About the Challenges Associated with Training the Cybersecurity Workforce in the Transportation Systems Sector (Web Scraping and Computational Text Analysis)?

To address Research Question 1, computational text analysis using Term Frequency-Inverse Document Frequency (TF-IDF) feature extraction and clustering techniques was conducted on a corpus of 44 documents, comprising 32 peer-reviewed academic publications and 12 industry and government reports, following the methodology described in Section 3.1. The TF-IDF clustering analysis identified seven thematic clusters, each related to a specific dimension of the challenges faced by the transportation cybersecurity workforce. This section provides a critical analysis of the patterns, contradictions, and structural gaps observed in the identified clusters. While the corpus captured a broad range of transportation cybersecurity workforce literature, some transportation subsectors were represented more extensively than others. This limitation is considered when interpreting the findings. The summary of the identified clusters with the corresponding sources is presented in Table 3.

Table 3. Thematic Clusters Identified Through TF-IDF Analysis (N = 44).

Cluster	Theme	<i>n</i>	Representative Sources
0	Maritime Cybersecurity Training	8	[7,25,26]
1	Critical Infrastructure Workforce	6	[27–29]
2	Sector-Specific Training Programs	4	[13,30]
3	Aviation/FAA Workforce	3	[31,32]
4	ITS & Transportation Systems	10	[33–35]
5	Skills Gap & Development	9	[28,36,37]
6	NICE Framework & OT	4	[16,17,38]

4.1.1. Differences in Workforce Maturity and Regulatory Readiness Across Sectors

One key finding from the data cluster analysis is that the transportation sectors differ significantly in their readiness to address cyber threats. Each mode operates under its own regulation, adopts unique technologies, and reaches different levels of workforce maturity. Understanding the differences between sectors is important because a strategy effective in one domain may not be applicable in another.

The maritime sector has received the most immediate regulatory attention. In January 2026, the cybersecurity training mandate for all MTSA-regulated entities issued by the U.S. Coast Guard [26] took effect. The Center for Strategic and International Studies describes this mandate as a catalyst for generational change, backed by \$25 billion in Coast Guard funding [39]. Now that the deadline has passed, the important question is whether the training received will produce long-lasting behavioral changes or merely compliance.

According to the analysis of the literature corpus, there are grounds for concern. In a phishing simulation conducted by GTMaritime [25], 15% of maritime personnel clicked simulated malicious links, a rate three times the global industry average of 2–5%. As 60% of cybersecurity incidents involve humans [40], it is obvious that regulatory compliance alone is far from sufficient to prevent attacks. Kenney & Macdonald [7] support this view, noting that even after increasing investments into cybersecurity, the maritime sector continues to struggle to meet new challenges.

In contrast, the aviation sector faces persistent challenges in developing workforce capacity to support increasingly digitized operational environments. The sector struggles to align cybersecurity with workforces designed for different eras of technology. As identified by The National Academies [31], technological modernization has outpaced workforce development, creating security vulnerabilities in increasingly sophisticated automated systems. This Report (TRB Consensus 341) noted that the FAA's existing workforce was not designed with cybersecurity in mind. Thus, switching to digital infrastructure requires developing competencies different from those possessed by current employees. To fill this gap, multiple NSF-sponsored programs aimed to design aviation-specific talent pipelines through initiatives such as the CyberCorps Scholarship for Service program, focused on securing aviation and aerospace cybersecurity [41]. However, as noted by Murisa & Coetzee [42], recruitment into aviation security operation centers remains difficult due to competition from tech companies offering higher pay scales. In contrast to maritime, where the challenge is translating regulatory compliance into competency, the aviation sector's challenge is creating a new professional identity grounded in a combination of safety and cybersecurity cultures.

Intelligent transportation systems (ITS) comprise the largest group of documents in the corpus ($n = 10$). ITS combines IoT sensors, V2X communication, and autonomous control, creating complex attack surfaces that cannot be addressed with general IT security training [35]. The particular difficulty in the ITS workforce landscape stems from the rapid pace of technology deployment and the slow pace of workforce adaptation. Asaju [33] identifies gaps in the standards for V2X technologies that require skills frequently absent from standardized academic curricula, and Barnes [43] finds knowledge gaps among state and local agencies responsible for maintaining and operating ITS. Overall, ITS faces a growing mismatch between rapidly evolving technologies and existing workforce development programs. Focusing solely on current standards may leave professionals unprepared for threats that lack corresponding standards.

According to ITS America [44], the ITS workforce faces critical gaps in cybersecurity, data analytics, and systems integration, with technology evolving faster than academic programs can adapt their curricula. Grahn et al. [45] further document that career pathways in ITS remain poorly defined, with few structured pipelines connecting academic preparation to the cybersecurity-specific roles that the sector increasingly requires.

Road and surface transportation present workforce challenges that are less visible than those in maritime or aviation but no less consequential. State departments of transportation manage vast networks of highways, bridges, traffic signals, and management centers, yet most lack dedicated cybersecurity personnel. The National Cooperative Highway Research Program (NCHRP) cybersecurity guide for state transportation agency CEOs [46] found

that as physical OT assets become increasingly connected through electronic networks and managed remotely by software, the imbalance between cybersecurity risk and workforce capacity at state DOTs has grown significantly. At the federal level, the U.S. Government Accountability Office [47] reported that TSA had not fully developed its cybersecurity workforce plan for surface transportation modes, and that four of six GAO recommendations to improve transportation cybersecurity remained unimplemented as of November 2024. TSA's proposed rulemaking on surface cyber risk management, issued in November 2024, would require pipeline and rail operators to establish cyber risk management programs and designate cybersecurity coordinators, creating new workforce roles that agencies must fill, but for which no standardized training pipeline yet exists.

At the community level, workforce shortages in surface transportation extend beyond cybersecurity. Peterson & Molina [48] document persistent driver and technical staff shortages in small urban and rural transit agencies, indicating that the broader workforce pipeline feeding into transportation operations is itself constrained. When combined with the cybersecurity imperative, these compounding shortages suggest that road and surface transportation agencies face a dual workforce crisis that neither traditional IT hiring nor general transit recruitment can resolve on their own.

Compared to the other transportation modes discussed above, railway cybersecurity appears to be the least developed. As assessed by Kour & Karim [13], the railway workforce's readiness to address cyber threats remains nascent, with most rail companies aiming for at least a basic level of security. The framework for modular cybersecurity training in maritime, developed by Oruc et al. [49], and the evaluation of the MarCy training program by Oruc et al. [49] can be potentially used in railways. Chupkemi & Mersinas [50] document compliance challenges in maritime that apply with equal force to rail operations. In principle, the railway can benefit from experience in maritime, aviation, and ITS. In practice, the corpus does not identify any mechanism for transferring knowledge between sectors. Every sector develops its own approach to workforce programs in isolation from others.

4.1.2. Entry Barriers and the Workforce Experience Gap

One of the most prevalent themes in the literature is the challenge of entering the transportation cybersecurity workforce. While employers require experienced workers, there is a notable lack of means to gain the necessary experience within the field. Ramezan et al. [17] examined 100 OT cybersecurity job advertisements and summarized the required criteria in Table 4.

Table 4. Operational Technology Cybersecurity Position Requirements ($n = 100$).

Requirement Category	% of Positions
Prior professional experience required	95
Bachelor's degree or higher required	82
Industry certifications (CISSP, GICSP) listed	64
Knowledge of OT/IT frameworks and standards	48
Strong communication skills	48
U.S. security clearance required	24

Note. Adapted from Ramezan et al. [17].

One of the findings from the analysis of OT cybersecurity postings includes that 95% of the job listings require previous professional experience. This creates a cyclical workforce challenge in which candidates are unable to gain experience without employment

opportunities, while employers continue to prioritize prior experience. To help address the challenge, the NICE Framework was designed to standardize work roles, linking academic preparation to employers' expectations [38]. This may be linked to employer risk avoidance, externalities of training investment, the lack of role of industry associations and a lack of institutional solutions like adequate curricula or internships. Ngambeki et al. [16] found that primary cybersecurity curricula fail to adequately prepare individuals for ICS requirements, resulting in graduates lacking the competencies required for cybersecurity roles in the NICE Framework.

In addition, budgetary constraints also create difficulties for employers. ISC2 [28] revealed that, for the first time, budget constraints surpassed qualified talent as the top cause of staffing shortages. This trend continued into 2025, with 33% of organizations reporting they lack the resources to adequately staff their cybersecurity teams [51].

In the sector-wide context, the described situation should be regarded as a market failure. Each organization pursues its own logical goal: demanding experienced personnel and investing neither in recruiting nor in training employees whom competitors can easily poach. As a result, the total labor pool shrinks, and the cost of hiring rises across all organizations in the industry. In transportation, this is especially problematic given the specificity of the tasks involved. While generic work roles may be sufficient for cybersecurity positions, in transport OT jobs, one needs to know about the specific technologies used in the sector (SCADA systems for rail transport, electronic chart display for maritime transport, traffic management center systems for ITS). These competencies cannot be acquired solely through general coursework, yet few internship or apprenticeship programs place cybersecurity students in operational transportation environments. No single employer is likely to break this cycle alone. Coordinated action is needed, whether through subsidized training programs, apprenticeship models, or public-private partnerships that distribute the cost of workforce development across the sector.

4.1.3. Workforce Supply–Demand Imbalance

In addition to the mentioned gap in workforce expertise, there is a general shortage of cybersecurity personnel in the transportation sector, as noted in the corpus. According to the Office of the National Cyber Director [52], the national cybersecurity workforce gap between employer demand and available supply stands at 32%. Regionally, the numbers are equally staggering. As indicated by Crichigno [36], there are over 27,000 unfilled cybersecurity jobs in the Carolinas, despite more graduates having the relevant qualifications. Moreover, according to Grosschmid [37], the maritime transportation sector is less prepared for cybersecurity challenges compared to sectors like banking, implying the same might be true for other transportation means due to common challenges of OT.

The unique aspect of the workforce shortage in the transportation sector relates to its specifics. In the aviation industry, there is a shortage of professionals to integrate cybersecurity into critical systems, which are maintained by engineers with a completely different skill set. In ITS, cybersecurity professionals need experience in securing V2X communications, as there are no curricula to train employees. In the maritime and railway industries, legacy OT systems often rely on decades-old software solutions with insufficient security, requiring approaches beyond those taught in contemporary IT curricula.

4.1.4. Training Innovations

Despite the difficulties involved, several innovative training approaches can offer practical ways forward, according to the literature reviewed. Four intervention approaches seem most relevant.

First, gamification. According to Ashley et al. [27], game-based learning in cybersecurity helps develop skills that are difficult to acquire through traditional classroom instruction. The results of their study demonstrate enhanced engagement and retention through the use of games. For transportation agencies looking to develop cybersecurity skills among employees, gamified training provides a scalable solution that requires minimal time commitment and is adaptable to any scale.

Second, cybersecurity wargaming. Ramon & Mosher [34] introduce an innovative wargaming methodology that enables small ITS teams to conduct cybersecurity exercises without investing in expensive training infrastructure. Given that most state and local transportation agencies lack the resources to build their own cyber ranges, the methodological contribution of this article is particularly relevant. It is adaptable and could be used by transit authorities, ports, and airport authorities if scenarios are appropriately crafted.

Third, federated cyber ranges. The SecAwarenessTruss platform by Smyrlis et al. [53] enables a shared training infrastructure across multiple organizations, thereby reducing the costs of cybersecurity education and training. It is useful for transportation agencies of all sizes, particularly smaller ones, because building in-house infrastructure to conduct cybersecurity exercises is expensive.

Fourth, scholarship programs in the sector. The NSF CyberCorps Aviation and Aerospace program [41] trains cybersecurity students for employment in the transportation sector, while the Infrastructure Investment and Jobs Act [29] provides a federal policy framework for sustaining such investments.

Despite the potential benefits of these approaches, a significant knowledge gap makes it difficult for transportation agencies to make well-informed decisions about investing in their workforce. There are no studies in the corpus that compare these approaches and provide insights into their relative strengths and weaknesses. While transportation agencies looking to invest in their workforce development face the question of choosing among the available training options, there is little to no information to help them make an informed decision. Specifically, there is no information on which strategy is more cost-efficient across organizational sizes, or on the expected results under different conditions.

4.1.5. Findings and Implications for RQ1

Table 5 presents the distribution of themes related to workforce challenges across the seven clusters. Many themes recur across multiple clusters, illustrating the complexity of these challenges. Drawing from all five subsections of this review leads to five conclusions.

Table 5. Cross-Cluster Distribution of RQ1 Workforce Challenge Themes.

Workforce Challenge Theme	Clusters	Documents
Skills Gap & Supply–Demand Imbalance	1, 5, 6	19
Sector-Specific Training Demands	0, 2, 3	15
Curriculum–Industry Misalignment	4, 6	14
Emerging Technology Challenges	1, 4	16
Innovative Training Interventions	1, 2, 4, 5	29

First, regulatory adherence cannot substitute for workforce readiness. The five transportation modes are subject to separate regulations and varying levels of maturity. Maritime faces a Coast Guard-imposed deadline, but it remains vulnerable to social engineering attacks among its staff. The aviation industry is adopting technology faster than it can train its workforce. The ITS sector lacks robust training for the attack surfaces it must contend with. Road and surface transportation agencies lack dedicated cybersecurity staff despite

managing critical OT infrastructure. Meanwhile, the railway is building baseline awareness. Therefore, the approach to workforce challenges must vary between transportation sectors, and generalization should be avoided.

Second, the experience requirement is a problem that cannot be resolved unilaterally. With nearly all OT jobs requiring experience and 82% a degree, capable candidates are blocked from applying. Employers, educators, and government stakeholders each hold complementary solutions, making collaboration mandatory.

Third, emerging technologies create new workforce challenges alongside opportunities. New requirements in the domain of V2X communications, autonomous vehicles, and IoT necessitate competencies that most programs do not cover. However, advances in pedagogy, such as wargames, gamification, and federated cyber ranges, can address this need. The training of the cybersecurity workforce needs to keep pace with changes in the systems it is meant to protect.

Fourth, the lack of cross-sector coordination leads to inefficiencies. All five modes (maritime, aviation, ITS, road/surface transportation, and railways) face similar workforce challenges. Training programs and hiring strategies are devised independently within their sectors, but modular training frameworks already developed for some modes [49] may benefit others. For instance, ITS-specific training, such as wargames [34], could help in securing ports. As a result, the sector as a whole incurs a greater cost than necessary.

Finally, the available literature exhibits certain shortcomings. Most documents in the corpus report workforce challenges without analyzing effective measures against them. Empirical studies, though available, focus on specific programs and organizations with no control groups or follow-up. Many unresolved issues arise in practice: how much cybersecurity training do different jobs require, which teaching methods ensure long-term competency, and what return on investment can be expected. Until better evaluative evidence is produced, agencies will continue making workforce investment decisions with limited empirical guidance. These gaps represent clear opportunities for future research, particularly comparative studies of training effectiveness across transportation modes.

4.2. How Can Universities Best Develop Curriculum, Mentorship, and Awareness Programs to Better Prepare Students for the Cybersecurity Workforce in the Transportation Sector (Qualitative Interviews)?

4.2.1. Aligning Academic Programs with Interdisciplinary Industry Needs

A central finding from the interviews is the urgent need for university cybersecurity programs to better align with the operational needs and realities of the transportation sector. Participants emphasized that curricula often remain too theoretical or overly generalized, failing to integrate the specific challenges, systems and protocols used in transportation environments. Some respondents argued that the slow pace of academia, where curricular updates can take 2–3 years, cannot keep pace with the fast-changing cybersecurity environment found in industry. Respondents suggested that certification programs offered alongside traditional four-year degrees could provide a faster, more targeted way to equip students with specialized skills. One interviewee stated, “When you are creating new programs, you need to clearly align them with what the knowledge, skills and abilities are that the student would need to be successful in that particular field.” Furthermore, participants stressed the importance of training students in both offensive and defensive cyber operations, enabling them to anticipate and respond to a wide range of threats. While acknowledging the importance of current knowledge, TCS faculty also emphasized the need to teach foundational field knowledge, e.g., data science, machine learning, and introductory cybersecurity concepts, thereby balancing basic and applied knowledge.

The participants agreed that workforce readiness requires programs that address both transportation and cybersecurity domains in an integrated, interdisciplinary manner,

rather than focusing on one at the expense of the other. For instance, the University of Houston's Cyber-Care (UTC Transportation Cybersecurity Center for Advanced Research and Education) emphasizes interdisciplinary curricula that integrate the transportation systems engineering program with cybersecurity knowledge.

4.2.2. Recruiting Faculty with Industry Expertise and Exposing Faculty to Industry Work

Another major theme was the call for universities to hire instructors and faculty with up-to-date, hands-on industry experience and the ability to offer project-based courses and certifications. Several interviewees noted that faculty who have spent considerable time in active cybersecurity roles within industry or a government lab bring a practical understanding of current threats, tools, and mitigation strategies that purely academic backgrounds often lack. This approach would ensure that students receive training that is not only theoretically sound but also grounded in the latest industry practices. Respondents also observed that such faculty could serve as valuable bridges between academia and industry, fostering partnerships, collaborative projects, and networking opportunities that can further enhance students' employability. Some respondents suggested that full-time faculty should use their summers to work in industry or government labs, so they can gain insight into industry needs and job/internship opportunities to share with their students.

4.2.3. Building High School Outreach to Attract the Next-Generation Cybersecurity Talent in the Transportation Sector

The participants highlighted strong support for early outreach initiatives to increase awareness of cybersecurity as a viable and rewarding career path. Many interviewees noted that by the time students reach college, some may already have chosen career trajectories unrelated to cybersecurity. Targeted high school programs delivered in partnership with universities, government and industry would introduce students to cybersecurity concepts, demonstrate the societal importance of protecting critical infrastructure and highlight the variety of career opportunities available in the transportation sector. These programs may include cybersecurity demonstrations or games. By sparking interest at an earlier stage, such outreach would help broaden the pool of potential entrants to college cybersecurity programs and the cybersecurity workforce, creating a steady talent pipeline for the transportation sector.

4.2.4. Alumni Networks to Share Opportunities with Students

Interviewees reported that universities should lean on their alumni networks, as many alumni work in industries or government agencies and can offer internships to current students, teach industry-relevant courses at their alma mater, and develop research collaborations with faculty and students.

4.3. *How Can Transportation-Related Government Agencies Design Effective Programs and Sustainable Funding Streams That Would Help Universities Prepare Workforce-Ready Cybersecurity Talent and Assist Employers in the Transportation Sector (Qualitative Interview)?*

4.3.1. Increasing and Sustaining Government Funding

Respondents strongly emphasized the role of government in catalyzing collaboration among government, universities and the transportation industry. Many argued that greater investment in faculty hiring lines, postdoctoral fellowships, doctoral student funding and undergraduate research assistant positions specifically geared toward transportation cybersecurity would help build a sustainable talent pipeline. Such investments using government funds (and to some extent industry funds) would allow universities to undertake long-term, sector-specific projects that respond directly to the transportation sector's challenges. University representatives cite resource constraints as an important reason limiting

their ability to deliver up-to-date TCS programs. More poorly resourced universities have high faculty teaching loads, which reduce their research output and their ability to mentor students seeking skills to enter the TCS industry.

Governments are also expected to provide more job training resources for the private sector. USDOT lists various programs within its Center for Transportation Workforce Development. These include the Transportation Education Development and Deployment program (TEDP), the Garrett A. Morgan Transportation Technology Education program (GAMTTEP), the On-the-Job Training Supportive Services (OJT/SS), and the National Summer Transportation Institutes (NSTI). The Federal Transit Administration (FTA) provides cybersecurity training through the Transportation Safety Institute (TSI) and in partnership with the National Transit Institute (NTI). These and other programs at the state and federal levels need better coordination and communication to be useful and actionable for employers.

4.3.2. Creating Uniform IT/OT and Cybersecurity Standards for Targeted Training

The divide between information technology (IT) and operational technology (OT) has emerged as a persistent challenge that undermines the effectiveness of cybersecurity in transportation. Interviewees noted that many cybersecurity professionals are well-versed in IT systems but lack the specialized training needed to secure OT environments, such as industrial control systems and embedded devices that underpin transportation infrastructure. IT teams are more willing to shut down systems to perform cybersecurity updates and secure organizational data. In contrast, OT teams want to minimize damage to the physical infrastructure or harm to product users and oppose shutdowns. This gap in approaches highlights a fundamental challenge: cybersecurity practices from the IT environments often do not translate smoothly into OT environments without disrupting critical production processes.

As a result, participants advocated for government-led initiatives to establish uniform standards that define essential competencies for bridging IT and OT security, as well as the broader required cybersecurity skills. The NIST competency standards are designed to assist non-IT transportation engineers in developing cybersecurity knowledge, thereby enabling clearer lines of communication with IT staff. Industry, in turn, should develop streamlined training programs to ensure these competencies are met, thereby increasing the interoperability and effectiveness of cybersecurity solutions across different operational contexts in the transportation sector. Government standards are important for universities seeking to develop curricula that provide industry-ready knowledge. For example, Clemson University has partnered with the Aviation Technician Education Council (ATEC) to develop a 2-year curriculum aligned with Federal Aviation Administration (FAA) standards that immediately qualifies graduates for technician and cybersecurity jobs.

4.4. *How Can the Transportation Industry Develop Effective Recruitment Programs for Cybersecurity-Related Roles Through Scholarships, Workshops/Conferences, Internships, or Co-Op Opportunities (Qualitative Interviews)?*

4.4.1. Offering Industry Curricula That Complement University Programs

Industry organizations can play a critical role in strengthening transportation cybersecurity workforce development by collaborating with universities to design and deliver industry-aligned curricula, experiential learning opportunities, and applied technical training. Such partnerships help bridge the gap between academic preparation and rapidly evolving workforce requirements in cybersecurity, operational technology (OT), intelligent transportation systems (ITS), and critical infrastructure protection.

University–industry partnerships can support curriculum modernization through applied coursework, industry-informed training modules, guest lectures, internships,

mentorship programs, cybersecurity laboratories, and experiential learning opportunities. These collaborative initiatives can help universities align cybersecurity education more closely with transportation-sector operational needs while simultaneously enabling transportation and cybersecurity organizations to identify, recruit, and develop future workforce talent.

Within the transportation cybersecurity sector, collaborative curriculum development initiatives may also help address persistent workforce gaps in IT/OT integration, transportation operational technologies, cybersecurity governance, infrastructure resilience, and sector-specific cybersecurity preparedness.

4.4.2. Expanding Internship Opportunities for Students in the Transportation Sector

Participants consistently highlighted the importance of internship programs as a bridge between academic training and professional jobs in industry and government. Internships provide students with first-hand exposure to the complexities of cybersecurity in transportation systems, allowing them to apply classroom knowledge to real-world scenarios and opening the door to their first industry job post-graduation.

While the industry has the responsibility to offer and fund such internship opportunities, universities are also expected to ease their students' entry into internships. Some participants support requiring students to complete an internship as part of the college degree program. Respondents recommended that universities and their career centers take a proactive role in seeking partnerships with government and industry in the transportation sector to expand and diversify internship opportunities. Such programs would not only build technical skills but also help students develop the professional competencies, teamwork abilities and sector-specific insights and skills necessary for long-term career success in the field. Many internships come from word of mouth through faculty with industry connections, which demonstrates the importance of faculty industry experience. University career centers should organize career fairs, inviting national and local employers. Transportation Studies departments should host seminars with industry representatives to expose students to such industry opportunities.

4.4.3. Elevating Cybersecurity as a Core Business Priority

Industry stakeholders in the study described a prevailing perception of cybersecurity as an operational burden rather than a strategic necessity. This mindset often results in underinvestment, delayed responses and reactive rather than proactive measures. Interviewees argued for a cultural shift within transportation companies, framing cybersecurity not as a cost center but as an essential safeguard against business disruption, data breaches and reputational damage.

Several interviewees noted that negative incidents, such as the hijacking of a transportation company's data, prompt businesses to pay more attention to cybersecurity than to foresight and prevention. Interviewees argued that it should not be only the CISO (chief information security officer), but also the CEO and other executives who should care about proactive cybersecurity measures. Prioritizing cybersecurity in this manner would encourage more robust workforce-oriented programs, better risk management practices and earlier adoption of innovative defenses that could prevent costly incidents. Governments can elevate cybersecurity as a business priority by creating regulations that drive business compliance and demand for TCS talent.

4.4.4. Removing Intellectual Property Barriers

Academic respondents reported dissatisfaction with the industry, which is unwilling to collaborate with academics due to restrictions on sharing intellectual property with universities. If there were formal and informal agreements between industry and univer-

sity that pre-empt IP disputes, it would clear a major obstacle toward university–industry collaboration on TCS-related projects. Faculty also noted the limitations of using simulations and hypothetical scenarios in TCS research and would benefit from data sharing with industry to produce more actionable research and expose their students to solving industry problems.

4.5. How Can Academia, Government, and Industry Effectively Collaborate to Improve the Cybersecurity Talent Pipeline in Transportation Systems (Qualitative Interviews)?

4.5.1. Focusing on the Strengths Across the Three Stakeholders

The interviewees stated that academia, government, and industry should leverage their respective resources and capabilities to strengthen the transportation cybersecurity systems (TCS) workforce development. Participants noted that universities play a key role in identifying talent among undergraduate and graduate students while providing foundational training, career services, research opportunities, and industry and government partnerships. Government agencies were viewed as essential for funding workforce initiatives, supporting research, developing national cybersecurity standards, and promoting transportation-sector resilience. Industry organizations were identified as important contributors through internships, workforce training, mentorship, applied research partnerships, and operational expertise related to TCS challenges.

While some participants believed that existing informal collaboration networks among academia, government, and industry were sufficient, others advocated for more formalized coordination mechanisms, including national conferences, collaborative workforce-development initiatives, and structured partnerships to exchange best practices and provide students with direct exposure to potential employers across government and industry sectors.

4.5.2. Emphasizing Workforce Development as a Key Performance Indicator

Interviewees across all sectors consistently emphasized that workforce development should be treated as a key performance indicator in transportation cybersecurity companies and university programs. They argued that the federal government has a responsibility to set this priority and hold all relevant actors, including universities, training institutions, and private industry, accountable for both cultivating new talent and ensuring retention within the field. By embedding workforce development into performance measurement, stakeholders believed it would create stronger incentives for sustained investment in education, upskilling, and career pathways that address the persistent shortage of qualified cybersecurity professionals in the transportation sector.

4.5.3. Harnessing Professional Associations for Workforce Development

Beyond the roles of industry, universities, and government, interviewees highlighted the value of leveraging professional associations such as the American Association of State and Highway Transportation Officials (AASHTO) to advance workforce development in transportation cybersecurity. These organizations play a critical role in shaping best practices for cybersecurity skill-building and serve as connectors between education and employment. Their internal job boards, in particular, were seen as valuable resources for recent graduates and job seekers, providing direct access to career opportunities while reinforcing the professional standards and competencies needed in the sector.

4.5.4. Interview Limitations

This study employed purposive sampling to recruit participants with expertise in transportation cybersecurity, workforce development, critical infrastructure protection, and related disciplines. While this approach facilitated the collection of informed, experience-based perspectives, the findings may not be fully representative of all stakeholder groups

in the transportation sector. The interview sample size was relatively modest and included participants from academia, industry, and government; however, certain transportation modes, organizational types, and geographic regions may be underrepresented.

As with most qualitative research, the findings are subject to potential response and interpretation biases. Participants may have emphasized challenges and priorities most relevant to their professional experiences, and responses may reflect evolving workforce and organizational conditions at the time of data collection. To enhance the trustworthiness of the findings, the study employed semi-structured interview protocols, systematic thematic analysis, peer review of coding decisions, and an audit trail documenting analytical procedures.

The purpose of the interviews was not to generate statistically generalizable conclusions but to obtain expert insights to identify emerging workforce challenges, preparedness gaps, competency requirements, and collaborative strategies within the transportation cybersecurity domain. Future research involving larger, more diverse stakeholder populations, longitudinal data collection, and sector-specific analyses would further strengthen the understanding of transportation cybersecurity workforce needs and organizational preparedness.

4.6. To What Extent Does Self-Assessed Cybersecurity Preparedness Align with the Adoption of Formal Cybersecurity Practices Among U.S. Public Transit Agencies (Survey)?

The analysis of the Mineta Transportation Institute (MTI) survey is presented here. Self-assessed preparedness and CPI were strongly and positively correlated (Spearman $\rho = 0.702$, $p < 0.001$, $N = 75$). In the 2024 data, the mean CPI increased with each level of perceived preparedness: from 3.7 (standard deviation (SD) = 7.3) at level 1 to 77.8 (SD = 22.8) at level 5 (see Table 6 below). This association was not an artifact of agency size. Within-tier Spearman correlations remained significant for small agencies ($\rho = 0.717$, $p < 0.001$, $n = 27$), mid-sized agencies ($\rho = 0.469$, $p = 0.043$, $n = 19$), and large agencies ($\rho = 0.682$, $p < 0.001$, $n = 28$). A partial Spearman correlation controlling for budget tier was $\rho = 0.662$ ($p < 0.001$). With the size, staffing, and leadership gradients reported in Section 4.7, this association provides supportive convergent and known-groups validity evidence for the CPI as a formative measure.

Table 6. Mean CPI by Self-Assessed Preparedness Level (2024 Data) [3].

Preparedness Level	<i>n</i>	Mean CPI	SD CPI
1 (Not prepared at all)	9	3.7	7.3
2	9	15.9	20.2
3	24	39.6	32.2
4	27	72.2	26.1
5 (Very prepared)	6	77.8	22.8

The quadrant classification indicated that the majority of agencies were perceptually aligned with their practice levels. Thirty-one agencies (41.3%) were classified as aligned-low: they reported low perceived preparedness and had low CPI scores. Twenty-eight agencies (37.3%) were aligned at the high level. Only five agencies (6.7%) were classified as overconfident (high perceived preparedness but CPI below 50), while eleven (14.7%) were classified as underconfident. The association between the two dimensions was statistically significant ($\chi^2 = 23.18$, $p < 0.001$). A sensitivity analysis using a stricter CPI cutoff (>50 instead of ≥ 50) yielded a similar pattern: total alignment was 80%, and overconfident agencies rose modestly to 7 (9%). An ordered logistic regression confirmed that CPI

significantly predicted self-assessed preparedness after controlling for agency budget tier (coefficient = 0.051, $z = 5.49$, $p < 0.001$, $N = 74$). The budget tier was not significant after accounting for CPI.

The preparedness–practice relationship was also observed in the 2020 public-file sample, though with a weaker association (Spearman $\rho = 0.373$, $p < 0.001$, $N = 103$). The 2020 pattern was similar but not strictly monotonic at the highest preparedness level (level 5, $n = 5$), reflecting the instability of small-cell estimates. The weaker 2020 correlation may also reflect the more homogeneous composition of that sample (predominantly large, urban agencies), which limits variance. These cross-year differences should be interpreted with caution, as the samples differ in composition and the instruments changed between waves, making interpretation of temporal trends difficult.

4.7. To What Extent Are Organizational Characteristics, Specifically Agency Size, Cybersecurity Staffing, and Leadership Structure, Associated with the Level of Formal Cybersecurity Practice Adoption (Survey)?

Agency size. CPI differed significantly across the three budget tiers (Kruskal–Wallis $H = 17.84$, $p < 0.001$). Agencies with budgets above \$50 million had a mean CPI of 64.3 ($SD = 34.2$), compared to 54.9 ($SD = 31.4$) for mid-sized agencies (\$5 M–\$50 M) and 25.3 ($SD = 31.1$) for small agencies (<\$5 M). The effect size for the smallest-versus-largest comparison was large (Cohen’s $d = 1.19$). Mid-sized and large agencies did not differ significantly from each other ($p = 0.268$), but both differed significantly from small agencies ($p \leq 0.002$).

Individual practice adoption by size. Size-based disparities were present across all six CPI practices and both workforce indicators, except for log retention (Table 7). After FDR correction, the largest gaps between the smallest (<\$5 M) and largest (>\$50 M) agencies were: certified cybersecurity staff (5% vs. 95%), annual training (14% vs. 79%), cybersecurity FTE (23% vs. 86%), and cybersecurity policy (26% vs. 75%). Log retention showed no significant size differential (37% vs. 36%).

Table 7. Practice Adoption Rates by Agency Budget Tier (2024 Data) [3].

Practice	All	<\$5 M	\$5 M–\$50 M	>\$50 M	p (FDR)
Core Practice Index items					
Cybersecurity policy	55%	26%	65%	75%	<0.001
Incident response plan	46%	22%	45%	71%	<0.001
Audit/accountability	46%	37%	45%	57%	0.206
Vendor contract clauses	44%	19%	47%	68%	<0.001
Log retention ≈ 1 yr+	38%	37%	44%	36%	1.00
Annual training	55%	14%	84%	79%	<0.001
Workforce indicators					
Certified cybersecurity staff	52%	5%	67%	95%	<0.001
Any cybersecurity FTE	54%	23%	50%	86%	<0.001

Note. p -values are from Fisher’s exact tests comparing agencies < \$5 M versus >\$50 M, adjusted using Benjamini–Hochberg FDR.

Cybersecurity FTE. The presence of at least one cybersecurity FTE was the strongest differentiating factor. Agencies with any cybersecurity FTE had a mean CPI of 69.7 ($n = 38$), compared to 20.4 ($n = 34$) for agencies with zero cybersecurity FTEs (Mann–Whitney $U = 1140$, $p < 0.001$, Cohen’s $d = 1.83$).

Regression models. Two OLS models were estimated on the same 71-agency sample to enable direct comparison (Table 8). Model A, with the budget tier alone, explained 26%

of the variance ($R^2 = 0.258$). Model B added cybersecurity FTE presence; the explained variance increased to 50% ($R^2 = 0.504$, $\Delta R^2 = 0.246$). In Model B, cybersecurity FTE presence was the strongest correlate of CPI in the model ($\beta = 43.4$, $p < 0.001$): agencies with any cybersecurity FTE scored approximately 43 points higher on the 0–100 CPI, controlling for budget tier. The large-agency budget coefficient, which was significant in Model A ($p < 0.001$), became non-significant in Model B ($p = 0.125$), while the mid-sized coefficient remained significant ($p = 0.015$). This suggests that workforce capacity accounts for a substantial share of the size gradient, particularly at the upper end of the agency size distribution. Since dedicated cybersecurity staffing both reflects and reinforces organizational capacity, we interpret the FTE indicator as an observable proxy for broader organizational commitment rather than as an isolated causal driver, and the cross-sectional design does not allow us to exclude reverse causality or self-selection.

Table 8. OLS Regression Models of CPI.

Covariate	Model A	Model B
Intercept	22.5 (5.7) ***	7.0 (6.3)
Budget \$5 M–\$50 M	31.4 (9.9) **	21.0 (8.7) *
Budget > \$50 M	41.2 (8.8) ***	14.0 (9.2)
Has cybersecurity FTE	n/a	43.4 (8.1) ***
R^2	0.258	0.504
ΔR^2	n/a	0.246

Note. Entries are β (HC3 robust SE). Reference: budget < \$5 M, no cybersecurity FTE. * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$. Both models were estimated on the same 71 agencies with non-missing CPI, budget, and FTE data.

A quasi-binomial GLM robustness check confirmed the OLS pattern: FTE remained strongly significant (log-odds = 1.980, $p = 0.002$) while the large-budget coefficient was attenuated ($p = 0.317$). A source-file sensitivity analysis adding a large/small file indicator showed that the FTE effect was unchanged ($\beta = 43.4$, $p < 0.001$) and the source indicator was non-significant ($p = 0.836$), indicating that file-level differences do not drive the findings.

Cybersecurity leadership. Among the 53 agencies with available data on cybersecurity leadership structure, CPI differed significantly by leadership type (Kruskal–Wallis $H = 20.90$, $p < 0.001$). Agencies with a dedicated CISO or equivalent had a mean CPI of 79.2 ($n = 20$); those with shared cybersecurity responsibility, 44.2 ($n = 24$); and those with no one assigned, 11.1 ($n = 6$). These results should be interpreted with caution, as the CISO variable was available for only 53 of 78 agencies, predominantly from the large-agency file.

4.7.1. Additional Survey Findings

Practice prevalence among low-adoption agencies. Among the 74 agencies with complete CPI data, the distribution of adopted practices was concentrated at the extremes: 17 agencies (23%) had adopted 0 of the 6 practices. In contrast, 26 (35%) had adopted five or all six. Among agencies with 1–3 practices ($n = 24$), annual training was the most commonly observed practice (54%), followed by log retention (33%), cybersecurity policy (29%), audit (25%), vendor contract clauses (25%), and incident response plan (12%). This pattern suggests that training may be the most accessible entry point for agencies beginning to build cybersecurity governance, while incident response planning may require greater organizational maturity.

Cybersecurity assessment validity. Of the 57 agencies reporting on assessment practices, 35 (61%) reported conducting cybersecurity assessments at least annually. However, among these 35 agencies, only 16 (46%) were identified as using a recognized cybersecurity

assessment tool (e.g., the CISA Cyber Resilience Review or the FTA Cybersecurity Assessment Tool for Transit). The remaining 19 (54%) either could not name the tool or listed tools that are not cybersecurity assessment instruments. This classification is based on a derived variable in the public data file; the raw assessment tool names and classification criteria are documented in the analysis code.

Cyber Insurance. Among 75 agencies with available data, 56 (75%) reported having cyber insurance. Among insured agencies reporting premium changes relative to three years prior, 22 of 32 (69%) reported premium increases. Seven agencies (9% of 77 respondents) reported experiencing a cybersecurity incident.

4.7.2. Survey Limitations

Several limitations apply to this analysis. Both datasets are convenience samples from APTA, AASHTO, and CTAA membership networks and may not represent all U.S. transit agencies. As a secondary analysis, this study did not design, administer, or distribute the survey instruments; original data collection and distribution were conducted by MTI, and sample sizes were fixed by the original studies, precluding an a priori power analysis. The CPI is a formative index of self-reported practice adoption rather than an objective audit or a reflective psychometric scale. The sample size ($N = 78$ in 2024) limits the complexity of multivariate models. The two 2024 sub-files differ in agency composition and variable availability; analyses of advanced organizational variables (e.g., CISO structure) are effectively restricted to the large-agency file. Cross-year comparisons between the 2020 and 2024 datasets are descriptive only, as the samples differ in composition and the instruments changed between waves. All associations are cross-sectional and should not be interpreted as causal effects; in particular, the strong association between FTE and CPI may partly reflect self-selection, as agencies with greater security awareness may be more likely to both establish a dedicated cybersecurity FTE and adopt formal practices. The datasets also contain no measures of threat environment, risk exposure, regulatory context, or rural versus urban setting. The observed budget-tier differences in CPI cannot be attributed solely to organizational capability, as they may also reflect differences in risk exposure or regulatory demand. The CPI captures practice adoption rather than its sufficiency for a given agency's risk profile.

4.7.3. Implications of the Survey Findings

First, overconfidence about cybersecurity preparedness appears uncommon among transit agencies. The more prevalent pattern is recognized under-preparedness combined with low adoption of foundational practices: 41% of agencies accurately perceive that they are not prepared; however, they have not adopted basic cybersecurity governance measures. This suggests that awareness is not the primary barrier; agencies need tangible organizational capacity-building support to translate awareness into action.

Second, small transit agencies (operating budgets below \$5 million) lag behind their larger peers in nearly every measured cybersecurity practice. Only 14% conduct annual cybersecurity training, only 5% have any staff member with a cybersecurity certification, and only 23% have a dedicated cybersecurity FTE, compared to 79%, 95%, and 86%, respectively, among agencies with budgets above \$50 million.

Third, the presence of at least one dedicated cybersecurity FTE is the strongest observable marker of organizational cybersecurity capacity. Agencies with any cybersecurity FTE score approximately 50 points higher on the practice adoption index. When FTE is included in regression models alongside budget tier, the explained variance nearly doubles (R^2 from 0.258 to 0.504 on the same sample), and the effect of large budget substantially weakens. This pattern suggests that workforce capacity accounts for a substantial share of

the size gradient in cybersecurity practice adoption, though the cross-sectional design does not permit causal inference.

These organizational-level findings reinforce the interview themes presented in Sections 4.2–4.5 and provide quantitative evidence that workforce development in transit cybersecurity is not only an individual skills issue but also an organizational staffing and implementation-capacity issue. The data suggest that workforce development interventions that focus solely on training and credentialing may need to be complemented by efforts to establish dedicated cybersecurity roles within transit organizations, particularly at small and rural agencies, where the workforce gap is most acute.

5. Discussion

The findings from the text analysis (Section 4.1), qualitative interviews (Sections 4.2–4.5), and organizational survey analysis (Sections 4.6 and 4.7) collectively demonstrate that the shortage of transportation cybersecurity talent is driven by broader workforce development, organizational, and systems coordination challenges. Transportation systems operate within highly interconnected cyber–physical environments where cybersecurity failures may directly affect operational continuity, public safety, infrastructure resilience, and public trust. Consequently, developing a qualified transportation cybersecurity workforce requires more than traditional cybersecurity training. It must incorporate transportation-specific operational knowledge, organizational preparedness, interdisciplinary collaboration, and the integration of information technology and operational technology competencies. These challenges continue to hinder the development of a sustainable pipeline of cybersecurity professionals capable of securing modern transportation systems.

The findings further underscore the critical role of organizational capacity in shaping cybersecurity preparedness across transportation agencies. Survey findings indicate that agencies with dedicated cybersecurity personnel exhibit higher adoption of formal cybersecurity practices and greater preparedness. In contrast, small and rural transit agencies remain particularly vulnerable due to resource limitations, staffing shortages, and limited access to specialized cybersecurity expertise. These disparities are consistent with differences in organizational capacity and staffing, although unmeasured differences in threat exposure, operating context, and regulatory requirements may also contribute and cannot be ruled out with the present data. These findings suggest that workforce-development strategies should extend beyond training individual professionals to include investments in cybersecurity leadership, staffing structures, governance frameworks, and long-term institutional capacity building.

Another important implication concerns the persistent divide between information technology and operational technology environments within transportation systems. Interview participants emphasized that many cybersecurity professionals possess strong information technology backgrounds but lack transportation-specific operational technology competencies required to secure intelligent transportation systems, connected infrastructure, rail signaling systems, industrial control systems, and other cyber–physical transportation technologies. As transportation systems continue to adopt automation, connectivity, and smart infrastructure technologies, workforce development programs must evolve to bridge these interdisciplinary competency gaps through integrated training, applied learning, and transportation-focused cybersecurity education.

The findings also reinforce the importance of sustained collaboration among academia, industry, and government to strengthen the capacity of the transportation cybersecurity workforce. Universities play a critical role through interdisciplinary curriculum development, experiential learning opportunities, internships, cyber ranges, research partnerships, and industry-aligned instruction. Government agencies remain essential in supporting

workforce development initiatives, funding transportation cybersecurity education and research, and promoting long-term policy coordination.

Industry organizations contribute operational expertise, internship pathways, mentorship opportunities, and practical workforce-development experiences that help align academic preparation with real-world transportation cybersecurity challenges. Stronger coordination across these sectors is essential to developing sustainable cybersecurity workforce pipelines capable of protecting increasingly digital and interconnected transportation systems.

Figure 1 presents an integrated transportation cybersecurity workforce framework derived from the study's findings. The framework illustrates how external drivers—including transportation digitalization and connectivity, IT/OT convergence, evolving cyber threats, regulatory and policy requirements, and transportation cybersecurity workforce shortages and skills gaps—create the need for cross-sector collaboration among academia, industry, and government. Through organizational capacity building and the development of transportation-specific cybersecurity competencies, these collaborative efforts contribute to a skilled interdisciplinary transportation cybersecurity workforce capable of strengthening organizational cybersecurity preparedness and resilience.

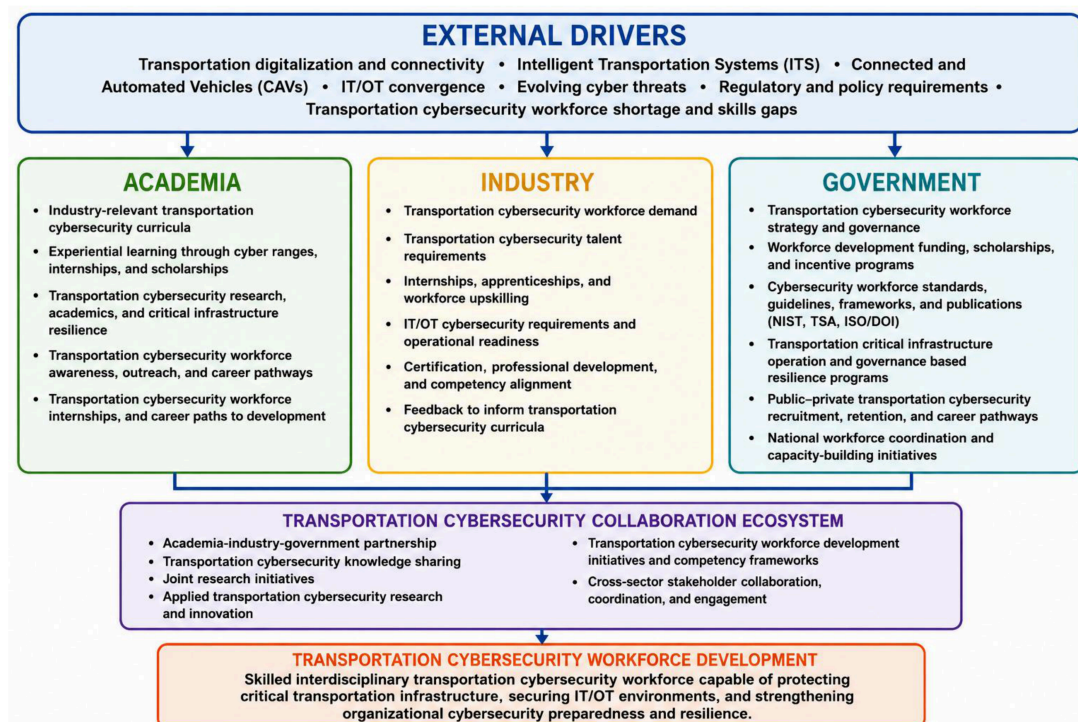


Figure 1. Transportation Cybersecurity Workforce Development Framework.

6. Critical Analysis, Limitations and Future Research

This study makes a valuable contribution by adopting a multi-method approach—combining text analysis of webscraped documents, stakeholder interviews, and MTI survey data—to examine the transportation cybersecurity workforce shortage, thereby addressing a notable gap in the transportation cybersecurity literature. Its strength lies in the holistic framing that moves beyond generic cybersecurity training to emphasize the unique demands of cyber-physical transportation environments, the IT/OT divide, and the disproportionate vulnerabilities faced by small and rural agencies. The proposed conceptual framework synthesizing cross-sector collaboration, organizational capacity, and specialized

competencies provides a practical roadmap for workforce development and transportation cybersecurity preparedness.

A critical implication of the findings is that transportation cybersecurity workforce shortages should not be viewed solely as an education and training problem; rather, they reflect broader organizational capacity, governance, staffing, and preparedness challenges that require coordinated action across academia, industry, and government. The findings further suggest that workforce-development initiatives focused exclusively on education, training, and certifications may be insufficient unless accompanied by organizational investments in cybersecurity staffing, leadership, governance, and long-term institutional capacity building.

Several limitations should be considered when interpreting these findings. First, although the study employed a mixed-methods design that integrated computational text analysis, qualitative interviews, and organizational survey data, each component contains inherent limitations related to sample composition, data availability, and generalizability. Second, the interview sample was purposive and relatively small, limiting the representativeness of perspectives across academia, industry, government, and transportation operators within the broader transportation cybersecurity ecosystem. Third, the survey findings are based on convenience samples and cross-sectional data, precluding causal inference and limiting the ability to assess changes over time. Finally, transportation cybersecurity continues to evolve rapidly, and workforce requirements may change as emerging technologies, operational environments, threat landscapes, and regulatory frameworks mature.

Future research should focus on developing and evaluating domain-specific workforce-development frameworks, transportation-focused cybersecurity curricula, experiential learning models, and technical training approaches that address the unique security requirements of transportation operational technology environments. Future studies should aim to expand sample size and diversity, including greater participation from private-sector operators, smaller transit agencies, and professionals across different regions to enhance the generalizability of results. Additional longitudinal studies are needed to assess the effectiveness of workforce-development interventions and organizational preparedness initiatives over time. Future research should also examine workforce challenges across specific transportation modes, including transit, rail, aviation, maritime, and connected and automated vehicle environments, to better understand sector-specific competency requirements and workforce-development needs. Future research should also evaluate the effectiveness of these interventions in improving workforce outcomes, organizational preparedness, and transportation cybersecurity resilience.

Overall, the study demonstrates that developing a resilient transportation cybersecurity workforce requires systemic, interdisciplinary, and collaborative approaches rather than isolated training efforts. Strengthening transportation cybersecurity resilience will require sustained strategic investment, workforce innovation, organizational capacity building, and long-term cross-sector coordination to protect increasingly digital and interconnected transportation systems.

7. Conclusions

This article highlights an urgent and growing challenge: the shortage of qualified cybersecurity professionals to protect the nation's transportation infrastructure. As transportation systems become increasingly interconnected and dependent on complex information technology and operational technology environments, the demand for transportation-specific cybersecurity expertise will continue to intensify. The vulnerabilities in transportation cybersecurity become more acute in the era of connected transportation ecosys-

tems, smart mobility infrastructure, and cutting-edge technologies such as driverless or autonomous vehicles. The findings from the textual analysis, qualitative interviews, and organizational survey analysis demonstrate that transportation cybersecurity workforce shortages are influenced by broader organizational, technological, and workforce-development challenges that hinder the creation of a sustainable cybersecurity talent pipeline.

The findings further demonstrate that strengthening transportation cybersecurity workforce capacity requires sustained collaboration among academia, industry, and government to better align workforce preparation with the evolving cybersecurity needs of transportation systems. This includes interdisciplinary curriculum development, expanded experiential learning opportunities, stronger internship and mentorship pathways, organizational investment in dedicated cybersecurity staffing, and improved integration of information technology and operational technology security competencies into workforce development programs. In addition, the findings indicate that small and rural transit agencies require additional organizational support and workforce resources to strengthen cybersecurity preparedness and implement foundational cybersecurity practices.

Ultimately, strengthening transportation cybersecurity resilience requires sustained strategic investment, interdisciplinary collaboration, organizational capacity-building, workforce innovation, and long-term cross-sector coordination to develop a qualified cybersecurity workforce capable of protecting increasingly digital and interconnected transportation systems.

Author Contributions: Conceptualization, A.A., L.L., and S.U.; methodology, A.A. and S.U.; software, F.A. B.O., and A.A.; validation, A.A. and S.U.; formal analysis, A.A. and F.A.; investigation, A.A. and L.L.; resources, A.A. and S.U.; data curation, A.A., L.L., and E.K.; writing—original draft preparation, A.A. and L.L.; writing—review and editing, A.A., L.L., S.U., C.A., F.A., E.K., B.O. and S.M.; visualization, A.A. and L.L.; supervision, L.L. and S.U.; project administration, A.A. and S.U.; funding acquisition, A.A. and S.U. All authors have read and agreed to the published version of the manuscript.

Funding: This research is supported by the National Center for Transportation Cybersecurity and Resiliency (TraCR), a U.S. Department of Transportation National University Transportation Center headquartered at Clemson University, Clemson, South Carolina, USA., under Prime Award No. 69A3552344812. This work was conducted under Subaward No. 2588-211-2026310. Any opinions, findings, conclusions, and recommendations expressed in this material are those of the authors and do not necessarily reflect the views of TraCR, and the U.S. Government assumes no liability for the contents or use thereof.

Institutional Review Board Statement: The study was conducted in accordance with the Declaration of Helsinki and approved by the Institutional Review Board of Morgan State University on 18 February 2025 (IRB #25/02-0034).

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: Publicly available datasets were analyzed in this study. The Mineta Transportation Institute (MTI) cybersecurity survey datasets used in the study are publicly available through MTI. Interview data are not publicly available due to privacy and confidentiality considerations. Additional materials may be available from the corresponding author upon reasonable request.

Acknowledgments: The authors acknowledge the support of the National Center for Transportation Cybersecurity and Resiliency (TraCR) and the participating experts and professionals who contributed to the interview component of this study. During the preparation of this manuscript, the authors used generative AI tools, including ChatGPT (OpenAI, GPT-5.5) and Grok (xAI, Grok 4), for language refinement and editorial support. All AI-assisted content was reviewed, revised, and validated by the authors, who take full responsibility for the accuracy, integrity, and originality of the manuscript.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Appendix A

Table A1. Interview Participant Categories.

Interview Subject No.	Occupation
1	Professor, Industrial Engineering
2	Professor, Transportation and Urban Infrastructure
3	Chief Executive Officer, Technology Industry
4	Postdoctoral Associate, Computer Science
5	Organizational Cybersecurity Development and Training Strategist
6	Professor, Civil, Construction, and Environmental Engineering
7	Principal Advisor, Government Transportation Agency
8	Transportation Law and Policy Analyst
9	Transportation Specialist, Government Transportation Agency
10	Professor, Computer Science
11	Professor, Computer Science
12	Professor, Transportation Studies
13	Vice President for Research and Economic Development
14	Professor, Industrial and Systems Engineering
15	Professor, Cybersecurity Engineering
16	Professor, Computer Science

Note: The interview participants represented academia, government, transportation, engineering, cybersecurity, policy, and industry sectors. Participant identities were anonymized in accordance with the approved Institutional Review Board (IRB) protocol and research ethics requirements.

References

1. Christiansen, B.; Piekarz, A. (Eds.) *Global Cybersecurity Labor Shortage and International Business Risk*; IGI Global: Hershey, PA, USA, 2018.

2. Belcher, S.; Belcher, T.; Greenwald, E.; Thomas, B. *Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness*; MTI Report 20–36; Mineta Transportation Institute: San Jose, CA, USA, 2020. [CrossRef]

3. Belcher, S.; Belcher, T.; Grimes, J.; Holmstrom, L.; Souders, A. *Does the Transit Industry Understand the Cybersecurity Risks, and Are They Being Appropriately Prioritized*; Mineta Transportation Institute: San Jose, CA, USA, 2025. [CrossRef]

4. Amin, M. Toward secure and resilient interdependent infrastructures. *J. Infrastruct. Syst.* **2002**, *8*, 67–75. [CrossRef]

5. SCB. *Over 60% of Logistics Companies Are Investing in Supply Chain Management Systems*; Supply Chain Brain: Peconic, NY, USA, 2023.

6. Sardarabady, N.J.; Durst, S. A systematic literature review on the economic impact of digitalization technologies in transport logistics. *Transp. Econ. Manag.* **2024**, *2*, 76–89. [CrossRef]

7. Kenney, M.; MacDonald, F. *Shifting Tides, Rising Ransoms and Critical Decisions*. Thetius. 2023. Available online: https://cyberowl.io/wp-content/uploads/2023/10/CyberOwl_HFW_Thetius-Cyber-Security-Report-2023-Shifting-Tides-Rising-Ransoms.pdf (accessed on 12 May 2026).

8. Probiez, B.; Kozak, J.; Hrabia, A. Clustering of scientific articles using natural language processing. *Procedia Comput. Sci.* **2022**, *207*, 3449–3458. [CrossRef]

9. Bureau of Labor Statistics. *Fastest-Growing Occupations*. 2024. Available online: <https://www.bls.gov/ooh/fastest-growing.htm> (accessed on 12 May 2026).

10. Nguyen, P. *Gig Economy and Cybersecurity Talent Shortage: Bridging the Gap*. Doctoral Dissertation, Marymount University, Arlington, VA, USA, 2024.

11. Beuran, R.; Chinen, K.-I.; Tan, Y.; Shinoda, Y. *Towards Effective Cybersecurity Education and Training*; Japan Advanced Institute of Science and Technology: Nomi, Japan, 2016.
12. Furnell, S. The cybersecurity workforce and skills. *Comput. Secur.* **2021**, *100*, 102080. [CrossRef]
13. Kour, R.; Karim, R. Cybersecurity workforce in railway: Its maturity and awareness. *J. Qual. Maint. Eng.* **2021**, *27*, 453–464.
14. Okolo, F.C.; Etukudoh, E.A.; Ogunwole, O.; Osho, G.O.; Basiru, J.O. A conceptual model for balancing automation, human oversight, and security in next-generation transport systems. *J. Front. Multidiscip. Res.* **2023**, *4*, 188–198. [CrossRef]
15. DiBiase, D.; Corbin, T.; Fox, T.; Francica, J.; Green, K.; Jackson, J.; Jeffress, G.; Jones, B.; Jones, B.; Mennis, J.; et al. The new geospatial technology competency model: Bringing workforce needs into focus. *URISA J.* **2010**, *22*, 55–66.
16. Ngambeki, I.; McBride, S.; Slay, J. Knowledge gaps in curricular guidance for ICS security. *J. Colloq. Inf. Syst. Secur. Educ.* **2022**, *9*, 6. [CrossRef]
17. Ramezan, C.A.; Coffy, P.M.; Lemons, J. Building the operational technology (OT) cybersecurity workforce: What are employers looking for? *J. Cybersecur. Educ. Res. Pract.* **2024**, *2024*, 6.
18. SANS Institute. SANS 2024 State of ICS/OT Cybersecurity. 2024. Available online: <https://www.sans.org/white-papers/sans-2024-state-ics-ot-cybersecurity> (accessed on 12 May 2026).
19. Christian, H.; Agus, M.P.; Suhartono, D. Single document automatic text summarization using term frequency–inverse document frequency (TF-IDF). *ComTech Comput. Math. Eng. Appl.* **2016**, *7*, 285–294.
20. Braun, V.; Clarke, V. Using thematic analysis in psychology. *Qual. Res. Psychol.* **2006**, *3*, 77–101. [CrossRef]
21. Glaser, B.G.; Strauss, A.L. *The Discovery of Grounded Theory: Strategies for Qualitative Research*; Aldine Publishing Company: Chicago, IL, USA, 1967.
22. Lincoln, Y.S.; Guba, E.G. *Naturalistic Inquiry*; Sage: Thousand Oaks, CA, USA, 1985.
23. Bollen, K.A.; Lennox, R. Conventional wisdom on measurement: A structural equation perspective. *Psychol. Bull.* **1991**, *110*, 305–314. [CrossRef]
24. Diamantopoulos, A.; Winklhofer, H.M. Index construction with formative indicators: An alternative to scale development. *J. Mark. Res.* **2001**, *38*, 269–277. [CrossRef]
25. GTMaritime. GT Maritime Launches Human Risk Management Cybersecurity Training and Monitoring Service. People Tech Maritime. 2025. Available online: <https://www.peopletechmaritime.com/post/gt-maritime-launches-human-risk-management-cybersecurity-training---monitoring-service> (accessed on 12 May 2026).
26. MAD Security. Training Your Crew: Meeting the January 2026 Cyber Training Deadline. MAD Security Blog. 30 September 2025. Available online: <https://madsecurity.com/madsecurity-blog/coast-guard-cybersecurity-training-2026> (accessed on 12 May 2026).
27. Ashley, T.D.; Kwon, R.; Gourisetti, S.N.G.; Katsis, C.; Bonebrake, C.A.; Boyd, P.A. Gamification of cybersecurity for workforce development in critical infrastructure. *IEEE Access* **2022**, *10*, 112487–112501. [CrossRef]
28. ISC2. 2024 ISC2 Cybersecurity Workforce Study. 2024. Available online: <https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study> (accessed on 12 May 2026).
29. U.S. Congress. Infrastructure Investment and Jobs Act, Pub. L. No. 117-58, 135 Stat. 429. 2021. Available online: <https://www.congress.gov/bill/117th-congress/house-bill/3684/text> (accessed on 12 May 2026).
30. Oruc, A.; Chowdhury, N.; Gkioulos, V.; Katsikas, S. Evaluation of Maritime Cyber Security (MarCy) training programme. *TransNav Int. J. Mar. Navig. Saf. Sea Transp.* **2024**, *18*, 743–763.
31. National Academies. *Looking Ahead at the Cybersecurity Workforce at the Federal Aviation Administration*; National Academies: Constitution Avenue, NW, USA, 2021.
32. National Science Foundation. *Cybersecurity and Critical Infrastructure Pathway for Aviation Industries*; NSF Award No. 2400855; Directorate for STEM Education: Alexandria, VA, USA, 2024. Available online: https://www.nsf.gov/awardsearch/showAward?AWD_ID=2400855 (accessed on 12 May 2026).
33. Asaju, B.J. *Standardization and Regulation of V2X Cybersecurity: Analyzing the Current Landscape, Identifying Gaps, and Proposing Frameworks for Harmonization*; Academia: Baden-Baden, Germany, 2024.
34. Ramon, M.C.; Mosher, S.E. *Cybersecurity Wargames for Small Intelligent Transportation Systems Teams*; United States Department of Transportation: Washington, DC, USA, 2024.
35. Thomas, O.; Salek, M.S.; Tine, J.M.; Rahman, M.; Hockstad, T.; Chowdhury, M. Cybersecurity in transportation systems: Policies and technology directions. *arXiv* **2025**, arXiv:2501.05356.
36. Crichigno, J. *NSF Cybersecurity Workforce Development Project*; University of South Carolina: Columbia, SC, USA, 2025.
37. Grosschmid, J. Addressing maritime workforce cybersecurity skills development. In *Maritime Cybersecurity*; Bauk, S., Ed.; Springer: Hoboken, NJ, USA, 2025; pp. 15–32.
38. Petersen, R.; Santos, D.; Smith, M.C.; Wetzel, K.A.; Witte, G. *Workforce Framework for Cybersecurity (NICE Framework)*; NIST Special Publication 800-181 Rev. 1; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020.

39. Ribeiro, A. CSIS: USCG poised for “generational change” in maritime cybersecurity with new tools, \$25B funding. *Industrial Cyber*, 27 October 2025. Available online: <https://industrialcyber.co/transport/csis-uscg-poised-for-generational-change-in-maritime-cybersecurity-with-new-tools-25b-funding/> (accessed on 12 May 2026).
40. Verizon. 2025 Data Breach Investigations Report. 2025. Available online: <https://www.verizon.com/business/resources/T16f/reports/2025-dbir-data-breach-investigations-report.pdf> (accessed on 12 May 2026).
41. Ochoa, O.; Garfield, K.A.; Haass, J.C.; Sampigethaya, R.; Niure Kandel, L. *CyberCorps Scholarship for Service: High-Skilled Workforce Development for the Aviation and Aerospace Cybersecurity Domains*; NSF Award No. 2146462; Directorate for STEM Education: Alexandria, VA, USA, 2022.
42. Murisa, W.; Coetzee, M. Strengthening aviation cybersecurity with security operations centres. In Proceedings of the 19th International Conference on Cyber Warfare and Security (ICWS 2024), Johannesburg, South Africa, 26–27 March 2024; Volume 19, pp. 481–489. [CrossRef]
43. Barnes, M.J. *Transportation Systems Cybersecurity and Cyber Resilience*; Report No. TTI-2023-1; Texas A&M Transportation Institute: Bryan, TX, USA, 2023.
44. ITS America. Workforce Gaps & the Future of Intelligent Transportation Systems. 2024. Available online: <https://itsa.org/wp-content/uploads/2024/11/ITS-America-Workforce-Gaps-the-Future-of-ITS-Final-10.29.24.pdf> (accessed on 12 May 2026).
45. Grahm, R.; Silverstein, C.; Fraser, J.L.; Campbell, M.; Morales, M.; Ayabae, J.-M.; Paull, S. *Career Opportunities in Intelligent Transportation Systems (ITS)*; Report No. FHWA-JPO-26-001; U.S. Department of Transportation Intelligent Transportation Systems Joint Program Office: Washington, DC, USA, 2025. Available online: <https://rosap.ntl.bts.gov/view/dot/89169> (accessed on 12 May 2026).
46. Ramon, M.C.; Dodson, A.T.; Wolff, J.P.; Sapphire, J.R. *Cybersecurity Issues and Protection Strategies for State Transportation Agency CEOs*; NCHRP Web-Only Document 355; National Academies Press: Washington, DC, USA, 2023. [CrossRef] [PubMed]
47. U.S. Government Accountability Office. Surface Transportation: TSA Is Taking Steps to Enhance Cybersecurity, but Additional Actions Are Needed (GAO-25-107947). 2024. Available online: <https://www.gao.gov/products/gao-25-107947> (accessed on 12 May 2026).
48. Peterson, D.; Molina, A. *Workforce Development and Driver Shortages in Small Urban and Rural Transit*; United States Department of Transportation: Washington, DC, USA, 2023.
49. Oruc, A.; Chowdhury, N.; Gkioulos, V. A modular cybersecurity training programme for the maritime domain. *Int. J. Inf. Secur.* **2024**, *23*, 1477–1512.
50. Chupkemi, D.C.; Mersinas, K. Challenges in maritime cybersecurity training and compliance. *J. Mar. Sci. Eng.* **2024**, *12*, 1844. [CrossRef]
51. ISC2. 2025 ISC2 Cybersecurity Workforce Study. 2025. Available online: <https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study> (accessed on 12 May 2026).
52. Office of the National Cyber Director. *National Cyber Workforce and Education Strategy: Unleashing America’s Cyber Talent*; The White House: Washington, DC, USA, 2023. Available online: <https://covacci.org/wp-content/uploads/2023/08/National-Cyber-Workforce-and-Education-Strategy-NCWES-2023.07.31.pdf> (accessed on 12 May 2026).
53. Smyrlis, M.; Floros, E.; Nikoloudakis, N.; Stavrou, E.; Merkouris, D.; Arvanitis, A.; Spanoudakis, G.; Papadakis, S.E.; Potamos, G.; Stavrou, S. SecAwarenessTruss: A federated cyber range solution for critical infrastructures. In *2025 IEEE International Conference on Cyber Security and Resilience (CSR)*; IEEE: Piscataway, NJ, USA, 2025; pp. 1063–1068.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.