ISSN: 2473-4901
v12 n6679

Bridging the Policy-Practice Gap in Cybersecurity Education: Developing a Cybersecurity Program for K-12 Career and Technical Education

Janet Hartkopf
jhartkopf@arizona.edu

Paul Wagner
paulewagner@arizona.edu

Josh Pauli
jjpauli@arizona.edu

University of Arizona
Tucson, AZ, 85747, USA

Abstract

This paper examines the misalignment between secondary Career and Technical Education (CTE) cybersecurity education and workforce requirements. Technology advancements, multi-year curriculum revision cycles, and certification-driven instructional models have created a policy-practice gap that limits students' readiness for modern cybersecurity roles. A Local Occupational Program (LOP) model is designed to address these challenges. The proposed model integrates a cyber-focused curriculum framework, providing a stable foundational core with flexible micro-modules that reflect emerging technologies and regional workforce needs. Grounded in the National Initiative for Cybersecurity Education Workforce Framework and informed by adversarial thinking concepts derived from MITRE ATT&CK, the program emphasizes experiential learning and applied skill development. In addition, the model incorporates an in-house student internship structure to address the lack of accessible work-based learning opportunities for secondary education students. Comparative analysis of existing secondary education cybersecurity pathways and their alignment with workforce Tasks, Knowledge, and Skills (TKSs) indicates that a modular, cyber-integrated instructional approach is designed to improve adaptability, relevance, and workforce alignment. This research contributes a scalable and flexible model for secondary education cybersecurity education that is intended to support workforce pipeline development, strengthen student engagement, and align with both regional economic needs and national security priorities.

Keywords: policy-practice gap, Career and Technical Education, cybersecurity workforce, local occupational program, NICE framework, experiential learning.

Bridging the Policy-Practice Gap in Cybersecurity Education: Developing a Cybersecurity Program for K-12 Career and Technical Education

Janet Hartkopf, Paul Wagner, and Josh Pauli

1. INTRODUCTION

Since the inception of Career and Technical Education (CTE) in the United States, industry has partnered with secondary education institutions to build a prepared workforce pipeline, initially through direct skills training leading to immediate employment. The expansion of digital infrastructure across all sectors has made cybersecurity a foundational component of national, economic, and individual security. As industries adopt cloud computing, artificial intelligence (AI), connected devices, and other advanced technologies, demand for qualified cybersecurity professionals continues to grow. Workforce studies consistently document a persistent gap between industry needs and the current talent pipeline (ISC2a, 2025).

This gap is most visible in entry and mid-level roles, where employers prioritize practical experience, applied problem-solving, and adaptability over traditional credentials and certifications. Secondary education operates on curriculum revision cycles that do not keep pace with rapidly evolving technology fields. Internship opportunities for students under 18 remain limited due to security clearance requirements, legal liability concerns, and restricted access to sensitive systems, reducing students' ability to gain the practical experience employers seek. Existing vocational education models (Payne, 2023; Work Based Learning Alliance, 2026) provide supervised, age-appropriate pathways for youth work-based learning; however, many high school programs intended to prepare students for careers in IT or cybersecurity are outdated, broad, light on experiential learning, or misaligned with current workforce expectations.

CTE is well-positioned to address this challenge by providing early exposure to career pathways, hands-on learning, and opportunities to build both technical and professional skills. High-quality CTE programs strengthen the connection between education and industry through workforce alignment, experiential learning, and partnerships with employers and post-secondary institutions. In emerging fields like cybersecurity, however, traditional CTE program structures often struggle to remain current because they rely on rigid standards, infrequent curriculum updates, and certification-driven models. Programs built around fixed content can become outdated before students complete the pathway, creating a disconnect between classroom learning and workforce realities.

This paper recommends a cyber-focused CTE Local Occupational Program (LOP) model built on foundational technical instruction and cybersecurity principles, organized around a flexible micro-module structure, and integrated with a student internship opportunity. The model is designed to improve alignment with workforce needs, support faster adaptation to technological change, and better prepare students for modern cybersecurity pathways.

In Arizona, LOPs are submitted when no existing CTE program framework covers a given occupational area. Schools submit LOPs to the state; once approved, they may operate the program using CTE funding.

2. LITERATURE REVIEW

Historically, CTE in the United States evolved in response to workforce development needs associated with industrial and technological change. Early vocational education initiatives emerged during the late Industrial Revolution to prepare students for skilled labor positions and were formalized through federal legislation such as the Smith-Hughes Act of 1917, which established state-supported vocational education systems (Steffes, 2020; Stringfield & Stone 2017). Over time, vocational education expanded beyond industrial training to encompass broader career-preparation models aligned with evolving workforce demands. Figure 1 illustrates the progression from early vocational education to the modern

ISSN: 2473-4901
v12 n6679

CTE framework, including the expansion of federally supported career pathways and career exploration initiatives.

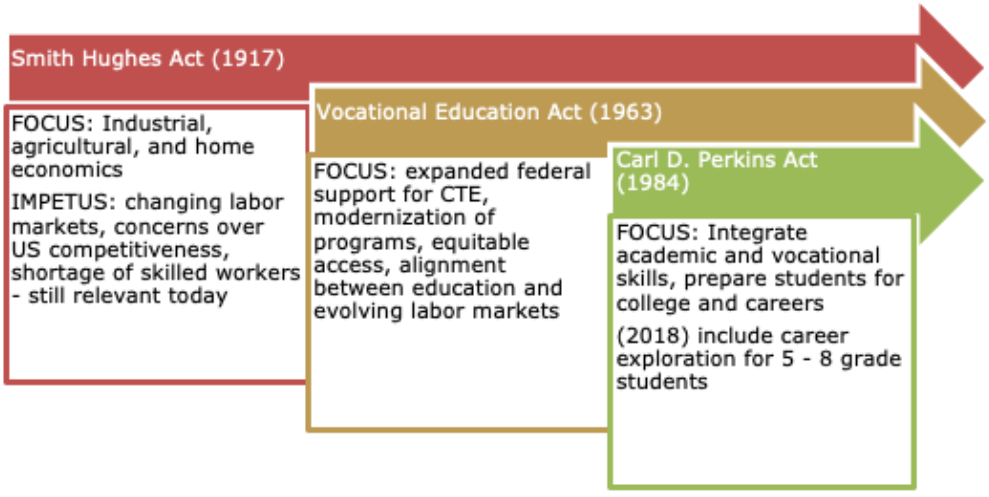

Figure 1: Historical Snapshot of Vocational to CTE Program Development

As technology-driven industries expanded during the third and fourth industrial revolutions, CTE programs increasingly incorporated information technology, automation, and computer science concepts to better align with workforce expectations (Xu et al., 2018; Xu, Lu et al., 2021). Modern CTE programs emphasize academic knowledge, technical competencies, and professional skills while maintaining close partnerships with industry, workforce organizations, and post-secondary institutions (Brand et al., 2013; Stone III, 2014). Program development commonly includes labor market analysis, advisory board involvement, curriculum review, and alignment with industry-recognized credentials and workforce frameworks.

Today, CTE programs are designed to provide multiple post-secondary and workforce pathways while supporting applied learning and workforce readiness. Figure 2 summarizes the contemporary CTE program development cycle, including labor market analysis, stakeholder engagement, standards development, and industry alignment. Although this structure supports accountability and workforce responsiveness, rapidly evolving fields such as cybersecurity challenge the traditional pace of curriculum revision and program governance.

Figure 2: CTE Program Development Cycle

2.1 Policy-Practice Gap

Despite significant investment in CTE and growing alignment efforts between education and industry, a persistent gap remains between the skills taught in secondary education programs and the competencies required by the cybersecurity workforce (ISC2, 2023). This disconnect, often described as a policy-practice gap, is more pronounced in rapidly evolving technological fields where curriculum structures struggle to keep pace with industry change.

ISC2 surveys (ISC2, 2023; ISC2b, 2025) confirm significant concern about the availability of skilled professionals, and the 2025 Cybersecurity Workforce Research Report (SANS | GIAC, 2025) finds that certifications alone are insufficient without combined on-the-job or experiential learning. Workforce projections indicate that by 2031, approximately 72% of U.S. jobs will require post-secondary education or training beyond high school (Georgetown University Center on Education and the Workforce, 2024), reflecting demand that continues to outpace the current talent pipeline.

The Greater Phoenix region's dense concentration of software, technology, and startup companies (Greater Phoenix Economic Council, 2024) drives substantial cybersecurity demand, with over 12,000 open positions in Arizona (CyberSeek, 2025) extending beyond offense and defense to awareness training and consultation for under-resourced startups and small organizations.

Most states revise CTE standards every three to five years (Strengthening Career and Technical Education for the 21st Century Act, 2018). While this process ensures consistency, accountability, and stakeholder involvement, it is not designed for fields like cybersecurity, where technology evolves continuously. Fields such as cabinetry or construction, where core competencies remain relatively stable across revision cycles, tolerate this pace; cybersecurity does not.

The Carl D. Perkins Career and Technical Education Act (Perkins V) provided significant annual federal investment in CTE programs (Advance CTE, 2026) and requires programs of study to align with both secondary and post-secondary education (Carl D. Perkins Career and Technical Education Improvement Act, 2006).

2.2 Limitations of State-Level CTE Curriculum Governance

State CTE governance provides accountability, quality assurance, and alignment with workforce requirements through formal review cycles involving advisory committees, state and local workforce boards, and state education agencies. While this process ensures transparency and program consistency, it slows updates in ways that affect fast-moving fields. Computer science, cybersecurity, and other emerging technologies evolve significantly faster than the traditional occupational sectors for which this governance structure was designed. A flexible curriculum model would provide continuity in technology programs while enabling more rapid standards revision as the field changes and allowing customization by location.

Studies from the mid-1940s began to show that vocational education was not producing the economic benefits originally anticipated, and that job training in these programs trailed industry's actual needs (Steffes, 2020). The pattern continues: as new frameworks emerge through industry participation, secondary education course frameworks lack current tools and practices. To compensate, educators rely on informal methods such as independent research, industry connections, and supplemental instructional materials. While these efforts reflect genuine professional commitment, they introduce variability in program quality and contribute to inequities across districts and regions.

Existing secondary education cybersecurity programs are situated within other CTE programs, such as computer science or IT. Arizona's Network Security CTE program is formally based on state-developed technical standards. However, in practice, instruction is frequently aligned to industry certifications such as CompTIA A+ and Network+, which emphasize foundational IT skills over deeper cybersecurity specialization. This is apparent in the program description of Network Security for the state of Arizona. The description outlines the objectives for students completing the sequence. It states they will,

> "Develop skills to analyze, test, troubleshoot, and evaluate existing network systems, such as local area network (LAN), wide area network (WAN), and Internet systems or a

> segment of a network system. Perform network maintenance to ensure networks operate correctly with minimal interruption. (Arizona Department of Education, 2025)"

Table 1 provides an excerpt of the full Table in Appendix A which illustrates the difference between the Arizona Network Security standards (Arizona Department of Education, 2025; Arizona Career and Technical Education Quality Commission, 2024) and the proposed model. The table shows that the distinction is not about the addition or removal of technical content, but in instructional orientation. The Arizona standards emphasize networking, system configuration, and troubleshooting as primary proficiencies, with cybersecurity concepts layered on top. While the Network Security standards include cybersecurity concepts, they are units within an IT-first structure. In contrast, the proposed model examines these same technical skills through a cybersecurity lens, where systems are analyzed in terms of risk, vulnerabilities, and adversarial behavior. This shift transforms foundational knowledge from isolated technical tasks into applied security reasoning, better aligning instruction with modern cybersecurity workforce expectations. The table focuses on the technical content related to the proposed model and not the professional development standards and sub-standards.

Standard 3.0 – Demonstrate Basic Mathematics for Network Security		
Arizona Standard	**IT-Centric**	**Cybersecurity-Centric**
3.1–3.4 Number systems (binary, hex, decimal)	Used for subnetting, IP addressing, and networking math	Used to interpret packet data, analyze logs, understand encoding, and examine malware signatures
3.5 Conversion methods	Procedural skill (manual/electronic conversion)	Applied skill for interpreting real-world cyber data (e.g., hex in Wireshark, hashes, memory artifacts)
3.6 Boolean logic	Basic logic for searches/scripting	Applied to detect logic, filtering rules, SIEM queries, and threat hunting

Table 1: Excerpt from Arizona Network Security Standards and Cybersecurity-Contextualized Framework Comparison

While certifications provide valuable foundational knowledge, they focus on IT support roles rather than cybersecurity-specific roles. This approach can limit students' exposure to critical areas such as threat analysis, risk management, governance, and emerging domains like cloud and Operational Technology (OT) security. The National Initiative for Cybersecurity Education (NICE) framework (Petersen et al., 2020) defines 41 workforce roles and the associated Task, Knowledge, and Skill (TKS) statements. Similarly, models like MITRE ATT&CK highlight the adversarial behaviors that students must understand to effectively apply those skills in practice (MITRE ATT&CK, 2026).

Equity concerns play a significant role in the policy-practice gap. Research suggests that access to advanced or college-aligned CTE programs, including those related to computing and cybersecurity, is frequently uneven across districts, with disparities linked to socioeconomic factors (Heller et al., 2025; Furey, 2025). Specifically, only 10% of Arizona schools offer cybersecurity courses and less than 1% of students have access to cybersecurity pathways (Wagner et al., 2026). Schools in rural or underserved areas may face additional barriers, including limited access to qualified instructors, fewer industry partnerships, and reduced availability of resources necessary to support technical programs. These disparities contribute to uneven workforce training and limit the diversity of the cybersecurity talent pipeline (Heller et al., 2025).

2.3 Barriers to Program Development

Cybersecurity, like many technology programs, faces more challenges than established programs. Challenges include the rapid growth in workforce demand, limited public understanding of cybersecurity career pathways, and persistent difficulties engaging students in cybersecurity education due to misconceptions about the field and the abstract nature of many cybersecurity concepts (ISC2, 2024). Another challenge is the lack of curricular guidance. School districts either add a cybersecurity course at the end of their computer science sequence or rely on the Network Security program, which was

structured around IT standards and requires significant adjustment to center cybersecurity. The result is a structural misalignment that the original program was never designed to resolve.

3. METHODOLOGY

This study employed a qualitative, design-based curriculum development approach to develop a proposed cybersecurity Local Occupational Program (LOP) for secondary education CTE. The approach consisted of four stages: a structured literature review of CTE policy and cybersecurity workforce challenges; a comparative analysis of existing cybersecurity education programs, certifications, and frameworks; a synthesis of workforce competencies drawn from the NICE Workforce Framework and related standards; and the development of a proposed LOP model integrating those findings. This approach draws on curriculum and instructional design literature (McKenney & Reeves, 2018; Richey & Klein, 2014) but does not constitute a completed Educational Design Research (EDR) cycle, since it does not include iterative prototyping, stakeholder co-design, or implementation-based evaluation; those steps are identified as future work in Section 7. Because this is a design-based curriculum development study rather than a hypothesis-testing study, the work is organized around the research questions below rather than hypotheses.

Four research questions guided the study: (1) how existing secondary cybersecurity CTE programs fail to align with workforce expectations defined by national frameworks such as the NICE Workforce Framework for Cybersecurity; (2) what instructional domains and structural features are necessary to prepare students for entry-level cybersecurity careers and post-secondary pathways; (3) how an LOP model can balance foundational stability with flexibility to address rapidly evolving workforce demands; and (4) what mechanisms can improve experiential learning opportunities and equitable access to cybersecurity instruction.

Sources fell into four categories. Workforce and industry research included cybersecurity workforce studies published by ISC2, SANS | GIAC, CyberSeek, and the Greater Phoenix Economic Council to identify workforce gaps and regional labor market demands. Federal and state policy documents, including the Smith-Hughes Act, Perkins legislation, Arizona Department of Education documentation, and Arizona CTE Quality Commission materials, were analyzed to establish the regulatory and structural context affecting cybersecurity CTE development. National workforce frameworks included the NICE Workforce Framework for Cybersecurity (NIST SP 800-181 Rev. 1), which served as the primary alignment standard for cybersecurity work roles, tasks, knowledge, and skills; the MITRE ATT&CK framework and Joint Task Force Cybersecurity Curricular Guidelines were also reviewed to support adversarial thinking and curricular prioritization. Peer-reviewed literature related to cybersecurity education, workforce alignment, experiential learning, and CTE program development was identified through ERIC, Education Source, and Google Scholar using search terms focused on secondary education and workforce preparation.

Trustworthiness was established through triangulation across workforce reports, framework mappings, comparative program analyses, and scholarly literature. Design decisions were documented through analytical matrices that connect curricular recommendations to supporting evidence and to nationally recognized frameworks, including NICE, MITRE ATT&CK, ACTE Quality CTE Program of Study guidance (Imperatore & Hyslop, 2018), and Hanover Research's program development model (Hanover Research, 2025).

4. ANALYSIS

4.1 Cybersecurity Program Analysis

Five cybersecurity programs and one industry certification were examined in a comparative analysis to identify strengths and limitations. The table in Appendix B synthesizes this examination across program, audience, domain, framework alignment, strengths, and limitations. Key observations include an emphasis on industry alignment and tools (e.g., Cisco), the prioritization of theoretical understanding and ethics (e.g., TeachCyber, RING), and a focus on accessibility and early exposure (e.g., CodeHS, Cyber.org). However, no single program integrates foundational knowledge, applied skills, and direct workforce alignment within a cohesive structure. Current pathways tend to develop only part of the skill set required for modern cybersecurity roles rather than a complete, workforce-ready profile. CompTIA

Security+, an entry-level cybersecurity credential, is certification-centric rather than pedagogical, designed for exam preparation rather than scaffolded student learning.

Table 2 maps the shift from traditional IT-centric instruction to a cybersecurity-centric model. Rather than teaching hardware, networking, and operating systems as isolated topics, the proposed approach embeds security within each concept. Areas typically omitted or minimized in existing programs, such as governance, risk management, and incident response, are intentionally integrated. The distinction is not in the content itself but in how it is framed, shifting from technical IT knowledge to applied cybersecurity thinking.

Domain	Used in current Programs?	Level taught	LOP Recommendation	Rationale
Hardware	Yes	Early, Technical	Foundational & Integrated	Required for all cyber roles
Networking	Yes	Early, Technical	Foundational & Integrated	Required for all cyber roles
Cloud Security	Varies	Intermediate, Optional	Modular Badge & Integrated	Industry demand
Ethics / Privacy	Varies	Later, Broad	Integrated	Long-term relevance
Risk / Governance	Rare	Later, Broad	Modular Badge & Integrated	Long-term relevance
OS / Linux	Yes	Early, Technical	Foundational & Integrated	Industry demand
Scripting	Varies	Intermediate, Technical	Integrated	Long-term relevance
IR Fundamentals	Rare	Later, Broad	Modular Badge & Integrated	Long-term relevance
Security Principles / Threat	Varies	Later, Broad	Foundational & Integrated	Required for all cyber roles

Table 2: Cybersecurity-Centric Program Model

4.2 Framework-Guided Domain Prioritization in Cybersecurity Curriculum Design

Yar et al. (2024) provided an overview of NICE and Joint Task Force (JTF) knowledge area mapping for cybersecurity education. The authors analyzed the similarities between NICE and JTF, created a comparative table of knowledge areas, and prioritized those areas across five NICE categories: securely provision, operate and maintain, protect and defend, oversee and govern, and investigate. Their summarized findings are outlined in Appendix C.

Human security and system security emerge as the primary knowledge areas across NICE-aligned categories, with data security also playing a significant role. In contrast, areas conventionally emphasized in early CTE pathways, such as hardware and general networking (component security), do not appear as central standalone priorities within this framework mapping. This finding highlights a key limitation in existing secondary education programs: many are structured around IT-centric foundations rather than cybersecurity-centric thinking. As a result, students may develop technical familiarity without a corresponding capacity to analyze risk, understand adversarial behavior, or evaluate human factors in security. The proposed foundation and micro-modules are designed to address this gap by prioritizing system-level thinking, human behavior, and security analysis within the foundational core rather than treating them as advanced or optional topics.

Secondary education programs also need to shift orientation from preparing students for current job openings to preparing them for the roles the field will require, as the 2025 Cybersecurity Workforce Research Report notes: "there is a need to prepare people for a future market, not the current market" (SANS | GIAC, 2025). A stable technical foundation paired with updatable micro-modules is intended to allow programs to do exactly that, giving students the grounding they need while preserving the flexibility to reflect where the field is headed.

5. LOCAL OCCUPATIONAL DEVELOPMENT (LOP) DEVELOPMENT

5.1 LOP Purpose

Unlike traditional CTE cybersecurity pathways that are often rooted in broader IT frameworks or certification-specific content, the proposed Local Occupational Program (LOP) is aligned with NICE Workforce Framework roles and competencies and incorporates developmentally appropriate adversarial-thinking concepts informed by the MITRE ATT&CK framework. The model combines a stable foundational cybersecurity core with flexible micro-modules in areas such as cloud security, AI, data analytics, and OT security, allowing programs to adapt to emerging technologies and regional workforce needs without requiring complete curriculum redesign. Through experiential learning, simulation-based instruction, and partnerships with industry and post-secondary institutions, the program emphasizes both technical and professional skill development while supporting workforce readiness, regional economic growth, and the long-term sustainability of the cybersecurity workforce.

5.2 The Foundational Core

The program's foundation focuses on essential cybersecurity concepts relevant across all roles in the field. These are not tied to a single certification or toolset but reflect lasting principles unlikely to become obsolete. Core areas include:

- Basic hardware, networking, and infrastructure concepts (taught in context)
- Systems thinking and administration
- Risk, threat, and vulnerability analysis
- Adversarial thinking and ethical security practices
- Security principles, including confidentiality, integrity, and availability
- Introduction to governance, ethics, and privacy
- Cybersecurity communication and career pathways (CTE requirement)

Rather than teaching hardware, operating systems, or networking as isolated technical units, these topics are integrated into the broader discussion of security. For example, networking is taught through the lens of attack surfaces and data flow, while operating systems are explored in terms of system vulnerabilities and access control. This approach helps students understand why these components matter, not just how they work, and allows more instructional time to be devoted to security-specific thinking rather than general IT support skills.

5.3 Micro Module Structure

Building on the foundational core, the program introduces a set of micro-modules that allow for targeted exploration of specialized topics. These modules are designed to be flexible and responsive to both industry trends and regional workforce needs. Examples of potential micro-modules include:

- Cloud and hybrid security
- Data analytics for cybersecurity
- AI and cybersecurity
- Operational technology (OT) and manufacturing security
- Incident response fundamentals
- Critical infrastructure support
- Governance, Risk, and Compliance (GRC)

Each module functions as a discrete learning unit that can be adjusted, replaced, or expanded without requiring a full redesign of the program. This is a key advantage over traditional CTE structures, where changes often require formal revision cycles that take years to implement. From a student perspective, micro-modules provide choice and relevance, allowing students to identify areas of interest while still building a broad cybersecurity foundation and exploring more specific career directions. From a program perspective, this structure allows educators to respond more quickly to changes in the operational environment.

Appendix D and Appendix E provide a sample lesson plan and student handout respectively to demonstrate how a cyber-focused instructional approach can be implemented. The activity guides students through the thought process of risk and mitigation, can be used at multiple levels to reinforce current knowledge and experience, and develops both foundational cybersecurity skills and professional skills such as communication, presentation, and teamwork.

5.4 Integration of Experiential and Project-Based Learning

A defining feature of this program is its emphasis on experiential and applied learning. Cybersecurity is not a field that can be effectively taught through lecture alone. Students must engage with scenarios, simulations, and problem-solving activities that mirror real-world conditions. Instructional strategies include simulation-based labs and cyber ranges, scenario-based risk assessments and tabletop exercises, project-based learning activities, and industry-informed case studies.

Projects are designed to reflect real-world challenges and encourage students to synthesize knowledge across multiple domains. Examples include developing a security awareness campaign for a target audience, analyzing a cybersecurity incident and presenting findings and recommendations, and designing basic security plans that address identified vulnerabilities. These activities require students to analyze information, communicate findings, and justify decisions, mirroring workplace expectations. Project-based learning also supports differentiation, as students can approach problems from different angles and demonstrate understanding in multiple ways.

This approach aligns with broader CTE requirements that emphasize hands-on learning, with approximately 51% of instruction focused on applied experiences (Arizona Department of Education, 2025). Students might respond to a mock phishing campaign, analyze suspicious network activity, or evaluate the security posture of a simulated organization. These experiences bridge the gap between theoretical knowledge and practical application in ways that traditional instruction cannot replicate.

5.5 Applied Tools and Professional Skill Development

Partnerships with industry and post-secondary institutions can provide access to advanced environments such as cyber ranges or specialized software platforms. However, the program is not dependent on high-cost tools. Many foundational concepts can be effectively taught using free or low-cost resources, making the program more accessible and scalable. The goal is not tool-specific training but to help students understand how tools function within cybersecurity practice.

Developing professional competencies is equally central to the program and a requirement in all CTE courses. Cybersecurity professionals must communicate effectively, work collaboratively, and adapt to rapidly changing situations. Instructional activities support communication skills through presentations and written reports, collaboration through group-based problem solving, and ethical reasoning through discussions of privacy, data protection, and societal impact. Critical thinking is reinforced throughout via open-ended scenarios and decision-making tasks. These skills are embedded across the curriculum rather than taught as separate units, reinforcing their importance in both academic and professional contexts.

5.6 Proposed Program Standards - Cyber Integrated Technical Education (CITE) Framework

The proposed cyber-focused standards framework is aligned with the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity (NIST SP 800-181). It defines cybersecurity work roles and their associated task, knowledge, and skill statements. This alignment ensures that secondary-level instruction is both pedagogically sound and workforce-relevant. Table 3 illustrates how each program standard maps to NICE work roles and associated TKS statements, reinforcing the program's applicability to real-world cybersecurity functions. The full table is in Appendix F.

ISSN: 2473-4901
v12 n6679

Program Standard	Aligned NICE Work Roles	TKS	Rationale for Alignment
1. Computing Systems & Hardware (Cyber-Contextualized)	Securely Provision (SP), Operate & Maintain (OM)	K0001, K0002, S0001, S0010	Foundational system knowledge is essential for identifying hardware vulnerabilities and securing endpoints

Table 3: Alignment of Standards to NICE Workforce Framework Competencies

Each program standard, derived from NIST SP 800-181, is expanded to include representative workforce tasks along with supporting knowledge and skill statements, emphasizing the application of cybersecurity competencies in real-world contexts. Standard 1 is outlined as an example; the remaining standards appear in Appendix G.

Standard 1: Computing Systems & Hardware (Cyber-Contextualized)
Expanded NICE Tasks and KSs
Tasks (T):

- Analyze system components to identify potential vulnerabilities
- Configure and maintain secure system settings
- Perform system diagnostics to identify hardware/software issues
- Apply security controls to protect endpoints and devices

Knowledge (K):

- K0001: Knowledge of computer architecture concepts
- K0002: Knowledge of operating systems
- K0003: Knowledge of hardware components and functions
- K0005: Knowledge of system vulnerabilities and weaknesses
- K0013: Knowledge of basic system security principles

Skills (S):

- S0001: Identify system components and functions
- S0010: Configure and manage system settings
- S0012: Diagnose hardware/software issues
- S0028: Apply security controls to systems

The result is that students do not just learn what hardware is but how that hardware becomes an attack surface and is utilized by threat actors.

5.7 MITRE ATT&CK Integration

Figure 3 illustrates a simplified adversarial model adapted from the MITRE ATT&CK framework. Rather than requiring full framework mastery, this model introduces the core stages of a cyberattack in a developmentally appropriate format: initial access, persistence, privilege escalation, lateral movement, and exfiltration. These concepts are reinforced and applied across hardware, networking, and data systems, enabling students to develop adversarial thinking while maintaining alignment with industry-relevant practices.

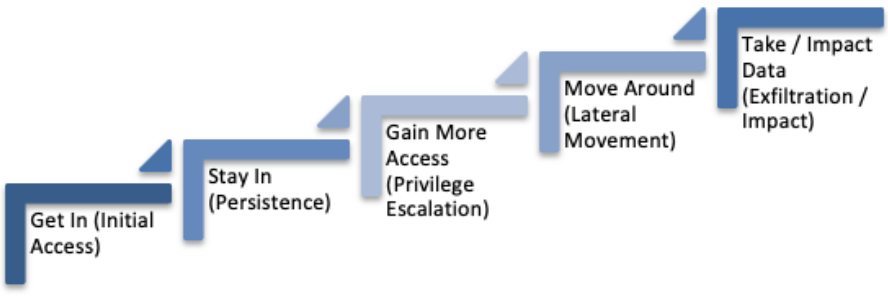

Figure 3: Simplified Adversarial Model Adapted from MITRE ATT&CK Framework

5.8 Applied Work-Based Learning: Student Internship Model

Identifying internships for students under 18 is challenging due to security clearance requirements, liability concerns, and restricted access to sensitive systems. Developing in-house alternatives addresses this gap while giving students structured opportunities to apply and demonstrate what they are learning. One approach is the cybersecurity clinic model. Cybersecurity clinics provide structured, supervised environments where students can obtain entry-level industry credentials, develop applied technical competencies, and perform appropriately leveled cybersecurity tasks that align with workforce expectations and their current stage of skill development. Advantages of this model include:

- Scaling internship experiences to more than just a few students
- Developing students' technical and professional skills, such as interviewing and public speaking
- Creating diverse opportunities beyond technical roles, such as marketing, curriculum development, and event coordination
- Enabling students to contribute to their community in settings where they are most comfortable

These clinics also provide a forum for industry professionals to work alongside and mentor students in direct and specific ways. This supports CTE program requirements while giving students resume-building experiences and an outlet to demonstrate their interest in cybersecurity outside the classroom.

Because clinic engagements may involve minors and, in some cases, live community organizations, the model incorporates the following safeguards before any student engagement begins:

- Adult supervision: a certified instructor or credentialed mentor is directly and physically present for all client-facing work; students do not access client systems or data unsupervised.
- Consent: written parental/guardian consent and student assent are obtained for each clinic engagement, separate from general course enrollment.
- Client and data eligibility: participating organizations and the systems or data they provide are screened before approval, excluding regulated data unless documented safeguards are in place.
- Privacy protections: client data is covered by confidentiality agreements, access is limited to what a task requires, and no client data is retained beyond the engagement.
- Prohibited activities: students may not perform offensive or adversarial actions against live systems, unauthorized scanning, or any task outside an approved, written scope of work.
- Tool permissions: software and tools are limited to a pre-approved list; any exception requires instructor sign-off.
- Incident escalation: a defined path (student, instructor, program coordinator, client contact) governs any unexpected finding or system issue, with required reporting timelines.
- Simulation-to-live progression: students begin in simulated or fictional-company environments built from synthetic or sanitized data; only students who have completed foundational instruction and clinic onboarding may progress to supervised live-client engagements under the controls above.

6. DISCUSSION

Traditional CTE models, while effective in more stable occupational fields, are often too inflexible to meet the demands of a cybersecurity workforce. Cyber-focused CTE frameworks that combine a stable foundational core with flexible micro-module specializations and an embedded student internship model are designed to respond to the policy-practice gap identified in current secondary cybersecurity education. Aligning instruction to workforce frameworks such as NICE, incorporating experiential learning, introducing developmentally appropriate adversarial thinking through MITRE ATT&CK-informed models, and providing internship opportunities through an in-house clinic structure are intended to offer a more complete preparation than existing programs achieve individually. The proposed model shifts the focus from narrow technical tasks and certification objectives to critical thinking about systems, risks, threats, and defenses, better reflecting the realities of modern cybersecurity work while preserving the career-connected purpose of CTE.

A foundation-and-micro-module structure is designed to provide stability where consistency is needed and adaptability where the field demands it. As education systems respond to workforce change, this

approach is intended to offer a scalable path for building secondary cybersecurity programs that remain relevant without requiring constant formal revision.

7. CONCLUSION

Cybersecurity touches everything. The challenge is not whether more professionals are needed, but whether secondary education is preparing students in ways that reflect current cybersecurity practice. The current structure of CTE technology programs is not keeping pace with workforce expectations, creating a policy-practice gap that affects both student readiness and the broader talent pipeline.

The proposed model is designed to address this gap through three interlocking elements: a stable foundational core grounded in lasting cybersecurity principles, flexible micro-modules intended to allow programs to adapt as the field evolves, and an in-house internship structure designed to provide meaningful applied experience. Aligning content to the NICE Workforce Framework and introducing adversarial thinking through simplified ATT&CK-informed concepts shifts the focus from memorizing content to understanding how systems work, how they can fail, and how they can be defended.

Access to meaningful, hands-on experience remains one of the most consistent barriers in secondary cybersecurity education. The clinic-style internship model is designed to address this directly by giving students opportunities to apply what they are learning, build professional skills, and engage with real audiences. These are the experiences that move students from understanding concepts to thinking like cybersecurity professionals.

Improving cybersecurity education at the high school level is not about adding more content. It is about rethinking how content is delivered and structured. A flexible, modular approach is designed to allow programs to adjust as technology changes without losing the foundational concepts students need. Aligning to workforce frameworks is intended to ensure that what students learn has relevance beyond the classroom, preparing them not just for an exam but for a career.

This paper presents a proposed model rather than a validated one. The literature review, comparative analysis, and framework synthesis reported here establish the rationale and design for the LOP model, but do not constitute implementation or evaluation. LOPs must be submitted and approved by the district prior to implementation. Future work should include pilot implementation with participating schools, expert and stakeholder review of the micro-module structure and cyber clinic model, and outcome data such as student participation rates and post-internship competency assessment.

As cybersecurity becomes central to every critical infrastructure sector, demand for a prepared and adaptable workforce will only grow. Secondary CTE programs are well-positioned to contribute to that pipeline. With the right structure, industry alignment, and commitment to applied learning, they can move from introductory exposure programs to meaningful entry points into the cybersecurity profession.

8. REFERENCES

Advance CTE. (2026). Secondary CTE Funding Basics. Retrieved from State of CTE: https://ctek12funding.careertech.org/cte-funding-basics/

Arizona Career and Technical Education Quality Commission. (2024, May 14). Network Security - 11.1999.00. Retrieved from Arizona Deparment of Education: https://www.azed.gov/cte/nt

Arizona Department of Education. (2025, October 24). Network Security 11.1999.00. Program Description, Industry Credential, Coherent Sequence, and Teacher Certification. Phoenix, Arizona: Arizona Department of Education.

Brand, B., Valent, A., & Browning, A. (2013). How Career and Technical Education can help Students be College and Career Ready: A Primer. Washington: American Institutes for Research.

Carl D. Perkins Career and Technical Education Improvement Act, S.250 (109th Congress July 25, 2006).

CyberSeek. (2025, August 4). CyberSeek - Workforce Map. Retrieved from CyberSeek: https://www.cyberseek.org/heatmap.html

Furey, J. (2025, January-December). College or Career Ready, But Not Both? Heterogeneity of Career and Technical Education (CTE) Programs and Income-Based Inequality in Access and Participation. AERA Open, *11(1)*, 1-13. https://doi.org/10.1177/23328584251334378

Georgetown University Center on Education and the Workforce. (2024). After everything: Projections of jobs, education, and training requirements through 2031. Georgetown: Georgetwon University. Retrieved from https://cew.georgetown.edu/cew-reports/projections2031/

Greater Phoenix Economic Council. (2024). Greater Phoenix Software Ecosystem. Phoenix: Greater Phoenix Economic Council.

Hanover Research. (2025, October 3). Ensure Future K-12 CTE Program Success in 3 Steps. Hanover Research. Retrieved from https://www.hanoverresearch.com/insights-blog/k-12-education/ensure-cte-career-technical-education-program-success-3-steps/

Heller, B., Kreisman, D., & Goldring, T. (2025). Equity in Career and Technical Education. Georgia Policy Labs. https://doi.org/10.57709/8WXE-MN61

Imperatore, C., & Hyslop, A. (2018). ACTE Quality CTE Program of Study Framework. Philadelphia: ACTE. Retrieved from https://www.acteonline.org/wp-content/uploads/2024/09/HighQualityCTEFramework2018-Aug2024.pdf

ISC2. (2023). 2023 ISC2 Cybersecurity Workforce Study. Alexandria: ISC2. Retrieved January 21, 2026, from https://edge.sitecorecloud.io/internationf173-xmc4e73-prodbc0f-9660/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf

ISC2. (2024). Global Cybersecurity Workforce Prepares for an AI-Driven World. Alexandria: ISC2. Retrieved January 23, 2026, from https://edge.sitecorecloud.io/internationf173-xmc4e73-prodbc0f-9660/media/Project/ISC2/Main/Media/documents/research/2024-ISC2-WFS.pdf

ISC2a. (2025). 2025 Cybersecurity Hiring Trends: Why Investing in Entry- and Junior-Level Talent is Key to Building a More Resilient Cybersecurity Workforce. Alexandria: ISC2. Retrieved from https://www.isc2.org/Insights/2025/06/cybersecurity-hiring-trends-study

ISC2b. (2025). 2025 ISC2 Cybersecurity Workforce Study. Alexandria: ISC2. Retrieved January 22, 2026, from https://www.isc2.org/insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study

McKenney, S., & Reeves, T. C. (2018). Conducting educational design research. London: Routledge. Retrieved from https://doi.org/10.4324/9781315105642

MITRE ATT&CK. (2026, April). https://attack.mitre.org/resources/faq/. Retrieved from attack.mitre: https://attack.mitre.org/

Payne, P., & Kuehn, D. (2023). Models of Youth Registered Apprenticeship Expansion: Evidence from the youth Apprenticeship Readiness Grants, U.S. Department of Labor. Retrieved from https://www.dol.gov/resource-library/models-youth-registered-apprenticeship-expansion-evidence-youth-apprenticeship.

Petersen, R., Santos, D., Smith, M. C., Wetzel, K. A., & Witte, G. (2020). Workforce Framework for Cybersecurity (NICE Framework). NIST Special Publication 800-181 Rev. 1. Retrieved from https://doi.org/10.6028/NIST.SP.800-181r1

Richey, R. C., & Klein, J. D. (2014). Design and Development Research. In Handbook of Research on Educational Communications and Technology. 141-150. New York, NY: Springer. https://doi.org/10.1007/978-1-4614-3185-5_12

SANS | GIAC. (2025). 20205 Cybersecurity Workforce Research Report. North Bethesda: SANS | GIAC.

Steffes, T. L. (2020, July 24). Smith-Hughes Act. Retrieved from Encyclopedia Britannica: https://www.britannica.com/topic/Smith-Hughes-Act

Stone III, J. R. (2014). More than One Way - The Case for High-Quality CTE. American Educator, 4-11.

Strengthening Career and Technical Education for the 21st Century Act, H.R.2353 (115th Congress July 31, 2018).

Stringfield, S., & Stone III, J. R. (2017). The Labor Market Imperative for CTE: Changes and Challenges for the 21st Century. Peabody Journal of Education, *92(2)*, 166 - 179. https://doi.org/10.1080/0161956X.2017.1302209

Wagner, P., Honomichl, R., Beasley, C., Reid, T., Bradford, L., Urbaszewski, A., (2026). Arizona's CyberSupply: Identifying Gateway-to-Cybersecurity and Cybersecurity Courses and Pathways in Secondary Education. Cybersecurity Pedagogy and Practice Journal *5(1)* 41-51. https://doi.org/10.62273/QPFS6373

Work Based Learning Alliance (2026). Retrieved from https://workbasedlearningalliance.org/ .

Xu, M., David, J. M., & Kim, S. H. (2018). The Fourth Industrial Revolution: Opportunities and Challenges. International Journal of Financial Research, 90-95. Retrieved from https://doi.org/10.5430/ijfr.v9n2p90

Xu, X., Lu, Y., Vogel-Heuser, B., & Wang, L. (2021). Industry 4.0 and Industry 5.0 - Inception, conception and perception. Journal of Manufacturing System, 530-535.

Yar, M. A., Goh, H. G., Adnan, K., & Gan, M.-L. (2024). Bridging Cybersecurity Education and Industry Demands: Mapping and Prioritizing Curriculum Guidelines. 2024 International Conference on Future Technologies for Smart Society (ICFTSS). 188-193. ResearchGate. https://doi.org/10.1109/ICFTSS61109.2024.10690269

APPENDIX A

Arizona Network Security Standards and Cybersecurity-Contextualized Framework Comparison.

Standard 3.0 – Demonstrate Basic Mathematics for Network Security		
Arizona Standard	**IT-Centric**	**Cybersecurity-Centric**
3.1–3.4 Number systems (binary, hex, decimal)	Used for subnetting, IP addressing, and networking math	Used to interpret packet data, analyze logs, understand encoding, and examine malware signatures
3.5 Conversion methods	Procedural skill (manual/electronic conversion)	Applied skill for interpreting real-world cyber data (e.g., hex in Wireshark, hashes, memory artifacts)
3.6 Boolean logic	Basic logic for searches/scripting	Applied to detect logic, filtering rules, SIEM queries, and threat hunting

Standard 5.0 – Utilize Best Practices for Computer and Network Risks and Threats		
Arizona Standard	**IT-Centric**	**Cybersecurity-Centric**
5.1 Risk management	Defined as a unit	Core, continuous mindset across all instruction
5.2 CIA triad	Conceptual understanding	Applied to real-world scenarios and decision-making
5.4–5.6 Threats	Identification	Threat modeling and adversarial thinking
5.7 Mitigation strategies	Best practices list	Evaluate effectiveness in real-world attack scenarios

Standard 6.0 Analyze Network Media and Network Technologies		
Arizona Standard	**IT-Centric**	**Cybersecurity-Centric**
6.1–6.4 Media, connectors, topology	Understand physical infrastructure and setup	Analyze attack surfaces (e.g., physical access, cable tapping, rogue devices)
6.5 Virtual vs. Physical Networks	Infrastructure design knowledge	Security segmentation (VLANs, isolation, lateral movement prevention)
6.6–6.7 Network characteristics	Speed, distance, performance	Risk analysis of wireless vulnerabilities, interception, and exposure points
6.8 Internet structure	Conceptual understanding	Understanding attack paths, distributed systems, and exposure vectors
6.9 Network devices	Identify and configure devices	Analyze device vulnerabilities, misconfigurations, and exploitation points

Standard 7.0 Analyze Network Protocols and Standards		
Arizona Standard	**IT-Centric**	**Cybersecurity-Centric**
7.1 Protocol definition	Functional understanding	Analyze how protocols are exploited (e.g., DNS tunneling, HTTP attacks)
7.2–7.3 TCP/IP & OSI models	Layered communication model	Map attacks and defenses to layers (e.g., MITM, application attacks)
7.4 Ports & ranges	Memorization of port numbers	Identify attack vectors (port scanning, open ports, exploitation targets)

7.5 Routing protocols	Network traffic management	Understand routing manipulation and attack paths
7.6 Common protocols (DNS, HTTP, etc.)	Usage and function	Analyze protocol misuse in attacks (phishing, spoofing, exfiltration)
7.7 TCP vs UDP	Communication differences	Security implications (reliability vs speed in attacks)
7.8 IP addressing	Addressing and subnetting	Identify spoofing, tracking, and attribution challenges
7.10 Remote access	System access tools	Security risks (RDP attacks, credential compromise)
7.11 Security protocols	Identify protocols	Evaluate effectiveness and weaknesses (VPN misuse, TLS issues)

Standard 8.0 Configure a Basic Network		
Arizona Standard	**IT-Centric**	**Cybersecurity-Centric**
8.1 Network design	Build functional networks	Design secure architectures (segmentation, zero trust concepts)
8.2 Routing setup	Enable connectivity	Analyze routing as potential attack pathways
8.6–8.8 Install/configure systems	System administration skills	Identify misconfigurations as vulnerabilities
8.9 Diagnostic tools (ping, traceroute)	Troubleshooting	Reconnaissance techniques used by attackers

Standard 9.0 Harden a Network		
Arizona Standard	**IT-Centric**	**Cybersecurity-Centric**
9.1 Hardening concepts	Secure after setup	Security-first mindset from initial design
9.2 Vulnerabilities	Definitions	Analyze human, system, and environmental vulnerabilities holistically
9.5 Segmentation	Improve performance/security	Prevent lateral movement and contain breaches
9.8 Firewalls	Configuration rules	Evaluate rule effectiveness against real threats
9.10 IDS/IPS, SIEM	Tool awareness	Use tools for detection, analysis, and response

Standard 10.0 Perform Network Maintenance and Resolve Issues		
Arizona Standard	**IT-Centric**	**Cybersecurity-Centric**
10.1 Troubleshooting process	Fix system issues	Investigate incidents (aligns to incident response lifecycle)
10.3 Utilities (netstat, nslookup)	Diagnosing network problems	Analyze indicators of compromise and suspicious activity
10.4 Wireshark	Troubleshooting traffic	Packet analysis for attack detection
10.6 Resolve issues	Restore functionality	Identify root cause of security incidents
10.7 Monitoring tools	Maintain uptime	Continuous security monitoring and detection

Standard 11.0 Investigate Legal and Ethical Issues Related to Network Security		
Arizona Standard	**IT-Centric**	**Cybersecurity-Centric**
11.1–11.6 Legal, privacy, ethics	Standalone unit	Embedded across all modules (decision-making, risk, AI, data use)

ISSN: 2473-4901
v12 n6679

APPENDIX B

Comparative Analysis of Existing Secondary Education Cybersecurity Pathways

Program	Audience	Domains	Framework Alignment	Strengths	Limitations
Cisco Networking Academy – Jr. Cyber Analyst Path	High School – Early College	Networking, Threat Awareness, Endpoint Security, SOC	NICE industry-aligned competencies	Clear scope and sequence; industry relevant; certification aligned	Tool and vendor emphasis; limited adaptability to emerging fields
CodeHS Cybersecurity	High School	Cyber fundamentals, digital safety, and scripting	CTE Network Securities standards, some NICE alignment	Accessible for beginners, flexible pacing	Weak security operations and threat analysis coverage
TeachCyber	High School	Core cyber concepts – networking, data & system security, risk, ethics & trust, societal impacts	NIST, ACM CSEC alignment to HS cyber curriculum guidelines,	Strong foundation-first, emphasizes enduring understanding, evidence-centered design, flexible modular units	Single year-long course, limited alignment to workforce roles such as NICE
RING	High School	10 units, ethics, trust, connectivity, data security, introduction to Python, system security, adversarial thinking, risk & implications	CAE-C partners and community-vetted course development	Free, year-long, easy entry for beginners	Course-centric, limited mapping to national workforce frameworks
Cyber.org	K-12 offerings	Material available for computing systems, digital citizenship, and security (networking, IoT, threats, cryptography)	Designed with cross-stakeholder input including education and industry, Sec+ aligned	Supports cybersecurity literacy and early career exploration	A collection of standard-aligned modules and lessons that require local assembly
CompTIA Sec+	Entry-level workforce (adaptations for High School)	Risk, Threats, Architecture, Operations & Governance	NICE, DoD 8140	Industry-recognized vocabulary and structure, simulations	Designed certification-centric not pedagogy

ISSN: 2473-4901
v12 n6679

APPENDIX C

Knowledge Area Mapping and Rank of Importance

Knowledge Area	Securely Provision	Operate and Maintain	Protect and Defend	Oversee and Govern	Investigate	Total KA	Rank
Human Security	21	14	5	11	5	56	1
System Security	12	8	7	26	6	59	2
Data Security	18	14	12	30	4	78	3
Connection Security	30	17	16	45	9	117	4
Organizational Security	37	30	30	19	13	129	5
Societal Security	46	34	21	23	7	131	6
Component Security	34	27	27	44	13	145	7
Software Security	51	36	26	54	15	182	8

APPENDIX D

Lesson Plan Example

Sample Lesson Plan
Cyber Risk & Adversarial Thinking Activity
Lesson: Understanding Cyber Risk through the "How do Hackers Think" Model. This lesson reflects a cyber-focused instructional approach aligned to NICE Workforce Framework competencies.

Grade Level: High School (9 – 12)
Time Required: 90 – 120 minutes

Learning Objectives
Students will be able to:
- Identify system components and potential vulnerabilities
- Apply the 5-stage cyber-attack model to real-world scenarios
- Analyze risk using structured reasoning
- Communicate cybersecurity concepts to a non-technical audience

Standard Alignment
- NICE Workforce Framework (related to threat analysis, risk, and system security)
- Program Standards: Systems, Networking, Threats and Defense

Materials Needed
- Student handout
- Scenario worksheet (home network or small business)
- Risk matrix template (optional)

Lesson Activities
1. Introduction (15 minutes)
   - Introduce the "How Hackers Think" model
   - Walk through each stage with simple examples
2. Scenario Analysis Activity (45–60 minutes)
Students analyze a scenario (example: home network or small business).

They must:
- Identify assets (devices, accounts, data)
- Identify vulnerabilities
- Map attacker actions using the 5-stage model:
  - How would an attacker get in?
  - Stay in?
  - Gain access?
  - Move around?
  - Achieve their goal?

3. Risk Evaluation (20–30 minutes)
Students will:
- Rank risks (high/medium/low)
- Propose mitigation strategies
- Justify their reasoning

4. Presentation / Communication (Optional Extension)
Students present findings to:
- Class
- Teacher
- Mock "client" (non-technical audience)

Assessment Criteria - Students demonstrate proficiency when they:
- Accurately identify vulnerabilities
- Apply the attack model logically

- Propose realistic mitigation strategies
- Clearly communicate reasoning

This lesson develops:

- Critical thinking → analyzing vulnerabilities
- Problem-solving → proposing mitigation
- Systems thinking → understanding interconnected risks
- Communication → translating technical concepts

Extension Opportunities

- Compare multiple scenarios
- Introduce basic logging or detection concepts
- Connect to real-world cyber incidents

APPENDIX E

Student Handout Example

"How Hackers Think" Model (Student View)
Purpose: This handout introduces students to a simplified model for understanding adversarial behavior in cybersecurity. The model below shows the common steps attackers take when targeting a system.

5 Stages of a Cyberattack:

1) Get In – How does the attacker gain entry? Where is the vulnerability? Was it through hardware, software, or reconnaissance work?
    a. Phishing emails
    b. Weak passwords
    c. Infected USB devices
2) Stay In – How does the attacker remain in the system? How does the attacker remain undetected?
    a. Installing malware
    b. Creating hidden accounts
    c. Using saved credentials
3) Gain More Access – How do they gain more control?
    a. Becoming an administrator
    b. Exploiting system weaknesses
4) Move Around - How does the attacker move from the entry point to other areas in the network? Where will they stop?
    a. Accessing other devices
    b. Scanning systems
    c. Using network connections
5) Take or Control Data (Exfiltration / Impact) – What is the main objective of the attack? What is their end goal?
    a. Stealing sensitive data
    b. Encrypting files (ransomware)
    c. Disrupting systems

Every system you use can be analyzed using this model. Understanding these steps can help you to identify vulnerabilities, think like a cybersecurity professional, and protect systems more effectively.

Apply: Think about a real-world scenario and ask yourself.

- How did the attacker get it?
- How could they stay in?
- What might they try to access or steal?

APPENDIX F

Alignment of Standards to NICE Workforce Framework Competencies

Program Standard	Aligned NICE Work Roles	TKS	Rationale for Alignment
1. Computing Systems & Hardware (Cyber-Contextualized)	Securely Provision (SP), Operate & Maintain (OM)	K0001, K0002, S0001, S0010	Foundational system knowledge is essential for identifying hardware vulnerabilities and securing endpoints
2. Operating Systems & System Administration	Operate & Maintain (OM), Protect & Defend (PR)	T1082, T1070, K0002, K0004, S0015, S0027	Misconfigurations are a leading cause of breaches; these standards build defensive system management skills
3. Networking Fundamentals & Security	Operate & Maintain (OM), Oversee & Govern (OV), Protect & Defend (PR)	T1046, T1040, K0037, K0038, S0034, S0050	Networking knowledge is critical for understanding attack vectors such as DDoS and MITM attacks
4. Cyber Threats, Vulnerabilities, and Defensive Strategies	Protect & Defend (PR), Analyze (AN)	T016, T0155, K0045, K0046, S0078, S0080	Direct alignment with core cybersecurity functions such as detection, analysis, and mitigation
5. Adversarial Thinking & Ethical Security Practices	Analyze (AN), Protect & Defend (PR)	K0060, K0061, S0092, A0035	Encourages a defensive mindset through understanding offensive strategies without promoting misuse
6. Data Security, Privacy, and Emerging Technologies	Oversee & Govern (OV), Securely Provision (SP)	K0018, K0059, S0057, A0022	Aligns cybersecurity with legal, ethical, and emerging technology considerations
7. Cybersecurity Communication & Career Pathways	Oversee & Govern (OV)	K0020, S0020, A0010, A0011	Supports workforce readiness and alignment to NICE role pathways

APPENDIX G

NICE TKS Breakdown As It Relates to Local Occupational Program Standards

Standard 1: Computing Systems & Hardware (Cyber-Contextualized)
Expanded NICE Tasks and KSs
Tasks (T):

- Analyze system components to identify potential vulnerabilities
- Configure and maintain secure system settings
- Perform system diagnostics to identify hardware/software issues
- Apply security controls to protect endpoints and devices

Knowledge (K):

- K0001: Knowledge of computer architecture concepts
- K0002: Knowledge of operating systems
- K0003: Knowledge of hardware components and functions
- K0005: Knowledge of system vulnerabilities and weaknesses
- K0013: Knowledge of basic system security principles

Skills (S):

- S0001: Identify system components and functions
- S0010: Configure and manage system settings
- S0012: Diagnose hardware/software issues
- S0028: Apply security controls to systems

The result of this format is that students don't just learn what hardware is but how that hardware becomes an attack surface and is utilized by threat actors.

Standard 2: Operating Systems & System Administration
Expanded NICE Tasks and KSs
Tasks (T):

- Manage system configurations to maintain secure operating environments
- Apply updates and patches to mitigate vulnerabilities
- Monitor systems and logs for suspicious or unauthorized activity
- Manage user accounts, permissions, and access controls

Knowledge (K):

- K0002: Operating systems concepts
- K0004: Access control and identity management
- K0006: System administration principles
- K0017: Authentication and authorization mechanisms
- K0022: Security configuration management

Skills (S):

- S0015: Perform system administration tasks
- S0027: Apply updates and patches
- S0031: Manage user accounts and permissions
- S0045: Monitor system performance and logs

Misconfigurations are among the most common real-world vulnerabilities. Understanding how and why these occur is important for creating effective defensive practices.

Standard 3: Networking Fundamentals & Security
Expanded NICE Tasks and KSs
Tasks (T):

- Analyze network traffic to identify anomalies or malicious activity
- Configure and manage network devices securely
- Identify vulnerabilities within network infrastructure
- Monitor network environments for indicators of compromise

Knowledge (K):

- K0037: Network protocols and communication methods
- K0038: Network security concepts
- K0040: Common network vulnerabilities
- K0041: Encryption and secure communication
- K0042: Wireless networking risks

Skills (S):

- S0034: Analyze network traffic
- S0036: Configure network devices
- S0047: Identify anomalous network activity
- S0050: Conduct vulnerability identification

Networks are the backbone of modern digital communication and are frequently targeted attack surfaces. Students learn not only how data moves across systems but also how threat actors exploit vulnerabilities within network infrastructure and communication protocols by framing networking concepts through a cybersecurity lens.

Standard 4: Cyber Threats, Vulnerabilities, and Defensive Strategies
Expanded NICE Tasks and KSs
Tasks (T):

- Conduct threat analysis to identify potential risks and attack vectors
- Perform vulnerability assessments to evaluate system weaknesses
- Detect and analyze cybersecurity threats and incidents
- Implement mitigation strategies to reduce risk and impact

Knowledge (K):

- K0045: Threat analysis methods
- K0046: Vulnerability assessment principles
- K0047: Malware types and behavior
- K0048: Cyber attack lifecycle
- K0052: Defensive cybersecurity strategies

Skills (S):

- S0078: Perform incident response activities
- S0080: Detect and analyze threats
- S0082: Conduct vulnerability scans
- S0084: Implement mitigation strategies

Understanding how cyber threats emerge and evolve helps students move beyond theory into defensive thinking. This standard emphasizes the identification of vulnerabilities, analysis of attack behavior, and implementation of mitigation strategies to develop foundational risk-awareness and incident response skills.

Standard 5: Adversarial Thinking & Ethical Security Practices
Expanded NICE Tasks and KSs
Tasks (T):

- Analyze attack vectors and adversarial techniques
- Simulate attack scenarios to understand system weaknesses (conceptual)
- Evaluate system security posture from an attacker perspective
- Apply ethical reasoning to cybersecurity decision-making

Knowledge (K):

- K0060: Adversarial tactics, techniques, and procedures (TTPs)
- K0061: Penetration testing concepts
- K0062: Social engineering techniques
- K0065: Legal and ethical frameworks

Skills (S):

- S0092: Analyze attack vectors
- S0095: Simulate attack scenarios (conceptual)
- S0098: Evaluate system weaknesses

Cybersecurity professionals should understand how attackers think, adapt, and exploit weaknesses within systems and human behavior. Introducing adversarial thinking in an ethical and developmentally appropriate manner allows students to analyze threats critically while reinforcing responsible decision-making and professional conduct.

Standard 6: Data Security, Privacy, and Emerging Technologies
Expanded NICE Tasks and KSs
Tasks (T):

- Apply risk management principles to protect sensitive data
- Evaluate privacy risks and ensure compliance with regulations

- Assess security implications of emerging technologies (e.g., cloud, AI/ML)
- Implement data protection strategies to safeguard information

Knowledge (K):

- K0018: Data protection methods
- K0059: Privacy principles and regulations
- K0063: Cloud security concepts
- K0067: AI/ML security implications

Skills (S):

- S0057: Apply risk management principles
- S0060: Protect sensitive data
- S0065: Evaluate emerging technology risks

As organizations rely on cloud computing, AI, and data-driven technologies, understanding the security and privacy implications of these systems becomes essential. This standard encourages students to evaluate emerging technologies through a risk-management perspective while emphasizing the importance of protecting sensitive information.

Standard 7: Cybersecurity Communication & Career Pathways
Expanded NICE Tasks and KSs
Tasks (T):

- Communicate cybersecurity concepts to technical and non-technical audiences
- Develop reports and briefings on cybersecurity findings
- Collaborate effectively within cybersecurity teams
- Explore and evaluate cybersecurity career pathways and roles

Knowledge (K):

- K0020: Cybersecurity roles and responsibilities
- K0021: Organizational security policies
- K0023: Workforce development pathways

Skills (S):

- S0020: Communicate technical information
- S0021: Develop reports and briefings
- S0023: Collaborate in team environments

Technical knowledge alone is insufficient in cybersecurity without the ability to communicate findings, collaborate with others, and understand workforce roles. This standard reinforces the importance of professional communication, teamwork, and career exploration to help students connect classroom learning to real-world cybersecurity pathways.