laboratories

MDPI

Article

A Modular Framework for Cybersecurity Laboratory Design in Higher Education

Sharon L. Burton

Department of Applied Aerospace Science, College of Aviation, World Wide, Embry-Riddle Aeronautical University, Daytona Beach, FL 32114, USA; burtons6@erau.edu

Abstract

The escalating frequency and complexity of cyber threats have made cybersecurity education a national priority, yet a practical gap persists between theoretical instruction and workforce readiness. This study presents a comprehensive, modular framework for designing and implementing cybersecurity laboratories in academic institutions, environments that foster hands-on learning, skill mastery, and curricular innovation. Using a mixed-methods, multi-stage case study approach, the research combined qualitative analysis of institutional practices and instructional methods with quantitative evaluation of learning outcomes to comprehensively examine technical and pedagogical considerations impacting lab development. Data sources included literature analysis, direct observation, document review, and semi-structured interviews. The study synthesized best practices across these domains into a scalable lab design model grounded in experiential learning theory. Results demonstrate that the framework supports enhanced student performance, instructional adaptability, and simulation fidelity. Case study data revealed measurable gains in participant competency, with all participants achieving at least a 20% improvement in post-training test scores, high engagement levels demonstrated through consistent session attendance and active participation in hands-on exercises, and successful adaptation to logistical and technological barriers, including facility relocations and system downtime incidents. The lab's modularity enabled curricular alignment, resource efficiency, and expansion to serve workforce training initiatives beyond the classroom. By integrating pedagogical (structured, teacher-guided instructional approaches) and andragogical (adult learning) design with technological scalability, this research contributes an actionable roadmap for institutions seeking to modernize cybersecurity education and respond effectively to evolving digital threats. The findings offer broad implications for future curriculum development, facilitator training, and sustainable program implementation.

Keywords: cybersecurity; laboratory; teaching; course development; experiential learning; lab management

check for updates

Academic Editor: Gassan Hodaifa

Received: 17 July 2025
Revised: 13 October 2025
Accepted: 16 October 2025
Published: 23 October 2025

Citation: Burton, S.L. A Modular Framework for Cybersecurity Laboratory Design in Higher Education. *Laboratories* **2025**, *2*, 21. https://doi.org/10.3390/laboratories2040021

Copyright: © 2025 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The relentless escalation of cyber threats has made robust cybersecurity education an imperative for organizations seeking digital resilience. Academic institutions now stand at the frontline, tasked not only with imparting technical expertise but with fostering the agility, judgment, and adaptability necessary for professionals to anticipate and mitigate sophisticated digital threats [1–3]. While traditional curricula offer foundational knowledge, they rarely suffice in preparing students for the complex, real-world challenges that define contemporary cybersecurity practice [4]. The central question thus emerges: How can

academic institutions construct and operationalize cybersecurity laboratories that transform theoretical comprehension into demonstrable expertise and innovation?

This investigation supports the view that a thoughtfully constructed, modular cybersecurity laboratory serves not just as a technical training facility but also as a vibrant environment fostering experiential learning, enabling cross-disciplinary collaboration, and supporting the management of institutional knowledge. Such laboratories not only cultivate technical proficiency but also reinforce the capture, refinement, and dissemination of intellectual capital, enabling organizations to adapt and thrive in an evolving threat environment. As underscored by [5], effective knowledge management in cybersecurity education is not merely about storing information, but about developing systems that enrich, contextualize, and deploy knowledge across stakeholders for immediate and long-term institutional benefit.

The current landscape is marked by a pronounced disconnect between conceptual instruction and hands-on application [6]. Addressing this gap requires not just technological investment, but also an adult learning vision, one that recognizes the lab as a mechanism for ongoing organizational learning, curricular evolution, and the creation of a sustainable intellectual ecosystem [2,7,8]. The purpose of this study is to develop a comprehensive, scalable framework for the design and management of cybersecurity laboratories that aligns with evolving industry standards, responds to the needs of diverse stakeholders, and embeds best practices in teaching and knowledge stewardship.

In pursuit of this goal, the article begins with an in-depth background on the evolution and current demands of cybersecurity education, before moving to discuss foundational assumptions, key limitations, and the specific scope (delimitations) of the study. This information is followed by a review of the research gap, an outline of the mixed methods methodology and design, an extensive literature review, development and critique of the conceptual framework, an original synthesis of best practices, and separate sections for the results, discussion, and conclusions.

This structure ensures a rigorous exploration of the subject and offers readers a clear pathway to comprehending the rationale and the innovations presented herein.

2. Background

The origin of cybersecurity laboratories can be traced to the growing need for practical, scenario-based training in response to escalating cyber threats [9]. Early educational models focused heavily on theory, leaving graduates underprepared for the complexities of real-world cyber defense [10]. As digital transformation accelerated, institutions recognized the necessity of integrating hands-on labs to simulate attack and defense scenarios.

Currently, cybersecurity labs serve as critical platforms for experiential learning, allowing students to engage with live systems, analyze vulnerabilities, and develop mitigation strategies [11]. Also, as given by [11], the relevance of such labs is underscored by the persistent skills gap in the cybersecurity workforce, which is exacerbated by the rapid pace of technological change. Academic institutions face the pressing challenge of keeping curricula aligned with industry demands and emerging threat landscapes.

A key problem addressed by this research is, as noted by [12], the lack of standardized frameworks for designing cybersecurity labs that cater to diverse educational objectives. Many existing labs are limited by resource constraints, outdated equipment, or insufficient alignment with current best practices [13]. This study aims to fill this gap by proposing a comprehensive model for lab construction and management that emphasizes adaptability, scalability, and integration with comprehensive learning objectives.

The significance of this research lies in its potential to inform best practices for academic institutions seeking to enhance their cybersecurity programs. By systematically

addressing the challenges of lab design, resource allocation, and curriculum integration, the article provides actionable guidance for educators and administrators. The following sections will delve into the assumptions, limitations, and delimitations of the proposed approach, identify the research gap, outline the methodology employed, the literature review, a case study, the conceptual framework and its critique, originality of the text, results, discussion, and conclusion, as well as future research.

3. Assumptions, Limitations, and Delimitations

Several foundational assumptions guide the development of a cybersecurity laboratory. It is assumed that institutional leadership supports the initiative and allocates sufficient resources for initial setup and ongoing maintenance. Another assumption is that facilitators possess or can acquire the necessary expertise to design and facilitate laboratory exercises.

Limitations are inherent in any laboratory project [14]. Budgetary constraints may restrict the acquisition of advanced equipment or the implementation of specific technologies. Physical space and infrastructure may also limit the scale of the lab, influencing the number of concurrent users and the complexity of scenarios that can be simulated. The MACLF development and evaluation was conducted within a single institutional context with one primary facilitator, which may limit the generalizability of findings across diverse educational settings. Institutions with varying resource levels, technological infrastructure, or facilitator expertise may experience different implementation outcomes. Additionally, cultural, organizational, and instructional methodology differences across institutions could influence the framework's effectiveness and require contextual adaptations.

Delimitations define the scope of the study [14]. This article focuses on academic institutions offering undergraduate and graduate cybersecurity programs. The discussion excludes specialized research labs dedicated solely to advanced threat analysis or government-sponsored facilities. The primary emphasis is on labs intended for teaching and course development, with secondary consideration given to research and outreach activities.

4. Research Gaps

Despite recent advancements in cybersecurity education, significant deficits remain in the frameworks that guide the systematic design, deployment, and management of academic cybersecurity laboratories [12]. Scholarly literature offers a patchwork of case studies and isolated technical interventions but lacks comprehensive written analyses and scalable models adaptable to diverse institutional and educational contexts [15,16]. This fragmentation contributes to persistent inconsistencies in curriculum quality and hinders the ability of academic programs to produce graduates who are proficient in conceptual comprehension and hands-on expertise. Recognizing these deficits is significant because it underscores the urgent need for holistic, scalable, and adaptable frameworks that can unify curriculum standards, advance hands-on learning, and better prepare graduates for the complexities of the cybersecurity profession. Addressing these issues is foundational to raising the quality, relevance, and impact of cybersecurity education at both institutional and systemic levels.

A primary deficiency is the misalignment between curricular goals and the dynamic needs of the cybersecurity workforce [17]. Numerous studies [12,17,18] have shown that graduates often enter professional roles lacking practical competence in advanced domains such as incident response, web application security, and cyber-physical systems management. The accelerated pace of technological innovation and the evolving threat landscape frequently outstrips the capacity of academic institutions to update curricula, allocate resources, or integrate new tools and learning modalities, thereby exacerbating this gap.

Compounding these challenges are practical barriers to sustaining effective laboratory environments. Institutions face constraints related to funding, infrastructure, and continuous professional development for facilitators. There is also a documented lack of standardized processes for updating laboratory content or integrating iterative industry and stakeholder feedback, which are crucial for maintaining relevance and fostering ongoing innovation. Additionally, while virtual labs and remote access environments offer promise for expanding educational access and mitigating resource disparities, their effectiveness in supporting sustained engagement, mastery of complex technical skills, and alignment with industry requirements remains underexamined in the literature. As noted by [19], the absence of rigorous, longitudinal research on these models further limits the ability of educators to adopt evidence-based practices that deliver measurable outcomes.

In summary, the research gap consists of three concerns. There is a lack of a holistic, adaptable framework for the design and management of cybersecurity laboratories that aligns pedagogy, andragogy, technology, and workforce requirements. Insufficient mechanisms exist for the integration of ongoing industry feedback and rapid technological advances within academic lab settings. Also, there is a scarcity of empirical studies examining the long-term impact of virtual and physical lab experiences on student outcomes and workforce readiness. Addressing these interconnected gaps is essential for developing resilient, future-proof cybersecurity education systems capable of producing graduates who are agile, technically competent, and prepared for the multifaceted challenges of the contemporary threat environment.

5. Materials and Methods

This study employed a mixed-methods, multi-stage case study approach, incorporating elements of action research to support iterative improvement and learner participation throughout laboratory development. The methodology included (a) semi-structured interviews with facilitators and participants; (b) direct participant observation during lab sessions; (c) structured document analysis of training and session logs; and (d) administration and statistical analysis of standardized pre- and post-training assessments. This combined fieldwork and data collection design offered insight into lived experiences, institutional dynamics, and real-world effectiveness of the lab, supporting both meaning-making (qualitative) and outcome measurement (quantitative).

In cybersecurity education, where curricula, infrastructure, policy, and learner behavior intersect, a combination of field research methods (i.e., participant observation, interviews, and action cycles) offers explanatory richness and depth; in contrast, quantitative metrics (test scores, completion rates) provide complementary evidence of measurable learning outcomes [17,20].

The multi-stage, mixed methods case study incorporated action research cycles encompassing planning, intervention, participant observation, structured reflection, and revision of lab processes. Fieldwork included semi-structured interviews, participant observation in live training sessions, and structured document review of curriculum materials and resource deployments. Quantitative learning outcome data were collected at multiple stages using pre- and post-training assessments and analyzed via descriptive statistics and comparative methods. Together, these processes ensured research credibility and a multidimensional understanding of educational, technical, and organizational factors.

Depth and Contextualization: The case study design supported detailed engagement with a specific educational setting [21]. It enabled the exploration of how cybersecurity labs were conceptualized and adapted in response to technical challenges, stakeholder needs, and institutional constraints. By examining design phases, implementation barriers, and user feedback loops, the research surfaced why and how certain practices succeeded

or required adjustment. These insights are crucial for model replication and scaling. In addition, quantitative pre- and post-training assessments provided direct measures of skill and knowledge gains, complementing the qualitative insights with objective evidence of learning impact.

Integration of Multiple Data Sources: The methodology combined field methods (i.e., semi-structured interviews, direct participant observation, periodic facilitator focus groups, and document analysis of course materials and session logs) with quantitative assessment of pre- and post-training outcomes. Thematic coding of qualitative data and descriptive statistical analysis of learning assessments were triangulated to reveal both subtle and overt influences on laboratory effectiveness, improving the depth and reliability of findings [15,22].

Adaptability: The action research framework enabled ongoing cycles of planning, intervention, field observation, reflection, and refinement across all project phases. As new insights emerged from field data, interview reflection, and performance assessment, instructional content and research protocols were systematically revised. This process supported rapid adaptation to disruptions and maintained the relevance and rigor of qualitative and quantitative data collection [20].

This approach aligns with literature identifying case study research as particularly effective in educational innovation contexts, where goals include building recursive models and practical frameworks informed by real conditions [17]. The research, therefore, produced outcomes that are robust and transferable to institutions seeking to apply or scale lab-based programs (i.e., cybersecurity). It also highlights the value of context-aware, practitioner-informed design processes that support continuous adaptation across diverse institutional environments.

Empirically, case study designs are widely recognized as the gold standard for educational innovation research where the phenomenon under study is intertwined with context; also where the aim is to develop or refine practical frameworks rather than test isolated hypotheses [2,17,20]. By employing a mixed methods inquiry built on action research principles, and emphasizing qualitative field methods and quantitative assessment within a case study structure, this article safeguards its findings are relevant, robust, and transferable to organizations seeking to amplify cybersecurity education.

Detailed Data Collection Procedures And Analysis Protocols: The detailed data collection procedures and analysis protocols were incorporated as a distinct subsection within the Materials and Methods to enhance methodological transparency and rigor. Semi-structured interviews were scheduled with facilitators and laboratory participants at three strategic points in each pilot cycle: before the start of the laboratory, at the mid-point, and upon completion. Interview guides solicited participants' perspectives on the instructional value, the relevance of laboratory experiences, encountered challenges, and suggestions for improvement. In addition to interviews, focus groups were convened at the end of each pilot session to promote collaborative reflection and to gather group-level insights on laboratory processes and learning culture.

Throughout all laboratory sessions, participant observation was conducted using a standardized observation checklist. This instrument was designed to capture participant engagement, collaborative dynamics, problem-solving strategies, and the efficacy of facilitator interventions. Observers recorded quantifiable actions (i.e., the frequency of active participation and the resolution of technical tasks), as well as qualitative impressions of instructional resilience and learner adaptability. This researcher also collected session logs, resource inventories, and training artifacts for supplemental analysis.

Interview and focus group sessions were audio-recorded and transcribed verbatim. All qualitative data, including observation notes, were analyzed for inductive coding.

Thematic codes were iteratively developed to identify patterns relating to instructional effectiveness, laboratory adaptability, and emergent barriers. To ensure reliability, subsets of the qualitative data were double-coded by two independent researchers, and discrepancies were resolved through consensus meetings. Member checking was employed by sharing preliminary findings with participants to validate interpretations and incorporate their perspectives.

The study followed explicit action research cycles: after each laboratory pilot, data from interviews, focus groups, and observations were rapidly analyzed and shared in debriefing sessions with facilitators and key participants. Feedback and reflective input were then used to refine the laboratory structure, update instructional materials, and adjust assessment tools and research protocols before the next pilot iteration. This systematic cycle of planning, action, observation, and reflection ensured that the laboratory environment and the research design remained adaptive, stakeholder-responsive, and continuously improved in alignment with evolving educational and technological demands.

Case Study

A pilot laboratory initiative was conducted across five separate six-week sessions to evaluate design feasibility and instructional effectiveness. Each pilot enrolled 15 to 25 adult learners, ages 23 to 55, all of whom had prior technical or operational work experience (minimum three years) and represented diverse professional and vocational backgrounds. Pre-training and post-training assessments were used to measure knowledge increases and broader learning outcomes quantitatively; at the same time, session observations and facilitator reflections offered qualitative process data, permitting a comprehensive mixed-methods evaluation. The in-person training delivered eight-hour sessions (with one-hour daily breaks) over multiple weeks, incorporating structured formative and summative assessments. Participants engaged in hands-on scenarios that involved system simulation, vulnerability testing, software use, classroom dialogue, and procedural walkthroughs [23]. Assessment mechanisms included quizzes, demonstrations, and applied system interaction tasks designed to quantitatively measure real-world ability attainment and offer numerical evidence of learning [24]. All participants improved their test scores by at least 20%, demonstrating alignment between training content, lab structure, and intended instructional outcomes.

Instructional Materials and Assessment Tools

Instructional content employed a variety of modalities, including:

- Manuals and scenario-based guides
- Video lectures and procedural demonstrations
- Software simulations and sandbox environments
- Readings, knowledge checks, and operator tasks

The sandbox, or virtual practice environment, was configured for safe experimentation with realistic system configurations [25,26]. The sandbox, or virtual practice environment, refers to a computer-based simulation designed to facilitate the development and testing of specific knowledge, skills, and capabilities. While sandbox environments have long been used in technical training and cybersecurity education, recent advancements have expanded their scope to include more complex, interdisciplinary competencies such as threat detection, ethical hacking, and strategic response planning. What distinguishes contemporary sandbox platforms is not their architecture. The evolving nature of the skills they assess reflects the dynamic demands of the cybersecurity workforce and the increasing emphasis on experiential learning. Logs recorded daily participation, observed behaviors, and instructional deviations. Feedback loops tracked what materials proved most useful based on participant performance and feedback, enabling fine-tuning between sessions.

Implementation Fidelity and Barriers

Facilitation consistency across all sessions was preserved by using the same lead instructor [27], a subject-matter expert with over two decades of experience and multiple academic credentials. Training fidelity was supported through structured adherence checks, real-time adjustments to accommodate learner needs, and explicit documentation of any training deviations or logistical workarounds. Two significant barriers were encountered:

Barrier One: Spatial Reassignment

During one session, a facility scheduling conflict required the training group to relocate. Through cooperation with another department, the facilitator secured a comparable space with equivalent technological infrastructure. This transition was implemented without incident. However, future efforts should account for the potential instructional impact of spatial disruptions on learner focus, logistical flow, and group cohesion.

Barrier Two: Sandbox Downtime

In another instance, the sandbox system was inaccessible due to pending software updates and interface adjustments. During this time, the facilitator redirected the instruction to theoretical discussions, concept-based assessments, and peer-led analysis to ensure continuity. These adaptations reflect the flexibility and resilience necessary in operational learning environments and underline the need for reliable infrastructure planning [22,25].

This case study, grounded in an iterative and responsive methodology, validated core elements of the proposed lab framework and also revealed nuanced variables influencing implementation success. These insights formed the empirical foundation for recommendations offered in later sections of this article. These findings contributed to a deeper comprehension of how educational design, technical infrastructure, and institutional dynamics interact to influence the effectiveness and sustainability of cybersecurity laboratory environments.

6. Literature Review

Evolution of Cybersecurity Education

Over the past two decades, cybersecurity education has undergone a paradigm shift from predominantly theoretical instruction to practice-oriented learning [6]. Initially, academic programs emphasized rote memorization and static conceptual frameworks, which proved insufficient in preparing students for the rapidly evolving threat landscape [9]. With the rise of sophisticated cyberattacks and systemic vulnerabilities across critical infrastructures, educational institutions recognized the necessity of incorporating experiential components better to equip learners with real-world problem-solving skills [6].

As a response to these deficiencies, the introduction of laboratory environments has become an increasingly vital learning methodology. Cybersecurity labs allow students to simulate attack-and-defense scenarios, investigate vulnerabilities, and test mitigation techniques in a controlled context [11]. These settings shift the learning experience from passive content absorption to active engagement, a transformation that aligns with contemporary learning science, emphasizing the significance of applying knowledge through hands-on exploration [1,2].

6.1. Best Practices in Laboratory Design

Designing effective cybersecurity laboratories requires thoughtful attention to modularity, scalability, and technological adaptability. A modular structure permits incremental lab development, enabling institutions to expand or tailor resources based on evolving instructional goals or technological demands [15]. Scalability ensures that laboratory environments can accommodate changes in enrollment size, curriculum breadth, and levels of

learner experience, which is essential for sustaining inclusive and accessible programming across diverse cohorts [18].

Virtualization stands out as a cornerstone of contemporary lab design, offering dynamic network simulations without the cost and rigidity of physical infrastructure. Leveraging virtual machines and containerized environments enables the recreation of complex cyber ecosystems using minimal hardware, thereby maximizing resource efficiency and educational effectiveness [28]. Additionally, embedding assessment tools within these environments allows instructors to track learner progress and proficiency in real time, informing adaptive feedback loops and instructional refinements [22].

6.2. Curriculum Integration and Instructional Alignment

A practical cybersecurity laboratory does not function in isolation; its value emerges through intentional alignment with curricular outcomes and comprehensive instructional design. Facilitator collaboration with instructional designers is vital to ensure that lab scenarios reinforce course objectives and foster domain-specific knowledge and transferable competencies, such as collaboration, decision-making, and analytical prowess [29]. Continuous alignment with frameworks like NICE further strengthens the lab's validity in preparing students for industry certification and workplace integration [12].

The integration of labs into broader programmatic structures supports longitudinal skill-building across multiple courses and learning stages. Research accentuates the significance of weaving hands-on exercises into theoretical instruction, where iterative lab progression builds from foundational awareness to advanced diagnostic and intervention capabilities [17]. This vertical alignment increases retention, reinforces comprehension, and enables students to scaffold learning effectively toward professional readiness.

6.3. Challenges and Critiques

Despite notable progress, substantive challenges persist in sustaining effective cybersecurity laboratories. Resource disparities among institutions create uneven access to advanced tools, facilitator expertise, and infrastructure necessary for state-of-the-art lab environments [30]. Smaller colleges or underfunded programs may struggle to implement virtualization technologies or develop realistic scenarios that mirror industry demands, placing their students at a disadvantage. These inequities highlight the ongoing need for collaborative consortia, open-source environments, and shared instructional assets to democratize access to quality instruction.

Moreover, facilitator development remains a persistent bottleneck. Studies reveal that many instructors lack experience with lab-based teaching and require targeted professional development to facilitate experiential learning [31] effectively. Institutional commitment to facilitator training and curricular innovation is therefore foundational to successful lab adoption [32]. The rapid pace of technological evolution further compounds these challenges, demanding regular updates to lab configurations and teaching materials to reflect current threats and tools [33].

6.4. Synthesis

Overall, the literature positions cybersecurity laboratories as indispensable components of 21st-century cyber education. They bridge the gap between abstract theoretical learning and high-demand workforce competencies, offering experiential depth and instructional agility. By implementing modular, scalable, and curriculum-integrated labs, academic institutions can foster innovation, improve learner outcomes, and reinforce digital resilience at the individual and organizational levels.

7. Conceptual Framework

The proposed framework for building a cybersecurity laboratory is grounded in experiential learning theory that was developed in 1984 by an American educational theorist and psychologist, David A. Kolb [1,7,29]. David Kolb's theory of experiential learning, influenced by the foundational work of John Dewey, Jean Piaget, and Kurt Lewin, conceptualizes learning as a cyclical process involving four distinct stages: concrete experience, reflective observation, abstract conceptualization, and active experimentation [1,7,16]. In this model, learners first engage directly with experiences, then reflect on those experiences, develop abstract ideas or theories from their reflections, and finally apply these concepts through experimentation in new contexts [1]. Kolb also delineated four learning styles (i.e., diverging, assimilating, converging, and accommodating), each representing a preferred approach to perceiving and processing experiences [1]. His framework has significantly shaped educational practices, particularly in disciplines that emphasize experiential and applied learning, such as cybersecurity, aviation, aerospace, and engineering. See Figure 1 for the framework.

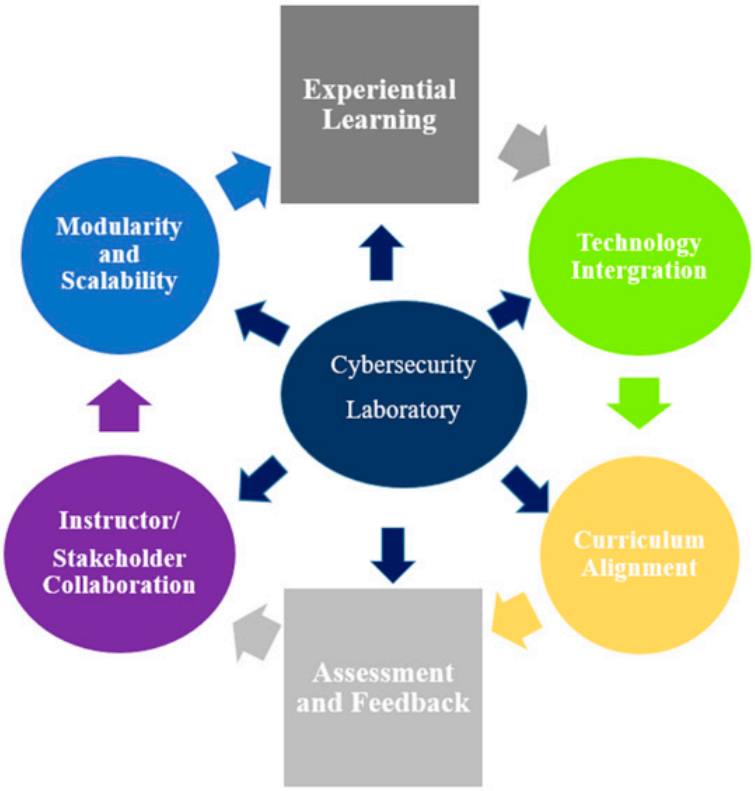


Figure 1. The Modular Adaptive Cybersecurity Laboratory Framework (MACLF) by Dr. S. L. Burton (2025). Modular, adaptive framework for academic cybersecurity laboratory design, highlighting core components and dynamic feedback integration. Created by Dr. Sharon L. Burton.

This approach emphasizes active engagement, reflection, and iterative improvement, enabling students to develop critical thinking and problem-solving skills [7,29,34]. This framework, created by Dr. S. L. Burton, incorporates modular design, virtualization, and continuous feedback, ensuring that the lab remains responsive to technological advancements as well as evolving learning requirements. Each modular adaptive framework's element directly corresponds to Kolb's experiential learning cycle. See Table 1.

Table 1. Alignment Between ACCLF Elements and KOLB's Learning Stages.

Modular, Adaptive Framework For Academic Cybersecurity Laboratory Design (MACLF)	**Kolb's Stage**
Hands-on Scenarios	Concrete Experience
Assessment/Feedback	Reflective Observation
Theoretical Integration	Abstract Conceptualization
Iterative Refinement	Active Experimentation

Note: The MACLF components are strategically aligned with Kolb's experiential learning cycle to facilitate complete learning progression from hands-on practice through theoretical understanding. This alignment ensures that cybersecurity laboratory experiences maximize practical skill development and conceptual mastery.

This modular, adaptive framework is optimal because it balances flexibility with structure, allowing institutions to tailor the lab to their unique requirements while maintaining alignment with best practices. The emphasis on experiential learning ensures that students graduate with practical competencies and the ability to adapt to emerging challenges. While this framework demonstrates effectiveness within the studied institutional context, future implementation should consider how varying institutional characteristics might influence outcomes. The MACLF's modular design addresses this limitation by permitting institutions to adapt components based on their distinctive resource constraints, facilitator expertise levels, and student populations. Institutions considering adoption should assess their technological infrastructure, available expertise, and learner demographics to optimize framework customization.

8. Conceptual Framework Critiques

One critique of the experiential learning framework is its reliance on significant facilitator expertise and ongoing professional development. Without sustained investment in facilitator training, the effectiveness of hands-on labs may be diminished [31]. Earlier, ref. [32] highlighted several key challenges that hinder the adoption of experiential learning strategies in higher education, notably citing facilitator hesitation, limited availability of time, and a lack of sufficient training as primary barriers.

Another significant consideration is the potential for resource disparities between institutions, which can affect the quality and accessibility of laboratory experiences [3]. Moreover, the rapid pace of technological change necessitates continuous updates to lab infrastructure and curricula, posing challenges for long-term planning and budgeting [33]. These factors emphasize the significance of developing adaptable strategies that can ensure equitable and effective laboratory learning opportunities across diverse educational settings.

Further, research examining inequities in educational resources indicates that conventional hands-on laboratories typically require significant financial investment in equipment and facilities, which can pose challenges for institutions with limited budgets [3]. While virtual and remote laboratory options have been developed to address these barriers and broaden participation, they may not fully capture the sensory experience or the collaborative dynamics inherent in traditional in-person labs. Additionally, research on faculty perception indicates that while many educators recognize the value of experiential learning, implementation barriers persist due to varying levels of comfort with hands-on learning approaches [35]. These critiques highlight the significance of institutional commitment, resource allocation, and strategic planning in the successful implementation of cybersecurity labs.

9. Originality of the Text

The originality of this article lies in its synthesis of contemporary best practices, theoretical insights, and practical strategies to construct a cybersecurity laboratory model tailored explicitly for academic teaching and course development. Unlike cybersecurity prior works that often focus on isolated technical solutions or narrow case studies, this research integrates diverse perspectives from recent literature, institutional experiences, and evolving industry demands to propose a holistic, adaptable framework. This integrative approach ensures that the model is not only grounded in current technological realities but also remains responsive to the rapid shifts characterizing the cybersecurity landscape [18,28,36].

For example, a research team [9] offered a critique of cybersecurity labs that emphasize technical depth (i.e., the use of virtual machines and attack–defense scenarios) without sufficient attention to instructional design. They argue that such labs often prioritize high-fidelity simulations at the expense of learning structure, resulting in environments that replicate real-world complexity without effectively supporting learner engagement.

A separate example of an infrastructure-heavy approach can be found in the 2023 research by [37]. This initiative centers on simulating cyber-attacks on smart grids using virtual environments, with a strong emphasis on technical fidelity and system realism. The lab was designed to support various training and experimental scenarios through virtual machines and network configurations. However, the model offered limited integration with pedagogical frameworks or learner-centered design, reinforcing concerns that technically robust environments may lack the instructional scaffolding necessary to support diverse educational outcomes. As such, it exemplifies an isolated technical solution, prioritizing simulation capabilities while underemphasizing educational adaptability and engagement.

In 2025, the research team [27] examined how cybersecurity frameworks have been implemented across educational institutions, supporting a tailored security model. Their analysis reveals that many existing frameworks prioritize technical controls while overlooking educational alignment (the fit between cybersecurity practices and the diverse teaching and learning needs of different learners and contexts) [27]. This information places their work within the grouping of isolated technical solutions; it illustrates how a strong technical emphasis may undermine instructional effectiveness and contextual adaptability.

Recent research emphasizes the necessity of holistic, adaptable frameworks for cybersecurity education that can keep pace with technological advancements and the shifting threat landscape [28,36]. For example, comprehensive surveys and guidance documents highlight the significance of modular, scalable lab environments that support hands-on, experiential learning and align with current industry standards, and instructional frameworks [18]. The integration of diverse methodologies and continuous feedback mechanisms is recognized as essential for maintaining relevance and fostering innovation in academic settings [18,29].

Additionally, the literature accentuates the significance of grounding laboratory models in real-world scenarios and ensuring that curricula are responsive to rapid changes in technology and threat vectors [36]. This integrative and forward-thinking approach not only addresses the limitations of earlier, narrowly focused works but also offers a replicable model that can be adapted to various institutional contexts, thus expanding access and improving the quality of cybersecurity education [18,29].

The MACLF's originality lies in three specific innovations that are lacking in existing models. First, existing models typically fall into two categories, technical approaches that prioritize simulation fidelity or educational frameworks that emphasize learning outcomes. This MACLF bridges both domains through explicit alignment with Kolb's experiential learning cycle, creating systematic learning grounding absent in either approach alone.

Second, unlike static, institution-specific models, the MACLF introduces true modularity through component-based architecture that enables customization while maintaining educational effectiveness across diverse institutional contexts. Third, this framework pioneers embedded continuous feedback mechanisms that facilitate real-time adaptation, contrasting sharply with conventional models where assessment occurs post-implementation rather than being integrated into the design process.

10. Results

Implementation of the proposed cybersecurity laboratory framework has yielded a constellation of concrete and meaningful outcomes for academic institutions. Foremost among these was a marked increase in student engagement, observed through robust participation in experiential exercises, heightened enthusiasm for solving complex cybersecurity challenges, and a demonstrable improvement in practical competencies. Mixed methods assessment findings indicated that learners steadily showed numerically noteworthy gains in post-training evaluations, recurrently exceeding their baseline performance by a significant margin. Quantitative results confirmed at least a 20% enhancement in test scores for all participants, while qualitative data contextualized these enhancements through observed behaviors and participant feedback. These results are presented not only as aggregate improvements but are further disaggregated to illuminate progress across various cohorts and demographic groups, thereby revealing the equity and reach of the laboratory's impact.

The modular architecture of the laboratory has proven instrumental in facilitating incremental expansion and technological adaptability. Institutions leveraging this design benefit from the ability to seamlessly integrate cutting-edge tools, respond efficiently to emergent threat vectors, and tailor instructional content to evolving industry standards. In practical terms, this action has translated into the delivery of increasingly complex simulation scenarios without necessitating substantial new investments in hardware infrastructure. Virtualization technologies, for example, have enabled the recreation of multifaceted attack-and-defense environments, thereby optimizing resource utilization and broadening the scope of instructional possibilities [8].

Institutional stakeholders reported ancillary benefits beyond student learning. The laboratory has catalyzed interdisciplinary collaboration, promoting shared projects and research initiatives that span departments and academic units [38]. According to this research team, virtual laboratories contribute to the improvement and progression of collaborative learning by incorporating mechanisms that facilitate communication and foster group awareness. Such environments permit consequential engagement between learners and instructors across diverse disciplines, thereby encouraging the co-construction of knowledge and collective problem-solving. Nonetheless, existing research underscores persistent limitations in the availability of structured tools to guide and regulate collaboration, highlighting critical directions for future investigation and design [38].

Another example is the work of the team that researched a multi-institutional cybersecurity lab platform designed for hands-on learning [39]. The work emphasizes interdisciplinary collaboration across IT, business, and e-commerce domains. It addresses the global cybersecurity workforce gap through outcome-based education and platform-driven training [39].

In 2025, Ohio University's SecureAcademy Partnership exemplifies the integration of interdisciplinary collaboration and experiential learning within cybersecurity education [40]. Through its B.S. in Cybersecurity Operations program, the initiative merged technical, analytical, and operational competencies by engaging departments such as Communication, Business, and Engineering. The program featured immersive threat simulation

laboratories, industry-recognized certifications, and gamified learning environments that mirror real-world scenarios. These elements were strategically designed to align with evolving industry expectations while fostering cross-disciplinary teaching and curricular innovation [40].

The Cybersecurity Field Training Experience (C-FTE), developed by the Commonwealth Cyber Initiative in 2025, addressed the critical shortage of cybersecurity professionals in Virginia, where over 51,000 job openings remain unfilled [41]. Recognizing that the current pipeline of degree-seeking candidates remains insufficient, the program strategically engaged students from nontraditional backgrounds (i.e., majors in IT, mathematics, and business) by equipping them with hands-on cybersecurity skills. The initiative pairs graduate student subject matter experts and project supervisors with undergraduate students, forming interdisciplinary teams that collaborate with industry and government partners. Graduate students continue to serve as technical mentors, guiding undergraduates through real-world project tasks while simultaneously cultivating their own leadership capabilities. This dual-impact model prepares undergraduates for entry-level cybersecurity roles and fosters the development of mid-level managerial competencies among graduate participants, thereby expanding and diversifying the cybersecurity workforce [41].

Such collaboration has underpinned the laboratory's role as a nucleus for curricular innovation, fostering the continuous refinement of program offerings and the alignment of educational objectives with the dynamic expectations of the cybersecurity workforce. Additionally, regular feedback mechanisms embedded within the laboratory's operations have illuminated strengths and areas for growth, thereby reinforcing a culture of evidence-based improvement and iterative redesign.

The laboratory model's scalability is further reflected in its capacity to accommodate fluctuating enrollments and to support outreach initiatives involving external partners. Notably, several institutions have leveraged the modular framework to deliver short-term training and certification programs for industry practitioners, amplifying the laboratory's visibility and bolstering institutional reputation.

Despite these gains, the implementation process was not without challenges. The case study encountered barriers related to resource allocation and infrastructure disruptions. The need for ongoing facilitator development was a concern and would be addressed in future studies. Documenting obstacles and their successful mitigation strategies has further contributed to a transparent and instructive narrative of laboratory advancement. Concluding, these results collectively attest to the efficacy and transformative potential of the proposed laboratory framework in nurturing graduates (e.g., cyber-capable) and catalyzing educational innovation within the academic landscape.

11. Discussion

The establishment of a cybersecurity laboratory signals a decisive strategic shift in the educational paradigm, positioning academic institutions at the forefront of preparing learners for a swiftly evolving digital world. Beyond its immediate instructional function, the lab's true meaning lies in its ability to cultivate a culture of innovation, critical inquiry, and institutional agility, qualities imperative for sustainable resilience in the face of ceaseless cyber threat evolution [42]. By serving as a nexus for experiential learning, interdisciplinary collaboration, and real-time problem solving, the laboratory empowers students and facilitators alike to engage proactively with emerging cybersecurity challenges and technologies.

A central significance of the results is the demonstration of how experiential, lab-based learning transforms abstract curriculum objectives into demonstrable competencies. Students are not merely passive recipients of theoretical content; instead, they emerge as

active agents equipped with the judgment, tactical acumen, and adaptability requisite for navigating complex real-world scenarios [43]. This transition from theory to practice closes the ubiquitous skills gap and renders graduates more competitive and workforce-ready.

For the facilitator and the academic institution at large, the cybersecurity lab could function as a nucleus of interdisciplinary synergy. It could encourage the breakdown of silos, facilitating collaborative research projects, knowledge exchange, and shared instructional approaches across departments. Such an adaptive cybersecurity innovation hub environment accelerates curricular innovation, continuously re-aligning program content with industry trends and regional workforce needs. The presence of a sophisticated laboratory infrastructure further enhances the institution's reputation, positioning it as a leader in delivering relevant, high-impact education.

The lab's modular and scalable design amplifies its strategic value. By accommodating fluctuating enrollments, integrating new technologies, and supporting outreach or certification programs for professionals, the lab transforms from a static educational asset to a dynamic platform for institutional growth and external engagement. This versatility ensures that the laboratory remains responsive to internal strategic priorities and external stakeholder demands, including those of industry partners and community organizations.

Nonetheless, the execution of such an ambitious initiative is not without its complexities. Resource allocation challenges, from funding to facilitator development, necessitate robust, visionary leadership and proactive strategic planning. Institutions are compelled to adopt flexible operational models, leveraging phased investments, fostering external partnerships, and embedding feedback mechanisms to ensure ongoing relevance and impact. The lab's success is ultimately measured not only by immediate learning gains but by its capacity to adapt, scale, and facilitate continual improvement.

Notably, the laboratory's openness to iterative refinement reflects a broader commitment to evidence-based educational practice. Regular assessment cycles, encompassing technical performance and learning outcomes, served as catalysts for reflective adaptation and innovation. Institutions that embrace this ethos are better positioned to respond to emerging cyber risks, capitalize on new technological advancements, and anticipate shifts in the educational landscape [44].

In sum, the results of this initiative accentuate the deep and enduring value of a thoughtfully conceived laboratory (i.e., cybersecurity, operations, management, etc.). Its most tremendous significance is found in the cultivation of an ecosystem that advances not only individual learner success, but also broad institutional and organizational excellence and societal readiness for the challenges of tomorrow's digital frontier. By fostering agile educational responses and collaborative innovation, the laboratory model empowers academic institutions to lead in shaping a resilient, future-oriented cybersecurity workforce.

12. Conclusions and Future Research

This comprehensive framework, Dr. S. L. Burton, outlined in this study for designing and implementing a cybersecurity laboratory, addresses a pressing educational need by bridging the gap between theoretical knowledge and applied skills. By integrating experiential learning principles and modular lab design, the framework equips students with practical competencies directly aligned with industry demands [1,7]. These findings reinforce the significance of a hands-on, adaptive educational environment in producing graduates who are workforce-ready and capable of responding to evolving cybersecurity challenges [8].

The original contribution of this research is its synthesis of current best practices and educational theory into a replicable lab model tailored for teaching, plus curriculum and course development. This model not only supports student achievement but also enhances

facilitator collaboration, institutional and organizational adaptability, and the scalability of cybersecurity programs [29]. The Modular Adaptive Cybersecurity Laboratory Framework (MACLF) is significant because it advances student achievement [45,46] and strengthens facilitator collaboration [45,46], enhances institutional adaptability [44,45], and enables scalable growth [45,46] of cybersecurity programs, ensuring that educational environments remain responsive to evolving industry demands and continuously foster innovation at organizational and systemic levels. Policy and management implications include the necessity of sustained resource investment, ongoing facilitator professional development, and continuous alignment with rapidly changing technological and threat landscapes [47,48]. The study also highlights the significance of regular assessment cycles and stakeholder feedback in maintaining the relevance and impact of lab-based education [2].

The limitations of this work are resource constraints, challenges in keeping laboratory infrastructure current with technological advancements, and the limited numerical generalizability associated with the sample size and lack of a control group for the quantitative assessments [38]. This factor may hinder widespread adoption in less-funded institutions [31]. Additionally, disparities in facilitator expertise and support can affect the quality of experiential learning opportunities [28]. Despite these challenges, the framework's emphasis on modularity and feedback-informed iteration provides a foundation for continuous improvement and adaptability across diverse educational contexts [30,49].

Future research should investigate the integration of emerging technologies (i.e., artificial intelligence, automation, and advanced simulation tools) into cybersecurity laboratory environments. To address this gap, future research should undertake extended studies that follow graduates over multiple years, assessing career progression, certification attainment, and workplace advancement. Additionally, longitudinal inquiry should examine how laboratory adoption influences broader institutional change, including program innovation, expansion, and interdisciplinary collaboration. These continued investigations will yield deeper insights for refining cybersecurity laboratory models and aligning education with evolving professional and organizational demands. By adopting the proposed model and fostering a culture of ongoing assessment and innovation, institutions and organizations will be better positioned to meet the needs of the digital future and to prepare graduates capable of safeguarding complex information environments.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Kolb, D.A. *Experiential Learning: Experience as the Source of Learning and Development*; Prentice-Hall: Hoboken, NJ, USA, 1984.
2. National Research Council. *Education for Life and Work: Developing Transferable Knowledge and Skills in the 21st Century*; The National Academies Press: Washington, DC, USA, 2012. [CrossRef]
3. National Research Council. *America's Lab Report: Investigations in High School Science*; The National Academies Press: Washington, DC, USA, 2006. [CrossRef]
4. John, S.N.; Noma-Osaghae, E.; Oajide, F.; Okokpujie, K. Cybersecurity Education: The Skills Gap, Hurdle! In *Innovations in Cybersecurity Education*; Daimi, K., Francia, G., III, Eds.; Springer: Cham, Switzerland, 2020; pp. 361–376. [CrossRef]
5. Dodla, T.R.; Jones, L. Identifying knowledge management strategies for knowledge management systems. *Access Sci. Bus. Innov. Digit. Econ.* **2023**, *4*, 261–277. [CrossRef]

6. Fantinelli, S.; Cortini, M.; Di Fiore, T.; Iervese, S.; Galanti, T. Bridging the gap between theoretical learning and practical application: A qualitative study in the Italian educational context. *Educ. Sci.* **2024**, *14*, 198. [CrossRef]
7. Matsuo, M. Supporting experiential learning for expanding successes: Extending Kolb's model. *Hum. Resour. Dev. Int.* **2025**, *28*, 423–445. [CrossRef]
8. Tuncel, A.; Atan, A. How to clearly articulate results and construct tables and figures in a scientific paper? *Turk. J. Urol.* **2013**, *39* (Suppl. S1), 16. [CrossRef] [PubMed]
9. Mukherjee, M.; Le, N.T.; Chow, Y.-W.; Susilo, W. Strategic approaches to cybersecurity learning: A study of educational models and outcomes. *Information* **2024**, *15*, 117. [CrossRef]
10. Hickey, D.T.; Kantor, R.J. Comparing cognitive theories of learning transfer to advance cybersecurity instruction, assessment, and testing. *J. Cybersecur. Educ. Res. Pract.* **2024**, *2024*, 19. [CrossRef]
11. ICS2. 2024 ISC2 Cybersecurity Workforce Study Prepares for an AI-Driven World. *ISC2*, 31 October 2024.
12. Karagiannis, S.; Magkos, E.; Karavaras, E.; Karnavas, A.; Nikiforos, M.N.; Ntantogian, C. Towards NICE-by-design cybersecurity learning environments: A cyber range for SOC teams. *J. Netw. Syst. Manag.* **2024**, *32*, 42. [CrossRef]
13. Sanchez, T. Bridging the Gap Navigating: The Challenges of Modern Cybersecurity, RSA Conference Blog. Available online: https://www.rsaconference.com/library/blog/key-takeaways-from-rsactm-2025-conference (accessed on 21 May 2025).
14. Saldaña, J. *The Coding Manual for Qualitative Researchers*, 4th ed.; Sage Publications: Thousand Oaks, CA, USA, 2021.
15. Irvine, C.E.; Thompson, M.F.; Khosalim, J. *Labtainers: A Framework for Parameterized Cybersecurity Labs Using Containers*; Naval Postgraduate School Technical Report; Calhoun Institutional Archive of the Naval Postgraduate School: Monterey, CA, USA, 2023.
16. Burton, S.L. Best Practices for Faculty Development Through Andragogy in Online Distance Education. Ph.D. Dissertation, The National Graduate School of Quality Management, Falmouth, MA, USA, 2014.
17. Towhidi, G.; Pridmore, J. Aligning cybersecurity in higher education with industry needs. *J. Inf. Syst. Educ.* **2023**, *34*, 70–83.
18. Ismail, M.; Madathil, N.T.; Alalawi, M.; Alrabaee, S.; Al Bataineh, M.; Melhem, S.; Mouheb, D. Cybersecurity activities for education and curriculum design: A survey. *Comput. Hum. Behav. Rep.* **2024**, *16*, 100501. [CrossRef]
19. Kebande, V.R. The impact of virtual laboratories on active learning and engagement in cybersecurity distance education. *arXiv* **2024**, arXiv:2404.04952. [CrossRef]
20. Harrison, H.; Birks, M.; Franklin, R.; Mills, J. Case study research: Foundations and methodological orientations. *Forum: Qual. Soc. Res.* **2017**, *18*, 19.
21. Waters, L.; Johnstone, A. Embedding Well-being into School: A Case Study of Positive Education Before and During COVID-19 Lockdowns. *J. Sch. Educ. Psychol.* **2022**, *2*, 60–77. [CrossRef]
22. Chernikova, O.; Heitzmann, N.; Holzberger, D.; Seidel, T.; Fischer, F. Simulation-based learning in higher education: A meta-analysis. *Rev. Educ. Res.* **2020**, *90*, 499–541. [CrossRef]
23. Kavak, H.; Padilla, J.J.; Vernon-Bido, D.; Diallo, S.Y.; Gore, R.; Shetty, S. Simulation for cybersecurity: State of the art and future directions. *J. Cybersecur.* **2021**, *7*, tyab005. [CrossRef]
24. Denton, K.; Simmons, M. Virtual Learning Assessment: Practical Strategies for Instructors in Higher Education. *J. High. Educ. Theory Pract.* **2021**, *3*, 42–48.
25. Aebersold, M. Simulation-based learning: No longer a novelty in undergraduate education. *Cent. Med. Simul.* **2018**, *23*, 1. [CrossRef]
26. INACSL Standards Committee; McDermott, D.S.; Ludlow, J.; Horsley, E.; Meakim, C. *Virtual Simulation: An Educator's Toolkit*; Centre for Faculty Development: Los Angeles, CA, USA, 2021.
27. Hidayatulloh, S.; Rahman, A.B. Comparative analysis of cybersecurity frameworks in educational institutions: Towards a tailored security model. *Int. J. Adv. Comput. Sci. Appl.* **2025**, *16*, 789. [CrossRef]
28. Gauthier, L.; Waqar, Y. High impact learning for facilitator training and development. *Int. J. Scholarsh. Teach. Learn.* **2021**, *15*, 6. [CrossRef]
29. Barbhuiya, I.A.; Laroiya, S.; Singh, R. *Holistic Cybersecurity Risk Management Framework*; Elsevier: Amsterdam, The Netherlands, 2024. [CrossRef]
30. Lehane, L. Experiential learning: David A. Kolb. In *Science Education in Theory and Practice*; Akpan, B., Kennedy, T.J., Eds.; Springer: Cham, Switzerland, 2025; pp. 241–257.
31. Takkouch, M.; Zukowski, S.; Campbell, N. Students' perspectives and experiences with equity, diversity, inclusion, and accessibility in online and in-person undergraduate science laboratory courses. *J. Perspect. Appl. Acad. Pract.* **2023**, *11*. [CrossRef]
32. Rodriguez, M.; Dooley, K.E.; Roberts, T.G. A phenomenological study of intensive experiential learning for university faculty professional development. *J. Exp. Educ.* **2024**, *47*, 685–703. [CrossRef]
33. Burrell, D.N. Innovations from Academia around Cybersecurity Workforce and Faculty Development. In Proceedings of the MWAIS 2019 Proceedings, Oshkosh, WI, USA, 21–22 May 2019; p. 21.
34. Blyznyuk, T.; Kachak, T. Benefits of Interactive Learning for Students' Critical Thinking Skills Improvement. *J. Vasyl Stefanyk Precarpathian Natl. Univ.* **2024**, *11*, 94–102. [CrossRef]

35. Wurdinger, S.; Allison, P. Faculty perceptions and use of experiential learning in higher education. *J. E-Learn. Knowl. Soc.* **2017**, *13*, 15–26.
36. Straight, R. Beyond human-centric models in cybersecurity education: A pilot posthuman analysis of the nice workforce framework for cybersecurity. *J. Cybersecur. Educ. Res. Pract.* **2024**, *2024*, 30. [CrossRef]
37. Anti, E.; Vartiainen, T. *Cybersecurity Virtual Lab as a Service*; University of Vaasa: Vaasa, Finland, 2023.
38. McCance, K.R.; Blanchard, M. Measuring the Interdisciplinarity and Collaboration Perceptions of U.S. Scientists, Engineers, and Educators. *AERA Open* **2024**, *10*, 23328584231218952. [CrossRef]
39. Kaziukonis, V. *How to Build a Culture of Cyber Resilience in Your Organization*; Forbes Technology Council: Boston, MA, USA, 2024.
40. Jones, L.A. Unveiling human factors: Aligning facets of cybersecurity leadership, insider threats, and arsonist attributes to reduce cyber risk. *Socioecon. Chall.* **2024**, *8*, 44–63. [CrossRef]
41. Judd, T.; Bisgin, H.; Huseinovic, A.; Derani, M.; Uludag, S. Coalescing Research into Modular and Safe Educational Cybersecurity Labs with AI Solutions. In Proceedings of the 2024 IEEE Frontiers in Education Conference (FIE), Washington, DC, USA, 13–16 October 2024; pp. 1–9. [CrossRef]
42. Vykopal, J.; Seda, P.; Švábenský, V.; Čeleda, P. Smart environment for adaptive learning of cybersecurity skills. *IEEE Trans. Learn. Technol.* **2023**, *16*, 443–456. [CrossRef]
43. Kurtz, M.; Benabbou, A.; Pons, C.; Broisin, J. Collaboration in virtual and remote laboratories for education: A systematic literature review. *Int. J. Comput.-Support. Collab. Learn.* **2025**. [CrossRef]
44. Vaish, A.; Kumar, A.; Bobek, S.; Sternad, D. Development of Cyber Security Platform for Experiential Learning. *J. Cybersecur. Educ. Res. Pract.* **2024**, *2024*, 22. [CrossRef]
45. Ohio University. *New Partnership Brings Increased Experiential Learning Opportunities in Cybersecurity*; Ohio University News: Athens, OH, USA, 2025.
46. Commonwealth Cyber Initiative. *Cybersecurity Field Training Experience (C-FTE): Funded Experiential Learning Projects*; Commonwealth Cyber Initiative: Arlington, VA, USA, 2025.
47. Grimus, M. Emerging technologies: Impacting learning, pedagogy and curriculum development. In *Emerging Technologies and Pedagogies in the Curriculum. Bridging Human and Machine: Future Education with Intelligence*; Yu, S., Ally, M., Tsinakos, A., Eds.; Springer: Singapore, 2020; pp. 127–151.
48. Fukasaku, Y. Management of Technological Resources for Sustainable Development. In *Encyclopedia of Life Support Systems (EOLSS)*; UNESCO-EOLSS Joint Committee: Paris, France, 2020.
49. Evanick, J. Improving Instructional Design: Feedback and Iterative Refinement. eLearning Industry, 2023. Available online: https://elearningindustry.com/improving-instructional-design-feedback-and-iterative-refinement (accessed on 17 July 2025).

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.