ISSN: 2473-4901
v11 n6391

Bridging the Cybersecurity Skills Gap by Leveraging Cybersecurity Clinics: Developing the Arizona Cybersecurity Clinic

Dr. Paul Wagner
paulewagner@arizona.edu

Dr. Robert Honomichl
rjhonomichl@arizona.edu

Dr. Shengjie Xu
sjxu@arizona.edu

Dr. Eric Mapp
mapp@arizona.edu

College of Information Science
University of Arizona
Tucson, Arizona 85747, USA

Abstract

As cybersecurity threats increase in frequency and sophistication, a widening gap is emerging between the theoretical knowledge offered by academic programs and the practical skills demanded by industry. Experiential learning has emerged as a critical pedagogical approach to bridge this gap by enabling students to apply classroom knowledge to real-world challenges. This paper explores the development of the Arizona Cybersecurity Clinic at the University of Arizona; a program offers hands-on cybersecurity training to students while providing essential services to underserved and under-resourced organizations throughout the state. Drawing inspiration from existing clinic models and leveraging partnerships with secondary and postsecondary institutions, the clinic integrates capstone coursework, micro-credentials, and community engagement to enhance student readiness and regional cyber resilience. The paper details clinic design decisions, curriculum structure, legal and operational documentation, recruitment strategies, and initial implementation outcomes. Notably, the clinic's partnership with Chandler Unified School District marks the first high school-based cybersecurity clinic in the nation, expanding access and pathways into the cybersecurity workforce. Early results suggest that the clinic model effectively supports workforce development, strengthens local cybersecurity postures, and fosters inclusive education through interdisciplinary and intergenerational collaboration. The paper concludes by outlining future directions, including statewide clinic expansion, the development of AI-enhanced capabilities, and efforts to secure sustainable funding. The Arizona Cybersecurity Clinic offers a replicable model for institutions seeking to combine education, service, and innovation in response to the nation’s cybersecurity workforce and resilience challenges.

Keywords: Cybersecurity, Cybersecurity Education, Cybersecurity Clinics, Skills Gap, Experiential Learning

ISSN: 2473-4901
v11 n6391

Bridging the Cybersecurity Skills Gap by Leveraging Cybersecurity Clinics: Developing the Arizona Cybersecurity Clinic

Paul Wagner, Robert Honomichl, Shengjie Xu, and Eric Mapp

1. INTRODUCTION

Cybersecurity threats are evolving their capabilities at an exponential rate, with industry and educational institutions struggling to keep up. Traditional educational methods often leave a significant gap in practical experience among graduates. Cybersecurity education often emphasizes theory over practice. While theoretical knowledge forms the foundation of cybersecurity education, the lack of hands-on experience limits students' ability to address real-world challenges. Students frequently lack opportunities to apply concepts practically, resulting in a workforce underprepared to tackle dynamic cybersecurity threats and organizational needs. Additionally, employers are increasingly dissatisfied with the ability of recent graduates to perform the required tasks for their job roles.

Experiential learning is a pedagogical approach emphasizing learning through action and application. In cybersecurity, it allows students to engage in simulated environments, hands-on labs, and real-world projects. Experiential learning bridges the gap between theory and practice, developing critical thinking, problem solving, and technical proficiency. Traditional options for experiential learning include labs, simulations, Capture the Flag (CTF) events, bootcamps, workshops, internships, and case studies. This paper will review the literature to understand the current state of the cybersecurity workforce, define experiential learning, and provide an overview of the development and expansion of cybersecurity clinics in the U.S. This paper will then review the development of the Arizona Cybersecurity Clinic, challenges, and initial outcomes. Finally, future work will be discussed, outlining several key initiatives.

2. LITERATURE REVIEW

The rapid global digitization of society, coupled with the increasing sophistication of cybersecurity threats, requires a competent and qualified cybersecurity workforce. However, literature increasingly indicates a disconnect between the competencies of recent college graduates in cybersecurity and related fields and the expectations of employers.

Workforce Development

The demand for skilled cybersecurity professionals continues to outpace the supply. According to ISC2's Cybersecurity Workforce Study (International Information System Security Certification Consortium [ISC2], 2023), there are nearly four million unfilled positions globally, and Cyberseek (Cyberseek, 2025) reports over 450,000 unfilled positions in the United States (U.S.). Employers increasingly feel pressure to fill this gap to protect critical infrastructure, sensitive data, and organizational assets. Despite efforts by academic institutions to expand cybersecurity programs, like those designated under the National Security Agency's (NSA) National Centers of Academic Excellence in Cybersecurity (NCAE-C) program (National Security Agency [NSA], 2025), employers report dissatisfaction with the readiness of recent graduates to meet industry demands.

Employers seek candidates with technical, analytical, and problem-solving skills blended with critical written and verbal professional skills to address the evolving challenges of cybersecurity. Studies indicate that employers are dissatisfied with recent graduates' lack of the necessary skills and experience in key areas such as hands-on technical proficiency, incident response and threat mitigation, as well as soft skills and effective communication. ISACA (2023) identified that only 26 percent of those surveyed believe that at least half of the applicants are well qualified for positions. Additionally, soft skills were identified as the most significant skills gap among cybersecurity professionals. Furthermore, despite 52 percent of organizations requiring a degree to fill entry-level cybersecurity positions, 72% of survey respondents neither agree nor strongly agree that university graduates are well prepared to meet the cybersecurity challenges within their organization (ISACA, 2023).

Experiential Learning

ISACA (2023) identified that prior hands-on cybersecurity experience was very important (72%) or somewhat important (23%), and hands-on training was very important (25%) or somewhat important (55%). Individuals entering into the cybersecurity field and undergraduate students face challenges in acquiring the experience and hands-on training that are important to employers. Experiential learning

provides an opportunity to integrate experience and hands-on training into formal education programs.

Experiential learning has been defined in multiple ways; however, most emphasize direct engagement rather than passive study (Houle, 1980; Smith, 2010; Kolb, 2015). Learners can enter the learning cycle at any point; however, all stages in the cycle must be addressed for meaningful learning to occur (Brock University, 2025).

Cybersecurity Clinics

Cybersecurity clinics are modeled after the clinic models found in law and medical schools. Cybersecurity clinics are typically housed and operated out of colleges and universities under the direction of faculty. Students within these colleges and universities train to provide free cybersecurity assistance to underserved and under-resourced community organizations like small businesses, nonprofits, cities and towns, school districts, and utility companies. Clinics provide skills-based experiential learning opportunities to develop the necessary knowledge, skills, and abilities to become a more effective cybersecurity professionals.

Several universities established security clinics providing the basis for a clinic program. The University of California (UC), Berkeley established a clinic in 2018 focusing on defending nonprofits at risk of politically motivated cyber-attacks (Berkeley Center for Long-Term Cybersecurity, 2025). Berkeley's clinic trains the next generation of digital security leaders, defending the social sector and growing the public-interest technology community (Berkeley Center for Long-Term Cybersecurity, 2025). In 2019, Indiana University (IU) and Massachusetts Institute of Technology (MIT) launched their clinics (The Consortium of Cybersecurity Clinics, 2025). IU's clinic model focuses on improving local and state cyber hygiene. The clinic is "the first of its kind to strive to enhance the critical infrastructure sector of under-resourced stakeholders focusing on local municipalities, counties, school corporations and small businesses (Indiana University, 2025)." MIT's cybersecurity clinic is open to registered students from MIT, Harvard, or Wellesley (Massachusetts Institute of Technology [MIT], 2025). The MIT clinic works with public agencies and urban infrastructures utilizing an approach called Defensive Social Engineering (DSE) and technical tools to defend against cyber-attacks (MIT, 2025).

UC Berkeley, IU, and MIT partnered with the University of Alabama in 2021 to form the Consortium of Cybersecurity Clinics. As of 2025, the Consortium consists of 34 active clinics and five allies (The Consortium of Cybersecurity Clinics, 2025). The Consortium aims to serve as a platform for faculty, students, trainers, and advocates to network and share knowledge, expand the reach of cybersecurity clinics, and lower the barriers for other higher education institutions to establish their own clinics. The overarching vision is to launch a university, college, or community-college based clinic in all 50 U.S. states by 2030 (The Consortium of Cybersecurity Clinics, 2025).

3. CLINIC DEVELOPMENT

Background

The University of Arizona (U of A) was one of 15 institutions awarded a grant to establish the Arizona Cybersecurity Clinic in June 2024, with a period of performance through 2031. U of A clinic personnel envisioned the clinic as a model for the entire state, developing affiliate clinics in collaboration with community colleges, universities, and other partners throughout the state. The Clinic's mission is to create unique and impactful student experiential learning opportunities by providing vital cybersecurity services to underserved under-resourced, and underrepresented organizations throughout Arizona. Its vision is to secure and empower underserved, under-resourced, and underrepresented organizations throughout Arizona by providing cybersecurity awareness training, risk and vulnerability assessments, and other services as needed while cultivating the next generation of cybersecurity leaders.

Prior to developing the clinic, faculty members met with clinic personnel from the University of Nevada Las Vegas (UNLV) (University of Nevada, Las Vegas [UNLV], 2025), Metro State University (Metro State University, 2025), Massachusetts Institute of Technology (MIT) (MIT, 2025), and the Louisiana State University (LSU) (Louisiana State University [LSU], 2025) to learn more about various clinic models. These institutions were selected due to the maturity of their programs, engagement with clinic directors at the Consortium of Cybersecurity Clinics welcome event hosted in June 2024 at the NICE Conference, and their partnerships in the NSA Centers of Academic Excellence in Cybersecurity (NCAE-C) community. Additionally, faculty reviewed all documents and curriculum shared by existing clinics through the Consortium of Cybersecurity Clinics. Finally, faculty attended

monthly Consortium of Cybersecurity Clinics meetings to learn about best practices and initiatives. Based on this analysis, the faculty determined there were three options for operating a cybersecurity clinic: through coursework (capstone, internship, or independent study), through a campus club, or as a paid opportunity. Table 1 outlines the pros and cons of each approach.

It was determined that the capstone model would be the best option for the initial pilot based on this analysis. The course capstone is typically the last course in the student's undergraduate academic journey. Students would have taken most of their program requirements prior to participating in the clinic, providing a solid foundation in cybersecurity concepts. The clinic capstone course has a capacity of 30 students per semester.

Model	Pros	Cons
Coursework	• Students already required to take the course. • Leverages existing student support structures (Advising, Faculty, Staff). • Builds on previous courses and learning.	• Only offered twice per year (Spring / Fall Semester). • Increases student workload. • Student participation limited to junior or senior years.
Campus Club/Unpaid Opportunities	• Option for students to engage earlier in academic journey. • Long-term experiential learning potential. • Not constrained by academic semesters.	• Student led, extra-curricular activity. • May lack experience necessary to develop and maintain the clinic. • Clinic may not be priority for participants. • Limited resources.
Paid Opportunity	• Option for students to engage earlier in academic journey. • Long-term experiential learning potential. • Not constrained by academic semesters. • Prioritizes clinic work.	• High operational costs.

Table 1 – Clinic Model Analysis

Curriculum

The curriculum was developed based on a review of existing curriculum, identifying gaps in the cybersecurity program, the ability to provide clinic opportunities to students not in the cybersecurity program, and the needs of the clients. Clinic personnel evaluated the Cybersecurity Maturity Model Certification (CMMC), NIST Risk Management Framework and Cybersecurity Framework, and the Center for Internet Security (CIS) Critical Security Controls Version 8.1. Based on that evaluation and input from the Consortium of Cybersecurity Clinic members, the CIS controls were selected as the assessment framework. The CIS Controls provdie a broad based adaptable cybersecurity framework that can be applied to organizations of any size or sector. Additionally, CIS provides extensive materials and guides to support assessments. The Arizona Cybersecurity Clinic focused on Implementation Group (IG) 1 Essential Cyber Hygiene, which outlines 56 cyber defense safeguards (Stocchetti, 2024). Table 2 outlines the curriculum developed for the Spring 2025 pilot. It is important to note that the capstone course includes additional lectures and resources, covering topics such as conducting academic research and professional development.

Micro-Credential

Micro-credentials, sometimes referred to as digital badges, are specialized courses that teach specific knowledge, skills, and abilities to prepare students for entry-level jobs. Micro-credentials enable institutions the ability to offer modular learning opportunities, problem-oriented and activity-based teaching, and case studies from industry (Eibl, 2024). Additionally, micro-credentials can offer flexible education tailored to individual learners. The U of A defines a micro-credential as, "a small program in a focused area of study," and a digital badge as, "artifacts, much like a diploma awarded to learners upon completion of a micro-credential program" (University of Arizona, 2025).

Module	Topic	Lecture Length
Module 1.1	Risk Overview	47 minutes
Module 1.2	Risk Management	19 minutes
Module 1.3	Threat Modeling	24 minutes
Module 1.4	Controls and Contingency Planning	24 minutes
Module 1.5	Risk Management Framework	14 minutes
Module 1.6	CIS Controls	14 minutes
Module 1 Supplementary	CIS Controls Documentation Review	12 minutes
Module 1 Supplementary	Clinic Legal Documentation	12 minutes
Module 2.1	Risk Assessment Overview	24 minutes
Module 2.2	Risk Assessment Process	27 minutes
Module 2.3	Clinic Risk Assessment	49 minutes
Module 2 Supplementary	Client Intake Form	35 minutes
Module 2 Supplementary	Rules of Engagement and Scoping	10 minutes
Module 3.1	General Research and Analysis	23 minutes
Module 3.2	Industry Research	40 minutes
Module 3.3	Benchmarks	21 minutes
Module 3.4	Vulnerabilities	29 minutes
Module 3 Supplementary	CISA Critical Infrastructure Sectors	10 minutes
Module 3 Supplementary	Hierarchical Cybersecurity Governance Framework	8 minutes
Module 3 Supplementary	Industry Reports Overview	9 minutes
Module 3 Supplementary	CIS Workbench	9 minutes
Module 4.1	Technical Report	49 minutes
Module 4.2	Presentation	29 minutes
Module 4 Supplementary	Technical Report and Presentation	18 minutes
Module 5.1	Vulnerability Assessment Overview	7 minutes
Module 5.2	Information Gathering	16 minutes
Module 5.3	Information Gathering Demo	40 minutes
Module 5.4	Scanning	19 minutes
Module 5.5	Scanning Demo	18 minutes

Table 2 – Risk Assessment Curriculum Modules

The University developed its micro-credential to ensure learners internal to and external to the University could receive a credential. The University's micro-credential will be available to high school, undergraduate, graduate, and continuing and professional education students. The National Association of Colleges and Employers (NACE) identifies eight career readiness competencies: career & self-development, communication, critical thinking, equity & inclusion, leadership, professionalism, teamwork, and technology (National Association of Colleges and Employers [NACE], 2024). The University's badge credentials aligned with career & self-development, critical thinking, professionalism, technology, and leadership competencies.

The minimum amount of time commitment to receive the micro-credential is 40 hours, which is outlined as:

Risk Assessment Modules (5) – 12 hours

- Cyber Risk and Vulnerability Assessment and Document Review – 15 hours
- Research and Analysis – 10 hours
- Report and Presentation Preparation – 12 hours

The minimum amount of time commitment to receive the micro-credential is 40 hours, which is outlined as:

- Risk Assessment Modules (5) – 12 hours
- Cyber Risk and Vulnerability Assessment and Document Review – 15 hours
- Research and Analysis – 10 hours
- Report and Presentation Preparation – 12 hours
- Report and Presentation Delivery – 1 hour

ISSN: 2473-4901
v11 n6391

Figure 1 – University of Arizona Micro-Credential

Documentation
Documentation was divided into two primary categories of legal and assessment. Clinic personnel met with the university's Office of General Counsel (OGC) to identify the forms necessary to meet with and provide services to clients. Additionally, agreement documents were established to develop affiliate clinics to expand the clinic model including the Memorandum of Understanding (MOU) Cybersecurity Clinic (affiliate clinics) (Appendix A), Cybersecurity Clinic Client Memorandum of Understanding (MOU) (Appendix B), Student Non-Disclosure Agreement (NDA) (Appendix C), and Student Code of Conduct (Appendix D).

Services
Initially, the clinic would work with clients to provide cybersecurity awareness training, risk assessments, and vulnerability assessments as needed. A series of cybersecurity awareness training presentations were developed to support clients and community organizations. Risk assessments would consist of an initial intake form (Appendix E) and a risk assessment checklist. This process would provide an initial baseline of clients for "Essential Cyber Hygiene." Clients could also request vulnerability assessments consisting of network, web application, and system scans using open source tools like Nmap, Zed Attack Proxy (ZAP), and OpenVAS. Enterprise tools such as Nessus and Burp Suite were evaluated and initially determined to be cost prohibitive. It is important to note that vulnerability assessments introduce risk to the assessment process, as potential students may not be qualified or trained to properly conduct these tests. Additionally, clients may have concerns with students actively engaging with their environment. Further, penetration testing was considered but ultimately would not be implemented until after the initial pilot due to increased risk.

Clinic personnel took several steps to minimize client risk and maximize quality. Data collection, specifically, sensitive data collection was minimized. All data, records, and documentation was hosted on the university's secure cloud platform. Students were provided read only access to any sensitive information to minimize risk of downloading or propagating information. Clinic personnel ran all vulnerability scans and provided the results to students. Additionally, clinic personnel established mock interviews to prepare for presentations and conducted multiple rounds of revisions for the technical report. Further, clinic personnel set up weekly office hours and set up group meetings to answer questions and keep assessments on track to meet deliverable timelines.

Client Recruitment
Initial client recruitment occurred in several ways. Upon receipt of the grant, local outlets published a story about the Arizona Cybersecurity Clinic (Burtch-Buus, 2024; Blaser, 2024). This led to organizations and community groups reaching out to connect, provide presentations, and provide security awareness training. Clinic personnel presented at local, regional, and national events and conferences to discuss the clinic and its services. Finally, partners within Arizona's cybersecurity education ecosystem were asked to participate in the pilot. This resulted in identifying nine clients for the initial pilot. Currently the clinic has capacity to support a maximum of 15 clients per semester.

Student Recruitment
Like client recruitment, clinic personnel recruited students in several ways. A presentation was provided to U of A's cybersecurity club. Although this was intended to recruit students for the Spring 2025 pilot, the perpetual club model was described to determine interest in establishing that model within the club. Additionally, the cybersecurity program manager, advisors, and career and engagement coordinator set up information sessions for students. Thirty slots were allocated in the senior capstone course for the pilot.

Upon completion of this initial outreach, students taking their senior capstone in Spring 2025 were notified of the opportunity to participate in the clinic. Students within the Cyber Operations, Applied Computing, and Intelligence and Information Operations (IIO) programs were included, providing an interdisciplinary approach to the clinic. It is important to note that students are predominantly online, adult learners. Interested students were required to complete an application expressing their interest, describe their motivation for participating, and complete an agreement form stating they would need to be available to meet with clients during Arizona business hours or as required. This was an

important distinction due to the typical asynchronous availability of online students and competing priorities of adult learners. Thirty-three students began the application process, with 31 students completing the application. Of those, 26 students were selected to participate in the Spring 2025 pilot.

Chandler Unified School District (CUSD)
U of A's cybersecurity program has worked closely with Chandler Unified School District's (CUSD) cybersecurity program. CUSD's program is offered through Basha High School's Institute of Cyber Operations and Networking (ICON). It is a Career Technical Education (CTE) program that provides students with up to four years of high school cybersecurity education, up to 30 college credits through their dual enrollment program, and articulated pathways with Chandler Gilbert Community College (CGCC) and U of A. Clinic personnel met with CUSD's cybersecurity director to discuss the possibility of partnering to provide the clinic opportunity to high school students. Presentations were provided to students at three district high schools: Basha High School, Arizona College Preparatory (ACP) High School, and Chandler High School.

Ninety-six students from these high schools began the Google Cybersecurity Certificate course in Fall 2024 to prepare for participation in a pilot clinic in Spring 2025. An agreement between the U of A and CUSD was signed in November 2024, establishing the district as the first affiliate cybersecurity clinic in Arizona and the first high school cybersecurity clinic nationally (Dowd, 2024).

The CUSD Cybersecurity Clinic was initially planned as a two phase program. Students would be enrolled in the Google Cybersecurity Professional Certificate program during the fall term and complete modules and activities for the U of A's micro-credential during the spring term. Students must complete the certificate before continuing with the micro-credential. Participation in the clinic was voluntary, and students were required to complete training and modules after school.

4. INITIAL RESULTS

Initial results for the program were assessed based on student participation, feedback provided from students and clients during After Action Reviews (AAR), Student Course Surveys, and faculty and staff reflections. This section is broken down into the high school cybersecurity clinic and post-secondary cybersecurity clinic pilots which concluded in May 2025. Clinic operations will be evaluated and assessed after each semester to identify additional lessons learned, key performance indicators, and opportunities.

Post-Secondary Cybersecurity Clinic
The Arizona Cybersecurity Clinic concluded the initial pilot program in May 2025. This section outlines the initial results and lessons learned from the pilot. The 26 post-secondary capstone students were initially divided into groups of three to support eight clients. These clients represented municipal governments (2), non-profits (2), small businesses (3), critical infrastructure (1). Although all students completed the training and the capstone course, only seven of the eight groups were able to provide the detailed report and present their findings to the client. The group that didn't complete the report and present the findings was due to timelines, scheduling conflicts, and other issues that couldn't be overcome during the academic semester. Despite the level of work required in the course and the challenges of participating in a pilot course, all students stated that they were glad that they participated in the opportunity and would recommend it to other students. Specific comments from student course surveys include:

"First, the application of concepts learned in the classroom to a real-world experience. Second, it was also challenging on multiple levels such as working independently and as a group, putting together and finalizing a client presentation and technical report, etc. This format allowed for learning multiple new skills."

"I really appreciated that we were able to conduct a "real life" risk assessment for a local company and apply our knowledge in the best and most interactive way possible while in class. This felt like an internship within an academic setting."

"It was a full circle moment, everything I learned in the cyber operations side was brought together, and I got to reflect on my journey here."

Despite the positive feedback from students and clients, there were many lessons learned. All students participated in an After Action Review (AAR) to identify what went well, areas of improvement, key takeaways, and assess whether the opportunity was worthwhile. Additionally, clinic staff, faculty, and mentors participated in a separate AAR to review the course materials and identify lessons learned. The following are the three major changes that will be implemented for the Fall 2025 cohort:

- Client Contracts: Contract delays shifted the timeline three to four weeks, reducing student-client engagement. Future

contracts will be finalized as soon as clients are identified to avoid disruptions.
- Group Assignment: Delays also postponed group formation and team norming. Going forward, groups will be assigned before the semester begins, with required early sessions to establish expectations and communication practices.
- Streamlining Requirements: Students previously completed multiple individual research deliverables that were later synthesized into the client report. In the future, groups will collaborate on these elements from the start, with faculty assessing the effectiveness of this approach.

High School Cybersecurity Clinic (CUSD)
CUSD held the ribbon cutting for their cybersecurity clinic on March 25, 2025. Government representatives; Department of Homeland Security (DHS); administrators, faculty and staff from secondary and post-secondary institutions, and industry and community partners attended the ribbon cutting. The event recognized the 59 students that completed the Google Cybersecurity Professional Certificate. Of the 59 students, 30 students opted to continue with the second phase of the program completing the Cybersecurity Risk and Vulnerability Assessment micro-credential. The primary reason cited by students for not continuing with phase two was the time commitment to meet after school.

Additionally, the district established an internship program for clinic students. Interns will lead study sessions for the Google Cybersecurity Professional Certificate with new clinic participants, develop and present cybersecurity awareness training to community organizations and businesses, attend small business meetings, and maintain a professional journal of outreach activities and reflections. This will further expand these students' professional and technical skills and build their professional network.

5. FUTURE WORK

The development and expansion of the cybersecurity clinics provide several opportunities to support student experiential learning and enhance the cybersecurity of citizens and communities. This section outlines several key initiatives to refine and expand clinic operations.

Clinic Refinement
Lessons learned from the CUSD, and U of A pilots will provide valuable insight into the curriculum, assessment tools, methodologies, and operations. Faculty, staff, students, and clients will be involved in analyzing the clinic model to enhance training while streamlining operations. The deliverable from this assessment is a comprehensive Standard Operating Procedure (SOP) that can be shared with other organizations to establish affiliate clinics in Arizona and support the broader Consortium of Cybersecurity Clinics.

Clinic Expansion
The Arizona Cybersecurity Clinic is partnering with Pima Community College (Tucson, Arizona), Estrella Mountain Community College (Avondale, Arizona), and Grand Canyon University (Phoenix, Arizona) to develop affiliate clinics to support Pima and Maricopa Counties. Faculty at the four institutions are going through professional development training and reviewing curriculum materials in Summer 2025 and a student pilot will begin in Fall 2025.

The U of A will explore a perpetual model like UNLV. The clinic is working with students to develop a plan to promote and support this initiative. Clinic expansion requires considerable resources to operate, both in terms of time and funding. These constraints may be a limiting factor. Additionally, most undergraduate cybersecurity students at U of A are remote, online, adult learners creating opportunities and challenges for developing this model.

Further, clinic operations will be evaluated to determine capacity and expansion within U of A's capstone course. Currently one section of the capstone course is offered each semester with a capacity of 30 students. This can support up to 15 clients with students working in groups of two. Clinic personnel will track the time required to support student groups and client engagement to determine the approximate time per client needed. Although client capacity has not been reached, clinic personnel will develop selection criteria for clients.

Finally, the CUSD model will expand due to interest and demand. The program will be expanded to a two year program. Year 1 will consist of the Google Cybersecurity Professional Certificate (Fall) and the Cybersecurity Risk and Vulnerability Assessment micro-credential (Spring). Students that completed these requirements during Academic Year 2024-2025 will be eligible to participate in the pilot of Year 2. Year 2 will have students apply what they learned and develop professional skills. Students will provide peer mentorship to Year 1 students, develop cybersecurity awareness training modules to support the school district and community

organizations, conduct cyber hygiene outreach to the community.

Community Engagement

Community engagement will expand in 2025. This will be achieved directly through client engagement during the pilot and through local, state, and national outreach efforts. Partnerships are critical to meet the goals and of the clinic. The Arizona Cybersecurity Clinic is working with government, non-profit, and industry organizations throughout Arizona to expand opportunities. Faculty and students will attend meetings, events, and conferences to share their experiences and findings. Additionally, the clinic will provide security awareness training to citizens and community organizations. This meets one of the clinic's core missions while generating leads for potential clients and expanding the clinic's footprint. Furthermore, the Clinic is collaborating with universities to develop and host statewide Capture the Flag events, run summer camps, and offer professional development for middle and high school students and teachers to promote cybersecurity awareness and competencies.

Funding

Initial funding supports foundational operations for the Arizona Cybersecurity Clinic. Additional funding is necessary to support student development and expansion of the clinic model throughout Arizona. Students, especially first-generation and minority students, often face the decision between seeking paid employment in unrelated fields or gaining cybersecurity experience through volunteer opportunities. Funding would provide students with the opportunity to obtain paid student worker positions within the clinic, thereby offsetting the need for an "either or" decision. Additionally, certifications are important for gaining employment in the cybersecurity field. The ability to provide students with certification vouchers removes barriers to obtaining these certifications. The clinic is well-positioned to provide training for students across a variety of certifications to support employment in the field. Further, certified students are better equipped to provide clinic services to clients. Finally, the ability for organizations and secondary and postsecondary schools to develop and sustain a clinic requires additional resources. These and other considerations will drive the identification of partnerships, grants, and donations to support the growth and expansion of opportunities for students.

AI-Driven Tasks

As technology evolves, artificial intelligence (AI) presents a significant opportunity to strengthen the clinic's impact by improving efficiency, scalability, and effectiveness in cybersecurity operations. AI can enhance vulnerability assessments by automating security assessments, analyzing threat intelligence, detecting anomalies, and generating reports. These tools enable continuous monitoring enabling real-time identification of weaknesses in networks, applications, and endpoints, reducing manual effort for students and faculty while improving quality.

AI can also improve cybersecurity awareness training. Adaptive learning platforms can tailor modules to individual knowledge gaps, while simulated phishing attacks identify employees susceptible to social engineering and guide targeted education. AI-powered chatbots can provide real-time guidance and reinforce best practices, while gamification and adaptive methods increase engagement and retention.

The clinic will further pursue research at the intersection of AI and cybersecurity. Priorities include ethical AI, bias mitigation, and explainable AI to ensure transparency and trust in automated decisions. Collaborations with industry and academia will also explore AI-powered threat intelligence sharing to advance real-time information exchange and collective defense.

6. CONCLUSIONS

The development of the Arizona Cybersecurity Clinic represents a strategic and timely response to the growing demand for experiential learning in cybersecurity education. By bridging the gap between academic theory and real-world practice, the clinic offers a model that not only enhances student readiness for the workforce but also provides vital cybersecurity support to underserved and under-resourced organizations. This case study demonstrates the potential of cybersecurity clinics to address workforce shortages, elevate community cyber hygiene, and promote interdisciplinary collaboration across educational levels.

The initial pilot at the University of Arizona, along with its partnership with Chandler Unified School District, illustrates the feasibility and scalability of a clinic-based experiential learning model. Key achievements include a well-structured curriculum, effective student and client recruitment strategies, and the development of supporting legal and educational documentation. Importantly, the implementation of micro-

credentials further supports flexible and inclusive access to cybersecurity education for learners across a broad spectrum.

The clinic's expansion through affiliate partnerships, AI-enhanced capabilities, and increased community engagement promises to deepen its impact. Sustained funding and strategic collaborations will be essential to ensure the model's long-term success and replicability. As cybersecurity threats continue to evolve, so too must our educational models. The Arizona Cybersecurity Clinic offers a compelling blueprint for how institutions can lead in this critical domain by combining pedagogy, public service, and innovation.

7. REFERENCES

About the Consortium. (2025). *About the consortium: History of the consortium*. The Consortium of Cybersecurity Clinics. https://cybersecurityclinics.org/about/

Berkeley. (2025). *UC Berkeley cybersecurity clinic*. Berkeley Center for Long-Term Cybersecurity. https://cltc.berkeley.edu/program/cybersecurity-clinic/

Blaser, S. (2024, June 13). *University of Arizona gets $1M from Google for new cybersecurity clinic*. *Arizona Daily Star.* https://tucson.com/news/local/business/university-of-arizona-cybersecurity-google-business/article_38751718-2909-11ef-aa25-bb580e88046d.html

Burtch-Buus, L. (2024, June 12). *Cybersecurity clinic will protect businesses from online threats, develop students' career skills*. *University of Arizona News.* https://news.arizona.edu/news/cybersecurity-clinic-will-protect-businesses-online-threats-develop-students-career-skills

Brock University. (2025). *Pedagogy of experiential education*. Centre for Pedagogical Innovation, Brock University. https://brocku.ca/pedagogical-innovation/resources/experiential-education/pedagogy-of-experiential-education/

Cyber Clinic. (2025). *UNLV Cyber Clinic*. Office of Economic Development, University of Nevada, Las Vegas. https://www.unlv.edu/econdev/cyber-clinic

Cybersecurity for the public good. (2025). *Welcome to the consortium: Cybersecurity for the public good*. The Consortium of Cybersecurity Clinics. https://cybersecurityclinics.org/

Cyberseek. (2025). *Cyberseek supply and demand heat map*. https://www.cyberseek.org/heatmap.html

Dowd, B. (2024, November 1). *Chandler district partners with UA to expand high school cybersecurity program*. *KJZZ Phoenix.* https://www.kjzz.org/education/2024-11-01/chandler-district-partners-with-ua-to-expand-high-school-cybersecurity-program

Eibl, G., Jungbauer, D., Litvyak, O., Luidold, C., & Völkl, P. (2024, September 13). *Proactive curriculum development for cybersecurity education: A model of micro-credentials and active blended learning*. *ACM.* https://doi.org/10.1145/3670243.3673882

Houle, C. (1980). *Continuing learning in the professions*. Jossey-Bass.

Indiana University. (2025). *A global challenge, a local priority: Indiana University cybersecurity clinic*. IU Cybersecurity Clinic. https://cyberrisk.iu.edu/career-prep/cyberclinic.html

International Information System Security Certification Consortium (ISC2). (2023). *How the economy, skills gap, and artificial intelligence are challenging the global cybersecurity workforce*. https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e

ISACA. (2023). *State of cybersecurity 2023: Global update on workforce efforts, resources, and cyberoperations*. https://www.isaca.org/state-of-cybersecurity-2023?utm_source=other&utm_medium=other&utm_campaign=pr_both_content_survey-report_state-of-cybersecurity-survey-2023_quarter-3-2023_state-of-cybersecurity-2023-press-release&utm_content=state-of-cybersecurity-survey-2023_state-of-cybersecurity-2023-press-release&cid=pr_3000043&Appeal=pr

Kolb, D. A. (2015). *Experiential learning: Experience as the source of learning and development*. Pearson Education. https://www.cisecurity.org/insights/white-papers/guide-implementation-groups-ig-cis-critical-security-controls-v8-1

Kolb, D. A. (2025). *What is experiential learning*. Institute for Experiential Learning. https://experientiallearninginstitute.org/what-is-experiential-learning/

Louisiana State University. (2025). *LSU cybersecurity clinic*. https://www.lsu.edu/cyberclinic/index.php

Massachusetts Institute of Technology. (2025). *Cybersecurity: A social engineering approach at MIT*. https://urbancyberdefense.mit.edu/cybersecurityclinic/

Metro State University. (2025). *MN Cyber Clinic*. https://www.metrostate.edu/mncyber/clinic

ISSN: 2473-4901
v11 n6391

National Association of Colleges and Employers. (2024). *Competencies for a career-ready workforce*. https://www.naceweb.org/docs/default-source/default-document-library/2024/resources/nace-career-readiness-competencies-revised-apr-2024.pdf?sfvrsn=1e695024_6

National Security Agency. (2025). *National Centers of Academic Excellence in Cybersecurity (NCAE-C).* https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/

Smith, M. (2010). *David A. Kolb on experiential learning*. The encyclopedia of pedagogy and informal education. https://infed.org/mobi/david-a-kolb-on-experiential-learning/

Stocchetti, V., Franklin, J., & Regnier, R. (2024, November). *Guide to implementation groups (IG) CIS critical security controls v8.1*. Center for Internet Security. https://www.cisecurity.org/insights/white-papers/guide-implementation-groups-ig-cis-critical-security-controls-v8-1

The Consortium of Cybersecurity Clinics. (2025). *Our member organizations*. https://cybersecurityclinics.org/about/our-members/

University of Arizona. (2025). *Micro-credentials and digital badges*. Office of the Registrar. https://registrar.arizona.edu/badge

APPENDIX A
Memorandum of Understanding Cybersecurity Clinic

MEMORANDUM OF UNDERSTANDING
Cybersecurity Clinic

This Cybersecurity Clinic Memorandum of Understanding (this "Agreement") is effective as of the latest date of signature below (the "Effective Date") between the Arizona Board of Regents, acting for and on behalf of the University of Arizona (the "University") and XXX (the "District").

RECITALS

A. The District is implementing a Cyber Security Academy program (the "Program"), wherein high school students enrolled in schools within the District will have the opportunity to study cybersecurity and to obtain real world experience in the field, such as assessing cybersecurity risks and working collaboratively under instructor supervision to implement cybersecurity policies and technical controls.

B. The University's College of Applied Science and Technology has developed a Cybersecurity Clinic (the "Clinic"), a program similar to the Program for University students.

C. As part of the Clinic, the University has developed and obtained resources and materials that could benefit the Program and enhance the education the District's students receive within the Program.

D. The parties desire to collaborate in order to strengthen both the Program and the Clinic, both in terms of educational benefits for students and for the Arizona community at large, as described in this Agreement.

AGREEMENT

A. **Scope of Collaboration.**

   a. Google Cybersecurity Professional Certificate training ("Google Training")
      i. University will provide the District with training seats for the online Google Training. The number of training seats provided to the District at any given time will depend on both training seat availability and District need.
      ii. District agrees that any training seats provided by the University will be used solely by students enrolled in the Program.

   b. Training and Mentorship
      i. The University will provide training and mentorship to the Program instructors and administrators as reasonably requested.
      ii. The University will also provide Google mentors to the District upon request for the purpose of presenting to Program students.
      iii. The University's ability to provide such Google mentors will depend upon receiving sufficient advanced notice from the District as well as the availability of the Google Mentors.

   c. Materials
      i. The University will provide Clinic materials to the District as reasonably requested for use in the Program. Such materials may include, but are not limited to, risk assessment questionnaires, study materials, and instruction materials.

B. **Compensation.** There will be no compensation provided to or by either party in connection with this Agreement.

C. **No Joint Venture.** It is expressly understood and acknowledged that the parties are entering into this Agreement as independent contractors and that this Agreement is not intended to create,

nor shall it be construed as creating, any type of partnership, joint venture, or franchise relationship between the parties. Each of the parties will direct its own activities pursuant to this Agreement. No party shall have authority to direct the other's activities.

D. **Intellectual Property.**

a. **Ownership.** The parties acknowledge that inventions, discoveries, and other technology that is patentable, or that is copyrightable software ("Intellectual Property") may also arise from the Research Project. University owns all Intellectual Property invented or authored by University personnel under the Research Project ("University Intellectual Property"). The parties will jointly own all Intellectual Property invented or authored jointly by University personnel and Sponsor personnel under the Research Project ("Joint Intellectual Property"). Inventorship and authorship will be determined in accordance with United States intellectual property laws. This Agreement does not grant either party any rights to any Intellectual Property developed outside the scope of the Research Project.

b. **Retained Rights.** Without limiting any other rights it may have, the University specifically reserves the right in and to the University Intellectual Property and Joint Intellectual Property for any research, public service, and/or educational purposes, and to grant licenses to other academic institutions for these same reserved rights.

E. **Arbitration.** The parties agree to arbitrate disputes filed in Arizona Superior Court that are subject to mandatory arbitration pursuant to A.R.S. § 12-133.

F. **Conflict of Interest.** This Agreement is subject to cancellation pursuant to the provisions of A.R.S. § 38-511 regarding Conflict of Interest.

G. **Indemnification.** Neither party to this Agreement agrees to indemnify the other party or hold harmless the other party from liability hereunder. However, each party will be responsible for any and all liability caused by the act, omission, negligence, misconduct, or other fault of their employees, agents, and officers arising from this Agreement.

H. **Insurance.** The parties recognize that the Arizona Board of Regents participates in the Arizona State Risk Management Program. Any liability of the State of Arizona resulting from any negligence of its employees shall be governed by Arizona's self-insurance statute A.R.S. § 41-621. The University of Arizona, as an agency of the State of Arizona, has no authority to use State funds to purchase insurance and any charges for insurance cannot be accepted.

I. **Governing Law.** This Agreement is made under and will be interpreted according to Arizona law.

Arizona Board of Regents	**XXX School District**
_____ Name	_____ Name
_____ Title	_____ Title
_____ Date	_____ Date

ISSN: 2473-4901
v11 n6391

APPENDIX B
Cybersecurity Clinic Client Memorandum of Understanding

CYBERSECURITY CLINIC CLIENT
MEMORANDUM OF UNDERSTANDING

This Cybersecurity Clinic Client Memorandum of Understanding (this "Agreement") is effective as of the latest date of signature below (the "Effective Date") between the Arizona Board of Regents, acting for and on behalf of the University of Arizona (the "University") and XXX ("Client").

RECITALS

E. The University's College of Applied Science and Technology sponsors the Cybersecurity Clinic (the "Clinic"), wherein enrolled students obtain real world experience in the field under instructor supervision by providing local businesses with cybersecurity services.

F. Client would like to engage students in the Clinic to provide such cybersecurity services.

AGREEMENT

J. **Scope of Services**. The Clinic will assign a student team to assess Client cybersecurity risk and work collaboratively under instructor supervision to implement cybersecurity policies and technical controls to enhance Client's cybersecurity defenses (the "Services"). The Services will begin on [Date] and will continue for a period of [time] (the "Service Period").

K. **Payment**. There will be no payment required for the Services.

L. **Client Cooperation**.
   a. Client is expected to provide access to knowledgeable personnel for interviews, meetings, and work product reviews in a timely manner throughout the Service Period.
   b. Client agrees to share relevant requested information about organizational data, technology, activities, practices, processes, context, environment, etc., unless restricted by law. Client understands that pertinent information and data related to cybersecurity systems, protocols, personnel, past experiences, etc. are critical to the Clinic delivering an accurate and meaningful cybersecurity enhancement.

M. **Confidentiality**.
   a. Clinic staff and students will adhere to industry-standard cybersecurity protocols to keep Client data and communication secure.
   b. The Clinic will restrict Client information access to only current students on the Client's assigned team and the Clinic instructor.

N. **No Warranty; Disclaimer.**
   a. The Clinic will make reasonable efforts but cannot guarantee protection against security incidents such as unauthorized access to Client systems, disclosure of Client data, etc.
   b. The Clinic provides its services to Client on an "as is" and "as available" basis, with the express understanding that Clinic has no obligation to monitor or control Client's computing infrastructure, devices, practices, or data following the conclusion of the Service Period. As such, Client's use of Services is at its own discretion and risk.
   c. The Clinic makes no claims or promises about the quality, accuracy, or reliability of the Services, their safety or security, nor the program's content. Accordingly, the Clinic is not liable to Client for any loss or damage that might arise, for example, from the service or from any future security vulnerabilities. The Clinic expressly disclaims all warranties, whether express or implied, including implied warranties of merchantability, fitness for a particular purpose, and noninfringement.

O. **Limitation of Liability**

a. In no event will the Clinic be liable to Client or any third party for any indirect, incidental, special, consequential, or punitive damages arising out of or relating to the services or any materials or information that the Clinic provides, whether based on warranty, contract, tort (including negligence), statute, or any other legal theory, whether or not the Clinic has been informed of the possibility of such damages, except in proportion to and to the extent such liability, loss, expense, attorneys' fees, or claims for injury or damages are caused by or result from the negligent or intentional acts or omissions of the University, its officers, agents, or employees.
b. Client will not be liable to the Clinic for any indirect, incidental, special, consequential, or punitive damages arising out of or relating to the Client's engagement with the Clinic, except in proportion to and to the extent such liability, loss, expense, attorneys' fees, or claims for injury or damages are caused by or result from the negligent or intentional acts or omissions of the Client.

P. **Governing Law.** This Agreement is made under and will be interpreted according to Arizona law.

APPENDIX C
Student Non-Disclosure Agreement

University of Arizona Cybersecurity Clinic
Participant Non-Disclosure Agreement

By signing below, I, _____ agree to abide by the following during my participation in the Cybersecurity Clinic (the "Clinic").

Proprietary Information
I understand that by participating in the Clinic, I will have access to Proprietary Information (as defined below) belonging to local entities that engage the Clinic to provide cybersecurity assessments (each, a "Client" and collectively, the "Clients").

I agree to protect the confidentiality of all Proprietary Information disclosed to, shared with, or accessed by me during my work in the Clinic. Proprietary Information includes all data, materials, products, technology, computer programs, specifications, manuals, business plans, software, marketing plans, financial information, and other information disclosed or submitted, orally, in writing, or by any other media, to me by the Clinic or a Client.

I further agree to:

- Hold and maintain the Proprietary Information in the strictest confidence for the sole and exclusive benefit of the Clinic and the Clients.
- Not disclose, permit access to, or reveal the Proprietary Information to any third party without the prior written consent of the Clinic or the Client.
- Use the Proprietary Information only for the purpose of my work in the Clinic and not for any personal gain or detrimental purpose.
- Notify the Clinic immediately upon discovery of any unauthorized use or disclosure of Proprietary Information, whether by me or another Clinic participant.

Return of Proprietary Information
Upon the conclusion of my work with each particular Client, or upon request by the Clinic, I agree to return all copies of Client Proprietary Information to the Clinic or destroy such material, at the Clinic's discretion, and certify in writing that such return or destruction has been completed.

Remedies
I understand that any violation or threatened violation of this Agreement may cause irreparable injury to the Clinic and to the Client, and that they will be entitled to seek injunctive relief in addition to all legal remedies.

Participant Name _____

Signature _____

Date _____

ISSN: 2473-4901
v11 n6391

APPENDIX D
Student Code of Conduct

University of Arizona
Cybersecurity Clinic Participant Code of Conduct

This Code of Conduct governs participation in the University of Arizona Cybersecurity Clinic. Participants who violate this Code of Conduct may be excluded from some or all Cybersecurity Clinic opportunities and events.

Clinic participants are expected to comply with the policies that govern all activities and behavior at the University of Arizona, in particular the Nondiscrimination and Anti-Harassment Policy, the Student Conduct policy, and the Acceptable Use of Computers and Networks Policy.
In addition, we expect all Clinic participants to abide by the following parameters:

- Be respectful to others. Do not engage in homophobic/homomesic, racist, transphobic/transmisic, ageist, ableist, sexist, or otherwise exclusionary behavior. Honor individuals' preferences for how they prefer to be addressed.
- Use welcoming and inclusive language. Exclusionary comments or jokes, threats or violent language are not acceptable while working in the Clinic. Do not address others in an angry, intimidating, or demeaning manner. Be considerate of the ways the words you choose may impact others. Be patient and respectful of the fact that English may be a second (or third or fourth!) language for Clinic participants.
- Do not harass people. Harassment includes unwanted physical contact, sexual attention, or repeated social contact. Know that consent is explicit, conscious and continuous—not implied. If you are unsure whether your behavior towards another person is welcome, ask them. If someone tells you to stop, do so.
- Respect the privacy and safety of others. Do not take photographs of others without their permission. Note that posting (or threatening to post) personally identifying information of others without their consent ("doxing") is a form of harassment.
- Be considerate of others' participation. Everyone should have an opportunity to be heard. While working in teams, please keep comments succinct so as to allow maximum engagement by all members. Be conscious and respectful of the fact that your team members may have different methods of communicating, and work to enable the most collaborative environment among your team.
- Don't be a bystander. If you see something inappropriate happening, speak up. If you don't feel comfortable intervening but feel someone should, please feel free to ask a member of the Clinic staff to intervene.
- As an overriding general rule, please be intentional in your actions and humble in your mistakes.

Operational Security
Working with the Cybersecurity Clinic will require engagement with its client organizations. These organizations and their staff, partners, and the communities they serve are often at risk of online or physical attacks. Therefore, adherence to Clinic operational security procedures is not just a requirement for academic success, but for safeguarding the lives and livelihoods of Clinic partners, students, staff, and their friends and families.
In order to facilitate a secure, safe working environment, all Clinic participants are expected to:

- Adhere strictly to any operational security requirements set for client communications by your team, by Clinic staff, or by the client.
- Do not seek to undermine existing security controls. Should you feel a security measure is ineffective, bring your concerns to Clinic staff before taking measures to alter any security systems or policies.
- Respect clients' perspectives. Even if we do not agree with a client's security concerns, we learn more about their security context by listening than telling. We do not know what we do not know.
- Keep track of any Clinic-owned devices assigned to you or your team. Ensure they are always under the control of you or your team, or are securely stored when not in use, and do not engage in any unlawful or unethical online or offline behavior with them. Do not change any

device settings in ways that would reduce device security. These devices are the gateway to our clients' and the Clinic's electronic infrastructure. You are the gatekeeper.
- Report any security incidents or concerns immediately to Clinic staff. This includes, but is not limited to, the loss, theft, or compromise of Clinic-owned devices or data stored on them.

Confidentiality
As a condition of allowing students to participate in the Clinic, including access to the Clinic's computers or other systems, all students agree to strictly protect any Confidential Information they receive as a result of their work with the Clinic. While the decision about whether information is "Confidential Information" depends on the specific information itself, some examples of Confidential Information include:
- The names of client organizations, their staff or clients, or other persons related to a Clinic project, or information likely to indicate identity.
- Any information related to organizational assessments or policy findings and recommendations.
- Any private communication or information regarding a specific client, a case, research data or analysis, including any underlying facts and circumstances not already revealed to the public.
- Any report or other written material, including that which the undersigned or their team has drafted, unless such document has been approved for release and properly redacted by a member of the Clinic supervising faculty or professional staff; and
- Identities or other personal information about clients required by applicable research protocols to remain confidential to minimize the risk to research subjects of participation in research.

The undersigned student agrees that they will not violate the confidentiality of the Clinic's interests or those of the Clinic's clients by revealing Confidential Information to those outside the Clinic. By signing this Agreement, the student agrees not to disclose Confidential Information orally or in writing, including through electronic media or any online forum, and not to write about any aspect of a Clinic case or project in any print or online publication without the express, prior permission of the Clinic's supervising faculty or professional staff. The obligation of each student to maintain the confidentiality of information is on-going and continues after the student's participation in the Clinic has ended. Clinic faculty and professional staff are available to answer any questions or concerns about this Agreement, or about disclosure of any specific information. Students who are uncertain about whether certain information is Confidential Information should ask mentors, Clinic faculty or professional staff before any disclosure.

Professionalism
Working with client organizations is a position of significant privilege and trust. Your work does not just represent you, but your team, the Cybersecurity Clinic, the College of Applied Science and Technology, and the University of Arizona at-large. Students are expected to be on time to all client meetings and to be attentive and respectful during all external-facing engagements.
Work product, communications, and other client-facing materials you may produce over your time with the Clinic must adhere to a very high standard of quality. The work that is done in this Clinic varies from team to team, but always keep in mind these three characteristics when preparing work for clients:
- **Rigor:** Be thorough in your research. Do not make recommendations for clients based on what you assume they need—all recommendations should have a rigorous explanation behind them.
- **Attention to Detail:** Spelling, grammar, design, organization—do not underestimate the importance of details. We want clients to rely on the materials we create when they are considering meaningful decisions about their security. Bad writing does not instill confidence.
- **Contextualize:** Think about who your audience is for any document or deliverable—whether it is an email, an organizational policy, or a report. Who is reading it? Who might read it? How technical are they? Do they read English? How well? Tailoring your work to your audience is critical to making the work meaningfully received and understood.

The undersigned agrees to abide by the terms of this Code of Conduct for the duration of their involvement with the Cybersecurity Clinic. Failure to do so may result in disciplinary action outlined within the code, or as required by University of Arizona policy.

Your Name (Printed): _____

Your Signature: _____

Date: _____

APPENDIX E
Client Intake Form

1. Company Information
Company Name:
Business Address:
Industry Sector:
Primary Contact:
Name:
Title:
Email:
Phone:
Secondary Contact (if applicable):
Name:
Title:
Email:
Phone:
Number of Employees:
Location(s) of Offices / Operations:
Website:
Social Media:
LinkedIn:
Instagram:
X:
Facebook:
TikTok:
Other:
Key Products or Services Offered by your organization:

1a. What services are you looking to obtain from the Arizona Cybersecurity Clinic?:
☐ Cybersecurity Awareness Training
☐ Cybersecurity Risk Assessment
☐ Organizational Research using Open Search Intelligence (OSINT)
☐ Website Vulnerability Assessment

1b. Have there been any recent security incidents or data breaches? If so, could you briefly describe them?

1c. What ongoing cybersecurity concerns or threats have been observed?

1d. What are the primary goals of the cybersecurity program (e.g., risk reduction, compliance, etc.)?

2. Security Policies and Procedures
2a. What are the current cybersecurity policies you have in place (if any)?

☐ Incident Response	☐ Acceptable Use
☐ Remote Access	☐ Network Security
☐ Data Management	☐ Disaster Recovery
☐ Employee Awareness	☐ Data Backup
☐ Vendor Management	☐ Data Retention
☐ Email	☐ Risk Management
☐ Change Management	☐ Access Control
☐ Password	☐ Vendor / Contractor
☐ BYOD	☐ Other

Please attach / provide your current policies and any specific procedures.

2b. Does your organization offer any employee training?
Annotate how often all employees are required to conduct training:
0 = No Current Requirement; 1 = Annually; 2 = Semi-annually; 4 Quarterly

Information Security	Mobile Security
Social Engineering	Phishing
Physical Security	Wireless
Security Awareness	Safe Internet
Email Security	Other

Please attach current links or documents on the required training.

3. Data and Information Management

3a. What types of data do you manage?

☐ Biometric	☐ Privacy
☐ Health	☐ Business
☐ Financial	☐ Intellectual Property
☐ Credit Card	☐ Classified / Sensitive
☐ Bank Account	☐ Trade Secrets
☐ Email Addresses	☐ Consumer (Name / Address / Phone, etc.)
☐ Membership	☐ Other

3b. Where is data stored?
☐ On-Premises (Physical)
☐ On-Premises (Digital)
☐ Cloud
☐ 3rd Party Data Center
☐ Other

3c. If your organization utilizes data backup solutions, where is the data stored?
☐ On-premises
☐ Cloud
☐ 3rd Party Data Center
☐ Other
☐ Unknown
☐ No data backup solution

3d. Are tests completed annually of data backup systems?
☐ Yes
☐ No
☐ Unknown

3e. If you have a data retention policy, is it being followed?
☐ Yes
☐ No
☐ Unknown

3f. Is your organization utilizing access control?
☐ Yes
☐ No
☐ Unknown

3g. If utilizing an access control, what type is it?

☐ Role Based	☐ Attribute-Based
☐ Mandatory	☐ Discretionary
☐ Rule Based	☐ Other

3h. Is access to sensitive information restricted based on a need-to-know basis?
☐ Yes
☐ No
☐ Unknown

3i. Are access controls reviewed and updated regularly?
☐ Yes
☐ No
☐ Unknown

3j. Do you maintain logs of access to sensitive information?
☐ Yes
☐ No
☐ Unknown

3k. Are user accounts regularly reviewed for necessary permissions?
☐ Yes
☐ No
☐ Unknown

3l. Are inactive accounts disabled promptly?
☐ Yes
☐ No
☐ Unknown

3m. Do you monitor and log account activity, especially for privileged accounts?
☐ Yes
☐ No
☐ Unknown

4. Network Security and Access Control
4a. Does your organization utilize any of the following network hardware? (Please denote type)
Network Equipment:

Load Balancer	NAC	UTM
IDS / IPS	VPN	SIEM
Web Filter	Switch	Router
Wi-Fi AP	Modem	Bridge
Repeater	Hub	Gateway
Other		

Server:

Mail	DHCP	Web
File	Database	Print
Application	Proxy	Reverse Proxy
FTP	DNS	Fax
Virtual	Cloud	Other

Firewall:

Stateful	Stateless	NGFW
WAF	Cloud	Packet Filtering

IPS:
☐ Network
☐ Host
☐ WIPS
☐ Other

IDS:
☐ Network
☐ Host
☐ WIDS
☐ Other

SIEM:
☐ Snort
☐ Splunk
☐ Qradar
☐ LogRhythm
☐ Other

EDR **XDR** **Email Security**

Please provide a detailed list of security assets, including make, model, version, and serial number.

4b. Do you use network segmentation (e.g., separate networks for different data types or roles)?
☐ Yes
☐ No
☐ Unknown

4c. Is Multi-Factor Authentication (MFA) utilized?
☐ Yes
☐ No
☐ Unknown

4d. How many clients (computers, tablets, cell phones) are currently being utilized in your organization?
☐ 1 – 20
☐ 21 – 50
☐ 51 – 100
☐ 101 – 250
☐ 251 - 500
☐ 501+

4e. Do employees use personally owned devices to conduct business functions?
☐ Yes
☐ No
☐ Unknown

4f. Does your organization use a password manager?
☐ Yes
☐ No
☐ Unknown

4fi. If so, which one is being used?

5. Wireless
5a. Does your organization utilize Wi-Fi?
☐ Yes
☐ No
☐ Unknown

5b. Are guests allowed to access your network?
☐ Yes
☐ No
☐ Unknown

5bi. If yes, do you have a separate network for them to connect to?
☐ Yes
☐ No
☐ Unknown

5c. If Wi-fi is being utilized what encryption is being used?
☐ WEP
☐ WPA Personal
☐ WPA2 Personal
☐ WPA3 Personal
☐ WPS
☐ WAP Enterprise
☐ WPA2 Enterprise
☐ WPA3 Enterprise
☐ Unknown

6. Endpoint and Application Security
6a. Is your organization utilizing a 3rd party Antivirus program? (Not Windows Defender)
☐ Yes
☐ No
☐ Unknown

ISSN: 2473-4901
v11 n6391

6b. If using a 3rd party AV, is it the free version?
☐ Yes
☐ No
☐ Unknown

6c. If using a 3rd party AV, please denote which one.
☐ Norton
☐ CrowdStrike
☐ Bitdefender
☐ Sophos
☐ McAfee
☐ AVAST
☐ Malware Bytes
☐ Other

6d. Does your organization utilize application listing?
☐ Yes
☐ No
☐ Unknown

6di. If yes, what type?
☐ Block / Blacklisting
☐ Allow / Whitelisting
☐ Unknown

6e. What is the frequency of your organization's patch management?
☐ Weekly
☐ Bi-Weekly
☐ Monthly
☐ Unknown
☐ Quarterly
☐ Annually
☐ Other

7. Compliance and Regulatory Requirements
7a. Are there any industry-specific compliance requirements?
☐ GDPR
☐ FERPA
☐ SOC 2
☐ FISMA
☐ CCPA
☐ Other
☐ SOX
☐ PCI-DSS
☐ GLBA
☐ HIPAA
☐ CMMC
☐ Unknown

7b. Does your organization perform annual security audits?
☐ Yes
☐ No
☐ Unknown

Please provide the compliance requirements for third-party vendors if applicable.

7c. Is sensitive data identified and classified?
☐ Yes
☐ No
☐ Unknown

7d. Are controls in place to prevent unauthorized access to sensitive data?
☐ Yes
☐ No
☐ Unknown

7e. Is data encrypted during transit and at rest?
☐ Yes
☐ No
☐ Unknown

8. Inventory and Control Software Assets
8a. Is there an up-to-date inventory of all installed software?
☐ Yes
☐ No
☐ Unknown

8b. Are unauthorized software installations detected and resolved promptly?
☐ Yes
☐ No
☐ Unknown

8c. Do you regularly review and validate the software inventory for compliance?
☐ Yes
☐ No
☐ Unknown

9. Continuous Vulnerability Management
9a. Do you conduct regular vulnerability scanning on all systems?
☐ Yes
☐ No
☐ Unknown

9b. Is there a process for timely remediation of identified vulnerabilities?
☐ Yes
☐ No
☐ Unknown

9c. Are vulnerability scan reports reviewed and acted upon regularly?
☐ Yes
☐ No
☐ Unknown

10. Controlled Use of Administrative Privileges
10a. Are administrative privileges granted only based on roles and responsibilities?
☐ Yes
☐ No
☐ Unknown

10b. Do you track and audit the use of administrative privileges?
☐ Yes
☐ No
☐ Unknown

10c. Is there a process to revoke administrative privileges when they are no longer required?
☐ Yes
☐ No
☐ Unknown

11. Secure Configuration for Hardware and Software
11a. Are secure configurations applied to all hardware and software upon installation?
☐ Yes
☐ No
☐ Unknown

11b. Do you regularly update and validate secure configurations?
☐ Yes
☐ No
☐ Unknown

11c. Are deviations from secure configurations detected and corrected promptly?
☐ Yes
☐ No
☐ Unknown

12. Email and Web Browser Protections

12a. Do you have mechanisms to filter out malicious email and web content?
☐ Yes
☐ No
☐ Unknown

12b. Are email and web browser security settings configured and regularly updated?
☐ Yes
☐ No
☐ Unknown

12c. Do you regularly train employees on email and web security best practices?
☐ Yes
☐ No
☐ Unknown

13. Limitation and Control of Network Ports, Protocols, and Services

13a. Are unnecessary network ports, protocols, and services disabled on all systems?
☐ Yes
☐ No
☐ Unknown

13b. Is there a process to regularly review and validate network port, protocol, and service configurations?
☐ Yes
☐ No
☐ Unknown

13c. Do you monitor and log network port, protocol, and service activities?
☐ Yes
☐ No
☐ Unknown

14. Secure Configuration for Network Devices

14a. Are secure configurations applied to network devices such as firewalls, routers, and switches?
☐ Yes
☐ No
☐ Unknown

14b. Do you regularly review and update network device configurations?
☐ Yes
☐ No
☐ Unknown

14c. Does your organization regularly utilize a vulnerability scanner to identify configuration faults?
☐ Yes
☐ No
☐ Unknown

14d. If so, what type? Please provide the latest report if available.
☐ Nessus
☐ OpenVas
☐ Other
☐ Unknown

14d. Are changes to network device configurations logged and audited?
☐ Yes
☐ No
☐ Unknown

15. Penetration Tests and Red Team Exercises
15a. Do you conduct regular penetration tests to evaluate security?
☐ Yes
☐ No
☐ Unknown

15b. Are results from penetration tests used to improve security measures?
☐ Yes
☐ No
☐ Unknown

15c. Do you employ red team exercises to simulate real-world attacks?
☐ Yes
☐ No
☐ Unknown

Acronyms and Glossary

AP – Access Point – A device that logically connects wireless client devices operating in infrastructure to one another and provides access to a distribution system, if connected, which is typically an organization's enterprise wired network.

Attribute-Based Access Control (ABAC) – An access control approach in which access is mediated based on attributes associated with subjects (requesters) and the objects to be accessed. Each object and subject have a set of associated attributes, such as location, time of creation, access rights, etc. Access to an object is authorized or denied depending upon whether the required (e.g., policy-defined) correlation can be made between the attributes of that object and of the requesting subject.

Blacklisting – The process used to identify: (i) software programs that are not authorized to execute on an information system; or (ii) prohibited universal resource locators (URL)/websites.

BYOD – Bring Your Own Device – A policy that allows employees to use their own devices for work. The devices can include smartphones, tablets, laptops, and USB drives

CCPA – California Consumer Privacy Act – Law that secures privacy rights for California consumers, including: the right to know about the personal information a business collects about them and how it is used and shared; the right to delete personal information collected from them (with some exceptions); the right to opt-out of the sale or sharing of their personal information; and the right to non-discrimination for exercising their CCPA rights.

CMMC – Cybersecurity Maturity Model Certification – An assessment framework developed by the U.S. Department of Defense (DoD) with the primary objective to enhance cybersecurity controls in place for organizations supplying the DoD, known as the Defense Industrial Base (DIB). The CMMC model aims to manage risk and verify that DoD contractors can safeguard information classed as Controlled Unclassified Information (CUI) and comply with NIST SP 800-171 DoD assessment requirements and other cybersecurity requirements.

Controlled Unclassified Information (CUI) – Information that the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency.

Defense Industrial Base (DIB) – The Defense Industrial Base Sector is the worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet U.S. military requirements.

DHCP – Dynamic Host Configuration Protocol – A network management protocol used on Internet Protocol (IP) networks for automatically assigning IP addresses and other communication parameters to devices connected to the network using a client–server architecture.

Discretionary Access Control (DAC) – An access control policy that is enforced over all subjects and objects in a system where the policy specifies that a subject that has been granted access to information can do one or more of the following: pass the information to other subjects or objects; grant its privileges to other subjects; change the security attributes of subjects, objects, systems, or system components; choose the security attributes to be associated with newly-created or revised objects; or change the rules governing access control. Mandatory access controls restrict this capability.

DNS – Domain Name System – A hierarchical and distributed name service that provides a naming system for computers, services, and other resources on the Internet or other Internet Protocol (IP) networks.

EDR – Endpoint Detection & Response – A cybersecurity technology that continually monitors an "endpoint" (e.g. a client device such as a mobile phone, laptop, Internet of things device) to mitigate malicious cyber threats.

Federal Educational Rights and Privacy Act – A United States federal law that governs the access to educational information and records by public entities such as potential employers, publicly funded educational institutions, and foreign governments.

FISMA – Federal Information Security Management Act – A law that protects the government's information, assets, and operations from threats. The law was originally passed in 2002 as the Federal Information Security Management Act but was updated in 2014 in response to a growing number of cyber-attacks on the federal government.

FTP – File Transfer Protocol – A standard for transferring files over the internet. FTP programs and utilities are used to upload and download web pages, graphics, and other files between local media and a remote server that allows FTP access.

GDPR – General Data Protection Regulation – A European Union law that protects the privacy and security of personal data. It applies to all EU member states and the European Economic Area (EEA).

GLBA – Gramm-Leach-Bliley Act – A law that requires financial institutions to protect consumer information. The law was enacted in 1999 and is also known as the Financial Services Modernization Act.

HIPAA – Health Insurance Portability & Accountability Act – Establishes federal standards protecting sensitive health information from disclosure without patient's consent.

IDS – Intrusion Detection System – A software application or device that monitors a network or system for malicious activity or policy violations. IDSs are a key component of network security defenses and can help identify security incidents, bugs, and device configuration issues.

IPS – Intrusion Prevention System – A network security tool that monitors network activity for malicious activity and takes action to prevent it

MFA – Multi-Factor Authentication – An authentication system that requires more than one distinct authentication factor for successful authentication. Multifactor authentication can be performed using a multifactor authenticator or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are.

NAC – Network Access Control – A computer security method that limits access to a network by unauthorized devices and users. NAC uses rules, protocols, and processes to control access to network resources, such as PCs, IoT devices, and network routers. It also applies to data and resources transmitted through the network, as well as virtual and software-defined resources.

NGFW – Next Generation FireWall – A cybersecurity tool that protects networks from cyber threats by combining traditional firewall technology with other network filtering functions. NGFWs can block modern threats like advanced malware and application-layer attacks, and they can also receive and act on threat intelligence feeds from external sources.

PCI-DSS – Payment Card Industry Data Security Standard – A set of guidelines that protect cardholder data and account information. The Payment Card Industry Security Standards Council (PCI SSC) creates and enforces the standard. PCI-DSS protects credit card information, prevents unauthorized access to account data, helps businesses detect and respond to security failures, helps businesses maintain security awareness, and helps businesses monitor and adapt to changes in cybersecurity threats.

Proxy – An application that "breaks" the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network and processes it and forwards it. Note: This effectively closes the straight path between the internal and external networks making it more difficult for an attacker to obtain internal addresses and other details of the organization's internal network. Proxy servers are available for common Internet services; for example, a hypertext transfer protocol (HTTP) proxy used for Web access, and a simple mail transfer protocol (SMTP) proxy used for e-mail.

Role Based Access Control (RBAC) – Access control based on user roles (i.e., a collection of access authorizations that a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.

Rule Based Access Control - Access control model that regulates user access to computer or network resources based on predefined rules aligned with the user's job functions and organizational structure. Instead of granting permissions directly to individual users, RBAC assigns user permissions based on their assigned roles. This streamlines access management and simplifies security policy enforcement.

SOC 2 – Service Organization Control – A report that can be provided to third parties to demonstrate a strong control environment; an audit performed by a third-party auditor (CPA) to provide said report; or the controls and "framework" of controls that allow an organization to attain a SOC 2 report. In other words, SOC 2 is a "report on controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy.

SOX – Sarbanes-OXley Act – A United States federal law designed to further protect shareholders and the public from general accounting fraud in public and private companies by improving the accuracy of corporate disclosures.

SIEM – Security Information and Event Management – Application that provides the ability to gather security data from information system components and present that data as actionable information via a single interface

Stateful Firewall – A firewall that keeps track and monitors the state of active network connections while analyzing incoming traffic and looking for potential traffic and data risks. This firewall is situated at Layers 3 and 4 of the Open Systems Interconnection (OSI) model.

Stateless Firewall – A type of firewall that filters network traffic based on individual packets without storing information about the state or context of connections. When comparing stateless vs. stateful firewalls, stateless firewalls make filtering decisions based only on the information present in each packet as opposed to stateful firewalls, which maintain a state table.

UTM – Unified Threat Management – Provides multiple security features and services in a single device or service on the network, protecting users from security threats in a simplified way. UTMs includes functions such as anti-virus, anti-spam, content filtering, and web filtering. Also known as a Next Generation Firewall (NGFW).

VPN – Virtual Private Network – A virtual network built on top of existing physical networks that can provide a secure communications mechanism for data and IP information transmitted between networks or between different nodes on the same network.

WAF – Web Application Firewall – A security tool for monitoring, filtering and blocking incoming and outgoing data packets from a web application or website. WAFs can be host-based, network-based or cloud-based and are typically deployed through reverse proxies and placed in front of an application or website (or multiple apps and sites).

WEP – Wired Equivalent Privacy – Security protocol specified in the IEEE Wireless Fidelity (Wi-Fi) standard 802.11b.

Whitelisting – An implementation of a default deny all or allow by exception policy across an enterprise environment, and a clear, concise, timely process for adding exceptions when required for mission accomplishments.

WIDS – Wireless Intrusion Detection System – a technology designed to protect wireless networks from unauthorized access. It does this by monitoring traffic on the network to identify any suspicious activity that may indicate a security breach.

WIPS – Wireless Intrusion Prevention System – A technology designed to protect wireless networks from unauthorized access using a combination of techniques to detect and prevent intrusions in real time. It not only monitors but also takes action to prevent rogue access points, man in the middle attacks, denial-of-service attacks, and other threats to the wireless network.

WPA – Wi-Fi Protected Access – A security protocol that protects wireless networks by using encryption and authentication to limit access to authorized users

WPS – Wi-Fi Protected Setup – A wireless security standard that allows users to connect devices to a network without entering a password. WPS is designed to simplify the process of setting up a secure wireless network, especially for users who are unfamiliar with wireless security.

XDR – eXtended Detection & Response – A cybersecurity solution that combines security tools into a single platform to detect and respond to threats. XDR can collect data from a variety of sources, including endpoints, networks, cloud workloads, and email, and use AI and automation to analyze it. This allows security teams to more quickly and accurately identify threats and respond to them.