CyberAlumni a Cybersecurity Collaboratory

Alejandro D. Ayala
University of Washington
Seattle, WA
aayala@uw.edu
0000-0001-8391-5131

Barbara Endicott-Popovsky
Portland State University
Portland, OR
endic@pdx.edu
0000-0002-8700-0358

Randy J. Hinrichs
University of Washington
Seattle, WA
avatar@uw.edu
0000-0002-8636-0319

***Abstract*—CyberAlumni is a case study of a new model for using peer to peer digital networks to make students breach ready. The CyberAlumni organization was founded in 2021 with the goals of pursuing continuing education and collaborations with academia, industry, and government to bridge the gap between curriculum and job placement. This model serves to accelerate the professional development and acquisition of top-level cybersecurity talent while recursively bolstering cybersecurity curriculum in the process. All goals were achieved within one year, leading to further investigation of applying this model at scale in conjunction with courses offered through NSA Centers of Academic Excellence.**

Keywords—Collaboratory, Scalability, Game-based Learning, NCAE-C, Non-traditional Students, Project-based Learning, Online and Remote Learning

I. INTRODUCTION

CyberAlumni is an exclusive social community that accelerates top level cybersecurity talent by offering opportunities to build digital communities, advance education, collaborate with cybersecurity experts, connect with mentors, and find jobs. Certified alumni of courses from the University of Washington's National Center of Academic Excellence in Cybersecurity (NCAE-C) founded this group in 2021 as a peer-to-peer digital network. This article will explore how this scalable model fits into cybersecurity education and career development.

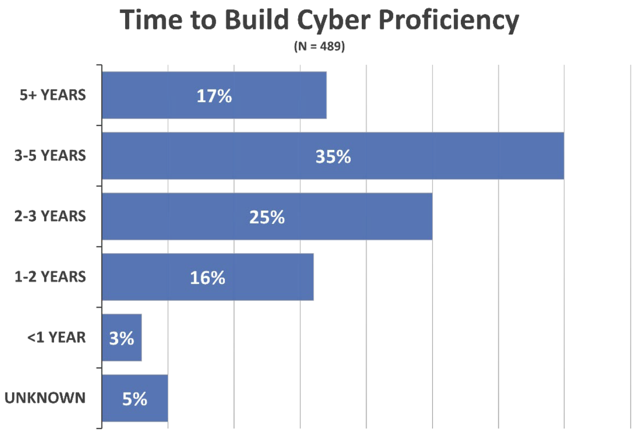

Fig. 1. Information Systems Security Association research result on industry polling [1].

II. PROBLEM STATEMENT

How do you advance competency after you graduate? Cybersecurity is rapidly evolving and severely understaffed [2], [3]. The current education models take years to train new cyber talent while the threat landscape changes in months (see Fig. 1). The field requires continuous professional education to fill the gap and maintain breach readiness [1]. Ralph Johnson, the third quarter faculty member and State Chief Information Officer, State of Washington, stated that "I need to stay current on the latest trends too. That is why I require the students to find a new article and submit it with critique every week" [4]. Academic institutions struggle to meet the demand for competent cybersecurity professionals that can continuously keep up with the changing threat landscape.

III. METHODOLOGY

This is a qualitative inquiry. Investigators evaluate a student-led program for nurturing cybersecurity talent. The collaborative nature and social networking tools of the cloud allow us to observe students and mentors working together to form ideas and critically think about solutions. Students work in close contact with each other over virtual environments. We examine our cybersecurity collaboratories as ethnographers to capture how students bend the technology to meet their communication needs and move from learning concepts to producing products. Students use Canvas, Office 365, and Google Suite. Students brainstorm in one set of tools, communicate in another, create learning assets in another. The process is seamless and economical with time and space reduced, allowing students to focus on content and increase experience in activities. They leverage mobile technology for quick response and pursue ideas by staying connected and productive. The anonymity of the individual can be explored off camera, so biases on gender, age, ethnicity, socio-economic aspects, and demographics are generally muted. The student focuses on content and delivery, rather than social interaction.

The method used here is to explore on-line collaboratories like the Avalumni [5], an avatar-based group organized in virtual worlds taught for ten years at the University of Washington's iSchool. Avalumni students come together in Second Life to advance development skills and engagement. They participate in shared academic writing and co-develop together. CyberAlumni repeats the same factors forming bonded, digital communities to advance continuing education, academic robustness, and career placement. Examined here are the individual elements that led to the success of the CyberAlumni in its first year of formation.

IV. APPROACH

A. *CyberAlumni Case Study*

CyberAlumni was formed in 2021 by graduates of the cybersecurity risk management certificate course at the University of Washington's NCAE-C. Professionals looking to accelerate their careers into management level positions brought decades of prior experience from various companies and government organizations. The rigorous nine-month course established a baseline competency aligned with Federal standards and formed a trusted, bonded community of peers. The Certificate program lacked a post completion pipeline to connect experience to career advancement.

Forming Cyber Alumni addressed that problem and connected the components using a systems approach to the design and implementation.

CyberAlumni started by working with EC-Council to review the technical training laboratories for the course and test their new tools. EC-Council received valuable feedback to improve their educational offerings, and the NCAE-C received new tools to scale their curriculum. The mutual benefit of involving industry and alumni in the review of curriculum establishes a feedback loop for PCE and for EC-Council.

UW and EC-Council agreed to connect their curricula. As a pilot, EC-Council provided scholarships for the students to pursue their three flagship industry certifications. These certificates provide students with access to industry-based content. Students have up to one year to complete the EC-Council certifications in Network Defense, Ethical Hacking and Digital Forensics. Cyber Alumni provides a collaboratory in which students study together to reach their goals.

This opened the opportunity to work with other certificate-based industry solution providers. The CyberAlumni were offered collaborative learning and peer testing as a group activity. Faculty negotiated volume price reductions if CyberAlumni could bring in ten participants. This became a valuable proposition for students to join.

The next collaboration involved an objective cybersecurity review of electronic ballot transfer technology that helped secure a $10 million congressional appropriation in research funding for the critical infrastructure of electronic voting.

Top level cybersecurity expert Mike Hamilton from Critical Insights engaged the newly formed CyberAlumni to work on this project for in-field experience. Mentors included the NCAE Executive Director and the Lead Instructor of the University of Washington's Certificate program as well as C-Suite industry executives.

The CyberAlumni conducted a thorough review of multiple available electronic ballot transfer technologies. Alumni delivered a technical review of security controls, threat matrix, risk assessment, and follow-on recommendation. The resultant unpublished white paper was released to state voting officials in response to skeptical reviews of the technology. Congress subsequently approved a large federal grant to research the efficacy of this type of technology, and twenty-six individual states have now approved its use.

In 2021, a Senior Officer from U.S. Cyber Command sought the collaboration of CyberAlumni and the University of Washington to explore new educational materials. The CyberAlumni were invited to test pilot new curriculum on cultural and linguistic blind spots in cybersecurity with a Russian focus offered through the NCAE-C. The students received certificates for participating in the pilot and learned a model for how to analyze Russian cybersecurity strategies and tactics.

CyberAlumni also partnered with the NROTC program at the University of Washington to explore development of curriculum for future cyberwarfare officers. Specifically, the Navy and Marine Corps had just begun to develop Military Occupational Specialties around cyberwarfare with no educational pipeline yet established at the university level. A student representative from the NROTC Program was awarded a scholarship to attend the NCAE-C courses and aid in the development of a new curriculum for future cyberwarfare officers as a member of the CyberAlumni.

For this small test pilot, the Cyber alumni sent three members and recruited an additional member post completion. While participating in the connection of educational standards across military and academia, the CyberAlumni gained a new certification, valuable social connections, and mentorship opportunities.

B. *The Anatomy of Cyber Alumni*

The make-up of the founding members is diverse. Students with over thirty years in IT seeking credentials in cybersecurity and provide in-field expertise. International students with backgrounds in computer science, business and marketing offer new perspectives. UW's NROTC students offer military robustness. A talented high school student who participated in the Russian Blind Spots certificate showed passion for thinking from a digital native perspective and challenged the group to think about gaming in cybersecurity. He joined our team to cover our own blind spots.

Fig. 2. CyberAlumni logo: Community, Collaboration, Continuous Learning

CyberAlumni established set roles and responsibilities, identity, and social outreach to begin connecting members to career opportunities (see Fig. 2). Through CyberAlumni's newly created network of peers, mentors, and collaborators, the first president of CyberAlumni was able to quickly accelerate her own career into a higher position at a new company. To make this success scalable, CyberAlumni is now working with industry partners to create direct pathways from CyberAlumni to employment opportunities.

The organization meets monthly. They elect their officers. They maintain shared assets in Microsoft One Note, use Zoom to meet frequently, use Office 365 to collaborate and deliver publishing quality results.

In one year, CyberAlumni formed a trusted, bonded community with presence and reputation in the field, successfully connecting the outcomes of certification courses to employment through continuing professional education and development. In future years, they will aim to increase their offerings for educational advancement, collaboration, and employment as they gain new members and connect to more NCAE-Cs across the country.

C. *The Model at a Glance*

Our Collaboratory Model in Fig. 3 is designed to add value to every stage of a cybersecurity career and foster continuous learning. Embedding a feedback loop into this model creates an adaptable pipeline for continuous and repeatable success.

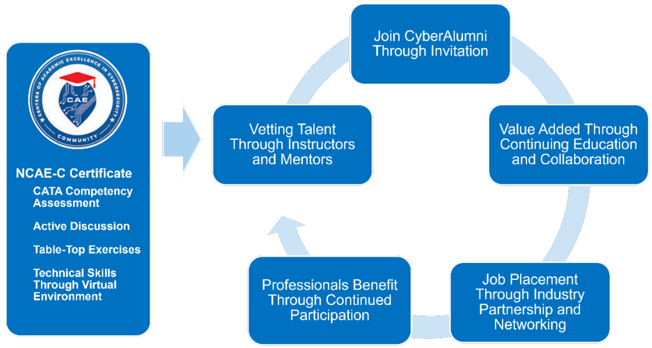
NCAE-C Certificate
CATA Competency Assessment
Active Discussion
Table-Top Exercises
Technical Skills Through Virtual Environment
Join CyberAlumni Through Invitation
Vetting Talent Through Instructors and Mentors
Value Added Through Continuing Education and Collaboration
Professionals Benefit Through Continued Participation
Job Placement Through Industry Partnership and Networking

Fig. 3. The CyberAlumni life cycle created by the Cyber Alumni

- Students complete rigorous certifications through an NCAE-C, including competency assessment, active discussion, table-top exercises, human and machine side content.
- High achieving graduates are vetted by trusted instructors and mentors, then invited to join the CyberAlumni.
- Individuals connect with peers and form digital communities to advance their education and pursue further certifications as a group.
- Through the CyberAlumni community, we provide mentorship and out of classroom learning opportunities to collaborate with government and industry partners on various projects.
- Members accelerate their careers or find new employment opportunities through the CyberAlumni network or industry partnerships.
- After transitioning into management careers or higher education, members can continue to participate in the large network of mentors and collaborators to influence cybersecurity education and find upcoming talent.

D. *The Three C's of CyberAlumni*

CyberAlumni established three principal functions that serve a significant role in the professional development of members.

1. Community
2. Collaboration
3. Continuing education

By developing members through this model, CyberAlumni also hopes to strengthen all three functions across the cybersecurity workforce. Stronger digital communities, wider and more productive collaborations, and the promotion of continuing education that ties directly to careers.

E. *Community*

A bonded, trusted community of peers and mentors provides support and motivation for continuing education. This model uses participants to drive each other's success. Current literature points to mentorship from qualified mentors as a high impact practice for strengthening cybersecurity education and advancement [6]. Peer mentorship has proven to be equally important [7].

Effective mentorship practices result in:

- increased interest in cybersecurity careers
- higher retention of course content
- better job placement
- stronger security awareness postures
- positive social impacts

Connecting individuals with a larger group to pursue further education makes more opportunities available and affordable. This creates value for the individual, prospective employers, and the community. Students also receive the opportunity to be a part of a larger network that follows through different companies and institutions. Instead of a purely student/graduate community, CyberAlumni connects with former and retired CISO / DISO mentors, government and industry partners, potential employers, and other educational institutions looking for collaborators.

F. Collaboration (and Co-creation)

Out-of-class learning through collaboration and co-creation with industry partners is a pathway for developing efficacy and professional competencies within CyberAlumni. Out-of-class learning is proven to be a "viable pedagogical mechanism," leading to professional and career development, intellectual growth, and awareness [8]. These opportunities are difficult to find in the standard cybersecurity curriculum.

This approach builds off the system-activity learning model used in the UW NCAE-C to incorporate experience with real world problem solving. The activity-based approach provides purposeful problem-solving opportunities within a structured professional environment where "Knowledge is treated, not as the end goal of the educational process (i.e., learning for a grade), but as a tool to solve practical, complex problems, creatively and independently, unleashing the learner's potential" [9]. CyberAlumni take this a step further by moving graduates from an engineered environment with specific methodologies to higher risk real life situations with the support of peers and mentors. Alumni are motivated to take ownership of the problem and utilize the provided tools to independently develop themselves as they reach creative solutions.

G. Continuing Education: The Next Step

Career advancement and success are tied to continuing professional education. The rapidly changing nature of cybersecurity demands that cyber professionals be lifelong learners [10]. Professionals at any point in their career from interns to CISOs can benefit from pursuing more effective and efficient professional education. CyberAlumni uses two parallel approaches to increase accessibility for members.

Pursuing new certifications and courses as a group increases student success and affordability. Increasing accessibility and engagement in continuing education through digital communities helps to meet the growing demand for competent cybersecurity professionals [11]. This opportunity provides career pathways for top-level talent vetted through CyberAlumni.

As a trusted community of vetted, certified cybersecurity professionals/students, CyberAlumni connects industry, government, and academia (see Fig. 4). Having the perspective of consumers and the background of cybersecurity professionals, CyberAlumni can partner with curriculum providers, government agencies, and industry leaders.

Each party has a personal stake in advancing the student through the education pipeline. Bringing industry to the table aligns curriculum to the current job market and cybersecurity landscape. This allows the industry to promote better security awareness and competency of incoming cybersecurity professionals. The government and military benefit from end-to-end pipeline educational material production and national security posture across sectors. Academic institutions and educational providers get high quality reviewers to improve their curriculum.

H. Scalability: Applying the model

This approach to creating a post completion pipeline works in parallel with strict federal educational standards and curricula developed through NCAE-Cs. NCAEs provide a strong baseline of competency, opening the flexibility to expand across the country [12]. Establishing a stand-alone organization that works in parallel with the academic centers allows alumni to carry their membership forward, expanding their digital network and adaptability.

More investigation into the scalability of mentorship programs is needed. Partnerships with the 6-State Consortium funded by the NSA Grant for the SmartGrid is our next target, expanding potential through the Pacific Northwest, and Oceania.

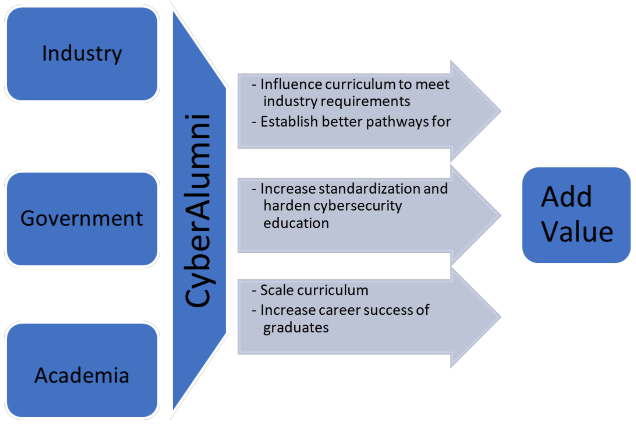
Industry
Government
Academia
CyberAlumni
- Influence curriculum to meet industry requirements
- Establish better pathways for
- Increase standardization and harden cybersecurity education
- Scale curriculum
- Increase career success of graduates
Add Value

Fig. 4. Outcomes of curricula review conducted through CyberAlumni

V. RESULTS / OUTCOMES

In 2021, CyberAlumni achieved their goals of pursuing continuing education, industry, and government collaborations, and establishing a trusted, bonded community. CyberAlumni was first composed of a handful of founding members. Few select individuals were invited to join within the first year as CyberAlumni set the groundwork for their first offerings to upcoming graduates.

There are no large-scale metrics available to gauge this model's success, but there are quantifiable outcomes of the organization's activity.

TABLE I. FIRST YEAR OUTCOMES

Engagements	
Follow-on certification opportunities	4
Professional work products produced	3
Curricula and tools reviewed	5

The first cohort of CyberAlumni gained access to four valuable certifications at no cost through collaborations to review curricula and tools. Three new EC-Council technical certifications were assessed and compared to their previous offering, then adopted into the NCAE-C Courses. Another collaboration opened the opportunity to attend a test pilot course on cultural and linguistic blind spots in cybersecurity. Additionally, CyberAlumni were able to arrange a 50% price reduction for future groups to earn the CISSP certification.

Productive collaborations with educational providers, industry, and government yielded positive outcomes ranging from adoption and improvement of educational tools to research funding acquisition.

Individual success of alumni can be used to gauge the effectiveness of the model. Among the founding members, two reaped great rewards from their involvement. One member was elevated to a higher-level position in recognition of the interdisciplinary experience and added value through their participation in the CyberAlumni. Another member was awarded by their Naval ROTC Unit, given additional scholarship, and promoted to a higher position because of educational collaborations and review of curricula.

VI. FUTURE DIRECTION

In the future, CyberAlumni plans to scale up their digital communities, investigate new educational tools and curricula, and form stronger connections to NCAE-Cs across the country.

Scaling up will involve increasing membership, mentoring opportunities, and industry partnerships. The UW NCAE-C has produced 1,600 qualified graduates. From this source, we will invite and vet CyberAlumni for their first large-scale offering. CyberAlumni also plan to secure agreements with industry and government partners to hire directly out of their community, establishing strong career paths forward for members.

CyberAlumni is currently investigating new gamified cybersecurity education tools for developing professional competencies and increasing engagement in younger demographics. Modern cyber ranges and competition may be crucial to providing real-world experience in a classroom setting, furthering the professional development of members, and raising the bar for future graduates. Further extending opportunities to engage in gamified cybersecurity to lower levels of education has potential to increase security awareness and the number of incoming students.

As the UW course model is adopted to other NCAE-Cs, CyberAlumni plan to join them in connecting graduates across the country together. To make sure the process is repeatable and continuously improving, further data driven metrics for success need to be established.

REFERENCES

[1] Oltsik J., Lundell B., (2021), *The Life and Times of Cybersecurity Professionals 2021*, in Enterprise Strategy Group Research Report, Information Systems Security Association, (July 2021).

[2] Hatton T., Effinger C., (2022), *Cybersecurity Jobs Surging*, in Lightcast Blog, Lightcast, (June 2022).

[3] CyberSeek, (2022), *Cybersecurity supply and demand heat map*, in CyberSeek, https://www.cyberseek.org/heatmap.html, last accessed December 11, 2022.

[4] Johnson, Ralph. (2022). Graduation Ceremony for NCAE 22 students, September 16, 2022.

[5] Avalumni, In Facebook. https://www.facebook.com/UWVWA/, last accessed September 15, 2022.

[6] Payne B., Mayes L., Paredes T., Smith E., Wu H., and Xin C., (2021), *Applying High Impact Practices in an Interdisciplinary Cybersecurity Program*, In Journal of Cybersecurity Education, Research and Practice, Kennesaw State University Institute for cybersecurity workforce development, (January 2021).

[7] Pinchot J., Cellante D., Mishra S., and Paullet K., (2020), *Student Perceptions of Challenges and Role of Mentorship in Cybersecurity Careers: Addressing the Gender Gap*, In Information Systems Education Journal, Information Systems and Computing Academic Professionals, (June 2020).

[8] Kam H. and Katerattanakul P., (2019), *Enhancing Student Learning in Cybersecurity Education Using an Out-Of-Class Learning Approach*, In Journal of Information Technology Education: Innovations in Practice, Informing Science Institute, (January 2019). https://doi.org/10.28945/4200

[9] Endicott-Popovsky B. and Popovsky V., *Activity-Based Approach to Developing Professionals within Higher Education Programs*, University of Washington Tacoma Institute of Technology.

[10] Endicott-Popovsky B. and Popovsky V., (2014), *Application of Pedagogical Fundamentals for the Holistic Development of Cybersecurity Professionals*, In Cybersecurity Education, The ACM Committee for Computing Education in Community Colleges, (March 2014).

[11] Noche E., (2021), *A Literature Review of Empirical Studies on Cyber Security Workforce Development*, In Asian Journal of Multidisciplinary Studies, Asian Journal of Multidisciplinary Studies, (14 December 2021).

[12] Dawson M., Wang P., and Williams K., (2018), *The Role of CAE-CDE in Cybersecurity Education for Workforce Development*, In Information Technology – New Generations, Springer C., (13 April 2018). https://doi.org/10.1007/978-3-319-77028-4_20

[13] Ellithorpe J., (2016), *The Role and Impact of Cyber Security Mentoring*, In Walden University College of Management and Technology, ProQuest Dissertations Publishing, (2016).

[14] Wang P., Sbeit R., (2020), *A Comprehensive Mentoring Model for Cybersecurity Education*, In 17th International Conference on Information Technology – New Generations, Springer C., (12 May 2020).

[15] Hinrichs R. and Wankel C., (2012), *Engaging the Avatar: New Frontiers in Immersive Education (Research in Management Education and Development)*, In Research in Management and Educational Development, Information Age Publishing, (1 March 2012).

[16] Hinrichs R. and Wankel C., (2011), *Transforming Virtual World Learning (Cutting-Edge Technologies in Higher Education)*, In Cutting Edge Technologies in Higher Education, Emerald Publishing, (3 October 2011).

[17] Hinrichs R., (1997), *Intranets: What's the Bottom Line*, In Prentice Hall Ptr, (1 January 1997).

[18] Crumpler W. and Lewis J., (2019), *The Cybersecurity Workforce Gap*, Center for Strategic and International Studies, Center for Strategic and International Studies, (January 2019).

[19] Opacki J., (2017), *Building a Security Culture: Why Security Awareness Does Not Work and What to Do Instead*, In ISACA Journal, ISACA, (16 August 2017).

[20] Janeja V. Faridee A., Gangopadhyay A., Seaman C., and Everhart A., (2018), *Enhancing Interest in Cybersecurity Careers: A Peer Mentoring Perspective*, In Proceedings of the 49th ACM Technical Symposium on Computer Science Education, Association for Computing Machinery, (21-24 February 2018). https://doi.org/10.1145/3159450.3159563