Cybersecurity Internship Impacts on Participant Professional Development and Employment: A Case Study

A DISSERTATION SUBMITTED TO THE GRADUATE DIVISION OF THE UNIVERSITY OF HAWAIʻI AT MĀNOA IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN

Communication and Information Sciences

May 2025

By

David J. Stevens

Dissertation Committee:

Scott Robertson, Chairperson
Guylaine Poisson
Jenifer Sunrise Winter
Rich Gazan
Dan Hoffman, University Representative

Keywords: Cybersecurity, Internships, Workforce Development

Acknowledgement

I want to thank my father for inspiring me to pursue this path. His steady encouragement and belief in the power of education gave me the confidence to take on this challenge and see it through. I'm also grateful to my dissertation committee for their support, insight, and professionalism throughout this process. Their example set a high bar and helped shape both the quality of this work and my own standards moving forward. I would also like to thank the faculty of the University of Hawai‘i Kapi‘olani Community College IT Program for their guidance and support throughout my academic journey. Special thanks as well to the U.S. Naval Information Warfare Center, and to our industry partners at Adapt Forward and Core4ce, for their collaboration and engagement. Their support was instrumental to the success of this work. And to my wife, Lee, thank you for your patience, your energy, and for being the "boots to my glutes" when I needed a push. This wouldn't have happened without you.

ABSTRACT

In response to the growing need for qualified cybersecurity professionals, this study examines the impacts of a unique cybersecurity internship program at the University of Hawai‘i (UH) in partnership with the U.S. Naval Information Warfare Center (NIWC) and industry partners. The ongoing program seeks to bridge the gap between academic training and real-world application, focusing on participant professional development and employment outcomes. This study covered the internship cycles from 2020 to 2023 using a mixed-method approach, surveyed 34 of the 46 program participants, and conducted follow-up interviews to assess the internship's effects on technical skills, professional development, personal growth, and employment.

The findings indicate that the internship significantly enhanced participants' communication, research, and technical cybersecurity skills. However, challenges related to industry certification requirements, hands-on technical training, and US government job application processes were identified. The study highlights the importance of mentorship, hands-on experience, and industry certification in preparing students for careers in cybersecurity. Recommendations for improving the internship program include greater emphasis on certification preparation, expanded practical learning opportunities, and clearer guidance on job applications, particularly within the government sector.

Table of Contents

Acknowledgement i
ABSTRACT ii
Table of Contents iii
List of Tables iv
Chapter 1. Introduction 1
Background and Research Questions 3
Implementation 6
Theoretical Framework 8
Research Questions 9
Chapter 2. Literature Review 11
Chapter 3. Methods 37
Study Population 37
Instruments 38
Procedures 38
Chapter 4. Results and Discussion 40
Data Analysis 40
Survey Questions 40
Likert Scale Survey Questions 40
Participant Open-ended Questions 49
Participant Follow-up Interviews 68
Instructor Interviews 77
Chapter 5. Study Conclusions 85
Appendix A - Surveys and Interviews 90
Appendix B - Interview Questions and Transcripts 98
References 143

List of Tables

Table 1: Survey – Part I: Personal Info…….……..40

Table 2: Survey – Part II, 1: Reasons for Internship Participation……..…42

Table 3: Survey – Part II, 2: Expected Gains from Internship……42

Table 4: Survey – Part II, 3: Impact on current and future employment……....42

Table 5: Survey – Part III: Professional Development (PD) ……..…43

Table 6: Survey – Part IV: Professional Skills (PS) ……..…44

Table 7: Survey – Part V: Personal Growth (PG) ……..…45

Table 8: Survey – Part VI: Personal Capabilities (PC) ……..…46

Table 9: Open-ended Questions - PII - 3,a.…….…...49

Table 10: Open-ended Questions - PIII – 1……51

Table 11: Open-ended Questions – PIV -1……..……..…53

Table 12: Open-ended Questions - PV – 1……..……..…55

Chapter 1. Introduction

The Internet is the ocean: a massive, interconnected entity supporting life, fostering growth, driving economies, shaping political landscapes, molding cultures, and providing immeasurable capabilities. A dominant force shaping life fundamentally through the flow of information, it enables communication, commerce, education, innovation, collaboration, personal growth, and the exchange of ideas.

Like the ocean, the Internet has the power to inflict great damage that can be unpredictable and far-reaching. When misused, it can spread misinformation, enable cybersecurity breaches, and fuel digital addiction, all of which can harm communities, prevent commerce, and impair personal security and mental health. Despite its vast infrastructure, the Internet relies on interconnected physical components, such as satellites, cables, routers, and data centers, vulnerable to disruption. Overreliance on the Internet can lead to the crash of global financial markets, the disruption of supply chains, and the interruption of emergency services.

Unlike the ocean, the Internet can come under purposeful attack. It is here that cybersecurity professionals are essential. The Internet, sprawling and intertwined with every part of modern life, creates an ever-growing patchwork of vulnerabilities. The more connected our lives become, the more exposed we are to exploitation. Cyber-attacks are not distant threats; they are immediate and frequent and can have catastrophic consequences. From ransomware that cripples entire businesses to data breaches that expose personal identities, cybercrime can unravel the very fabric of trust that keeps economies and societies afloat. In this chaotic digital sea, cybersecurity professionals serve as the first and often the last line of defense, working to secure the essential structures on which modern life depends.

These professionals are responsible for safeguarding personal privacy and national security. The Internet is a vast repository of personal data, from financial information to health records and social identities, all of which are ripe targets for cybercriminals. But beyond individual threats, the entire infrastructure of nations is at stake. Critical resources, such as electric grids, hospitals, and transportation systems, are vulnerable to malicious cyber operations that could disrupt services, endanger lives, and cause widespread panic (Krause, 2021). Unlike

the natural ebb and flow of the ocean, these disruptions are intentional, malicious, and ever more sophisticated. It is cybersecurity professionals who stand between these threats and the collapse of essential systems, ensuring the safety of individuals and nations alike.

The Internet is also the backbone of the global economy. But a single breach can destroy a company's reputation, disrupt business operations, and erode consumer confidence (Cremer, 2022). Without trust in the security of digital transactions and communications, commerce would falter. The Internet's role in driving global economic growth hinges on the public's faith in its safety and reliability. Cybersecurity professionals, working diligently in the background, fortify this trust, ensuring that the Internet continues to function as the vital economic engine it is. They are the unseen hands that keep the machinery running, protecting businesses from potentially crippling information system compromises and helping them navigate the constant dangers of an increasingly digital marketplace.

Governments around the world have come to recognize the dangers of leaving this vital resource unprotected. To address these risks, they have enacted stringent regulations such as the General Data Protection Regulation (GDPR) in Europe and the Health Insurance Portability and Accountability Act (HIPAA) in the United States, demanding that organizations safeguard sensitive data. These laws reflect an acknowledgment that the Internet must be shielded from those who seek to exploit its weaknesses. Cybersecurity professionals ensure compliance with these regulations, serving as the frontline defense against data breaches, identity theft, and corporate negligence.

Yet even with the most advanced technologies, the human element remains one of the weakest links. Human error, whether through carelessness, ignorance, or deliberate malice, opens the door to network intrusions (Ncubukezit, 2022). Phishing scams, social engineering, and insider threats continue to pose risks that no system can fully prevent. Cybersecurity professionals not only build and maintain technical defenses but also work to educate individuals and organizations, promoting awareness and resilience. By fostering a culture of vigilance, they minimize the risks posed by human error, guiding us away from potential dangers just as careful navigation steers a ship clear of treacherous waters.

The Internet, like the ocean, offers boundless opportunities for growth and connection, yet it remains a volatile space fraught with potential dangers. Cybersecurity professionals are the guardians who ensure that this vast and vital resource continues to function safely and

effectively. They are the ones who stand watch, defending against the unseen threats that lurk beneath the surface, ensuring that the Internet remains a force for progress and collaboration, rather than chaos and destruction. Their vigilance keeps us all afloat in an increasingly digital world, steering society safely through the shifting tides of the modern era.

Recognizing the vital role of cybersecurity professionals in protecting critical digital infrastructure, it is essential to examine how educational programs are preparing future experts to meet the growing demands of the field. As cyber threats become more complex and widespread, the need for academic experiences that combine technical training with real-world application has never been greater. This case study investigates a uniquely structured cybersecurity internship program at the University of Hawai‘i (UH), developed through an unprecedented partnership with the United States Naval Information Warfare Center (NIWC) and industry collaborators. What sets this program apart is its intentional use of a collaborative model that integrates academic institutions, federal defense entities, and private sector partners to create a holistic, immersive training environment.

By embedding students directly into projects shaped by operational needs and guided by both academic mentors and industry professionals, the program offers a rare opportunity to experience the full spectrum of cybersecurity practice, from theoretical foundations to applied operations. This study contributes new academic knowledge by examining how such partnerships can be designed and implemented to improve learning outcomes, workforce readiness, and long-term career trajectories. It provides a grounded analysis of how multi-sector collaboration can enhance internship effectiveness and may serve as a model for future cybersecurity education initiatives across higher education.

Background and Research Questions

In 2019, representatives from the NIWC visited several UH campuses in Hawai‘i on the island of O‘ahu, one of which was Kapi‘olani Community College (KapCC). While there, the representatives told the faculty of the information technology (IT), program that the NIWC was looking for ways to increase the number of cybersecurity personnel in their organization, and they were visiting college campuses to try to build an educational pipeline of future cybersecurity workers.

The KapCC IT Program already had a diverse educational program that provided advanced instruction and experience in IT, and each IT student was required to participate in an internship with a local company performing IT operations (i.e., programming, networking, cybersecurity, computer maintenance, etc.), for one hundred twenty hours during one of their final semesters before graduation.

While working at a company, the interns were also required to enroll in an internship class and participate in professional development activities under the supervision of KapCC IT faculty. Completion of these activities demonstrated achievement of the internship learning outcomes of developing skills in communication, writing, job searches, interviewing, and career advancement, including résumé creation, industry certification, career research, mock interviews, and professional social media profile creation.

The following list contains some examples of the professional development learning outcome activities included.

Professional Etiquette Instruction

This online course addressed professional etiquette in the modern workplace and focused on the students' relationships with other people. It also dealt with social and emotional intelligence and described behavioral traits shared by successful professionals.

Resume Writing Instruction

This was an online course that presented techniques for constructing a résumé and cover letter that stand out among other job candidates. Several résumé and cover letter formats were provided to assist the student in presenting professional skills to be more competitive in today's job market. This course also covered methods to transform an average résumé and cover letter into a refined and effective marketing tool.

Resume Creation Project

For this assignment, students were required to review résumé creation tips from an online employment search website and then create a résumé containing information about their education, certifications, skill sets, work experience, and other related professional information.

Certification Research Project

This assignment required students to create a research paper detailing what IT industry certification exams are available, what jobs they lead to, how much the certifications cost, and what certifications build on others. Then, the students were required to describe what they might do in preparation to pass those certification exams.

IT Jobs and Career Paths Project

This project required students to research various career paths in the IT sector and describe the requisite skills and knowledge for each. For example, when researching different jobs in the networking or cybersecurity fields, what knowledge, certifications, etc., would each job require? What does each job pay? And how much experience would one need to advance in that field?

Professional Social Media Profile Creation

For assignment credit, students must create a professional social media account at LinkedIn.com using a parallel (same name) Gmail account. In the Profile section of their LinkedIn site, students must upload personal artifacts (evidence) from both their technology classes and their outside/off-campus achievements, demonstrating their experience in IT and cybersecurity.

Interviews

Students are given two choices for credit in this assignment as described below.

First option:

Participation in three mock interviews assigned at the annual KapCC IT Advisory Day event. Each spring, the Information Technology (IT) Program hosts an IT Advisory meeting that serves two primary purposes. First, advisory board members share current industry trends, workforce needs, and employer expectations, providing valuable insights that help KapCC IT faculty align the program curriculum with local industry demands. Second, students nearing graduation participate in mock interviews with board members, gaining practical experience in

articulating their skills and career goals. These interactions not only strengthen the program's connection to the local IT community but also support students' transition into the workforce.

For credit**,** students must submit a report that includes the titles of all the jobs they were interviewed for and their interviewers' contact information.

Second option:

Students must research interview basics (students are provided with links to professional employment websites). For credit**,** students must write a two-page summary describing what guidance they found most useful.

Internship Summary Professional Paper

For the last assignment, students are required to submit a detailed, concise report on what they gained from their internship experience, the positive aspects of their internship, how the internship experience can be improved, and any other comments they wish to add.

Required information for both the Mid-Term and Final assignments is gathered using a Google survey, allowing the student's work supervisor to submit an evaluation of each student's performance. The first survey is sent after the student has completed approximately 50 percent of their internship work hours and serves as their midterm evaluation. Feedback from this survey helps assess the student's early performance, professionalism, and ability to apply classroom knowledge in a real-world setting. The second survey is administered at the end of the semester and functions as the student's final evaluation. This assessment reflects the student's overall growth, technical development, and readiness for employment. Together, these evaluations contribute directly to the student's course grade, providing a structured measure of progress and ensuring accountability throughout the internship experience.

Implementation

The KapCC IT faculty suggested that the NIWC help create a unique cybersecurity internship by combining the applied cybersecurity instruction by NIWC instructors, focusing on the knowledge and skills required by the NIWC, and a professional development internship class taught by the KapCC IT Program faculty.

In Fall 2020, the Naval Information Warfare Center (NIWC) Pacific partnered with the University of Hawai‘i to launch the first NIWC Cybersecurity Internship, enrolling 17 students. The program was considered a success by both NIWC and UH, largely due to its strong student participation and positive feedback. As a result, NIWC continued to fund the internship annually for the next four years, supporting its growth across the University of Hawai’i system.

My name is David Stevens, and I’m an Assistant Professor of Information Technology and Cybersecurity at the University of Hawai’i Kapi‘olani Community College. I teach a variety of technology-related courses, including programming, databases, network security, project management, cloud-based computing, ethical hacking, incident response, and forensics. Before transitioning to academia, I spent 20 years working in the IT industry, where I held roles as a programmer, website developer, project manager, and cybersecurity specialist.

I hold a Master of Science in Information Systems (MSIS) from Hawai’i Pacific University, and both a Certified Information Systems Security Professional (CISSP) and Project Management Professional (PMP) credentials. Currently, I am pursuing my Ph.D. at the University of Hawai’i Mānoa, with my research focusing on cybersecurity internships.

As an educator, I try to practice continuous improvement when creating lectures, curriculum, course content, formative assessments, and summative exams. I create and teach classes that thoroughly cover the planned learning objectives and evaluate the knowledge gained by my students. Based on the results, I adjust accordingly to more effectively engage my students and achieve better results the next time I teach the course.

This internship was a unique opportunity to blend relevant industry knowledge with a professional development course. I was excited to participate in an effort to help students learn advanced cybersecurity skills while also learning skills essential to the success of any industry professional. Most internships place the student in an environment that helps them become competent in their chosen field. This new internship would also include professional development activities. In this paper, I document the results of this learning experience in an attempt to determine the impacts on the participants.

This dissertation is a case study of the UH NIWC Cybersecurity Internship, examining its impacts on participants' professional development and skills, personal growth and capabilities, and employment.

This study is important because it provides valuable recommendations to commercial, government, and educational organizations regarding the creation, improvement, and advancement of cybersecurity internships, which can improve cybersecurity students' professional skills, personal growth, problem-solving abilities, and work-related experience.

Theoretical Framework

Social Learning Theory: Understanding Observational Learning

Since Albert Bandura introduced Social Learning Theory, its significance in the field of psychology has been widely recognized (Bandura, 1977). Bandura's theory posits that individuals learn by observing the behaviors of others and the consequences of those behaviors rather than through direct reinforcement or classical conditioning. This approach challenges traditional behaviorist views by emphasizing the role of cognitive processes in learning (Bandura, 1986). Bandura's research on observational learning has profoundly impacted educational practices, social psychology, and therapeutic interventions (Bandura, 1963).

Bandura also introduced the concept of self-efficacy, which refers to an individual's belief in their ability to succeed in specific situations. Self-efficacy plays a crucial role in Bandura's Social Learning Theory, as individuals with high self-efficacy are more likely to engage in challenging tasks and persist in the face of obstacles (Bandura, 1997). Bandura's research on self-efficacy has been instrumental in understanding motivation, performance, and resilience in various domains, including education, career development, and mental health (Bandura, 2001).

Bandura's Social Learning Theory provides a valuable framework for understanding the relationship between academic internships and learning experiences. According to Bandura (1977), individuals acquire knowledge and skills through direct instruction, observation, modeling, and reinforcement. Academic internships allow students to observe and participate in real-world work environments, providing a platform for experiential learning rooted in Bandura's principles.

During academic internships, students can observe professionals in action, model their behaviors and practices, and receive feedback on their performance. This process aligns with Bandura's emphasis on observational learning and the role of vicarious reinforcement in shaping

behavior (Bandura, 1986). By immersing themselves in workplace settings, students can enhance their skills, develop new competencies, and expand their understanding of their chosen field through hands-on experiences.

Bandura's concept of self-efficacy is particularly relevant to the context of academic internships. As students engage in internship activities and tasks, their confidence in their abilities to perform effectively in professional settings grows (Bandura, 1997). Strong self-efficacy beliefs can lead to increased motivation, persistence, and adaptability, which are essential for success in both academic and professional environments.

Additionally, Bandura's Social Learning Theory highlights the importance of social interactions in the learning process. During academic internships, students can collaborate with colleagues, seek guidance from mentors, and receive constructive supervisor feedback. These social interactions enhance the learning experience and provide a supportive environment for skill development and knowledge acquisition (Bandura, 2001).

Social learning theory is related to this study because academic internships offer a valuable platform for applying Bandura's Social Learning Theory in practice. Incorporating Bandura's principles into the design and implementation of internship programs can enhance the learning outcomes and prepare students for successful transitions from academia to the workplace.

This case study adds useful knowledge to research regarding how internships play a crucial role in shaping students' knowledge, skills, and self-efficacy beliefs by providing students with opportunities for observational learning, modeling, vicarious reinforcement, and social interactions.

Research Questions

The research questions of the study are as follows:

Q1 – How did the UH NIWC Cybersecurity Internship program have an impact on students' professional development?

Q2 – How did the UH NIWC Cybersecurity Internship program have an impact on the professional skills of students?

Q3 – How did the UH NIWC Cybersecurity Internship program have an impact on the personal growth of students?

Q4 – How did the UH NIWC Cybersecurity Internship program have an impact on students' post-internship employment in the cybersecurity industry?

This study examined the unique model of the UH NIWC internship that combines cybersecurity work experience under the supervision of NIWC, cybersecurity industry instructors, and classroom participation in professional development activities under the supervision of KapCC IT faculty.

These activities provide knowledge and skills required for communication, writing, job searches, interviewing, and career advancement, including creating a professional résumé, mock interviews, creating a professional social media profile (i.e., LinkedIn), and writing academic research papers on topics such as cybersecurity industry certifications and possible cybersecurity career pathways.

Chapter 2. Literature Review

As the world becomes increasingly reliant on digital platforms, the importance of cybersecurity has never been more pronounced. From securing personal data in everyday transactions to defending national security systems, cybersecurity plays a pivotal role in safeguarding the digital infrastructure of modern society (Dawson & Thomson, 2018).

Cybersecurity Workforce Challenges and Required Competencies

As cyber threats grow more sophisticated, the demand for a highly skilled cybersecurity workforce has intensified, yet most research focuses primarily on technical proficiency. The growing prevalence and complexity of cyber threats underscore the urgent need for a highly skilled cybersecurity workforce. Cyberattacks have evolved beyond simple data breaches, now targeting critical infrastructure, national security, and financial institutions (IEEE Public Safety Technology Initiative, 2024). These increasing threats demand a workforce equipped not only with technical expertise but also with problem-solving capabilities to address sophisticated cyber challenges. However, despite this growing need, organizations continue to face a shortage of qualified cybersecurity professionals, limiting their ability to effectively respond to emerging threats (Burrell, 2020).

While technical expertise remains a fundamental requirement, addressing the cybersecurity workforce shortage requires a broader understanding of the skills necessary for success in the field. Beyond technical proficiency, cybersecurity professionals must navigate complex problem-solving scenarios, adapt to evolving threats, and effectively communicate risks to stakeholders.

Recognizing these challenges, Dawson and Thomson (2018) argued that successful cybersecurity professionals require a combination of technical skills, cognitive flexibility, and social intelligence to thrive in an evolving digital landscape. Their study reviewed existing literature on cybersecurity workforce development, highlighting a gap in understanding the non-technical attributes necessary for effective cyber performance.

The authors proposed six core traits essential for cybersecurity professionals: systemic thinking, teamwork, continuous learning, strong communication, civic duty, and a balance of technical and social skills. They emphasized that cybersecurity is not just about defending

networks but also about understanding human behavior and mitigating risks introduced by user vulnerabilities. Their findings suggest that organizations must integrate psychological and social assessments into cybersecurity hiring and training processes, ensuring that professionals can effectively collaborate, communicate risks, and adapt to emerging threats.

Dawson and Thomson (2018) concluded that developing a resilient cybersecurity workforce requires a holistic approach that extends beyond technical expertise. By incorporating social and cognitive metrics into recruitment and training, organizations can build teams that are not only technically adept but also capable of addressing the human factors that influence cybersecurity success.

The Role of Internships in Bridging Academic and Industry Gaps

As organizations struggle to fill critical cybersecurity roles, practical training models such as internships have become essential for bridging the gap between academic preparation and industry demands. Internships provide students with real-world exposure to security protocols, risk mitigation, and hands-on experience with evolving cyber threats, better preparing them for the workforce.

As internships become an essential bridge between academic learning and professional practice, ensuring their effectiveness requires coordinated collaboration. Internships provide students with valuable opportunities to apply classroom learning in professional settings, develop technical and soft skills, and build industry networks (Coco, 2000).

Internships also play a crucial role in workforce preparation by helping students develop hands-on skills. Coco (2000) explored the increasing importance of internships as a bridge between academic learning and professional employment. Once considered an optional supplement to education, internships have now become a crucial differentiator for students entering the workforce. The study highlighted that three out of four students complete internships before graduation, underscoring their perceived significance in developing practical skills, professional competence, and career readiness.

However, not all internships are created equal. The effectiveness of internship programs depends on structured mentorship, clear learning objectives, and integration between academic institutions and industry partners. Research on internships has identified key factors that

contribute to successful outcomes, emphasizing the need for well-designed programs that align with workforce demands (Akhtar, 2024).

Internship Design and Stakeholder Collaboration

Benavides, Dicke, and Holt (2013) explored how partnerships between universities, students, and host organizations create high-quality internship experiences. The study outlined the historical development of internships in public administration and evaluated how structured internship models contributed to student preparedness for the workforce.

The authors introduced a framework that positions internships at the intersection of three key stakeholders: universities, which provide academic oversight; government and nonprofit organizations, which offer real-world experience; and students, who engage in applied learning. The research highlighted that successful internships depend on clear expectations, structured supervision, and integration of academic and practical components. Findings from surveys conducted in Network of Schools of Public Policy, Affairs, and Administration (NASPAA)-accredited programs underscore the need for intentional program design, mentorship, and assessment strategies to maximize the impact of internships.

The study also addressed policy developments, including the Federal Internship Improvement Act, which aimed to streamline internship programs and facilitate career transitions for students. Benavides et al. (2013) emphasized that internships must be more than just temporary work placements—they should serve as comprehensive learning experiences that benefit students and host organizations alike. By fostering strong collaboration among stakeholders, internship programs can better prepare students for careers in public service while reinforcing the value of experiential education in higher learning.

Student and Employer Perspectives on Internship Effectiveness

Henry, Rehwaldt, and Vineyard (2001) further explored the effectiveness of internship programs by examining the perspectives of both student interns and worksite supervisors. Their study identified key academic and workplace competencies that contribute to a successful internship experience, emphasizing the importance of alignment between educational institutions and employers. The research found that mismatched expectations often hindered learning

outcomes, reinforcing the need for structured mentorship, clear learning objectives, and continuous assessment to ensure meaningful skill development.

Educational Design Principles and Instructional Support

A key factor in optimizing learning outcomes in internship programs is the intentional design of instructional and interactive elements, particularly when digital learning environments are involved. Research by Stevens (2022) highlighted how structured visual cues—such as bolded text, directional arrows, and interactive buttons—can enhance engagement and improve user task efficiency in educational software.

These findings suggested that similar principles can be applied to internship programs, where clear guidance and structured frameworks can optimize student learning experiences and performance. Beyond enhancing individual learning, well-designed internships offer broader advantages that extend to multiple stakeholders. Internships provide mutual benefits for students, employers, and educational institutions. Students gain hands-on experience, improve technical and analytical skills, and enhance adaptability in dynamic work environments.

For businesses, internships serve as a low-risk recruitment tool, allowing them to evaluate potential employees before making full-time hiring decisions. Universities also benefit, as internships help validate curriculum relevance and improve graduate employability (Rose, 2013). However, proper selection processes and structured mentorship programs are essential in ensuring meaningful, skill-building opportunities (Qubati, 2021).

To further explore the impact of structured internships, Hurst and Good (2010) examined how internship quality influences career preparedness and long-term professional success. Their research highlighted key trends in the evolving landscape of internships, including the increasing prevalence of paid opportunities and the critical role of employer-educator partnerships in shaping meaningful internship experiences. Their findings underscored the importance of internship quality, showing that students who participated in well-structured programs with clear responsibilities and mentorship opportunities reported higher job preparedness and career confidence. The study also revealed disparities in access to paid versus unpaid internships, emphasizing the potential implications for economic equity in workforce development. These disparities highlight the need to examine not only the availability of internships but also their long-term effects on career outcomes.

Long-Term Career Outcomes and Equity in Internship Access

The impact of internships on post-graduate employment outcomes is well-documented. Sagen, Dallam, and Laverty (2000) conducted a study examining the extent to which internship experiences influence students' career trajectories, employer hiring preferences, and long-term professional success. Their research found that students who participated in internships were significantly more likely to secure full-time employment in their chosen fields compared to those without internship experience. Additionally, their study highlighted that employers increasingly rely on internship experience as a key criterion in hiring decisions, viewing it as a reliable indicator of job readiness and future performance. These findings underscore the growing importance of internships not just as learning opportunities but as a strategic advantage in the competitive job market.

Wolniak and Engberg (2019) further explored the long-term benefits of internships, emphasizing how these experiences contribute to both professional growth and overall career success. Their study examined post-graduate employment trends among students who had completed internships, finding that participation in such programs significantly increased job placement rates and early career earnings. The research also highlighted that internships serve as a powerful tool for social mobility, helping students from diverse backgrounds gain access to competitive job opportunities. Additionally, their findings underscored that internship experiences not only improve technical competencies but also enhance critical soft skills such as adaptability, networking, and professional confidence. These insights reinforce the growing recognition of internships as essential stepping stones to career advancement, positioning them as a key factor in workforce readiness.

Internship Effectiveness: Design and Mentorship Matter

Hora, Chen, Parrott, and Her (2020) examined the 'skills gap' narrative surrounding internships and found that while internships can be a powerful tool for bridging educational and professional competencies, their effectiveness is often hindered by a lack of structured learning goals and inconsistent employer engagement. Their findings reinforce the notion that simply offering an internship is not enough—intentional design, oversight, and alignment with industry expectations are necessary to ensure meaningful skill development.

This concern is further supported by research that highlights how internship experiences can vary significantly depending on factors such as mentorship quality, workplace integration, and alignment with academic training. Holyoak (2013) explored the variability in internship experiences, emphasizing the role of intern-supervisor relationships in shaping learning outcomes. The study found that interns who received structured guidance, constructive feedback, and professional mentorship were more likely to develop critical workplace competencies and transition successfully into full-time roles. Conversely, interns in loosely structured or poorly supervised placements often struggled to gain meaningful skills, highlighting the importance of intentional design and oversight in internship programs. Recognizing the significance of well-structured internships, researchers have examined their broader role in shaping workforce readiness and career outcomes.

A national survey of business schools confirmed the growing prevalence and impact of internships. Over 90%of institutions reported offering internship programs, with a significant percentage leading to full-time employment. The study concludes that internships are a "try before you buy" arrangement, benefiting all stakeholders and solidifying their role as an essential component of modern education and workforce development (Coco, 2000).

Employer Perspectives and the Value of Internship Experience

As competition in the job market intensifies, employers increasingly seek candidates with practical experience. Gault, Leach, and Duey (2010) investigated the value of business internships from the employer's perspective, surveying 185 employers who supervised 392 interns enrolled in an Association to Advance Collegiate Schools of Business (AACSB)-accredited business college. Their study explored how internship participation influences hiring decisions, salary offers, and perceptions of candidate readiness.

Findings indicated that students with internship experience are significantly more likely to receive full-time job offers than non-interns. Even average-performing interns are preferred over candidates without internship experience, while high-performing interns command higher starting salaries. Employers also report that internship programs enhance job-specific skills, improve workplace adaptability, and increase long-term career success. The study further highlighted that high intern performance positively influences employer perceptions of the overall value of internship programs.

Gault et al. (2010) concluded that internships play a crucial role in bridging the gap between academic training and industry expectations, reinforcing their importance as a core component of business education. Their findings advocate for stronger university-employer partnerships and expanded internship opportunities to enhance student employability and workforce readiness.

Beyond individual benefits, the research underscored the broader implications for universities and businesses. Employers view internships as an effective talent pipeline, reducing hiring costs and improving recruitment efficiency. Additionally, structured internship programs contribute to higher job satisfaction, faster promotions, and greater organizational commitment among former interns. Given these benefits, employers increasingly view internship experience as a valuable indicator of a candidate's readiness for the workforce.

Hodges (2007) explored how employers evaluate the skills and competencies of graduates entering the workforce, emphasizing the importance of internship experience in hiring decisions. The study found that while technical expertise is highly valued, employers also prioritize soft skills such as communication, teamwork, and adaptability. Additionally, Hodges highlighted that structured internships provide students with opportunities to develop workplace professionalism, problem-solving abilities, and industry-specific knowledge. The research concluded that well-designed internship programs play a crucial role in enhancing student employability, bridging the gap between academic learning and industry expectations. However, access to these opportunities can be influenced by various factors, including financial constraints and career goals, which shape students' ability to participate in internships.

Equity and Access in Internship Participation

Eagan, Lozano, Hurtado, and Case (2013) analyzed national trends among first-year college students, focusing on factors such as financial concerns, career aspirations, and internship participation. Their study highlighted that students increasingly view internships as a critical component of career preparation, particularly in fields where professional experience is highly valued. Findings also suggested that financial barriers can limit access to internships, raising concerns about equity in career development opportunities. While financial constraints can hinder student participation, employers also face challenges in structuring internships that effectively balance accessibility, skill development, and organizational needs.

Cojocariu, Cîrtiţă-Buzoianu, and Mareş (2019) examined employer perspectives on internship programs, identifying both the benefits and challenges associated with these initiatives. Their study found that while many employers valued internships as a means of recruiting skilled talent and assessing potential employees, inconsistencies in intern preparedness and employer expectations often hindered program effectiveness. The research emphasized the need for closer collaboration between universities and businesses to ensure that internship curricula align with industry requirements and provide students with relevant, real-world experience.

Historical and Financial Perspectives on Experiential Learning

Beyond serving as a recruitment pipeline, internships also contribute to broader economic and financial benefits, particularly when designed to align with sustainable employment strategies. Seelye and Selby (2018) examined the role of apprenticeships in colonial America, highlighting how these early training models addressed labor shortages and facilitated workforce development in emerging industries. Their research provided historical insights into the origins of experiential learning, illustrating how structured skill acquisition has long been a foundational component of workforce preparation. By drawing parallels between historical apprenticeships and modern internships, the study reinforced the continued relevance of hands-on learning in developing industry-ready professionals. This historical perspective aligns with earlier research on apprenticeships as foundational workforce training models, highlighting their long-standing role in skill development.

Rorabaugh (1986) explored the role of apprenticeships in early American society, emphasizing their significance in skill acquisition and workforce development before the rise of formalized education systems. His study detailed how apprenticeships served as a primary means of training young individuals in trades, providing both structured learning and labor contributions. While apprenticeships offered essential technical training, they were also shaped by rigid social and economic structures that dictated access to skill development opportunities. As industrialization progressed, these models gradually declined in favor of institutionalized education and wage labor systems. Rorabaugh's research underscored the historical foundations of experiential learning, highlighting how modern internship programs continue to evolve as a critical bridge between academic knowledge and workforce readiness. Building on this

foundation, contemporary research has explored additional benefits of structured internships beyond skill development, particularly their role in financial preparedness and career decision-making.

Miralles-Quirós and Jerez-Barroso (2018) emphasized that structured internship programs not only facilitate skill development but also enhance financial literacy and decision-making among early-career professionals. Their research underscored how internship experiences contribute to long-term career stability, ensuring that participants gain the knowledge necessary to navigate financial planning, job market fluctuations, and sustainable employment trends. This highlighted the importance of internships not just as training opportunities but as foundational experiences that shape professionals' long-term financial and career trajectories.

Further supporting this perspective, Urquía-Grande and Pérez Estébanez (2021) highlight how internships foster financial decision-making skills by providing students with real-world exposure to budgeting, investment considerations, and financial planning within their professional environments. Their findings suggest that internships serve as critical learning experiences that shape students' long-term financial acumen, reinforcing their ability to make informed career and economic decisions post-graduation. Beyond financial literacy, internships also play a pivotal role in shaping students' overall career trajectories by equipping them with the practical skills and industry exposure needed to transition successfully from academia to the workforce.

Industry-Academia Collaboration in Workforce Development

As the IT industry continues to expand, the demand for industry-ready graduates has intensified, exposing gaps between academic training and employer expectations. Manisha and Manuja (2011) explored the design challenges of industry-academia collaboration, analyzing how structured engagement can bridge these gaps and improve graduate employability. Their study focused on Infosys's Campus Connect initiative, a large-scale collaboration model implemented across engineering institutions in India to align curriculum content with industry requirements.

The paper identified four primary approaches to industry-academia partnerships: in-house corporate training, outsourced training programs, corporate universities, and direct academic

collaboration. The authors argued that a comprehensive partnership model is the most effective strategy, integrating faculty training, industry-relevant coursework, and student skill development initiatives. The Campus Connect program employed a four-step framework—curriculum enhancement, faculty enablement, student training, and real-world problem-solving exercises—to systematically improve graduate competencies. Challenges in scalability, sustainability, and performance measurement remain central concerns.

The study highlighted key evaluation metrics, including recruitment impact, faculty development effectiveness, and student learning outcomes. Findings suggest that structured collaborations significantly improve student preparedness, reduce corporate training costs, and foster long-term institutional reform. Manisha and Manuja (2011) concluded that while industry-academia partnerships require sustained effort and institutional buy-in, they represent a viable solution for addressing workforce readiness challenges in the rapidly evolving IT sector.

One key component of these partnerships is the integration of internship programs, which serve as a bridge between academic learning and industry demands. However, despite their significance, the effectiveness of internships varies widely, and their evaluation remains inconsistent across higher education institutions.

Assessment and Evaluation of Internship Outcomes

Internships play a crucial role in preparing students for the workforce, yet their evaluation remains inconsistent across higher education institutions. Haddad-Adaimi, Abi Zeid Daou, and Ducq (2022) explored the challenges of assessing internship learning outcomes and proposed a structured, performance-based approach to evaluation. Their study identified the absence of standardized models for internship assessment, noting that existing quality assurance systems prioritized theoretical coursework while neglecting the impact of practical learning experiences.

The authors introduced a framework that incorporates both qualitative and quantitative performance indicators to measure student progress before, during, and after internships. By comparing self-evaluations with supervisor assessments, the model minimized subjectivity and enhanced the reliability of internship evaluations. Additionally, the study highlighted the importance of linking internship outcomes with industry expectations, emphasizing that structured performance measurement can provide actionable insights for curriculum improvement.

Findings suggested that a data-driven approach to internship evaluation not only enhances student preparedness but also ensures alignment between academic institutions and employers. The study advocated for universities to adopt systematic assessment methods that track competency development, identify gaps in student skills, and implement corrective measures where necessary. Haddad-Adaimi et al. (2022) concluded that integrating performance-based evaluation into internship programs strengthens the connection between higher education and labor market demands, ultimately improving graduate employability. However, enhancing employability requires more than just effective evaluation; it demands a shift in how institutions approach skill development.

Embedding Employability into Higher Education Curricula

As higher education institutions face growing pressure to improve graduate employability, educators must move beyond fragmented approaches to skill development. Knight and Yorke (2003) argued that employability is not merely about acquiring discrete skills but is deeply tied to complex learning processes that require systemic integration into higher education curricula. Their study critiqued conventional efforts such as work placements, career services, and isolated skill-building modules, claiming these approaches fail to address the broader learning environments necessary for long-term employability.

The authors proposed a model in which employability emerges from a combination of subject knowledge, practical skills, self-efficacy, and metacognitive awareness. Rather than focusing on short-term interventions, they advocated for curriculum-wide strategies that embed employability into the learning process, ensuring that students develop problem-solving abilities, adaptability, and reflective learning habits over time. Their findings highlighted that effective employability development spans entire programs, emphasizing holistic learning experiences rather than piecemeal solutions.

The study also challenged the reliance on employment statistics as a measure of educational success, arguing that true employability is demonstrated through graduates' ability to adapt, innovate, and thrive in evolving job markets. Knight and Yorke (2003) concluded that higher education institutions must rethink their approaches to learning and teaching, ensuring that employability is cultivated through integrated, systemic educational frameworks rather than isolated, add-on initiatives. This need for a comprehensive, embedded approach is particularly

relevant in fields like cybersecurity, where professionals must possess not only technical expertise but also the problem-solving and interpersonal skills necessary to navigate an increasingly complex threat landscape.

High-Impact Educational Practices in Cybersecurity

As cybersecurity education continues to evolve, ensuring that graduates possess both technical expertise and professional skills is critical for workforce readiness. Payne et al. (2021) explored how high-impact educational practices (HIPs) enhance student learning and engagement in an interdisciplinary undergraduate cybersecurity program. The study focused on five key HIPs: learning communities, undergraduate research, internships, service learning, and electronic portfolios.

Findings indicated that integrating HIPs into cybersecurity curricula improves student retention, communication skills, and applied problem-solving abilities. Learning communities foster peer collaboration and industry awareness, while undergraduate research enables students to develop critical thinking and technical expertise. Internships provide hands-on experience, reinforcing coursework through real-world applications. Service learning strengthens civic engagement and soft skills, particularly in cybersecurity awareness initiatives, and electronic portfolios allow students to showcase their competencies to potential employers.
Despite implementation challenges, such as faculty buy-in, employer partnerships, and student participation barriers, the study concluded that HIPs are essential for producing well-rounded cybersecurity professionals. Payne et al. (2021) recommended that institutions integrate experiential learning opportunities throughout cybersecurity curricula, cultivate cross-disciplinary collaboration, and emphasize writing and communication as core competencies. Their findings reinforce that a holistic, practice-oriented approach to cybersecurity education better prepares students for dynamic industry demands.

High-Impact Educational Practices and Workforce Preparation

English et al. (2021) also examined the effectiveness of HIPs in preparing students for careers in science, technology, engineering, and mathematics (STEM) fields. Their study assessed the impact of experiential learning methods such as internships, undergraduate research, and capstone projects in fostering job readiness. The findings emphasized that students who

engaged in HIPs developed stronger critical thinking skills, communication abilities, and professional networks compared to those who relied solely on traditional coursework. Furthermore, the research underscored the importance of mentorship and structured reflection in maximizing the benefits of these practices. By integrating HIPs into cybersecurity education, institutions can ensure that graduates are not only technically proficient but also possess the professional skills necessary for workforce success.

Building on this perspective, Brownell and Swaner (2009) examined the broader impact of HIPs across various disciplines, highlighting their role in enhancing student engagement, skill development, and long-term academic success. They explored the effectiveness of HIPs in fostering student engagement, skill development, and long-term academic success. Their study examined the impact of experiential learning strategies, including internships, learning communities, and service learning, across a wide range of disciplines. The findings emphasized that HIPs significantly enhance students' critical thinking abilities, communication skills, and overall career preparedness. Importantly, their research highlighted that structured, reflective experiences—such as internships with integrated mentorship and guided learning opportunities—yield the most substantial benefits. These insights reinforce the necessity of incorporating HIPs into cybersecurity education, ensuring that students develop the practical competencies required to navigate an increasingly complex digital landscape.

Cyber Threats and the Urgency for Skilled Defenders

As cyber threats continue to evolve, the need for well-prepared cybersecurity professionals becomes even more urgent. The growing sophistication and frequency of cyberattacks pose significant risks to individuals, organizations, and governments, underscoring the importance of a workforce equipped to respond effectively.

The sophistication and frequency of cyberattacks have escalated dramatically over the past decade, leaving individuals, organizations, and governments vulnerable to significant disruptions. These threats are not only becoming more complex but are also targeting a wider range of digital assets, from personal data to critical infrastructure (IEEE Public Safety Technology Initiative, 2024).

The IEEE Public Safety Technology Initiative (2024) explored the cybersecurity challenges facing critical infrastructure sectors, including energy, transportation, and water management, emphasizing the need for enhanced security measures.

The report identified common vulnerabilities in Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) environments, such as outdated software, weak authentication mechanisms, insecure remote access, and lack of network segmentation. Cyber attackers exploit these weaknesses to gain unauthorized access, deploy malware, and disrupt industrial operations. Recent attacks targeting power grids, oil pipelines, and automated emergency response systems illustrate the growing risk posed by sophisticated threat actors, including nation-state adversaries.

The study highlighted best practices for securing ICS/SCADA systems, including implementing network segmentation, adopting zero-trust security models, and deploying continuous monitoring tools. The report also underscored the importance of regulatory compliance, with guidelines from the National Institute of Standards and Technology (NIST) and the North American Electric Reliability Corporation (NERC) playing a crucial role in strengthening critical infrastructure resilience.

The IEEE Public Safety Technology Initiative (2024) concluded that addressing ICS/SCADA cybersecurity requires a multi-layered approach, incorporating technological advancements, regulatory enforcement, and public-private collaboration to safeguard essential services from evolving cyber threats.

As cyber threats grow in sophistication, securing critical infrastructure demands more than just regulatory measures and technological advancements; it requires a workforce capable of anticipating, mitigating, and responding to these evolving risks. While frameworks and policies provide essential safeguards, their effectiveness ultimately hinges on skilled professionals who can implement, monitor, and adapt security measures in real-time.

The increasing reliance on digital systems across industries has only amplified the urgency for a well-equipped cybersecurity workforce, one that can navigate the ever-expanding threat landscape and counteract emerging vulnerabilities before they escalate into full-scale crises.

Workforce Shortages and Industry Expectations

Despite increased investment in cybersecurity measures, organizations across industries struggle to find professionals with the necessary skills to combat these threats (Ramezan, Coffy, & Lemons, 2023). The complexity of modern cyberattacks requires professionals with interdisciplinary expertise, yet the current workforce remains insufficient in both quantity and preparation. This shortage of cybersecurity talent presents a major vulnerability, limiting organizations' ability to prevent, detect, and respond to threats in a rapidly evolving digital environment.

Ramezan, Coffy, and Lemons (2023) analyzed 100 job postings to determine the most sought-after qualifications for operational technology (OT) cybersecurity roles. Their study identified key prerequisites, including prior professional experience, academic credentials, industry certifications, technical skills, and soft skills required by employers.
Findings indicated that OT cybersecurity roles are typically not entry-level, with 95% of positions requiring prior professional experience and 82% requiring at least a bachelor's degree. Additionally, 64% of job postings list industry certifications such as CISSP and GICSP as preferred or mandatory. Employers also emphasize strong communication skills, knowledge of OT frameworks (e.g., International Electrotechnical Commission (IEC) 62443, NERC Critical Infrastructure Protection (CIP)), and familiarity with IT-OT networking protocols. Security clearance requirements appear in 24% of postings, while 29% of roles include travel obligations. The study emphasized the need for structured career pathways, suggesting that aspiring OT cybersecurity professionals should prioritize gaining hands-on experience, pursuing relevant certifications, and developing both technical and soft skills. Ramezan et al. (2023) concluded that educational institutions must align cybersecurity curricula with industry needs, integrating experiential learning opportunities to better prepare students for the evolving OT cybersecurity landscape.

However, preparing a cybersecurity workforce that is not only skilled but also diverse is equally critical. As the field continues to expand, ensuring equitable access to cybersecurity careers becomes a key factor in strengthening the workforce and addressing industry-wide talent shortages. Diversity and inclusion are crucial in developing a well-rounded cybersecurity workforce. The National Association of Colleges and Employers (NACE) conducted its 2021 Internship & Co-op Survey to assess various facets of employers' internship and co-op programs,

including hiring projections, program structures, compensation, and diversity metrics. The findings indicate that men hold a significant majority in both intern and co-op positions, accounting for 57.6% and 67.5% respectively. Additionally, white students are predominantly represented, comprising 62% of interns and 71% of co-ops. These statistics suggest a misalignment between employers' stated DEI objectives and the actual demographic makeup of their internship cohorts. NACE Executive Director Shawn VanDerziel emphasizes this concern, noting that while employers often cite a diverse and inclusive workforce as a strategic priority, their internship and co-op programs do not reflect this commitment. The report underscores the need for organizations to critically evaluate and enhance their recruitment and selection processes to foster greater diversity and inclusivity within these pivotal programs.

A more inclusive approach to talent development is particularly important in fields like cybersecurity, where the demand for skilled professionals continues to outpace supply. Despite the growing need for cybersecurity expertise, organizations still struggle to find qualified professionals who can effectively mitigate evolving threats. The demand for cybersecurity expertise has risen significantly, yet there remains a notable shortage of qualified professionals equipped to handle the increasing variety of threats (Dawson & Thomson, 2018).

Several factors contribute to the shortage of cybersecurity professionals. First, rapid technological advancements outpace traditional education programs, leaving many graduates unprepared for real-world cyber challenges (Tsado, 2019). Second, there is a disconnect between industry needs and educational training, with many programs focusing heavily on technical skills while neglecting soft skills such as problem-solving and communication. Third, organizations often struggle to provide ongoing training and professional development, making it difficult for employees to keep up with the ever-changing cybersecurity landscape (Tetteh & Otioma, 2024). These factors, combined with an increasing demand for cybersecurity expertise, exacerbate the workforce gap and highlight the need for new approaches to cybersecurity education and training.

Challenges in Cybersecurity Education and Training

Tsado (2019) explored how higher education institutions can address this shortage through a top-driven, school-wide approach to cybersecurity education. The study emphasized that cybersecurity is not solely a technical discipline but requires expertise across multiple fields,

including law, business, and policy. By integrating cybersecurity concepts into both technical and nontechnical programs, institutions can expand the pipeline of qualified professionals while enhancing workforce readiness.

The paper highlighted the role of the National Security Agency (NSA) and the Department of Homeland Security (DHS) in designating Centers of Academic Excellence (CAEs) to guide cybersecurity curriculum development. However, many institutions lack CAE designation, limiting their ability to produce cybersecurity talent. Tsado argued that universities should adopt a structured, multidisciplinary strategy incorporating cybersecurity education at all levels, regardless of CAE status.

Findings suggested that a successful cybersecurity program requires institutional leadership support, faculty engagement, and strong partnerships with industry. Tsado (2019) concluded that a top-driven, interdisciplinary approach is essential for reducing the cybersecurity skills gap, fostering collaboration across disciplines, and ensuring that graduates possess the technical expertise and problem-solving skills needed to combat evolving cyber threats.

However, even with interdisciplinary strategies in place, the effectiveness of cybersecurity education is often undermined by a lack of practical, hands-on experience. Without direct exposure to real-world security challenges, graduates may struggle to apply their knowledge effectively in high-stakes environments. Current training programs often fall short of providing practical, hands-on experience. This lack of focus on immediate security challenges leaves graduates underprepared for the workforce (Dawson & Thomson, 2018).

The Need for Continuous Learning and Upskilling

Moreover, the importance of continuous learning cannot be overstated in the cybersecurity field. Professionals must constantly adapt to new and emerging threats, yet many organizations are unable to offer the training and development opportunities necessary to maintain these skills (Tsado, 2019). This gap in ongoing education further exacerbates the shortage, making it difficult for the workforce to stay adequately prepared.

Research further suggests that upskilling plays a crucial role in mitigating the adverse effects of cyberattacks on organizations. In particular, Tetteh and Otioma (2024) found that firms investing in continuous cybersecurity education and training experience a lesser decline in productivity following security breaches. Their study underscored the importance of human

capital development in strengthening an organization's ability to manage cyber risks, reinforcing the argument that cybersecurity resilience is not solely about technology but also about workforce preparedness.

This gap between the need for cybersecurity professionals and the availability of qualified individuals creates a significant vulnerability in the security infrastructure of organizations worldwide. With the growing reliance on digital infrastructure and the increasing frequency of cyber threats, closing the cybersecurity workforce gap has become a critical priority. Organizations, governments, and educational institutions must implement targeted strategies to expand and strengthen the cybersecurity workforce. A comprehensive approach—including policy reforms, expanded training programs, and alternative learning models—is necessary to ensure that the next generation of cybersecurity professionals is equipped to address emerging threats effectively.

National Strategies for Cyber Workforce Development

Given the increasing threat landscape, it is imperative to close the gap in the cybersecurity workforce. Developing a proficient cyber workforce should be a top priority for governments, educational institutions, and industries (Office of the National Cyber Director, 2024).

The growing demand for cybersecurity professionals necessitates a coordinated national strategy to bridge workforce gaps and enhance cyber education. The Office of the National Cyber Director (2024) reported on the initial implementation of the National Cyber Workforce and Education Strategy (NCWES), which seeks to remove barriers to cyber careers, promote skills-based hiring, and establish education-to-workforce pathways.

The strategy emphasized a whole-of-nation approach, requiring collaboration between government, industry, and academia to address workforce shortages. Federal agencies have begun adopting skills-based hiring models, reducing reliance on traditional degree requirements. Additionally, the establishment of registered apprenticeships and scholarship programs has expanded opportunities for diverse candidates to enter cyber careers. The report highlighted key federal initiatives, including investments in cybersecurity training, expansion of the National Centers of Academic Excellence in Cybersecurity (NCAE-C), and workforce pipeline development through K-12 and higher education institutions.

The Office of the National Cyber Director (2024) concluded that continued investment in workforce development, skills training, and employer partnerships is critical to national security and economic stability. The report underscored the need for ongoing collaboration to ensure the successful implementation of the NCWES and sustain the momentum in strengthening the nation's cybersecurity workforce.

A key component of this effort is equipping graduates with the practical skills needed to navigate real-world security challenges. To strengthen the link between academic learning and industry expectations, higher education institutions are increasingly turning to experiential learning models.

Work-Integrated Learning as a Workforce Solution

As industries demand graduates with real-world competencies, higher education institutions increasingly incorporate Work-Integrated Learning (WIL) into curricula. Smith, Ferns, and Russell (2014) investigated the effectiveness of WIL in enhancing student employability, using a multi-university study to assess how placements and simulated work experiences contribute to work readiness. Their research explored six key employability dimensions: professional practice, theory-practice integration, lifelong learning, collaboration, informed decision-making, and commencement readiness.

The study found that students who engage in high-quality WIL placements exhibit significantly greater confidence in their workplace capabilities compared to those without such experiences. Placement quality plays a crucial role, with well-structured and supervised internships yielding the most substantial benefits. Simulations, while valuable, contribute to employability at a lower level than direct workplace placements.

Employers emphasize that WIL enhances critical workplace skills such as communication, problem-solving, and adaptability. The study highlighted the importance of structured preparation, supervision, and reflective debriefing to maximize student learning outcomes. Findings suggested that embedding WIL across curricula, rather than as a standalone experience, produces the most work-ready graduates.

Smith et al. (2014) advocated for universities to strengthen industry partnerships, refine placement structures, and incorporate simulation-based learning where placements are impractical. Their research underscored that WIL is a powerful mechanism for bridging the gap

between academic knowledge and professional application, reinforcing the necessity of experiential learning in higher education. As industries increasingly rely on internships and other experiential learning opportunities to develop workforce-ready graduates, it is essential to examine how well these programs align with industry expectations.

Aligning Internship Design with Industry Competencies

Jones et al. (2017) investigated the competencies advertised in IT internship postings, comparing them to the professional standards outlined by the Association for Computing Machinery (ACM) and the Institute of Electrical and Electronics Engineers (IEEE). Through text mining and content analysis of 86 internship postings, the study identified trends in the skills that students are expected to gain through WIL experiences.

Findings indicate that while internship postings emphasize technical skills, such as web administration, programming, and system architecture, there is less focus on general competencies like communication, teamwork, and problem-solving. This imbalance raises concerns about whether internships are adequately preparing students for the multifaceted demands of IT careers. The study also highlighted the inconsistency in internship descriptions, with some postings lacking clarity on expected learning outcomes.

Jones et al. (2017) concluded that to maximize the effectiveness of IT internships, employers and academic institutions must work together to create structured, competency-based programs that integrate both technical expertise and essential workplace skills. Their findings underscored the need for standardized internship frameworks that ensure students gain well-rounded, industry-relevant experience. In fields like cybersecurity, where threats evolve rapidly, the need for well-structured, practical training becomes even more critical. Without comprehensive education and hands-on experience, the workforce may struggle to keep pace with emerging security challenges.

Immediate investments in cybersecurity education, training, and recruitment are essential for ensuring that organizations can protect their digital assets from growing threats. One effective approach to addressing the cybersecurity workforce shortage is through internships.
While universities play a crucial role in preparing students for cybersecurity careers, traditional classroom instruction alone is insufficient to meet industry demands. Many academic programs focus on theoretical knowledge, leaving graduates without the hands-on experience needed to

tackle real-world security threats (Tsado, 2019). To bridge this gap, work-based learning opportunities—such as internships—have emerged as a promising solution for equipping students with the necessary skills and experience before they enter the workforce.
By immersing interns in practical security operations, these programs offer a bridge between academic knowledge and professional practice, making them a powerful tool for workforce development.

Cybersecurity-Specific Internship Benefits and Challenges

Internships, in general, have long been recognized for their ability to resolve the disconnect between theoretical learning and professional experience (Williams, 2010). Williams (2010) explored the key elements that define effective work-based learning (WBL) and examined its role in nursing education. The study critically reviewed existing literature, identifying three fundamental aspects of WBL: the importance of learning in real-world contexts, the necessity of reflective practice, and the role of professional autonomy in shaping meaningful learning experiences.

The research stressed that while WBL is often perceived as mere task-based training, its true value lies in its ability to foster critical thinking and lifelong learning among nurses. The study finds that for WBL to be effective, organizations must cultivate a learning culture that supports self-directed education, encourages professional reflection, and integrates theoretical knowledge with clinical practice. Furthermore, structured facilitation and mentorship play a crucial role in ensuring that learners can effectively translate new insights into practice.

Workplace-Based Learning as a Catalyst for Professional Growth

Williams (2010) argued that shifting from a predominantly classroom-based approach to a workplace-centered model requires careful planning and institutional support. The study underscores the need for healthcare organizations to implement structured learning frameworks that empower nurses to take control of their professional development. Ultimately, the findings suggest that workplace-based learning (WBL), when effectively implemented, has the potential to enhance clinical decision-making, improve patient care, and drive continuous professional growth in the nursing field.

The value of WBL extends beyond the healthcare sector, playing a pivotal role in fields where practical experience is essential for competency. In cybersecurity, where threats evolve rapidly, the ability to apply theoretical knowledge in real-world environments is crucial for developing effective professionals. Structured internships and hands-on training opportunities connect classroom learning and industry demands, equipping students with the skills needed to navigate complex security challenges. While internships play a crucial role across various fields, their design and implementation can vary depending on industry-specific needs.

Industry-Specific Insights: Designing Internships for Applied Learning

Mailhiot (2022) analyzed internship programs in the entertainment technology sector, examining their role in preparing students for careers in media, digital design, and technical production. The study revealed that internships in this field often differ from traditional corporate internships, requiring students to engage in project-based learning, creative problem-solving, and collaboration with industry professionals. Findings suggested that well-structured entertainment technology internships enhanced career readiness by immersing students in real-world production environments where adaptability and innovation were key.

Martin, Quillen, and Shaw (2013) specifically analyzed intelligence internships, investigating how these programs prepare students for high-stakes roles in cybersecurity, law enforcement, and national defense. Their research highlighted the unique demands of intelligence-related internships, such as security clearances, analytical problem-solving, and exposure to classified or sensitive information. The study emphasized that these internships not only develop technical expertise but also instill critical thinking, ethical decision-making, and adaptability—competencies that are essential in cybersecurity and intelligence professions. When applied to cybersecurity, the following benefits become even more critical.

Knowledge Application

Interns can apply their academic learning to real-world situations, deepening their understanding of cybersecurity concepts like threat analysis and incident response (Thrombre, 2022).

Thombre and Velankar (2022) explored the effectiveness of cybersecurity internships in bridging the gap between theoretical instruction and industry application. Their study examined

how structured internship programs enhance students' ability to apply classroom knowledge to real-world security challenges. Through a combination of simulated cyberattacks, vulnerability assessments, and incident response exercises, students developed practical problem-solving skills while gaining exposure to evolving threat landscapes. The findings emphasized that hands-on cybersecurity training significantly improves workforce readiness by fostering technical competence, adaptability, and critical thinking. Their research underscores the need for experiential learning opportunities in cybersecurity education, reinforcing the idea that well-designed internships play a crucial role in preparing students for the demands of the profession.

Development of Soft Skills

In addition to technical skills, internships help students cultivate non-technical competencies such as communication, teamwork, and problem-solving, which are essential for success in the workplace (Ritter, 2018).

Ritter et al. (2018) explored how management education must evolve to meet these expectations, emphasizing the role of soft skills—such as communication, leadership, and collaboration—as key differentiators in the job market. Their study highlighted a curriculum redesign at a business school that integrates soft skill development into the core management coursework.

Using a backward design framework, the authors outlined a structured approach that ensured students not only understood management principles but also developed the competencies necessary to navigate complex workplace dynamics. The revised curriculum incorporated experiential learning techniques, emphasizing real-world applications of teamwork and leadership.

Results from standardized assessments, student surveys, and employer feedback indicated that graduates of the redesigned program demonstrated significantly improved collaboration skills and workplace readiness.

Beyond individual student benefits, the study underscored the broader impact of aligning academic programs with employer needs, suggesting that institutions prioritizing soft skill development create a more competitive and adaptable workforce. Ritter et al. (2018) argued that higher education must proactively address the gap between traditional business education and

evolving industry expectations, reinforcing that soft skills are no longer supplementary but essential components of professional success.

Improved Employment Prospects

Internships are a proven entry point to full-time employment, with research showing that participation significantly increases the likelihood of securing a job post-graduation (Smith, 2014).

Networking Opportunities

Internships provide a gateway to professional networks that can lead to job offers and career growth (Knight & Yorke, 2003).

Aligning Internship Design with Learning Outcomes

Extensive research highlights the positive outcomes of effective internships, with Luk and Chan (2022) emphasizing their role in equipping students with valuable skills and experiences across multiple key areas. As internships become an integral part of engineering education, assessing students' learning outcomes is essential for refining internship course design.

Luk and Chan (2021) explored engineering students' self-reported learning from internship experiences in Hong Kong, using qualitative research methods to analyze responses from ten undergraduate engineering students. The study employed content analysis to classify learning outcomes into four categories: industry and disciplinary knowledge, academic-related generic competencies, non-technical generic competencies, and technical skills.

Findings indicated that students commonly gain industry-specific knowledge, enhance problem-solving and writing skills, and develop interpersonal and teamwork competencies through internships. However, the application of theoretical knowledge to real-world problems remains limited, with most students observing rather than actively practicing engineering concepts. Variability in student experiences also suggests that internship learning is unpredictable, influenced by workplace structure, assigned tasks, and mentorship quality.

Luk and Chan (2021) concluded that internship programs must align intended learning outcomes with actual workplace experiences. They recommend stronger collaboration between

academia and industry, structured reflection activities, and a learning contract to ensure clear expectations. Their findings emphasize the importance of designing internships that provide meaningful, structured learning opportunities to enhance students' transition from academia to industry.

Internships provide students with a range of benefits that enhance both their academic and professional development:

- First, internships enhance students' knowledge in specific domains. For example, in cybersecurity, students can build expertise in areas such as threat analysis, incident response, and vulnerability management. Additionally, internships help students develop competencies relevant to academic success, including technical writing, research, and analytical thinking.
- Second, beyond academic abilities, internships play a crucial role in the development of non-technical skills. These include essential soft skills like adaptability, time management, and effective communication, which are necessary for successfully navigating workplace dynamics.
- Lastly, internships offer hands-on opportunities to build technical skills, particularly in fields like cybersecurity. Students gain practical experience in IT areas such as encryption, networking, and systems security, making them more prepared for professional challenges.

The Unique Demands and Value of Cybersecurity Internships

The process of conducting successful internships involves providing adequate mentorship, offering exposure to real-world challenges, and creating opportunities for interns to contribute meaningfully to security operations. A well-structured internship program should balance the acquisition of both technical and non-technical skills, preparing students for a smooth transition into full-time roles (McDonald, 2022).

Cybersecurity internships stand out due to the nature of the field. While internships have been widely studied across various fields, cybersecurity internships present unique challenges and opportunities. Unlike other disciplines, cybersecurity requires professionals to stay ahead of constantly evolving threats, work with highly sensitive data, and navigate ethical and legal

considerations. These distinctive demands shape the structure and effectiveness of cybersecurity internships, necessitating specialized approaches to ensure that students gain the skills and experiences required for success in this field (Sussman, 2023).

The evolving threat landscape demands that interns not only master foundational technical skills but also stay adaptable to the rapid changes in security protocols and technologies. Cybersecurity interns often engage in tasks such as vulnerability assessments, security audits, and incident response simulations, providing them with a unique blend of theoretical knowledge and real-world experience (Tsado, 2019).

Moreover, cybersecurity internships often require interns to handle sensitive information and adhere to strict ethical and legal guidelines, further distinguishing these experiences from other fields. The combination of technical rigor, ethical responsibility, and hands-on learning makes cybersecurity internships an invaluable tool in shaping the next generation of professionals.

The Need for Structured Cybersecurity Internships

In light of the increasing cyber threats and the significant workforce gap, it is clear that developing a skilled cybersecurity workforce is of paramount importance. Internships provide a viable solution by equipping future cybersecurity professionals with the knowledge, skills, and experience needed to succeed in this fast-evolving field. Through well-structured cybersecurity internships, organizations can facilitate the transition between academia and industry, fostering a competent and prepared workforce ready to tackle the challenges of the digital age.

Purpose of this Study

This case study examined a unique implementation of a cybersecurity internship at the University of Hawai‘i (UH) in collaboration with the United States Naval Information Warfare Center (NIWC) and industry partners. This internship began at one of the campuses of UH, Kapi‘olani Community College (KapCC), and due to the perceived success of the pilot program, over the following four years, it grew to serve all ten of the UH campuses. This internship’s structure is a partnership between academia (UH), the cybersecurity industry (Core4ce, AdaptForward), and US Federal government agencies (NIWC Pacific and Atlantic).

Chapter 3. Methods

This chapter presents the methodology used to investigate the impact of the UH NIWC Cybersecurity Internship program on student learning, skill development, and career readiness. As the program's co-creator, I designed this study to examine not only how participants developed technical and professional competencies but also how a structured, collaborative internship model involving academia, government, and industry can shape student outcomes. To explore these questions, I used a mixed-methods approach grounded in Bandura's Social Learning Theory.

The study focused on past internship participants from 2020 to 2023 and included a structured online questionnaire, follow-up interviews with students, and interviews with faculty and NIWC instructors. These instruments were selected to capture both quantitative and qualitative data related to students' experiences and perceptions. By analyzing how students learn through observation, modeling, mentorship, and applied practice, this research aims to provide deeper insight into how collaborative, experiential learning programs can help close the gap between cybersecurity education and workforce needs.

Study Population

This study focused on a targeted group of students who completed the UH NIWC Cybersecurity Internship between 2020 and 2023. The survey was sent to all 46 graduates of the program, and 34 responded, resulting in a strong response rate of 73.91 percent. These participants were selected because of their direct involvement in the internship and their connection to a program specifically aligned with the US Department of Defense, NIWC, and the State of Hawai‘i. Their active engagement in the internship and their continued relationships with NIWC and KapCC faculty likely contributed to the high level of participation in this research.

Instruments

The data and information I collected for this study came from interviews with the KapCC IT faculty and NIWC instructors, an online questionnaire sent to students who completed this internship program, and follow-up interviews with selected students.

For this study, I used a structured survey *(see Appendix A)* to collect data from the internship participants. I then conducted follow-up interviews with a subset of internship participants using a structured interview *(see Appendix B)*. I then conducted interviews with the NIWC internship instructors using a structured interview *(see Appendix B)*.

Procedures

Surveys

I distributed the survey to graduates of the 2020–2023 UH NIWC Cybersecurity Internship using Google Surveys (see Appendix A). The survey included an explanation of the study and provided participants the option to opt out or request that their names be included in the results. By default, all responses were anonymized, with no names or identifying information published. The survey was adapted from a previous study on business and finance internships in Pakistan (Anjum, 2020) and used a mixed-methods approach to assess the strengths and limitations of the UH NIWC internship program. The structured questionnaire included six sections designed to capture a range of data on student experiences and outcomes.

- Part I: This section assesses demographic information with short answers.
- Part II: This section assesses participants' reasons for participation in the UH NIWC internship, and includes short answer or open-ended questions.
- Part III–Part VI: These sections assess information regarding professional and personal growth and skills improvement with 35 close-ended questions.

The questions from parts III-VI address Bandura's research findings related to internships. The questions in Part III relate to Bandura's research findings that students can enhance their skills, develop new competencies, and expand their understanding of their chosen field through hands-on experiences.

The questions in Part IV relate to Bandura's claims that students participating in experiential learning acquire knowledge and skills through direct instruction, observation, modeling, and reinforcement.

The questions in Part V relate to Bandura's contention that observational learning and vicarious reinforcement play critical roles in shaping behavior by supporting students' collaboration with colleagues, seeking guidance from mentors, and receiving constructive supervisor feedback.

The questions in Part VI relate to Bandura's assertion that internships impart upon students' strong self-efficacy beliefs that can lead to increased motivation, persistence, and adaptability.

In parts III-VI of the questionnaire, the first question was an open-ended question for greater depth and understanding of the internship experience.

All other questionnaire variables in Parts III-VI were assessed using a 5-point Likert scale, where 1 is strongly disagree, 2 is disagree, 3 is neutral, 4 is agree, and 5 is strongly agree.

Follow-up Interviews

I conducted follow-up interviews with a randomly chosen subset of study participants to gather more detailed information regarding survey answers.

Interviews

I used structured interviews *(see Appendix B)* to gather information about this internship from UH faculty and NIWC instructors. I began the interview with an explanation of the study and statements allowing the interviewee to opt out and/or request their name be included in the study results. The default option was to fully anonymize the data, with no names or identifiers published.

Chapter 4. Results and Discussion

This chapter presents an analysis of the data collected from surveys and interviews with participants and instructors of the UH NIWC Cybersecurity Internship program. The findings are organized around the study's core research questions and Bandura's Social Learning Theory, highlighting how the internship influenced participants' professional development, skill acquisition, personal growth, and career outcomes.

Data Analysis

The study employed descriptive analyses to evaluate the impact of the UH NIWC internship program on cybersecurity students' personal and professional growth and skills. The descriptive techniques include percentage and frequency analysis of the participants' demographic characteristics. The interview data was analyzed for keywords and phrases connecting this internship with Bandura's theoretical framework of Social Learning Theory.

Survey Questions

Likert Scale Survey Questions

Table 1: Survey – Part I: Personal Info

Item	Frequency	Percentage
Age Range (34 responses)		
18-21	3	8.8%
22-25	12	35.3%
26-28	6	17.6%
28+	13	38.2%
Did you graduate from a High School in the state of Hawai‘i? (34 responses)		
Yes	25	73.5%
No	9	26.5%

Which participating UH campus did you attend during the internship? (34 responses)		
University of Hawai‘i Mānoa	13	38.2%
University of Hawai‘i Hilo	0	0.0%
University of Hawai‘i West O‘ahu	5	14.7%
University of Hawai‘i Maui College	3	8.8%
Kapi‘olani Community College	9	26.5%
Kauai Community College	0	0%
Honolulu Community College	3	8.8%
Windward Community College	0	0%
Leeward Community College	1	2.9%
Hawai‘i Community College	0	0.0%
Did you graduate from a university with a degree? (34 responses)		
Yes	28	82.4%
No	6	17.6%
What degree have you earned? (32 responses - multiple degrees possible)		
AA / AS		
BA/BS	13	40.6%
MA / MS	21	65.6%
Ph.D.	3	9.4%
BAS	0	0%
Certificate of Specialization or Graduate Diploma	1	3.1%
not applicable	1	3.1%
Are you currently employed? (34 responses)		
Yes	27	79.4%
No	7	20.6%
Are you employed in a cybersecurity or related position? (34 responses)		
Yes	14	41.2%
No	18	52.9%
not applicable	2	5.9%
Are your work duties related to your major or last earned degree? (34 responses)		
Yes	26	76.5%
No	5	14.7%
not applicable	3	8.8%
In what US state or territory do you currently work? (33 responses)		
Hawai‘i (HI)	28	82.4%
California (CA)	1	2.9%
District of Columbia (DC)	1	2.9%
Oregon (OR)	1	2.9%
Pennsylvania (PA)	1	2.9%
South Carolina (SC)	1	2.9%
outside the United States	0	0.0%
no response to this question	1	2.9%

Table 2: Survey – Part II, 1: Reasons for Internship Participation

Item	Frequency	Percentage
What was the reason you participated in this internship? (34 responses - multiple reasons possible)		
department requirement	9	26.5%
advisor recommendation	11	32.3%
to gain practical industry experience	28	82.4%
other	4	11.8%

Table 3: Survey – Part II, 2: Expected Gains from Internship

Item	Frequency	Percentage
What did you expect to gain from the internship? (34 responses - multiple reasons possible)		
academic credit	20	58.8%
to link classroom learning to workplace reality	27	79.4%
to better prepare for independent life	20	58.8%
other	2	5.9%

Table 4: Survey – Part II, 3: Impact on current and future employment

Item	Frequency	Percentage
I was interested in working in cybersecurity before this internship. (34 responses)		
strongly agree	15	44.1%
agree	14	41.2%
neutral	3	8.8%
disagree	2	5.9%
strongly disagree	0	0.0%
I believe the internship experience helped me get my current job. (34 responses)		
strongly agree	8	23.5%
agree	8	23.5%
neutral	12	35.3%
disagree	5	14.7%
strongly disagree	1	2.9%
I believe my internship experience will help me get promotions in the future. (34 responses)		
strongly agree	8	23.5%
agree	11	32.4%
neutral	12	35.3%
disagree	2	5.9%
strongly disagree	1	2.9%

Table 5: Survey – Part III: Professional Development (PD)

Item	Frequency	Percentage
PD1 – open-ended question discussed later	n/a	n/a
PD2 - My internship program changed me professionally. (34 responses)		
strongly agree	6	17.6%
agree	19	55.9%
neutral	5	14.7%
disagree	3	8.8%
strongly disagree	1	2.9%
PD3 - The internship program helped clarify my professional goals. (34 responses)		
strongly agree	7	20.6%
agree	17	50.0%
neutral	6	17.6%
disagree	2	5.9%
strongly disagree	2	5.9%
PD4 - I applied my classroom knowledge during the internship program. (34 responses)		
strongly agree	9	26.5%
agree	21	61.8%
neutral	2	5.9%
disagree	2	5.9%
strongly disagree	0	0.0%
PD5 - The internship program helped me to gain practical work experience in my field of interest. (34 responses)		
strongly agree	8	23.5%
agree	12	35.3%
neutral	7	20.6%
disagree	5	14.7%
strongly disagree	2	5.9%
PD6 - I encountered difficulty seeking and accepting internship work assignments. (34 responses)		
strongly agree	3	9.1%
agree	8	24.2%
neutral	7	21.2%
disagree	14	42.4%
strongly disagree	1	3.0%

Table 6: Survey – Part IV: Professional Skills (PS)

Item	Frequency	Percentage
PS2 – open-ended question discussed later	n/a	n/a
PS2 - The internship program improved my communication and interpersonal skills. (34 responses)		
strongly agree	11	32.4%
agree	18	52.9%
neutral	3	8.8%
disagree	1	2.9%
strongly disagree	1	2.9%
PS3 - The internship program enhanced my decision-making and problem-solving skills. (34 responses)		
strongly agree	8	23.5%
agree	16	47.1%
neutral	8	23.5%
disagree	1	2.9%
strongly disagree	1	2.9%
PS4 - The internship program improved my ability to work as part of a team. (34 responses)		
strongly agree	3	8.8%
agree	12	35.3%
neutral	15	44.1%
disagree	2	5.9%
strongly disagree	2	5.9%
PS5 - The internship program enhanced my critical thinking skills. (34 responses)		
strongly agree	10	29.4%
agree	20	58.8%
neutral	3	8.8%
disagree	1	2.9%
strongly disagree	0	0.0%
PS6 - The internship program improved my computer, networking, and data analysis skills. (34 responses)		
strongly agree	7	20.6%
agree	16	47.1%
neutral	6	17.6%
disagree	3	8.8%
strongly disagree	2	5.9%
PS7 - The internship program improved my skills in cybersecurity. (33 responses)		
strongly agree	6	18.2%
agree	18	54.5%
neutral	4	12.1%
disagree	4	12.1%
strongly disagree	1	3.0%

Table 7: Survey – Part V: Personal Growth (PG)

Item	Frequency	Percentage
PG1 – open-ended question discussed later	n/a	n/a
PG2 - The internship program helped me improve professionally and personally. (34 responses)		
strongly agree	11	32.4%
agree	20	58.8%
neutral	3	8.8%
disagree	0	0.0%
strongly disagree	0	0.0%
PG3 - The internship program changed my personal career goals. (33 responses)		
strongly agree	8	24.2%
agree	6	18.2%
neutral	11	33.3%
disagree	7	21.2%
strongly disagree	1	3.0%
PG4 - The internship program positively changed my interest in cybersecurity. (34 responses)		
strongly agree	9	26.5%
agree	8	23.5%
neutral	10	29.4%
disagree	4	11.8%
strongly disagree	3	8.8%
PG5 - I developed a habit of accomplishing tasks before the set target date. (33 responses)		
strongly agree	8	24.2%
agree	15	45.5%
neutral	5	15.2%
disagree	5	15.2%
strongly disagree	0	0.0%
PG6 - The internship program allowed me to apply concepts I learned in the classroom. (34 responses)		
strongly agree	9	26.5%
agree	17	50.0%
neutral	4	11.8%
disagree	4	11.8%
strongly disagree	0	0.0%

PG7 - The internship program changed my aspirations in some ways. (34 responses)		
strongly agree	11	32.4%
agree	11	32.4%
neutral	9	26.5%
disagree	3	8.8%
strongly disagree	0	0.0%

Table 8: Survey – Part VI: Personal Capabilities (PC)

Item	Frequency	Percentage
PC1 – open-ended question discussed later	n/a	n/a
PC2 - The internship program improved my conscientiousness and ethics. (34 responses)		
strongly agree	5	14.7%
agree	18	52.9%
neutral	11	32.4%
disagree	0	0.0%
strongly disagree	0	0.0%
PC3 - The internship program enhanced my respect for people different than myself. (34 responses)		
strongly agree	9	26.5%
agree	14	41.2%
neutral	10	29.4%
disagree	1	2.9%
strongly disagree	0	0.0%
PC4 - The internship program improved my ability to learn. (34 responses)		
strongly agree	10	29.4%
agree	19	55.9%
neutral	2	5.9%
disagree	3	8.8%
strongly disagree	0	0.0%
PC5 - The internship program improved my time-management skills. (34 responses)		
strongly agree	6	17.6%
agree	20	58.8%
neutral	6	17.6%
disagree	2	5.9%
strongly disagree	0	0.0%

PC6 - The internship program improved my social relationships. (34 responses)		
strongly agree	4	11.8%
agree	16	47.1%
neutral	13	38.2%
disagree	1	2.9%
strongly disagree	0	0.0%
PC7 - The internship program encouraged me to take the initiative. (34 responses)		
strongly agree	11	32.4%
agree	17	50.0%
neutral	6	17.6%
disagree	0	0.0%
strongly disagree	0	0.0%

Analysis and Summaries of Likert scale survey questions

The analysis of the Likert scale survey responses highlights several key trends and recurring themes. In terms of interest and career trajectory, the majority of respondents expressed a strong pre-existing interest in cybersecurity before starting the internship; 85.35 respondents marking - “Strongly agree” or “Agree”). This was evident from the frequent selection of "Strongly agree" when asked about their initial interest in the field. This was also true when it came to the impact of the internship on securing current jobs (47% respondents marking - “Strongly agree” or “Agree”) or future promotions (55.9% respondents marking - “Strongly agree” or “Agree”). While some participants felt the internship helped clarify their professional goals (70.6% respondents marking - “Strongly agree” or “Agree”), this did not necessarily translate into a direct impact on immediate employment (47% respondents marking - “Strongly agree” or “Agree”). However, participants did feel it had a positive effect on career advancement (55.9% respondents marking - “Strongly agree” or “Agree”).

In terms of skill development, the internship was generally viewed as beneficial across several areas. Many participants felt the experience enhanced their communication and interpersonal skills (85.3% respondents marking - “Strongly agree” or “Agree”), problem-solving (76% respondents marking - “Strongly agree” or “Agree”), and critical thinking (88.2% respondents marking - “Strongly agree” or “Agree”), while some participants weren’t convinced that the internship has a positive impact on their ability to work as part of a team (44.1% respondents marking - “Strongly agree” or “Agree”). The dominant sentiment in these areas was positive, with most respondents selecting "Agree” or “Strongly Agree”. However, when it came to practical skills specific to cybersecurity and technical analysis, the responses were more mixed. Some participants felt the program had room for improvement in providing direct technical training, as shown by a combination of "Neutral" and "Agree" responses in these categories.

The internship also contributed positively to participants' personal and professional growth. Respondents agreed that the program improved traits such as conscientiousness and ethics (67.6% respondents marking - “Strongly agree” or “Agree”), and respect for diversity (67.7% respondents marking - “Strongly agree” or “Agree”). Additionally, many felt that their time management (76.4% respondents marking - “Strongly agree” or “Agree”), decision-making (70.6% respondents marking - “Strongly agree” or “Agree”), and initiative (82.4% respondents

marking - “Strongly agree” or “Agree”) improved as a result of the internship. These areas were frequently identified as significant benefits of the program, contributing to their overall development.

Despite these advantages, some participants did not feel that the internship had an immediate effect on their employability. Responses regarding the impact of the program on gaining current job positions or promotions (35.3% respondents marking - “Neutral”) were often neutral, suggesting that while the internship was valuable for personal growth and skill development, it did not directly influence job acquisition for all participants in the short term. The internship program appears to have contributed significantly to the participants' professional and personal development, especially in areas related to communication, teamwork, and clarifying professional goals. However, the direct connection between the internship and immediate job placements or promotions remains less clear.

There is also a relationship between graduating from a high school in Hawai‘i and the current work location of respondents. The survey responses showed that the majority of internship graduates currently work in Hawai‘i (82.4%). Overall, 79.4% of internship graduates are currently employed, while 73.5% of internship participants graduated from Hawai‘i high schools, 64.7% currently work Hawai‘i. This suggests a strong tendency for graduates of Hawai‘i high schools to remain in the state for work after completing the UH NIWC Cybersecurity Internship.

Participant Open-ended Questions

The answers to these questions are recorded exactly as provided by participants.

Part II - 3,a - In a few sentences, please identify the internship program experiences that had the most impact on your current or future employment.

Table 9: Open-ended Questions – Part II - 3,a

#	Answer
1	My internship did not impact my current or future employment. I went into a different sector in relation to my degree.
2	mentorship and professional networking during the internship can offer long-lasting career guidance and open doors to future job
3	*no answer provided*

4	The most helpful parts of the NIWC internship was going over Network configuration diagram and discussing best practice and what was wrong with it. We also went over something like a security controls assessment.
5	The UH NWIC experience was a life changing event because it provided with ample opportunities to excel. I was able to get industry knowledge, and I was able to academia knowledge.
6	Great access to mentors, awesome deliverable, phenomenal exposure to material
7	Exposure to cybersecurity professionals and connecting directly to Adapt Forward LLC employees during presentations had a great impact. Hearing the stories of cybersecurity professionals helped piece together a possible roadmap from various perspectives.
8	I have a high interest in research within the academic field, the internship helped me refine research and writing skills that I can apply to any future job or field I want to go into.
9	Gained experiences to prepare for future employment, helps a lot when you have an internship experience compare to no experience
10	I remember learning a little bit about Python and R during my research at the internship. It has helped me in my current position.
11	*no answer provided*
12	Mentorship from expert instructors helped clarify the demands of the path forward as well as the culture.
13	Not sure if anything had a direct impact on my current employment, other than making my resume more attractive. However, I expect this to change as I pivot into a DoD role. In that role, I expect the introduction to STIGs and RMF to be useful. Learning to write a research paper will likely be useful for employment later on, but somewhat indirectly, as I probably won't be writing a literature review.
14	The fact that I interned with NWIC, which is a part of the U.S Navy, shows that I was a part of something in the government. The ability to do research and present it to the big folks at NWIC shows that I have the experience in doing all those things. Regardless of the result, it was a learning experience for me that can be applied in the cyber field.
15	The internship offered opportunities like working alongside with other aspiring cybersecurity professionals, alongside with experienced professionals-- building that web of network between each other. As for the program itself, I would say it definitely enhance my understanding of real-world applications when it comes to cybersecurity. I think that's something that I'm able to take and learn from for my future employment.
16	The internship program was centered around a cybersecurity research project that culminated in a written paper and a poster presentation. This experience has been useful as I have often mentioned my research project during internship interviews.
17	Learning about professionalism, completing a cyber security project, and having a mentor.
18	The final project that involved making a presentation.
19	The internship program experiences that had the most impact on my current or future employment were related to the poster board and paper research. Since I am now in the middle of my third year, I am more confident about my experience and capable in research for my capstone project, which may have an effect on future internships and employment.
20	I believe that going through the process of writing the research paper and presenting at a poster sessions had the most impact. It has made me become a more capable writer and more adept at explaining technical topics to a non technical audience.
21	Collaborating with people who worked in the cybersecurity field to learn more about what they do gave me valuable insights about the field that I didn't previously know. This program allowed me to network with several professionals in the field who informed me of how software engineering concepts are utilized in cybersecurity.
22	Presenting my poster at the ICS showcase along with doing the quick presentation in front of NIWC employers & Mazie Hirono/Ed Case had the most impact because it helped improve my public speaking/presenting skills. Also, being able to meet and network with various people from NIWC along with other interns was beneficial.

23	The internship helped me mostly financially. The internship's program did not really impacted my cybersecurity knowledge, skills, nor expertise. The internship's program enhanced my research and writing skills.
24	I was able to put the internship on my resume. Which added to my skills and training.
25	It definitely helped me with researching skills and understanding cyber security. My research paper included the security of the network of smart cars because of how much technology is inside modern cars.
26	Learning about the agencies hiring, talking to people that had jobs in the field, learning about requirements such as the Sec+ and the security clearance.
27	Other than academic style research practice, I'm not too sure how much of an impact it will have in the future.
28	I'd say that the topic of research I chose opened up new perspectives and may also peak interest from my colleagues and/or employers. It also served as a good addition to my resume and made me aware of that element within the cybersecurity field. In addition, being exposed to the experience of performing research is also something that I'm aware about as something to note for future employment.
29	The independent research nature and ability to choose your project had the most impact on my current employment. The flexibility of researching something that I wanted to go into and was interested in helped in the sense that this internship looked good on my resume (according to my current employer: I work IT @U.S. District Courts, District of Hawai‘i)
30	The internship program taught me a lot about Cybersecurity and what the work in this field is like. It prepared me for my current employment. In addition, I have a job at the Naval Information Warfare Center because I had a chance to apply for the position directly with the NIWC Pacific division head Eric. He came to visit us towards the end of the program.
31	Doing independent research
32	I had the chance to research a good amount about data analytics during the internship which directly relates to my current job.
33	Although I’m no longer pursuing a career I. Cybersecurity, this internship helped improve my critical thinking and research skills.
34	During my internships, the most impactful experiences for future employers were hands-on projects involving real-world threat detection and the network of people I met in the process.

Part III - 1 - In a few sentences, please identify the internship program experiences that had the most impact on your professional development.

Table 10: Open-ended Questions – Part III - 1

#	Answer
1	It made me aware of the opportunities in this field.
2	During cybersecurity internship, practical application of cybersecurity principles, like conducting vulnerability assessments and responding to threats, likely significantly enhanced your technical skills. Mentorship from seasoned cybersecurity professionals would have provided valuable insights into complex security issues and industry best practices, enriching your professional approach. Additionally, building a network with industry professionals could open up future career opportunities and keep you informed about emerging trends and demands in cybersecurity.
3	*no answer provided*
4	This internship pushed me out of my comfort zone. I'm terrible at networking (the meeting people kind), presentations and academic papers, this internship had me doing all three.
5	I was able to find work that deals with risk management and also getting an opportunity to see the other side of the business aspects.

6	The mentors were amazing. Having a research deliverable was helpful to provide material to employers. I also enjoyed having such a wide array of exposure to different cybersecurity concepts
7	I believe researching certification and employment paths, reviewing resources required for research, and condensing many hours of work down to 5-10 (shorter or longer) minute presentations was very impactful.
8	*no answer provided*
9	Lecture was really informative and helps me understand more about cybersecurity and get my Security + certification
10	Collaborating with experienced professionals helped me understand the industry better.
11	The internship made me better at research and allowed me to work with a team and also independently
12	Guidance from instructors and faculty on how to progress.
13	Introduction to STIGs and RMF had the most direct impact. Learning to write a research paper helped to an extent, but a literature review isn't how I plan to conduct research later on in my academic or professional career.
14	I think the research part had the most impact on my overall professional development. I never liked doing research as I'm more of a technical person and want to run command lines instead of writing papers. However, I learn a few new things that I didn't know about before as I was doing the research paper. I think this knowledge can come in handy in the future when I get to the point I write my own vulnerability researching papers, perhaps.
15	During my internship at NIWC, the most impactful experience were working with the homework assignments be it that they're the "cleaned" version because this hands-on involvement allowed me to gain some practical knowledge so that I have at least some sort of idea of what to expect in the actual work field. Before this internship, I had some classroom knowledge but no actual idea of the kind of work I would be dealing with.
16	This was my first experience with cybersecurity, and I benefited most from the opportunity to focus on a single research project for an extended period of time.
17	*no answer provided*
18	The final project.
19	Meeting to discuss high level policy details was new to me and something I've never experienced. This was great for consideration as an experience.
20	In terms of professional development, what sticks out most was the resume development and writing experience. The online course had many helpful tips for wording the experiences section.
21	Having weekly sit downs with my project supervisors allowed me to develop my time management and professionalism. These supervisors consistently made me improve my ability to get tasks done in a timely and efficient manner. Through the guidance of my supervisors, I was able to get through tasks that were completely new to me with ease.
22	This internship was my first exposure to cybersecurity and I believed the knowledge I gained from it will help with my professional development. The experience with the most impact is learning about public keys cryptography because I actually had to use this at work in order to send an encrypted file to another company. Therefore, it was useful to have that background knowledge.
23	Financial impact
24	Being able to get guidance from professionals that currently work I the field of cybersecurity.
25	Researching and being well educated with a lot of academic published articles regarding IT
26	The social networking was one of the most important aspects for me. From the Internship I learned about a fellow group of students that was forming a student club for computing, and a group of students participating in the National Cyber League. Both these opportunities in turn opened other doors and got me more experience.
27	*no answer provided*
28	This internship helped me to develop my research skills. Despite not being a fan of research work though as I find it intense, I learned methods of being able to perform the task should it be needed in the future (especially graduate school).

29	The experience as a whole being a quantitative research experience helped my development within the field because I learned from experts in an area that was outside of the realm of college education and within practical research and experience.
30	The fundamental knowledge of the CIA triad. The risk management framework, security technical implementation guide, and the research skills on prevalent Cybersecurity breaches. There are more but the experience was beneficial for any Cybersecurity enthusiast.
31	*no answer provided*
32	Working with others in a professional setting helped me improve my communication skills, etc.
33	*no answer provided*
34	During my internships, the most impactful experiences were hands-on projects involving real-world threat detection and response.

Part IV - 1 - In a few sentences, please identify the internship program experiences that had the most impact on your professional skills.

Table 11: Open-ended Questions – Part IV -1

#	Answer
1	No impact
2	During cybersecurity internship, Professor Stevens provided the hands-on experience of implementing security measures and tackling real-time cybersecurity threats would have significantly developed your technical and analytical skills. Also, Regular interactions and feedback from seasoned professionals in the field would have enriched your problem-solving abilities and understanding of industry standards.
3	Learned about how to present my poster.
4	This was the starting point to me developing the comprehension skill to read complicated peer reviewed journals about CyberSec. I now do that constantly for work, not journals, per se, but CyberSec related articles.
5	The overall program itself provided me with a working knowledge of what to expect and what is needed to be successful in the cybersecurity field.
6	Having access to knowledgeable mentors and sme's was an interesting and helpful experience. The opportunity to present helped with presentation presence and interpersonal communication skills used in interviews.
7	The construction of the research paper, seeking out credible, recent and academic sources, interacting with professionals and career-path likeminded peers were the most impactful.
8	Writing and critical thinking. For the internship program we were tasked to write about a current cybersecurity problem and do research on it. This experience helped me chose a topic I was unfamiliar about but interested in.
9	The lecture and research paper helped me understand more about cybersecurity and improved my research and writing skills
10	I learned to apply my knowledge to practical situations and developed problem-solving abilities.
11	Research skills were the most impacted and were definitely improved
12	I learned cybersecurity is every person's responsibility and the path forward is forged by individual desire to pursue the subject matter versus chasing monetary compensation. The drive it takes to keep up in Cyber must be fueled by real passion, or the practitioner becomes a constraint to the mission.

13	In terms of hard, technical skills, I did not gain much from this internship. Learning to overcome my weakness of academic writing was very beneficial however.
14	I was never good at writing research papers. So the ability to write a decent research paper has improved my writing skills overall, which is important especially in the field of cybersecurity where we need to have a good writing skill to communicate with our clients. The internship program has given me a chance to improve my writing skills, and it did.
15	Not so much about professional skills yet as the internship was more focused on research versus technical, and I'm not currently working in cybersecurity and at the time of internship. But as I mentioned before, I have all those knowledge that I'm glad I could take to my future employment.
16	This was my first experience with reading cybersecurity research articles and my first time solving variational physics problems with gradient descent, professional skills I will treasure and practice throughout my career.
17	*no answer provided*
18	The final presentation.
19	Doing the research paper and poster board had the most impact on my professional skills.
20	Same point on the writing and explaining information to non technical audiences.
21	In the internship we developed our communication and collaboration skills with each other through group discussions and feedback sessions. At the end of the internship we presented our final project and provided feedback to each other, this experience developed my public speaking and communication skills. The program also required each of us to develop decision making when creating our final presentation board and speech that properly portrayed what we worked on for the semester in a concise manner.
22	Having to present our research findings at the end of the internship helped improve my professional skills. Having to do a lot of research on our topic of choice and being able to condense that down into a paper & present the information in a poster.
23	The internship's program enhanced my research and writing skills.
24	*no answer provided*
25	Presenting my research to class helped me get better at public speaking at work
26	The research, paper writing and presentation to NIWC drove home the point that soft skills were very important in the field. Not only would I need to know the technical side, but being able to talk and write about it eloquently or in layman's terms would help further my career.
27	Academic researching
28	The experience of performing research is something
29	My ability to research and the confidence to dive into a research paper that I may not fully understand was definitely developed during this internship. Albeit, I don't currently use this skill that much in my job other than on the programming side when I'm writing applications for the court, but the overall research experience helped me as a whole.
30	I think the research and public speaking skills. These skills are vital in preparation for the new employment and future professional development.
31	*no answer provided*
32	Communication skills in a workplace setting helped me.
33	The internship helped me transition into a growth and professional mindset.
34	During my internships, the most impactful experiences on professional skills were hands-on projects involving real-world threats and networking with a team of people who varied in qualifications.

Part V - 1 - In a few sentences, please identify the internship program experiences that had the most impact on personal growth.

Table 12: Open-ended Questions – Part V - 1

#	Answer
1	No impact
2	The Cybersecurity Internship has fostered my personal growth through intensive technical skills development. Dealing with complex cybersecurity tools and techniques to manage real-time threats and vulnerabilities will enhance your technical proficiency and problem-solving abilities. Additionally, conducting rigorous debugging and security audits under the guidance of experts such as Stevens professors is likely to improve your attention to detail and ability to work under pressure, which are critical skills in any technology-driven environment.
3	*no answer provided*
4	NIWC was the hardest thing I've had to do in my career. Finding and organizing relevant information from research papers and writing about a topic that I knew very little about was extremely hard. For comparison, I took a CISSP at UHWO that was very difficult, but the NIWC internship was way more difficult.
5	The internship program gave a boost of confidence to continue on with my academic and IT journey.
6	Mentor access, subject exposure
7	The individual nature of my research paper and presentation was a great challenge in a field I have only classroom experience in - so meeting this challenge was a wonderful experience. Excelling in some areas allowed me to assist peers with their own challenges.
8	*no answer provided*
9	By having experiences with an internship job, I become more confident while seeking a job and asking questions.
10	Just interacting with professionals gave me a sense of what being in a real workplace is like.
11	*no answer provided*
12	The depth of content encouraged in the research project identified the program as just the entry point to a vast world of learning ahead. The perspective that a major global great power competition in the Cyber domain was well underway. the program also reminded my that the Oath I took as a prior service veteran years ago was a promise and commitment for life to the U.S.A.
13	I fell behind early on in the internship, since I have a weakness with academic writing. Fortunately, I was allowed to come up with my own plan to tackle the overarching assignment, which gave me some confidence in creating an unorthodox plan and executing it to success.
14	I feel that the internship program experience allowed me to grow as a person. I have never had a contract with the government before, never presented in front of a group of real government-working people, so being able to do all of those things allowed me to grow as a person. It also helps with my ability to present in front of other people and my presentation skills.
15	As for personal growth, I was glad I was able to take part in this internship, particularly through the challenging research and presentation phase that pushed me out of my comfort zone because of the interaction in a professional environment with experienced professionals.
16	In the beginning of the internship, I was exploring several cybersecurity research ideas simultaneously in an effort to determine which was most fruitful. I experienced the most personal growth when I decided to abandon this approach and prematurely choose one research idea to focus on with my full attention.
17	*no answer provided*
18	The final presentation and being helped on it by the organizers.
19	Working around other students that were more advanced in their academic journey was inspiring and insightful.
20	I learned a lot from going through the process of researching the topic for the literature review. It also helped narrow down my potential topic of interest within cybersecurity which is really nice given how vast the field is.

21	The program developed my ability to be disciplined in my work and by taking responsibility over every aspect of my project. While I worked closely with my mentors, I had grown more comfortable with asking for help and advice when needed.
22	Because I was doing NIWC along with working and taking other classes, this internship forced me to improved my time management skills in order to meet the internal deadlines.
23	The internship's program enhanced my research and writing skills.
24	*no answer provided*
25	Working with the other interns helped me become a better team member professionally
26	With this internship I was able to jumpstart my career in Networking/Cybersecurity. I've often heard that the hardest part of breaking into the field is getting your first "experience" to put on your resume. After adding this internship to my resume, I was able to fully transition to computing and have been working in the field full time since.
27	Unsure
28	I'd say that the experience of taking on graduate-level work involving research papers as someone who recently graduated from high school was a major challenge. This experience made me more aware about what I'm able to manage and to be more cautious of what I put on my plate.
29	Personally, I realized that while going into this internship I had an interest in Cybersecurity, it wasn't as deep an interest I thought. It was more so wanting to feel secure about different aspects of computer science that I had an interest in such as artificial intelligence and software development.
30	I expanded my knowledge of Cybersecurity and improved my soft skills.
31	*no answer provided*
32	This internship helped me realize what aspects of IT that I was interested in. I had the chance to sort of feel out what I liked and disliked.
33	*no answer provided*
34	During my internships, the most impactful experiences on personal growth were the opportunities to work in a team setting and with industry professionals.

Analysis and Summaries of Open-ended Questions

The open-ended responses from participants of the survey provide insights into how the program impacted their future employment, professional development, professional skills, personal growth, and personal capabilities.

I first analyzed these answers using Luk and Chan's (2022) framework, which focuses on knowledge, academic-related generic competencies, non-technical generic competencies, and technical competencies. I identified the following common themes and areas for improvement.

The first open-ended question I analyzed was from PII-3,a.

Question: "In a few sentences, please identify the internship program experiences that had the most impact on your current or future employment."

Participants widely appreciated the mentorship and exposure to cybersecurity professionals, but there is room to enhance technical skill-building and ensure alignment with participants' career trajectories.

Common Themes

Many participants noted that the internship significantly helped in developing their research and writing abilities, which are essential academic competencies. The focus on cybersecurity-related projects, configuring networks, and hands-on tasks such as threat detection were often mentioned as critical elements of their learning experience. Several participants specifically highlighted learning to write research papers, participating in poster presentations, and exploring various cybersecurity topics as skills that they felt would benefit their future careers.

In addition to technical skills, many participants found that the internship improved their non-technical abilities. Adaptability, public speaking, and professionalism were frequently cited as valuable outcomes. Participants mentioned that presenting their work enhanced their communication skills, especially when explaining complex technical concepts to non-technical audiences. These improvements in non-technical skills, such as adaptability and public speaking, left participants feeling more confident and prepared for professional environments.
Although some participants mentioned gaining technical skills during the internship—such as learning programming languages like Python and R, or understanding encryption—there was less

focus on these areas compared to research skills. A few respondents noted exposure to cybersecurity concepts and tools, such as Security Technical Implementation Guides (STIGs) and the Risk Management Framework (RMF). However, some participants felt they did not experience significant technical growth in other areas like IT, encryption, or networking.

Professional networking and mentorship emerged as some of the most impactful aspects of the program. Participants frequently described the value of building connections with professionals in the cybersecurity field, engaging with mentors, and learning about potential career paths. These relationships gave participants a deeper understanding of the industry and made a lasting impression that they felt would benefit them in future employment opportunities.

Areas for Improvement

Some participants expressed concerns about the alignment of the internship with their career paths, especially if they transitioned to fields outside of cybersecurity. A few respondents indicated that the skills and knowledge gained might become more relevant if they moved into roles with the Department of Defense or similar sectors. This suggests a gap between the program's focus and the immediate career needs of participants who did not remain in cybersecurity.

Another area for improvement noted by participants was the level of hands-on technical experience offered during the internship. While some appreciated the exposure to real-world cybersecurity tools and threat detection techniques, others felt that the internship lacked deeper technical training. This feedback indicates that the program could benefit from offering more technical projects or certifications, such as Security+, to help participants develop skills more aligned with cybersecurity roles.

Another key theme that emerged from the feedback was the internship's varied impact on participants. Participants who did not pursue careers in cybersecurity or related fields found the internship to be less impactful overall. Although they acknowledged gains in research and critical thinking, the program may benefit from offering clearer pathways or greater flexibility for those who choose non-cybersecurity career paths.

The second open-ended question I analyzed was from PIII-1.

Question: "In a few sentences, please identify the internship program experiences that had the most impact on your professional development."

Participants reported that the NIWC Cybersecurity Internship effectively developed their research, communication, and foundational cybersecurity knowledge. However, enhancing the program's technical focus and career alignment could further benefit participants, particularly those pursuing specific roles in the cybersecurity industry.

Central Tendencies and Common Themes

Many participants reported that the internship provided valuable learning experiences in cybersecurity concepts and threat analysis. Engaging in hands-on projects such as real-world threat detection, public key cryptography, and vulnerability assessments allowed them to apply theoretical knowledge to actual problems. These practical exercises were instrumental in helping them understand key cybersecurity principles. Additionally, learning from experienced professionals gave participants deeper insights into industry best practices and threats, enhancing their overall understanding of the field.

A large number of participants also highlighted the significance of the research and academic tasks they undertook during the internship. Writing research papers, conducting literature reviews, and presenting findings were skills that many participants developed over the course of the program. While some initially felt hesitant about the academic research component, they later recognized its importance in improving their ability to conduct thorough research and synthesize complex information. These skills, gained through the internship, proved valuable in both academic and professional settings.

The internship also helped participants develop important non-technical skills, particularly in the areas of communication, adaptability, and time management. Participants noted how the program gave them experience in public speaking and presenting technical content to non-technical audiences. Additionally, the structured mentorship they received helped them develop time management skills and a sense of professionalism, allowing them to better manage their tasks and responsibilities within a workplace setting. Networking with industry professionals further enriched their professional growth, giving them exposure to broader industry dynamics.

Although participants mentioned developing technical skills during the internship, there was less focus on this aspect compared to other outcomes. Some participants learned encryption techniques, networking fundamentals, and IT security frameworks like the CIA triad and Security Technical Implementation Guides (STIGs). However, several participants felt that the program could have offered more in-depth technical training or certifications, which would have enhanced their preparedness for roles in cybersecurity.

Areas for Improvement

One key area identified for improvement was technical skill development. While some participants did gain technical competencies, many expressed the need for more hands-on technical training and opportunities for certification, such as the Security+ certification. Expanding the focus on technical skills related to encryption, networking, and IT security could increase participants' readiness for cybersecurity careers.

Another area of concern was the alignment between the internship and participants' long-term career goals. Some participants felt that the internship's impact on their professional development was limited, especially if they were not pursuing careers in cybersecurity. Offering more tailored experiences or flexible pathways within the program would help ensure that it benefits participants with diverse career goals, including those in related fields like IT or risk management.

Finally, participants expressed a desire for more real-world applications of cybersecurity principles. While research and academic skills were highly valued, there was a clear interest in expanding opportunities for practical projects. This could include more hands-on activities such as simulations in threat detection and incident response, which would make the program more relevant for those seeking careers in technical areas of cybersecurity.

The third open-ended question I analyzed was from PIV–1.

Question: "In a few sentences, please identify the internship program experiences that had the most impact on your professional skills."

Participants reported that the NIWC Cybersecurity Internship provided them with valuable research, communication, and knowledge-building experiences. However, there is room

to improve the focus on technical competencies and practical applications to better meet the needs of those pursuing careers in cybersecurity.

Common Themes

Several participants emphasized the value of hands-on projects involving real-world cybersecurity threats, which played a significant role in developing their professional skills. These experiences allowed them to apply theoretical knowledge to practical situations, such as threat detection and response, helping address the disparity between academic learning and real-world application. Through their interactions with industry professionals and subject matter experts, participants gained deeper insights into industry best practices and cybersecurity standards, further enhancing their understanding of the field.

The internship also had a strong impact on participants' research and writing abilities, which were critical areas of growth. Many participants noted that writing research papers and conducting literature reviews improved their critical thinking and academic research skills. The opportunity to present research findings through written reports and poster presentations helped them refine their ability to communicate complex information effectively to both technical and non-technical audiences. This aspect of the program was widely recognized as an important contributor to their overall academic and professional development.

In addition to technical knowledge, the internship fostered the development of non-technical skills, such as communication, adaptability, and collaboration. Participants frequently mentioned that group discussions, presentations, and feedback sessions improved their public speaking abilities and enhanced their capacity to work effectively in teams. The chance to present research to diverse audiences, including non-technical stakeholders, proved particularly valuable in sharpening their communication and presentation skills. These experiences contributed to their preparedness for professional work environments where collaboration and clear communication are essential.

Although technical skill development was mentioned less frequently, some participants did acknowledge that the internship provided opportunities to apply theoretical knowledge to practical problems. Writing code, learning about cybersecurity frameworks, and dealing with real-world cybersecurity incidents were some of the experiences mentioned. However, several participants felt that the internship’s focus on research limited the time spent on building

technical skills. Some expressed a desire for more hands-on experience with areas like encryption and networking, feeling that these practical competencies were not as thoroughly addressed.

Areas for Improvement

One area identified for improvement was the need for a stronger focus on technical skill development. Several participants felt that the internship placed more emphasis on academic research and writing, leaving them with limited opportunities to work directly with cybersecurity tools, frameworks, or real-world scenarios. Increasing hands-on experiences related to technical aspects of cybersecurity would better prepare participants for technical roles in the industry and provide more balanced learning opportunities.

Another area where participants saw room for growth was in balancing research with practical application. While research skills were a valuable part of the internship, some participants expressed a desire for more opportunities to apply their cybersecurity knowledge to real-world problem-solving. Strengthening this balance between research and practical application would enhance the learning experience for those more inclined toward technical roles and problem-solving tasks.

Finally, some participants who did not pursue careers in cybersecurity or were uncertain about their career paths felt the internship had limited relevance to their professional development. Providing more flexibility within the program, such as offering tailored experiences that align with different career goals, could improve outcomes for participants with diverse professional aspirations. By addressing this need for customization, the program could cater more effectively to a wider range of career trajectories.

The fourth open-ended question I analyzed was from PV–1.

Question: "In a few sentences, please identify the internship program experiences that had the most impact on personal growth."

Participants reported that the NIWC Cybersecurity Internship contributed significantly to their personal growth by enhancing their research, communication, and time management skills.

However, more hands-on technical experience and clearer career guidance could further improve the program's impact on their personal and professional development.

Central Tendencies and Common Themes

Several participants noted that the internship provided valuable exposure to the cybersecurity field, helping them gain a deeper understanding of the subject. Through hands-on experience with cybersecurity tools, engaging in research, and interacting with industry professionals, participants were able to see how cybersecurity principles are applied in real-world settings. For some, this experience helped them focus on specific areas of interest within the broader field, giving clarity to their professional goals.

Many participants found the research component of the internship to be particularly impactful. Writing research papers and conducting literature reviews, often on unfamiliar topics, challenged them to think critically and organize information from complex sources. These tasks helped them improve not only their research and writing skills but also their overall academic confidence. Several participants reflected on how these experiences pushed them out of their comfort zones and contributed to personal and professional growth.

The development of non-technical skills, such as time management and communication, was another common theme. Participants often had to balance multiple responsibilities, including research projects, presentations, and sometimes academic work or other jobs. Many commented that this experience helped them improve their ability to meet deadlines and communicate effectively with peers, mentors, and professional audiences. The opportunity to present their research also improved their public speaking skills, boosting their confidence when addressing professional groups.

Although technical skills were mentioned less frequently, some participants indicated that they developed these abilities through hands-on tasks, such as debugging, conducting security audits, and working with cybersecurity tools. For others, the technical aspect of the internship was more about exploration, allowing them to gain exposure to different areas of IT and cybersecurity. This exploration helped participants identify which fields they were most interested in pursuing.

Areas for Improvement

Some participants felt that while the research aspect of the internship was valuable, there could be more emphasis on practical, hands-on technical work. They expressed a desire for more direct engagement with cybersecurity tools and real-world scenarios, suggesting that a better balance between academic research and practical application could enhance the overall learning experience.

A few participants noted that the internship helped them realize their interests lay outside cybersecurity, within other areas of IT. Offering more opportunities for career exploration or mentorship focused on various cybersecurity and IT pathways could help participants gain a clearer sense of direction earlier in the program. This would allow them to make more informed decisions about their career trajectories.

Lastly, some participants mentioned the positive impact of working in teams, but also suggested that this aspect could be expanded. They felt that more structured opportunities for collaboration and peer-to-peer learning would help simulate real-world work environments. Encouraging teamwork and professional collaboration within the internship would allow participants to develop important skills needed for success in cybersecurity roles, where team dynamics are often crucial.

The fifth open-ended question I analyzed was from PVI–1.

Question: "In a few sentences, please identify the internship program experiences that had the most impact on personal capabilities."

The participants reported that the NIWC Cybersecurity Internship provided valuable opportunities for personal growth in research, communication, and technical problem-solving. The program could be strengthened by offering more hands-on technical training and expanding collaborative experiences to support participants' personal and professional development.

Common Themes

Many participants highlighted how the internship significantly contributed to their development of technical skills and understanding of cybersecurity concepts. Engaging in hands-on activities, such as managing cybersecurity threats and performing audits, allowed them to

enhance their problem-solving abilities and critical thinking. Working alongside experienced professionals offered valuable insights into real-world cybersecurity practices, increasing their competence in areas like encryption, incident response, and research. These experiences deepened their technical proficiency and gave them a solid foundation in cybersecurity tools and techniques.

The research and writing component of the internship was another area where participants saw substantial growth. They frequently mentioned how navigating complex topics, writing detailed literature reviews, and producing high-quality research reports helped refine their academic abilities. The challenges of organizing information from various sources and effectively presenting their findings allowed them to improve their skills in synthesizing information and communicating it clearly. Many participants reported feeling more confident in their academic and professional abilities after successfully completing these research tasks. Non-technical skills, such as time management and communication, were also widely developed during the internship. Many participants explained how juggling the program's demands, such as meeting deadlines, conducting independent research, and preparing presentations, strengthened their time management skills and their ability to work under pressure. Communication skills also improved, particularly in presenting complex cybersecurity topics to peers, mentors, and industry professionals. These experiences boosted their confidence in public speaking and teamwork, essential skills for both academic and professional settings.

While direct technical skill development was less frequently mentioned, some participants did acknowledge gains in areas like working with cybersecurity tools and software. However, many responses focused on the personal growth achieved through teamwork and collaboration. Participants valued the opportunity to work within professional teams, interact with mentors, and receive constructive feedback. For some, the internship marked their first experience in a professional setting, which helped build their self-confidence and sharpen their technical and interpersonal skills.

Areas for Improvement

Although research skills were a major focus of the internship, some participants felt there could be more opportunities for direct technical training. They suggested that incorporating more

hands-on experience with cybersecurity tools and real-world applications would complement the research-heavy structure and help further develop their technical abilities.

Balancing the workload was another challenge mentioned by several participants. They reported difficulty managing the various tasks and tight deadlines associated with the internship. Providing more guidance on time management and organizational strategies could help participants handle the workload more effectively and develop stronger skills in these areas. Finally, while many participants appreciated the teamwork and collaborative opportunities provided by the internship, some felt that these aspects could be further expanded. They recommended incorporating more structured, team-based projects or practical simulations to enhance their ability to apply both technical and non-technical skills in real-world cybersecurity situations. This would help participants gain a deeper understanding of collaborative problem-solving in professional cybersecurity environments.

When I analyzed the open-ended responses, several key aspects of Bandura's Social Learning Theory emerged as central themes. These themes relate to the participants' learning experiences, particularly in relation to the theory's four components: attention, retention, reproduction, and motivation.

Attention: Learning through Observation and Interaction with Experts

A key theme across participants' responses was the value of observing and interacting with experienced professionals. Many participants noted that working alongside seasoned cybersecurity experts, such as mentors and instructors, provided them with a model for how to approach real-world cybersecurity problems. This aligns with Bandura's assertion that individuals learn by paying attention to the behaviors of others. Participants frequently mentioned the impact of observing professional practices during hands-on tasks, cybersecurity audits, and real-world threat management. By focusing on these role models, they developed their own approaches to problem-solving and gained insights into industry standards.

Retention: Reinforcing Knowledge through Research and Practice

Several responses highlighted the importance of retaining new information through research projects, presentations, and hands-on experiences. Social Learning Theory suggests that after observing a behavior, individuals must retain the knowledge to apply it in future scenarios.

In the NIWC internship, participants were frequently tasked with conducting research on complex topics, writing literature reviews, and presenting their findings. This process helped reinforce cybersecurity concepts and technical knowledge. The repeated exposure to cybersecurity tools and techniques through independent research and presentations allowed participants to retain and internalize the skills they were developing.

Reproduction: Applying Learned Skills in New Situations

Reproduction, or the ability to reproduce observed behaviors, was another prominent theme in the internship experience. Participants mentioned applying the skills they learned during the internship to real-world scenarios, such as job interviews, capstone projects, and even in their current roles. The act of conducting research, presenting findings, and engaging in professional discussions helped them practice and refine these skills. For example, many participants found that public speaking and communication were critical components of the internship, and they used these opportunities to practice and improve their presentation skills. This process of reproduction directly mirrors Bandura's idea that individuals must practice observed behaviors to master them.

Motivation: Gaining Confidence and Personal Growth through Positive Reinforcement

The final component of Bandura's theory is motivation, which drives individuals to continue learning and applying new behaviors. Across the responses, participants frequently expressed how their confidence grew as they completed challenging tasks and received feedback from mentors and peers. This aligns with Bandura's concept of reinforcement, where positive outcomes encourage the continued practice of learned behaviors. Several participants noted that the successful completion of their research projects, presentations, and interactions with professionals boosted their self-efficacy. The sense of accomplishment gained from overcoming challenges in the internship, such as difficult research tasks or tight deadlines, served as motivation to further pursue their cybersecurity goals.

Peer Learning and Collaborative Growth

An additional theme related to Bandura's Social Learning Theory is the role of peer learning. Many participants mentioned that working alongside fellow interns helped them gain

new perspectives and provided opportunities to share knowledge. This peer interaction allowed participants to observe how others approached problems, giving them alternative strategies to apply in their own work. Collaborating with peers during group discussions, feedback sessions, and presentations mirrors Bandura's idea that social environments are crucial for learning, as individuals constantly observe and model behaviors from those around them.

In summary, Bandura's Social Learning Theory is reflected in several aspects of the NIWC Cybersecurity Internship experience. Participants learned by observing professionals and peers, retaining knowledge through research and practice, reproducing behaviors in new contexts, and gaining motivation through positive reinforcement and personal growth. The internship provided a rich social environment for learning, where participants could model behaviors, practice new skills, and gain the confidence needed to apply their knowledge in real-world situations. This combination of observation, interaction, and reinforcement contributed to the participants' overall development, both personally and professionally.

Participant Follow-up Interviews

Analysis and Summaries of Follow-up Interviews

Follow-up interviews were conducted with three participants in order to gain a more comprehensive look at participants' experiences in the internship. These follow-up interviews with selected participants from the UH NIWC cybersecurity internship offer a deeper understanding of the program's effectiveness and impact on participants. They provide a comprehensive look at participants' experiences in the internship, offering valuable insights into how the program could evolve to better meet the needs of future participants.

Participant 1

The participant shared their post-internship experiences, including challenges faced, the role of the internship in securing job offers, and the ultimate decision to pursue a different career path. Several key themes and narratives emerged that provide a deeper understanding of the strengths and areas for growth within the NIWC cybersecurity internship.

Key Themes and Insights

One major theme that emerged from the participant's experience was the absence of industry certifications, such as the Certified Information Systems Security Professional (CISSP). These certifications are essential in the cybersecurity sector and often serve as prerequisites for many positions. The participant believed that having these certifications would have improved their qualifications and made them more attractive to potential employers. While the internship provided solid technical knowledge, incorporating training focused on obtaining industry-recognized certifications could better prepare participants for the competitive job market.

In terms of post-internship employment, the participant was offered a cybersecurity analyst role with a company affiliated with NIWC. However, they ultimately chose a software engineering position because it offered better compensation and greater flexibility during negotiations. This decision was not a reflection of disinterest in cybersecurity but was instead influenced by the financial benefits, which included a higher salary and relocation support. This highlights the significant role that economic factors, such as pay and benefits, play in career decisions. Offering more competitive compensation packages within the cybersecurity field could help retain talent that is well-prepared for these roles.

The participant also highlighted the distinction between the technical training and the research component of the internship. While the technical skills gained were highly relevant to the job market and provided useful material for interviews, the research experience, although valuable, had less immediate relevance to job opportunities. The technical lessons focused on core cybersecurity concepts, while the research project served more as a portfolio piece. This suggests that placing more emphasis on practical, hands-on training, rather than theoretical research, might better align the program with the needs of the industry. The research component could be adjusted to include more projects that reflect real-world cybersecurity challenges.

Mentorship was another aspect of the internship that the participant appreciated, particularly the guidance from Dr. Adamove and Dr. Arnold. Both were described as approachable and highly knowledgeable, providing a solid support system throughout the program. However, the participant expressed a need for more structured guidance around industry certifications and career pathways in cybersecurity, which could have better prepared them for the job market after the internship. Strengthening the career advising component of the program could further enhance its value to participants.

Despite being well-equipped for a career in cybersecurity, the participant ultimately chose a software engineering role due to the financial advantages it offered. The software engineering position came with a significantly higher salary and relocation benefits, making it a more appealing option. The participant indicated they would have been equally satisfied with a cybersecurity role from a technical and intellectual standpoint, but the economic factors swayed their decision. This demonstrates the importance of competitive compensation in retaining talent, even when they are well-prepared for roles in cybersecurity.

The participant also encountered difficulties with the application process for a position at NIWC through USAJobs.gov. They found the platform confusing and difficult to navigate, which ultimately led to an incomplete application. Simplifying this application process or providing clearer instructions would likely improve the experience for internship participants applying for government cybersecurity roles.

Overall, the participant had a very positive view of the internship, even though they chose a different career path. They valued the industry exposure, mentorship, and unique opportunities the program offered, such as presenting to prominent figures like Senator Mazie Hirono and Representative Ed Case. The participant expressed interest in repeating the internship if possible, emphasizing the program's educational and professional benefits. This feedback highlights the success of the internship in providing real-world experience and development opportunities while pointing to potential improvements, such as better certification guidance and streamlined application processes.

Themes and Narratives Exploration

The participant's narrative reveals several critical insights into the internship's strengths and areas for growth. Key elements that stand out include the practical technical training provided, the value of mentorship, and the economic factors influencing post-internship career decisions. While the internship prepared the participant well for cybersecurity roles, challenges related to certification gaps, competitive compensation, and confusing application processes hindered their ability to fully capitalize on the experience.

This interview also highlights the importance of mentorship and real-world exposure. The participant frequently emphasized the knowledge and support of their mentors, who played a

crucial role in their learning experience. Additionally, opportunities to interact with industry professionals and present to influential figures enhanced the overall value of the internship. At the same time, the participant's decision to pursue a career in software engineering—largely driven by higher pay—points to a broader issue of compensation competitiveness within the cybersecurity field. While the participant expressed an equal interest in both cybersecurity and software engineering, the financial incentives in the latter field ultimately guided their career choice.

Conclusion

Overall, the participants' feedback suggests that the internship offers a strong foundation in technical skills and professional development, but additional enhancements could make it even more effective in helping students transition into cybersecurity careers. By addressing these challenges, the program could further strengthen its role in preparing a pipeline of skilled professionals for the cybersecurity workforce.

Participant 2

This follow-up interview highlights the program's success in building confidence and exposing students to new career paths, while also revealing areas where additional support is needed. The interview touches on the importance of industry certifications, practical hands-on learning, and clear communication about job application processes.

Key Themes and Insights

One of the major challenges the participant identified was the difficulty of securing cybersecurity positions due to the lack of industry certifications and experience. Like Participant 1, this individual found that many job postings required certifications such as Security+ and several years of experience. Although the internship boosted their confidence in applying for roles, they quickly realized they were not competitive without these qualifications. The participant suggested that structured support for obtaining these certifications could greatly improve the employability of those completing the internship. Offering certification preparation

or guidance on how to secure these essential qualifications could significantly enhance the value of the program.

A recurring theme in the participant's feedback was the importance of practical, hands-on experience. They appreciated the real-world exposure they gained through their part-time job, such as working with firewalls and servers. These tasks helped reinforce the concepts learned during the internship. However, the participant expressed a desire for more hands-on opportunities within the internship itself. They felt that live demonstrations or simulations during the program would have deepened their understanding of cybersecurity applications. This suggests that while the internship introduced important concepts, there is room to incorporate more interactive, real-world training that could better prepare participants for the demands of the cybersecurity industry.

Mentorship played a significant role in the participant's positive experience. The internship gave them the confidence to consider a career in cybersecurity, a field they had not previously considered. Initially, they saw themselves as a programmer due to their academic background, but through the internship and the support of their professor, they discovered new opportunities. The mentorship helped them build confidence and provided critical mental support during their career transition. This highlights the importance of mentorship not just for technical development but for building self-confidence and encouraging career exploration.

The participant also faced challenges in applying for cybersecurity roles, particularly with government organizations like NIWC. Although interested in these positions, they were unfamiliar with the process of using the USAJobs.gov platform and felt hesitant about contacting NIWC staff for guidance. This lack of clarity about the application process discouraged them from pursuing opportunities with NIWC. The participant's experience underscores the need for clearer instructions and more proactive guidance from the program on navigating government job applications, which could make the transition from internship to full-time employment smoother.

In terms of career decisions, the participant entered the program with an interest in programming, influenced by their coursework at UH Mānoa. However, the internship opened their eyes to the broader possibilities within the cybersecurity field, leading them to pursue further education and certifications in that area. The hands-on experience they gained through both the internship and their part-time job reinforced their decision to shift their career focus

toward cybersecurity. This shift highlights the value of offering diverse experiences within internships, allowing students to explore different fields and career paths that may not have been part of their original plan.

The academic portion of the internship also played an important role in helping the participant transition into the workforce. They credited the program with improving their resume writing and teaching them how to present themselves professionally in interviews. These skills were instrumental in helping them secure and succeed in their current part-time job. This suggests that professional development, particularly in communication and presentation skills, is just as critical as technical training in preparing students for success in the job market.

Themes and Narratives Exploration

The participant's experience aligns closely with that of Participant 1, particularly regarding the barriers to entering the cybersecurity field. Industry certifications and work experience remain significant obstacles for new graduates. This indicates that even though the internship provides a solid foundation in cybersecurity, more support is needed to help participants obtain the certifications that are often required for entry-level roles.

Another key theme is the role of mentorship in helping students build confidence and navigate career transitions. The participant's transformation from a programmer to a cybersecurity professional illustrates how essential mentorship is in guiding students through periods of self-doubt. This highlights the need for not only technical training but also personal encouragement and career guidance to support students as they explore new fields.

The participant's desire for more hands-on learning also reflects a broader trend in technical education. Many students crave practical experience that allows them to apply what they have learned in real-world settings. The internship could benefit from incorporating more interactive experiences, such as simulations or on-the-job training, to help participants gain a deeper understanding of cybersecurity in practice.

The challenges the participant faced in applying for roles at NIWC further reveal a communication gap that could be addressed by the program. Clearer guidance on navigating government job applications and more direct support from internship organizers could help bridge this gap, encouraging more participants to apply for these opportunities.

Finally, the participant's shift in career focus from programming to cybersecurity demonstrates the value of internships in expanding students' understanding of their career options. The internship exposed them to new areas within computer science that they had not previously considered, ultimately leading them to pursue a different career path. This underscores the importance of offering diverse experiences within internships to allow students to explore fields they may not have encountered in their academic coursework.

Conclusion

The participant's experience mirrors many aspects of the feedback from Participant 1, particularly in terms of the barriers to entering cybersecurity and the critical role of mentorship in shaping career decisions. While the internship played an instrumental role in guiding the participant toward a cybersecurity career, there is a clear need for more structured support in obtaining industry certifications, navigating job applications, and gaining hands-on experience. Addressing these areas would further enhance the program's impact and help participants successfully transition into cybersecurity roles.

Participant 3

The follow-up interview with this participant offers an in-depth look into their experiences post-internship with the University of Hawai‘i (UH) Naval Information Warfare Center (NIWC) cybersecurity internship. The participant shares several challenges and insights related to their pursuit of a career in cybersecurity, emphasizing a passion for the field despite facing notable barriers.

Key Themes and Insights

The participant identified several barriers to entering the cybersecurity field, including ageism, the need for prior experience, and the requirement for security clearances. They expressed concerns that the industry tends to favor younger candidates, suggesting that ageism could be a factor in the hiring process. In addition, they pointed out that many positions require security clearances and a significant amount of prior experience, which puts those without these qualifications at a disadvantage, even if they hold multiple degrees and certifications. The participant described cybersecurity as a "gated community" where employers seem to prefer

candidates who already have these qualifications, making it difficult for newcomers to break in. This reveals a broader issue within the industry and suggests that providing more opportunities for gaining clearances or relevant experience during internships could help align academic preparation with industry needs.

The participant also noted cultural and structural challenges within the cybersecurity industry. They expressed frustration with outdated organizational systems and leadership strategies that seem to avoid directly addressing cybersecurity challenges. Another issue they encountered was the lack of communication from employers after submitting job applications, a phenomenon they referred to as "ghosting." This lack of transparency adds to the difficulties of navigating the job market. Clearer communication from employers and better support in navigating platforms like USAJobs.gov could alleviate some of these frustrations, improving the experience for interns seeking employment after completing their programs.

Hands-on learning and mentorship were highlighted as key factors in the participant's experience. While they appreciated the academic knowledge gained during the internship, they felt that more practical, hands-on experience would have been extremely valuable. They believed that real-world applications, such as simulations or lab-based exercises, would have enhanced their learning. Mentorship played an important role in shaping their journey, with mentors like Dr. Arnold providing guidance and helping them understand the field's demands. Combining strong mentorship with more opportunities for practical application could give students a better foundation in cybersecurity and increase their confidence as they pursue careers in the field. Despite the challenges, the participant remains passionate about cybersecurity, driven by a sense of national duty and a desire to protect digital infrastructure. Their career path has shifted from management and data analysis to cybersecurity, where they feel they can have a meaningful impact. They continue to invest in their education, pursuing a master's degree in data analysis and obtaining additional certifications. The NIWC internship played a crucial role in reinforcing their interest in cybersecurity, though it did not fully prepare them for the challenges they now face in breaking into the field.

The participant offered several recommendations to improve the internship program. They suggested expanding the program to include more advanced opportunities, such as integrating CISA ROTC initiatives, and providing more hands-on learning experiences. They also emphasized the importance of including community college students, who may bring

valuable skills in areas like language and intelligence. Expanding the scope of the NIWC program and offering more diverse learning opportunities could better prepare future participants for the complex and rapidly evolving cybersecurity landscape.

Exploration of Themes Across All Three Interviews

Across all three interviews, several common themes consistently emerged. One major challenge for participants was the difficulty in securing cybersecurity positions, often due to the lack of necessary certifications, security clearances, or industry experience. While the internship provided them with foundational knowledge, they found themselves unprepared for the strict qualifications demanded by the job market.

Mentorship played a crucial role during the internships for all participants. Professors and mentors helped build their confidence by guiding them through both technical challenges and the transition into a cybersecurity career. The support they received was essential in helping them navigate the complex field of cybersecurity.

A need for more hands-on, practical experience was another recurring theme. Although the internship offered a strong theoretical foundation, participants noted a gap between academic knowledge and real-world application. They expressed a desire for more opportunities to apply what they learned in practical settings, which they believed would better prepare them for professional roles in the industry.

For each participant, the internship also served as a transformative experience that broadened their career perspectives. It often led them to redirect their professional goals toward cybersecurity. Despite the challenges they faced, participants expressed a strong passion for staying within the field, driven by the opportunities and insights they gained during the program. Another significant issue that emerged was the difficulty in navigating the job application process, particularly through platforms like USAJobs.gov. Participants reported a lack of guidance and clarity in how to successfully apply for cybersecurity positions, which created additional barriers as they transitioned from internship to employment.

These experiences can be connected to Albert Bandura’s Social Learning Theory, which highlights how people learn through observation, imitation, and modeling within a social context. The role of mentorship in the NIWC internship aligns closely with Bandura's concept of observational learning. Participants learned by observing their mentors and industry professionals, who provided valuable guidance and modeled successful behaviors in

cybersecurity. This process allowed participants to develop both technical skills and an understanding of how to navigate the field.

A key component of Bandura's theory is self-efficacy, or the belief in one's ability to succeed. The participants' growing confidence throughout the internship reflects this concept. Through mentorship and hands-on experiences, they developed not only technical competence but also the self-assurance necessary to pursue a career in cybersecurity.

Motivation and reinforcement also play an important role in Bandura's framework. Despite facing challenges such as job application difficulties, ghosting, or perceived ageism, participants remained passionate about cybersecurity. Their intrinsic motivation, often rooted in a desire to contribute to national security or protect digital infrastructure, continued to drive them forward. This motivation, reinforced by the sense of purpose they gained from the internship, helped them persist in the face of external obstacles.

While the NIWC internship effectively fostered observational learning and self-efficacy, there are areas where it could further align with Bandura's principles. Providing more opportunities for hands-on practice and offering structured support for obtaining certifications could enhance the practical learning experience and provide stronger reinforcement, helping participants feel more prepared for the demands of the cybersecurity industry.

Instructor Interviews

I interviewed the three other instructors who, along with me, were involved in creating and implementing the UH NIWC Cybersecurity Internship.

Dr. Robert Adamove

Dr. Adamove is a highly accomplished leader and portfolio manager with a distinguished career spanning both military service and federal employment. He began as a soldier in the United States Army, where he quickly excelled and became recognized as one of the top professionals in his field. Following his military service, Dr. Adamove transitioned to federal employment, where he led the Project Management Team in a Cyber Security Program for the Combat Capabilities Development Command of the U.S. Army. He now serves as a Senior Associate at Core4ce, where he continues to support critical cybersecurity initiatives.

Dr. Adamove plays an essential role as one of the key instructors for the University of Hawai‘i Naval Information Warfare Center (UH NIWC) cybersecurity internship. In this capacity, he has been instrumental in mentoring and guiding students, sharing his expertise in cybersecurity and project management while helping to prepare the next generation of professionals for the challenges of the field.

He holds the Project Management Professional (PMP) certification from the Project Management Institute (PMI) and is a Certified Agile SAFe Scrum Master. His extensive expertise includes the development and implementation of comprehensive program and project management processes. Dr. Adamove has vast experience overseeing complex programs that integrate hardware, software, operational infrastructure systems, and command, control, and information systems, along with the logistical deployment of platforms. Additionally, he holds a CompTIA Security+ certification, further reinforcing his proficiency in cybersecurity.

As an educator, trainer, and mentor, Dr. Adamove has demonstrated strong leadership in both academic and professional settings. His ability to manage cross-functional teams, develop detailed documentation, and implement assessment methodologies has made him a proactive leader in every role he undertakes. His commitment to fostering talent and providing guidance through mentorship has been pivotal to the success of his students and teams.

Dr. Adamove earned his Doctorate of Management in Project Management from Colorado Technical University, underscoring his dedication to continuous academic and professional growth. His vast knowledge in cybersecurity, leadership, and program management, combined with his role in the UH NIWC internship program, positions him as a key contributor to the advancement of the cybersecurity workforce.

Dr. Curtis Arnold

Dr. Curtis Arnold is the Chief Scientist for Cyber at Core4ce, where he helps to shape the strategic direction and senior level planning for the Department of Defense (DoD), Department of Homeland Security (DHS) and others. Likewise, Dr. Arnold is responsible for several academic engagements including the Naval Information Warfare Center (NIWC) Atlantic intern engagement at the University of Hawaii. Previously, Dr. Arnold was the President of Arnold & Associates Inc and Chief of the Sustaining Base Network Assurance Branch at the U.S. Army Research Laboratory. The Sustaining Base Network Assurance Branch is responsible for performing a wide range of Defensive Cyber Operations (DCO) activities from Research & Development to providing 24/7 CyberSecurity Services. CyberSecurity Service Provider (CSSP) duties include oversight of more than 300 external customers and monitoring of over 500 intrusion detection sensors around the world.

Dr. Arnold has supported the DoD and Federal Agencies for over 20 years in a variety of leadership, policy, and technical roles. Before joining ARL, Dr. Arnold was a Non-Commissioned Officer in the U.S. Army Judge Advocate General's Corps. Dr. Arnold holds a BS in Information Security and an M.S. in Information Technology from Johns Hopkins University and a D.Sc. in Cybersecurity from Capitol Technology University.

Dr. Steven Singer

Dr. Singer has had a distinguished career in both education and technology, with a focus on curriculum development, information technology, and distance education. He earned his BA in English Literature from the University of California at Riverside in 1976, followed by an MA in Teaching English as a Second Language from San Francisco State University in 1979. In 1994, he completed his EdD in Curriculum and Instruction at the University of Hawai‘i at Mānoa, with a dissertation titled Multiple Case Study of Freshmen Writing Students in a Networked Writing Environment.

From 2000 to 2022, Dr. Singer served as a Professor of Information Technology and Information Computer Systems at the University of Hawai‘i Kapi‘olani Community College (KapCC), where he played an essential role in shaping the IT program. In addition to his teaching and administrative duties, he was the IT Program Internship Coordinator from 2012 to 2022, a role that saw him overseeing and guiding students in gaining practical, hands-on experience in the field. His leadership in this role was critical to the success of the University of Hawai‘i Naval Information Warfare Center (UH NIWC) cybersecurity internship, where he served as one of the key KapCC academic instructors, helping to mentor and prepare students for careers in cybersecurity.

Dr. Singer’s work also extends to distance education, having served as a course developer and producer for the Hawai‘i Interactive Television System within the University of Hawai‘i system from 1995 to 2000. Earlier in his career, from 1984 to 1995, he held various technical and administrative roles, including Network Administrator and Language Arts Technical Liaison at KapCC.

Dr. Singer has been the recipient of numerous educational and Career and Technical Education (CTE) grants aimed at renewing the curriculum, software, and hardware resources for the IT program at KapCC. His contributions to both education and the field of information technology have been invaluable in preparing the next generation of IT professionals.

The interviews with Dr. Curtis Arnold, Dr. Robert Adamove, and Dr. Steven Singer offer a comprehensive look into the development, evolution, and future prospects of the NIWC cybersecurity internship program, which is closely linked with Kapi‘olani Community College (KCC) and the University of Hawai‘i (UH). The overarching goal of this program is to address

the shortage of qualified cybersecurity professionals and to build a talent pipeline for the Department of Defense (DoD), especially the Navy. Throughout the interviews, key themes related to program development, mentorship, challenges in the hiring process, and collaboration with academia were consistently highlighted.

Additionally, when analyzed through the lens of Bandura's Social Learning Theory, the internship program reveals strong connections with the concepts of observational learning, modeling, mentorship, and reinforcement.

Individual Interview Summaries

The interviews with Dr. Curtis Arnold, Dr. Robert Adamove, and Dr. Steven Singer revealed several key themes related to the success and evolution of the NIWC internship program. These themes include the crucial role of collaboration between academia and industry, the importance of mentorship in developing both technical and soft skills, challenges in securing employment with the Department of Defense (DoD), and the program's ongoing expansion.

Collaboration Between Academia and Industry

A recurring theme across all interviews was the vital collaboration between the University of Hawai‘i system and the Navy's NIWC division. Dr. Arnold, Dr. Adamove, and Dr. Singer all emphasized that the partnership is a cornerstone of the internship program's success. This collaboration bridges the gap between academic learning and real-world application, allowing students to gain practical experience while addressing the Navy's cybersecurity needs. Dr. Arnold, in particular, highlighted the program's origins in 2019, noting that it was designed to address the shortage of cybersecurity professionals in Hawai‘i. Dr. Singer echoed this sentiment by discussing how the program fits seamlessly with KCC's long-standing goal of preparing students for industry roles. The internship model has created a mutually beneficial relationship, with academia fostering student development and the Navy gaining from the students' contributions to cybersecurity initiatives.

Mentorship and Skill Development

All three interviewees emphasized the program's strong focus on mentorship and hands-on problem-solving. The internship connects students with professionals who provide guidance

on technical challenges and career development. This mentorship not only helps students build technical competencies, such as threat analysis and systems security, but also fosters critical soft skills, including problem-solving and communication. Dr. Arnold stressed that mentorship is central to the program's success, as students learn from observing and working closely with experienced professionals. This aligns with Bandura's observational learning theory, where students enhance their skills by watching experts in action.

The importance of soft skills development was particularly highlighted by Dr. Singer. He pointed out that the program goes beyond technical training by helping students with professional development activities, such as mock interviews, resume building, and creating LinkedIn profiles. These experiences prepare students for career success beyond the technical aspects of cybersecurity. Dr. Adamove also underscored this point by noting how students are required to present their research at the end of each semester, which strengthens their communication and presentation abilities.

Challenges in the Employment Process

While the program has been successful in equipping students with technical and soft skills, Dr. Arnold and Dr. Adamove both identified challenges in the employment process, specifically the complexity of the USAJobs.gov platform. This federal hiring system is described as a significant barrier for students seeking employment with the DoD. Both interviewees noted that the platform's complexity and lengthy application process often discourage students from pursuing positions in cybersecurity within the government. Simplifying or streamlining this process is seen as a critical step in improving student outcomes and facilitating their transition into DoD roles.

Program Expansion and Future Growth

The program's evolution and expansion were another common theme in the interviews. All three interviewees discussed how the NIWC internship has grown from a small initiative at KCC to a larger program that now includes several University of Hawai‘i campuses and extends to students in Guam. Dr. Arnold mentioned plans for further expansion, such as the creation of a laboratory where students can work with Department of Defense-related data. This hands-on

approach aims to give students even more opportunities to apply their cybersecurity skills in a real-world context.

Dr. Adamove and Dr. Singer also noted the increasing data-centric nature of the program. As it evolves, the internship is incorporating more research-based projects and technical challenges that mirror the real-world demands of cybersecurity professionals. This evolution ensures that students are not only learning cutting-edge skills but are also staying current with the rapidly changing cybersecurity landscape.

The NIWC internship program's success is rooted in the strong collaboration between the University of Hawai‘i system and the Navy, a comprehensive mentorship framework, and a balanced focus on both technical and soft skills. However, challenges remain, particularly with the complexity of the USAJobs.gov hiring process, which affects students' ability to transition into government roles. Despite these challenges, the program is expanding and evolving, offering increasing opportunities for hands-on learning and preparing students for the cybersecurity challenges of the future.

Connections to Bandura's Social Learning Theory

Bandura's Social Learning Theory asserts that learning occurs through observation, imitation, and modeling. The interviews highlight several aspects of the internship program that align with the following principles:

Modeling and Mentorship: In all three interviews, the role of mentorship is consistently emphasized. Students are paired with experienced professionals who model the behaviors, skills, and problem-solving approaches required in cybersecurity. This aligns with Bandura's idea that individuals learn by observing the actions of others, especially those in a mentoring capacity. Reinforcement of Skills and Behaviors: The positive outcomes of the internship, including successful job placements and the development of professional networks, serve as reinforcements. Students receive feedback from their mentors, which helps them improve and refine their skills. The program's structure ensures that students have multiple opportunities to receive feedback and adjust their approach.

Self-Efficacy through Practical Application: The program's emphasis on hands-on learning, real-world problem-solving, and exposure to professional settings helps build students'

self-efficacy—their belief in their ability to succeed. Through the internship, students gain confidence in their ability to tackle cybersecurity challenges and contribute to DoD objectives.

Observational Learning and Experiential Knowledge: The structured mentorship, coupled with exposure to real-world data and problems, enables students to engage in observational learning. They see how experienced professionals handle cybersecurity tasks, allowing them to model these behaviors in their own work. This type of experiential learning is crucial for preparing students for the workforce.

Conclusions from the Instructor Interviews

The NIWC cybersecurity internship program, as described in the interviews, exemplifies how Bandura's Social Learning Theory is applied in an educational and professional setting. Through mentorship, collaboration, and hands-on learning, students not only gain technical skills but also develop self-efficacy and professional confidence. The program's success in fostering talent for cybersecurity roles and its expansion to other regions reflects its adaptability and potential for continued growth.

Limitations

The study population was small and highly focused, presenting a view of internship methods, expectations, and results limited to the field of cybersecurity, specifically aligned with the US Dept. of Defense (DoD), the NIWC, and the State of Hawai‘i. There were 34 survey responses out of the 46 graduates of the NIWC cybersecurity internship from 2020-2023. One possible weakness in this study's reliability is that participants were chosen from a pool of students from at least one of the UH System campuses in the State of Hawai‘i and were also accepted to participate in the UH NIWC internship. This small and specific sample size may influence the validity of the research.

Chapter 5. Study Conclusions

This chapter examines the outcomes of the University of Hawai‘i (UH) Naval Information Warfare Center (NIWC) Cybersecurity Internship, highlighting its role in developing participants’ skills, confidence, and career direction, while also identifying areas for improvement such as hands-on technical training, certification support, and clearer employment pathways.

The study sheds light on how effectively the internship prepares students by equipping them with both technical and non-technical skills. Analyzing survey responses, interviews, and instructor feedback reveals that the internship played a key role in boosting participants' confidence, technical abilities, and career readiness. However, some areas for improvement have been identified, particularly in relation to certification preparation, practical hands-on experience, and job application support.

The internship made a significant contribution to participants' professional development by exposing them to real-world cybersecurity threats, tools, and operations. According to Luk and Chan's (2022) framework on engineering internships, participants developed both technical skills—such as threat detection, network security, and encryption—and non-technical skills—such as communication, adaptability, and teamwork. Many participants also noted improvements in their research and writing skills through assignments like literature reviews and presentations, which reinforced their academic competencies. However, a recurring theme was the need for more hands-on training to enhance their technical skills, particularly in areas like encryption, programming, and systems security.

Albert Bandura’s Social Learning Theory provides a useful framework for understanding the benefits participants gained from this internship. The mentorship model closely reflects Bandura’s concepts of observational learning, modeling, and reinforcement. Participants consistently emphasized the value of learning from experienced professionals who served as mentors and role models, reinforcing their technical behaviors and professional attitudes in real-world contexts. Bandura’s idea of self-efficacy, or the belief in one’s ability to succeed, also emerged as a central outcome. As participants took on more challenging tasks, such as incident response simulations and technical presentations, their confidence in their abilities grew. This confidence, supported by mentor feedback and successful task completion, proved crucial in

their decision to pursue careers in cybersecurity. However, while the program succeeded in fostering observational learning, the lack of direct, practical applications limited the ability to fully translate learned behaviors into real-world practice.

While the internship improved participants' technical and professional skills, the transition to employment yielded mixed results. Some participants secured cybersecurity positions, but others encountered difficulties due to the lack of industry certifications and challenges navigating government job platforms like USAJobs.gov. Certifications such as Security+ and relevant work experience were often cited as barriers to obtaining full-time roles, reflecting broader structural challenges in the cybersecurity industry, where even entry-level roles demand qualifications that recent graduates often do not have. However, for many, the internship provided clarity regarding their career paths, especially for those unsure about cybersecurity initially. Mentorship and role modeling helped enhance career motivation, consistent with Bandura's theory. Nonetheless, some participants chose to pursue other technical fields, such as software engineering, largely due to higher compensation in those areas, indicating that economic factors also play a significant role in career decisions.

Participants widely acknowledged the value of professional networking opportunities during the internship. Interactions with NIWC professionals, industry partners, and government agencies expanded their professional networks and exposed them to potential career pathways. In addition, the internship significantly improved participants' soft skills, such as communication, teamwork, and public speaking, which are essential in any technical field. Professional development activities embedded in the program, such as résumé writing, mock interviews, and LinkedIn profile creation, further prepared participants for the job market. These activities align with the non-technical competencies described in Luk and Chan's framework, highlighting the importance of such skills in enhancing employability.

While the internship program effectively prepared students for cybersecurity careers, several areas for improvement were identified. Participants expressed a desire for more hands-on experience with cybersecurity tools and techniques. Expanding the program to include more technical projects, lab simulations, and incident response drills could help enhance the connection between theoretical knowledge and practical application. In addition, given the importance of certifications in the cybersecurity job market, the program could incorporate structured support for obtaining certifications like Security+. Providing resources for

certification exam preparation would better position participants for competitive entry-level roles.

Another challenge participants faced was navigating the job application process, particularly for government positions. Many found platforms like USAJobs.gov difficult to use. Offering workshops or individualized support to help students navigate these platforms could increase their chances of successfully applying for cybersecurity positions. Furthermore, some participants opted for careers outside cybersecurity due to better financial incentives in other fields. The program might benefit from exploring ways to highlight the long-term value of cybersecurity careers. Partnering with industry and government agencies to offer competitive compensation packages for entry-level positions could help retain talent in the field.

Overall, the UH NIWC cybersecurity internship provided valuable professional development opportunities, fostering both technical and non-technical skills. Through mentorship and real-world experience, the internship aligned well with Bandura's Social Learning Theory by enhancing participants' self-efficacy and motivation to pursue cybersecurity careers. However, there remains a critical need for more hands-on training, certification support, and job application guidance to ensure that future participants can fully capitalize on the opportunities provided by the program. Addressing these areas will strengthen the program's ability to meet the growing demand for a skilled and prepared cybersecurity workforce capable of addressing the digital security challenges of today's world.

Advancing Cybersecurity Education Through Collaborative Internship Design

As an assistant professor and university instructor with more than a decade of experience teaching programming, network security, ethical hacking, and internship courses at the University of Hawai‘i, I have long sought more effective ways to prepare students for immediate entry into the cybersecurity workforce. My goal has always been to ensure that students graduate not only with technical proficiency but also with the confidence, clarity, and adaptability needed to succeed in professional environments.

With this in mind, I developed the UH NIWC Cybersecurity Internship in collaboration with the United States Naval Information Warfare Center and industry partners. My intent was to create a meaningful pathway that would support students' technical growth, foster their professional and personal development, and help them build a sense of self-efficacy. I designed

the program to provide hands-on experience within operational environments, guided by mentors from academia, government, and industry; a collaborative trifecta that mirrors the real-world contexts in which cybersecurity professionals operate.

This dissertation is not simply a program evaluation. It is a research study that contributes new academic knowledge by examining a distinctive, collaborative internship model through the lens of Bandura's Social Learning Theory. By analyzing how students learn through observation, modeling, vicarious reinforcement, and social interaction, this case study reveals how structured experiential learning can shape both technical competency and self-belief. The findings provide insight into the specific skills and experiences that are most effective in bridging the gap between education and industry expectations in the cybersecurity domain.

The results of this study affirm the value of the trifecta model, academia, government, and industry, as a powerful structure for developing workforce-ready professionals. Each partner plays a distinct and essential role: academia offers foundational knowledge and continuity, government brings mission-driven priorities and access to national security frameworks, and industry contributes cutting-edge tools, operational insight, and workforce relevance. Together, these partners create a dynamic learning environment that no single sector could provide alone. The study demonstrates that when these three forces are aligned, the outcome is a learning experience that is technically rigorous, professionally meaningful, and personally transformative for students.

In doing so, this research adds to the growing body of literature on work-integrated learning (WIL) and reinforces the value of high-impact practices (HIPs) in higher education. The UH NIWC Cybersecurity Internship exemplifies how these practices can be implemented in a technical field, resulting in deeper student engagement, more robust skill development, and greater career readiness. Additionally, the study highlights the increasing importance of soft skills, communication, collaboration, and adaptability as essential complements to technical expertise in cybersecurity education.

Ultimately, this work offers a replicable model of cross-sector collaboration that can inform the design of future internship programs. It provides both practical and theoretical contributions to our understanding of how experiential learning enhances cybersecurity education and prepares students to meet the complex demands of a critical and rapidly evolving field.

The Future of the UH NIWC Cybersecurity Internship Program

The UH NIWC Cybersecurity Internship program was recognized as a successful model and received additional funding from the United States Navy to continue its operations. Beginning in the 2024–2025 academic year, this funding now supports program offerings in both the Spring and Fall semesters year-over-year, expanding access and continuity for students across the University of Hawai‘i System. In response to the positive feedback and outcomes documented through student surveys, NIWC leadership also committed to establishing a permanent cybersecurity laboratory at the UH Mānoa campus. This lab will provide participants with more extensive hands-on training, data-centric projects, and real-world challenges that simulate professional cybersecurity operations.

Notably, the internship program continues to serve students from all ten University of Hawai‘i campuses across four major Hawaiian islands and has recently expanded its reach to include students from the University of Guam and Guam Community College. This expansion reflects the program's alignment with Department of Defense interests across the broader Indo-Pacific region, including growing engagement with territories like Guam and, potentially, Palau. This regional outreach not only broadens access but also strengthens Hawai‘i's strategic role in national cybersecurity workforce development.

As the program continues to grow, future studies should consider evaluating long-term participant outcomes, particularly income levels and career progression, five or more years after graduation. This type of longitudinal analysis would provide critical insights into the economic and professional impact of collaborative internship models, especially those that unite academic institutions, federal agencies, and industry partners in a shared commitment to workforce readiness.

Appendix A - Surveys and Interviews

Student Survey

University of Hawai‘i
Consent to Participate in a Research Project
Dr. Scott Robertson, Principal Investigator
Project title: Cybersecurity Internship Impacts on Participant Professional Development, Employment, and Income: A Case Study

---

Aloha! My name is Dave Stevens, and you are invited to participate in a research study. I am a graduate student at the University of Hawai‘i (UH) at Mānoa in the Communication and Information Sciences (CIS) Program, and I am conducting a research project as part of my Ph.D. requirements.

What am I being asked to do?

If you participate in this project, I will send you a link to a Google survey you may complete at your convenience.

Taking part in this study is your choice.

Your participation in this project is entirely voluntary. You may stop participating at any time. If you stop being in the study, there will be no penalty or loss to you.

Why is this study being done?

My project aims to evaluate the impacts of post-secondary cybersecurity internships in the State of Hawai‘i. You are being asked to participate because you participated in the UH Naval Information Warfare Center (NIWC) Cybersecurity Internship between 2020-2023.

What will happen if I decide to take part in this study?

The survey will consist of approximately 35 questions. It will take approximately 15 - 20 minutes. The survey questions will include questions like, “Were you interested in working in cybersecurity before this internship?” and “Do you believe your internship experience helped you get your current job?”

This survey will be sent via email.

What are the risks and benefits of taking part in this study?

I believe there is little or no risk to you in participating in this research project. However, if you become stressed or uncomfortable while answering any of the survey questions, you can skip the question or withdraw from the project altogether.

Participating in this survey will not directly benefit you. However, the results of this project may help improve cybersecurity internship planning in the future.

Privacy and Confidentiality:

I will keep all study data secure. It will be in digital form, in a cryptographically secure and access-controlled storage area. Only my UH advisor and I will have access to the information. Other agencies that have legal permission have the right to review research records. The University of Hawai‘i Human Studies Program also has the right to review research records for this study.

After I gather survey responses, I will keep the results for a period of one year. Then, I will erase the survey data. When I report the results of my research project, I will not use your name or official title without your permission.

Compensation:

There is no compensation for participating in this research project.

Future Research Studies:

Identifiers will be removed from your private information. After the identifiers are removed, the data may be used for future research studies or distributed to another investigator for future research studies, and we will not seek further approval from you for these future studies.

Questions:
If you have any questions about this study, please email me at david.stevens@hawaii.edu. You may also contact my advisor, Dr. Scott Robertson, at (808) 956-3500 or scottpr@hawaii.edu. You may contact the UH Human Studies Program at 808.956.5007 or uhirb@hawaii.edu. to discuss problems, concerns, and questions; obtain information; or offer input to an informed individual who is unaffiliated with the specific research protocol. Please visit http://go.hawaii.edu/jRd for more information on your rights as a research participant.

Your submission of the digital survey will constitute your informed consent to participate in this survey.

If you do participate in the survey, please select “email me a copy of my responses” before selecting “submit”.
Mahalo!

Survey Questions:

Part I. Personal Info

I, 1. What is your age? *(Please select range, 18-21, 22-25, 25-28, 28+)*
I, 2. Did you graduate from a high school in the state of Hawai'i*? (Please select Yes or No)*
I, 3. Which participating UH campus did you attend? *(Please select from the following*
University of Hawai'i Mānoa,
University of Hawai'i Hilo,
University of Hawai'i West O'ahu,
University of Hawai'i Maui College,
Kapi'olani Community College,
Kauai Community College,
Honolulu Community College,
Windward Community College,
Leeward Community College,
Hawai'i Community College)
I, 4. Did you graduate from a university with a degree? (Please select Yes or No)
I, 5. If yes, what degree(s) have you earned? *(Please select all that apply or not applicable*
AA/AS
BA/BS
MA/MS
Ph.D.)
I, 6. Are you currently employed? *(Please select Yes or No)*
I, 7. Are you employed in a cybersecurity or related position? *(Please select Yes, No, or not applicable)*
I, 8. Are your work duties related to your major or last earned degree? *(Please select Yes, No, or not applicable)*
I, 9. In what US state or territory do you currently work? *(Please select a US State or territory, Outside the United States, or not applicable)*

Part II. Reasons for Internship Participation

II, 1. What was the reason you participated in this internship? *(Please check all that apply)*
a) department requirement
b) advisor recommendation
c) to gain practical industry experience
d) Other *(please explain)*

II, 2. What did you expect to gain from the internship? *(Please check all that apply)*
a) Academic credit
b) To link classroom learning to workplace reality
c) To better prepare for independent life
d) Other *(please explain)*

II, 3. Impact on current and future employment

a) In a few sentences, please identify the internship program experiences that had the most impact on your current or future employment.

The remainder of the survey questions in this section will obtain answers based on a scale with the following values:

1. *Strongly disagree*
2. *Disagree*
3. *Neutral*
4. *Agree*
5. *Strongly agree*

b) I was interested in working in cybersecurity before this internship.
c) I believe the internship experience helped me get my current job.
d) I believe my internship experience will help me get promotions in the future.

Part III. Professional Development

III,1 – In a few sentences, please identify the internship program experiences that had the most impact on your professional development.

The remainder of the survey questions in this section will obtain answers based on a scale with the following values:

1. *Strongly disagree*
2. *Disagree*
3. *Neutral*
4. *Agree*
5. *Strongly agree*

III,2 – The internship program changed me professionally.
III,3 – The internship program helped clarify my professional goals.
III,4 – I applied my classroom knowledge during the internship program.
III,5 – The internship program helped me to gain practical work experience in my field of interest.
III,6 – I encountered difficulty seeking and accepting internship work assignments.

Part IV. Professional Skills

IV,1 – In a few sentences, please identify the internship program experiences that had the most impact on your professional skills.

The remainder of the survey questions in this section will obtain answers based on a scale with the following values:

1. *Strongly disagree*
2. *Disagree*
3. *Neutral*
4. *Agree*

5. *Strongly agree*

IV,2 – The internship program improved my communication and interpersonal skills.
IV,3 – The internship program enhanced my decision-making and problem-solving skills.
IV,4 – The internship program improved my ability to work as part of a team.
IV,5 – The internship program enhanced my critical thinking skills.
IV,6 – The internship program improved my computer, networking, and data analysis skills.
IV,7 – The internship program improved my skills in cybersecurity.

Part V. Personal Growth

V,1 – In a few sentences, please identify the internship program experiences that had the most impact on personal growth.

The remainder of the survey questions in this section will obtain answers based on a scale with the following values:

1. *Strongly disagree*
2. *Disagree*
3. *Neutral*
4. *Agree*
5. *Strongly agree*

V,2 – The internship program helped me improve professionally and personally.
V,3 – The internship program changed my personal career goals.
V,4 – The internship program positively changed my interest in cybersecurity.
V,5 – I developed a habit of accomplishing tasks before the set target date.
V,6 – The internship program allowed me to apply concepts I learned in the classroom.
V,7 – The internship program changed my aspirations in some ways.

Part VI. Personal Capabilities

VI,1 – In a few sentences, please identify the internship program experiences that had the most impact on personal capabilities.

The remainder of the survey questions in this section will obtain answers based on a scale with the following values:

1. *Strongly disagree*
2. *Disagree*
3. *Neutral*
4. *Agree*
5. *Strongly agree*

VI,2 – The internship program improved my conscientiousness and ethics.
VI,3 – The internship program enhanced my respect for people different than myself.
VI,4 – The internship program improved my ability to learn.
VI,5 – The internship program improved my time-management skills.

VI,6 – The internship program improved my social relationships.
VI,7 – The internship program encouraged me to take the initiative.
Instructor Interviews

University of Hawai‘i
Consent to Participate in a Research Project
Dr. Scott Robertson, Principal Investigator
Project title: Cybersecurity Internship Impacts on Participant Professional Development, Employment, and Income: A Case Study

Aloha! My name is Dave Stevens, and you are invited to participate in a research study. I am a graduate student at the University of Hawai‘i at Mānoa in the Communication and Information Sciences Program. I am doing a research project as part of the requirements for earning my graduate degree.

What am I being asked to do?

If you participate in this project, I will interview you via collaborative media (i.e., Zoom) at a time convenient for you.

Taking part in this study is your choice.

Your participation in this project is entirely voluntary. You may stop participating at any time. If you stop being in the study, there will be no penalty or loss to you.

Why is this study being done?

My project aims to evaluate the effectiveness of post-secondary cybersecurity internships in the State of Hawai‘i. You are being asked to participate because you taught in the UH NIWC Cybersecurity Internship between 2020 and 2023.

What will happen if I decide to take part in this study?

The interview will consist of 10-15 open-ended questions and will take approximately 30 - 45 minutes. I will ask questions such as “What was your original goal when helping to create this internship?”.

Only you and I will be present during the interview, which will be conducted via collaborative media (e.g., Zoom). With your permission, I will record the session audio. You will be one of several people I will interview for this study.

What are the risks and benefits of taking part in this study?

I believe there is little or no risk to you from participating in this research project. However, you may become stressed or uncomfortable answering any of the interview questions or discussing

topics with me during the interview. If you do become stressed or uncomfortable, you can skip the question or take a break. You can also stop the interview or withdraw from the project altogether.

Participating in this survey will not directly benefit you. However, the results of this project may help improve cybersecurity internship planning in the future.

Privacy and Confidentiality:

I will keep all study data secure in digital form in a cryptographically secure and access-controlled storage area. Only my University of Hawai ʻi advisor and I will have access to the information. Other agencies that have legal permission have the right to review research records. The University of Hawai ʻi Human Studies Program has the right to review research records for this study.

After I write a copy of the interviews, I will keep the audio/video recordings for one year. Then, I will erase them. When I report the results of my research project, I will not use your name or official title without your permission.

Compensation:

There is no compensation for participating in this research project.

Future Research Studies:

Identifiers will be removed from your identifiable private information, except for your official title. After the removal of identifiers, the data may be used for future research studies or distributed to another investigator, and we will not seek further approval from you for these future studies.

Questions:

Questions:
If you have any questions about this study, please email me at david.stevens@hawaii.edu. You may also contact my advisor, Dr. Scott Robertson, at (808) 956-3500 or scottpr@hawaii.edu. You may contact the UH Human Studies Program at 808.956.5007 or uhirb@hawaii.edu. to discuss problems, concerns, and questions; obtain information; or offer input to an informed individual who is unaffiliated with the specific research protocol. Please visit http://go.hawaii.edu/jRd for more information on your rights as a research participant.

If you agree to participate in this project, please print, sign, date, scan this signature page and return it to: david.stevens@hawaii.edu.

Keep a copy of the informed consent for your records and reference.

Signature(s) for Consent:

I give permission to participate in the research project "*Business Continuity Planning (BCP) in Election Systems."*

Please initial next to either "Yes" or "No" to the following (the default will be "No" unless you choose otherwise):

_____ Yes _____ No I consent to be audio-recorded for the interview portion of this research.

_____ Yes _____ No I consent to having my name included in this study.

_____ Yes _____ No I consent to having my work title/position included in this study.

Appendix B - Interview Questions and Transcripts

Instructor Interview Questions

1. What is the history of this effort by the NIWC to recruit cybersecurity workers?
2. How did you become involved in this effort?
3. Why did you come to speak with the IT faculty at Kapi ʻolani Community College (KapCC)?
4. What were your initial thoughts about an NIWC cybersecurity internship at KapCC?
5. What were your expected outcomes from this internship?
6. How has this internship changed since the first time it ran in the Fall of 2020?
7. From your perspective, has this internship produced the original expected outcomes?
8. What would you attribute that to?
9. What changes do you plan to make to this internship in the future?
10. From your perspective, what are some obstacles experienced by NIWC applicants?

Instructor Interview - Dr. Curtis Arnold, D.Sc.
24 June 2024, 10:30 am HST

[David Stevens] Okay, we're recording.

[David Stevens] So, thanks for signing the consent guide, and thanks for participating in my research study. We talked about some of the questions already that I was going to ask, and, you know, that was to get you to kind of think about the responses you might give, and so I'm going to be documenting this. Let me turn on the captions.

[David Stevens] Okay, question one. Do you have the questions in front of you, by the way?

[Curtis Arnold] I do not. I don't think I ever got the questions. I know you met with Rob and Jesse.

[David Stevens] Okay, let me share the questions. You should be looking at them now. And let's just go over these.

[Curtis Arnold] Okay. Just want me to start working my way down it?

[David Stevens] Yeah, if you would, please, that would be great.

[Curtis Arnold] All right. The history of the effort goes back to 2019. When I first joined, I came out of government service, and I started supporting NIWC, and one of the things they wanted to do is they were looking to stand up a regional operations center in Hawai ʻi, so I went out with them, and they had some people already, but they said they had a problem with actually hiring on-island, because there's so few people that were qualified that can actually work for the DoD there.

[Curtis Arnold] And so one of the things, having a past experience with working with a lot of academia, I asked them if they had been working with the university or any of the schools there, any of the university system, and they said they had not and had never thought about it. So I talked to them a little bit about what we've done in the past with working with academia, how we've had partnerships for both programs and internships, and they said that would be great, and they would be more than happy to fund an internship if we could get one focused the right way with cyber. And so that's how it came to be, and then because I had all the experience, they asked me to take the lead on it, which is how I became involved in the effort, right? And so what we did was we went and we reached out to all of the schools.

[Curtis Arnold] I knew Matt Dunlap, for example, from West O ʻahu because he was at West Point before. So we went and talked to him, and then I just cold reached out to all the schools, and you were at KCC were one of the first people that were responsive, and so you were one of the first people we went out to visit. And I would say you guys have been the most engaged throughout the entire program, which is why we keep going back and talking to you all the time because we've formed a pretty good, I think, professional relationship, friendship, where you've always wanted to be engaged and involved, and that's why we keep going back to KCC, and we look for in the future where else to be involved.

[Curtis Arnold] We have participated like in your academic reviews, your once-a-year advisory panels, things like that, and did the mock trials with the student, not mock trials, mock interviews with students. Trials, if you ask them, that could be. Yeah, it could be.

[Curtis Arnold] So that's kind of how we came and started to speak into KCC and just kept the relationship going, right? Do you want me to stop there real quick? Do you have any, like, you need other points out of it?

[David Stevens] Yeah, I think you covered one through three already. Yeah. So, yeah, just, this is really important.

[David Stevens] We're trying to differentiate between what all of our expectations were going into this effort, and here we are four years later. You know, are we aligning our efforts, or have

we changed? How have we changed? You know, what's our initial thoughts going into this effort from your point of view?

[Curtis Arnold] The initial thoughts, I mean, it was to form a relationship, which I think we did successfully over four years. We have enough of a track record and everything to show that, A, we're both good partners.

[Curtis Arnold] I know on the Navy side, the DoD side, they know, A, we've been able to do this consistently, and they see it as a positive, rewarding experience. I know the command has briefed what we've been doing to multiple organizations, both within the DoD and, like, congressional visits, things like that, as an example of how a good program can run when you have both sides talking to each other. But the goal was to be able to identify students and then move them on in their professional, you know, career, make sure that they're good to go forward, and we, I think, have been very successful in that.

[Curtis Arnold] I would say that NIWC hasn't done a good job of hiring them. We've just had recently a few that have gone on to NIWC, but that was because of an internal process, which I think we have fixed now. That has nothing to do with KCC or any of the other schools or the University of Hawai ʻi system.

[David Stevens] That's good to know. That's good information. Thank you.

[Curtis Arnold] Yeah, so the school has been doing great. The students, all the ones we've talked to, we've had multiple where they've asked myself, I think you and Rob Adamove, to be referrals or actually sit in on their clearance review and be on their contact information, which we've done every time. And so we've had pretty good luck there.

[David Stevens] Okay, so it sounds like for the most part, you're saying that for number four or number five, your expected outcomes, you're checking all the boxes pretty much that you expected to check.

[Curtis Arnold] Okay. Yeah, everything that we expected to do occurred.

[Curtis Arnold] We got great students, had a great relationship, and everything that we initially set out to do, we did, which is why we're looking to expand the program moving on.

[David Stevens] Well, that brings us right into question number six. How has the internship changed since the first time we ran it in fall 2020?

[Curtis Arnold] So the first time, it was really about just getting in and trying to figure out what the schools were like and what the students were like and what they could do.

[Curtis Arnold] And it was just preparing them. The idea then was that we were going to have to prepare them for multiple follow-on internships. And what we found along the way is that the schools and the students are both competent.

[Curtis Arnold] They've got good programs. We worked with the advisory panels from multiple schools to kind of tweak them a little bit. But for the most part, they were ready to go.

[Curtis Arnold] The way the internship program ran is we actually had a technical side, and that was important to give them some skill. However, what we did was we did more of a research project and a problem-solving exercise having to do a lot with like literature reviews, things like that. And we gave them a problem.

[Curtis Arnold] And then we were more interested in how did the students go about looking into that problem? What was their problem-solving abilities, right? And we found out for the most part, all the students really had a good base understanding as far as how to get there. There were, like I said, we tweaked with some of the schools as far as, hey, we need them to be a little more technical in this area. So when they got to this part, they actually understood it a little better.

[Curtis Arnold] But for the most part, it's hard to teach. It's easier in some ways to teach the technical side and give them that underpinning and then actually trying to teach them how to logically go through and solve a problem, right? That's much harder. That's a soft skill that takes a while in classrooms and course work a while to do and develop.

[Curtis Arnold] And we believe they were getting that strong underpinning already, right? So what we're looking to do is going forward, the next phase is to kind of create a laboratory there where students can come in. They already have that underpinning of how to solve problems. They might need a little mentorship and classes along the way, but have a lab where when it comes time for them to do their individual projects, their capstones, internships, whatever they need to do, that there's a laboratory there with data and problems that are related to the DoD for them to fall in and work on.

[Curtis Arnold] That way we get to evaluate the students, but they also have real world problems and data that they're working on that they can then put on their resume that's tied to a mentor or something that lets them put it on and actually have that exposure before they ever graduate college, right? And it also gives them a chance to, like I said, they'll be aligned with a mentor, whoever had the problem, to look and see, am I doing this right? Getting that feedback, which can also lead a lot that one-on-one relationship to other positions, jobs, future referrals, contacts, networking, all that good stuff.

[David Stevens] The way you answered that question, I think answers question number seven as well, right? We've covered that. You've actually, you had some original expectations and the way you proceeded through this, you pretty much checked all those boxes and produced the outcomes you were looking for.

[David Stevens] And let's go move into the changes we're going to see this fall coming up. We're changing the internship. We're making some drastic changes and let's discuss that.

[David Stevens] What are the changes you're making and why are you doing that?

[Curtis Arnold] So we're doing it because, like I said, we think the students can do more if we give them more access and more problems and give them more of a structured thing, more of a framework for them to do their academic pursuits. And that's why we're, what we're doing in the fall is we're, well, I should say going into fall of 25, right? We want to have a laboratory stood up where we can bring students in working on data and solving problems. The fall of 24 and the spring of 25, what we're doing is we're bringing in a group of students to actually go through and work with us and you and the professors to actually develop what does that lab look like? How does it tie into the UH system? How can every campus play with it and work with it? And where? Does it make sense, right? The two-year students might work on it different than a four-year computer science student.

[Curtis Arnold] And so we want to account for everybody that might be touching it. So the fall, the idea is that they're going to come in and work on, all right, what data do we need to have in the lab? How do we want to structure the problems? How do we want to tag the data we've written in the lab? How do we want to structure it for students to actually use it and work off of it? And what does that look like, right? So the end of the semester, we have a good straw man on and a plan in place for how we would execute and stand up the laboratory. Then the spring of 25, that set of interns is going to be working on standing it up and having it go IOC, right? Some initial operating capability.

[Curtis Arnold] And so that they're going to come up with the bare minimum of, you know, what we need in AWS. How is it going to look? Where are we going to, we're actually going to collect some data and put it there, stage it for students, things like that. And that way, in the fall of 25, we can actually get all the interns aligned to where they should be working on their capstones, things like that.

[Curtis Arnold] If we do it right, it's going to be a no brainer to have that framework in place for every student to go in and do their capstone. They don't have to worry about where they're going to go do their internship, where they're going to go do their capstone. We have a list of problems, you know, aligned with the data that you would need to solve them, along with the DoD kind of mentoring and expertise, as well as the professors.

[Curtis Arnold] So they can just fall in and start working on that and get that real world experience, which is the goal, right? So that's the idea of the plan.

[David Stevens] I love that plan. One of the changes I wanted to mention, we made a change to not pay the interns for fall of 2024.

[David Stevens] Kind of an experiment. And we have seen a reduction in the number of applicants, but I have not done recruiting. We'll see if we can raise those numbers.

[David Stevens] That might be something that we study in the future. What do you think?

[Curtis Arnold] Okay, it absolutely does. Again, the outcomes or the incentives that are important to each student and where they're at in their program is different, right? The two-year, you know, I went to a two-year school way back in the day.

[Curtis Arnold] Then I was working, I was trying to figure out how I was going to make ends meet and everything else. And having that paid internship might be that incentive we need to get them in and get them innovated and actually looking towards going on to other programs.

[Curtis Arnold] Four-year students, they signed up for the four years. They have to get out, right? They're interested in what's coming next. And how are they going to get that skill set to put on that resume, right? And so their interests and motivations are different.

[Curtis Arnold] And so we're going to see kind of what we get this year. And we are applying for, as you know, for grants to bring in other money to help pay for the students and some of the professors' time. And that might be the answer is that, hey, for two-year students, we need to pay for interns.

[Curtis Arnold] And that's, it's not a bad answer. It's just the answer, right? And then we, now that we know that, then we can go after it.

[David Stevens] Excellent.

[David Stevens] I think we already discussed number nine. Your perspective was some of the obstacles experienced by the NIWC applicants. So what is your thought? This is my main question about those obstacles.

[David Stevens] What is your thought about USA Jobs, the website and the application process? Do you think that rigorous process is one of the obstacles they might be experiencing?

[Curtis Arnold] Absolutely. The USA website, I know people that have been out in the field for two decades that are having problems understanding the USA Jobs website. It's not conducive for students, right? And there's multiple programs out there for students, and none of them really are highlighted on USA Jobs.

[Curtis Arnold] And so there's a lot of issues out there with it. And so I think there's multiple problems with USA Jobs in order to get it. And really, if we're going to require the students to go there and do it, then we should include like a class on that.

[Curtis Arnold] They need to also understand, like if they sit there and say, hey, they need two years of experience, the students need to understand that, you know, to the college or to USA Jobs and to contract companies, the degree counts as years, right? And so that when you talk about labor categories or LCATs, that counts, your college education counts as time. And so that's important, like, hey, don't read that and get discouraged. That really, you can fix that and apply to that here.

[Curtis Arnold] And I don't think anyone's really doing a great job across the board of educating the college students on that. It's a gap. I mean, I know we've talked to them about a little bit, but not nearly, I think, as much as they could.

[Curtis Arnold] But I think that's definitely causing a lot of them to not apply, right? Unless someone goes and talks to them and actually meets with them.

[David Stevens] Agreed. Yeah.

[David Stevens] And thank you. That's all the questions I have. Would you like to add anything else at the end?

[Curtis Arnold] No, you know, I appreciate you and everything you do.

[Curtis Arnold] I think this is a great effort. This will help us across the board as far as, you know, gaining input on where should the internship go, as well as going after the grants and the additional funding. I think the senator and the congressman that came to visit that you brought in, this is going to be the kind of stuff they want to see.

[Curtis Arnold] I do have that Native Hawai ʻian organization that's coming in to partner with us. So we're going to have them as well that they can set aside money to and stuff like that. So almost everything we're doing in the area.

[Curtis Arnold] Oh, and the willingness to expand to Guam and bring on that's, you know, DoD has concerns in other areas. I've got another meeting here pretty soon with, I actually might be briefing the president of Palau.

[David Stevens] Oh, yes.

[David Stevens] I've been reading about Palau.

[Curtis Arnold] So there's a bunch of stuff going on there and they'd like to look at and see if they can get involved. You know, this might turn into a bigger thing, but that's, you know, University of Hawai ʻi and your willingness to be open and adapt to Indo-PACOM's needs as well is really kind of endearing this system to the military out there.

[Curtis Arnold] Right.

[David Stevens] That's wonderful to hear. And we do have one applicant for fall 2024 that's been accepted from the University of Guam.

Yep.

[David Stevens] So we have expanded. That's great.

[David Stevens] We're excited about. Let me, let me end the recording and save the transcript really quick.

Instructor Interview - Dr. Robert Adamove, D.M.
28 June 2024, 09:12 am HST

[David Stevens] Okay, we're recording. I'm also capturing live transcripts in real time. The recording is just so I can confirm that my transcript is accurate, but I'll be using the AI-generated transcript from Zoom to confirm in my appendices exactly what people said in the interview and in the dissertation itself.

[David Stevens] I'll summarize comments. Also, I've been promising my interviewees that I will send them my summaries prior to me publishing so they can tell me, yes, I believe that's what I said, or can you doctor that because I sounded stupid? So anything in that realm would be okay. I just want you to be satisfied because this is getting published and these are gonna be words attributed to you, so I get it.

[David Stevens] I'm gonna give you a chance to help me out on that front. But whatever we say is being recorded in real time. Are you okay with that?

[Robert Adamove] Yes.

[David Stevens] Awesome. Let me just preface this by saying these are the questions I wanna ask, but we don't need to go in order in any way at all. Pick out that first question, answer it, and the way it's gone in the past two interviews is questions like one through five get answered in the first 10 minutes of just talking.

[David Stevens] So I'll be listening carefully to your answers, but just tell me about question number one. And you don't have to be super detailed, but just give me your impression. Why was this going on? How'd you get involved?

[Robert Adamove] Okay, regarding question one, what is the history of this effort by the NIWC to recruit cybersecurity workers? In that regard, there is definitely a shortage of trained cyber personnel.

[Robert Adamove] I know that that shortage has been a growing concern for not only the Department of Defense, but also for Hawai‘i as a whole. The need is definitely outpacing the supply. A lot of people are impacted by that shortage.

[Robert Adamove] That shortage leaves people vulnerable, organizations, government organizations, both. And when working with the Navy like I have, and Dr. Arnold also has, that talent gap has surfaced a handful of times. I'm not sure exactly how Curtis made that first introduction with Kapi ‘olani Community College or the University of Hawai‘i, but regardless of how it was made, he quickly contacted me and said that there is an internship opportunity here.

[Robert Adamove] He and I have done similar type of internships for the Army in the past, both were government personnel. And we tried to leverage our knowledge and experience with the Army to benefit both the Navy and hopefully the students in the University of Hawai‘i program. Basically that lack of specialized training is what brought this about and hoping to create a

pipeline to allow the pool of candidates and potential workers to benefit the Department of Defense, specifically the Navy, and hopefully the program itself.

[Robert Adamove] A run on answer, if it were written, there'd be a lot of run on sentences, but please let me know if there's anything to follow up or if I didn't answer correctly for this question.

[David Stevens] No, I think you're doing rather well. Go ahead and just keep knocking them out.

[David Stevens] I think you covered one pretty clearly.

[Robert Adamove] Okay, so number two was how did you become involved in this effort? Gonna kind of recap some of the information I already provided, but I was introduced to the program through Dr. Curtis Arnold. I believe that was back in 2020 when he first contacted me.

[Robert Adamove] And in fact, I see on the question six, it's called 2020. We leveraged some of our past experience. Dr. Arnold is being a doctorate.

[Robert Adamove] His is in computer science, whereas mine is in project management. We split the effort between the two of us where he'll focus on the more technical pieces of the class. And for the past few years, it's the internship program has been very research heavy based.

[Robert Adamove] With it being so research based, I've led the students through the research portion of the program, where they were doing cybersecurity research. We tried to align their topics to topics that are of interest to the interns, but also would be beneficial to the Navy and the Department of Defense. So we would pull the students, find out what some of their interests are, and then draw a linkage between their interest and how to benefit the Navy or the Department of Defense.

[Robert Adamove] And that's how a lot of them wound up on the topic. So again, while Dr. Arnold focused on the technical piece, I tried to focus on the research piece, lead them through the research methodology, help them write their papers, review their papers step-by-step in increments. And then for the past few years, the research projects themselves resulted in a poster presentation at the end of the semester.

[Robert Adamove] That would be brief to both NIWIC staff and personnel within the University of Hawai‘i. We'd also sometimes have special guests. And last year, two particular guests were Senator Hirono and Representative Hicks. [note – this was U.S. Rep. Ed Case]

[Robert Adamove] So that kind of speared off the question of how I became involved, but knowing a little bit of background shows how I was more involved in this effort. For number three, why did you come to speak with the IT facility at Kapi ‘olani Community College? Again, that was through the introduction done by Dr. Arnold. He brought me on to help assist him as he was working with others to help develop this program.

[Robert Adamove] And again, the program, I believe, is due to that shortage that I previously mentioned regarding trained cyber personnel and how the need has outgrown the pace of which people are entering the community. What were your initial thoughts about a NIWC cybersecurity internship at Kap-CC? I was very excited. Having worked in cybersecurity for about the last 10 years, again, anything we can do to help grow the field and identify potential employees for the future and especially be able to identify the ones who stand out amongst others and allow for future opportunities.

[Robert Adamove] One success story is a student who got hired by NIWC as a government personnel. I know there's been other interests and NIWC itself is trying to secure more funding for more positions in the future. So being able to be a part of that is very exciting for me.

[Robert Adamove] And I'm only hoping and seeking more success for the program as we go forward and hear more about that. As far as number five, what were your expected outcomes from this internship? Just that, to continue to help grow and improve the program itself, knowing that it can lead to these future opportunities that I just mentioned.

[Robert Adamove] Number six, how has the internship changed since the first time it ran in the fall of 2020? Let me think about this one for just a second.

[Robert Adamove] I know that it has changed in the fact that we're looking at growing the program. I know at first it started with KapCC. I believe the last two semesters have been ran through the Mānoa campus.

[Robert Adamove] We also are looking to expand throughout INDOPACOM. We had involvement with the University of Guam this year and received an applicant from there. And also we want to refine the research that's being done, try to make it more infrastructure data related.

[Robert Adamove] Dr. Arnold has more details regarding that, but I've been building out a project management plan for the upcoming semester and the schedule and make it more hands-on for the students. I think both the students can benefit from more hands-on, experience, the experience, knowledge that Dr. Arnold can share in that regard. And then also we can try to have the students work on particular topics of interest to the Department of Defense and we can pull them for those topics that they would like the students to work on. That's my answer for number six.

[Robert Adamove] Number seven, from your perspective, has this internship produced the original expected outcomes? The answer is yes. We have grown it, but again, can only work on continuously trying to improve it and expand it and make it even better.

[Robert Adamove] I do think that we have shown the students and the interns some of the opportunities that exist within the Department of Defense and specifically on the island of Hawai‘i. Hawai‘i is very unique in the fact that all branches of the military are there on O‘ahu and has many opportunities. Like I said, getting all the positions in the new field is critical.

[Robert Adamove] And I think this was making the students aware of that attributes to success and helps them realize that there's opportunities for them to have a decent career that pays well and allows them to stay on island. And I think that's important as well. When it comes to what changes that we plan to make to the internship in the future, I've kind of already hit on that as well and making it more data centric and hands-on as well as expanding it to Guam and other potential opportunities.

[Robert Adamove] Like to get more involvement from the NIWC leadership. Hopefully funding will come through to allow for more positions for those top students who are identified to get future opportunities. One of the things that I think is beneficial is while in school and first learning about some of the cyber programs and the cybersecurity and opportunities that exist.

[Robert Adamove] By speaking to our guest speakers, our instructors, the students themselves might get a better feel for areas that interest them more than others. And I think just as importantly, learning what you like, it's just as important to learn what you don't like. So you don't necessarily continue down the path further and further to realize, oh, I got to backtrack or turn around.

[Robert Adamove] Hopefully we help people identify their interests so they can be on the right path from the beginning.

[Robert Adamove] And then for number nine, from your perspective, what are some obstacles experienced by NIWC applicants? I would say USA Jobs is not the easiest application to navigate your way through. There's certain nuances behind it and it's rather lengthy.

[Robert Adamove] If you've never dealt with USA Jobs, it can be a little bit daunting and overwhelming and just navigating your way through it. So if there's an easier way to do that, that'd be great. One of the things that we have done in the past, and I hope to continue to leverage in the future is having students or interns provide me a resume that I know they work on with Professor Stevens.

[Robert Adamove] And then I pass those resumes on to NIWC leadership so that they can take a look and become a little bit more familiar with the interns as well. Hopefully that answers the questions. Let me pause and see if there's any follow-up questions or comments by you at this time.

[David Stevens] No, thanks. You were super thorough and I'm just kind of chuckling to myself about your comments regarding USA Jobs because that was one of the things that Curtis, Dr. Arnold brought up and I totally agree. I have dealt with USA Jobs before.

[David Stevens] Being somebody who's worked for the DOD and the military, it is daunting. I mean, you used eloquent and delicate words to describe USA Jobs.

[Robert Adamove] If it helps to build on that, the amount of time that it takes.

[Robert Adamove] USA Jobs is a very lengthy process. Most of the time, even hearing that your application was selected for further review can take up to like six months, let alone how much longer it can take to actually get an offer letter or be hired. And then also another perspective that makes for obstacles is always funding.

[Robert Adamove] While the need exists, the government process of securing funding for positions is also a really lengthy process. So a lot of government positions are lost to contractors and the fact that a person who needs employment may pursue commercial work or contracting work while they're waiting for government, but after they're in the system, why would they want to wait and wait and wait? So the amount of time can hinder the government in causing this sometimes leads very qualified candidates to other programs.

[David Stevens] Yeah, I completely agree.

[David Stevens] I think that's USAjobs.gov is a prime example of what it's like when somebody works for the state or federal government takes an existing process and moves it to the internet and they don't consider the ramifications of that process. You can't just put the paper in an internet form and have it work. And I agree with you, the amount of time is just ridiculous.

[David Stevens] There's no sense of urgency, I don't think to move processes forward. So frequently our graduates become contractors and it's quick money, it's more money. And even if they only work six months out of the year, they're making the same as they make with NIWC.

[David Stevens] The only problem is they have to create their own retirement account, right? So I agree with you. Thank you for your time. And I greatly appreciate you participating in this effort.

[David Stevens] And as I said before, I'm gonna get it back to you so you can see how I summarized your comments. I'm here to make this internship fantastic. That's my goal.

[David Stevens] However, we need to collect the real data and make an objective assessment of how we're doing. So like you said, we can practice continuous improvement. So I'm excited about this opportunity.

[David Stevens] Thanks for participating.

[Robert Adamove] Thank you as well. I hope it helps.

[David Stevens] I'm gonna stop the recording here.

[David Stevens] And the recording is in progress. Okay, looking at these questions, starting with number one, why don't you just cover the history of this effort and NIWC from your perspective, as you remember.

[Steven Singer] As I remember.

Yeah, that's the caveat.

[David Stevens] I'm telling you, we've got to go back to 2019.

[Steven Singer] Thank you. I was going to ask for that, too.

[David Stevens] Yep. 2019 is when we're going back to.

[Steven Singer] Well, the whole thing, I believe, for internships in general for the IT program has been to find places for our students in the final semester of their studies to do an internship that would then, with a high probability, lead to a position in the industry in that particular sector of IT. Because we've always had, the IT program at Kapiʻolani has always had an advisory board that has been used for, as you would suspect, advice, you know, on how we're doing and how the industry is going and that sort of thing. We have tended to try to pull possible hosts for our interns from the advisory board because that kind of, it strengthens the relationship, you know, we have with them.

[Steven Singer] When the opportunity came up for a closer relationship with NIWC, it only made sense to me that we kind of take advantage of the situation, you know. Students like to be paid. Who doesn't? Maybe me, not so much, but I'm different.

[Steven Singer] But most people, when they're younger, want to be paid. I get that. I truly get that.

[Steven Singer] They want to be compensated just for what I feel that they have value, you know, worth. And plus, hey, they have bills to pay. So, and NIWC was very interested in not only bringing the students on with pay, but also providing them with specific kinds of instruction, with training in particular areas.

[Steven Singer] Well, for them, in this case, cybersecurity, that would make them even more desirable in the industry. And to me, it was like, wow, this is a great opportunity for students. I think early on, I was at that point still teaching in the internship, but you were the cybersecurity contact, Dave.

[Steven Singer] So I was like, okay, this is an opportunity for us to work together and get these people in. I'm not sure. Did I answer your question?

[David Stevens] Yes, you did. And you brought up a really important topic that NIWC actually asked to be part of our advisory board.

[Steven Singer] Yes.

[David Stevens] Yeah.

[Steven Singer] And that just made perfect sense. Yeah. I mean, seriously, it made not only perfect sense for them, but also it kind of, you know, it jived with what we were doing already and kind of what we're thinking about doing in the future is like, yes, this is exactly what we want to do because we can kind of see, you know, if we could do this with NIWC, and in particular, in this case, cybersecurity, we might even be able to do this with other, you know, sub-sectors of the IT industry, say with data analysis or networking or whatever, whereby we get a group of a single organization or a group of organizations to support, to underwrite, you know, these opportunities for our students.

[David Stevens] Correct me if I'm wrong, the internship class that you had prior to NIWC coming aboard and creating this internship. That's the class that we use as the template to engage the NIWC participants. So the NIWC candidates would have classroom exercises where they'd learn cybersecurity from NIWC instructors.

[David Stevens] But also on the other hand, in our internship classes, we would have them create a LinkedIn profile, create a resume, do a mock interview, do certification research, you know. Find out if they actually wanted to be in this industry or if they should run screaming. But these are important skills that we added to an internship that was industry-experienced focused, right? Which in this PhD, in this dissertation that I'm studying, actually, I'm emphasizing the fact that we had an industry experience-focused internship that also provided soft skills and professional development.

[David Stevens] But I think I attribute all of those tasks to you. And I wanted to ask you specifically, how did that come about? Because that was in our IT program anyway, before we even started this. That's an important piece of history.

[Steven Singer] Okay. Well, okay. I'm going to go in before I was doing internship, okay? We had Sandra Lai, Professor Lai, and Kevin Yokota after her, even, that taught internships.

[Steven Singer] And the things that they did that I liked were the idea of writing some short papers. They had them do, let me see, I'm trying to get, they do, I can't remember, I can't remember, they had them write, it wasn't dealing with certifications, but it was kind of like, where do they see themselves in five years kind of thing. And I liked that idea of introspection.

[Steven Singer] And they also had them do the journals, weekly journals. And I thought, again, introspection, because I've always believed that one of the things that is sometimes missing in educational programs is that metacognitive aspect, whereby they try to step outside of what they're just doing, doing, doing, and try to understand what does it all mean? Where is this

going? How does this all fit together? And I thought journals were a good way of connecting those dots, so I took that from them. I took the journals, and then the short, they had one short paper about where do they see themselves in five years, and I said, okay, I want to expand that.

[Steven Singer] At a couple of conferences I went to, and at least one other like volunteer project, I was involved in doing these, you know, speed dating kind of interviews. I liked that aspect. I wanted students to be exposed to people in industry, and I want people in industry to be exposed to our students, to get a feeling for who they were.

[Steven Singer] But I didn't want this to take an enormous amount of time. I thought first, when we were having, you know, face-to-face advisory board meetings, that I would just attach it to that, and that worked fine, whereby I would have students do three interviews, you know, 15 minutes, go, next, next, next. And I thought that worked well, because it got them kind of exposed to new people, not the faculty that's in IT, and it got people in industry kind of exposed to them, and I think that was a win-win.

[Steven Singer] After we, because of COVID, we moved away from the face-to-face and got into more virtual type experiences. I thought, okay, let's take advantage of that. Let's take the interview process, and at that point, a lot of the first-level interviews were going Zoom anyway, and I said, look, we'll do Zoom interviews, and we'll do this just like you would with a prospective employer.

[Steven Singer] You would arrange a time and a day and set it up, and I made up, I researched, looking on the internet, different kinds of interview questions to ask, different kinds of rating systems to make, and I made up my own based off of what I could pull together and sent it out to the students so they knew exactly what they were being assessed on and gave it to the advisory board members and other people who were doing the interviews, so everybody kind of knew what was, you know, what they're going to be graded on, and I think that is a good experience. Then, because as a group, as a faculty, we had, I think we decided pretty early on, and I worked on this with the curriculum, on developing these specialties within the program that basically led to certifications without really teaching to the certifications. Later on, we did add that component as well, because for some students, that was helpful.

[Steven Singer] They needed help in just how do I take the dang test, man? I'm not familiar with it, but earlier on, I just wanted them to have the skill sets for that particular certification. Then, okay, well, let's have the students reflect upon that. Again, write a short paper.

[Steven Singer] What kind of certifications would you like? Then, add it on to that, because I had been working with different organizations. I'm not sure how detailed to go here, but organizations to donate money to our foundation account, that we could then use some of that money to reimburse students to get those certifications. I thought, hey, here's a really nice way.

[Steven Singer] The curriculum has been modified. We have these short little certs within KCC. It would help students get the necessary skill set to take a cert in Network Plus, Security Plus, whatever.

[Steven Singer] Then, we tell the students, hey, do a good job. We'll reimburse you for this. That was kind of incentive.

[Steven Singer] I mean, how nice to me. How nice would it be to be able to restore? They are community college students. A lot of them don't have the means by which to pay for all this stuff.

[Steven Singer] It's costly. I said, hey, let's do that. I added that to get the certifications.

[Steven Singer] We had the interviews. We did the certifications. We did what else? What's next? Help me out.

[David Stevens] That about covers it. We have people research certifications and say why they want to do that. They research career options and what it takes to get there, what certifications are required.

[David Stevens] We have them do a lot of research, mock interviews is another one. I like the social media profile we make them get for two reasons. One, they got to have a professional profile, and they got to see how to do that.

[David Stevens] Two, it helps us contact them afterwards. We were losing a lot of people.

[Steven Singer] That's a win-win. I agree 100%. Mind you, at some point, some of these people, as you mentioned in another conversation, kind of fall off the radar for various reasons, security, et cetera. In general, it helps us stay in touch, know what's going on.

[Steven Singer] All we have to do is kind of plug into the social media thread, and we can figure out where they're at and what they're doing. It is really, really nice to see where they're going. I will confess to being a lurker of sorts.

[Steven Singer] I will sometimes look at people, and I just smile, seriously. I just look and see, okay, they're here, they're there. That's really nice.

[Steven Singer] I'm glad. I'm always glad that they're progressing. They're moving forward.

[Steven Singer] It's positive. Sometimes people move at different speeds. That's going to be the case always, but they're still moving ahead.

[David Stevens] I think we've covered question one through four. Okay. This is great.

[David Stevens] Let's move on to question five. This is important to analyze outcomes and expectations. What were your thoughts about the outcomes of the internship as it originally was intended?

[Steven Singer] Outcomes for whom?

[David Stevens] For the students, I think.

[David Stevens] What were we trying to achieve for our students with this internship?

[Steven Singer] For those students who are getting into the NIWC internship, one, I know they wanted to get money. They wanted to be paid for internship. You're paid to study.

[Steven Singer] How great is that? That's getting a grant of sorts. I wanted them to get money. I wanted them to feel good.

[Steven Singer] Two, sometimes people don't know what they really want to do in life until they start doing it, at least a little bit more. I always think it's best that students get that exposure as soon as possible so as not to waste any more time, any more of their valuable time. I thought this was a good opportunity for them to get a little bit deeper into cybersecurity.

[Steven Singer] Three, obviously, it's always nice when these internships lead to positions. As we had originally structured it, there's going to be a two-part internship. One part, it was open to everybody, pretty much.

[Steven Singer] The second part, students would get a security clearance or a temporary clearance to be able to go on to, I believe, PEARL. Is that right? PEARL, to be able to do some work. It's still with NIWC.

[Steven Singer] It would just be a step up, and then that just kind of led into positions with NIWC.

[David Stevens] I remember that was the original intention. Phase two was supposed to be a Joint-Base Pearl Harbor Hickam.

[Steven Singer] Yes.

[David Stevens] I remember that.

[Steven Singer] That was looking good. One of the things you recognize right away was that, although this was happening at Kapi‘olani, we had other programs in other campuses that also had IT students who were studying cybersecurity, and this would work for them as well. Why not have an internship that was pan-campus? NIWC provided that format, and I think from that, we also considered, hey, if we can do this with cybersecurity, we might be able to do this with some other disciplines as well, which I think really is still the way to go, but it takes a lot of work.

[David Stevens] I have great hope for this.

[David Stevens] We'll see what comes out of my dissertation and who reads it. Hopefully, it's going to be used in a grant solicitation eventually, because I hope to get good data out of this. This supports our efforts, and it's looking that way so far.

[David Stevens] How has the internship changed since 2020? I know you retired last year, but you saw three years of this.

[Steven Singer] Again, the main thing, I believe, is it's being more embraced by the other UH system campuses. While it started off at Kapi ʻolani and went to Honolulu, hey, we've got it at Mānoa, which is often called the mothership, and this kind of goes, hey, if they can embrace it and we can do this at multiple levels, I think we have it now as students taking this as a 200-level class and a 300-level class for Mānoa students, and they're getting credit for the same class, a little bit different work, but it is the same class.

[Steven Singer] That is wonderful. Seriously. I really had not expected that part to happen.

[Steven Singer] I really did not think that was going to happen. It has happened. I think as this gets more publicized and more out there, I know the pandemic threw a big wrench in the whole thing, but as this gets more publicized, I think this is something that can be presented to other sub-industries within IT, as I mentioned earlier, the data analysis for one, could be networking even for another one, the cloud, virtual, setting up virtual networks and servers.

[Steven Singer] All this stuff has potential that we can really get a small group of people to help us with, and they would get the opportunities, cream of the crop, as it were, and it would not cost them that much. I'm sorry. It would be well worth it.

[Steven Singer] Plus, if they do pay a little something, they got skin in the game. They're going to try their best to make sure these students are exposed to the relevant ideas and tools. That's what I want students to have.

[Steven Singer] I want them to have this kind of exposure. I still think this has great potential. I hope it really does blossom more.

[David Stevens] Yeah, me too. I think we're seeing that in the shift to the Pacific from the Navy and asking us to include Guam in the next iteration.

[Steven Singer] Hawai ʻi has always done a lot of work with Guam.

[David Stevens] Yeah, I'm excited about it. We're going to have to write another paper on this when we see how this pans out, because I just heard this morning we might add Palau.

[Steven Singer] Oh, okay.

[David Stevens] We're going way west and way south. The entire Pacific is in our scope now.

[Steven Singer] These are the natural connections for Hawai ʻi.

[Steven Singer] Because for a U.S.-based organization, Hawai ʻi is a natural place. I'm very happy to hear this is going to transpire. This would be good.

[David Stevens] Yeah, I'm very happy about it, too. I'm very happy about some of the results we're getting back and some of the student surveys. Let me ask you question seven here.

[David Stevens] Let me just formulate this question a little bit better. Did we check any boxes on our outcomes? What did we achieve, really, from our original outcomes? Did we achieve the deliverables we'd hoped for?

[Steven Singer] Well, I think so. Again, we have students who are getting exposure, getting their feet wet in a particular part of the industry and discovering whether or not it's a good fit for them.

[Steven Singer] For some, it is. For some, it's not. That's good to find out.

[Steven Singer] As an aside, I have a niece who has just graduated from med school and now has decided she really doesn't want to be a doctor. I go, really? Couldn't you have made this discovery about seven years ago? And saved yourself and the family a whole lot of time and money? Anyway, so now she's back to square one. I had no idea.

[Steven Singer] Did we reach deliverables? I think so. I think above and beyond, especially if we can expand this, this can become a template for other sectors. I think this can be something.

[Steven Singer] Because Hawai ʻi is not that big. It's big enough to be able to start requiring collaboration, but it's not so big that it makes that collaboration impossible. We're right here.

[Steven Singer] We're all in the same time zone. Come on. I think the state can do this.

[Steven Singer] That's got to be seen, but I think so.

[David Stevens] I think the last two questions might not be relevant to you. Question eight, because I mean…

[Steven Singer] I'm not teaching.

[David Stevens] …and question nine, because I think that's more geared towards the NIWC instructors. But we've shifted this internship now to an unpaid internship, and we've seen a dramatic 50% so far reduction in applicants. So we're going to have to do further studies to find out what's going on there.

[David Stevens] But different students have different motivations. So we're going to have to...

[Steven Singer] So this is decided by NIWC?

[David Stevens] This was decided by the Navy.

[David Stevens] Okay. The interview is over, so I'm going to stop the recording.

Follow-up Interview Questions

1. Can you describe any specific challenges or barriers you encountered during the process of applying for a cybersecurity position after completing your internship?
2. How aligned do you feel the skills and experiences gained during the internship were with the job opportunities available after your internship?
3. What were the most significant factors that influenced your decision to pursue or not pursue a cybersecurity career after completing the internship?
4. In what ways, if any, do you think the internship program could better prepare participants for cybersecurity roles?
5. What type of support or guidance, if any, would have encouraged you to apply for a cybersecurity role at NIWC following your internship?
6. Do you feel the academic portion of the internship program (i.e., resume creation, career research, etc.) helped you find a job after graduation or helped you advance in your current career?

Follow-up Interview: Participant 1

Note: this internship participant did not want to be identified in this interview. Any information regarding specific employers or areas of residence has been omitted in this transcript.

[David Stevens] Do you mind if I record this interview?

[internship participant] No.

[David Stevens] Great. I'm recording because I'm going to put all these transcripts from the actual conversations in the appendices in my dissertation so that if somebody wanted to evaluate our conversation more effectively, they could just read the transcript, right?

[internship participant] Okay, sounds good.

[David Stevens] Okay, I'm going to start you off with the first question.

[David Stevens] I'm going to paste it into the chat as well so you can keep track of the questions too. There's the first one. Can you please describe any specific challenges or barriers you've encountered during the process of applying for the cybersecurity position or any cybersecurity position after completing your internship?

[internship participant] Yeah, so I guess the only one would be just lack of industry certifications. I know a few people wanted me to have my CSSP, I believe it was. That and then a few wanted like some practical pen testing, you know, like hack the box type things. Other than that, I can't think of any specific challenges or barriers.

[David Stevens] Okay, so can you tell me what you did after the internship? Yeah, certainly. So, let's see, I did the internship in [not identified], I think. Gosh, I, yeah, I think it was [not identified]. And that following semester, I worked as a grader Sorry, can you still hear me okay with that background noise?

[David Stevens] Oh, yeah. No, I can't hear the background noise at all.

[internship participant] Okay, great. So, after that semester, I worked as the linear algebra and differential equations. I believe it was <course not identified>. I worked as a grader for that course.

[internship participant] So, nothing, you know, specifically or strictly computer science related. Then the semester after that, I started applying to positions a little bit more seriously as it was my last full time semester. And, you know, not to internships, but rather full time positions.

[internship participant] And I did apply to a few, you know, security analyst positions. I was actually offered a job directly for <company not identified>, which is the company that was like the internship is kind of through them for NIWIC.

[David Stevens] Commercial partners. Dr. Adamove and Dr. Arnold both have that company on the side as an intermediary contractor with the Naval Information Warfare Center.

Yes. Okay. So, <company not identified>. I was moving back to <area not identified> on account once I graduated on account of that this is just where I'm from. Luckily, <company not identified>, actually has a place here and they did offer me a position as a cybersecurity analyst.

[internship participant] And because of the internship, I actually had kind of an in, I don't know if you would say like an in, but I was able to reach out to the HR person who I had been in

contact with for the internship. And they went so far as to create a new listing for me through their site. Anyways, for reasons unrelated to the job itself, I ended up declining that position and I became a software engineer at the <company not identified>.

[internship participant] But yeah, I would say that the internship was really helpful in that I got a literal job offer on data at the very least. Not to mention my current position was of course happy with that experience as well. So, that's kind of the course that I took after my internship semester.

[David Stevens] Wow. Excellent. Thank you for that. Okay. Let me get the next question here. Okay.

[David Stevens] How do you feel, I mean, how aligned do you feel the skills and experiences gained during this internship are with the job opportunities that were available after you graduated?

[internship participant] So, the internship was, I guess I would kind of mentally break it into two parts. There was our research that we did and then there were like technical lessons scattered throughout the semester. I think that the technical, the more technical lessons aligned really well with the job opportunities that I had been seeing.

[internship participant] You know, we definitely managed at least most of, if not, you know, like we had a great majority of the, you know, cybersecurity buzzwords that, you know, you see on every job requirements list. We had made it through most of those, which that was really helpful, you know, for talking points during interviews and discussing skills. I would not say that the research part was overwhelmingly helpful with job opportunities, specifically just because, I mean, you know, research skills and writing an extensive research paper.

[internship participant] It was definitely an interesting and great learning experience. However, you know, doing one really solid, really detailed research project, unless your research project happened to be, you know, really, really in line with one of the specific, you know, buzzwords, I guess, would be a way to say it for cybersecurity. That part didn't end up being super helpful, other than having a project to showcase.

[internship participant] But as far as the actual skills required for creating that research paper, they did not align as well as the skills that we obtained through the technical lessons.

[David Stevens] Okay. Do you think any of those skills are being used by you in your current position?

[internship participant] As far as research skills, not particularly. I ended up going outside of the field of cybersecurity and became a software engineer, so it's certainly not useless. I definitely used some of the ideas that we had discussed, and, you know, when I write code, I do consider things through the lens of writing secure code, of course. But something that has been very helpful, specifically, even though I don't use any, like, STIG analysis, like, STIG compliance, anything like that for my job, there's a lot of that language floating around me in my workplace, because we are government contract work as well.

[internship participant] And having had that experience, which just gets you to such a really wide array of cybersecurity skills, was very helpful in, I guess, contextualizing my environment.

[David Stevens] Well, that's good to know. Okay. So, I wanted to dig a little deeper into your pursuit of a career post-graduation. So, the next question, what were the most significant factors that influenced your decision to pursue or not pursue a cybersecurity career after completing the internship? You spoke a little bit about it, but can you go any deeper?

[internship participant] Yeah, absolutely. So, I am, just a personal, like, preference is that as long as my work is technical and challenging, I'm happy.

[internship participant] So, I definitely believe that I would have been very happy in a cybersecurity career just as well as I am happy now in my software engineering, the beginning of my software engineering career. It might sound kind of shallow, but, yeah, I mean, the only, like, difference, it just seemed the, first of all, the pay was about, like, $25,000 better for my software engineering position, which is pretty considerable. I would say that the cybersecurity position that I was offered fell a little bit below the mark as far as what the industry standard is.

[internship participant] And the company was simply unwilling to negotiate any aspects of compensation, whereas the other company that I did end up with, they were willing to negotiate compensation, they were a little more aligned with the industry standards, and at the end of the day, they were both technical positions that I would have seen myself being happy in.

[David Stevens] That is really good data. Thank you. I'm going to share that with them if you don't mind.

[internship participant] Yeah, I mean, did I mention, like, numbers specifically? Is that something that you would be looking for?

[David Stevens] If you'd like, that's up to you.

[internship participant] Sure. So, the position that I was offered from <company not identified> was an annual compensation of $75,000 base salary a year. They did have the opportunity for bonuses, but, you know, there were not enough specifics provided around that to where I felt comfortable considering it as part of the income and compensation package.

<company not identified> benefits were slightly better than my current company's. However, my current company offered me $92,500 straight off the bat with a $5,000 relocation stipend. Yeah, I mean, the 401k matching isn't as good as <company not identified>, but I mean, a nearly $20,000 pay jump certainly covers that.

[David Stevens] Yeah. Thank you for sharing those numbers. I just wanted to confirm with you that it's okay that this goes in my dissertation. The reason I'm confirming that is because it's going to be a public document. It's going to get published. So, these numbers are going down in the public record. Is that okay with you?

[internship participant] Is my name anonymous? Your name is anonymous if you'd like it to be, yes.

[internship participant] I don't mind you including the figures if it is anonymous, and I would prefer that you don't mention my current company's name. But other than that, the information is okay to go in.

[David Stevens] Okay. Good to know that's on the record. If I use those numbers, I will not mention your current company or <company not identified> then because I don't want people to be able to do any open source intelligence and zero in on your identity.

[internship participant] Okay. I appreciate that. Thank you.

[David Stevens] Yeah, no worries. Okay. Let me take a moment. Okay, good. I think this is a well-formulated question. In what ways, if any, do you think the internship program could better prepare students or participants for cybersecurity roles?

[internship participant] I think insight from both Dr. Adamove and Dr. Arnold on what, you know, maybe like a little spiel on what certifications from their experience have been valuable or not valuable for cybersecurity and recommendations on which certifications, if any, to pursue would have been helpful.

[internship participant] Other than that, maybe just like a few additional technical lessons. We did have quite a few of them, and they were like scattered throughout the semester. And I particularly enjoyed them and would have loved many more of them.

[David Stevens] Okay.

[internship participant] Other than that, just, yeah, I mean, I think both Dr. Adamove and Dr. Curtis, they both really knew their stuff. And Dr. Arnold, sorry.

[internship participant] They both really knew their stuff. And they were great, great resources, like being able to interact with them and, you know, get their input on your questions, stuff like that. That I found very valuable.

[David Stevens] Okay. The next question has a lot to do with the origins of the cybersecurity internship program that we created with the Naval Information Warfare Center. The original, I guess, context or mission of this internship was to create a potential employee pipeline, you know, a pipeline of employees for the Naval Information Warfare Center.

[David Stevens] We're trying to assess if that actually is a checkbox that we can check. And we don't know yet. So, we're asking around.

[David Stevens] So, this question has to do specifically with NIWC. What type of support or guidance, if any, would have encouraged you to apply for cybersecurity role at NIWC following your internship? You know, I would have to check. But I think I did apply to NIWC in Hawai ʻi.

[internship participant] Because originally, I was not going to be moving back to <area not identified>. And I was looking for a job on the island. And I'm pretty sure I did apply to NIWC there.

[internship participant] I'd have to double-check that to give you a certain answer.

[David Stevens] But let me interject a little bit more then. Did you use USAjobs.gov?

[internship participant] No, I did not. I went through the NIWC website.

[David Stevens] Okay. So, they don't, NIWC didn't make you go through USAjobs.gov?

[internship participant] Gosh. You know what? I know that I have a USAjobs account. Let me log in real quick. Sign in. Authentication app. Okay. Here we go. Okay. We are in. Just kidding.

[internship participant] Now it's asking me to create a profile after I logged in. Okay. Perhaps I will have to follow up with you for that.

[internship participant] Let me add a note. Follow up for to NIWC. And is that specifically to NIWC Pacific? Or does it matter if it was any NIWC?

[David Stevens] No, I think originally we started with NIWC Pacific, but we have included NIWC Atlantic. So, it would be either one. It doesn't really matter. I think it's the, you know, organizational wide need for cybersecurity workers that we were trying to advance.

[internship participant] Okay. Yeah, definitely. I will definitely get back to you on whether or not I did apply. I think I did.

[David Stevens] Okay. All right. This last question, if we're ready to move on.

[internship participant] Yes.

[David Stevens] This is completely selfish on my part. And you do not have to answer this if you don't want to, but I'd really like some feedback on this. You remember in the internship, you had a classroom portion, which was NIWC instructors, but you also had the other portion, the academic portion, which was with me. So, that's the last question.

[David Stevens] Anything that you did in the academic portion? So, do you feel the academic portion of the internship program, i.e., resume creation, career research, et cetera, helped you find a job after graduation or helped you advance in your current career?

[internship participant] Did you do that for students taking it at UH Mānoa?

[David Stevens] I did, except for one semester. Yours might have been a semester I didn't. Do you remember taking that?

[internship participant] No, I don't remember doing it.

[David Stevens] Okay. Of course. Well, you missed out.

[David Stevens] Yeah. That's all the questions I've got for you. I'd love to hear anything more you'd have to say about the internship, your experience, or how it might've helped you.

[internship participant] Yeah, absolutely. I really enjoyed the entire internship. And in fact, I recommended it to many peers.

[internship participant] And also, I would've done it over and over and over again if I didn't have courses I had to fill up my hours with. I feel like I could've done that internship 10 times and gotten just as much out of it each time. I thought that the instructors were really good at what they do.

[internship participant] They were very respectable. They had great answers to all of my questions. And they were really helpful and insightful.

[internship participant] Let's see. Yeah. It was my only experience as an undergrad doing any type of research.

[internship participant] So, it was helpful to have a project to point to like that one. Like the one that I did for that internship. Yeah.

[internship participant] Honestly, I thought it was great. I would do that internship again and again and again. I thought it was really cool to get exposure to presenting to a senator and a representative.

[internship participant] I thought it was really awesome to have access to people in the industry who knew so much. And yeah, I do think it was really, really helpful as a resume builder. I think it was helpful as an experience. And it definitely gave some good insight into the industry.

[David Stevens] Thanks for reminding me that you were there when we had a visit by Senator Mazie Hirono and Representative Ed Case, both from the U.S. Congress.

[internship participant] Yes.

[David Stevens] Good to know. I will try to arrange that again. That was quite a rock to pick up. That was a heavy load, getting them to visit us. Oh, yeah. Their schedules are busy.

[internship participant] I bet. I bet so. Yeah. That was definitely a really cool experience. I mean, that's not really something... Talking to people like that and getting that type of audience is not

something I would do in any of my other experiences. Not something I have done in any of my other experiences. So, that was very cool.

[David Stevens] Well, wonderful to know. And thank you for all this information. I'm going to write this up and I'm going to send the transcript to you, edited as you agreed that we could do, taking out some of the information you don't want to share. And I'm going to ask you to give me your confirmation that that could be published.

[internship participant] Absolutely. I will get back to you as soon as possible once I get that.

[David Stevens] Thank you. I'd like to graduate at some point. I appreciate your help being a fellow student. And congratulations on your career. And I'm sure our audience reading this transcript is not going to realize, but there's a hurricane nearby. So, please stay safe.

[internship participant] Oh, yes. Yes. Thank you. I appreciate that. And soon to be, congratulations, Dr. Stevens.

[David Stevens] Oh, yeah. I'm almost Dr. Dave. Thank you very much.

[internship participant] Awesome. Well, have a good rest of the day.

[David Stevens] You too. Aloha.

Later the same day, the participant sent me an email that provided more details regarding their application experience with the NIWC.

What follows is the body of that email:

David,

Just following up on the mentioned USAJobs application:
I could have sworn that I did apply to NIWC, however when attempting to log in to USAJobs it did not recognize my email nor my university email. I searched through my inbox for anything containing 'NIWC' or 'USAJobs' but did not find anything relating to a completed application, so I must have been mistaken.
I guess it goes without saying, given that I thought I had applied, but I certainly was open to applying for and working with NIWC, and I know that I did apply and reach out to their partner contractor (<company not identified>). It's definitely a head scratcher that I cannot find anything to support my claim that I did apply to NIWC.

I do however have one additional experience that may or may not be helpful to you: I did apply for the NSA CAE summer internship program. Unfortunately, it seems that the organizational structure they have to review applicants was somewhat lacking, as I had to provide the same

documentation for my application multiple times to separate entities claiming it was not part of my application (even after resubmission and confirmation of receipt of said documents). While I did receive a CJO (conditional job offer) for their SIPST (Summer Intern Program for Science and Technology) and CSDIP (Cybersecurity Directorate Intern Program). I was told both of these programs were in Maryland, and declined (all of this in Oct. <year not identified>), then in Jan <year not identified>, received an email from a NSA program in Hawai‘i about my processing for the internship, to which I replied in confusion, and they stated they had selected me as ‘a student they were interested in’ but had received notice I was not interested. Basically, I tried to get in with the NSA CAE internship in Hawai‘i, received acceptances to other programs not located in Hawai‘i, declined those, and then got some correspondence that indicated I may have been selected for the program in Hawai‘i after all…needless to say, it did not end up working out.

Hope this helps!
- [internship participant]

Follow-up Interview: Participant 2

[internship participant] Do you need me to turn on the video? Do you need me to turn on my camera?

[David Stevens] No, no cameras necessary. I'm just going to transcribe the audio file.

[David Stevens] We all set?

[internship participant] Yes, sir.

[David Stevens] Okay, I'm going to turn it on. Sorry. Close captioning. Okay. I just have a couple of questions to drill down into some more detail. And I'd like your feedback.

[David Stevens] This is kind of open-ended. I won't narrow this down to yes or no. I just really want you to dig deep. Tell me how you really felt about the internship program and your experience inside of it. And I also need you to know that I'm keeping this anonymous. So anytime any kind of identifying information comes up, I'll take that out of the transcripts, but I'll be saving the transcripts at the end of this.

[David Stevens] And after I edit them, I'll send them back to you for approval. So you know what I'm going to put in my dissertation. And you need to know that that's going to be published. So it's public information. So do you have your permission to record now?

[internship participant] Yes, Professor.

[David Stevens] Oh, super. Thank you. Okay, I'm going to paste the questions into the chat, and then I'll repeat them for the transcript. Stand by.

[David Stevens] First one in the chat there. Can you describe any specific challenges or barriers you encountered during the process of applying for a cybersecurity position after completing your internship?

[internship participant] Yes. I think after taking the internship with cybersecurity, that one we have completed. I think I'm getting more encouraged to go for the cybersecurity position. But in the real life, in the summer, I tried to apply for a cybersecurity position, but I think there's a lot of limitations, such as you have to, I think some require you have to have some certificate and degrees. And most of them require you have two, three years of experience.

[internship participant] I think that's the challenge to apply for a cybersecurity job.

[David Stevens] Can you maybe describe some of the things you tried and were discouraged to find out these things? Maybe some job application processes, some jobs you applied to, maybe some interviews you went to?

[internship participant] Well, yes. I kind of went to a few, the one virtual internship. I tried to apply a couple of positions with them, but I did an interview. But at the end, I think I only got a wonderful offer, but it's not really about cybersecurity. It's really about AI thing, like more like coding.

[David Stevens] So when you applied for the position, it wasn't a cybersecurity position? It was more of a coding position?

[internship participant] It's a few position is a cybersecurity position. Yes.

[David Stevens] Okay. Well, let's try another one. Okay. I'm going to put it in here.

[David Stevens] How aligned do you feel the skills and experiences gained during the internship were with the job opportunities available to you after your internship?

[internship participant] Oh, I think there's a lot of skills aligned to my... Actually, I have a current part-time job, and it's kind of an official job, but it's not... I'm in kind of like a network group, but we not only limited to network, we're doing some of the firewalls with Cisco, and also we have a cybersecurity team. I realized what we did in the internship, the project and basic theory, it's really helped to get me to easy to understand when they're talking about how the cybersecurity work in the real world.

[David Stevens] Interesting. So you do deal with some security functions, even in a network group?

[internship participant] Yes. Yes. I think the reason is the current, let's say, director in the company, he was in a network position. So he is basically in charge of all the teams, like a network team, cybersecurity team, and programmer. So he's the director, but that's why I think

he's involved in everything. Also, he tried to have more experience to do firewall setup, not just the application side. It's the Cisco servers firewall. It's actually a physical firewall too.

[David Stevens] Oh, the appliance?

[internship participant] Yes.

[David Stevens] Got it. All right. Let's do another question. It's in the chat here. What were the most significant factors that influenced your decision to pursue or not pursue a cybersecurity career after completing the internship? And if you could go into some detail, tell me a little story about your decision-making process.

[internship participant] Yes. I think before I joined this internship, I feel like I'm more like a programmer because I think in UH Mānoa, the most class is programming class. I mean, most classes are programming class. There's only, I think one or two is about data security.

[internship participant] And after taking the internship, I feel like for me, it's kind of open another door. Like, oh, in the computer science, there's not only one job is called programmer. There's also a cybersecurity job or career. So I really enjoy when doing the internship. And let's start from there. And I try to get my security class.

[internship participant] And yeah. And I think in the future, I will pursue the cybersecurity job for my career. Okay.

[David Stevens] Did you say you got the cybersecurity or the security plus?

[internship participant] Oh, I'm working on that. I did it. Working on it. Yeah.

[David Stevens] Okay. Wow. Good luck.

[internship participant] Yeah. I heard it's hard.

[David Stevens] All right. Here's the next one. In your own words, tell me in what ways, if any, do you think the internship program could better prepare students for cybersecurity roles? Oh, for the internship program, I think the most design for students is already best.

[internship participant] I feel like it is more like a research internship. If we can have a chance, have more guests and have some like a demo or drill practice in the cybersecurity relate, I think it will bring us more experience.

[David Stevens] More experience.

[internship participant] Yes.

[David Stevens] Can you elaborate on what experience?

[internship participant] Oh, actually, yes. I learned this because like in the server, I do get a chance to watch them how to work on the service room. And I did get a one time in the data center. How to set up. I think of this Linux and set up the service and how to use start and single setting for the firewall.

[internship participant] It's really interesting. I think it's on-hand practice is I think also is a significant experience for the, I think, for the new grad or student.

[David Stevens] Have you had a chance to do that in your new position?

[internship participant] Yeah, I have a chance to do the current part time job. Yeah. I think they just put me like because I am, I think they think I'm new and they say, hey, just do, just try, try, try, just play around. I said, OK, so I just do that.

[internship participant] Yeah, I do got a Dell and HP servers set up and they have also I learned they have like a remote remote function. I know an ad hoc for the Dell and HP servers. It's really interesting.

[internship participant] And yes, it's really, I think it's very different. Well, I compare what I learned from the school. I mean, also, I mean, they're still in school, but yeah, it's really interesting.

[David Stevens] OK, OK. This next one is kind of focused on the original mission of this NIWC internship. The original mission was kind of to try to make a supply chain, if you would, of new cybersecurity workers for the Naval Information Warfare Center.

[David Stevens] So this question kind of deals with that.

[David Stevens] What type of support or guidance, if any, would have encouraged you to apply for cybersecurity role at NIWC following the internship? Oh, I think the one encouraging me to pursue cybersecurity job in the future, I think is you, you do agree to write me a recommendation letter. That's really, really helped me to think, oh, I mean, I may have a potential capability to do the cybersecurity stuff, because I always thinking I'm not that smart, like everyone in the computer field.

[internship participant] So I don't have that much confidence. But at the end, you are really encouraging me to continue to do the cybersecurity career. I think it's most like a mental support, something. Yes, Professor.

[David Stevens] Well, thank you. I had a curiosity, though. Did you actually apply for a position with NIWC or?

[internship participant] Oh, I didn't. I didn't. I didn't apply the position for NIWC yet.

[David Stevens] Do you plan to in the future? If I get a chance, yes.

[David Stevens] And just out of curiosity, what's holding you back?

[internship participant] Oh, I think I'm a graduate should be next spring. And I'm trying to, uh, because, you know, I think I don't know if you remember, you read me a recommendation letter for the scholarship.

[internship participant] And I do in the scholarship right now. And they told me I can continue work on my master degree. So I plan to find the professors and read me a recommendation letter to do the apply for the master degree in next year fall.

[David Stevens] Oh, yeah, I'd highly recommend that. So you're talking about the SFS scholarship, the scholarship for service through the US Cyber Corps, right?

[internship participant] Yes.

[David Stevens] Right, right. We're both part of that. And great program. So when you get done with your graduate degree, you'll have to serve a number of years with either a federal, tribal or state or county organization or nonprofit.

[internship participant] And when you do that, do you plan to try to work for the Naval Information Warfare Center?

[internship participant] Of course.

[David Stevens] Oh, wonderful. Okay.

[internship participant] Of course.

[David Stevens] Okay. I was just wondering. Yeah.

[internship participant] Oh, thank you.

[David Stevens] Trying to find out why people are or not going towards NIWC after the internship.

[internship participant] Okay, because I think most students don't know how to apply to the NIWC position. At least I don't know how to apply position to the NIWC.

[David Stevens] So you've never been given any guidance on how to complete an application to NIWC?

[internship participant] Yes, we do have an internship. We do have a meeting with NIWC. I think the director, I forgot his name. And there's a guest. I do have their email, I think a NIWC email. But I feel like I'm afraid just email them. Hi, can I apply a position or something? To stream or not? Not respecting. That's why. Yeah, they didn't really talk about how to apply a position to NIWC.

[David Stevens] Oh, that's too bad. That's good information to know, though. So we're always striving to improve. So this is great information.

[internship participant] Thank you for that feedback. Just so you know, to get into NIWC or any government organization, really, you have to go through a website called usajobs.gov.

[internship participant] Oh, okay.

[David Stevens] And I'm not going to tell you what kind of experience it is, but I'm not going to tell you it's great.

[David Stevens] But when you go there and start working with it, you might need some assistance.

[internship participant] Okay.

[David Stevens] But I did not know that you didn't know about that site. So that's good to know.

[internship participant] Got it.

[David Stevens] I've got one more question for you.

[internship participant] Yes, Professor.

[internship participant] And this has to do with the academic portion of the internship, more the resume creation and career research part of the internship, the part that I taught in my class.

[internship participant] So this is the question. Do you feel the academic portion of the internship, like resume creation, career research, etc., helped you find a job after graduation or helped you advance in your current career?

[internship participant] Of course. I think this is significant help. It's really help. That's why I know how to run my resume. I know how to work professionally in my current part-time job.

[internship participant] And yeah, they was wondering how do I like it? They seem like they know I'm a student, but they seem like I'm like a work. I have years or certain years of experience because after taking your class, I know how to dress professionally and behave professionally.

[David Stevens] You think it helped you?

[internship participant] Of course.

[David Stevens] That's how that's good.

[internship participant] Yeah. And they told me they read my resume and that's how they got me.

[David Stevens] Well, that's great. Can you give me a couple more examples? Maybe I just dig deep.

[internship participant] I don't know how to. Yeah, I think the one apply for the position. There's a lot of UH students. I think I got this is from a UH email. I found out there's a position, so I applied. They told me there's a lot of students try to apply for this job. And this, so my resume is really make attention from them.

[internship participant] And they call me, see if I want to do an interview. I say, OK. And I went there and we talk about it. And they said, I feel like I'm a. How to say behavior person like a like a professional one. I say, OK. And they say, if you want to come to work and we discuss in the time and and the payment, something.

[internship participant] And I start my current current position. And after one or two, I think after not just one, the one month and they call, they take me to the director, take to me his office and increase my salary by five percent.

[David Stevens] Really?

[internship participant] Yes. He said, yeah, he's he's. I think they're looking for someone. I'm not saying I'm a really good, but I think the class I was taking from you is really educating me how to, you know, email resume.

[internship participant] How do you work? How do you perform in the workplace is really helping me. And, yeah, they. They did increase my five percent. Yes, that's making me very happy. Right.

[David Stevens] That would also make me very happy. I understand.

[internship participant] Thank you. Yeah, I don't know. Yes, I don't know how other students think, but it's really I feel like it is really helpful. It's really, really helpful. In the real world.

[David Stevens] That is great information. Thank you.

[internship participant] Yes.

[David Stevens] In a couple of sentences, maybe, I don't know, a couple in our last minute or so. Yes. Can you just explain your feelings about the internship? Give me a little bit more about how this helped you succeed. How you felt is a positive experience, negative experience. You needed more.

[David Stevens] What could we do to make it better?

[internship participant] Yes, professor, I think this internship is a really direct students' attention to the cyber security career in a huge one. We are most students. I think they just in a general track in the computer science.

[internship participant] Only few people know they can in the cybersecurity side. No more. I think an eighty five percent of them in the general track, even me.

[internship participant] So they don't know what they really pursue. Maybe they just know all we're going to in our computer science field, but they don't really know what they're going to get data or programmer or cyber security. I think these programs really help.

[internship participant] People, students to build confidence and lies in open eyes to know all the cyber security is really good, have a really good future and can help the society. Communicating government is really is really important for our our country even in. For the internship also, I think if we can have more guests have a real real demo or real practice can bring more experience for the students.

[internship participant] They can more understand what is cyber security does. And I think they will help student more understanding what is security, cyber security, and I think more and they can from there and they can decide to pursue the cybersecurity or not. Yes, professor.

[David Stevens] Fantastic information. Thank you so much for your time. And I really appreciate that you just hopped on a call with me on the same day I emailed you.

[internship participant] No, I'm already appreciate. I don't got a chance. And that's why I really appreciate your you was guide me and like a mental sport and help me. Yeah, I was. Yeah. Before I meet you. As I was, I don't know if you know, I was in the <not identified>, so I still in the transition. I can, yeah, not really. Yeah, not really know what I do.

[internship participant] But now I think you really helped me to be with a confidence in everything, making me know what I can, what I will do. But yeah, because I because I after registered the class, I realized I'm in your class. So I'm afraid to say that I appreciate your help or something.

[internship participant] And just in case you think, oh, because I'm your student and try to get some like good grade or something, I don't really got a chance to say thank you to you.

[David Stevens] Well, I thank you for that. And you use the key word, "confidence".

[David Stevens] Do you do you feel that after this internship, you have a greater degree of confidence or what we refer to as self-efficacy?

[internship participant] Of course. Of course.

[David Stevens] That's good.

[internship participant] Yeah, I talk to right now, I can in the cyber security team, what we have right now, I can even talk to them a little bit. I am confident to talk to them about some like stuff. Yes.

[David Stevens] Wow, that's that's great information. We really went into depth and thank you for that. I will get this transcript to you as soon as I edit it.

[internship participant] And I'll wait for you to say yes or no, you're okay with me publishing it. Because, you know, your interview is going to go down in history. And I promise to keep you anonymous. That was our original agreement with everybody. You're anonymous.

[David Stevens] So thank you again for your time.

[David Stevens] And good luck in all your endeavors. I wish you the best, and if you ever need help, please reach out.

[internship participant] Okay, thank you, Professor.

[David Stevens] Okay, Aloha.

[internship participant] Okay. Have a nice weekend.

[David Stevens] You too, sir.

Follow-up Interview: Participant 3

[David Stevens] Okay, here we go. Okay, I'm recording and just so you know, I'm recording this follow-up interview for my research, and my research is going to be published in a dissertation for my PhD, which means everything you say here is going to be published in the public space forever, and I just want to make sure you're okay with that, and I will send you the transcript of our conversation as soon as I edit it for anything that might be used to target you personally and identify you. So if you identify an employer, or a person, or a place, or something like that, I'll edit that out so the transcript in my appendices for my dissertation doesn't identify you, so you remain anonymous.

[David Stevens] That was our agreement, right?

[internship participant] Cool.

[David Stevens] All right, how have you been? It's been a while.

[internship participant] Yeah, plugging away, forever student.

[David Stevens] No, that's fantastic. I think I picked you out of the crowd because I know you are a unique individual. You have been through a unique journey, in my opinion, without really telling anybody what it was.

[David Stevens] You have a unique perspective, and because of that, I highly value your opinion, and I wanted to know your opinion of some stuff, and I have a basic five or six questions that I'll paste in the chat, but I would love you just, you know, dig into some detail. Tell me a couple stories and expand where you need to so I get as much out of this interview as possible, because I will tell you the first two interviews I did, I got some surprises, which were good surprises, but surprises nonetheless. All right, I'm going to put the first question up.

[David Stevens] Can you describe any specific challenges or barriers you encountered during the process of applying for a cybersecurity position after completing your internship?

[internship participant] Yeah, so, you know, I'm grateful to be having these experiences. NIWC was, of course, like the pinnacle, but I've just been really, like, struggling to understand the whole ecosystem. So, I took my roadshow onto LinkedIn to try and connect internationally and nationally with a lot of people so I can understand, you know, because I did some organizational culture consultations before when I was in grad school, and I needed to understand the cyberculture because it's kind of like a head-scratcher, you know, it's like, oh, there's no callback.

[internship participant] So, it's kind of like, is it a gated community? That's kind of the conclusion that I've drawn to, and I just went to this thing at HCC [Honolulu Community College], and I was talking to tech system recruiters, and yeah, I mean, it's even looking at all the stuff that I have, like, I have three associate degrees, one in cloud security, the first guy under <person not identified>, and then another ICS, and now another associate. So, I'm working towards the bachelor's, and I worked at this place, <organization not identified>, and I know my record is clean, but I just don't know what the secret is. So, I've been digging into it through, because I'm trained in <vocation not identified> management as well, and there is a notion that says that there's like a screening protocol, like a pre-screening protocol so that employers can strive to be best employers by embracing a workforce that's viewed as ideally balanced.

[internship participant] So, I don't think I qualify there, so I'm trying to find out what the qualifiers are, and looks like what I'm getting is clean record, prior security clearance, I'm over age <age not identified>, it's like, forget it, you know. So, that's kind of I shifted to data, and I can still, cyber is my first love, it will always be my first love, and that's where my passion is, I'm still like driving towards that, doing everything, but I also realize I may not be able to get in, and I just, I'm kind of baffled by that, but at the same time, I would, I would love to know if there's something in my, you know, record or something, or if it's just like maybe what those people are saying, where employers want that top rating, so they just ghost everyone off the protocol, because there's very few spots, so I don't know what's true, but it doesn't, it doesn't affect me, I'm just moving forward at the same speed, if not accelerating.

[David Stevens] So, this is very interesting, I have not heard this perspective before, that, and how would I put this, ageism might be an issue.

[internship participant] Well, it could, I mean, I was going to do a data science project, because, you know, I'm into the politics thing, and I got called off, because basically the data's out, it's like there's 6.7 million men, you know, education's a big deal when it's low, that are just like, they've given up, it's, in the 1954, it was like 2.3, now it's like huge, it's like 10.5, it's like, it's glaring that for some reason, this identified workforce out of, you know, Department of Labor, their stats is just showing a hard, kind of, for lack of a better term, kind of like a harm class in whatever process, so that could just be bleeding over into the whole cyber thing, but also what I've found out from, you know, hanging out with, with some, you know, some pretty, pretty heavy guys, I've been able to use my personality to befriend people, at least digitally, it's kind of like, they feel like people that have an existing clearance, it's easier for the employers to onboard, and because the, the wage in cyber went so far up, and there's this huge need, there, anyone that can just, like, do the exam dump with the existing clearances in there, and then, so the question is, the discussion is, does that affect mission performance, and it seems like, you know, it seems like there's a lot of data breaches going on, so, yeah, I don't know, to me, like, my perspective is that people with a passion should have some way to assist the mission, and what I have heard of, and why I'm, where I'm investing my progress now is, is with CISA, so they're, they're trying to start kind of like a CISA ROTC in the community colleges, and I'm hoping I can get qualified for that, because I would love to learn, you know, I'm, I'm a natural blue teamer, but with some real good red team instincts, but I, I need, I need mentoring and training, you know, and I'm just going out and just seeking it everywhere, so that's kind of my perspective.

[David Stevens] So CISA, the C-I-S-A, Cybersecurity Infrastructure and Security Agency, that's what you're talking about?

[internship participant] Yeah.

[David Stevens] Okay.

[internship participant] So I've been hanging out with those guys, like, getting all the training, getting, you know, getting my, my names in the, in the database, so to speak, I'm going to be doing, they're starting the awareness month, I'm going to be a part of that in terms of the webinar, and just absorb straight from the source, like, like what's going on, because, because there's a huge need, the White House is trying to pick up on it, so the thought process in the community is, so all these positions exist, yet, is that, do they exist not to be filled, do they exist to blow up budgets, do, you know, there's just a lot of people going around, it's even international, like, there's all this stuff coming up on how it's hyped, like, talking to people in India and stuff, and I'm definitely not being at the forefront, you know, I'm like, I'm part of the team, so I'm not trying to make, like, it's a bad thing, I'm just understanding and trying to assimilate, I'm a, I'm an adapter guy, so I will always adapt and never die, so I don't care what it is, I just like to figure out, you know, what's the best way in, and I thought that program is going to be really good, unless it, unless there's any truth to the, the pre-employment filters that, you know, could, could kind of pre-select on the hiring process, but supposedly, <name not identified> is picking this up, I got a friend, he's a big DC lawyer in there, and after the election, it's going to be like, you know, a way to kind of say goodbye, and it's fueled by, I guess, what happened with SCOTUS against Harvard, so it's this big thing that's bubbling, that's, I don't know, I don't know how, how much political stuff is, but I hope cyber is left out of it, because the mission is just so critical, you

know, so anything I can learn of, anything that's offered here, I'm looking forward to, you know, that 300 level security class, whenever, whenever that clears the plate, you know, doing whatever I can, I was going to ask you, like, so Cisco's having a CEH, you know, training, and I kind of have access to that, I was like, oh, hey, I gotta, I gotta ask you if you think that's, that's worthwhile, just to get the skills back up, I'm like all going into data now, so it's like, I want to keep the primary skills up, and then also, I'm also working to develop, I'm thinking, be part of the change, so, you know, the <organization not identified> is, it's here, I mean, who's, they got their <product not identified>, it's gonna go straight forward, whether that's gonna help the people that don't have the skills to, you know, keep the ZTNA networks going, or whatever it is, either way, we'll be better off, so I'm kind of embracing that, that edge of, you know, automation, and generative AI is just gonna be, I think, crazy on this, so I'm kind of, like, leaning my training more towards Kali Purple now, because I think that's gonna be that, and I got my certification as a applied AI professional through IBM, so I'm not trying to replace anyone's job, I'm just trying to have the skills in case things shift, where, you know, we're just gonna develop and take on, take on our adversaries, because they're doing it already, you know, and my other concern is, I think, the draw for all these people that feel locked out, they have skills, and there is money on the dark side of the force, and it's, like, it's a huge draw. For me, out of the question, I took my oath, even though it was a long time ago, but I understand it's for life, but as a patriotic American, I kind of worry, you know, what's on the other side, because a lot of kids are not financially secure, and with this talent, you can get, like, ransomware as a service, and, you know, with AI-assisted tools, it just, I think we're leading to a world of overmatch, not to mention the geopolitical tensions, but that's a whole other story.

[David Stevens] Yeah, yeah. Okay, let me give you the second question here.

[internship participant] All right.

[David Stevens] How aligned do you feel the skills and experiences gained in the internship were with the job opportunities available after your internship?

[internship participant] Yeah, so I don't know if it's my case specifically, but everywhere I've gone, in terms of local government, you know, I worked for the city, and I thought it was great, but I've also learned a lot about culture, and what the CIOs go through, and what they go through without the CISOs to burn. It's like, there's so much, you know, the thing is, security is like, it's like, the CIOs don't want to know, kind of.

[internship participant] It's like, if they're, you know, it's like, how are they going to explain that to their boss? And, you know, if you're stuck with these antiquated systems, and, you know, sweep it into the purgatory help desk thing, and hear no evil, see no evil, speak no evil, you know, we're infiltrated. I mean, I've done some looking around as a, where I could, and, you know, I have a strong suspicion that there's foreign APTs [Advanced Persistent Threats] that have infiltrated supportive government, and the first thing they're going to go for is infrastructure for, like, our location, because if you cut off the support personnel that supports the military in any way possible, that's how, it's all cyber kinetic now. I mean, our water system, I worry, actually, I see, to, you know, just run some shodan over there, see how it's, if anything's showing

on the servers, because, you know, I want to be part of the part of the mission, and not part of the problem.

[internship participant] And but at the same time, I think, I think, current leadership strategies, for whatever reason, at least locally, it's, it's unacceptable to me that you would, oh, we'll just, we'll just use jump boxes to make sure this, this other stuff. It's like, no. And then, you know, the pressure to keep everybody on remote when VPN is so insecure.

[internship participant] It's like, man, I just think, I think it'll just be a cakewalk in the first wave. And so my thing is, I'm going to be part of the cleanup crew that's already trained in, in AI, and we'll push back like there's a, it's not like a Pearl Harbor coming, but I do have knowledge, you know, how they how they put in the virtual network overlays, and the persistence. And, you know, those guys, CCP, it's a different, it's a different manpower training.

[internship participant] They're just like these guys from five years old with the talents that are just like, totally like as patriotic as we are. But this is all they do. They don't think about money, they think about the fame that goes with their, their mission, and they all work together.

[internship participant] And then they mercenary, they they'll outsource talent on the dark web. And it's like, we're in for a fight, man, you know, and I can't even, I can't even, you know, volunteer services to, to train. And that's not necessarily anyone's fault.

[internship participant] That's just the way the structure is. It's like, the giant’s asleep, man, you know, it's like, and I've been trying to wake them up. But what can one guy do, right?

[David Stevens] Right.

[David Stevens] Okay, third one, what were the most significant factors that influenced your decision to pursue or not pursue cybersecurity career after completing the internship? Okay, so like, I got out of <vocation not identified>, because it was, I did 25 years there. And it was the best choice to like, retire. And then I just looked, and I saw this thing.

[internship participant] I'm like, wow, cybersecurity is as higher placement than physicians on the need. So I like, I'm like, man, that seems rough. I'm going to try.

[internship participant] But then I started it fits my personality. My personality is that of like a family protector type person. So as long as you expand that rollout to the like national security, it's like perfectly fit.

[internship participant] So it will always be something I completely invest a lot of time into. And that's what drew me to it. What what's kept me to it is, it's just the passion to try and fit in and be part of the solution in any way possible.

[internship participant] So because I think it's just, it's just where we're there, you know, I mean, they're cybers on DEFCON 2. And every but, you know, the private industry supporting the public industry, there's so many gaps in there with and the data breaches, it's like, we kind of

need a better solution. So I'm hoping to be a part of that in any way possible, knowing that that's probably not going to be where it's at.

[internship participant] But so I'm doing a master's in DAE right now, simultaneously, because I think data is a future data is going to be what lasts. But I also feel like what happened to the programmers is it's going to happen in cyber because it cyber is a cost, you know, so if you can't get any value, and there's other options coming to the market, particularly, it's going to be like, DISA approved, it's like, I think, there's going to be a huge shockwave through the force. And I'm talking to a lot of old time guys that are already getting locked out and kicked out the door with a lot of experience.

[internship participant] So, you know, it's change, change sometimes, but I'm a lemonade guy. So it's like, there's no lemon sour enough for me not to, not to drink the juice from, I guess.

[David Stevens] Okay. All right. We're digging down here. This is great.

[David Stevens] Okay. Tell me in what ways, if any, do you think the internship program could better prepare students for cybersecurity roles?

[internship participant] So, you know, I was thinking about this. I'm like, man, I wonder what you think.

[internship participant] I think it's a great, it's like a great precursor, because, you know, like Curtis in particular, he really opened like my vision as to what, what the job really is, you know, it's like, wow, you know, you get a, you get a glance.

[David Stevens] And then I was…that was Dr. Arnold. Yeah.

[internship participant] Yeah. Yeah. Yeah.

[internship participant] And then, you know, Rob was great on the preparation of the paper stuff, but I just looked, I was just looking pretty much to Curtis, because I'm like that chameleon guy. So it's like, give me a mentor and I'll suck the blood out of them, you know, just in terms of trying to get the knowledge and, you know, that's just how it is. But I think it would be such a compliment.

[internship participant] I don't know. I mean, I don't know what, what your 300 level thing is, or what else is in the works. And I'm, I'm hoping you're, you're part of that conversation, but man, to kick that up as a precursor to, they say the CISA ROTC, particularly with our demographics, how we can pull in like a lot of like Asian speakers and stuff for signals INTEL it's like, wow, I think we're just, we'll be right there.

[internship participant] So I'm going to be trying to, trying to pick out information and see how fast that's rolling forward. And hopefully it's a really like a, a broad qualification, because that could be, you know, it could be a compliment to what, what, what you're doing now. And it's

like, cause CISA's they're like, they're kind of like, we're doing everything, you know, they're trying to figure it out too.

[internship participant] It's like, it's some kind of internal dynamic. Personally, I do believe it's a gated community and that that's not necessarily a bad thing, but I'm like, it depends if the lock gets rusty and, you know, everyone's got a duplicate key or, you know, who's getting through that gate. I don't know, you know.

[David Stevens] That's a good metaphor. Okay. Next one.

[David Stevens] What type of support or guidance, if any, would have encouraged you to apply for a cybersecurity role at NIWC following your internship? Oh, I would, I would, I would hop all over it. I, I, I've talked to those guys. I'm just not like the top candidate.

[internship participant] I'm like, oh, okay. I've done triple, triple the work of, of my peers and, you know, getting a second master's degree. I'm like submerged with like the movers and shakers in the field.

[internship participant] It's like, I don't know, you know, I know my record's clean. I mean, I just worked at, at <organization not identified> and the guys who run that, it's all good. So I'm like, I'm just scratching my head and I'm not jumping to any conclusions either.

[internship participant] I'm just like, oh, for whatever reason, my path is to wait. So I'll wait and just keep, keep working on that. But I would love to work for, I would love to work for NIWC.

[internship participant] I would love to work with any type of, you know, hands-on experience just to, just to put the academics into use. Cause without experience, it's kind of, it remains academic, you know.

[David Stevens] Have you created a profile on usajobs.gov by any chance?

Yeah, I, I actually went, went through all those guys and it's, it's the same thing.

[internship participant] It's like, it's like the ghost wall comes up and then I'm just not, I'm, I'm a busy student and doing all kinds of, if I get a ghost wall, like I won't ever apply for another position again, unless somebody asked me to. Cause then I'm like, okay, that's keys to the city. They're not offering you the job, but they're saying you should apply here.

[internship participant] It's like, okay, that's, that's worth my effort. You know, even like with <person not identified> and, and his thing, I mean, he's having limited success filling, filling the roles. It's like, you know, he's having limited success getting internships, getting, getting his people place.

[internship participant] And of course he's going to try and take care of the <group not identified> first. So, you know, I'm, I don't know if Maui's still going, but I'm, I'm on this, working towards that short list to jump as soon as that APC's done, or maybe even before, you

know, I'm going to be jumping over, over to West O‘ahu and, you know, get some seat time with those guys and just, just go from there, you know, as well.

[David Stevens] Okay. Yeah. Maui's still going, by the way.

[internship participant] Oh, it is.

[David Stevens] Yeah. Yeah.

[internship participant] Okay.

[David Stevens] You can do, you can do your degree over there too.

[internship participant] I know it's preferable. It just was a shorter route and it seemed, it seemed like because of the curriculum over there, they kind of mimic that <institution not identified> thing where it's like, you got, you need to be here at least one day a week.

[internship participant] And I need to, you know, it's so old school, whereas the rest of the world has moved to completely, completely digital. And that's, that's, I love that training. I mean, you can do it at your, at your competence level.

[internship participant] And I think it's, it's at a premium and anyone can be trained so it's just, just in between, but I guess you got to get, do the degree hunt, got to get the bachelor's next. And that might be the path of least resistance for me as I work on the other grad level side.

[David Stevens] Yeah. UH Maui is a hundred percent remote.

[internship participant] Yeah. Oh, you know, the only reason it's less, my particular file, like <individual not identified> looks through my file and you know, it's, there's a lot, a lot more classes I'd have to take just to, just to meet the Maui reach.

[internship participant] I got like two bachelor's degrees from UH as it is, you know, I'm like gonna, I'm going to set the record. By the time I leave <institution not identified>, I will have literally every certificate and degree offered. And I cherish, I cherish the knowledge and the mentor, the mentorship and any opportunity to, to help or be part of the community or anything.

[internship participant] I'm like all over that cause you know, it's the big pictures and I have an island mentality. So it's like, you know, you bring to the family what the family can value. So.

[David Stevens] Full disclosure, with all those things you said, it's going to be hard to make you completely anonymous.

[internship participant] That's all right.

[David Stevens] Okay. Just want you you're one of the star performers. So it's, it's going to be easy to zero in on you with just a couple of data points in this conversation, but if you're okay with it, that's great. Cause I love having you around. It's, it's wonderful.

[David Stevens] Hey, our last one, this is, this is my kind of selfish question that I added in here. It's like, cause I teach the academic portion of the internship, right?

[internship participant] Right.

[David Stevens] Do you feel that that academic portion of the internship program, like the resume creation and the career research, et cetera, helped you find a job after graduation or helped you advance in your current career? I know you're still looking, but how can you describe that?

[internship participant] I would, I would love to have taken the NIWC after I took it. I don't know if there was the first one, but like Rob was in there doing most of the academics and, you know, I would love to, if you're, you're, if you're doing that role, man, I would be, I would like, love to take that again, even though it's not possible, but that's how highly regarded I consider your experience with that. You know, that would be a, that would be a great thing.

[internship participant] If they could let, have level two NIWC guys, man, I would be like beaten on the door to get in that one, you know.

[David Stevens] Oh, mahalo for that. Yeah. You know what, wrapping this up, just give me some, some of your like, your feelings, your, your conceptual picture, your perspective on the internship as a whole and how you regard it, this NIWC internship. Yeah.

[internship participant] So the NIWC internship made it real for me.

[internship participant] It was like, before it was like, oh yeah, I got to relearn all this stuff. It was kind of rough. And then it was like, oh, it's very interesting.

[internship participant] And then when I got in there, I was like, oh, and I, you know, you started getting invited to all these other things, like, like I'm there. They're like, oh, who is, who is this guy? Oh, that's that student guy. You know, it's like, it, it was, it just, I feel like it lit my, it lit the cyber candle for me.

[internship participant] You know, that whole thing was just like, I mean, I'm, I'm not even being compensated, but I'm totally staying on the cyber path and I'm not ever going to get off. Cause I think it's that important to learn those skills. I'm even getting a master's in data so I can be potentially better at cyber when, when the AISOCs are just like, like standard, you know, cause I think, I think we're, the, the flight's going to get pretty hot.

[internship participant] And I also, my, my, I think it really prepared me to look at things from the cyber kinetic evolution mindset. Cause what I find out with the old guys is they're like, oh no, no, no, we hit the keyboards. That's for special ops and stuff.

[internship participant] And I'm just like, oh, I'm just waiting for, you know, Tesla's to start taking people out and neutralizing targets, you know?

[David Stevens] That was in a movie. Yeah. That was in a movie. I remember that. Oh, was it in a movie? Oh, yes. It's actually in a movie. Yeah.

[internship participant] I thought the KIA is man, have you seen the videos on the KIAs? It's like, it's crazy. I think they, they plug that hole, but you know, it's we're, we're in a whole, we're in a whole new world and that's why it's like blue team is just going to have to rise to, I mean, you talk about expanding surface area, man, blue team's got their hands full already.

[internship participant] It's going to be crazy, but I want to be there to help whatever it's going to be.

[David Stevens] That is where most of the work is. Okay. I appreciate this. I'm going to wrap this up and then I'll stop the recording. Then we can talk a little bit more, but I just want to share one more thing.

[David Stevens] I am going to get this all edited and send it over to you. Wait for your response via email to say, yeah, I'm okay with that or not. And if you need any changes and then it gets put into the dissertation.

[internship participant] Yeah. If it, if it helps expedite the process in any way, I'll just, I'll give my clearance. I'm used to taking lumps for, you know, speaking my mind.

[David Stevens] Okay. All right. Let me stop the recording.

References

1. Henry, J. S., Rehwaldt, S. S., & Vineyard, G. M. (2001). Congruency between student interns and worksite supervisors regarding critical elements of an internship experience. Information Technology, Learning, and Performance Journal, 19(1), 31-41.
2. Coco, M. (2000). Internships: A Try Before You Buy Arrangement. S.A.M. Advanced Management Journal (1984), 65(2), 41.
3. Ritter, Barbara A., Erika E. Small, John W. Mortimer, and Jessica L. Doll. (2018), "Designing Management Curriculum for Workplace Readiness: Developing Students' Soft Skills." Journal of Management Education 42, no. 1: 80–103.
4. Smith, C, Sonia Ferns, and L Russell. (2014) The Impact of Work Integrated Learning on Student Work-Readiness. The Office for Learning and Teaching.
5. Knight, P. and Yorke, M. (2003). Employability and Good Learning in Higher Education. Teaching in Higher Education, 8(1), pp.3-16.
6. National Association of Colleges and Employers (NACE), (2021), 2021 Internship & Co-Op Survey Report.
7. Williams, C. (2010). Understanding the Essential Elements of Work-Based Learning and Its Relevance to Everyday Clinical Practice. Journal of Nursing Management, 18.
8. Benavides, Abraham D., Lisa A. Dicke, and Amy C. Holt. "Internships Adrift? Anchoring Internship Programs in Collaboration." Journal of Public Affairs Education : J-PAE. 19, no. 2 (2013): 325–53.
9. Harris, F. (2019). The Underprepared Cyber Workforce: A ticking Timebomb. Cyber Risk Management Journal, 13 (7), 100-105.
10. Khan, M. A. (2005). User Interfaces in the Digital Age. Information and Software Technology, 47 (1), 67-76.
11. Stevens, David. (2022) "Optimizing Visual Cues in Educational Software." In Augmented Cognition, 287–303. Lecture Notes in Computer Science. Springer International Publishing.
12. Gault, J., Leach, E., & Duey, M. (2010). Effects of business internships on job marketability: The employers' perspective. Education & Training (London), 52(1), 76–88.
13. English, Peter, Margarietha Johanna de Villiers Scheepers, David Fleischman, Jacqueline Burgess, and Gail Crimmins. "Developing Professional Networks: The Missing Link to Graduate Employability." Education & Training (London) 63, no. 4 (2021): 647–61.
14. Haddad-Adaimi, Marianne, Roy Abi Zeid Daou, and Yves Ducq. "Internship Assessment and Evaluation in Higher Education." International Journal on Integrating Technology in Education 11, no. 1 (2022): 17–33.
15. Hurst, Jessica L, and Linda K Good. "A 20-Year Evolution in Internships: Implications for Retail Interns, Employers and Educators." The International Review of Retail, Distribution and Consumer Research 20, no. 1 (2010): 175–86.
16. Martin, Chris, Chris Quillen, and Tim Shaw. "Lessons Learned from Intelligence Internships from Three Midwest Universities." Journal of Strategic Security 6, no. 3 (2013): 207–13.
17. Rorabaugh, W. J. The Craft Apprentice : From Franklin to the Machine Age in America. New York: Oxford University Press, 1986.
18. Sagen, H.B., Dallam, J.W. & Laverty, J.R. Effects of Career Preparation Experiences on the Initial Employment Success of College Graduates. Research in Higher Education 41, 753–767 (2000).

19. Manisha, and Manoj Manuja. “Industry Academia Collaboration Model: The Design Challenges.” In 2011 24th IEEE-CS Conference on Software Engineering Education and Training (CSEE&T), 111–20. IEEE, 2011.
20. Dawson, J., & Thomson, R. (2018). The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. Frontiers in Psychology, 9, 744–744.
21. Cojocariu, V.-M., Cîrtiţă-Buzoianu, C., & Mareş, G. (2019). Opportunities and Difficulties in Conducting Internships in Higher Education from the Employer’s Perspective. Postmodern Openings, 10(2), 1-27. doi:10.18662/po/69
22. Hora, M., Chen, Z., Parrott, E., & Her, P. (2020). Problematizing college internships: Exploring issues with access, program design and developmental outcomes. International Journal of Work-Integrated Learning, 21(3), 235–252.
23. Jones, F. R., Mardis, M. A., McClure, C. R., Ma, J., Ambavarapu, C., & Spears, L. I. (2017). Work-integrated learning (WIL) in information technology An exploration of employability skills gained from internships. Higher Education, Skills and Work-Based Learning, 7(4), 394–407.
24. Hodges, M. S. (2007). Computers: Systems, Terms and Acronyms, 17'th Edition. Winter Springs, FL: SemCo Enterprises, Inc.
25. Moore, B. (1979). Waiting At The Terminal. Journal of Academic Librarianship, 4(6), 443.
26. Brownell, J. E., & Swaner, L. E. (2009). High-impact practices: Applying the learning outcomes literature to the development of successful campus programs. Peer Review : Emerging Trends and Key Debates in Undergraduate Education, 11(2), 26.
27. Ramezan, C., Coffy, P., & Lemons, J. (2023). Building the Operational Technology (OT) Cybersecurity Workforce: What are Employers Looking for? Journal of Cybersecurity Education, Research & Practice, 2024(1).
28. Tsado, L. (2019). Cybersecurity Education: The Need for a Top-Driven, Multidisciplinary, School-Wide Approach. Journal of Cybersecurity Education, Research & Practice, 2019(1).
29. Bandura, A., & Walters, R. H. (1963). Social learning and personality development. Holt, Rinehart and Winston.
30. Bandura, A. (1977). Social learning theory. In Social learning theory. Prentice Hall.
31. Bandura, A. (1986). Social foundations of thought and action: A social cognitive theory. In Social foundations of thought and action: A social cognitive theory. Prentice-Hall.
32. Bandura, A. (1997). Self-efficacy: The exercise of control. In Self-efficacy: The exercise of control. W.H. Freeman and Company.
33. Bandura, A. (2001). Social cognitive theory: An agentic perspective. Annual Review of Psychology, 52(1), 1–26.
34. Anjum, S. (2020). Impact of internship programs on professional and personal development of business students: A case study from Pakistan. Future Business Journal, 6(1), 1–13.
35. Luk, L. Y., & Chan, C. K. (2022). Students’ learning outcomes from engineering internship: a provisional framework. Studies in Continuing Education, 44(3), 526-545.
36. Thombre, S., & Velankar, M. (2022). Quantitative analysis of comprehension and skill acquisition of engineering students from the cybersecurity virtual internship program. Graduate Research in Engineering and Technology, 18–26.
37. Cybersecurity of Critical Infrastructure with ICS/SCADA Systems—IEEE Public Safety Technology Initiative. (n.d.). Retrieved February 8, 2025, from https://publicsafety.ieee.org/topics/cybersecurity-of-critical-infrastructure-with-ics-scada-systems

38. Office of the National Cyber Director. (2024). Initial stages of implementation of the National Cyber Workforce and Education Strategy. The White House.
39. Payne, B. K., Mayes, L., Paredes, T., Smith, E., Wu, H., & Xin, C. (2021). Applying High Impact Practices in an Interdisciplinary Cybersecurity Program. Journal of Cybersecurity Education, Research & Practice, 2020(2).
40. Holyoak, L. (2013). Are all internships beneficial learning experiences? An exploratory study. Education & Training (London), 55(6), 573–583.
41. Urquía-Grande, E., & Pérez Estébanez, R. (2021). Bridging the gaps between higher education and the business world: Internships in a faculty of economics and business. *Edu*cation & Training (London), 63(3), 490–509.
42. Tetteh, G. K., & Otioma, C. (2024). Cyberattack, cyber risk mitigation capabilities, and firm productivity in Kenya. Small Business Economics.
43. Mailhiot, B. M. (2022). Entertainment Technology Internships in Community Colleges: A Behind the Scenes Case Study. ProQuest Dissertations Publishing.
44. Wolniak, G. C., & Engberg, M. E. (2019). Do "High-Impact" College Experiences Affect Early Career Outcomes? Review of Higher Education, 42(3), 825–858.
45. Seelye, J. E., & Selby, S. (2018). Apprenticeships. In Shaping North America: From Exploration to the American Revolution (Vol. 3). ABC-CLIO.
46. Miralles-Quirós, M. M., & Jerez-Barroso, L. (2018). The Interrelationship between Internship and Employability: A Critical Literature Review. Proceedings, 2(21), 1328.
47. Eagan, K., Lozano, J. B., Hurtado, S., & Case, M. H. (2013). The American Freshman: National Norms Fall 2013. Higher Education Research Institute.
48. Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. The Geneva Papers on Risk and Insurance - Issues and Practice, 47(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6
49. Ncubukezit, T. (2022). Human Errors: A Cybersecurity Concern and the Weakest Link to Small Businesses. International Conference on Cyber Warfare and Security, 17(1), Article 1. https://doi.org/10.34190/iccws.17.1.51
50. Krause, T., Ernst, R., Klaer, B., Hacker, I., & Henze, M. (2021). Cybersecurity in Power Grids: Challenges and Opportunities. Sensors, 21(18), 6225. https://doi.org/10.3390/s21186225
51. Burrell, D. (2020). An Exploration of the Cybersecurity Workforce Shortage (pp. 1072–1081).
52. Akhtar, F., & Parkar, T. (2024). Measuring the Effectiveness of Internship Programs in Aligning Education with Industry during Covid-19: A Case Study. International Journal of Instruction, 17, 537–556.
53. Rose, P. (2013). Recruiting and Selecting Graduate Employees via Internships. Asia Pacific Journal of Business and Management, 4(2), 39–54.
54. Qubati, T., & Tamim, K. (2021). The Role of Internship Programs in Enhancing Graduates' Employability.
55. McDonald, M., & Wilson-Mah, R. (2022). The Role of Mentorship in Internships. Papers on Postsecondary Learning and Teaching, 5, 42–50.
56. University of Southern Maine, & Sussman, L. (2023). Reinventing Cybersecurity Internships During the COVID-19 Pandemic. Journal of Cybersecurity Education Research and Practice, 2022(2).