Information Systems Frontiers (2023) 25:431–450
https://doi.org/10.1007/s10796-022-10332-y

RQ Labs: A Cybersecurity Workforce Skills Development Framework

Clinton Daniel[1] · **Matthew Mullarkey**[1] · **Manish Agrawal**[1]

Accepted: 12 August 2022 / Published online: 30 August 2022

Abstract
This research contributes to the knowledge of how Information Systems (IS) researchers can iteratively intervene with practitioners to co-create instructional programs with a framework designed for fast-paced, rapidly changing IS fields such as cybersecurity. We demonstrate how complex fields, such as cybersecurity, have the need for a skilled workforce that continues to rapidly outpace supply from universities. IS researchers partnering with practitioners can use this research as an exemplar of a method to design, build, and evaluate these innovative co-curricular IS programs. Moreover, we find these co-curricular IS programs are essential to upskilling students, integrating training on the latest tools, systems, and processes in these rapidly evolving disciplines.

Keywords Cybersecurity workforce skills shortage · Cybersecurity training program design · Elaborated action design research

1 Introduction

Governments, academia, and cybersecurity practitioner firms across the globe are actively exploring methods to address the cybersecurity workforce skills shortage problem (Furnell, 2021). In no small part, the growth of Secure Knowledge Management (SKM) systems used by firms to collect, organize, and disseminate various levels of sensitive information fuels the continuous demand for skilled cybersecurity workers. In-turn, these cybersecurity SKMs attract actors with malicious intent to attack and compromise these systems. Defending SKM systems from such attacks contributes to the global demand for a skilled cybersecurity workforce (Sahay et al., 2021).

To address this growing demand for cybersecurity workforce skills, we propose the design of a novel training program framework capable of evolving with the dynamic demands of the cybersecurity workforce. We find that in industries and sectors, such as cybersecurity, the IS tools, systems, and processes are evolving so rapidly that all cybersecurity training possesses a shrinking half-life for application. We find evidence to suggest that one critical means of assuring relevant cybersecurity training is a tight partnership between academia and leading edge IS firms in the co-creation, co-delivery, and authentic co-evaluation of cutting-edge, hands-on training for post-secondary students. We hypothesize that this innovative design-centric approach to closing the skills gap in cybersecurity applies equally well to all rapidly evolving IS technologies, including Social, Mobile, Artificial Intelligence (AI), Machine Learning (ML), Cloud Computing, Data Science, Distributed Blockchain Ledger, Virtual Reality, and Internet of Things (IoT).

The scientific contributions of this research include the method for the co-design, co-delivery, and, importantly, authentic, concurrent co-evaluation of innovative practice-centered cybersecurity training. We offer a generalizable framework for researchers to use the guided, emergent, and practice-inspired elaborated action design research (Mullarkey & Hevner, 2019) methodology to adapt the framework to similar contexts for learning innovation in rapidly evolving IS domains. The framework design also includes a novel pedagogy and measurable utilities that can be used by cybersecurity firms to evaluate the fitness of the firm's cybersecurity workforce preparation. A unique partnership between a public R1 research university and a global

✉ Clinton Daniel
cedanie2@usf.edu

Matthew Mullarkey
mmullarkey@usf.edu

Manish Agrawal
magrawal@usf.edu

[1] School of Information Systems and Management, University of South Florida, Tampa, FL 33594, USA

Deloitte "Technology Fast 500" awarded cybersecurity firm helped refine the framework over a multi-year period. The partnership includes access to practicing cybersecurity professionals, university research faculty, undergraduate and graduate university students, hybrid classroom learning environments (online and in-person), online learning management systems, and a cloud-based cybersecurity technology platform. The consequential research partnership contributes knowledge that serves the academic and practitioner communities for the growth of skilled workforces in rapidly evolving IS domains.

2 Motivation

This research is motivated by gaps in the academic literature in cybersecurity training program design. The growth in demand for cybersecurity practitioners addressed by academics with a unique opportunity to partner with cybersecurity professionals with access to cutting-edge cybersecurity software tools, data, systems, and processes greatly facilitated this research. Academic literature gaps were identified through a comprehensive review of cybersecurity industry surveys, reports, and academic research in cybersecurity training and skills development. The cybersecurity practitioner demand was motivated by the partnering cybersecurity firm's workforce needs, which led to a funded university research project. Faculty were provided unique access to the firm's proprietary resources and people over a 5-year period to investigate the issue and develop the co-curriculum framework described herein.

It has been argued within government, academic, and practitioner journals that cybersecurity education initiatives are a critical solution to the cybersecurity workforce skills shortage problem domain (Baker, 2016). Additionally, researchers agree that the effectiveness of the program design and implementation must be measurable and capable of dynamically adjusting to the current demands of the practical applications observed in cybersecurity (Beuran et al., 2016). However, there is a lack of understanding of the types of cybersecurity instructional programs that can be designed and implemented to effectively address the cybersecurity workforce skills shortage. The challenge is exacerbated by the rapid evolution of software tools, systems, and processes in this highly complex, dynamic, and adaptive IS domain, where the typical post-secondary education program teaches skills that are outdated at the time of training on tools with a technology half-life of less than two years (Daniel et al., 2022).

On October 2, 2018, the CEO of the cybersecurity firm ReliaQuest (RQ), Brian Murphy, committed $1 million to the University of South Florida (USF) for the purpose of preparing students for careers in cybersecurity. Murphy's motivation was clear in his statement, "*In the face of what the industry refers to as a talent shortage, we believe that cybersecurity is actually suffering from a skills shortage*" (Morelli, 2018). Along with the financial contribution from RQ, additional commitments were made by USF research faculty and RQ technical staff to co-create a training program called "RQ Cybersecurity Labs at the USF Muma College of Business (RQ Labs)" that would continuously operate over a 5-year period.

This co-created program offered USF researchers a unique opportunity to study how a novel cybersecurity training program could be designed to address the cybersecurity workforce skills shortage problem domain. A unique feature of this program was the integration of the body of theoretical and standards-based knowledge with the proprietary knowledge and operating environment of RQ to address the cybersecurity workforce skills shortage problem. Eventually, the commitment of the time, talent, and energy of two dozen RQ professionals proved to equal the academic funding in terms of the design, delivery, and evaluation of the training program. For example, by the fourth year of the program, nine of ten training program mentors provided by RQ were prior graduates of the RQ Labs hired by RQ in the intervening years.

3 Literature Review

The cybersecurity workforce skills shortage problem is well documented by industry (primarily to estimate the magnitude of the problem) and academia (primarily to identify mechanisms to address this problem). A summary of these streams is provided below.

3.1 Industry Estimation of Current State of the Cybersecurity Workforce

According to a survey $(ISC)^2$ conducted in 2021, the global cybersecurity workforce is estimated to be 4.19 million professionals with the largest number in the United States at 1.14 million ((ISC)2, 2021). Of the 14 country-specific, workforce estimates (NA, LATAM, EUROPE, and APAC), all estimates demonstrated some level of growth between 2019 and 2021. In 2021, the top three countries with the highest cybersecurity workforce increase were Germany (+165%), Singapore (+61%), and the United States (+30%).

The U.S. Bureau of Labor Statistics (BLS) projected Information Security Analysts to grow 33% from 2020 to 2030 (Bureau of Labor Statistics, 2021). This growth is much faster than the average for Computer occupations at 13% growth and all other occupations at 8% growth as reported by the BLS. According to recent surveys of Cybersecurity leaders and Chief Information Security Officers by

Table 1 Profiles of cybersecurity functions. Reproduced based on data collected in EY Global Information Security Survey 2021 (Burg et al., 2021)

Cybersecurity executive profile	Area of focus	Strengths	Weaknesses
Security expert	All things security	Deep subject matter expertise	Lack of business acumen
Tech advocate	Technology solutions and tools	Technology oriented	Siloed thinking
Risk and regulatory pros	Risk, controls, and compliance	Good for highly regulated sectors	Lack of technology acumen
Business transplants	Business integration	Business connectivity	Lack of technology and security acumen
Part-timers and job splitters	Split between cybersecurity and other primary roles	Cost saving	"Jack of all trades; master of none"

Gartner and E&Y, not finding the required competencies, particularly versatile and multi-skilled cybersecurity professionals, was cited as the top reason organizations struggle to hire cybersecurity professionals (Addiscott & Olyaei, 2021; Burg et al., 2021). The EY survey concluded that trying to find individuals with all the cybersecurity skills in current demand is like trying to recruit a "unicorn." Instead, the authors of the survey received feedback from respondents (executives) that recommended organizations build teams of professionals that balance a combination of cybersecurity talent, including business and technology expertise (see Table 1). Gartner called this "… *building a 'unicorn security team', rather than trying to assemble a team of security unicorns"* (Addiscott & Olyaei, 2021). The 2021 $(ISC)^2$ study also reported a desire among employers for a workforce with a mixture of skills, technical and non-technical, to accommodate multi-dimensional roles across various industries. The top attribute reported in the $(ISC)^2$ study was "*strong problem-solving abilities.*"

Table 1 summarizes the cybersecurity profiles identified by executives who responded to the 2021 EY survey. Cybersecurity executives identified 5 different cybersecurity professional profiles that can be described by their "areas of focus," "strengths." and "weaknesses." Conceptually, cybersecurity executives agree that a multi-talented workforce is required to form teams that combine the expertise of technical and non-technical skills.

3.2 Industry Assessment of Cybersecurity Workforce Skills

The 2021 report by the Chartered Institute of Information Security (CIISec) entitled "The Security Profession" collected information about the cybersecurity profession, the workforce roles, successes, failures, and challenges experienced in the business environment when responding to security and cyber risks (Wilson, 2021). CIISec members include affiliates from academia and the cybersecurity industry. The 2021 CIISec survey cites "*analytical thinking/problem solving*" among the highest regarded skills for new professionals entering the cybersecurity workforce. Additionally, 63% of respondents stated that the critical skills shortage was in "*Experienced*" personnel versus 37% reporting a shortage of "*New Entrants.*" This data indicates a continued demand for experienced cybersecurity professionals, and new entrants do not demonstrate adequate skills to meet industry needs.

The 2021 $(ISC)^2$ Cybersecurity Workforce Study reported a snapshot of the cybersecurity workforce and its industry distribution ((ISC)2, 2021). Of the 4,753 global cybersecurity professional survey respondents, 24% were in IT services, 10% in Financial services, 10% in Government, 8% in Manufacturing, 5% in Consulting, 4% in Healthcare, 4% in Retail/Wholesale, and 4% in Telecommunications. This distribution suggests a need for cybersecurity professionals across most industry sectors.

Industry assessments suggest that the cybersecurity workforce shortage problem has made little progress in the last few years. For instance, the Information Systems Audit and Control Association (ISACA), an international professional organization dedicated to information technology governance, published several reports between 2019 and 2021 on the global state of cybersecurity and its workforce efforts (ISACA, 2019) (ISACA, 2020) (ISACA, State of Cybersecurity 2021, Part 1: Global Update on Workforce Efforts, Resources and Budgets, 2021). Survey results, seen in Figs. 1 and 2, have shown insignificant changes over the three years, indicating evidence supporting the continuous cybersecurity workforce shortage problem.

Figure 1 illustrates minimal change reported by organizations regarding their perception of meeting staffing demands. Similarly, Fig. 2 illustrates the lack of progress over the three-year period in reports of vacant cybersecurity positions. In addition to the vacancy and staffing demands, all three surveys report significant delays in filling vacant cybersecurity positions. For instance, 44% of respondents in 2021 reported that cybersecurity vacancies took three to six months to fill with a qualified candidate. The overall conclusion from these industry surveys is an enduring shortage of competent cybersecurity professionals.

In response to this shortage of cybersecurity professionals, the National Institute of Standards and Technology (NIST) led the development of the National Institute

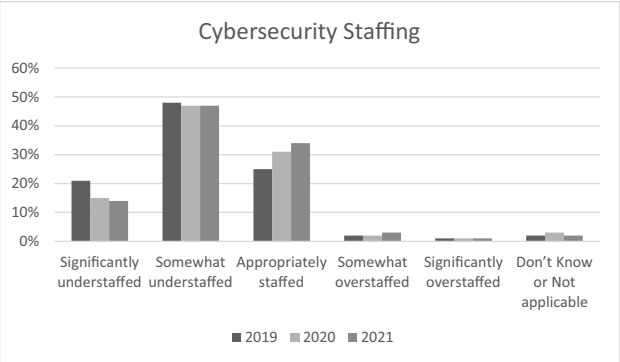

Fig. 1 Perception of cybersecurity staffing levels based on organizations surveyed from 2019 through 2021 using the *State of Cybersecurity Survey* conducted by ISACA

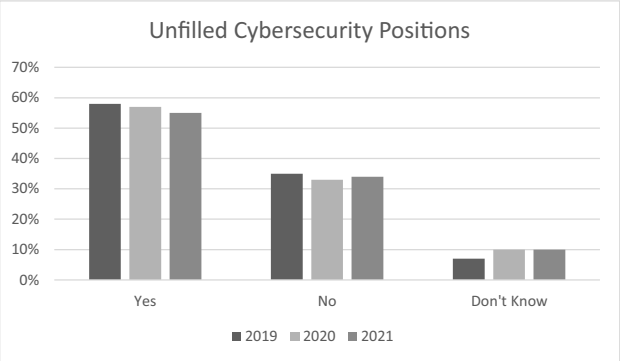

Fig. 2 Unfilled (open) cybersecurity positions based on organizations surveyed from 2019 through 2021 using the *State of Cybersecurity Survey* conducted by ISACA

for Cybersecurity Education (NICE) framework. NICE is a community-based partnership, including government, academia, and privately-owned organizations (Newhouse et al., 2017). The focus of the partnership is to strengthen the cybersecurity posture of organizations through the engagement of education, training, and workforce development. NICE published the Cybersecurity Workforce Framework (CWF) Special Publication 800–181 (Newhouse et al., 2017) in 2017 and revised it in November 2020 (Peterson et al., 2020).

The NICE CWF partitions cybersecurity work into seven categories: (1) securely provision, (2) operate and maintain, (3) oversee and govern, (4) protect and defend, (5) analyze, (6) operate and collect, (7) investigate.[1] Each of these categories has multiple specialty areas, and each specialty area has one or more work roles. For example, the securely provision category has specialty areas of risk management, software development, systems architecture, technology R&D, systems requirements planning, test and evaluation, systems development. We can see this specialty area focuses on developing new technologies to address cybersecurity challenges. Other specialty areas focus on important cybersecurity areas, such as policy development, incident response, etc. Thus, the NICE CWF framework provides a comprehensive mapping of cybersecurity roles and responsibilities to help leaders identify areas of weakness within their organizations.

The CWF can be used as a resource to describe the interdisciplinary nature of cybersecurity work performed by individuals and teams. The authors of the CWF recognized that prior to the establishment of NICE in 2010, the cybersecurity workforce roles had not been formally defined to provide a standard training and recruitment framework for cybersecurity roles within the U.S. federal government. The NICE CWF can also serve as a useful starting point for academics to establish courses and curricula to train graduates to serve in one or more specialty areas. One way to leverage the NICE CWF in workforce development is for faculty to begin by identifying the specialty areas most closely aligned to their curriculum. Then, they can identify missing knowledge units needed for graduates to take work roles related to that specialty area and update their curricula to incorporate these knowledge units. This approach would greatly improve the fit between student preparation and workforce needs as well as help address the ongoing shortage in the cybersecurity workforce.

3.3 Cybersecurity Program Design

In addition to following guidelines such as the NICE CWF, faculty have adopted multiple approaches to addressing the challenge of cybersecurity program design. One approach is the development of domain specific curriculum in areas of concern, such as information security in supply chain management (Murphy & Murphy, 2013). Another area of curriculum focus is emerging cyber-education opportunities, such as the behavioral demands of cybersecurity (Caulkins et al., 2016).

The Centers of Academic Excellence in Information Assurance Education (CAE/IAE) and Research (CAE/R) (Spidalieri & McArdle, 2016), CAE-Cyber Defense (CAE-CD) (Tang, et al., 2020) have also strongly influenced cybersecurity curriculum design due to the popularity of their credentials among students and universities. The CAE/ IAE curriculum is organized around specific groupings of knowledge and skills called knowledge units (KU); accordingly, cybersecurity programs often design curricula based on KUs (Conklin et al., 2014a, b). Examples of cybersecurity KUs

[1] https://niccs.cisa.gov/about-niccs/workforce-framework-cybersecurity-nice-framework-work-roles

include Networking, Operating Systems, Programming, Data, Policy, and others. Special topic KUs can be executed with a stackable curriculum with mappings to standards-based practice, such as CAE, designed to advance the student from entry level skills to more advanced levels (Katz, 2018). KUs implemented in program designs are often derived from industry certifications (Knapp et al., 2017), university faculty expertise (Cabaj et al., 2018), or tailored phase-developed learning based on job-specific knowledge, skills, and abilities (KSAs) (Baker, 2016).

Although program alignment with these standards-based curricula is common, pedagogical innovations add significant value to students (Endicott-Popovsky & Popovsky, 2014). Strengthening problem-solving skills and emphasizing hands-on experience within the program design can be particularly helpful. The pedagogical approach to hands-on cybersecurity learning can vary among practitioners and academia. For instance, one study concludes that web-based learning theory can improve the interaction with student learners such that automated training content is followed by a system generated cyber-attack (Tang et al., 2017). In another study from Japan, researchers studied the effectiveness of cybersecurity education and training with hands-on experience using cyber ranges (Beuran et al., 2016). This Japanese study supports the value of cyber ranges being used in virtual environments as a means of gaining practical experience and skills through effectively handling cybersecurity incidents.

Program designers have considered the target audience when understanding how concepts are taught, incorporating the individual backgrounds of students when deciding on the pace and content of learning. To this point, student culture can be relevant to cybersecurity course design and should be considered when iteratively refining the content (Gonzalez-Manzano & de Fuentes, 2019). Culture has been identified as the intrinsic habits of students, such as their cooperation and commitment to cybersecurity course content. Student groups exhibit various levels of cooperation and commitment to learning in an online environment. Therefore, student behaviors can be used to decide on the course content and level of difficulty.

This literature review suggests that though several approaches for cybersecurity education, without expertise in hands-on skills and problem-solving skills (even a curriculum aligned with the KUs or specialty areas), could remain highly conceptual, and graduates will find limited interest among employers. Therefore, there is a need for faculty to combine the knowledge areas identified by practitioners with pedagogical innovations from academia. The approach in this paper aims to offer a roadmap to accomplish this objective.

From a methodological perspective, researchers can apply scientific methodologies and principles to cybersecurity program design. We believe that the Design Science paradigm is appropriate for our problem domain. Design science is rooted in understanding how generalizable artifacts can be used in creative and innovative ways to solve a problem (Hevner et al., 2004), which is accomplished through iterative methods designed to build and evaluate artifacts created to address a problem domain. For instance, one emerging study proposes the use of Action Design Research (ADR) as an iterative methodology for revising and testing a college cybersecurity program framework design (Ward, 2021). Researchers developed ADR as a method that not only iteratively addresses the problem domain through building and evaluating artifacts, but also considers the organizational context and learning based on interventions (Sein et al., 2011). As a principle of ADR, design decisions and interventions are interwoven into the iterative methodology process through authentic and concurrent evaluation. Furthermore, ADR has been elaborated by researchers, called eADR, to allow for a more flexible, extended approach to abstractions in the artifact that may occur within any activity of an iterative ADR cycle (Mullarkey & Hevner, 2019).

While we believe that eADR can be an effective methodology for targeted curriculum design, its use in the design of cybersecurity programs to address the cybersecurity workforce skills shortage is limited. In this paper, we present the results of our efforts to use eADR for targeted cybersecurity program design.

4 Cybersecurity Workforce Skills Development Framework

Although the RQ Labs cybersecurity skills training program was co-created between a single cybersecurity firm and a set of Information Systems researchers from a university over a multi-year period of time, we argue that the academic literature, cybersecurity industry survey data, cybersecurity practitioner intervention, and a rigorous action design research methodology can be applied collectively to design a generalizable ensemble artifact in the form of a framework that addresses the IS workforce skills shortage problem domain. In particular, we find that dynamic, rapidly evolving IS fields demand a much more aggressive intervention with practitioners to eliminate the gap in skills between the typical academic course and the industry requirements. Design Science Research (DSR) seeks to solve challenging IS problems through a guided emergent design activity. It proposes a pragmatic paradigm in solving these problems where the research team seeks utility and usefulness, especially when solving novel problem domains where the solution domain is poorly understood. (Hevner et al., 2004) Action Research (AR) promotes an intervention, often in situ, where the researcher and client (organization) interact to take an

action and observe the outcomes of that action (Susman & Evered, 1978).

The Action Design Research (ADR) method applies AR to the build and evaluation of IS solutions – artifacts—within the DSR theoretical paradigm (Sein et al., 2011). Mullarkey and Hevner (2019) created the Elaborated ADR (eADR) to extend the ADR method to allow for stages in the research from Diagnosis to Design to Implementation in a typical innovative IS system construction. In addition, eADR offers the research team guidance on the actions taken in each iterative intervention cycle to design, build, evaluate, and reflect concurrently with practitioners in a co-creative, authentic evaluation of each incremental artifact in the IS solution design and implementation (Mullarkey & Hevner, 2019). Consequently, the RQ Labs program design activities started with a collaborative engagement in the Fall of 2018 between USF research faculty and RQ practitioners—including analysts, engineers, and human resource personnel. The purpose of the initial engagement was to understand – diagnose—in detail the nature of the problems experienced by practice in the cybersecurity workforce skills development and hiring domain.

In practice, the firm's human resources personnel reported that the growth of the firm's demand for recruiting skilled cybersecurity professionals was rising at a higher rate than the supply of qualified applicants. The highest volume of demand in human resources included entry-level analyst positions designed to occupy multiple shifts within their Security Operation Center (SOC). Additionally, HR professionals cited significant challenges in finding potential employees who had not only the required technical skills for the position but also the behavioral fitness to meet the desired cultural core values of the firm. Entry-level cybersecurity skills in demand by the firm could potentially be identified by industry certifications or university degree specialty. However, due to the rapid changes in skills demand, HR personnel in consultation with cybersecurity analysts and engineers experienced difficulty "finding" talent to maintain the level of hires required. Their hypothesis was that it would be better to develop and train their own "pipeline" of entry level cybersecurity workers. At the same time, they recognized significant limitations in their capacity to build a training program – for university students for example – without some sort of partnership with academia.

To better understand the human resource challenges associated with recruitment, our IS researchers had to engage closely with the operating environment of RQ security analysts and engineers. The study team (the academics and practitioners collaborating) began the diagnosis with an examination of the 24/7 RQ SOC work environment. Our observations were that all security analysts must possess a high level of competency and understanding of soft skills (such as communicating with teams or customers), excellent report writing capabilities (such as grammar and spelling), the ability to focus on the details of the technical content, a fundamental desire to perpetually learn as threats evolved, the desire to help others in need of assistance, the desire to seek help with problem solving, and a commitment to being accountable for their professional decisions.

The study team then evaluated the existing degree programs available at the partner institution and in the marketplace (for profit and not-for-profit). This information was compared to the needs expressed by the technical professionals and with the experiential observations of the HR personnel. The resultant evaluation led to the conclusion that there was not an evident skills gap "replacement" program that would meet the need. In addition, the study team was able to gain considerable insight into the importance of balancing soft and technical skills in a practicing SOC environment. This practical knowledge directly contributed toward the design of the RQ Labs cybersecurity workforce development framework (Daniel et al., 2022).

In eADR, as the study team moves from the Diagnosis stage to the Design stage, we anticipate the development of guiding principles in the design of the evolving innovative IS. These guiding design principles also form the foundation of the nascent theoretical framework for the specific context of innovative IS solution.

The study team observed that the design of the RQ Labs program would benefit from the development of an approach that combined a rigorous research method with key needs of the principal stakeholders – technical practitioners, HR practitioners, faculty, and students. Therefore, the researchers conceptualized a group of co-dependent components to meet the requirements of the desired outcome. RQ Labs had to include educational components that supported the demands, in soft and technical skills, of the cybersecurity workforce. In addition, the RQ Labs would need to meet student availability for an extra-curricular learning program. The research faculty needed to combine the university resources with those provided by the partnering firm to maximize the quality of engagement between the program instructors, practitioner mentors, and student participants. The roles of security analysts, security engineer, and HR personnel had to be considered to drive the direction of the program content, delivery, and outcome evaluation. Ultimately, the partnering cybersecurity firm was motivated to improve the workforce skills shortage problem while the research faculty were motivated to study the problem and inform academia with the newly discovered knowledge. Figure 3 below displays the conceptual diagram of the proposed cybersecurity workforce skills development framework.

As seen in Fig. 3, the RQ Labs cybersecurity workforce skills development framework consists of four dependencies that drive the evolution of the RQ Labs training program over the 5-year funded period. At the center of the

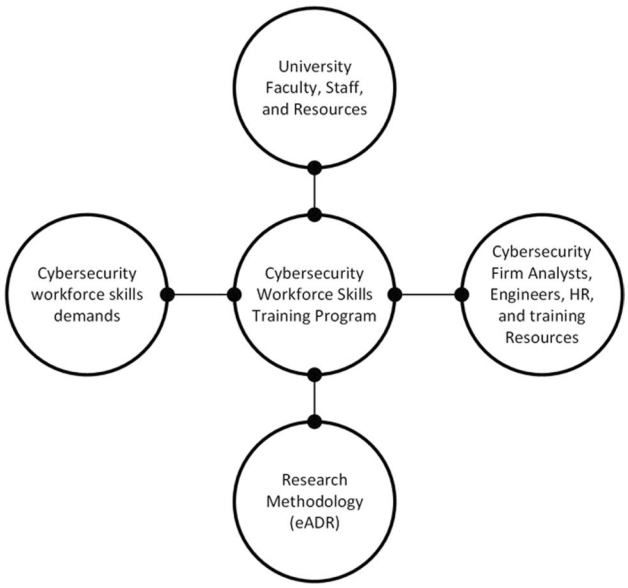

Fig. 3 Conceptual diagram of the components of cybersecurity workforce skills development framework

conceptual framework is the cybersecurity workforce skills training program design. The design of the program includes attributes such as course content, evaluation metrics, and instructional resources. A cybersecurity study team is first assembled and divided between university and cybersecurity firm resources. Next, our framework is dependent upon the implementation of a research methodology, such as eADR, to iteratively build and evaluate the program's ability to address the cybersecurity workforce skills shortage domain class of problem. Finally, it is essential that cybersecurity workforce demand is included within the framework. Workforce demand is communicated and driven by the needs of the cybersecurity firm and its stakeholders.

4.1 Cybersecurity Workforce Skills Training Team

Due to the 5-year commitment of funds and resources provided by the university's partnering cybersecurity firm, considerable effort was made toward the design of the cybersecurity skills training program by USF research faculty and practicing cybersecurity professionals. We defined the co-creation of the training program as a collaborative relationship between researchers and cybersecurity practitioners where research faculty are embedded with the practicing cybersecurity analysts, engineers, education specialists, and human resource personnel. The cybersecurity analysts offered practical insight into the daily operational tasks of a Security Operations Center (SOC) while the engineers offered insight into the infrastructure that supports the overall workflow of the SOC. Education specialists were used within the cybersecurity firm to support an internal training infrastructure called ReliaQuest University (RQU), which was implemented independently by RQ to address the continuous educational needs of cybersecurity practitioners and their customers. The firm's human resources personnel were responsible for management and coordination of potential, new, and existing employees.

An important resource detail of the cybersecurity workforce skills training program design was to understand how each cybersecurity practitioner participant contributed to the success of the program. Cybersecurity analysts work in a 24/7 year-round SOC that supports customers and their operational security. Among the daily tasks of a cybersecurity analyst includes the investigation of security alerts generated by the customers' information system environment. Specifically, cybersecurity analysts at RQ use modern security tools and a proprietary platform developed by the firm, called RQ GreyMatter™, which is designed to use machine learning (ML) to reduce the complexities of investigating an incident within a customer's environment. Although the RQ analysts use a platform that helps them reduce the data and tools required to conduct the investigation of a cyber event, they integrate internal tools with industry partner tools and a rigorous analytical template to navigate the complexities of alert information.

As investigations are completed by analysts, all content is permanently stored within a content management system. This practice of SKM grows exponentially over time, adds value to the firm and its customers, and serves as an internal repository of cyber threat intelligence. The study team found that it also feeds the "intelligence" of GreyMatter™ and, interestingly, could be used to continuously update the RQ Labs training content. Therefore, cybersecurity analysts contribute extensive technology skill, cybersecurity expertise, customer experience, threat intelligence content knowledge, and investigative methodologies that are captured by the SKM and used to generate the educational content for the student participants of a cybersecurity workforce skills training program.

Cybersecurity engineers can be involved in a variety of infrastructure supporting roles within a SOC. Specifically, it is common for a cybersecurity engineer to manage or support cloud resources or other application services required for the cybersecurity firm and its customers. These skills offer a necessary service to the cybersecurity workforce skills training program with the need to setup and manage cloud-based cybersecurity lab environments for the student participants in a separate instance of the operating system firewalled explicitly for RQ Labs.

Cybersecurity education specialists (RQU) have an extensive professional background in cybersecurity and education. In many instances, they serve as instructional designers for the firm's internal training courses, such as what we observed with RQU. Additionally, they manage educational

content in Learning Management Systems (LMS) used by firms to deliver training courses for cybersecurity employees and their customers. The education specialist is an integral part of the cybersecurity workforce skills training program team. The education specialist can organize all the educational content in the LMS, coordinate the training schedule with all student and cybersecurity firm employee participants, communicate with university faculty and staff, and manage the overall instructional design.

Human resource (HR) personnel are responsible for the interviewing and selection decisions made for all student participants throughout the multiple phases of a single cybersecurity workforce skills training cycle. In the case of RQ Labs, HR personnel communicate closely with a university Student Success specialist when planning each RQ Labs cycle recruitment strategy. The university Student Success specialist is responsible for the university campus-wide student recruitment campaign and sign-up process, which is used to collect all student contact information. Then, the student sign-up information is passed along to the cybersecurity firm's HR team and used to prepare for a training program cycle.

Equally important to the resource details of the training program design success includes an understanding of the experience profile contributed by university research faculty. In the case of RQ Labs, two USF Information Systems research faculty were involved with each RQ Labs training cycle. One research faculty, with prior executive level management experience, focused on the communication with the cybersecurity firm's leadership to ensure the direction of the program was effectively and objectively meeting its demands by all stakeholders involved. Additionally, this research faculty previously completed a formal leadership-focused Externship with the cybersecurity firm prior to the creation of the RQ Labs program. The other research faculty, with prior professional cybersecurity experience, focused on the communication with the training program team to ensure an acceptable pedagogy was objectively executed and measured. University research faculty collaborated, together and separately, with the training program team to communicate, document, recommend changes, inform academic theory, influence pedagogy, and manage the implementation of the eADR methodology.

4.2 Cybersecurity Workforce Skills Demand

The cybersecurity workforce skills demand for RQ Labs was driven by the cybersecurity firm's leadership, practitioners, and stakeholders. Although the forces for cybersecurity workforce skills demand can come from any outside source, such as academic research, standards-based organizations, or industry reports, we aligned the content included within our framework in consultation with the cybersecurity firm's needs. In the case of ReliaQuest, leaders decide for the global firm and its customers, with offices located in the United States, Europe, and Asia. Those decisions are aligned with the demands of business, technology, and the skills required to operate a cybersecurity workforce.

The cybersecurity workforce skills demand focus for the engagement with RQ was based on the skills needed for a university student to enter the cybersecurity workforce as an entry-level cybersecurity analyst with the potential to work within a SOC. Although a SOC analyst is the most sought-after job placement for students who complete the RQ Labs program, some students have entered the cybersecurity workforce as business analysts and development operations (DevOps) engineers. Additionally, many students have been recruited as interns into various departments within the cybersecurity firm to include Incident Response, Security Engineering, Threat Management, and Product Management.

5 Research Methodology—eADR

The cybersecurity workforce skills training program was developed using a guided emergent, co-creation design engagement between university research faculty and practicing cybersecurity professionals. The collaborative relationship between researchers and practitioners offered an opportunity for an Action Design Research (ADR) project. In this research, we adapted the ADR methodology from the traditional use of creating an innovative IT system to the creation of an innovative cybersecurity skills training program. We found the eADR methodology ideally suited to this rapidly evolving IS training environment where the problem domain and solution domain were poorly understood by researchers and practitioners.

We determined early in the research process that neither practice nor academia had all the knowledge of or the competencies to independently design and deliver the ideal cybersecurity training program. Most of the knowledge of what to teach on what platform resided with the practitioners and their SKM while most of the knowledge of how to design and deliver content to university students (and even how to recruit active university students) resided with the faulty researchers. The eADR methodology offers researchers and practitioners a continuum of interventions in situ using iterative cycles within each stage (diagnose, design, implementation, and evolution) of an innovative system. Each iterative eADR cycle within a stage offers an opportunity for a researcher to formulate the problem (P), create an artifact (A), evaluate the artifact (E), reflect on the results of the evaluation (R), and learn from the reflection (L). An iterative eADR cycle can be used by a researcher to inform

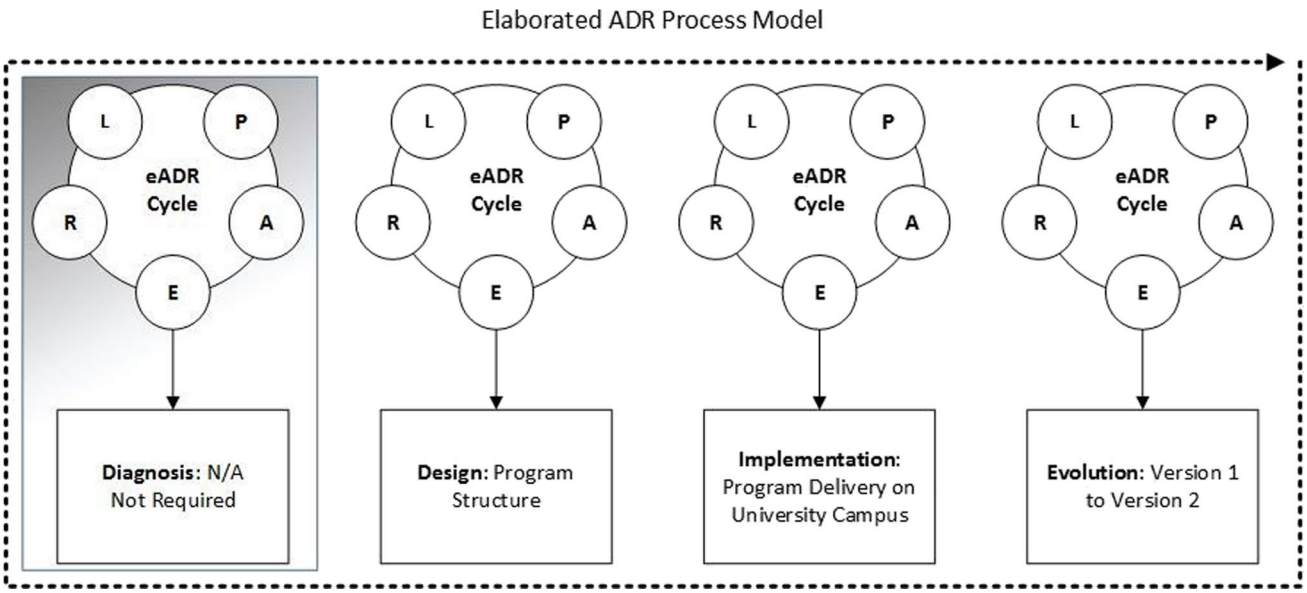

Fig. 4 RQ Labs eADR process model

the diagnosis, design, implementation, or evolution stages of an ADR process (Mullarkey & Hevner, 2019).

The study team used prior research of the problem domain during a faculty externship that confirmed the significant skills gap between university students and those of successful hires as well as an extensive literature review to support the diagnosis stage to begin the eADR process (Daniel et al., 2022). In year 1 of the program, the study team began the process of designing the structure of the RQ Labs cybersecurity skills training program as a co-creation activity with practitioners and university researchers in accordance with Fig. 3. Therefore, the flexibility of the eADR process model allowed the study team to begin its research by entering at the design stage of the ADR process. In the Fall of 2018, an eADR cycle was initialized to design the first version of the program structure. Thus, the version designed was implemented and evaluated in situ as the RQ Labs was completed each semester.

In time for the following RQ Labs training, the study team completed an evaluation of the performance of the recent past RQ Labs to modify the design. Also, the study team evaluated the evolution of the available cybersecurity tools and processes to modify the design of the RQ Labs delivery and content. This structure would then be used for the first through sixth cohorts of university students. Version 1 of the program structure was planned for implementation in late Fall of 2018. Version 1 of RQ Labs was designed in the Summer 2018 and delivered in the Fall 2018 during a 6-week cycle of RQ Labs coursework.

Upon completion of the first cycle, data was collected and evaluated to understand the pros and cons of the implemented structure. The study team continued to iterate RQ Labs in future university semesters from 2018 through 2022. Within each iteration of the program design, the study team of cybersecurity practitioners and faculty – with input solicited from students and HR personnel—intervened in the program structure and an evolution of the program was created in the form of a new version (Version *n*) (See Fig. 4). Also, each version of RQ Labs contributed to the RQ SKM and the RQU LMS (Daniel et al., 2022).

The RQ Labs eADR Process Model illustrates the interventions at each stage of the eADR method used to design the co-created cybersecurity skills training program (Adapted from Mullarkey & Hevner, 2019). [Note: in the eADR cycle: P = Problem Formulation/Planning, A = Artifact Creation, E = Evaluation, R = Reflection, and L = Learning].

5.1 Cybersecurity Skills Training Program Design: RQ Labs Case

The cybersecurity skills training program can be described as a comprehensive cybersecurity training program implemented as an extra-curricular college student engagement that provides a solution to a class of problem – skills education for rapidly evolving innovative IS domains (like cybersecurity, ML, AI, social, mobile, etc.)—within the cybersecurity workforce skills talent shortage domain. In the case of RQ Labs, the training program design activities are summarized in Table 2.

The summarized program design in Table 2 describes a training program that includes a total of 23 h of classroom instruction over a 6-week period. Each classroom instructional session includes individual hands-on activities,

Table 2 RQ Labs program design summary

Week	Activity	Description	Timing
1	Pre-Boot Camp	Introduce program purpose and general understanding of cybersecurity domain. Designed to filter out students not interested in cybersecurity training program	3 h
2	System Admin Boot Camp	Cybersecurity and networking Fundamentals	4 h
3	Attack Surface	Enterprise networking, security tools, data security, and kill chain	4 h
4	Anatomy of an Attack	Application Security	4 h
5	Detect, Response, & Mitigate	Incident Response Fundamentals	4 h
6	Capstone Assessment	Capstone Analysis using cyber investigation analysis methodologies	4 h

group activities, industry case studies, and mentoring sessions. This high-level view of the program is the result of co-creation activities conducted during each program cycle using the eADR methodology. Since the eADR methodology offers the opportunity for intervention based on a continuum of design activities, the training program successfully evolved over six iterations between the Fall of 2018 to the Spring of 2022. Table 3 summarizes the significant interventions made by cybersecurity practitioners or faculty to improve the overall rigor and relevance of the program design. Each intervention was informed by a pro (positive) or con (negative) experience during a given program cycle.

In Table 3, it is evident that the program design has gone through multiple changes based on interventions from university faculty or cybersecurity practitioners. In the first cohort iteration of the program, Fall 2018, it was observed that students were overloaded with technical content and software. For instance, RQ instructors observed little value in students engaging with both QRadar (a SIEM system) and CarbonBlack (an Endpoint Detection tool) tools while learning a new cybersecurity analysis methodology. Therefore, it was concluded that the Endpoint Detection tool should be eliminated from the program design. Additional challenges experienced by overexposure of various technology stacks introduced to students throughout the various program cycles has resulted in a program design that carefully considers the training environment and its supporting tools. For example, a Systems Administration boot camp and study groups were added to the program design by university faculty to improve the understanding of technical concepts and tools introduced to the students throughout the program.

Starting with the Spring 2019 cohort, the program design was significantly impacted by COVID-19 restrictions. The impact offered an opportunity to adapt the program design for delivery in face-to-face, 100% online, and hybrid (a blend of face-to-face and online) modes. As a result, the program is now adaptable to any of these common modes of delivery in any university environment. Additionally, the RQ practitioner work environment adapted over time to a virtual schedule. Due to the increase in engaged learning activities online and changes in RQ mentor work schedules, the program cycle schedule was affected, resulting in an increased number of RQ mentors and a change in program cycle from twice a calendar year to once per calendar year. Due to the expansion of RQ mentors in the program design, it was also decided that senior mentors be assigned to ensure the quality of knowledge transfer between program cohorts.

One interesting intervention of significance in the program design occurred during the end of the Spring 2019 cohort. The output of the Spring 2019 cohort resulted in only four student offers for part-time or full-time employment at RQ as opposed to 10 in the prior cohort iteration. Upon questioning the RQ HR and practitioners about what they observed as the potential reasoning for this sharp decline in numbers, they reported that students overall performed poorly in the behavioral/cultural interviews. It was then recommended by university faculty to add a module taught by a well-known researcher in the domain of emotional intelligence. The idea was that if students were aware of their behavior and ability to communicate effectively, this awareness would directly improve the outcome of the interviews.

After one iteration of an emotional intelligence module being used in the program design of the Fall 2019 cohort, the number of students recruited by RQ recovered to 10. Interestingly, the feedback from RQ HR and practitioners was that the increase in numbers recruited had no direct correlation with the student performance in the behavioral/cultural interviews. Instead, RQ HR and practitioners attributed the recovery of the numbers recruited to the overall improvement in the program's content and delivery. However, the introduction to the paradigm of emotional intelligence in the program design added an overall awareness to the importance of observing student behavior during training activities. The training modules were adapted by the instructors to continuously consider opportunities to reinforce the importance of student behavior in specific cybersecurity investigation scenarios and teamwork activities. The observation of student behavior became such an important part of the program that the RQ mentors from the Spring 2022 cohort implemented an intervention that involves the development

Table 3 Summary of significant interventions made with each RQ Labs program cycle using eADR

RQ Labs Cycle	Cycle Pros	Cycle Cons	Significant Intervention
Fall 2018	AWS setup, Learning Management System implementation, IBM QRadar SIEM	Student difficulty with CarbonBlack (EDR), Technical content overload with students	Eliminate CarbonBlack (EDR), Add Study Group sessions, System Admin Boot Camp
Spring 2019	Study group sessions and System Admin Boot Camp helped students with technical content	Written content was on multiple mediums, face to face instruction disrupted by COVID restrictions, Students had difficulty with behavioral/cultural interviews	Create RQ Labs written manual, Migrate program to 100% Online, Add Emotional Intelligence module
Fall 2019	Successful test of RQ platform (GreyMatter) with students	Virtual online experience made it difficult to scale group participation, Emotional Intelligence module had no impact on behavioral/cultural interviews	Add RQ Mentors, Add GreyMatter, Change program cycle to once per year, Remove Emotional Intelligence module
Spring 2020	Mentor sessions improved online experience and student communication, Slack for students to communicate with mentors	Schedule disruptions of RQ Mentors due to virtual work affected by COVID	Change program cycle to once per year, Increase number of new Mentors for students
Spring 2021	COVID restrictions are eased for face to face instruction	Some knowledge transfer was necessary for new RQ Mentors	Add Senior Mentors for Mentors, Add Hybrid delivery
Spring 2022	Hybrid delivery success	Increased cohort size challenges	Student scorecard to measure behavior

of a measurable behavioral scorecard that will be used in all future program iterations.

All significant program interventions described in Table 3 were considered when configuring the overall structure of the program design. To describe the program design in detail, we start with week 1, where approximately 100+ students from any major across the university are recruited through various communication channels to participate in a pre-boot camp. A pre-boot camp was developed into the design after observing a significant number of students who were interested in participation within the first iteration of the program and communicated to the instructors that they misunderstood what was required of the cybersecurity domain. Therefore, the pre-boot camp is designed to introduce any student to the cybersecurity domain so that they can decide whether they should move forward with competing for a training slot in the remainder of the program. Pre-boot camp content includes cybersecurity terminology, the CIA (Confidentiality, Integrity, and Availability) triad, careers in cybersecurity, expectations of the program, and testimonies from Security Operation Center analysts. Students are given an opportunity to participate in a question and answer session with the practicing analysts so that they have a complete understanding of what the cybersecurity workforce does on a daily basis.

Since the capacity of the RQ Labs program in weeks 2 through 6 is limited to approximately 50 to 60 students per program iteration, students are offered an opportunity to compete for a slot or decline to move forward. If students would like to pursue the opportunity for the program, they are asked to complete an online general cybersecurity knowledge assessment and sign up for a behavioral interview. Students compete for one of the available slots in weeks 2 through 6 through an initial behavioral interview conducted by a RQ human resource specialist team. In any given cycle, a human resource specialist team could conduct up to 80 or more interviews between weeks 1 and 2 of the program. The initial interviews are designed to select the best candidates from the students who elect to move forward in the program. The interviews are designed to gain a general sense of the student's potential fitness in the cybersecurity workforce. At this stage, fitness is measured subjectively based on the student's responses to behavioral questions. Technical questions are not used within interviews at this stage.

Once the human resource team selects the student candidates for weeks 2 through 6, students are invited to an optional Systems Administration boot camp in week 2. This boot camp is designed for students who do not have an extensive technical background in systems. Those who elect to participate in the week 2 Systems Administration boot camp are given hands-on classroom instruction using a Linux virtual machine by university faculty. The content covered in the Systems Administration boot camp includes

Linux operating system and networking commands and concepts. Although the Systems Administration boot camp uses the Linux operating system as its medium for training, it is clearly communicated that all other operating systems are equally important for this knowledge unit. Linux was selected simply because of its free use and open source capability for a custom technical learning environment. Additionally, students are exposed to how the content is directly linked to the context of fundamental cybersecurity, concepts such as application, data, and network security.

Weeks 3 through 6 of the RQ Labs program are designed to immerse the student in hands-on cybersecurity training focused on activities typically experienced by a practicing security operations center analyst. The training in weeks 3 through 6 is completely conducted by practicing RQ cybersecurity analysts and engineers with varying levels of experience. Additionally, university faculty members co-participate with the RQ analyst and engineering instructors throughout all training sessions conducted between weeks through 3 through 6. The expectation of this co-participation experience is to offer opportunity for university faculty to transfer relevant cybersecurity practical knowledge that can be used later to inform an academic curriculum. In many cases, faculty can directly observe the student response and performance to specific training content. For instance, university faculty co-participate in group instructor-led break-out sessions where students engage in a detailed discussion about specific cybersecurity concepts and scenarios experienced by RQ practitioners. The faculty contribute to the pedagogy of the discussion by periodically evaluating the quality of the student responses to specific questions challenged by practitioners in the break-out session.

In week 3, students are broken up into 5 or 6 groups of 10 students each. Groups were formed to reinforce the necessary skill for security analysts to work and communicate in teams. Each group is given a name and assigned 2 RQ cybersecurity practitioners who serve as direct mentors to all students in the group. A mentor-to-team pedagogical model was added to the program design based on improvements and suggestions experienced throughout each program iteration. It was discovered that mentors could micro-respond and provide the acceptable help necessary for students to successfully solve individual or team focused problems and challenges throughout the program. Each mentor set up a mobile app communication channel with Slack (https://slack.com/) so that students could communicate questions in between weekly training sessions. Mobile app communication was added after multiple iterations of the program design revealed that students and mentors typically communicate ad hoc issues with their peers in the mobile environment when compared to other methods.

The mentor's responsibility is to explain and reinforce all concepts covered in the content of the program each week to any student within their assigned group. Each week, during weeks 3 through 6, students are assigned homework activities on a Learning Management System (LMS); these homework activities are evaluated by their mentors for reinforced feedback. Additionally, each mentor uses a rubric that was co-developed between university faculty and RQ practitioners to evaluate the technical and behavioral performance of each student within the group. The technical rubric includes objective measures recorded by the mentor of the student's successful or unsuccessful ability to complete and apply the weekly lab activities to an expected scenario. For instance, in the "Detect, Mitigate, and Respond" training module, students are scored from 0 to 100% on their understanding of the Kill Chain, events, and ability to identify artifacts of significance. The behavioral rubric includes a group of observable behaviors aligned with the firm's core values that allow a mentor to set a score level between 1 and 3 on criteria such as the student's ability to demonstrate accountability, adaptability, focus, helpfulness, a positive attitude, and a responsible effort.

Additionally, the mentors are incentivized with a reward from RQ if their group outperforms all other groups in the program during the semester cycle. Performance incentives were added to the program design by RQ after observing the competitive behavior of mentors and their assigned students throughout multiple program iterations. Performance of the mentor is directly measured by the overall team rubric scores as well as how many students within their group successfully complete the program and have the potential for conversion to a full-time or part-time cybersecurity position.

To maintain the sustainability and quality of the mentor experience from iteration to iteration of the training program, a senior lead mentor is assigned to at least 2 student mentors to provide visibility into the program's progress, guidance to the mentors, and professional experience, if necessary. Senior lead mentors include experienced cybersecurity practitioners who may have advanced to leadership positions throughout the firm. Senior lead mentors are responsible for communicating daily with their assigned mentors when needed and participating in a weekly group meeting. The weekly group meetings are designed to allow direct communication between the senior lead mentors and the student mentors so that professional guidance can be appropriately implemented into the weekly RQ Labs iteration.

The content covered in week 3 of the program includes an understanding of the Attack Surface. To understand the Attack Surface, a student must gain competency in enterprise architecture, including its networking and tools used to manage or evaluate its functionality. Students are instructed on how data flows through an enterprise and can be used as a means for motivating an attack. Finally, students are introduced to cases that include scenarios that demonstrate the structure of an attack through a cyber kill chain. Then,

Table 4 Partial capture of an RQ Lab hands-on activity completed by students

Endpoint Fundamentals: Network Recon Lab
Objectives/ References • I will gain an understanding of the concepts surrounding Nmap and Host discovery Topics to reference: • Standardization of network protocols • Network addressing • TCP/ IP protocol suite of the Internet • Network protocols • OSI and TCP/ IP suite of protocols • TCP vs UDP protocols • Network mapping and scanning • Footprinting • Fingerprinting • Port scanners • Banner grabbing Exercise #1 scenario: 1. Nmap is by far one of the most popular tools in the world of information security. This popularity can be attributed to many factors. One of which is the fact that it is extremely effective. N map was introduced as a port scanner, but it's far outgrown that title at this point. We will be using it in this exercise to do basic network discovery. We will start with a *ping* scan. Enter the following to discover all the devices on your network. Remember your network might be in a different range that the example. So make sure you're scanning your actual network range nmap -sn $yournetworkrange/24

the cases are reproduced in a custom virtual lab environment hosted in Amazon Web Services (AWS). AWS was selected as the technical platform to host the technical labs because RQ has an existing enterprise agreement with its services and resources. Sharing resources, such as AWS, between the university environment and RQ are essential to the overall quality and success of the program design.

In week 4, students are introduced to the anatomy of an attack by examining security vulnerabilities experienced in various applications. Essential training in this week includes an introduction to exploits, web server security, and offensive security concepts. Students link the types of attacks to the parts of the attack surface covered in week 3. Additionally, various types of attacks, the attack lifecycle, and an understanding of threat actors are covered. Then, these concepts are reproduced as online hands-on labs within the AWS environment. The hands-on labs include a scenario, a fundamental technical concept, a required task to implement the concept on a scenario, and an analysis of the results related to the required task. For instance, Table 4 below is a partial capture of a hands-on lab requiring students to learn about Endpoint Fundamentals using Network Reconnaissance.

As seen in Table 4, the learning objectives are clearly communicated to understand the desired outcome of the hands-on activity. A comprehensive review of this fundamental technical concept is first covered in a class lecture followed by a demonstration of its practice. Once the fundamental concepts are completely discussed, the instructors introduce a scenario, such as the one described in Table 4. Students then login to the AWS virtual lab environment and complete the assigned activity. Mentors are available to their assigned students throughout the hands-on activities to improve the success and understanding of the student labs.

Week 5 content is designed to introduce the students to how to detect, respond to, and mitigate cybersecurity events that have been generated by a security information and event management (SIEM) system. Students are introduced to a cybersecurity investigation analysis methodology that helps to guide them through the analysis process. We learned through multiple iterations of the program design that many of the RQ mentors had previously worked for other cybersecurity firms as a security analyst. In all cases, the RQ mentors reported that a methodology was used to guide the analysis of a cybersecurity event. The common attribute of the various analysis methods discussed was that they include an iterative process of identifying key artifacts of significance to advance the narrative with the goal of eventually recommending a resolution to the customer's cybersecurity event. In the case of RQ Labs, the RQ mentors used a specific analysis methodology designed to improve consistency among investigations conducted on customer technical environments by multiple analysts within the SOC.

Initial iterations of the RQ Labs program used third-party SIEM and End Point Detection (EDR) tools hosted on AWS as learning mechanisms. However, more recent iterations of the program have offered an opportunity for students to learn on the RQ proprietary platform. The RQ proprietary platform encourages and reinforces the same workflow of analysis methodology being trained by the RQ mentors in the RQ Labs program. Due to the design of the proprietary RQ platform, this evolution of the program was added to

Table 5 RQ Labs evaluation 8-stage process

Stage	Evaluation description	Value measure description	Data	Metric
1	Completion of Week 1	General Cybersecurity Knowledge Assessment	Online cybersecurity baseline assessment quiz	Score
2	Completion of Week 1	Behavioral Interview	Verbal interview	Fit/Not Fit
3	Completion of Week 3 through 6	Final Capstone Assessment	Rubric based on capstone tasks	Score
4	Completion of Week 6	Technical Interview	Verbal Interview	Acceptable technical knowledge or Not
5	Personality Assessment Online	Personality type	Vendor assessment results	Personality type
6	Cultural/Behavioral Fit	Behavioral/Cultural Interview	Verbal interview	Cultural/Behavioral Fit/Not fit
7	Final Interview	Mixed Interview: Technical/Behavioral/Cultural	Verbal Interview	Full-time or Part-time Job Offer
8	Full-time or Part-time job offer	Verbal or written response	Verbal or written response	Student accepts offer or declines

Table 6 Student counts in various stages of multiple RQ Labs program iterations

Stage	Fall 2018	Spring 2019	Fall 2019	Spring 2020	Spring 2021	Spring 2022	Total
Hands-on training experience							
1	82	66	91	107	180	200	726
2	52	56	70	80	111	156	525
3	34	43	50	53	58	60	298
Multi-stage cybersecurity interview experience							
4	29	27	47	37	39	24	203
5&6	18	13	11	37	29	24	132
7	16	11	11	37	29	24	128
* Only a limited number of students can be selected based on availability							
8	10	4	10	12	9	12	57

improve the likely success of the student's ability to implement the desired cybersecurity investigation analysis methodology on common security platforms that may be used in other security operation centers.

Finally, week 6 of the program includes a comprehensive capstone assessment of the student. Program mentors assign cybersecurity event scenarios to students with simulated data based on prior customer experiences. Students are expected to evaluate the cybersecurity event scenario using all the tools, technologies, and methodologies exposed to them throughout the program. Upon completion of the analysis of the event, students submit a comprehensive report of their findings to their mentors for evaluation. Mentors score the students' level of success in completing the comprehensive capstone assessment.

6 Evaluation of RQ Labs

Upon completion of each 6-week program iteration, data was collected to measure the value added to the cybersecurity firm and the university students. Value-based data was recorded for program evaluation at eight different stages during and following the completion of a program iteration. Once the program evaluation process was completed, RQ practitioners collaborated with university researchers to improve the program structure for the next iteration. This engagement resulted in continuous improvements of the program design. Table 5 summarizes the data points captured at different stages of the program evaluation process.

Table 6 summarizes the data collected after completion of six program iterations. During each program iteration, a total count of students was collected as each university semester program iteration advanced to the next stage.

Seven hundred twenty-six USF undergraduate and graduate students from various colleges were sampled to begin Stage 1 of the RQ Labs program. Prior to the design of this program, RQ had reported trivial success with undergraduate and graduate students passing the initial job interviews with the firm. Essentially, human resources reported that no students were hired in the prior four years. Upon completion of Week 1 in all program iterations, Stage 1 of the RQ Labs was completed and the total sample size had been reduced to 525 students. Two hundred and one of 525 students did not attempt to pursue a required effort to complete Stage 1 evaluation for advancement into Stage 2 of the program. Upon completion of the Stage 2 evaluation

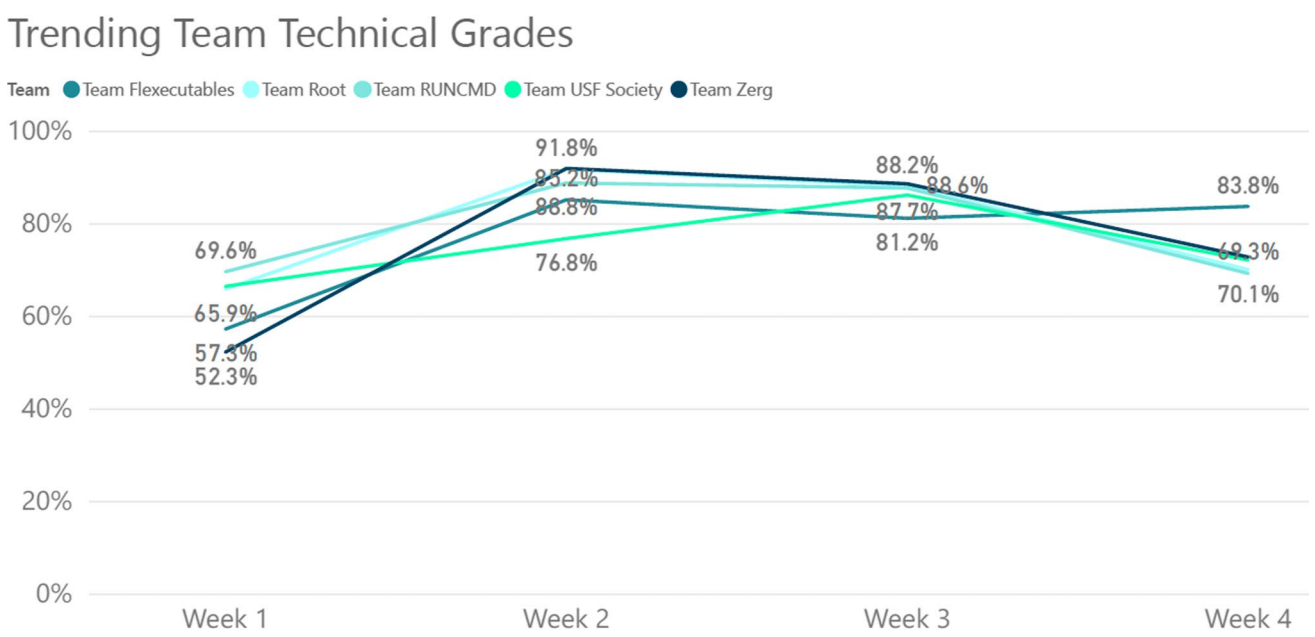

Fig. 5 RQ Labs dashboard report illustrates the overall technical performance grade trends from Spring 2020 student participant teams

process with all program iterations combined, RQ had selected 298 students to participate in Stage 3 of the RQ Labs program.

During Stage 3, a minimal number of students quit or failed to complete various points of the 4-week stage of the program for various reasons, such as other job offers, personal causes, or difficulty with the academic load. Additionally, the student performance scorecard managed by the RQ mentors is used to score students based on technical and behavioral performance. Technical performance is measured based on student results after completing each of the cybersecurity labs. Behavioral performance is measured based on the mentor's observation of the student's demonstration of RQ core values throughout Stage 3 of the program. Each lab has a required objective that is clearly explained to the student prior to assignment. The mentor scores the assignment followed by subjective comments on the student's strengths and areas of opportunity for improvement.

One notable difference found in week 6 (the capstone week) includes an evaluation of spelling and grammar. It is important to cybersecurity analysts that their written analysis and documentation demonstrate professional spelling and grammar. Each week (weeks 3 through 6), scores are aggregated and the top student performers from each group are recognized by their mentors and peers. Upon completion of week 6, a final score is calculated along with ratings for spelling, grammar, analysis methodology performance, and overall strengths with opportunities for improvement. A copy of the performance scorecard is included as a supplementary spreadsheet with this paper.

A dashboard report example developed by RQ showing the results in technical performance of five RQ Labs student teams during the Spring 2020 cohort is in Fig. 5 below.

Although individual students are graded by mentors on each team, Fig. 5 tells the story of how students learn to cohesively operate and compete as a team. For instance, Team Zerg is the worst technical performer in week 1 of the RQ Labs Stage 3 (weeks 3 through 6) cycle. However, they quickly rise to the top competitive position by week 2 with a finish in second place by the final week. This example is a significant indicator that teamwork in cybersecurity is an important skill toward success in a professional cybersecurity workforce environment.

Upon completion of Stage 3, Stages 4 through 8 of the program evaluation process involve a progressive set of interviews by human resources and other practicing cybersecurity staff. Stages 4 through 8 were added to the program design for several reasons. Based on experience from the cybersecurity firm's human resource team, university students were inexperienced with the interview process and its expectations for a cybersecurity position. Therefore, failure of university students to perform well in an interview was a common experience from the firm's human resources team. To respond to this problem, human resources recommended that the RQ Labs program include a set of interview stages. These stages could be used as not only a means for recruiting a limited number of available positions with the firm, but also an opportunity for university students to experience the workflow of a cybersecurity job interview.

During Stage 4 evaluation of the training program, a total of 95 students were eliminated due to poor technical

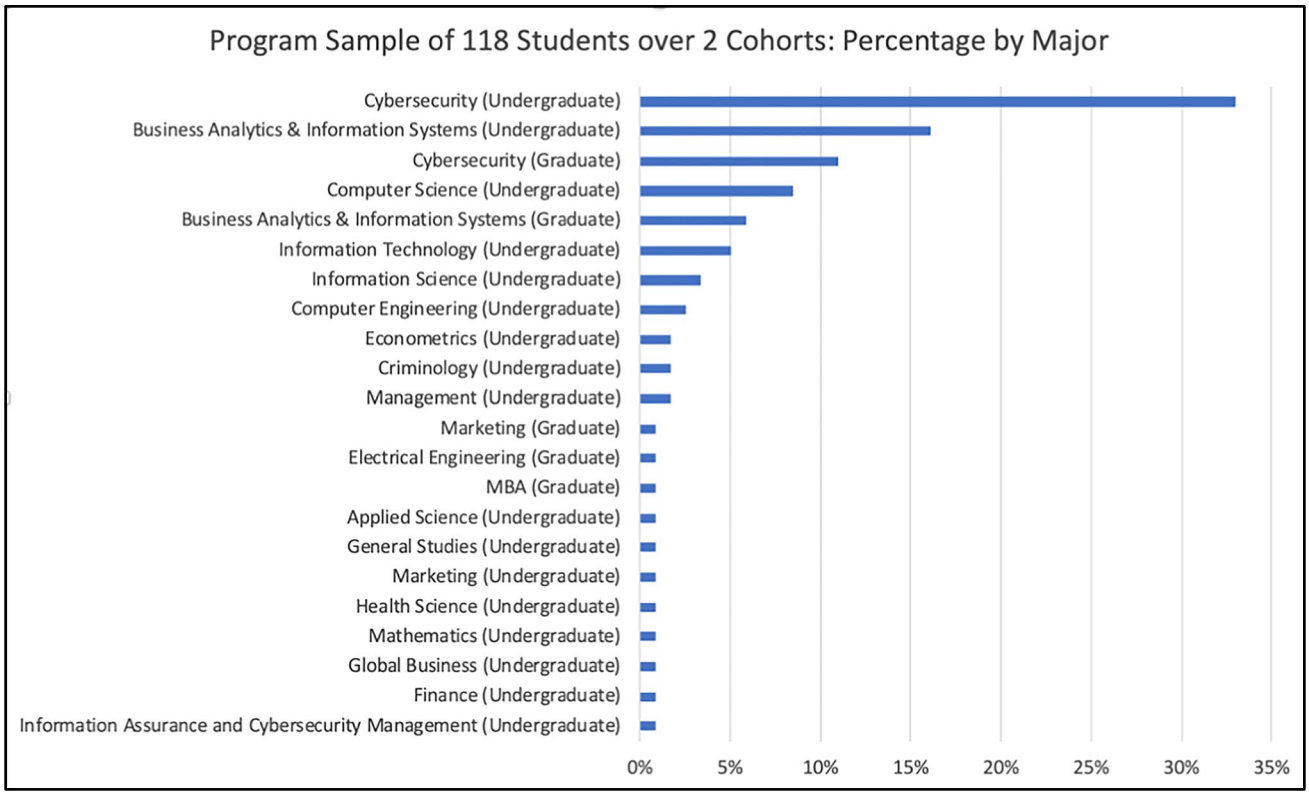

Fig. 6 RQ Labs student participation sample

interview responses, reducing the total number of students between all program iterations to 203. All students passing Stage 4 of the evaluation process were required to complete Stage 5 for a personality type classification. This assessment was completed to better place them in teams if they pass the entire evaluation process. Upon completion of Stage 6 evaluation, four students were judged as being behaviorally unfit for an RQ position, reducing the total number of students to 128. Finally, of the 128 students evaluated in Stage 7, 71 were eliminated due to lack of behavioral fitness or lack of in-depth technical knowledge. The Stage 7 final interview was designed to revisit and elaborate further on questions asked in Stages 4 and 6. This reduction left the final pool of students in Stage 8 with a limited availability of 57 part-time or full-time cybersecurity job offers by RQ.

Although part-time or full-time cybersecurity job offers by RQ for students were limited during each cohort cycle, this number was not a single measure of success for the participants of the program. Throughout the life of the RQ Labs program, students have participated in the initial pre-boot camp from at least 10 different colleges at the University of South Florida in more than 50 different majors in undergraduate and graduate programs. A sample of 118 student participants from two separate program cohorts, which significantly represents the overall population of student participants over the life of the program, was examined. In the sample of students, seen in Fig. 6, a diverse set of majors is represented. While Cybersecurity, Information Systems, and Computer Science students dominate the population of students represented in the sample population, many other majors are motivated to apply cybersecurity to their domain of interest. The result of this diverse sample includes a significant population of students with no specific interest in competing for a part-time or full-time cybersecurity position with RQ. Instead, the students expressed interest in applying the cybersecurity skills gained in RQ Labs to workforce positions acquired within their specific major domain.

Additionally, beyond the limited number of students offered part-time or full-time jobs at RQ are numerous cases where students who successfully completed the program were able to acquire employment elsewhere. For instance, a foreign graduate Information Systems student secured an internship as a Security Operations Center Analyst for an IT services company in Tampa, Florida. The student reported to university faculty that prior to the RQ Labs participation, many cybersecurity firms would not consider a foreigner for employment in a cybersecurity role due to employment requirements or contractual agreements with some U.S. government agencies. However, upon completion of the RQ Labs program, this student was able to secure an internship

that led to a conversion of employment as a full-time Compliance Management Engineer specializing in IT Security. This student success case has inspired other foreign students in the Information Systems program to pursue their interests in employment supported by cybersecurity roles.

Finally, in the results of the most recent Spring 2022 cohort seen in Table 6, a noticeable trend was observed in the data between stages 3 and 4 of the program iteration. This iteration resulted in the sharpest decline of students who completed the program at stage 3 but had no intention of advancing to interviews with RQ at stage 4. Although there was a 60% decline in interest by students to advance toward an interview in stage 4, RQ HR still hired 12, or 20%, of the students from the overall Spring 2022 cohort. A 20% recruitment by RQ HR for part-time or full-time cybersecurity positions is slightly above the overall average recruitment performance of 19.3% in six program iterations. Upon querying this trend further, the decline is largely attributed to student interest in cybersecurity positions or opportunities at firms outside of RQ. With the growth in popularity among university students interested in cybersecurity positions with or without RQ, as evident by stages 1 through 4 results of the Spring 2022 iteration, the RQ Labs program is trending as a diverse competitive means for cybersecurity workforce recruitment.

7 Discussion and Conclusion

Upon evaluation of the data collected from multiple iterations of the RQ Labs case, academic literature, cybersecurity industry survey data, cybersecurity practitioner intervention, and rigorous action design research methodology, we conclude that our proposed cybersecurity workforce skills development framework is an ensemble artifact that contributes significantly to addressing the cybersecurity workforce skills shortage problem domain. We observed value added to the university student and a practicing cybersecurity firm. Producing a mutual benefit among all stakeholders involved in this funded project has directly impacted its success. RQ benefited directly by adding a number of new cybersecurity employee hires based on availability over the course of six academic semesters of the program conducted between 2018 and 2022. In addition to the students hired by RQ, all program student participants benefited by adding an employable skill to their student resume, hands-on experiential learning, and experience with the workflow of a cybersecurity job interview. In some cases, students who were not hired by RQ at the end of program iterations were hired for a cybersecurity job by another firm. Additionally, RQ directly benefited from the program design by improving their internal hiring and training practices.

Improvements have been reported by RQ staff, university students, and university research faculty based upon what was learned throughout the various program design iterations. Throughout the multiple program design iterations, RQ human resources personnel have had opportunities to evaluate how they hire and onboard new employees. The RQ Labs program produced groups of new entry-level employees over the six iterations. Additionally, human resources interviewed hundreds of USF student participants in the program, allowing them to better understand how they can clearly identify fitness for potential employees within their firm and the cybersecurity workforce.

As a global cybersecurity firm, RQ was able to demonstrate to peer cybersecurity companies that a university partnership can benefit the advancement toward improving the cybersecurity workforce skills shortage problem domain. Measurable outcomes of the program are evidence that a university to practitioner partnership is a beneficial component to a cybersecurity workforce skills development framework. In addition to addressing the workforce skills shortage problem domain, cybersecurity firms can have a direct and iterative influence on the university curriculum to continuously help cybersecurity training programs stay rigorous and relevant to the current demands of the workforce.

Metrics collected throughout the RQ Labs program case include evidence suggesting that relevant cybersecurity practice knowledge is gained by participating university students. The RQ Labs cybersecurity workforce skills development framework implements an experiential learning program that benefits university students of all majors and levels. In some cases, the program supplies enough foundational knowledge for students to pursue industry certifications. Another added advantage for student participants in the RQ Labs program includes the opportunity to experience a cybersecurity interview, which includes multiple technical and behavioral phases used by human resource professionals and others in the cybersecurity workforce.

University research faculty directly benefited from the design of this proposed framework through direct engagement with a practicing cybersecurity firm. Direct access by university researchers to practicing cybersecurity firms offers a unique opportunity to understand and study the problem domain. Additionally, research access to a practicing cybersecurity firm's people, data, innovative services, and products adds a novel and competitive advantage to generating new knowledge that can be used to further inform the global academic community on the relevance of the cybersecurity workforce skills shortage domain problem. Faculty engagement with the practicing firm not only informs research, but also offers an opportunity for diffusion of relevant knowledge within the university's development of cybersecurity curriculum.

We found that the rigorous application of eADR led to a controlled, measurable improvement in the design, delivery, and outcomes of the RQ Labs; also, it provided a meaningful contribution to the SKM for the partner institution. This contribution to the firm's SKM cannot be overstated as it contributed to the ongoing internal training of the firm's practicing professionals, the evolution of the firm's LMS, and understanding the firm's hiring resources for the evaluation of recent college graduates for roles as cybersecurity analysts and engineers.

Our experience suggests that without the rigorous design, build, and evaluation processes inherent in the eADR method, the study team would have found it difficult to respond semester-to-semester to: (1) student success outcomes from a given cohort, (2) evaluation of program performance by practitioners and academics, and, (3) the rapid changes in the software, processes, and systems that occur in these rapidly evolving IS domains like cybersecurity. In sum, without the eADR contribution in the DSR paradigm, we would have experienced a less than optimal static implementation of an initial program that did not account for the probability that extracurricular leading-edge IS training programs must evolve with every instance/cohort of the program's delivery.

Finally, we suggest that the RQ Labs program provides a method, course structure, and training framework that offers a solution to a class of problem in addressing the cybersecurity workforce skills shortage. We further suggest that this approach can be generalized to skills training programs for multiple audiences across many instances of leading-edge rapidly evolving IS domains. Additionally, we suggest that the eADR methodology allows the flexibility for researchers to begin an innovative artifact creation research activity at any point of entry in the IS skills training development process. Although the artifact has addressed a well diagnosed and understood class of problem, more research is required to understand if this design can be implemented at other academic institutions and cybersecurity firms with a similar opportunity for collaboration.

8 Contributions and Future Research

In fast paced, rapidly evolving IS domains, such as cybersecurity, it should not be surprising that standard university curriculum will not keep up and provide students with currency in the discipline and its requisite skill sets. In these cases, a collaborative co-creation with practitioners serves to ensure the content is relevant and the skills students earn are relevant to the work environment where the jobs exist. To co-create in this environment, our research identifies an iterative guided emergent program design artifact, in or out of the traditional university curriculum, where an approach like eADR works well. The evaluation of the program design artifact thus developed must show benefit not only for the student and the faculty, but also for the partnering practitioner firm.

This research clearly addresses a novel pedagogy and measurable utility that can be used by cybersecurity firms and universities to evaluate the fitness of a training program designed to prepare students for the skills required of the cybersecurity workforce. The approach taken in this research also contributes to the knowledge of how Information Systems (IS) researchers can iteratively intervene with practitioners to co-create instructional programs for fast-paced, rapidly changing IS fields. Emerging IS fields that require the need for skilled workers continue to rapidly outpace supply from universities. IS researchers partnering with practitioners can use this research as an exemplar of a method to design, build, and evaluate these innovative co-curricular IS artifacts.

We find that the iterative interventions within cycles also add to our knowledge of the distinct roles of research faculty and practitioners in the co-create activities for these innovative IS artifacts and the knowledge they contribute to practitioner and academic SKMs, LMSs, and courses. A methodology that embraces the co-creation design of IS program curriculum between practitioners and academia is necessary to respond to rapidly changing problem domains, such as the cybersecurity workforce skills shortage. More research is needed to better understand how the eADR methodology can be used to motivate the future of IS curriculum design – potentially even within the typical degreed undergraduate and graduate majors in these rapidly evolving application domains.

Supplementary Information The online version contains supplementary material available at https://doi.org/10.1007/s10796-022-10332-y.

Acknowledgements This article and its primary research would not have been possible without the support, resources, and participation of cybersecurity firm ReliaQuest, LLC, in partnership with the University of South Florida (USF) to create the RQ Cybersecurity Labs at the USF Muma College of Business. Through ReliaQuest's $1 million 5-year grant to the USF Foundation, faculty were able to work with practitioners to offer cybersecurity training and certification to hundreds of students. The training benefited enormously from its use of a training instance of the latest in Cybersecurity secure operations technologies, including ReliaQuest's GreyMatter™ security platform. In addition, a portion of the grant funding supported three research streams, of which this article focuses on one critical aspect of our approach to innovative cybersecurity education.

Declarations

Conflict of Interest The University of South Florida's (USF) Foundation has received funding up to $1 million over a 5-year period from ReliaQuest starting in 2018 for the purposes of research and management of the RQ Labs program. The lead author, Dr. Clinton Daniel, has received USF salary stipends from this funding for his efforts in managing the RQ Labs program at the University of South Florida. Dr. Matthew Mullarkey has participated in a USF Funded Externship with

ReliaQuest within the past five years. Dr. Manish Agrawal is currently participating in funded research in partnership between the University of South Florida and ReliaQuest.

References

(ISC)2. (2021). *A Resilient Cybersecurity Profession Charts the Path Forward, (ISC)2 Cybersecurity Workforce Study, 2021.* (ISC)2.

Addiscott, R., & Olyaei, S. (2021). *Emerging Cybersecurity Leaders Are Needed Now to Sustain Security Program Effectiveness.* Gartner, Inc.

Baker, M. (2016). Striving for effective cyber workforce development. *Software Engineering Institute*, 1–26.

Beuran, R., Chinen, K.-i., Tan, Y., & Shinoda, Y. (2016). *Towards Effective Cybersecurity Education and Training*. School of Information Science, Graduate School of Advanced Science and Technology. Japan Advanced Institute of Science and Technology.

Bureau of Labor Statistics. (2021). *Occupational Outlook Handbook*. (U.S. Department of Labor) Retrieved December 2021, from Information Security Analysts: https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

Burg, D., Maddison, M., & Watson, R. (2021). *Cybersecurity: How do you rise above the waves of a perfect storm?* Retrieved December 2021, from EY Building a better working World: https://www.ey.com/en_us/cybersecurity/cybersecurity-how-do-you-rise-above-the-waves-of-a-perfect-storm

Cabaj, K., Domingos, D., & Respicio, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of masters programs. *Computers & Security, 75*, 24–35.

Caulkins, B. D., Badillo-Urquiola, K., Bockelman, P., & Leis, R. (2016). Cyber Workforce Development Using a Behavioral Cybersecurity Paradigm. *2016 International Conference on Cyber Conflict (CyCon U.S.)* (pp. 21–23). Washington, DC: IEEE.

Conklin, W., Cline, R. E., & Roosa, T. (2014a). Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors. *2014a Hawaii International Conference on System Science* (pp. 2006–2014a). IEEE Computer Society.

Conklin, W., Cline, R., & Roosa, T. (2014b). Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors. *47th Hawaii International Conference on System Science*, 2006–2014b.

Daniel, C., Mullarkey, M., Agrawal, M. (2022). RQ Labs: A Cybersecurity Workforce Talent Program Design. In: Krishnan, R., Rao, H.R., Sahay, S.K., Samtani, S., Zhao, Z. (eds) Secure Knowledge Management In The Artificial Intelligence Era. SKM 2021. Communications in Computer and Information Science, vol 1549. Springer, Cham.

Endicott-Popovsky, B. E., & Popovsky, V. M. (2014). Application of Pedagogical Fundamentals for the Holistic Development of Cybersecurity Professionals. *Cybersecurity Education, 5*(1), 57–68.

Furnell, S. (2021). The cybersecurity workforce and skills. *Computers & Security, 100*, 1–7.

Gonzalez-Manzano, L., & de Fuentes, J. M. (2019). Design recommendations for online cybersecurity courses. *Computers & Security, 80*, 238–256.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly, 28*(1), 75–105.

ISACA. (2019). *State of Cybersecurity 2019, Part 1: Current Trends in Workforce Development.* ISACA.

ISACA. (2020). *State of Cybersecurity 2020, Part 1: Global Update on Workforce Efforts and Resources.* ISACA.

ISACA. (2021). *State of Cybersecurity 2021, Part 1: Global Update on Workforce Efforts, Resources and Budgets.* ISACA.

Katz, F. H. (2018). Breadth vs. Depth: Best Practices Teaching Cybersecurity in a Small Public University Sharing Models. *The Cyber Defense Review, 3*(2), 65–72.

Knapp, K. J., Maurer, C., & Plachkinova, M. (2017). Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance. *Journal of Information Systems Education, 28*(2), 101–114.

Morelli, K. (2018, October). *USF/Reliaquest Partnership Aims to Fill the Talent Gap in the Emerging Cybersecurity Field*. Retrieved December 2021, from USF Muma College of Business Newsroom Articles: https://www.usf.edu/business/news/articles/181002-reliaquest-partnership.aspx

Mullarkey, M. T., & Hevner, A. R. (2019). An elaborated action design research process model. *European Journal of Information Systems, 28*(1), 6–20.

Murphy, D. R., & Murphy, R. H. (2013). Teaching Cybersecurity: Protecting the Business Environment. *Curriculum Development Conference 2013* (pp. 88–93). Kennesaw: ACM.

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.* U.S. Department of Commerce. National Institute of Standards and Technology.

Peterson, R., Santos, D., Smith, M. C., Wetzel, K. A., & Witte, G. (2020). *Workforce Framework for Cybersecurity (NICE Framework).* U.S. Department of Commerce. National Institute of Standards and Technology.

Sahay, S. K., Goel, N., Jadliwala, M., & Upadhyaya, S. (2021). Advances in Secure Knowledge Management in the Artificial Intelligence Era. *Information Systems Frontiers, 23*, 807–810.

Sein, M. K., Henfridsson, O., Purao, S., Rossi, M., & Lindgren, R. (2011). Action Design Research. *MIS Quarterly, 35*(1), 37–56.

Spidalieri, F., & McArdle, J. (2016). Transforming the Next Generation of Military Leaders into Cyber-Strategic Leaders: The role of cybersecurity education in US service academies. *The Cyber Defense Review*

Susman, G. I., & Evered, R. D. (1978). An assessment of the scientific merits of action research. Administrative science quarterly, 582-603

Tang, D., Pham, C., Ken-ichi, C., & Razvan, B. (2017). Interactive Cybersecurity Defense Training Inspired by Web-based Learning Theory. *2017 IEEE 9th International Conference on Engineering Education (ICEED)* (pp. 90–95). IEEE.

Tang, C., Tucker, C., Servin, C., Geissler, M., Stange, M., Jones, N., …, Schmelz, P. (2020). *Cybersecurity Curricular Guidance for Associate-Degree Programs.* Association for Computing Machinery (ACM), Committee for Computing Education in Community Colleges (CCECC).

Ward, P. (2021). Constructing a Methodology for Developing a Cybersecurity Program. *Proceedings of the 54th Hawaii International Conference on System Sciences* (pp. 44–53). Honolulu, HI: University of Hawaii at Manoa, Hamilton Library.

Wilson, P. (2021). *The Security Profession, 2020–2021*. Chartered Institute of Information Security.

Dr. Clinton Daniel, DBA is an Associate Professor of Instruction in the School of Information Systems and Management in the Muma College of Business at the University of South Florida teaching undergraduate and graduate level courses in business intelligence, business data communications, business application development, distributed information systems, managing information resources, case method publications, systems analysis and design, and cybersecurity. His current research interests include design science research, social media analytics, case research, and cybersecurity. He completed his Doctor of Business Administration degree at the University of South Florida (Tampa).

Dr. Matthew Mullarkey, Ph.D. is a Professor of Instruction in the School of Information Systems and Management in the Muma College of Business at the University of South Florida in Tampa, Florida. He is the Director of the Doctor of Business Administration program, Executive Director of the USF-TGH People Development Institute, and an Extraordinary Research Scientist at North West University (South Africa). His current research interests include the guided emergent design of innovative technology systems, processes, products and services with an emphasis on cybersecurity, data science, smart cities, education and analytics in healthcare, finance, manufacturing, defense and tech industries. His articles have appeared numerous peer-reviewed proceedings and journals including the INFORMS Journal on Computing, European Journal of Information Systems, IEEE TEM, CAIS and Information Systems Frontiers. His research has been funded by more than $12 million in public and private grants including more than $4 million from the National Science Foundation. He is a Fulbright Core Research Scholar. He is a graduate of the United States Military Academy (West Point), the University of Southern California, and completed his Ph.D. at the University of South Florida (Tampa).

Dr. Manish Agrawal is a Professor in the School of Information Systems and Management in the Muma College of Business at the University of South Florida in Tampa, Florida. His current research interests include technology workforce development and academic program outcomes. His articles have appeared in journals including Management Science, MIS Quarterly, INFORMS Journal on Computing and Information Systems Frontiers. His research has been funded by the National Science Foundation. His research also received the Design Science Award from the INFORMS Information Systems Society. He completed his Ph.D. at SUNY Buffalo.