https://doi.org/10.48009/1_iis_2019_88-99

Issues in Information Systems
Volume 20, Issue 1, pp. 88-99, 2019

DESIGNING A DOCTORAL PROGRAM IN CYBERSECURITY FOR WORKING PROFESSIONALS

Ping Wang, Robert Morris University, wangp@rmu.edu
Fred Kohun, Robert Morris University, kohun@rmu.edu

ABSTRACT

Cybersecurity is an emerging and fast-growing field, and there has been a large and increasing demand for cybersecurity experts, leaders and college faculty with advanced education. Doctoral education is expected to produce advanced researchers and leaders in various areas, and working professionals are a significant part of doctoral student population, who prefer online education to accommodate their busy work schedules. Doctoral program curriculum, courses and learning activities should be designed to support and achieve the course learning outcomes, program objectives as well as educational and professional goals for students. This paper proposes a doctoral curriculum design model and a new Ph.D. program in Cybersecurity for working professionals using the case of a private non-profit university in northeastern United States. The program proposal presents the doctoral program and curriculum design based on the proposed design model and survey findings among working professionals for doctoral education in Cybersecurity, discusses key components of the curriculum design and examines their value and relationships to the goals and objectives of doctoral education.

Keywords: Cybersecurity, doctoral program, educational goals, professional goals, research, innovation

INTRODUCTION

Doctoral level education emphasizes research and knowledge creation to advance a certain field, and a doctorate degree, such as Doctor of Philosophy (Ph.D. or PhD), is a special personal quality and identity of having acquired the breadth and depth of knowledge and skills as well as an advanced level of competence and original contribution necessary for research, leadership, and judgment in a disciplinary or professional field (Wang, 2018; Yazdani & Shokooh, 2018). Professionally speaking, leadership talent with experience, technical expertise, and advanced education is the most valuable workforce component in any industry, especially in the cybersecurity industry (Aufman & Wang, 2019). Cybersecurity is a fast-growing field, and there has been a large and increasing demand for cybersecurity experts, leaders and college faculty with advanced education preferably at the doctoral level.

Cybersecurity is the process, activity or capability of protecting or defending information and communications systems and data in cyberspace against damage, unauthorized access, disruption, modification, or exploitation (NICCS, 2018). A recent cybersecurity workforce study shows that the shortage of cybersecurity professionals is close to three million globally and about half a million in North America, and the majority of the companies surveyed reported concerns of moderate or extreme risk of cybersecurity attacks due to the shortage of dedicated cybersecurity staff ((ISC)^2, 2018). The employment of information security analysts alone is projected to grow 28 percent from 2016 to 2026, which is 4 times higher and with better pay than the average for all occupations (US Labor Department BLS, 2019). The fast growth in the cybersecurity industry and workforce will also demand more leaders and college faculty with advanced education in the field. Search results from HigherEdJobs.com show a large number of over 300 unfilled Cybersecurity-related college and university faculty positions that require or prefer a relevant doctorate degree (HighEdJobs, 2019).

In addition, there are growing and abundant needs and opportunities for advanced research for doctoral programs and students in Cybersecurity, which is multidisciplinary involving computer information systems, computer science, technology, business management, leadership, communication, critical thinking, problem-solving and analytical skills (Wang, 2018). Opportunities for research and publications in Cybersecurity are on the rise, including peer-reviewed scholarly research publications, regional, national and international conferences and symposia, and research centers focusing on cybersecurity research and education at universities. To help promote cybersecurity education and mitigate the shortage of cybersecurity talent and workforce, the US National Security Agency (NSA) and Department of Homeland Security (DHS) jointly sponsor the National Centers of Academic Excellence in Cyber Defense (CAE-CD) program. The CAE-CD designations are the gold standard quality assurance for cybersecurity education. The CAE-CD designations include CAE in CD Education (CAE CDE) for Associate, Bachelor, Masters and Doctoral Programs and CAE in CD Research (CAE-R) primarily for doctoral programs (NSA, 2019).

More innovative doctoral programs are needed to meet the needs of nontraditional and older-aged students who are a significant component of doctoral student population. Compared with the traditional doctoral students who are typically younger (thirty or under), white male, unmarried, not having a full-time career but funded by a teaching or research assistantship, nontraditional doctoral students are more diverse and increasingly female, over 30 years old, self-funded, and married with children and/or dependent parents along with a full-time career outside the doctoral study (Offerman, 2011). The latest demographic data on US doctoral students indicate that over 60% of doctorate degree recipients are over the age of 30 and that about 50% of doctoral graduates of age 41 and older reported self-funding for the doctoral study compared with only 4% of the doctoral graduates aged 30 or younger (National Science Foundation, 2018). The doctoral study process can be a stressful process with high risks of attrition for nontraditional students who may have to juggle and balance between life, family, work, and study (Ali & Kohun, 2006; Fung, Southcott, & Siu, 2017; Martinez, Ordu, Sala, & McFarlane, 2013; Offerman, 2011; Sverdlik, Hall, McAlpine, & Hubbard, 2018). Therefore, nontraditional students including working professionals need innovative program and curriculum design and program management to meet their needs and the goals of doctoral studies.

As nontraditional students, working professionals bring valuable professional experience to doctoral programs. To help these students succeed in the doctoral study and reach educational and professional goals of doctoral education, doctoral programs need to offer innovative and nontraditional program and curriculum design, such as online asynchronous delivery with minimal residency, to address the students' multi-faceted challenges of life, family, work, and study. The goal of this research paper is to propose a systematic model of doctoral program and curriculum design and share a sample program design of a PhD in Cybersecurity for working professionals based on the proposed model and survey findings on student interests. The following sections of the paper will present a relevant background review, the proposed model, the survey method and findings, and description and discussions of the sample doctoral program and curriculum design. The paper concludes with suggestions for future studies on this topic.

BACKGROUND

This section reviews the theoretical background for the general and common goals, directions, and models of innovation for doctoral education that guide the design of doctoral programs, curricula and courses. This section also identifies key cybersecurity knowledge units and skill areas that a doctoral program in Cybersecurity should focus on and align with for quality assurance. In addition, this section identifies appropriate program delivery format to meet the needs of nontraditional students and support the academic and professional goals of doctoral education in Cybersecurity for working professionals.

A doctorate degree, such as a PhD, is commonly recognized as the highest academic degree and a special personal quality and identity that indicates a certain level of competence, scholarship and creation of original contribution (Yazdani & Shokooh, 2018). Doctoral education has certain general educational goals in common that distinguish doctoral programs from master's programs, including creativity, innovation, critical thinking, research and problem solving that have been and should be the most important goals for doctoral education (Wang, 2018). Among the common goals, creativity is the most essential to advancing existing knowledge and often associated with originality and innovation. Originality emphasizes novel knowledge seeking in research while creativity is seeking novelty with disciplinary relevance or value, and innovation highlights problem-solving and application with economic relevance (Baptista et al., 2015; Wang, 2018). Creativity is also a journey of inventive process for doctoral students that features independence and critical thinking and leads to a creative product such as the dissertation (Brodin, 2018; Brodin & Avery, 2014). Doctoral education should reach the higher levels of learning taxonomy featuring the abilities to create a new product or point of view and analyze and evaluate with complex and critical thinking (Anderson & Krathwohl, 2001; Harris & Patten, 2015; Inouye & McAlpine, 2019; Krathwohl, Bloom, & Masia, 1964; Wang, 2018). Therefore, the goals and objectives of a doctoral program and the learning outcomes and learning activities of the curriculum and courses of a doctoral program should support the general and common goals of student creativity, originality, innovation, critical thinking, knowledge creation, and problem solving. These common goals are also fundamental principles for the design of a doctoral program and curriculum.

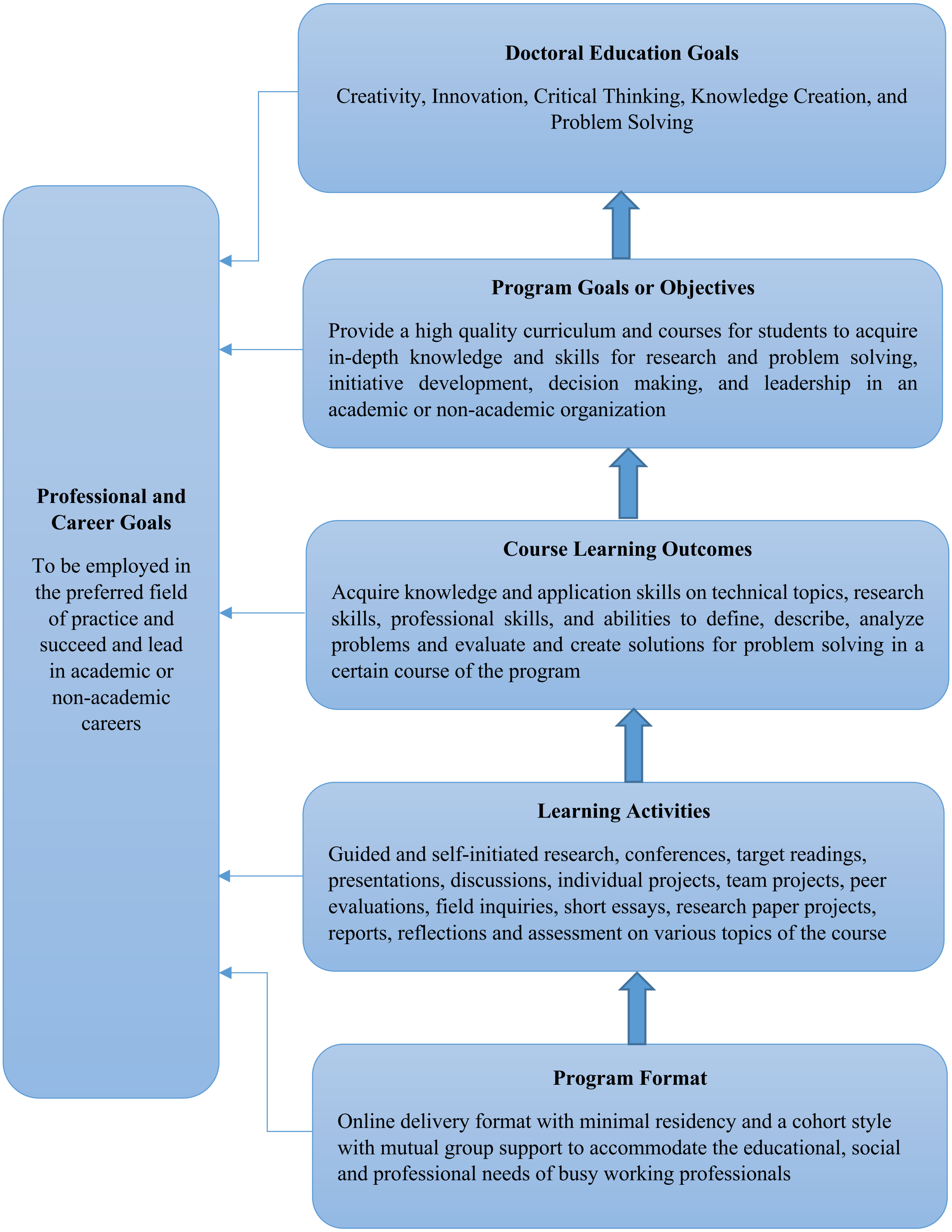
In practice, professional and career goals are equally important for nontraditional doctoral students who usually invest substantial amounts of money and time out of their busy work and family schedules to complete the challenging doctoral degree program. The most common reason for nontraditional students who are working professionals to pursue the doctorate degree is to enhance the opportunities of their existing careers or to transition to a different career (Offerman, 2011). Research on the employment trend for doctoral programs shows that doctoral graduates are increasingly going to work in organizations and industry outside academia (Hoyne, Alessandrini, & Fellman, 2016). The doctoral education programs and curricula often fail to meet the professional needs of the majority of students. A case in point is that the science curriculum for doctoral programs in the U.S. has continued the same basic format for almost 100 years with the primary focus on preparing academic researchers whereas over 60% of new doctoral graduates in science will not have careers in academic research (CESAER, 2015). To help students reach their diverse professional and career goals, the design of graduate programs and curricula should include a wide range of professional skills including specialized technical skills, teamwork and leadership skills and interpersonal skills in addition to critical thinking and problem solving skills (Hoyne, Alessandrini, & Fellman, 2016; Hasib, 2015; Wang, 2018; Wang & Sbeit, 2017).

Doctoral programs need to follow benchmark standards in curriculum design for quality assurance. This is especially important for the emerging academic field of Cybersecurity. In reality, a recent study shows that top universities in the U.S. were failing at cybersecurity education with a lack of clear cybersecurity requirements for graduates and slow updates in curriculum and courses (White, 2016). The national Centers of Academic Excellence in Cyber Defense (CAE-CD) designation program jointly sponsored by the US National Security Agency (NSA) and Department of Homeland Security (DHS) has been the most reputable national standard for certifying and maintaining high quality of cybersecurity education with rigorous requirements for program evaluation and assessment of cybersecurity knowledge units. The CAE-CD designation and quality standard apply to doctoral programs as well and specifies comprehensive and knowledge unit (KU) areas for cybersecurity curriculum mapping and quality assurance. The current CAE-CD KUs and descriptions include 3 Foundational KUs, 5 Technical Core KUs, 5 Non-Technical Core KUs, and dozens of Optional KUs for selection and mapping (NIETP, 2019). The Foundational KUs include the areas of cybersecurity foundations, principles, and IT system components; the Technical Core KUs include areas of networking, cryptography, programming, network defense, and operating systems; the Non-technical Core KUs cover the topics of cyber threats, cybersecurity planning and management, security policy and risk analysis. The Optional KUs provide a wide variety of security topics and emerging topics, such as cloud security and embedded system security. The KU areas are updated annually for currency and should be valuable resources for designing and mapping the curriculum and courses for a high quality doctoral program in Cybersecurity.

Finally, innovative and effective program format should be an important consideration in designing a doctoral program for working professionals. Doctoral students who are working professionals have to balance life, family, career, and doctoral study at the same time, which may lead to various challenges and barriers to their successful completion of the doctoral program (Fung, Southcott, & Siu, 2017; Martinez, Ordu, Sala, & McFarlane, 2013; Offerman, 2011; Sverdlik, Hall, McAlpine, & Hubbard, 2018). While the residency requirement is necessary for doctoral students to have in-person contacts and meetings with professors and classmates, excessive residency and travel requirements may create additional burden for them on top of their busy schedules. Online delivery with asynchronous learning format and minimal residency may be the best solution to provide a flexible learning environment to accommodate students' busy schedules while maintaining necessary minimum residency requirements. In the age of technology, online learning has become a significant and growing delivery modality in higher education (Allen, Seaman, Poulin, & Straut, 2016). Research shows that effective teaching, learning, teamwork and assessment can be implemented in an online graduate program in Cybersecurity (Wang & Sbeit, 2017). Well-designed online programs can create successful learning communities for doctoral students as well (Berry, 2017). In addition, a cohort format for doctoral programs is found to be able to increase interpersonal communication and support, reduce social isolation and anxiety, and foster a positive, supportive and collaborative learning community for working professionals (Ali & Kohun, 2007; Berry, 2017; Pemberton & Akkary, 2010; Sverdlik, Hall, McAlpine, & Hubbard, 2018).

MODEL

The proposed model for designing doctoral programs for working professionals is shown in Figure 1. The model is an improvement of the Doctoral Course Design Model (Wang, 2018), which was limited to the design of individual doctoral courses. The remainder of this section explains the model, its components and their relationships.



Doctoral Education Goals

Creativity, Innovation, Critical Thinking, Knowledge Creation, and Problem Solving

Program Goals or Objectives

Provide a high quality curriculum and courses for students to acquire in-depth knowledge and skills for research and problem solving, initiative development, decision making, and leadership in an academic or non-academic organization

Course Learning Outcomes

Acquire knowledge and application skills on technical topics, research skills, professional skills, and abilities to define, describe, analyze problems and evaluate and create solutions for problem solving in a certain course of the program

Learning Activities

Guided and self-initiated research, conferences, target readings, presentations, discussions, individual projects, team projects, peer evaluations, field inquiries, short essays, research paper projects, reports, reflections and assessment on various topics of the course

Program Format

Online delivery format with minimal residency and a cohort style with mutual group support to accommodate the educational, social and professional needs of busy working professionals

Professional and Career Goals

To be employed in the preferred field of practice and succeed and lead in academic or non-academic careers

Figure 1. Proposed Model for Designing Doctoral Programs for Working Professionals

The proposed model in Figure 1 above is a generic model for designing doctoral programs and curricula for working professionals. The model is of a hierarchical structure made up of these components: Professional and Career Goals, Doctoral Education Goals, Program Goals or Objectives, Course Learning Outcomes, Learning Activities and Program Format. Doctoral Education Goals include Creativity, Innovation, Critical Thinking, Knowledge Creation, and Problem Solving, which are common high level accomplishments desired for all doctoral programs. Professional and Career Goals are the practical need for doctoral graduates to obtain or enhance full-time employment in their areas of professional interest and be able to succeed and take up leadership in academic or non-academic career fields. The Professional and Career Goals are as at least equally important as (if not more important than) Doctoral Education Goals. Accomplishment of Professional and Career Goals depends on the success of other components in the model.

The high level Doctoral Education Goals in general refer to competencies in creativity, innovation, critical thinking, knowledge creation and problem solving acquired through the doctoral program of study. These goals depend on successful realization of the doctoral program goals or objectives, the learning outcomes and learning activities of each course as well as an appropriate and effective program format for delivery. The Doctoral Education Goals should support and contribute to the Professional and Career Goals of doctoral students because the competencies of creativity, innovation, critical thinking, knowledge creation, and problem solving are key indicators of successful performance and leadership in any professional field (Wang, 2018).

Doctoral Program Goals or Objectives depend on a high quality curriculum and courses for students to acquire in-depth knowledge and skills for research and problem solving, initiative development, decision making, and leadership in an academic or non-academic organization. Program Goals should directly support the general Doctoral Education Goals as well as the Professional and Career Goals. The knowledge, skills, and abilities obtained after completion of the doctoral program should prepare the doctoral students for success and leadership in their professional fields. Quality assurance of the doctoral curriculum through benchmark standards is essential to students' learning and fulfillment of the program goals and subsequently their educational goals and professional and career goals. For example, mapping the program curriculum and courses to the knowledge units and program criteria for the CAE-CDE designation is a strong mechanism for maintaining program quality for cybersecurity programs.

The Course Learning Outcomes component is course specific and directly supports the Program Goals or Objectives and the Professional and Career Goals. The course learning outcomes should include knowledge and application skills on technical topics, research skills, professional skills, and abilities to define, describe, analyze problems and evaluate and create solutions for problem solving on specific topics in a certain course of the program. The learning outcome descriptors of the CAE-CDE KUs provide specific learning outcomes for each topic area of Cybersecurity (NIETP, 2019). In technical programs such as Cybersecurity, the course topics and learning outcomes need to be reviewed and updated regularly and frequently in order to maintain currency and relevance of the course content and address emerging issues and topics.

Learning Activities directly support Course Learning Outcomes and contribute to students' Professional and Career Goals. Doctoral programs and courses should provide a wide variety of enriching and stimulating learning activities to help motivate student learning. Typical course activities in cybersecurity programs include target readings, presentations, discussions, individual technical projects, team projects, peer evaluations, research paper projects, progress reports, and reflections and self-assessment on various topics of the course. Activities on research methods and academic writing should also be included as both are essential skills that distinguish doctoral students from master's students (Inouye & McAlpine, 2019).

Finally, the Program Format directly contributes to the success of students' learning activities and Professional and Career Goals. The preferred program format for working professionals is online delivery with minimal residency along with a cohort style. Online delivery assisted by information and communication technologies creates a flexible and asynchronous learning environment with virtual conferencing, advising and team collaboration and only requires minimal travel by students for on-campus residencies reserved for critical face-to-face sessions and meetings. Such a schedule and delivery format would enable working professionals to find time to engage in and complete doctoral studies while maintaining their goals and responsibilities for their full-time careers, families, and personal life. A cohort style is another important element in the program format for working professionals, which creates abundant opportunities for doctoral students to receive mutual support from the group in academic, social and emotional respects that are critical to their success in the program.

METHODOLOGY

This research study uses a combined methodology of a survey and a case study. The survey is used to collect data to identify the interest, demand, and preferences for a potential PhD program in Cybersecurity for working professionals. The case study is to use the case scenario of a private non-profit university in the U.S. for the proposal of a PhD program in Cybersecurity for working professionals.

The survey was conducted online for a 4-week period using QuestionPro. The survey was set to allow completion once only per IP address using the QuestionPro cookie setting. All responses remain anonymous even though the respondent IP addresses were logged to prevent duplicate answers from the same respondent. The subjects and expected respondents of the survey who were given the online access to the survey were primarily working professionals with some IT or Cybersecurity background, including technical and management staff of a defense contractor organization in the U.S. and students and recent graduates from the master's programs in IT and Cybersecurity from two regionally accredited non-profit universities in the U.S. with both online and on-ground enrollment. Research shows that frequent and lengthy surveys these days lead to "survey fatigue" among survey subjects such as college students, which has significant impacts on the generalizability and external validity of the findings from surveys (Van Mol, 2017). To minimize the "survey fatigue" effect, the online survey of this study is designed to be very brief with only 3 required quick questions for the most important data needed: (1) Potential interest in pursuing a PhD degree in Cybersecurity in the near future (Yes or No); (2) Have a busy work schedule (Yes or No); and (3) Important feature(s) of a doctoral program in Cybersecurity that would interest the subject most (select one or more). Question 3 options include learning opportunities and focus in the program, program delivery format and residency, faculty, cost, and the "Other" option for write-in answers. The raw data was exported to Excel for analysis, including Pearson *r* value calculation for linear correlations.

This research also uses the case study method in proposing a PhD program in Cybersecurity for a regionally accredited private non-profit university in the northeast of the U.S. that serves traditional students and non-traditional students including working professionals from all over the U.S. and around the world. The program and curriculum design of the proposed PhD program in this case is based on the findings of the online survey on potential students and uses and illustrates the doctoral program design model explained above. The following section presents and discusses the findings of the survey and the program and curriculum design of the proposed PhD program in Cybersecurity.

FINDINGS

The total number of access and views of the online survey is 366. The total number of responses received is 237. The response rate is 64.75%, which is pretty high probably due to the short online survey design with a flexible response schedule and properly targeted audience. Table 1 below reports the data and results on the three survey questions (Q1 – Q3). Demographic data was not collected because the survey was conducted among a focused target audience of working professionals with some relevant IT and cybersecurity background.

The data on the responses to Question 1 shows that 83.54% of the respondents have an expressed interest in pursuing a Ph.D. degree in Cybersecurity in the near future. The finding indicates a strong demand for doctoral education in the Cybersecurity field given the fast growing student population of undergraduate and graduate (master's) programs and working professionals in IT and cybersecurity fields sampled by this question. Demand for doctoral education as reflected in stated personal interest is the most important justification for proposing and sustaining a doctoral program.

The response data on Question 2 shows that an overwhelming majority of 87.34% of respondents reported a busy work schedule. This finding should be a very important consideration in designing a doctoral program to help busy working professionals to succeed in the program while allowing them to maintain their professional and career goals.

The positive response rate (87.34%) is slightly higher than the positive response rate of 83.54% to Question 1, suggesting that some respondents may be too busy to have an expressed interest in pursuing the doctoral degree.

Question 3 has multiple answer options allowing one or more selections, and the results ranked from high to low are: (1) 71.31% of all respondents selected "Primarily online learning with minimal residency to accommodate your work schedule"; (2) 68.78% of respondents selected "Strong faculty with cybersecurity background"; (3) 66.24% of respondents selected "Opportunities for learning advanced cybersecurity knowledge and research skills"; (4) 52.74% of respondents selected "Affordable cost"; (5) 48.95% of respondents selected "Opportunities for learning advanced cybersecurity leadership and management skills"; and (6) 5.91% of respondents selected "Other" with various write-in input, including cohort format, preparation for college faculty positions, publication opportunities, scholarship and travel assistance, accommodation for family responsibilities. In addition, the Pearson correlation coefficient *r* value between Q2 answers and Q3 selection for primarily online with minimal residency is 0.83 and indicates a strong linear correlation between busy work schedule and preference for online learning with minimal residency. The findings on Question 3 selections reveal the preferences and concerns of prospective student population and provide important priorities for consideration in designing a cybersecurity doctoral program and curriculum for working professionals.

Table 1. Response Data on Survey Questions

Questions (Q1-Q3)	**Answers**	**Totals**	**Percentages**
Q1: Would you be interested in pursuing a Ph.D. degree in Cybersecurity in the near future?	Yes	198	83.54%
	No	39	16.46%
Q2: Do you have a busy work schedule?	Yes	207	87.34%
	No	30	12.66%
Q3: What important feature(s) of a doctoral program in Cybersecurity would interest you most? (Select one or more)	Primarily online learning with minimal residency to accommodate your work schedule	169	71.31%
	Strong faculty with cybersecurity background	163	68.78%
	Opportunities for learning advanced cybersecurity knowledge and research skills	157	66.24%
	Affordable cost	125	52.74%
	Opportunities for learning advanced cybersecurity leadership and management skills	116	48.95%
	Other	14	5.91%

CASE STUDY: PHD IN CYBERSECURITY

This section presents and discusses the sample proposal of a doctoral program named "Ph.D. in Cybersecurity" for a private non-profit university in the northeast of the U.S. The case institution for the program proposal is a regionally accredited and nationally ranked doctorate-granting university and values excellence, innovation, professional focus, inclusion and global perspective. The design of proposed program incorporates the Model for Designing Doctoral Programs for Working Professionals and the key findings from the survey presented above.

Here is an overview of the proposed program: The Ph.D. in Cybersecurity is a 3-year comprehensive multidisciplinary research program that prepares experts, researchers and leaders in various areas of Cybersecurity. The program is delivered primarily online with minimal residency for the first two years to accommodate working professionals. Students work as a cohort, and each student is required to complete a minimum of 54 credits including 36 credits of course work and 18 credits of dissertation. The proposed program goals/objectives are: (1) Have the knowledge, skills and abilities to conduct advanced research and analysis on cybersecurity vulnerabilities, threats, attacks, risks, countermeasures, and compliance; (2) Be able to assess and evaluate cybersecurity risks and recommend comprehensive solutions for protection, prevention, and incident response based on scientific research; (3) Be able to use research and data analysis for making strategic and operational decisions on cybersecurity issues for organizations; and (4) Provide leadership in cybersecurity research, planning, management and innovation with professional ethics. The program goals and objectives support the common goals of doctoral education and focus on the most important issues and topic areas in Cybersecurity to maintain academic rigor, excellence and currency that contribute to students' professional and career goals. The online format and minimal residency along with a cohort group style accommodate the needs of busy working professionals by providing more flexible and asynchronous study schedule and more opportunities for academic and social interactions and mutual support within the cohort group.

A rigorous and relevant curriculum is a key element of a successful doctoral program. Table 2 below summarizes the cohort curriculum and course sequence for the proposed program. The 9 credits each semester are the required minimum course work required for each student to complete the degree program. The special topics courses focus on significant current and emerging issues in Cybersecurity and may change from time to time. The courses of Doctoral Research in Cybersecurity I and II encourage students to explore advanced research in Cybersecurity that leads to quality publications and/or identification of a topic area for dissertation. Advanced research methods, data analysis methods and tools, dissertation process, and quality publication standards are also covered in these courses. Students are expected to complete the dissertation research, report and oral defense during the third year, but the optional Continuing Dissertation offering is available to students who need it. An optional Independent Study (3 credits max) is available for students to work with a doctoral faculty member on a relevant topic not currently offered in the curriculum. In addition, the program offers on-ground seminars and individual advising during residencies as well as regular online conferencing and other interactions as supplemental learning activities.

Table 2. Proposed Curriculum and Course Sequence

Year (Credits)	**Semester 1 Courses (credits)**	**Semester 2 Courses (credits)**
Year 1 (18 credits)	DCYB 8000 Cybersecurity Foundation (3) DCYB 8010 Research Methodology (3) DCYB 8020 Cybersecurity Management and Innovation (3)	DCYB 8030 Cyber Investigations and Incident Response (3) DCYB 8040 Advanced Network Security (3) DCYB 8050 Secure Systems Analysis and Design (3)
Year 2 (18 credits)	DCYB 8045 Data Security and Analytics (3) DCYB 8055 Special Topic: Economics of Cybersecurity (3) DCYB 8060 Doctoral Research in Cybersecurity I (3)	DCYB 8070 Advanced Cloud Security (3) DCYB 8075 Special Topics in Cybersecurity (3) DCYB 8080 Doctoral Research in Cybersecurity II (3)
Year 3 (18 credits)	DCYB 9010 Dissertation I (9)	DCYB 9020 Dissertation II (9)
Additional and optional course offerings include: DCYB 9030 Continuing Dissertation (6 credits each) DCYB 9040 Independent Study (3 credits max)		

The course work at the proposed doctoral program will include a variety of academically and intellectually stimulating and enriching activities, including guided and self-initiated research, conferencing, target readings, presentations, discussions, individual projects, team projects, peer evaluations, field inquiries, short essays, research paper projects, reports, reflections and assessment on various topics of the course. Each of the courses will have clearly defined learning outcomes that are assessed by the course learning activities and directly support the program objectives. For quality assurance and academic excellence, the curriculum and courses of the program are mapped to the current knowledge units (KUs) of the National Centers of Academic Excellence in Cyber Defense (CAE-CD) program (NIETP, 2019). Table 3 below summarizes the KU mappings to meet the standards and expectations of CAE-CD.

Table 3. CAE-CD KU Mapping with Ph.D. in Cybersecurity

CAE-CD Knowledge Units (KUs) (3 Optional KUs + Dissertation)	**Courses in Ph.D. in Cybersecurity**
Advanced Network Technology and Protocols (ANT)	DCYB 8000 Cybersecurity Foundation; DCYB 8040 Advanced Network Security
IA Architectures (IAA)	DCYB 8040 Advanced Network Security; DCYB 8070 Advanced Cloud Security
Vulnerability Analysis (VLA)	DCYB 8000 Cybersecurity Foundation; DCYB 8050 Secure Systems Analysis and Design

To maintain program quality and student success, certain admissions requirements and conditions need to be implemented prior to student enrollment. A relevant master's degree in IT or Cybersecurity is required for admission to the program and for curriculum mapping to the CAE-CD KUs for quality assurance. Provisional admissions may be granted to an applicant whose master's degree is not in a relevant field but who is willing to complete at least 18 credits of course work or the master's degree at the MS in Cybersecurity and Information Assurance program available both on-ground and online at the host institution in this case. Additionally, international students whose native language is not English must demonstrate their language proficiency through standard testing, such as TOEFL or IELTS. International perspectives and cooperation in cybersecurity research are important for developing solutions to rising challenges in Cybersecurity that involve various regions and countries in the world.

CONCLUSION

This research paper proposes a model of doctoral program and curriculum design for nontraditional student populations, including working professionals who have special needs and challenges in juggling between their career, family, and education. The proposed model delineates the key components of and relationships between professional and career goals, common doctoral education goals, program goals/objectives, course learning outcomes, learning activities and program format. This research uses an online survey for data collection to identify and confirm the interests, demand and preferences among working professionals. The findings from the survey provide valuable insight and priority considerations for designing a doctoral program in Cybersecurity for working professionals. This paper also contributes a sample proposal of program and curriculum design for a Ph.D. in Cybersecurity program for working professionals. The proposed program is of a cohort format with primarily online learning and minimal residency and has a rigorous curriculum and courses mapped to the knowledge units for the national Center of Academic Excellence in Cyber Defense Education (CAE-CDE) for quality assurance.

This paper is only a beginning research effort on proposing and designing a special doctoral program in Cybersecurity for working professionals. Once the program is implemented with valuable data accumulation, evaluation reports and sharing of experience and lessons learned will be considered for follow-up research on this topic. There should be expanding opportunities for research in each of the course areas of the program for the future as well. In addition, future progress and accomplishments in implementing the curriculum mapped to the CAE-CDE knowledge units could be shared with wider cybersecurity research and professional communities.

REFERENCES

Ali, A., & Kohun, F. (2006). Dealing with isolation feelings at IS doctoral programs. *International Journal of Doctoral Studies, 1*, 21-33.

Ali, A., & Kohun, F. (2007). Dealing with social isolation to minimize doctoral attrition – A four stage framework. *International Journal of Doctoral Studies, 2*, 33-49.

Allen, I. E., Seaman, J., Poulin, R., & Straut, T.T. (2016, February). Online report card: Tracking online education in the United States. Retrieved from http://onlinelearningsurvey.com/reports/onlinereportcard.pdf

Anderson, L., & Krathwohl, D. (Eds.). (2001). *A taxonomy for learning, teaching, and assessing: A revision of bloom's taxonomy of educational objectives.* Boston, MA: Allyn & Bacon, Pearson Education Group.

Aufman, S., & Wang, P. (2019). Discovering student interest and talent in graduate cybersecurity education. In S. Latifi (Eds.), *Information Technology - New Generations. Advances in Intelligent Systems and Computing, vol 55x* (pp.102-109). Springer International Publishing. DOI: 10.1007/978-3-030-14070-0

Baptista, A., Frick, L., Holley, K., Remmik, M., Tesch, J., & Åkerlind, G. (2015). The doctorate as an original contribution to knowledge: Considering relationships between originality, creativity, and innovation. *Frontline Learning Research, 3*(3), 55–67.

Berry, S. (2017). Student support networks in online doctoral programs: Exploring nested communities. *International Journal of Doctoral Studies, 12*, 33-48.

Brodin, E. M. (2018). The stifling silence around scholarly creativity in doctoral education: Experiences of students and supervisors in four disciplines. *High Educ, 2018* (75), 655-673.

Brodin, E. M., & Avery, H. (2014). Conditions for scholarly creativity in interdisciplinary doctoral education through an Aristotelian lens. In E. Shiu (Ed.), *Creativity research: An inter-disciplinary and multidisciplinary research handbook* (pp. 273–294). London: Routledge.

CESAER (Conference of European Schools for Advanced Engineering Education and Research). (2015). Innovative doctoral training at universities of science and technology. Retrieved from https://www.cesaer.org/content/statements-and-publications/2015/innovative-doctoral-training-at-universities-of-science-and-technology-discussion-paper.pdf

Charaniya, N. K., & Walsh, J. W. (2015). A case for collaborative inquiry in doctoral education. *New Directions for Adult and Continuing Education*, 147 (Fall 2015), 47-58. DOI: 10.1002/ace.20141

Cohen, J. B., Gammel, J. A., & Rutstein-Riley, A. (2016). Learning like adults: A hybrid interdisciplinary doctoral program for mid-career professionals. In P. Blessinger & D. Stockley (Eds.), *Emerging directions in doctoral education (Innovations in Higher Education Teaching and Learning, vol. 6,* pp. 189-205*)*. UK: Emerald Group Publishing Limited.

Denecke, D., Feaster, K., & Stone, K. (2017). *Professional development: Shaping effective programs for STEM graduate students*. Washington, DC: Council of Graduate Schools.

Druin, A., Jaeger, P. T., Golbeck, J., Fleischmann, K. R., Lin, J., Qu, Y., Wang, P., & Xie, B. (2009). The Maryland Modular Method: An approach to doctoral education in information systems. *Journal of Education for Library and Information Science, 50* (4), 293-301.

Fung, A. S. K., Southcott, J., & Siu, F. (2017). Exploring mature-aged students' motives for doctoral study and their challenges: A cross border research collaboration. *International Journal of Doctoral Studies, 12,* 175- 195.

Harris, M. A., & Patten, K. P. (2015). Using Bloom's and Webb's taxonomies to integrate emerging cybersecurity topics into a computing curriculum. *Journal of Information Systems Education, 26* (3), 219-234.

Hasib, M. (2015). *Cybersecurity leadership, 3rd ed*. Tomorrow's Strategy Today, LLC.

HighEdJobs. (2019, March 7). Faculty Positions. Retrieved from https://www.higheredjobs.com/faculty/

Hoyne, G., Alessandrini, J., & Fellman, M. (2016). Doctoral education for the future: Through the looking glass. In P. Blessinger & D. Stockley (Eds.), *Emerging directions in doctoral education (Innovations in Higher Education Teaching and Learning, vol. 6,* pp. 21-38*)*. UK: Emerald Group Publishing Limited.

Inouye, K., & McAlpine, L. (2019). Developing academic identity: A review of the literature on doctor-al writing and feedback. *International Journal of Doctoral Studies, 14,* 1-31.

Krathwohl, D. R., Bloom, B. S., & Masia, B. B. (1964). *Taxonomy of educational objectives: The classification of educational goals.* New York, NY: David McKay.

(ISC)^2. (2018). Cybersecurity professionals focus on developing new skills as workforce gap widens: (ISC)² cybersecurity workforce study 2018. Retrieved from https://www.isc2.org/research

Martinez, E., Ordu, C., Sala, M.R.D., & McFarlane, A. (2013). Striving to obtain a school-work-life balance: The full-time doctoral student. *International Journal of Doctoral Studies, 8, 2013,* 39-59.

National Science Foundation. (2018, December). 2017 Doctorate Recipients from U.S. Universities. Retrieved from https://ncses.nsf.gov/pubs/nsf19301/

NICCS (National Initiative for Cybersecurity Careers and Studies). (2018, November 28). Retrieved from https://niccs.us-cert.gov/about-niccs/glossary

NIETP (National IA Education & Training Programs). (2019). Centers of Academic Excellence in Cyber Defense (CAE-CD) 2019 Knowledge Units. Retrieved from https://www.iad.gov/NIETP/CAERequirements.cfm

NSA. (2019). National Centers of Academic Excellence. Retrieved from https://www.nsa.gov/resources/students-educators/centers-academic-excellence/

Offerman, M. (2011). Profile the nontraditional doctoral degree student. *New Directions for Adult and Continuing Education, 129, Spring 2011,* 21-30.

Pemberton, C.L.A., & Akkary, R.K. (2010). A cohort, is a cohort, is a cohort…or is it? *Journal of Research on Leadership Education, 5*(5), 179-208.

Sverdlik, A., Hall, N. C., McAlpine, L., & Hubbard, K. (2018). Journeys of a PhD student and unaccompanied minors. *International Journal of Doctoral Studies, 13,* 361-388.

US Labor Department BLS (Bureau of Labor Statistics). (2019). Retrieved from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

Van Mol, C. (2017). Improving web survey efficiency: The impact of an extra reminder and reminder content on web survey response. *International Journal of Social Research Methodology, 20* (4), 317-327. DOI: 10.1080/13645579.2016.1185255

Wang, P. (2018). Designing a doctoral level cybersecurity course. *Issues in Information Systems, 19(1)*, 192-202.

Wang, P., & Sbeit, R. (2017). A constructive team project model for online cybersecurity education. *Issues in Information Systems, 18* (3), 19-28.

White, S. K. (2016, April 25). Top U.S. universities failing at cybersecurity education. *CIO.* Retrieved from https://www.cio.com/article/3060813/it-skills-training/top-u-s-universities-failing-at-cybersecurity-education.html

Yazdani, S., & Shokooh, F. (2018). Defining doctorateness: A concept analysis. *International Journal of Doctoral Studies, 13,* 31-48.