Issues in Information Systems
Volume 19, Issue 1, pp. 192-202, 2018

DESIGNING A DOCTORAL LEVEL CYBERSECURITY COURSE

Ping Wang, Robert Morris University, wangp@rmu.edu

ABSTRACT

Doctoral education is often expected to produce advanced researchers and leaders in various areas. The curriculum and courses for each doctoral program need to be continually updated and improved to address rapid changes in society, especially for programs related to information systems and technology. Cybersecurity has become a fast-growing and increasingly significant area for information systems research and education and should be included in doctoral programs in information systems. This paper proposes a doctoral course design model with a case study of a new seminar course in Cybersecurity for a research doctoral program in Information Systems and Communications at a private university in northeastern United States. This case study analyzes key components of the course design and examines their value and relationships to the goals and objectives of doctoral education in general.

Keywords: Cybersecurity, goals, outcomes, research, creativity, innovation, problem solving, critical thinking

INTRODUCTION

Doctoral level education in general emphasizes research and knowledge creation to advance a certain field. The graduates of a doctoral program are usually expected to have obtained the breadth and depth of knowledge and skills necessary for research, leadership, and judgment in various fields or interdisciplinary fields. A major challenge for doctoral education is to continually update, improve, and transform the doctoral programs and courses in order to address the changing needs of students and society in general (Blessinger & Stockley, 2016). Due to rapid changes in technology, doctoral programs related to information systems and technology in particular need to be constantly reviewed, updated and improved to address the developments in technology, economy, and society. Cybersecurity has emerged as a significant and fast-growing subject area of professional and academic interests for practitioners and researchers and should be adequately addressed by a doctoral program related to information systems. This paper proposes a doctoral course design model and an inquiry-based seminar in Cybersecurity for the Doctor of Science in Information Systems and Communications (DISC) degree program at Robert Morris University (RMU), a private university in northeastern United States accredited by the Middle States Commission on Higher Education (MSCHE). The DISC program at RMU for the case study in this paper is a three-year program delivered in a cohort format. Designed to allow students to work full time while pursuing the degree, the program has low residencies for a total of 16 days (mostly weekends) per semester. The curriculum requirements include a sequence of seminars and a dissertation for a total of 63 credits beyond a master's degree. The program is inter-disciplinary and accepts students of diverse background. However, there is no course in Cybersecurity in the curriculum yet. Therefore, the case study proposes a 3-credit Cybersecurity Seminar course, which is designed to strengthen the DISC curriculum at RMU and support the DISC program objectives to "address the expanding needs of professionals who conduct research, manage information resources; solve information, communication and technology-related problems in organizations; or who educate or train others in applications of information systems and communications" (RMU DISC, para. 1).

Cybersecurity is a significant problem-solving area for the DISC program at RMU and similar programs at other institutions. Cybersecurity is the process of protecting information and communications systems from data breaches or unauthorized access, disruption, modification, or exploitation. There have been over 8,000 known data breaches with over 10 billion records breached since 2005 according to data from Privacy Rights Clearinghouse (PRC, 2018). The average cost of a data breach is over $3.6 million according to the 2017 study report by IBM Security and Ponemon Institute (Ponemon Institute, 2017). So Cybersecurity has become a very important and challenging problem related to information, communication, and technology for various organizations to solve and should have in-depth coverage in the curriculum of information systems programs like DISC at RMU.

Cybersecurity has strong intellectual merit and presents expanding opportunities for doctoral students to conduct advanced research. Cybersecurity is a multidisciplinary and sophisticated field that involves computer information

systems, computer science, technology, business management, communication, critical thinking, problem-solving and analytical skills. There have been growing peer-reviewed scholarly research publications and national and international conferences and symposia dedicated to the field of Cybersecurity, which has also become a priority area for funding support from NSF (National Science Foundation) and NSA (National Security Agency). In reality, advanced research centers and/or doctoral programs and courses in Cybersecurity have been in existence in many research universities, including University of Pittsburgh, Carnegie Mellon University, Northeastern University, University of Maryland, Purdue University, Georgia Tech, and MIT. The learning outcomes and course topics and activities designed for the proposed Cybersecurity Seminar will support the general goals of research, problem solving, critical thinking, and knowledge creation for doctoral education as well as the specific goals of programs like DISC at RMU. In addition, RMU is in the process of applying for the prestigious joint designation of Center of Academic Excellence in Cyber Defense Education (CAE-CDE) from NSA and DHS (Department of Homeland Security). The designation will enable RMU to become a national leader in cybersecurity education. The implementation of the proposed research seminar in Cybersecurity at the DISC program will be an important step in promoting cybersecurity education at RMU to a higher level and will help RMU to pursue the further designation of Center of Excellence in Research (CAE-R) in the future.

The proposed seminar in Cybersecurity will also help students at the doctoral programs like DISC to enrich their knowledge and better prepare them to address the expanding professional needs for Cybersecurity. A recent cybersecurity trend report concludes that the shortage of skilled employees is the biggest obstacle to stronger cybersecurity in organizations. The career outlook published by US Labor Department Bureau of Labor Statistics shows that the employment of information security analysts, an example of cybersecurity jobs, is projected to grow 28 percent from 2016 to 2026, much faster and with better pay than the average for all occupations (US Labor Department BLS, 2018). Search results from online job sites indicate a growing demand for senior level researchers, scientists, and educators in Cybersecurity, which require or prefer a relevant doctorate degree. The proposed course in Cybersecurity is valuable to doctoral students who plan to be educators to train future professionals in information systems and communications. The goal of this research is to share the proposed doctoral course design model and the course design case study with similar programs in information systems and technology at other institutions.
The following sections of the paper will review the theoretical background for the goals, directions, and models of innovation for doctoral education, formulate and describe the model for the proposed Cybersecurity Seminar case study, and analyzes and discusses the course learning outcomes and activities and how they are related to and support the goals for DISC-like programs and doctoral education in general. The paper concludes with suggestions for future and follow-up studies on this topic.

BACKGROUND

This section reviews the theoretical background for the goals, directions, and models of innovation for doctoral education that guide the design of doctoral curricula and courses. This section also identifies and discusses important outcomes and skills that support the academic and professional goals of doctoral education.

Creativity, innovation, critical thinking, and problem solving have been and should be the most important goals for doctoral education. Creativity is essential to advancing existing knowledge. Creativity is often associated with and defined with reference to the concepts of novelty, originality, and innovation. Baptista et al. (2015) recognize that creativity, innovation, and originality share a common focus on novelty in doctoral research. While originality emphasizes novel knowledge seeking, creativity is defined as seeking novelty with disciplinary relevance or value whereas innovation highlights problem-solving and application with economic relevance (Baptista et al., 2015). In addition, creativity for doctoral students is considered a journey of creative process that features independence and critical thinking and leads to a creative product such as the dissertation (Brodin, 2018). The creative process highlighting critical thinking is described as a journey in which the doctoral students learn "to critically think, act and speak, in individually novel, valuable, feasible and ethically defensible ways that may lead to a dissertation which is assessed to be outstanding by the community of peers" (Brodin & Avery, 2014, p. 277). The abilities to create a new product or point of view and analyze and evaluate with complex and critical thinking are categorized as the higher levels of learning taxonomy (Anderson & Krathwohl, 2001; Harris & Patten, 2015; Krathwohl, Bloom, & Masia, 1964). Therefore, the goals and objectives of a doctoral program and the learning outcomes and learning activities of the curriculum and courses should support the general goals of student creativity, innovation, critical thinking, and problem solving.

Professional and career goals are also very important for doctoral students who usually invest large amounts of money and time to complete the doctoral degree programs. The common practical concern for doctoral students is to obtain a better professional position upon completion of the program. A new trend in doctoral student demographics is that there are more and more mid-career professionals with diverse professional background (Cohen, Gammel, & Rutstein-Riley, 2016). The employment trend for doctoral programs is that more and more doctoral graduates go to work in organizations and industry outside academia (Hoyne, Alessandrini, & Fellman, 2016). The design of curriculum and courses for doctoral programs has to keep up with the career trends for doctoral students. In reality, however, the doctoral education system often fails to meet the needs of the majority of students. For example, over 60% of new doctoral graduates in science in the United States will not have careers in academic research, but the science curriculum for the doctoral programs has continued the same basic format for almost 100 years with primary focus on preparing academic researchers (CESAER, 2015). Given the increasingly competitive traditional academic job market and growing interest among doctoral students in non-academic careers, doctoral programs and courses should prepare their students for professional careers involving both academic and nonacademic activities and skills (Heflinger & Doykos, 2016). To help students reach their professional and career goals, the training at programs of doctoral education 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).

Teamwork and leadership skills are very important for the professional success of doctoral students. The design of doctoral curricula and courses should provide opportunities for collaborative learning. Collaborative knowledge construction and collaborative inquiry should be accepted as a normative aspect of doctoral education and integrated in the doctoral curriculum design (Charaniya & Walsh, 2015). Team-based collaboration is also recommended as a pedagogical model for complex problem solving in doctoral education especially for interdisciplinary programs (Bosque-Perez et al, 2016). Successful collaborative learning through teamwork can be achieved in tandem with reaching individual success. Individual motivation must be coordinated within a team community to minimize conflict and maximize team harmony and productivity. Team projects are a great example of learning activity that simulate a real world community of practice with professional interactions and knowledge sharing and knowledge creation in order to provide students with realistic teamwork experience and skills (Wang & Sbeit, 2017). The teamwork experience will also provide specific leadership roles in various professional areas for different student team members and help to develop their leadership skills and interpersonal skills. Assessment of both teamwork and individual participation and contributions is necessary to ensure effective implementation of team projects. The assessment measures will motivate team members to do their best collaboratively as a team and encourage each member to reach his or her best potential. Peer reviews including ratings and specific comments on each team member on the aspects of participation, contribution, collegiality, and communication are recommended for the team success (Wang & Sbeit, 2017). Peer-reviews are also necessary for reaching academic standards and excellence in research in doctoral education (University of Oulu, 2018).

To help students achieve multiple skills in doctoral studies in areas of information systems and technology, a pedagogically feasible approach to the curriculum and course design is necessary. Programs in information studies are interdisciplinary and multi-disciplinary in nature, involving disciplines such as computer science, information systems, digital technology, business management, social sciences, and quantitative and qualitative research skills. Students admitted to doctoral programs are increasingly of diverse professional and academic background. The Maryland Modular Method (M^3) designed by Druin et al. (2009) for the doctoral program in information studies at University of Maryland provides an exemplary modular approach to curricula and course design for doctoral education. The M^3 approach consists of the following four lenses (i.e. boundary objects connecting different disciplines) based on the notion that doctoral students will learn and grow better by examining academic topics and issues through these multiple "lenses" or perspectives: (1) The people lens that focuses on people who access and use information and the impact of information, systems, and contextual environment on people's work, life, and learning; (2) The systems lens that focuses on technical and organizational systems including hardware, software, networking, and processes and how they affect people's interaction with information; (3) The environment lens deals with the infrastructure surrounding people and systems and its impact on how people access and use information; and (4) The information lens as the core of information studies that examines how information interacts with people, systems, and environments (Druin et al., 2009). The lenses were used to define the modules of study, and each module was a 2-week long sub-course with self-contained research topics with suggested lenses, readings, and research questions. The modular design with iterative use of lenses allows course content to be constantly updated to keep up with changes in

information technology and their impacts on society and research. For example, the emerging cybersecurity topics, issues, and challenges identified by Fischer (2016) are closely related to information studies topics and involve people, systems, information, and environment. Such topics and perspectives have substantial value for researchers and practitioners and should be addressed in the curriculum for doctoral programs in information studies.

MODEL FOR DOCTORAL COURSE DESIGN

Based on the literature review in the section above, the following generic model for doctoral course design is proposed. This section describes the components of the model and their relationships. Figure 1 below illustrates the proposed hierarchical model.

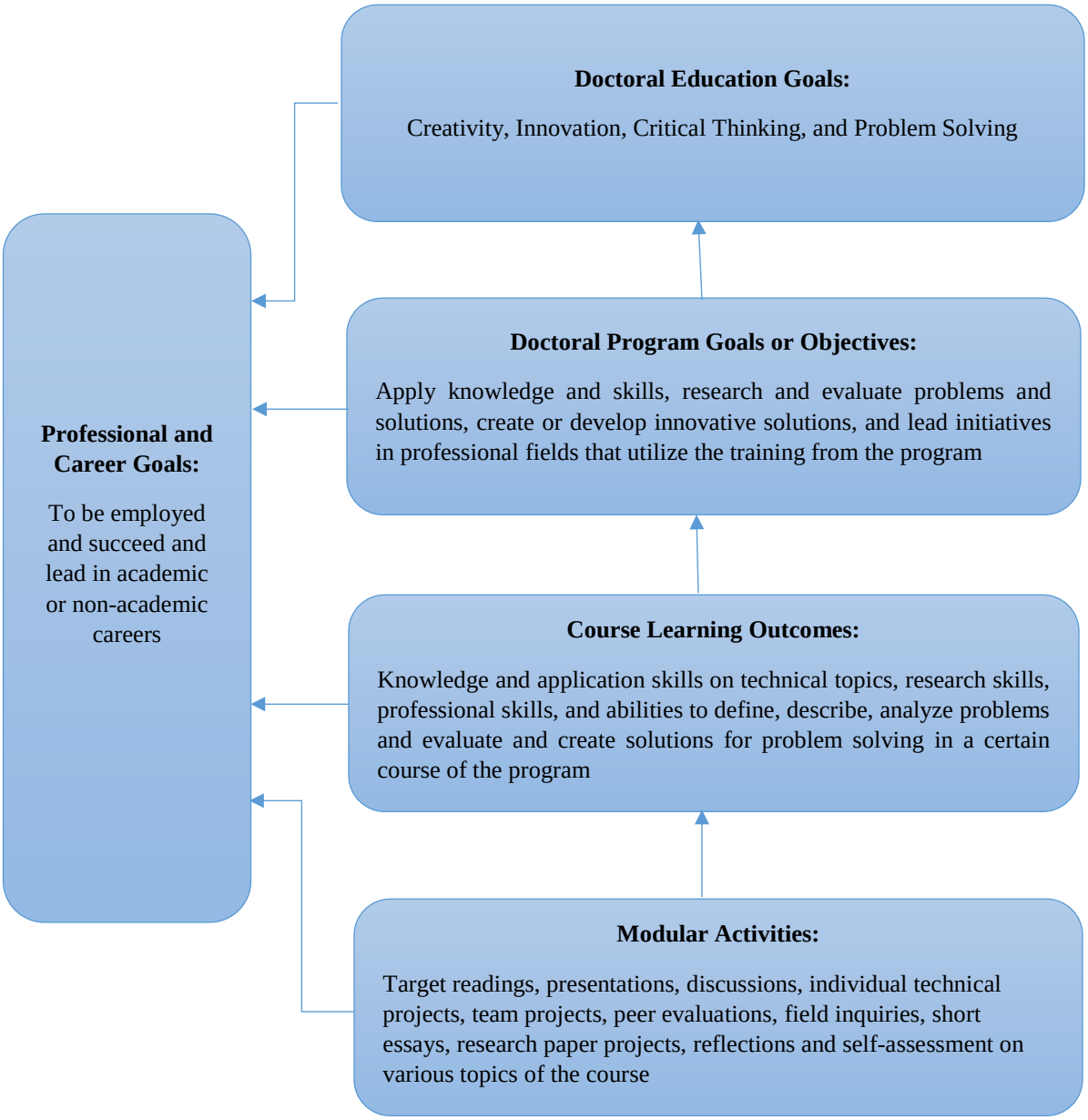

Figure 1. Doctoral Course Design Model

As shown in Figure 1 above, the doctoral course design model is placed in a larger context and the components of the model consist of Doctoral Education Goals, Professional and Career Goals, Program Goals or Objectives, Course Learning Outcomes, and Modular Activities. The model is hierarchical in general with Doctoral Education Goals at the top. Professional and Career Goals refer to the need for doctoral graduates to obtain full-time employment in their areas of professional interest and be able to succeed and take up leadership in academic or increasingly non-academic career fields. The Professional and Career Goals are as at least equally important as (if not more important than) Doctoral Education Goals and depend on successful implementations of other components of the model.

Doctoral Education Goals in general refer to competencies in creativity, innovation, critical thinking, and problem solving acquired through the doctoral program of study. These goals depend on successful implementation of the doctoral program goals or objectives as well as the learning outcomes and course activities of each course. The Doctoral Education Goals should support the Professional and Career Goals of doctoral students because the creativity, innovation, critical thinking, and problem solving competencies are key indicators of successful performance and leadership in any professional field. ‘

Doctoral Program Goals or Objectives should directly support the general Doctoral Education Goals as well as the Professional and Career Goals. The program goals and objectives are usually program specific and should include abilities to apply knowledge and skills, research and evaluate problems and solutions, create or develop innovative solutions, and lead initiatives in professional fields that utilize the training from the program. 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.

The Course Learning Outcomes component should directly support the Doctoral Program Goals or Objectives as well as the Professional and Career Goals. The course learning outcomes are course specific and 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 in a certain course of the program. In information systems and technology programs, the course topics and learning outcomes have to be frequently reviewed and updated in order to maintain currency and relevance of the course content and address emerging issues and topics (Blessinger & Stockley, 2016; Druin et al., 2009).

Finally, the Modular Activities component refers to the course specific activities that directly contribute to the Course Learning Outcomes and support the Professional and Career Goals. Typical course activities in information systems and technology programs include target readings, presentations, discussions, individual technical projects, team projects, peer evaluations, research paper projects, reflections and self-assessment on various topics of the course. These activities should be designed to provide opportunities for students to pursue both independence and team collaboration in research and technical work. The course activities should also embed various perspectives including the “lenses” of people, information, systems, and environment in studying information related topics (Druin et al., 2009).

The following section of the paper is to present a case study in designing a Cybersecurity Seminar course for a research-oriented doctoral program in Information Systems and Communications at a private US university. The goal of the case study is to illustrate the proposed course design model and share with similar programs elsewhere.

CASE STUDY: CYBERSECURITY COURSE DESIGN

Using the proposed doctoral course design model above, this section presents the case study of designing a Cybersecurity Seminar course for the Doctor of Science in Information Systems and Communications (DISC) degree program at Robert Morris University (RMU).

Here is a brief description of the proposed 3-credit course:

> This seminar reviews the fundamental concepts, principles, and practice in Cybersecurity and explores research issues in cybersecurity challenges, solutions, technologies, practices, and management. The course

topics include cybersecurity goals and concepts, vulnerabilities, threats, attacks, controls, security risks and management issues, security technologies and practices, software security, network security, cloud and Internet of Things (IoT) security, and cybersecurity education and workforce development. The course emphasizes critical thinking and problem solving in evaluating cybersecurity problems, solutions, practices, technologies, and challenges.

Cybersecurity is the process of protecting information and communications systems (NICCS, 2017). It has been a significant emerging topic area of research and practice for information systems and technology and should be included in doctoral programs related to information systems. Since this is the first course in Cybersecurity proposed for the DISC program and there is no cybersecurity prerequisite for the students in the program, it is necessary to cover the essential topics related to all aspects of securing information and information systems. The coverage of the fundamental topics in Cybersecurity also ensures that all students will have the technical knowledge, skills, and abilities on this important topic for their future careers. As this is a doctoral level course, the course content does emphasize higher cognitive skills of research, evaluation, and critical thinking and problem solving regarding cybersecurity technologies, issues, solutions, and emerging and potential challenges.

The course learning outcomes reflect the course emphasis and directly support the program goals and objectives as well as the professional and career goals of the students. Here are the proposed course learning outcomes:

1. Define cybersecurity goals, assets, threats, vulnerabilities, risks, and attacks
2. Describe fundamental cyber defense strategies and security design principles
3. Develop cybersecurity assurance policies for organizations
4. Analyze and evaluate strategies and plans for managing IT security and risks
5. Apply quantitative and qualitative methods to security risk analysis
6. Describe and evaluate access control problems, solutions, and challenges
7. Describe and evaluate software and operating system security problems, solutions, and challenges
8. Describe and evaluate wired and wireless network security problems, solutions, and challenges
9. Evaluate the developments in cloud and IoT security solutions
10. Identify professional organizations, resources, and forums for cybersecurity education and research
11. Critique and analyze sample research publications in Cybersecurity
12. Develop an initial research plan on a selected cybersecurity topic

The listed course learning outcomes emphasize technical knowledge and skills and critical thinking and problem solving skills on the most important existing and emerging topics in Cybersecurity. Theses outcomes directly support the overall objectives of the DISC program to address "the expanding needs of professionals who conduct research, manage information resources; solve information, communication and technology-related problems in organizations; or who educate or train others in applications of information systems and communications" (RMU DISC, para.1). The course learning outcomes also support the specific professional and career goals of the DISC program, which is designed for "professionals with decision-making and problem-solving responsibilities related to information systems, communications and technology, including:

- Chief information officers, chief knowledge officers, network administrators, in-house consultants, training specialists and other managers of information technology resources in corporate and professional organizations
- Educators and academic administrators in two-year, four-year and graduate institutions, as well as information officers and managers in educational institutions
- Professionals with a master's degree whose qualifications will be enhanced by such a doctoral degree, including those in fields such as accounting, finance, MIS, management, marketing, health care administration, telecommunications and corporate communications" (RMU DISC, para.3).

According to the latest data breach and investigations report by Verizon and the actual known cases of data breach since 2005 compiled by Privacy Rights Clearinghouse (PRC), cybersecurity attacks have occurred to all public and private sectors including financial and insurance services, retail, other businesses, educational institutions, healthcare and medical services, government and military, and nonprofits (PRC, 2018; Verizon, 2018). Therefore, the professionals and leaders listed above and targeted by the DISC program should have systematic training in

Cybersecurity at the doctoral level in order to handle challenging cybersecurity risks and incidents with adequate knowledge and skills, sound judgment and professional leadership. In addition, all educators from grade schools to postgraduate institutions need to know the critical knowledge, skills, and abilities for future cybersecurity professionals according to the National Initiative for Cybersecurity Careers and Studies (NICCS, 2018).

The course learning outcomes are also designed to support the stated interdisciplinary academic goals of the DISC program, which are:

- Develop and apply skills in a range of investigative methods, including qualitative methods grounded in economic, social and ethnographic disciplines, and quantitative methods grounded in statistical and social scientific disciplines.
- Conduct research and design innovative, effective solutions to information management and information resource problems.
- Stimulate field-based information management initiatives that link information, communications, technology and systems within organizations.
- Track new information technology and assist in incorporating it into an organization's strategy, planning and practice (RMU DISC, para.5).

The academic goals of the DISC program directly support the Doctoral Education Goals in general. Table 1 below presents the specific mappings between the general Doctoral Education Goals, the DISC program goals, and the course learning outcomes of the proposed Cybersecurity Seminar course:

Table 1. Mappings of Doctoral Education Goals, Program Goals, and Course Learning Outcomes

Doctoral Education Goals	**DISC Program Goals**	**Cybersecurity Course Learning Outcomes**
Creativity, Innovation, Critical Thinking, and Problem Solving	Develop and apply skills in a range of investigative methods, including qualitative methods grounded in economic, social and ethnographic disciplines, and quantitative methods grounded in statistical and social scientific disciplines.	Outcomes # 5, 11, 12
Creativity, Innovation, Critical Thinking, and Problem Solving	Conduct research and design innovative, effective solutions to information management and information resource problems.	Outcomes # 3, 4, 6, 7, 8, 9, 12
Creativity, Innovation, and Critical Thinking	Stimulate field-based information management initiatives that link information, communications, technology and systems within organizations.	Outcomes # 1, 2, 3, 4, 10
Innovation, Critical Thinking, and Problem Solving	Track new information technology and assist in incorporating it into an organization's strategy, planning and practice.	Outcomes # 1, 2, 3, 4, 9, 10

The planned activities for the Cybersecurity Seminar course are modular in design and involve on-ground residencies and online learning using Blackboard. The modular design features a different sub-topic in Cybersecurity for each residency session or week of online learning. There are a variety of learning activities, including target reading assignments, presentations, discussions, individual technical projects, team projects, peer evaluations, field inquiries, short essays, research paper projects, reflections and self-assessment on various topics of the course. The learning activities support the course learning outcomes as well as the professional and career goals for the students.

The target reading assignments include textbook chapters, selected research papers, technical reports, and resource links that center on various cybersecurity issues, risks, solutions, emerging challenges, research methods, and sample case studies. The required textbooks are *Computer security: Principles and practice* (4th ed.) by Stallings and Brown (2018) and *Publication Manual of the American Psychological Association (6th ed.)* (APA, 2010). These textbooks cover the fundamentals of the cybersecurity domain, technology, and management and academic writing skills required for the program. The *Research Methods for Cyber Security* by Edgar and Manz (2017) is also recommended for students to be familiar with the major quantitative and qualitative research methods used in the cybersecurity field. Supplemental readings will also be provided by the instructor. In addition, doctoral students are expected to explore additional literature through the library and other sources to conduct thorough and in-depth research on the topics for the course. The reading assignments along with other learning activities provide abundant opportunities for students to obtain a solid background in Cybersecurity and reach the course learning outcomes. Table 2 below shows the specific mapping between the course activities and supported course learning outcomes.

Table 2. Mappings of Learning Activities and Course Learning Outcomes

Learning Activities	**Supported Course Learning Outcomes**
Target reading assignments, presentations, and discussions	Outcomes # 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12
Individual technical projects	Outcomes # 2, 4, 6, 7, 8, 9
Team projects and peer evaluations	Outcomes # 1, 2, 3, 4, 5, 10, 11, 12
Field inquiries and short essays	Outcomes # 1, 2, 3, 4, 9, 10
Research paper projects	Outcomes # 1, 2, 4, 5, 11, 12
Reflections and self-assessment	Outcomes # 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12

In addition, the individual and teamwork activities including research presentations, discussions, team projects and peer reviews will provide valuable opportunities and experience for students to practice and improve their teamwork and leadership skills, scholarly discourse skills, research and investigation skills, and professional and interpersonal communication skills. These skills will contribute to students' professional and career goals as they are important for student success in obtaining and maintaining full-time careers in their areas of interest.

CONCLUSIONS

This paper proposes a doctoral course design model and presents a case study of designing a doctoral level Cybersecurity Seminar course for information systems and technology programs. Doctoral education is expected to produce advanced level researchers, professionals, and leaders that distinguish themselves in creativity, innovation, critical thinking, and problem solving. Doctoral program goals and objectives should support and contribute to the general goals of doctoral education as well as practical career and professional goals for doctoral students. There have been rapid changes and developments in information technology. Doctoral program curricula and courses, especially those related to information systems and technology, should be frequently reviewed and updated to keep up with the technical developments in order to stay current and relevant to educational and professional goals. Cybersecurity has emerged as a significant and fast-growing professional field and area of interest for research. Cyber attacks have affected all public and private organizations where doctoral students come from and work at, so Cybersecurity should be an important component in any doctoral curriculum related to information systems and technology.

The case study in this paper is a proposed 3-credit Cybersecurity Seminar course for the Doctor of Science in Information Systems and Communications (DISC) degree program at Robert Morris University (RMU). This course covers fundamental concepts, principles, and practice in Cybersecurity and explores research issues in cybersecurity

challenges, solutions, technologies, practices, and management. The course learning outcomes directly support the doctoral program goals and emphasize application of key technical knowledge and skills and higher level cognitive competencies in creativity, innovation, critical thinking, and problem solving. The learning activities for the course provide adequate resources and opportunities for students to achieve these learning outcomes and improve their teamwork and leadership skills and communication skills. These outcomes and skills will also contribute to students' professional and career goals. The design of the course in the case study should be applicable to similar programs in information systems and technology at other institutions.

The case study only presents first cybersecurity course proposed for the DISC curriculum at RMU and similar programs elsewhere. Improvements can be made after running the course. Future studies may include data and reports on the implementation and feedback results from running the proposed new course. This first course is expected to stimulate students' professional and research interested in the cybersecurity field. More specialized follow-up courses, such as cybersecurity management, security engineering, network security, and cloud security can be added and offered for interested students. It would also be desirable to have future collaboration with other institutions in doctoral curriculum and course design especially on cybersecurity topics. Once a sequence of courses in Cybersecurity have been successfully implemented, a new doctoral program in Cybersecurity could be an option for consideration with increasing demand for advanced education in this field.

REFERENCES

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.

APA (2010). *Publication manual of the American Psychological Association* (6th ed.). Washington, D.C.: American Psychological Association.

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.

Blessinger, P., & Stockley, D. (2016). Innovative approaches in doctoral education: An introduction to emerging directions in doctoral education. In P. Blessinger & D. Stockley (Eds.), *Emerging directions in doctoral education (Innovations in Higher Education Teaching and Learning, vol. 6*, pp. 1-20*)*. UK: Emerald Group Publishing Limited.

Bosque-Perez, N. A. et al. (2016). A pedagogical model for team-based, problem-focused interdisciplinary doctoral education. *BioScience, 66,* 477-488. doi:10.1093/biosci/biw042

Brodin, E. M. (2018). The stifling silence around scholarly creativity in doctoral education: Experiences of students and supervisors in four disciplines. *Higher Education,* 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.

CASAER (Conference of European Schools for Advanced Engineering Education and Research). (2015). Innovative doctoral training at universities of science and technology. Retrieved from http://www.cesaer.org/en/news items/news/innovative-doctoral-training-at-universities-of-science-and-technology-discussion-paper-now-availabl/

Charaniya, N. K., & Walsh, J. W. (2015). A case for collaborative inquiry in doctoral education. *New Directions for Adult and Continuing Education,* 147, 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.

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.

Edgar T. W., & Manz T. O. (2017). *Research methods for cyber security*. Cambridge, MA: Elsevier Inc.

Fischer, E. A. (2016, August 12). Cybersecurity issues and challenges: In brief. Retrieved from https://fas.org/sgp/crs/misc/R43831.pdf

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.

Helfinger, C. A., & Doykos, B. (2016). Paving the pathway: Exploring student perceptions of professional development preparation in doctoral education. *Innovative Higher Education,* 41(4), 343-358.

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.

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

NICCS (National Initiative for Cybersecurity Careers and Studies). (2018). Retrieved from https://niccs.us-cert.gov/formal-education

NICCS (National Initiative for Cybersecurity Careers and Studies). (2017). Retrieved from https://niccs.us-cert.gov/glossary

Ponemon Institute. (2017). 2017 Cost of data breach study. Retrieved from https://www.ibm.com/security/data-breach

PRC (Privacy Rights Clearinghouse). (2018). Data breaches. Retrieved from https://www.privacyrights.org/data-breaches

RMU DISC (Robert Morris University Doctor of Science in Information Systems and Communications). (2018). Retrieved from http://www.rmu.edu/OnTheMove/wpmajdegr.major_desc?iCalledBy=WPMAJDEGR&idegree=DS&imajor=ISCO&ischool=G

Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice* (4th ed.). Hoboken, New Jersey: Pearson Education, Inc.

University of Oulu. (2018). Seven principles for innovative doctoral training. Retrieved from http://www.oulu.fi/uniogs/training_principles

US Labor Department BLS (Bureau of Labor Statistics). (2018). Retrieved from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

Verizon. (2018). 2018 data breach investigations report (11th ed.). Retrieved from http://www.verizonenterprise.com/

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