



NEW PROGRAM PROPOSAL FORM

Sponsoring Institution(s): University of Central Missouri
Program Title: MS, Cybersecurity and Information Assurance/C1, Cybersecurity
Degree/Certificate: Master of Science/Certificate 1
Options: None
Delivery Site(s): Main Campus in Warrensburg, Missouri and Central Summit Campus in Lee's Summit, Missouri
CIP Classification: 11.1003
Implementation Date: Fall 2016
Cooperative Partners: None

AUTHORIZATION:

Dr. Kim Andrews, Vice Provost for Academic Programs and Services



11/18/2015

Name/Title of Institutional Officer

Signature

Date

Dr. Xiaodong Yue, yue@ucmo.edu

660-543-4930

Person to Contact for More Information

Telephone

Rationale for the MS in Cybersecurity and Information Assurance program

The Cyberspace Policy Review, published in 2009, argued for a national strategy to develop a cybersecurity workforce adequate in numbers and expertise to secure the United States in cyberspace. The existing workforce in cybersecurity is comprised of professionals who studied computer science or a related major for their undergraduate degree. This is because cybersecurity is a relatively new major and was not available when the present workforce was in college. Given the strong market demand, many such professionals recognize the need to get a formal education in Cybersecurity and Information Assurance to better protect and serve the needs of their organizations. A graduate degree in Cybersecurity and Information Assurance is an excellent option for such professionals. The MS in Cybersecurity and Information Assurance program has been designed to provide a strong foundation of principles of Cybersecurity and its applications. Since there is a legal, ethical, and risk analytics aspect of Cybersecurity that is integral to any solution, the program was designed to include a strong Information Assurance component in its curriculum. The program provides options for students to specialize in advanced cybersecurity skills like malware analysis, mobile and wireless security, secure programming, etc., through electives and special topics courses.



STUDENT ENROLLMENT PROJECTIONS

Year	1	2	3	4	5
Full Time	5	10	15	20	25
Part Time	5	5	5	5	5
Total	10	15	20	25	30

Please provide a rationale regarding how student enrollment projections were calculated:

Due to high market demand in the region and an insufficient number of Cybersecurity professionals available to fill the open positions, the program is expected to grow and achieve the above projections.

Provide a rationale for proposing this program, including evidence of market demand and societal need supported by research:

Market demand

The market demand for highly skilled cybersecurity professionals continues to grow. Almost four in 10 IT security positions went unfilled in 2013, according to a survey of more than 500 organizations by the Ponemon Institute, which studies privacy, data protection, and information-security policy [1]. The figure was almost six in 10 for senior security jobs [1]. It is increasingly becoming common for companies to require a graduate degree to hire cybersecurity professionals in senior positions.

According to the Bureau of Labor Statistics [2], the outlook for cybersecurity jobs (a typical position is information security analyst) is very positive.

Information Security Analysts	
2012 Median Pay	\$86,170 per year
Entry-Level Education	Bachelor's degree
Work Experience in a Related Occupation	Less than 5 years
On-the-job Training	None



Number of Jobs, 2012	75,100
Job Outlook, 2012-22	37% (Much faster than average)
Employment Change, 2012-22	27,400

According to another Bureau of Labor Statistics data reported by www.careerinfonet.org, cybersecurity is the second fastest growing occupation in the United States with a projected growth rate of 37% over the next decade [3].

Top 10 Fastest-Growing Occupations in US

#	Occupation	Employment		Percent * Change
		2012	2022	
1	<u>Interpreters and Translators</u>	63,600	92,900	46%
2	<u>Information Security Analysts</u>	75,100	102,500	37%
3	<u>Meeting, Convention, and Event Planners</u>	94,200	125,400	33%
4	<u>Market Research Analysts and Marketing Specialists</u>	415,700	547,200	32%
5	<u>Geographers</u>	1,700	2,200	29%
6	<u>Personal Financial Advisors</u>	223,400	283,700	27%
7	<u>Operations Research Analysts</u>	73,200	92,700	27%
8	<u>Biomedical Engineers</u>	19,400	24,600	27%
9	<u>Cost Estimators</u>	202,200	255,200	26%
10	<u>Actuaries</u>	24,300	30,600	26%

In Missouri, cybersecurity is the third fastest growing occupation with a projected growth rate of 28% over the next decade [3].

Top 10 Fastest-Growing Occupations in Missouri

#	Occupation	Employment		Percent * Change
		2012	2022	
1	<u>Interpreters and Translators</u>	960	1,270	33%
2	<u>Food Scientists and Technologists</u>	630	820	30%
3	<u>Information Security Analysts</u>	1,490	1,910	28%
4	<u>Meeting, Convention, and Event Planners</u>	2,020	2,580	28%
5	<u>Operations Research Analysts</u>	910	1,150	27%
6	<u>Market Research Analysts and Marketing Specialists</u>	6,520	8,240	26%
7	<u>Logisticians</u>	2,240	2,790	25%



#	Occupation	Employment		Percent * Change
		2012	2022	
8	<u>Geographers</u>	30	40	24%
9	<u>Cost Estimators</u>	5,010	6,190	23%
10	<u>Actuaries</u>	610	750	23%

Based on inputs from several members of our Computer Science Advisory Board (comprising of our alumni in senior positions at companies in the region like Cerner, Garmin, etc.), we found that many computer science working professionals with an undergraduate degree in computer science or a related field want to specialize in cybersecurity and would like to do graduate level study in cybersecurity. Such individuals would like to move into cybersecurity teams in their organization after completing a master's degree in cybersecurity. This move to cybersecurity teams is popular because of the high market demand and high salaries in cybersecurity. A survey reported by CIO revealed that Cybersecurity salaries are three times the national average [4].

Many cybersecurity jobs in government require super specialized cybersecurity skills like malware detection, cryptographic protocol design, etc., that can only be offered at a graduate level [1]. A large number of such private and government jobs are in the Kansas City area. Several such jobs remain unfilled for long due to shortage of highly skilled cybersecurity professionals in the region.

In a survey of 183 institutions offering cybersecurity programs, the largest segment of degree programs was the master's degree [5]. In the same survey, one of the characteristics of the top 10 institutions offering cybersecurity programs was that they offered both a bachelor's and master's program in cybersecurity [5]. With the undergraduate cybersecurity program beginning in Fall 2015, the addition of a graduate program will not only show UCM's commitment to serving the region's needs but also uniquely place UCM as a go to institution for major employers in the region to hire cybersecurity professionals.

Student demand

Many students, both domestic and international, inquire about graduate level offering in cybersecurity at UCM. A graduate level program in cybersecurity would provide an opportunity for students from different but related majors to specialize in cybersecurity and serve the region's and nation's growing need for cybersecurity professionals.

Societal need

Missouri ranks 5th in the U.S. in the number of cybersecurity breaches according to the St. Louis Business Journal [6]. Recent cyber attack on Anthem-one of the largest health insurance provider-again highlighted the need for increased cybersecurity education and training of existing workforce and preparing a new generation of cybersecurity workers ready for securing our cyberspace from intruders and attackers [7]. Many other cyber attacks in recent times have caused significant financial loss and inconvenience to many businesses and citizens. The following facts illustrate the impact of a few of these cyber attacks.

- \$445 billion is lost annually to cybercrime and espionage across the entire world economy, according to the Center for Strategic and International Studies.
- 182,000 beneficiaries of Medicaid and the Children's Health Insurance Program had their personal information stolen, and about 25,000 Social Security numbers were compromised in a 2012 breach of the Utah Department of Health.



- 53% of U.S. companies expressed little to no confidence to stopping security breaches in the next 12 months.
- The National Nuclear Security Administration, an arm of the Energy Department, records 10 million attempted hacks a day.
- 50 million people in North America were without power for as long as four days after an August 2003 cyberattack on the electrical grid, according to a study by the U.S. and Canadian governments.
- 6 million social security numbers were exposed in a 2012 data breach of South Carolina's Department of Revenue.

The Federal government has recognized the importance of cybersecurity at all levels and a Comprehensive National Cybersecurity Initiative (CNCI) was established by President George W. Bush in 2008 and continued by President Obama [8]. CNCI Initiative#8 puts emphasis on expanding Cyber Education "to develop a technologically-skilled and cybersavvy workforce with the right knowledge and skills".

Duplication and Collaboration: If similar programs currently exist in Missouri, what makes the proposed program necessary and/or distinct from the others at public institutions, area vocational technical schools, and private career schools?

Given the University of Central Missouri's statewide mission in applied sciences and technology programs, UCM is in some way a natural home for the proposed M.S. in Cybersecurity and Information Assurance program. By searching the program inventory provided by Missouri Department of Higher Education (<http://collegesearch.mo.gov/>) using the CIP code 11.1003 designated for the proposed program, two universities in Missouri are currently offering master programs in Cybersecurity: Missouri State University and Washington University in St. Louis. Both programs are management orientated while our program is technical oriented. Due to geographically unbalanced locations of master Cybersecurity programs, the closest institution offering a graduate Cybersecurity program is more than 110 miles away from Warrensburg and Lee's Summit. On the other hand, a clear majority of UCM students are from our traditional 21 service counties and are tied to this area by jobs and/or family responsibilities. Many of the students have circumstances making going elsewhere to college impossible. The options available to them are largely determined by the options provided at UCM. Furthermore, there are family concerns requiring entry into the selected program as fast as feasible for financial reasons. As a comprehensive regional university with a statewide mission in applied sciences and technology programs, it is our mission to provide Missouri citizens in our service region and/or beyond more access to affordable graduate study in Cybersecurity and Information Assurance within reasonable driving distance.

Does delivery of the program involve a collaborative effort with any external institution or organization? If yes, please complete Form CL.

No. The current Computer Science faculty members at UCM are qualified and sufficient to handle the new program. Delivering the program will not involve collaborative efforts with any external institution or organization.

References



1. "The U.S. Government Wants 6,000 New 'Cyberwarriors' by 2016" by Dune Lawrence. April 15th, 2015. Bloomberg Business. Available online at: <http://www.bloomberg.com/bw/articles/2014-04-15/uncle-sam-wants-cyber-warriors-but-can-he-compete>.
2. Bureau of Labor Statistics, U.S. Department of Labor, Occupational Outlook Handbook, 2014-15 Edition, Information Security Analysts, on the Internet at <http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm>
3. On the Internet at <http://www.careerinfonet.org/oview1.asp?next=oview1&Level=edu3&optstatus=&jobfam=&id=1&nodeid=3&socode=&stfips=&ShowAll=>
4. "Cybersecurity Pros in High Demand, Highly Paid and Highly Selective" by Kenneth Corbin. CIO, Aug 8th, 2013. Available online at <http://www.cio.com/article/2383451/careers-staffing/cybersecurity-pros-in-highdemand--highly-paid-and-highly-selective.html>
5. "2014 Best Schools for Cybersecurity" Ponemon Institute Research Report. February, 2014. Available online at: http://www.hp.com/hpinfo/newsroom/press_kits/2014/RSAConference2014/Ponemon_2014_Best_Schools_Report.pdf
6. "Missouri ranks No. 5 in US for cybersecurity breaches" <http://www.bizjournals.com/stlouis/blog/2014/05/missouri-ranks-no-5-in-u-s-for-cybersecurity.html>
7. "Anthem Cyber Attack: 5 Things That Could Happen to Your Personal Information". Available online at: <http://abcnews.go.com/Business/anthem-cyber-attack-things-happen-personal-information/story?id=28747729>
8. The Comprehensive National Cybersecurity Initiative. Available online at: <http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/nationalinitiative>



PROGRAM STRUCTURE

M.S. in Cybersecurity and Information Assurance Program Structure

A. Total credits required for graduation: 30

B. Residency requirements, if any: N/A

C. General education: Total credits: N/A

D. Courses (specific courses OR distribution area and credits):

Required Graduate Courses (15 hrs)

CS 5310 Design of Cryptographic Algorithms and Protocols (3 credit hours)

CS 5920 Software Security Assessment (3 credit hours)

CS 4820 Introduction to Information Assurance (3 credit hours)

CS 5800 Advanced Computer Networking and Security (3 credit hours)

CS 5300 Advanced Algorithms and Data Structures (3 credit hours)

Elective Group I (9 hrs)

CS 4140 Web Applications Security (3 credit hours)

CS 4840 Ethical Hacking (3 credit hours)

CS 5140 Introduction to Malware (3 credit hours)

CS 5050 Special Topics in Cybersecurity (3 credit hours)

CS 5060 Internship in Cybersecurity (3 credit hours)

Elective Group II (6 hrs)

CS 4600 Database Theory and Applications (3 credit hours)

CS 5500 Advanced Operating Systems (3 credit hours)

CS 5910 Advanced Software Engineering (3 credit hours)

CS 5900 Compiler Design and Construction (3 credit hours)

E. Free elective credits: N/A

(Sum of C, D, and E should equal A.)

F. Requirements for thesis, internship or other capstone experience:

Internship (CS 5060 Internship in Cybersecurity) is optional to the students.

G. Any unique features such as interdepartmental cooperation:

N/A



PROGRAM STRUCTURE

C1 Graduate Certificate in Cybersecurity Program Structure

A. Total credits required for graduation: 15

B. Residency requirements, if any: N/A

C. General education: Total credits: N/A

D. Major Requirements: Total credits: 15

Course Number	Credits	Course Title
CS 5310	3	Design of Cryptographic Algorithms and Protocols
CS 5920	3	Software Security Assessment
CS 5140	3	Introduction to Malware
CS 4820	3	Introduction to Information Assurance
CS 4840	3	Ethical Hacking

E. Free elective credits: N/A

(Sum of C, D, and E should equal A.)

F. Requirements for thesis, internship or other capstone experience: N/A

G. Any unique features such as interdepartmental cooperation: N/A



PROGRAM CHARACTERISTICS AND PERFORMANCE GOALS

Institution Name: University of Central Missouri
Program Name: MS in Cybersecurity and Information Assurance/CI Graduate Certificate in Cybersecurity
Date: Fall 2016

(Although all of the following guidelines may not be applicable to the proposed program, please carefully consider the elements in each area and respond as completely as possible in the format below. Quantification of performance goals should be included wherever possible.)

1. Student Preparation

- Any special admissions procedures or student qualifications required for this program which exceed regular university admissions, standards, e.g., ACT score, completion of core curriculum, portfolio, personal interview, etc. Please note if no special preparation will be required.

To be admitted to the program

- *a student must have an undergraduate degree in computer science or a related discipline. Applicants who have degrees in some non-computing fields will also be considered for admission provided they have completed at least one programming course and one data structures course with a grade of B or better;*
- *student must have a minimum undergraduate grade point average (GPA) of 2.8; and*
- *applicants must complete the Graduate Record Examination (GRE) with a minimum combined score of 291 (1000 on the old scale) in Verbal and Quantitative reasoning.*
- Characteristics of a specific population to be served, if applicable.

N/A

2. Faculty Characteristics

- Any special requirements (degree status, training, etc.) for assignment of teaching for this degree/certificate.

Ph.D. in Computer Science or a closely related area.

- Estimated percentage of credit hours that will be assigned to full time faculty. Please use the term "full time faculty" (and not FTE) in your descriptions here.

All courses will be taught by full-time faculty.

- Expectations for professional activities, special student contact, teaching/learning innovation.



Faculty teaching in this program will be expected to be professionally active, as evidenced by peer reviewed publications and/or externally funded grants. Faculty will also be expected to attend and/or present at professional meetings, participate in workshops/seminars in areas related to their specialties and involve in other related professional activities (e.g. editor of a professional journal, referee for peer reviewed journals and conference proceedings, hold an office in a regional, national or international organization, etc.). Furthermore, faculty are expected to continue improving their teaching by keeping up to date on material or pedagogy.

3. Enrollment Projections

- Student FTE majoring in program by the end of five years.

25 students

- Percent of full time and part time enrollment by the end of five years.

83.4% full time, 16.6% part time

4. Student and Program Outcomes

- Number of graduates per annum at three and five years after implementation.

Three years-10, Five years-15

- Special skills specific to the program.

Graduates of the program would have the advanced skills in Cybersecurity. After completing the program, they should be able to design, implement, and deploy cybersecurity solutions for protecting an organization's information resources on a computer network.

The graduate with a Master of Science degree in Cybersecurity and Information Assurance will use the knowledge and skills obtained in the program to:

- 1. Design, implement and analyze an organization's information security policies.*
- 2. Design, implement, and deploy cybersecurity solutions for protecting an organization's information resources.*
- 3. Identify the appropriate cryptographic algorithms and protocols to be deployed in the context of an organization's security policy.*
- 4. Assess the security vulnerabilities of an organization's networks against cyber adversaries.*
- 5. Design and implement secure software.*
- 6. Design and implement appropriate incident response and handling procedures in case of a security breach.*
- 7. Address the needs of society with a sense of professionalism*
- 8. Adapt to a dynamic multidisciplinary technological environment through teamwork, ethical concerns, and effective communication*
- 9. Stay abreast of advancements in the area of Cybersecurity and Information Assurance*

- Proportion of students who will achieve licensing, certification, or registration.



N/A

- Performance on national and/or local assessments, e.g., percent of students scoring above the 50th percentile on normed tests; percent of students achieving minimal cut-scores on criterion-referenced tests. Include expected results on assessments of general education and on exit assessments in a particular discipline as well as the name of any nationally recognized assessments used.

None available.

- Placement rates in related fields, in other fields, unemployed.

95% in Cybersecurity related fields, 5% in other fields, 0% unemployed

- Transfer rates, continuous study.

N/A

5. Program Accreditation

- Institutional plans for accreditation, if applicable, including accrediting agency and timeline. If there are no plans to seek specialized accreditation, please provide a rationale.

UCM will also seek recognition as a National Security Agency (NSA) designated Center for Academic Excellence (CAE) in Information Assurance/Cyber Defense (IA/CD).

6. Alumni and Employer Survey

- Expected satisfaction rates for alumni, including timing and method of surveys.

Around 90% satisfaction. A paper survey will be sent to graduates at periods of one and three years after their graduation to gauge how the program has prepared them for their careers. Data from the survey will be compiled and analyzed to improve the quality of the program. An electronic version of the survey will also be available on the department website.

- Expected satisfaction rates for employers, including timing and method of surveys.

Around 90% satisfaction. Survey will be sent to employer(s) every summer. Data from the survey will be compiled and analyzed to improve the quality of the program. An electronic version of the survey will also be available on the department website.

7. Institutional Characteristics

- Characteristics demonstrating why your institution is particularly well equipped to



support the program.

Founded as a teacher's college in 1871, the University of Central Missouri has maintained its commitment to excellent teaching. UCM has a statewide mission in applied sciences and technology programs. Our average undergraduate class size is 24. UCM's six-month job-placement rate for undergraduates is 92 percent, and, reflecting our excellent financial support packages, our students benefit from one of the lowest student-debt ratios in the state. Publicly supported, richly diverse in our people and programs, UCM offers a remarkable educational experience.