



New Program Report

Date Submitted:

04/15/2019

Institution

University of Missouri-St. Louis

Site Information

Implementation Date:

6/3/2019 12:00:00 AM

Added Site(s):

Selected Site(s):

University of Missouri-St. Louis, 1 University Blvd, St. Louis, MO, 63121-4400

CIP Information

CIP Code:

111003

CIP Description:

A program that prepares individuals to assess the security needs of computer and network systems, recommend safeguard solutions, and manage the implementation and maintenance of security devices, systems, and procedures. Includes instruction in computer architecture, programming, and systems analysis; networking; telecommunications; cryptography; security system design; applicable law and regulations; risk assessment and policy analysis; contingency planning; user access issues; investigation techniques; and troubleshooting.

CIP Program Title:

Computer and Information Systems Security/Information Assurance

Institution Program Title:

Cybersecurity

Degree Level/Type

Degree Level:

Bachelor's Degree

Degree Type:

Bachelor of Science

Options Added:

Computer Science (CS)

Information Systems and Technology (IST)

Collaborative Program:

N

Mode of Delivery

Current Mode of Delivery

Classroom

Hybrid



New Program Report

Online

Student Preparation

Special Admissions Procedure or Student Qualifications required:

None

Specific Population Characteristics to be served:

n/a

Faculty Characteristics

Special Requirements for Assignment of Teaching for this Degree/Certificate:

Normative departmental standards in Computer Science and Information Systems and Technology will apply.

Estimate Percentage of Credit Hours that will be assigned to full time faculty:

75% for Full-Time Faculty

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

Faculty are actively involved in prof. dev., student mentoring and guidance toward developing applied cybersecurity (CYBSEC) skills, as well as activities related to community outreach, partnership dev., and service. Core CYBSEC faculty are also involved in developing innovative lab infrastructures, assignments, and learning tools for students by drawing on external grant funding, donations from/partnerships with CYBSEC related firms, and collaborations with other academics in and outside UMSL.

Student Enrollment Projections Year One-Five

Year 1	Full Time: 28	Part Time: 12	
Year 2	Full Time: 89	Part Time: 38	
Year 3	Full Time: 142	Part Time: 61	Number of Graduates: 14
Year 4	Full Time: 188	Part Time: 81	
Year 5	Full Time: 231	Part Time: 99	Number of Graduates: 38

Percentage Statement:

n/a

Program Accreditation

Institutional Plans for Accreditation:

UMSL has already been designated a Center of Academic Excellence in Cyber Defense Education (CAE-CDE) by the National Security Agency and the US Department of Homeland Security for its existing cybersecurity certificates. This degree program is designed to comply with the CAE-CDE undergraduate degree standards and is expected to meet CAE guidelines when designation is reviewed/renewed in 2021.

Program Structure

Total Credits:

126



New Program Report

Residency Requirements:

Transfer students must complete at least 30 hours and at least 15 major hours in residence.

General Education Total Credits:

42

Major Requirements Total Credits:

111

Course(s) Added

COURSE NUMBER	CREDITS	COURSE TITLE
INFSYS 3806	3	Managerial Apps of Object-Oriented Prog. I
SCMA 3301	3	Introduction to Supply Chain Management
SCMA 4347	3	Introduction to Project Management
CMP SCI 2750	3	System Programming and Tools
CMP SCI 1250	3	Introduction to Computing
CMP SCI 3760	3	Cyber Threats and Defense
INFSYS 2800	3	Information Systems and Technology Concepts and Applications
MATH 3000	3	Discrete Structures
CMP SCI 2250	3	Programming and Data Structures
CMP SCI 4782	3	Information Security
ENGL 3120/3130	3	Business Writing or Technical Writing
BUS AD 2900	3	Legal Environment of Business
SCMA 3300	3	Business Analytics and Statistics
INFSYS 3815	3	Object Oriented Applications in Business
CMP SCI 4700	3	Computer Forensics
COMP SCI EMPH	9	Major Specific Electives
ACCTNG 2410	3	Managerial Accounting
MGMT 3600	3	Management and Organizational Behavior
INFSYS 3868	3	Secure Software Development
INFSYS 3820	3	Introduction to Systems Administration
INFSYS 3845	3	Database Management Systems



New Program Report

ACCTNG 2400	3	Fundamentals of Financial Accounting
CMP SCI 4794	3	Introduction to Security of IoT Systems
INFSYS 3842	3	Data Networks and Security
MKTG 3700	3	Basic Marketing
MGMT 4219	3	Strategic Management
IST	6	Major Specific Electives
MATH 1105	3	Basic Probability and Statistics
CMP SCI 3130	3	Design and Analysis of Algorithms
CMP SCI 3780	3	Software Security
MATH 1320	3	Introduction to Probability and Statistics
FINANCE 3500	3	Financial Management
INFSYS 3848	3	Introduction to Information Security
ECON 1001	3	Principles of Microeconomics (MOTR ECON 102)
CMP SCI 3010	3	Web Programming
INFSYS 3858	3	Advanced Security and Information Systems and Technology
	3	Cultural Diversity Requirement
CMP SCI 4750	3	Introduction to Cloud Computing
CMP SCI 4730	3	Computer Networks and Communications
MATH 1800	5	Analytic Geometry and Calculus I
CMP SCI 4760	3	Operating Systems
INFSYS 3878	3	Information Security Risk Management and Business Continuity
ECON 1002	3	Principles of Macroeconomics (MOTR ECON 101)
CMP SCI 4732	3	Introduction to Cryptography for Computer Security
MATH 1100	3	Basic Calculus
MATH 1030	3	College Algebra (MOTR MATH 130)



New Program Report

CMP SCI 2700	3 Computer Organization and Architecture
CMP SCI 2261	3 Object-Oriented Programming

Free Elective Credits:

13

Internship or other Capstone Experience:

none (internship included as a major specific elective)

Assurances

I certify that the program is clearly within the institution's CBHE-approved mission. The proposed new program must be consistent with the institutional mission, as well as the principal planning priorities of the public institution, as set forth in the public institution's approved plan or plan update.

I certify that the program will be offered within the proposing institution's main campus, CBHE-approved service region or CBHE-approved off-site location.

I certify that the program will not unnecessarily duplicate an existing program within the geographically applicable area.

I certify that the program will build upon existing programs and faculty expertise.

I certify that the program can be launched with minimal expense and falls within the institution's current operating budget.

I certify that the institution has conducted research on the feasibility of the proposal and it is likely the program will be successful. Institutions' decision to implement a program shall be based upon demand and/or need for the program in terms of meeting present and future needs of the locale, state, and nation based upon societal needs, and/or student needs.

Contact Information

First and Last Name: JANA MOORE

Email: moorejan@umsystem.edu

Phone: 573-882-6398

University of Missouri - Saint Louis
Bachelor of Science in
Cybersecurity

Table of Contents

Executive Summary	7
1. Introduction.....	8
2. Fit with University Mission and Other Academic Programs.....	9
2.A. Alignment with Mission and Goals	9
2.B. Duplication and Collaboration Within Campus and Across System	10
3. Business-Related Criteria and Justification	10
3.A. Market Analysis	10
3.A.1. Need for Program.....	10
3.A.2. Student Demand for Program	12
3.B. Financial Projections.....	14
3.B.1. Additional Resources Needed.....	14
3.B.2. Revenue.....	15
3.B.3. Net Revenue.....	16
3.B.4. Financial and Academic Viability	18
3.C. Business and Marketing Plan: Recruiting and Retaining Students.....	18
4. Institutional Capacity	21
5. Program Characteristics.....	22
5.A. Program Outcomes.....	22
5.B. Structure.....	23
5.C. Program Design and Content	28
5.D. Program Goals and Assessment.....	28
5.E. Student Preparation.....	29
5.F. Faculty and Administration.....	29
5.G. Alumni and Employer Survey	31
5.H. Program Accreditation	31

Tables

Table 1a. Student Enrollment Projections (anticipated total number of students enrolled in program during the fall semester of given year).....	14
Table 1b. Student Enrollment Projections (anticipated number of students enrolled during the fall semester of given year who were new to campus).	14
Table 1c. Projected Number of Degrees Awarded	14
Table 2. Financial Projections for Proposed Program for Years 1 Through 5.	17

Table 3: Enrollment at End of Year 5 for Program to Be Financially and Academically Viable 18

Table 4. BS Cybersecurity Degree Crosswalk with NICE CWF Categories 23

Appendices

Appendix A: B.S. Cybersecurity, Computer Science Emphasis, 4-Year Plan 32

Appendix B: B.S. Cybersecurity, Information Systems and Technology Emphasis, 4-Year Plan 34

Appendix C: Existing Supporting Infrastructure 36

Appendix D: Letters of Support..... 38

Appendix E: BS Cybersecurity Financial Projections 46

Executive Summary

Cybersecurity has become one of the most critical issues facing individuals, organizations, governments, and society. Breaches in cybersecurity continue to cause great harm. Security of information and critical infrastructure is not only crucial for business organizations but also a matter of national security. However, reports indicate a continuing shortage of skilled cybersecurity talent in both the private and public sectors. For example, the *Frost & Sullivan and (ISC)² 2017 Global Information Security Workforce Study* projects that 1.8 million cybersecurity jobs will remain unfilled by year 2022. Cyberseek.org estimates close to 313,000 current cybersecurity job openings in the United States (U.S.) with more than 5,300 in Missouri alone. The U.S. Department of Labor predicts a 28% growth in the information security analyst job role by 2026 and reports a median annual wage of \$95,510 based on 2017 data.

Necessary faculty, courses, and infrastructure required to start this degree are already in place. Funds for marketing and additional resources are built into the financial plan as the program grows. The financial plan includes enrollment contingent new faculty resources to adequately sustain growth. Consistent with the national impetus to address the growing cybersecurity talent needs, the University of Missouri–St. Louis (UMSL) began a cybersecurity strategic initiative in Fall 2014. Since cybersecurity is both a technical as well as a business issue, the departments of Information Systems and Technology (College of Business Administration) and Computer Science (College of Arts and Sciences) collaborated to create multi-disciplinary undergraduate cybersecurity certificate and minor programs in Fall 2015. In addition, given the call from industry for more applied skills in cybersecurity, UMSL has made significant investments in developing physical and virtualized cybersecurity lab environments to support hands-on skills development. UMSL currently has five faculty lines dedicated to cybersecurity. These initiatives led to UMSL being designated as a *National Center of Academic Excellence in Cyber Defense Education (CAE-CDE)* by the National Security Agency (NSA) and the U.S. Department of Homeland Security (DHS).

The proposed **Bachelor of Science (B.S.) in Cybersecurity** degree builds on these investments. Industry and government organizations in the region have provided strong letters of support for this degree. This STEM designated interdisciplinary program will be jointly delivered by the departments of Information Systems and Technology and Computer Science. The curriculum aligns with the NSA-DHS CAE-CDE knowledge unit requirements and the National Initiative for Cybersecurity Education, Cybersecurity Workforce Framework guidelines. In addition, industry Advisory Boards provided input to the curriculum and will continue to advice on industry needs in future. In this challenging and multi-faceted degree, students develop technical and theoretical foundations along with strong applied skills relevant to industry and government employers. At the time of admission, students choose either a Computer Science or an Information Systems and Technology emphasis. The Computer Science emphasis provides greater technical exposure while the Information Systems and Technology emphasis includes business foundations and management aspects of cybersecurity. The program will allow graduates to pursue high-demand work-roles such as Cybersecurity Specialist, Cyber Defense Analyst, Cyber Defense Incident Responder, Information

Security Analyst, Vulnerability Assessment Analyst, Security Architect, and a variety of other entry-level cybersecurity and Information Technology (IT) related roles.

In summary, the proposed program has strong and demonstrated demand from industry and students; it has been identified as a priority within the UM System as well as at state and national agencies; it will strengthen the University of Missouri; and address the growing need for cybersecurity talent.

1. Introduction

Cybersecurity is one of the most critical issues facing individuals, organizations, and governments today. Information systems face constant attack and any successful breach inevitably results in adverse consequences for stakeholders. Despite the strong public outcry that such breaches provoke and the calls for accountability and improved safeguards, industry and government reports indicate a severe and sustained shortage of skilled cybersecurity talent in public and private sectors.

This proposal seeks to add a STEM designated **Bachelor of Science (B.S.) in Cybersecurity** degree at the University of Missouri-St. Louis (UMSL). The program addresses the current and future predicted talent shortages in the broad field of cybersecurity.

Cybersecurity is a technical as well as a managerial issue for organizations so the program is designed to be multi-disciplinary in its curriculum. Such an approach ensures a nimble and responsive orientation to a rapidly changing field. The program builds on UMSL's current designation by the National Security Agency (NSA) and U.S. Department of Homeland Security (DHS) as a *National Center of Academic Excellence in Cyber Defense Education* (CAE-CDE). It is designed to address the NSA/DHS cybersecurity knowledge-unit requirements as well as the National Initiative for Cybersecurity Education - *Cybersecurity Workforce Framework* (NICE-CWF) Knowledge, Skills, and Abilities guidelines. Program and learning outcomes are mapped to these guiding frameworks¹. In addition, the program incorporates industry perspectives on curricula and skills through an advisory board focused on cybersecurity.

In this challenging and multi-faceted program, students develop both theoretical foundations and applied skills through hands-on labs, workshops, projects, competitions, and internships. The program will allow graduates to pursue high-demand work roles such as Cybersecurity Specialist, Cyber Defense Analyst, Cyber Defense Incident Responder, Information Security Analyst, Vulnerability Assessment Analyst, Security Architect, among a variety of other entry to mid-level cybersecurity related roles².

¹ Please see [https://cyberedwiki.org/index.php?title=Category:Foundational_KUs_\(2020\)](https://cyberedwiki.org/index.php?title=Category:Foundational_KUs_(2020)) for an overview of Foundational, Core, and Optional Knowledge Units and associated learning outcomes required for CAE-CDE designations.

² Please see <https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework> for a description of the NICE Cybersecurity Workforce Framework and associated KSAs, Tasks, and work roles.

The B.S. in Cybersecurity requires students to choose an emphasis in Computer Science (120 credit hours) or an emphasis in Information Systems and Technology (126 credit hours). The selection is made at the time students apply for admission. In addition to coursework specific to the emphasis selected, students must complete a common set of courses and meet all general education requirements.

The proposed degree represents an intentional evolution that began in 2014 as part of UMSL's strategic efforts to develop significant learning and delivery capacities in Cybersecurity. In the Fall of 2014, UMSL hired tenure track and non-tenure track cybersecurity faculty and created undergraduate and graduate certificates as well as an undergraduate minor in cybersecurity. Supporting infrastructure was developed to deliver a robust cybersecurity education in the form of a dedicated physical cybersecurity laboratory as well as innovative fully virtualized cybersecurity lab environments. The courses developed for the undergraduate cybersecurity certificate and minor are embedded in the B.S. program currently being proposed. The program draws on a multidisciplinary set of courses to create the holistic and well-rounded pathway scholars in cybersecurity education and workforce development advocate³.

UMSL recently created a Cybersecurity Institute, designed to bring national attention to UMSL and the State of Missouri by coordinating cybersecurity education, research, economic development, and outreach activities. The cybersecurity degree program will be coordinated by the Director of Cybersecurity Institute.

2. Fit with University Mission and Other Academic Programs

2.A. Alignment with Mission and Goals

The mission of the University of Missouri-St. Louis is "*We transform lives.*" As the metropolitan, land-grant, research institution serving the most diverse and economically important region in Missouri, the University of Missouri–St. Louis delivers exceptional educational, research and engagement experiences that inform, prepare, challenge and inspire. UMSL's strategic focus revolves around the five *compacts* shared by the broader UM System. Among these compacts, "Excellence in Student Success" and "Excellence in Community Engagement and Economic Development" directly support the creation of the B.S. in Cybersecurity. The programs would augment UMSL's current efforts to make a broader impact on the region by bringing industry, government, schools, community colleges, and other stakeholders together to develop and enhance a vibrant cybersecurity eco-system.

Cybersecurity programs and related initiatives have been identified as strategic priorities at the department, college, and campus level. Campus administrators have voiced strong support for cybersecurity programs including the certificates and minor that provide the foundation of the proposed degree program. Cybersecurity has been identified as a

³ Please see: Hoffman, L., D. Burley, & C. Torgas. 2012. Holistically Building the Cybersecurity Workforce. *IEEE Security & Privacy*, 10(2): 33-39

growth area and the campus is committed to continue develop strong programming in this area.

2.B. Duplication and Collaboration Within Campus and Across System

The UM System does not offer a full undergraduate cybersecurity degree program at any of its four campuses. Among non-UM System public institutions, University of Central Missouri, Northwest Missouri State University and Southeast Missouri State University have undergraduate degrees. Importantly, these are regional programs that do not adequately support the St. Louis region. Among private universities in the greater St. Louis region, Lindenwood University, Fontbonne University, and Maryville University have undergraduate degrees in cybersecurity. Thus, among public institutions, there is no duplication within the UM System and little overlap among public institutions, given the wide geographic separation across the state among the institutions mentioned above.

A critical advantage of UMSL is its current NSA/DHS CAE-CDE designation. This accolade distinguishes our courses and programs apart from non-designated programs in the State of Missouri. The B.S. in Cybersecurity will further strengthen Missouri's standing among the National Centers of Academic Excellence in Cyber Defense Education community. UMSL will also be poised to partner with other UM System Campuses to further strengthen cybersecurity education in Missouri as well as to promote strong economic development in the region. This is due in part to the UM System President's effort to spearhead systematic collaboration on cybersecurity education, research, and economic development related areas across campuses. In addition, the B.S. in Cybersecurity, combined with two-year programs such as the one offered by St. Louis Community College (STLCC), will contribute to a sustainable pathway for cybersecurity talent development in the region. STLCC received the CAE-2yr. designation from NSA/DHS in 2017.

In summary, UMSL's leadership position in cybersecurity education as a CAE-CDE, minimal overlap with competing programs, alignment with UM System and State-wide collaboration initiatives, and strong overall demand for cybersecurity talent in the Saint Louis Metropolitan region, provide ample support for this new program.

3. Business-Related Criteria and Justification

3.A. Market Analysis

3.A.1. Need for Program

The field of cybersecurity is currently facing dramatic talent shortages in the public and private sectors at local, regional, national, and international levels. This shortage is an issue of national security as unmet talent needs in the field of cybersecurity play an increasingly significant role in the theft or destruction of strategic and proprietary information as well as national security. The *Frost & Sullivan* and *(ISC)² 2017 Global Information Security Workforce Study* projected that 1.8 million cybersecurity positions

will remain unfilled worldwide by year 2022—a 20% increase from a previous estimate for 2020⁴.

The occupational outlook for cybersecurity professionals is strong. According to the U.S. Bureau of Labor Statistics, Information Security Analyst positions—just one potential work role—is expected to experience a 28% increase between 2016 and 2026. The median annual wage was \$95,510 in 2017. Further, the St. Louis region is currently ranked within the Top 15 metropolitan areas with the highest level of employment in the “Information Security Analyst” occupation with a location quotient double the national average⁵.

Cyberseek.org⁶ rates the supply of cybersecurity professionals in Missouri as “very low” and estimates close to 313,000 cybersecurity related job openings around the United States and more than 5,300 in Missouri alone. The Missouri Economic Research and Information Center’s (MERIC) long-term employment projections indicate that the top STEM occupations with the highest projected increase in job openings in Missouri include many Computer and Information Systems and Technology professionals⁷.

According to a Gallup survey, reported in Missouri’s “WORKFORCE 2030: A Call to Action,” 56% percent of Missouri business leaders are not satisfied with the availability of skilled workers in this state. In the report, one CEO noted, “We cannot find enough workers with the right skills. There is a mismatch, and unless somebody does something soon, we won’t be able to grow in Missouri.” Similar to the analysis by MERIC, the Missouri Workforce 2030 report showed that the fastest growing jobs are in fields that encompass computer professionals⁸.

The increasing attention and interest that cybersecurity concerns generate among business and government organizations mean that new programs and expanded capacities will be necessary to meet current and future demand. Further, cybersecurity transcends the IT domain with broad strategic impacts and repercussions on businesses and governments. Industry trends suggest that security is finally becoming part of the conversation among chief executives and in corporate board rooms. In other words, cybersecurity is increasingly a strategic priority for organizations. Thus, academic programs that produce highly skilled cybersecurity talent are a necessity.

The Saint Louis region has a growing contingent of Federal agencies with high demand for cybersecurity related talent. For example, UMSL is in close proximity to the Scott Air

⁴ Report presented by ISC², Booz Allen Hamilton, Alta Associates, and Frost & Sullivan, Global Information Security Workforce Study, Available online at <https://iamcybersafe.org/wp-content/uploads/2017/07/N-America-GISWS-Report.pdf>

⁵ Please see: <https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-1> and <https://www.bls.gov/oes/current/oes151122.htm>

⁶ Data obtained Nov 21, 2018; Cyberseek.org is a project supported by the National Initiative for Cybersecurity Education (NICE), a program of the National Institute of Standards and Technology in the U.S. Department of Commerce

⁷ MERIC https://www.missourieconomy.org/occupations/occ_proj.stm

⁸ Workforce2030: A Call to Action <http://mochamber.com/wp-content/uploads/2018/05/Workforce2030.pdf>

Force Base and the recently opened Defense Information Systems Agency (DISA) Global Operations Command. In addition, the National Geospatial-Intelligence Agency (NGA) and their new, expanded NGA West location in North Saint Louis adds to the expanding footprint of government organizations in need of cyber talent within the Saint Louis region. The Department of Defense Cybersecurity scholarship program requires scholarship recipients to pursue a degree at an NSA/DHS CAE designated institutions such as UMSL, and graduates of such programs are often preferred by “hiring authority” arrangements that follow Federal hiring process guidelines.

The State of Missouri has identified cybersecurity as a priority for protecting the State’s information resources and for ensuring future competitiveness through the creation of well-paying jobs within the state. Among four-year institutions in the State of Missouri, only UMSL holds the National Center of Academic Excellence in Cyber Defense Education designation. UMSL’s efforts to create this degree will bolster Missouri’s standing within the national CAE community and lead the way for other UM System schools as well as area institutions to pursue this prestigious designation. Thus, the B.S. in Cybersecurity will contribute to regional capacities and is expected to produce a steady pipeline of cybersecurity talent that will promote economic development.

A direct economic impact can be seen through high-paying cybersecurity jobs in the state but the indirect impacts are far more significant. Without a sufficiently robust pool of cybersecurity talent, organizations currently in the state may move to regions where it is readily available. Similarly, the lack of cybersecurity talent may result in relocating corporations dismissing Missouri as a viable option. The competitiveness of entrepreneurial cybersecurity startups for funding opportunities such as the Six-Thirty Cyber⁹ fund and the ability of Missouri institutions to pursue government and private sector cybersecurity grants are also impacted. With just the certificates, minors, and CAE designation, UMSL was able to secure three grants bringing approximately \$500,000 to UMSL and the State. Having the B.S. in Cybersecurity will further improve our ability to pursue opportunities such as the National Science Foundation’s CyberCorps Scholarship for Service grant.

In summary, the new undergraduate cybersecurity degree program will help address the talent shortage, make Missouri competitive, and represents significant opportunities for direct and indirect economic impacts. Letters of support from industry, government, and alumni (please see Appendix D – Letters of Support) indicate the significance of the proposed degree program in addressing the talent needs within cybersecurity.

3.A.2. Student Demand for Program

Demand for the program and enrollment is expected to be extremely robust. Public awareness and public fear of cybersecurity threats make the program particularly appealing to students. In addition, demand for cybersecurity talent and the vigorous

⁹ <https://sixthirtycyber.com/about-sixthirty-cyber/>

support of regional and national employers make this program a smart career choice and solid financial investment for students.

Prospective students have identified cybersecurity as a key interest area. According to the UMSL Office of Admissions, cybersecurity was the *second most requested degree program* that UMSL did not offer based on data collected using inquiry cards during site visits to high schools and community colleges. In 2016-2017, 54 students identified cybersecurity as their desired major on inquiry cards. This suggests that student demand is likely to be robust.

Enrollment projections for this degree proposal were constructed relying on real enrollment data from related programs and the previously described projections of the U.S. Bureau of Labor Statistics and industry reports/initiatives (e.g., cyberseek.org). With regard to related undergraduate programs, UMSL offers an Undergraduate Certificate in Cybersecurity and a Minor in Cybersecurity. UMSL began offering these programs in the Fall of 2015. As of Fall 2018, there are 25 students pursuing the Cybersecurity Minor and 22 pursuing the Undergraduate Certificate in Cybersecurity. Both the undergraduate certificate and minor programs directly map to a portion of the requirements in the new degree and could also act as feeder programs for the full degree.

Five-year projections¹⁰ for the total number of students enrolled in the B.S. in Cybersecurity each fall are presented in Table 1a. Approximately 30% of total students enrolled are considered to be part-time based on recent UMSL enrollment data. The number of new students the degree is expected to attract (not those currently enrolled that may switch majors) is reported in Table 1b. In both tables, data are adjusted to reflect graduation and attrition rates. In other words, the tables reflect the number of students enrolled in a given year and not just entry of new students into the program. Appendix E (Financial Projections Spreadsheet) contains all enrollment and financial projections calculations. UMSL's university-wide current graduation data suggest that 60% of the undergraduate students complete their degrees within 6 years¹¹. We use this approximation to take 60% of the Year 1 New Enrollments as the number of students graduating in Year 6. However, approximately 20% of undergraduate students transfer to UMSL from other institutions such as community colleges. A large percentage transfer in with enough credit hours to be classified as Juniors or Seniors (approximately 60-70% of all transfer students). Thus, we anticipate graduations among this population as early as year 3 with estimates based on 20% transfer students (70% of which are at the Junior or Senior level). For example, for Year 1, 40 total students enrolled is projected. Eight of those students (20% will be transfer students). Of those eight, 70% (rounded-up) would be at the Junior or Senior rank and could therefore potentially graduate in year 3. This same approach is used iteratively for Year 4 and 5. Starting with Year 6, we estimate a 60% graduation rate for first-time first-year freshmen and 3-year graduation rates for transfer students as already described.

¹⁰ The financial projections spreadsheet attached as Appendix E contains detailed calculations used to arrive at tables 1a, 1b, and 1c.

¹¹ <http://blogs.umsl.edu/news/2017/10/23/upperclassman-financial-aid/>

Table 1a. Student Enrollment Projections (anticipated total number of students enrolled in program during the fall semester of given year).

Year	1	2	3	4	5
Full-Time	28	89	142	188	231
Part-Time	12	38	61	81	99
Total	40	127	203	269	330

Table 1b. Student Enrollment Projections (anticipated number of students enrolled during the fall semester of given year who were new to campus).

Year	1	2	3	4	5
Full-Time	21	76	124	165	204
Part-Time	9	32	53	71	87
Total	30	108	177	236	291

Table 1c. provides an estimated number of degrees awarded. Estimates were derived using the approach described above. Please see Appendix E for full data.

Table 1c. Projected Number of Degrees Awarded

Year	1	2	3	4	5	6	7	8	9	10
# of Degrees Awarded	0	7	14	14	38	68	68	68	68	68

3.B. Financial Projections

3.B.1. Additional Resources Needed

UMSL currently has sufficient capacity to establish the B.S. Cybersecurity program due to investments made by university administration over the past four years in faculty, curriculum, and infrastructure (labs). Thus, no initial expenditures (one-time costs) or additional resources will be required to deliver the program in year 1. As enrollments grow, two contingent faculty lines (total \$210,000 with a 2% annual increase) are requested starting year 2 to grow course capacities. One additional faculty line (\$130,000 with a 2% annual increase) is requested starting year 3 to support further increase in enrollments by year 3. These faculty line requests are based on differences in current and projected course capacities of existing courses in the proposed program. If enrollment targets are not met then the additional faculty lines will not be needed.

In order to promote strong enrollment numbers, the university administration will support marketing expenses of \$50,000 in year 1; \$40,000 in year 2; \$30,000 in year 3; and \$25,000 per year from year 4 onward. The greater spending on marketing in initial years is designed to create the necessary momentum for the new program. Subsequent

advertising and promotion are crucial to raising and sustaining awareness and exposure to the program.

Additionally, a one-time investment of \$75,000 in Year 3 will be supported to scale-up and improve the cybersecurity lab infrastructure. This one-time expense will allow greater server and network capacity to support more student users in the virtualized lab environments.

3.B.2. Revenue

Revenue projections are provided in Table 2, *Financial Projections*. For the purposes of our estimates, revenue sources were limited to Tuition Fees and Supplemental Fees from students new to campus. Total Program Revenue thus reflects projected cumulative total student enrollments adjusted for attrition and graduations as shown in Table 1a. The total program revenue figures are then adjusted to include only students new to campus (using numbers from Table 1b) as described below. Estimates should be considered baseline as they rely solely on in-state per credit hour tuition rate.

The “proforma new program spreadsheet” attached as Appendix E was used to calculate revenue projections. Per Year revenue figures were arrived at as follows. Number of full-time students enrolled in the program in each year (from Table 1a) was multiplied by per student undergraduate course load of 24 credit hours per year. This results in an estimate that is more conservative than the 15 hours per semester many students register for. It partially accounts for students who may take longer to complete the program but are not part-time. Number of part-time students was multiplied by a per student undergraduate part-time course load of 12 credit hours per year. The sum of full-time and part-time credit hours resulted in Total Credit Hours per year. Total number of credit hours was then multiplied by per credit hour fee for in-state tuition, resulting in the Tuition Fee sub-total.

In addition, courses delivered in this program will be subject to existing supplemental fees. These fees are assessed on a per credit hour basis and are included in our revenue projections. Supplemental fees on courses offered through UMSL College of Business were multiplied by 30%¹² of the total credit hours while supplemental fees for courses offered through UMSL College of Arts and Sciences were multiplied by 70%. The sum of these revenues is reflected in the Supplemental Fee sub-totals. The sub-total for tuition and supplemental fee revenue were added together to produce a sub-total that was then adjusted to reflect the discounted tuition rate. Most students do not pay full tuition so accounting for the discrepancy is necessary to make accurate revenue projections. UMSL’s discount Tuition Rate of 19% (AY2018) was used to estimate future discount rates on projected revenue. Thus, the Total Program Revenue reflects the sum total of tuition and fees minus tuition rate discounts.

¹² Due to the program’s multi-disciplinary focus, approximately 30% of course credits are through the College of Business Administration and the remaining from College of Arts and Sciences.

3.B.3. Net Revenue

As indicated above, if the program were to meet enrollment targets two contingent faculty lines would become a recurring expense beginning in Year 2 and an additional faculty line will be added from year 3. A one-time lab infrastructure improvement expense is incorporated under year 3. In addition, marketing and advertising expenses listed above appear as recurring expenditures. The total expenditures per year were subtracted from the total program revenue to obtain the Direct Margin to Campus figures. From the Direct Margin to Campus figures, revenue generated from “within-campus transfers” was subtracted to retain only that revenue that was attributable to students who are new to the campus. This produced the Net Margin to Campus estimates. The respective figures appear in Table 2. Overall, this program is net revenue positive from year one based on reasonable projected new student enrollments (Table 1b).

Sensitivity Analysis

A sensitivity analysis (please see Appendix E spreadsheet) assessed the viability of the program given a 25% reduction in the anticipated enrollment figures. The program remained net revenue positive.

*** Space left blank to incorporate table on next page***

Table 2. Financial Projections for Proposed Program for Years 1 Through 5.

	Year 1	Year 2	Year 3	Year 4	Year 5
1. Expenses per year					
A. One-time	0	0	0	0	0
<i>New/Renovated Space</i>					
<i>Equipment</i>			\$75,000		
<i>Library</i>					
<i>Consultants</i>					
<i>Other: Advertising</i>	\$50,000	\$40,000	\$30,000	\$25,000	\$25,000
Total one-time					
B. Recurring					
<i>Faculty</i>		\$210,000	\$314,200	\$320,484	\$326,894
<i>Staff</i>					
<i>Benefits</i>		\$74,802	\$111,918	\$114,156	\$116,440
<i>Equipment</i>					
<i>Library</i>					
<i>Other</i>					
Total recurring	0	\$284,802	\$426,118	\$434,640	\$443,333
Total expenses (A+B)	\$50,000	\$324,802	\$531,118	\$459,640	\$468,334
2. Revenue per year					
<i>Tuition/Fees</i>	\$189,179	\$694,667	\$1,161,251	\$1,579,301	\$1,986,306
<i>Institutional Resources</i>					
<i>State Aid -- CBHE</i>					
<i>State Aid -- Other</i>					
Total revenue	\$189,179	\$694,667	\$1,161,251	\$1,579,301	\$1,986,306
3. Net revenue (loss) per year	\$139,179	\$369,865	\$630,133	\$1,119,661	\$1,517,972
4. Cumulative revenue (loss)	\$139,179	\$509,044	\$1,139,177	\$2,258,838	\$3,776,811

Additional calculations available in Appendix E.

No one time startup costs, renovation costs, etc. are anticipated. Exciting facilities are deemed enough. A \$75,000 upgrade for lab equipment is included only in year 3.

Additional faculty lines requested in second and third year contingent on enrollment projections.

Revenue includes tuition/fees subtract revenue from transfers within campus.

3.B.4. Financial and Academic Viability

The program is financially and academically viable (see Table 3 for minimum enrollments). While the program is projected to be net revenue positive at the end of first academic year, the minimum number of enrollments required at year 5 to break-even is 108. This approximation was derived by setting the projected cumulative enrollments at years 1 through 5 at a value that would make the Margin After Campus Overhead figures become positive at year 5. Importantly, this minimum enrollment number covers expenditures that include the contingent faculty lines. If the contingent faculty lines are not included in projections for Year 2 and beyond, the minimum enrollment required for financial viability would be significantly lower.

In terms of academic viability, in order to graduate an average of 10 students per year beginning in year 5, we need an enrollment of about 15 students per year in the degree program.

In summary, based on the make-up of the program, the number of existing courses, faculty resources, healthy student demand, and existing UMSL capabilities, we believe that the new program will be academically and financially viable within the first 5 years.

Table 3: Enrollment at End of Year 5 for Program to Be Financially and Academically Viable.

Viability	Minimum Enrollment
Financial	108*
Academic	15
<i>* will be significantly lower if enrollment contingent expenses are excluded in break-even calculations</i>	

3.C. Business and Marketing Plan: Recruiting and Retaining Students

The B.S. in Cybersecurity will leverage UMSL's existing campus wide recruitment initiatives such as the Bridge program, UMSL Day, etc., while supplementing these with targeted efforts. The primary target for recruitment into the Bachelor of Science in Cybersecurity degree program will be students interested in STEM related fields. Geographically, initial recruitment efforts will center on the Saint Louis Metropolitan area as a way to rapidly bootstrap the enrollments. However, the recruitment strategy is scalable and the intent is to market throughout the Midwest region as well as on a national scale. As indicated in the financial projections section (3B), the university administration plans to provide robust support for marketing in order to grow and sustain this program. Advertising and marketing strategies include focused paid online advertisements (Google Adwords, Facebook Ads), social media outreach and promotions, as well as free and paid print media publications. In addition, both the College of Arts and Sciences and the College of Business Administration have dedicated and focused recruitment and retention initiatives.

Web Advertising

- 1) A mobile-enabled (cross platform) website will be created using UMSL's existing Content Management System. The site will be Search Engine Optimized with keywords that depict key aspects of the new cybersecurity education opportunities at UMSL.
- 2) A substantial portion of the advertising budget is devoted to a reasonable and scalable web advertising campaign through Google Adwords and if possible, Facebook Ads.
- 3) Social media accounts using the "UMSL Cybersecurity" brand will be created to maximize the potential use of social media to complement paid advertising.

Print Advertising and Other Promotion Efforts

- 1) UMSL's existing publications and other UM System publications will be asked to feature the new programs and associated developments.
- 2) When feasible, we will take out reasonably priced advertisements in the St. Louis Post Dispatch and St. Louis Business Journal before program launch.
- 3) UMSL's faculty are also active contributors to media inquiries related to cybersecurity incidents, and they participate in radio and TV segments on cybersecurity.
- 4) UMSL proudly hosts a regional conference on cybersecurity, STL CyberCon.org. The conference typically takes place in the second or third week of November and attracted close to 700 registrants in Nov 2018. The conference is a unique confluence of students, teachers, practitioners, and researchers. It is open to the general public with no registration costs. It features presentations by distinguished speakers on a variety of topics bridging theory and practice. The conference also includes a "Capture the Flag" ethical hacking competition which was attended by close to 150 high-school and community college students—a key recruitment target population.
- 5) The College of Business has a full-time college level Recruitment Coordinator as well as a dedicated Internship Coordinator.

Outreach and Scholarships

- 1) UMSL has good relationships with community colleges in the area and will actively work with them to bring in their graduates with associates degrees into the new program.
- 2) Similarly, UMSL has cultivated strong relationships with high schools through its various initiatives targeted toward students interested in IT and Cybersecurity fields in particular. For example, UMSL regularly hosts summer camps for high

school and middle-school students from St. Louis, the St. Louis Global Game Jam, various hackathons, and the newly started Cybersecurity Converge tour where middle and high school students are brought to campus for basic lessons in cybersecurity curricula and fun “ethical hacking” exercises.

- 3) In addition, UMSL recently hosted about 20 high school students from North County Technical High School for an overview of ethical hacking and for participation in a Capture the Flag Competition. A similar event was hosted in early 2018 for about 30 students from the Jennings School District. We plan to continue hosting at least two to three such events each year as they directly target the student body most interested in cybersecurity related education.
- 4) UMSL, the Information Systems and Technology department, and the Computer Science department have a robust alumni network which is very active in promoting and supporting our programs. This is evident by various industry advisory boards such as the IS Advisory Board and the Computer Science Advisory Board. The faculty are deeply engaged with the broader cybersecurity community among the public and private sectors. The departments and faculty will leverage these relationships to further promote the programs.
- 5) UMSL has developed relationships with national and regional organizations to bring in cybersecurity scholarships. Currently, U.S. Bank has awarded \$10,000, Mastercard has awarded \$10,000, and the Society of Information Management Gateway 2 Cyber City initiative has awarded \$2,000 annually from 2018 to 2021. UMSL will also pursue grants for providing full scholarships and stipends (approximately \$40,000 awards per student per year) through the U.S. DoD and NSF CyberCorps programs. These scholarships can provide excellent help in recruiting efforts while truly making an impact on students.

Student Retention

In addition to campus-wide retention efforts we will particularly leverage the following:

- 1) The UMSL Office of Student Retention Services (UMSL-SRS) manages and integrates a variety of on-campus support services into early and meaningful Academic Intervention Programs aimed at reducing student failure and improving retention. In particular, the UMSL-SRS manages the “*MyConnect Early Alert System*” which is used by faculty, advisors, and intervention units to better engage students in their coursework and intervene early to help at-risk student succeed. The application provides faculty with a mechanism for early reporting and identification of students that may be at-risk of not achieving success in a course. Faculty “flag” at-risk students and SRS conducts a needs assessment to determine what supports the student may need. Flags range from aspects such as “Poor Attendance” and “Danger of Failing” down to “Failure to submit major assignment.” Faculty can also provide “Referrals” for students to relevant on-campus support services ranging from retention services to writing or math

tutoring. These mechanisms allow Success Coaches from support entities to intervene in a timely fashion and do so effectively.

- 2) The Information Systems and Technology department has a long-standing Student Mentorship program that is strongly supported by alumni. This program augments retention efforts delivering regular events pertaining to academic success, career advice, and skills development. This program not only provides opportunities to network and be part of the professional community but also plays an important role in building a supportive community of classmates.
- 3) The College of Business has a full-time college level student support assistant as well as a full-time Retention Coordinator.
- 4) The Director of Cybersecurity coordinates the degree program and will provide additional retention support.

4. Institutional Capacity

UMSL has the existing capacity to initiate high-quality B.S. in Cybersecurity degree program due to its previous investment in cybersecurity certificate programs and support of UMSL leadership. It is aligned with institutional priorities as evidenced by prior investments. In 2014, three tenure-track faculty and one non-tenure track faculty dedicated to cybersecurity curriculum development and course delivery were hired. Another tenure-track faculty line will be diverted to cybersecurity in 2019. Most of the cybersecurity core courses are taught by full-time faculty with terminal degrees. Experienced cybersecurity professionals also teach some of the cybersecurity courses. All of the courses required to deliver the program are already implemented and are being taught with current faculty resources, save one. The new degree requires the creation of one new course which can easily be accommodated by current faculty. As explained in Section 3, if enrollment targets are met, we will request additional faculty lines to increase course capacities through additional sections and to incorporate new courses as the cybersecurity field evolves. Thus, the creation of this new degree program will be supported with existing resources and have no negative impact on existing certificate programs.

Existing Supporting Infrastructure

UMSL has invested in a dedicated physical cybersecurity laboratory which is already operational to support previously approved cybersecurity certificate and minor programs. In addition, the faculty have spent considerable effort in creating fully virtualized cybersecurity lab environments to accommodate more students than currently enrolled in the certificate programs. Importantly, the infrastructure is highly scalable and can be further expanded should the need arise. UMSL also has existing access to software tools relevant to cybersecurity through Academic Alliances with Microsoft, IBM, and VMware among others (please see Appendix C for a brief description of these lab environments and other supporting infrastructure). One of these virtualized lab environments was supported by a \$294,519 grant from the National Security Agency. Another National

Security Agency grant of close to \$200,000 supports Internet of Things (IoT) research and teaching. Existing classroom facilities are adequate for supporting the program.

5. Program Characteristics

5.A. Program Outcomes

The programmatic learning outcomes for the B.S. in Cybersecurity, as previously noted, were created to align with and map to the specific *Knowledge Units* set forth by the NSA and DHS. Such a strategy ensures a best-practices approach and provides a strong foundation for a CAE designation of the program.

CAE designation requires specific unit level learning outcomes. The BS Cybersecurity degree maps to three of the Foundational Knowledge Unit Requirements¹³, five of the Technical Core Knowledge Unit Requirements¹⁴, and up to 14 Optional Knowledge Unit Requirements¹⁵.

Broad Learning Outcomes

1. Understand and Describe the Confidentiality, Integrity, and Availability security objectives and key security principles that enable the development of security mechanisms
2. Demonstrate an understanding of physical, data link, network, transport, and application layers of data networking and identify potential information security pitfalls at each layer
3. Describe important secure software development principles and common web application security vulnerabilities
4. Describe common applications of cryptographic, network, application, and systems security defense mechanisms to improve information security
5. Understand the role of systematic information security risk management in fostering information security within organizations and the role of management and control frameworks such as NIST Special Publications and ISO 27000 series standards in doing so.

NICE Cybersecurity Workforce Framework “Degree Crosswalk”

In addition to the broad learning goals and CAE mappings, the B.S. in Cybersecurity degree also maps to several top-level categories in the NICE Cybersecurity Workforce Framework (CWF). This complies with CAE designation criteria requiring designated programs to specify a “cross-walk” of the program with NICE CWF. The CWF contains seven top level categories and CAE designated programs must map to at least one of these seven categories. The B.S. in Cybersecurity maps to four of these categories

¹³ [https://cyberedwiki.org/index.php?title=Category:Foundational_KUs_\(2020\)](https://cyberedwiki.org/index.php?title=Category:Foundational_KUs_(2020))

¹⁴ [https://cyberedwiki.org/index.php?title=Category:Technical_Core_KUs_\(2020\)](https://cyberedwiki.org/index.php?title=Category:Technical_Core_KUs_(2020))

¹⁵ [https://cyberedwiki.org/index.php?title=Category:Optional_KUs_\(2020\)](https://cyberedwiki.org/index.php?title=Category:Optional_KUs_(2020))

including Securely Provision (SP), Operate and Maintain (OM), Oversee and Govern (OG), and Protect and Defend (PD). Descriptions of these NICE CWF categories are listed in Table 4.

Table 4. BS Cybersecurity Degree Crosswalk with NICE CWF Categories

Category	Description
Securely Provision (SP)	Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.
Operate and Maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
Oversee and Govern (OV)	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
Protect and Defend (PR)	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.

5.B. Structure

The interdisciplinary cybersecurity degree program has a common set of courses and two emphasis areas:

- 1) Computer Science Emphasis (120 credit hours) *or*
- 2) Information Systems and Technology Emphasis (126 credit hours)

Students must choose either the Computer Science Emphasis or Information Systems and Technology Emphasis at the time of application for admission. Based on the student's choice, application processing, admission decisions, advising, and graduation processing will be handled by the appropriate college (Arts and Sciences for the Computer Science Emphasis; Business Administration for the Information Systems and Technology Emphasis).

Both emphasis areas provide a blend of technical- and business-oriented skills designed to prepare students for a variety of cybersecurity and IT related careers. The Computer Science Emphasis provides enhanced technical depth whereas the Information Systems and Technology Emphasis offers stronger preparation for business and management aspects of cybersecurity.

Common Required Courses

The B.S. in Cybersecurity requires 36 credit hours of core coursework and the selection of an emphasis in Computer Science or Information Systems and Technology. The emphasis area selected determines the remaining requirements of the degree.

Computer Science Emphasis Requirements

The B.S. in Cybersecurity with Computer Science emphasis requires a minimum total of 120 credit hours. All College of Arts and Sciences general degree requirements apply.

Candidates for the B.S. in Cybersecurity with Computer Science emphasis must complete a program of 80 credit hours of required courses. This includes 36 credit hours that are part of the core coursework in cybersecurity and 44 credit hours specific to the Computer Science emphasis. There are 13 credit hours of Free Electives.

Required Courses Specific for Information Systems and Technology Emphasis

The B.S. in Cybersecurity with Information Systems and Technology Emphasis requires a minimum total of 126 credit hours. All general degree requirements from the College of Business Administration apply.

Candidates for the B.S. in Cybersecurity degree with Information Systems and Technology Emphasis must complete a program of 111 credit hours of required courses. This includes 36 credit hours that are part of the core coursework in cybersecurity and 75 credit hours specific to the Information Systems and Technology emphasis. There are no Free Electives.

*** Space left blank to incorporate table on next page***

PROGRAM STRUCTURE

1. Total credits required for graduation: 120 for Computer Science Emphasis and 126 for Information Systems and Technology Emphasis

2. Residency requirements, if any: Transfer students must complete at least 30 hours and at least 15 major hours in residence

3. General education

Total credits for general education courses: 42 (major requirements fulfill a portion of these credits as shown below)

Courses (specific course or distribution area and credit hours):

<i>Computer Science Emphasis</i>		<i>Information Systems and Technology Emphasis</i>	
<i>Distribution Area</i>	<i>Credits</i>	<i>Distribution Area</i>	<i>Credits</i>
First Year Writing	3	First Year Writing	3
Communications Proficiency	3	Communications Proficiency	3
Mathematics Proficiency ^a	0/3	Mathematics Proficiency	0/3
Information Literacy	0/3	Information Literacy	0/3
US History & Government	3	US History & Government	3
Humanities & Fine Arts ^b	9	Humanities & Fine Arts	6/9
Social Sciences ^c	9	Social Sciences	0/9
Math & Sciences	0/9	Math & Sciences	0/9
GENERAL EDUCATION TOTAL (42 total hours - 15 hours included as major requirements)	27	GENERAL EDUCATION TOTAL (42 total hours - 27 hours included as major requirements)	15

4. Major requirements

Total credits specific to degree: Computer Science Emphasis = 80; Information Systems and Technology Emphasis = 111.

Courses (specific course or distribution area and credit hours):

Course Number	Credits	Course Title
Core Courses Applicable to Both Emphasis Areas		
ENGL 3120/3130	3	Business Writing or Technical Writing
MATH 3000	3	Discrete Structures
INFSYS 3848	3	Introduction to Information Security
INFSYS 3868	3	Secure Software Development
INFSYS 3878	3	Information Security Risk Management and Business Continuity
CMP SCI 1250	3	Introduction to Computing
CMP SCI 2250	3	Programming and Data Structures
CMP SCI 2261	3	Object-Oriented Programming
CMP SCI 2700	3	Computer Organization and Architecture
CMP SCI 2750	3	System Programming and Tools
CMP SCI 4700	3	Computer Forensics
CMP SCI 4732	3	Introduction to Cryptography for Computer Security

	36	Core courses applicable to both emphasis areas
Computer Science Emphasis		
MATH 1320	3	Introduction to Probability and Statistics
MATH 1800	5	Analytic Geometry and Calculus I
CMP SCI 3010	3	Web Programming
CMP SCI 3130	3	Design and Analysis of Algorithms
CMP SCI 3760	3	Cyber Threats and Defense
CMP SCI 3780	3	Software Security
CMP SCI 4730	3	Computer Networks and Communications
CMP SCI 4750	3	Introduction to Cloud Computing
CMP SCI 4760	3	Operating Systems
CMP SCI 4782	3	Information Security
CMP SCI 4794	3	Introduction to Security of IoT Systems
	9	<i>Major Specific Electives</i>
	44	Total Required for Computer Science Emphasis Area
Information Systems and Technology Emphasis		
MATH 1030	3	College Algebra (MOTR MATH 130)
MATH 1100	3	Basic Calculus
MATH 1105	3	Basic Probability and Statistics
ECON 1001	3	Principles of Microeconomics (MOTR ECON 102)
ECON 1002	3	Principles of Macroeconomics (MOTR ECON 101)
BUS AD 2900	3	Legal Environment of Business
	3	<i>Cultural Diversity Requirement</i>
INFSYS 2800	3	Information Systems Concepts and Applications
ACCTNG 2400	3	Fundamentals of Financial Accounting
ACCTNG 2410	3	Managerial Accounting
SCMA 3300	3	Business Analytics and Statistics
SCMA 3301	3	Introduction to Supply Chain Management
MGMT 3600	3	Management and Organizational Behavior
FINANCE 3500	3	Financial Management
MKTG 3700	3	Basic Marketing
MGMT 4219	3	Strategic Management
INFSYS 3820	3	Introduction to Systems Administration
INFSYS 3842	3	Data Networks and Security
INFSYS 3806	3	Managerial Applications of Object-Oriented Programming I
INFSYS 3815	3	Object-Oriented Applications in Business
INFSYS 3845	3	Database Management Systems
INFSYS 3858	3	Advanced Security and Information Systems
SCMA 4347	3	Introduction to Project Management
	6	<i>Major Specific Electives</i>
	75	Required for Information Systems and Technology Emphasis Area

5. Free elective credits

Total free elective credits: Computer Science Emphasis = 13; Information Systems and Technology Emphasis = 0.

The sum of hours required for general education, major requirements and free electives should equal the total credits required for graduation.

6. Requirement for thesis, internship or other capstone experience: No requirement (internship included as a major specific elective).

Given the great importance of practical work experience in cybersecurity, we include an Internship Course as an elective course. This allows us to strongly encourage students to pursue hands-on work experience, incentivize the student pursuit with credit toward graduation, as well as provide flexibility for those who are already in the work-force or those who cannot perform an internship for some reason.

7. Any unique features such as interdepartmental cooperation:

Given the multidisciplinary nature of the broad field of cybersecurity, this program builds upon previous collaboration between the Information Systems and Technology and the Computer Science departments in the College of Business Administration and College of Arts and Sciences respectively. In addition, relevant courses from various other departments across campus are included toward creating a holistic curriculum that provides a strong multi-disciplinary background to our graduates.

5.C. Program Design and Content

Process Used to Design Curriculum and Meet Program Outcomes

A multi-disciplinary curriculum committee designed the curriculum with the overall goal of keeping the content relevant and maintaining a dynamic fluidity to accommodate the extreme and accelerating evolution within the field of cybersecurity. Informed by the Knowledge Unit requirements set forth by the NSA and DHS for CAE designations as well as the NICE-CWF, the committee developed a structure that would meet these expectations while efficiently and equitably distributing responsibilities. The CAE-CDE designation process was a primary driver in the curriculum development and helps to ensure that the program will address student and industry needs equally well.

Course Sequences

Appendices A and B provide the 4-Year Plans for the Computer Science and Information Systems and Technology emphasis areas, respectively.

Descriptions of Courses

All of the courses in the program are already existing and detailed descriptions are available through UMSL Bulletin (<http://bulletin.umsl.edu>).

5.D. Program Goals and Assessment

Process for Assessing Learning Outcomes

Learning outcomes will be evaluated through course embedded assessments. Specifically, and per the NSA/DHS CAE-CDE guidelines, we will assess knowledge through quizzes, tests, and assignments. Most of the quizzes, tests, and assignments have already been designed to fulfill one or more of the CAE-CDE Knowledge unit requirements and learning outcomes. In addition, skill acquisition and practical task ability will be evaluated through the use of hands-on lab experiences integrated throughout the cybersecurity curriculum. For the Information Systems and Technology emphasis, assessments of business-related coursework will be carried out as part of the overall College of Business Administration assessment program through the business capstone course.

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

Not Applicable.

Performance on national and/or local assessments.

Not Applicable.

Goals for Retention and Graduation Rates

Our goals for retention and graduation are 100%.

Number of graduates per annum at years three and five

Year	1	2	3	4	5
# of Degrees Awarded	0	7	14	14	38

Placement rates in related fields, in other fields, unemployed

The placement rate from this program is expected to near 100% due to a number of factors. The number of cybersecurity-related professionals in Missouri is “very low.” As of November, 2018, cyberseek.org estimates more than 300,000 cybersecurity-related job openings with more than 5,300 in the State of Missouri. In addition, the US Bureau of Labor Statistics is predicting increased demand for cybersecurity-related talent including 28% growth in Information Security Analyst positions between 2016 and 2026. Notably, St. Louis is ranked among the Top 15 metropolitan areas with the highest level of employment in that category. Finally, the Missouri Economic Research and Information Center’s (MERIC) long-term employment projections indicate that the top STEM occupations with the highest projected increase in job openings in Missouri include many Computer and Information Systems and Technology professionals. Taken together, these factors offer strong support for post-graduation success.

5.E. Student Preparation

The B.S. in Cybersecurity does not require specialized preparation or a background in cybersecurity. It is designed to offer broad access to a high-demand field and engage a diverse student population. However, potential students would certainly benefit from prior exposure to computer programming, data networking, and systems administration at high-school or community college levels.

Describe any special admissions procedures or student qualifications required for this program which exceed regular university admission, standards, e.g., ACT score, completion of core curriculum, portfolio, personal interview, etc.

No special admission procedures or qualifications that exceed regular university criteria are required

Describe the characteristics of a specific population to be served, if applicable.

Not applicable.

5.F. Faculty and Administration

Individual(s) Responsible for Success of Program

- Dr. Shaji Khan (Director of Cybersecurity Institute and Assistant Professor of Information Systems) – 20%
- Dr. Dinesh Mirchandani (Chairperson, Department of Information Systems and Technology)
- Dr. Cezary Janikow (Chairperson, Department of Computer Science)

UMSL currently has sufficient faculty capacity to support this program. As explained in Section 3, if program meets enrollment targets, additional faculty lines will be requested starting Year 2.

Faculty Characteristics, Special Requirements, Percentage of Credit Hours to Full-time Faculty

Approximately 75% of core cybersecurity credit hours are expected to be taught by full-time faculty with terminal degrees. The program is augmented by experienced cybersecurity professionals in the St. Louis region that are active in the field. These professionals teach courses part-time as adjunct faculty but possess highly respected industry certifications (e.g., Certified Information Systems Security Professional—CISSP). All other normal Computer Science and Information Systems and Technology department faculty requirements apply.

- Dr. Shaji Khan, Assistant Professor of Information Systems and Technology (teaches core cybersecurity courses, full-time).
- Assistant Professor of Information Systems and Technology / Cybersecurity (replacement hire to join in Fall 2019, will teach core cybersecurity courses, full-time)
- Dr. Jianli Pan, Assistant Professor of Computer Science (teaches core cybersecurity courses, full-time).
- Dr. Mark Hauschild, Assistant Teaching Professor of Computer Science (teaches core cybersecurity courses and technical foundations courses, full-time).
- Dr. Sanjiv Bhatia, Professor of Computer Science (teaches technical foundations courses, full-time).
- Dr. Ankit Chaudhary, Assistant Teaching Professor of Computer Science (to join in Fall-2019 and will teach cybersecurity courses)
- Assistant Professor of Computer Science / Cybersecurity (to join in Fall 2019, will teach core cybersecurity courses, full-time)
- Assistant Professor of Information Systems and Technology / Cybersecurity (to join in Fall 2019, will teach core cybersecurity courses, full-time)
- Mr. Jeffrey Robertson, Lecturer, MA, Saint Louis University, (teaches one to two cybersecurity courses, part-time)
- On average two other part-time industry professionals to teach up to two courses as needed

Faculty Involvement in Professional Activities, Student Contact, and Teaching/Learning Innovation

All faculty members are actively involved in professional development, student mentoring, and guidance toward developing applied cybersecurity skills, as well as in various activities related to community outreach, partnership development, and service. Core cybersecurity faculty are consistently involved in the development of new innovative lab infrastructure, assignments, and learning tools for student. These activities are often supported by external grants, donations and/or partnerships with cybersecurity-related firms, and collaborations with other academics within and outside UMSL.

5.G. Alumni and Employer Survey

Congruent with the program goal to provide a high-quality curriculum that remains relevant in a rapidly evolving field, stakeholders will be actively engaged in the general program assessment and fine-tuning outcomes. Specifically, surveys of alumni and employers will be coordinated with the help of a Cybersecurity Advisory Board.

First, graduating seniors and new alumni will be surveyed using an “organizational development” approach geared toward assessing what has worked and what could be improved in terms of the a) curriculum itself, b) quality of instructors, and c) supporting resources such as lab infrastructures and career placement help.

Second, strong existing relationships with business and government organizations employing our graduates will be leveraged to conduct brief annual surveys on both the quality of our graduates as well as the changing needs of the employers. Many of these regional employers are expected to have representation on our Cybersecurity Advisory Board.

5.H. Program Accreditation

UMSL is currently designated as a National Center of Academic Excellence in Cyber Defense Education (CAE-CDE) by the U.S. Department of Homeland Security and the National Security Agency. This designation is widely viewed as the most prestigious in Cybersecurity education. Within the State of Missouri, UMSL is the only 4-year CAE-CDE University. The designation applies to existing programs and remains active through 2021. In addition, UMSL also holds a “Focus Area Designation” in Security Policy Development and Compliance.

Upon approval, the B.S. in Cybersecurity will be submitted for evaluation and is expected to be included in the current and future cycles of the CAE-CDE Designation process. If accepted by the NSA and DHS, the new program will also receive CAE-CDE designation and be eligible for renewal with the certificates and minor in 2021. The CAE-CDE designation must be renewed every 5 years.

Appendix A: B.S. Cybersecurity, Computer Science Emphasis, 4-Year Plan

Semester 1		15
IntDsc 1003	University Studies	1
Math 1800*	Calculus I	5
Communication proficiency	<i>choose</i>	3
First year writing	<i>choose</i>	3
US History & Government	<i>choose</i>	3

*May need to start with Math 1030/1035 based on HS math or math placement result

Semester 2		15
Cmp Sci 1250*	Introduction to Computing	3
Math 1320	Applied Statistics	3
Humanities and Fine Arts**	<i>choose</i>	3
Social Sciences**	<i>choose</i>	3
Free elective	<i>choose</i>	3

*Cmp Sci 1250 and 2250 available in one semester to computer literate students

**One course must also satisfy cultural diversity requirement

Semester 3		15
Cmp Sci 2250	Programming and Data Structures	3
Cmp Sci 2700	Computer Organization and Architecture	3
Math 3000	Discrete Structures	3
Social Sciences	<i>choose</i>	3
Humanities and Fine Arts	<i>choose</i>	3

Semester 4		15
Cmp Sci 2261	Programming and Data Structures	3
Cmp Sci 2750	Computer Organization and Architecture	3
Cmp Sci 3130	Design and Analysis of Algorithms	3
InfSys 3848	Introduction to Information Security	3
Engl 3130	Technical Writing	3

Semester 5		15
Cmp Sci 3010	Web Programming	3
Cmp Sci 3780	Software Security	3
Cmp Sci 4730	Computer Networks	3
InfSys 3868	Secure Software Development	3
Social Sciences	<i>choose</i>	3

Semester 6		15
Cmp Sci 4700	Computer Forensics	3
Cmp Sci 3760	Cyber Threats and Defense	3
Cmp Sci 4732	Cryptography for Computer Security	3
InfSys 3878	Information Security Risk Management and Business Continuity	3
Humanities and Fine Arts	<i>choose</i>	3

Semester 7		15
Cmp Sci 4750	Introduction to Cloud Computing	3
Cmp Sci 4782	Information Security	3
Major elective		3
Major elective		3
Free elective	<i>choose</i>	3

Semester 8		15
Cmp Sci 4760	Operating Systems	3
Cmp Sci 4794	Introduction to Security of IoT	3
Major elective	<i>choose</i>	3
Free elective	<i>choose</i>	3
Free elective	<i>choose</i>	3

Major Electives from:

- Infsys 3858, 3898
- Crimin 1100, 3310
- Phil 1160, 2254
- Cmp Sci 3990, 4020, 4220, 4222, 4300, 4500, 4610, 4792
- Others need approval

Appendix B: B.S. Cybersecurity, Information Systems and Technology Emphasis, 4-Year
Plan

Students must have 42 hours of General Education coursework. Courses listed in **bold print** count toward the 42 hours. Courses in *italics* count toward the College of Business Administration Good Standing Policy.

FIRST SEMESTER

MATH 1030 College Algebra
ENGL 1100 First Year Writing
CRIMIN 1100 Introduction to Criminology & Criminal Justice
*INFSYS 2800 Information Systems Concepts and Applications**
PHIL 2254 Business Ethics
INTDSC 1003 University Studies (1 hr)

THIRD SEMESTER

ACCTNG 2400 Fundamentals of Financial Accounting
ECON 1002 Principles of Macroeconomics
INFSYS 3806 Managerial Applications of Object-Oriented Prog. I
SCMA 3300 Business Analytics and Statistics
CMP SCI 2250 Programming and Data Structures

FIFTH SEMESTER

SCMA 3301 Introduction to Supply Chain Management
MGMT 3600 Management and Organizational Behavior
CMP SCI 2700 Computer Organization and Architecture
CMP SCI 2750 Systems Programming and Tools
INFSYS 3842 Data Networks and Security (also global awareness)

SEVENTH SEMESTER

INFSYS 3868 Secure Software Development
INFSYS 3815 Object Oriented Applications in Business
CMP SCI 4732 Introduction to Cryptography for Computer Security
INFSYS 3858 Advanced Security and Information Systems
Cybersecurity Elective **

SECOND SEMESTER

MATH 1100 Basic Calculus
ECON 1001 Principles of Microeconomics
PHIL 1160 Critical Thinking
Humanities and Fine Arts/Cultural Diversity course (cannot be a Philosophy course)
CMP SCI 1250 Introduction to Computing

SUMMER COURSE

MATH 1105 Basic Probability and Statistics

FOURTH SEMESTER

ACCTNG 2410 Managerial Accounting
BUS AD 2900 Legal Environment of Business
CMP SCI 2261 Object-Oriented Programming
COMM 2240 Persuasive Communication
INFSYS 3820 Introduction to Systems Administration

SUMMER COURSE

ENGL 3120 Business Writing

SIXTH SEMESTER

FINANCE 3500 Financial Management
MKTG 3700 Basic Marketing
MATH 3000 Discrete Structures
INFSYS 3845 Database Management Systems
INFSYS 3848 Introduction to Information Security (also global awareness)

EIGHTH SEMESTER

MGMT 4219 Strategic Management / MGMT 4220 Business Test
CMP SCI 4700 Computer Forensics
SCMA 4347 Introduction to Project Management
INFSYS 3878 Information Security Risk Management & Business Continuity
Cybersecurity Elective **

* The prerequisite for INFSYS 2800 Information Systems Concepts and Applications is INFSYS 1800: Computers and Information Systems. It can be waived by exam. See website:
<http://mis.umsl.edu/B.S.%20in%20I.S./1800waiverrequest.html>

** Choose from the following courses:

BUS AD 3090 Internship in Business Administration
+INFSYS 3898 Seminar in Information Systems (Special/Emerging Topics)
CMP SCI 4750 Introduction to Cloud Computing

SCMA 3345 Predictive Analytics and Data Mining
CMP SCI 4782 Information Security
SCMA 4350 Prescriptive Analytics and Optimization
MKTG 3776/SCMA 3376 Transportation Security, Safety and Disaster Preparedness.

+ If offered and approved by the department faculty and the department chair.
College of Business Administration Academic Advising website:
http://www.umsl.edu/divisions/business/undergrad_advising/ Program Subject to Change

Appendix C: Existing Supporting Infrastructure

The Cybersecurity and Information Technology Innovation Lab (CITIL): The CITIL is UMSL's central hub for cybersecurity courses and programs. CITIL currently has two major components: (1) a virtual lab, and (2) a physical lab. These facilities are critical to providing a high-impact educational experience for students.

Dedicated Cybersecurity Virtual Lab: Students have access to a fully virtualized and sandboxed ethical hacking and penetration-testing environment where students learn the basics of network, host, and web application security. The lab is accessible remotely to students enrolled in cybersecurity courses. Work is currently under way to deploy a fully self-service private cloud infrastructure based on "OpenStack" that will allow students to create their own virtualized lab setups.

Dedicated Cybersecurity Physical Lab: The physical lab is designed to be the hub of student activity where they have a variety of tools and infrastructure to learn, play, and innovate. The physical cybersecurity lab (located in Room 204 Express Scripts Hall) is a state of the art facility with a student-capacity of 40. It features fully reconfigurable furniture to facilitate student collaboration and three 60-inch plasma screens. The lab includes a section dedicated to student exercises in computer forensics and other hands-on activities (e.g., monitoring network traffic). Pre-configured machines with software such as Wireshark and Oracle VirtualBox are available for lab exercises and are secured via a dedicated laptop cart in the room. The lab also hosts dedicated servers configured to provide a self-service private cloud for students and faculty. While the virtual lab provides a limited number of network and application setups the private cloud allows students to fully experience cloud computing and, more importantly, create test/practice labs. Faculty and students have access to scalable computing resources and ready-to-use virtual machine images customized to carry out a variety of tasks.

Academic Alliances and Resulting Access to Various Software/Teaching Resources: UMSL has academic alliances with Microsoft, IBM, and VMware, as well as smaller vendors of analytics and security products. UMSL is part of the Microsoft DreamSpark Premium initiative that gives students access to full versions of most Microsoft software (desktop/server operating systems, development environments, applications, and security tools). The IBM Academic Initiative partnership provides useful teaching resources to faculty in the areas of cloud, analytics, and security, among others. Students have unrestricted access to IBM's Bluemix® PaaS Cloud platform (renewable yearly). UMSL's academic subscription with VMware provides students with access to full versions of VMware's enterprise class virtualization products and hypervisors. In addition, UMSL has academic licenses for fast growing tools from emerging security vendor, Rapid7. These tools include Metasploit Pro®, one of the most widely used framework and supporting tools for Penetration Testing, and Nexpose Enterprise®, an enterprise-class security risk intelligence tool. There is also a vast array of open source tools available to students as the cybersecurity programs routinely compile information and download links to make it easier for students.

Tutoring Centers for Mathematics and Writing. UMSL is home to a state-of-the-art Mathematics and Writing Academic Center that includes a welcoming modern space with technology tools for tutoring and directed team study. Tools include desktop workstations and "collaboration stations" with multiple monitors and associated hardware.

Appendix D: Letters of Support

Unisys Corporation
11720 Plaza America Dr.
Tower III
Reston, VA 20190

O: 703.439.5347
peter.odonoghue@unisys.com

March 8, 2018

Dr. Shaji Khan
Director of Cybersecurity Institute
Assistant Professor of Information Systems
College of Business Administration
University of Missouri-Saint Louis
234 Express Scripts Hall, One University Blvd.
Saint Louis, MO 63121

Dear Dr. Khan:

I am writing to support the creation of new Cybersecurity degree programs at the University of Missouri-St. Louis (UMSL). Unisys, a global company, has been in St. Louis for almost two decades and has supported UMSL's Information Systems Advisory Board (ISAB). Unisys has enjoyed watching UMSL's technical certificate and degree programs mature and become nationally recognized.

The growing number of security breaches (both publicized and unpublicized) across the United States demands increasing awareness, attention and solutions. The demand for talented cybersecurity professionals grows faster than it can be met which is why we wholeheartedly support the creation of the new Cybersecurity degree programs at the University of Missouri-St. Louis (UMSL).

Sincerely,



Peter O'Donoghue
Vice President, Application Services
Unisys Corporation

March 9, 2018

Dr. Shaji Khan
Director of Cybersecurity Institute
Assistant Professor of Information Systems
College of Business Administration
University of Missouri-Saint Louis
234 Express Scripts Hall, One University Blvd.
Saint Louis, MO 63121

Dear Dr. Shaji Khan,

As a UMSL IS alumni, I'm writing to letter to show my support for the creation of a new Cybersecurity degree program at my alma mater. During my time at UMSL, I thoroughly enjoyed my experience in the IS department and it helped shaped my career path. I was lucky enough to be one of the first few to attend the new cybersecurity courses that was taught by you, and what I learned from those courses, help contributed to my success during my time as a Cybersecurity Co-Op at Ameren.

After being in the field for over two years as a Cybersecurity Analyst, I've learned that one of the most concerning national challenges in cybersecurity is the lack of talent for the growing demand. PwC estimated that by 2019, we'll face a cybersecurity workforce gap of 1.5 million openings. Most universities in the Saint Louis area has already started a Cybersecurity degree program to help tackle the widening gap. I believe that with the resources UMSL has to offer, UMSL can deliver a much more valuable and top-tier program, compared to what this region has to offer.

If a few cybersecurity courses from UMSL help developed a cybersecurity professional such as myself, I can't imagine what a Cybersecurity degree program will produce.

Sincerely,



Dante Thong Nguyen
UMSL IS Alum, Class of 2016

Cybersecurity Analyst II - Situational Awareness
tnguyen@ameren.com
Ameren Services
1901 Chouteau Ave Saint Louis, MO 63103



March 8, 2018

Dr. Shaji Khan, Director of Cybersecurity Institute
Assistant Professor of Information Systems
College of Business Administration
University of Missouri-Saint Louis
234 Express Scripts Hall, One University Blvd.
Saint Louis, MO 63121

Dear Dr. Khan,

I am writing to express my very strong support for new Cybersecurity degree programs at the University of Missouri-St. Louis.

As you know, Cybersecurity is an extremely important topic that is front and center for every business. Almost every customer that my IBM colleagues and I talk to want to hear IBM's Point of View on Cybersecurity, understand what we are doing to fight this threat, and lastly, how we can help them. The solution to this threat is multi-dimensional, far-reaching, and impacts everything we do as a society. To that end, UMSL must provide Cybersecurity education for your students so they have the awareness, insights, and skills needed to tackle this very serious threat to our industry and economy.

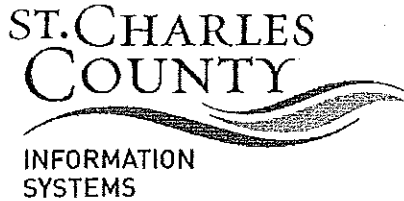
Even though we are rapidly transforming to a digital society, the national and regional Cybersecurity unfilled and open positions widen every year. This year in the United States there is a need for more than 1 million Cybersecurity workers yet there are 285,000 jobs not filled. In Missouri, we have a need for over 18,000 workers but there is a gap of over 4,400 unfilled jobs. This gap in skills is not sustainable and must be closed for the United States to lead the digital economy and protect ourselves from Cyber threats.

Thank you for making Cybersecurity a focus for UMSL. UMSL's significant commitment to Cybersecurity will make a real difference for our regional and national economy and security.

Sincerely,

A handwritten signature in black ink, appearing to read "Mark P. Stanley", is written over a white background.

Mark Stanley
IBM Executive
Sales & Distribution



Simon Huang
Director

Dr. Shaji Khan
Director of Cybersecurity Institute
Assistant Professor of Information Systems
College of Business Administration
University of Missouri-Saint Louis
234 Express Scripts Hall, One University Blvd.
Saint Louis, MO 63121

I am writing to support the creation of new Cybersecurity degree programs at the University of Missouri-St. Louis. Cybersecurity is, and will continue to be, an important need for all organizations and any program that can help address the talent shortage would be welcome.

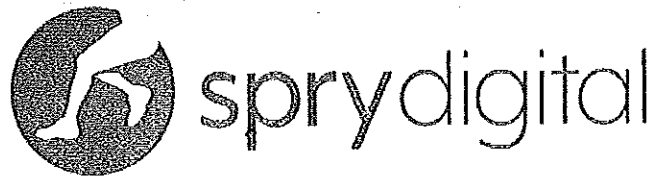
In 2017, the US has approximately 350,000 cybersecurity job openings according to the US Dept of Commerce¹. We have ourselves seen the impact at the regional level in St. Louis, and at the local level in St. Charles County, in our ability to attract such talent.

It is my hope that increasing the supply of cybersecurity graduates allows ALL organizations to better secure their computing infrastructure.

Sincerely,

A handwritten signature in black ink, appearing to read "S. Huang". The signature is fluid and cursive, with a long, sweeping tail on the final letter.

¹<https://www.csoonline.com/article/3200024/security/cybersecurity-labor-crunch-to-hit-35-million-unfilled-jobs-by-2021.html>



March 8, 2018

Dr. Shaji Khan
Director of Cybersecurity Institute
Assistant Professor of Information Systems
College of Business Administration
University of Missouri-Saint Louis
234 Express Scripts Hall, One University Blvd.
Saint Louis, MO 63121

Dear Dr. Shaji Khan,

I am writing to support the creation of new Cybersecurity degree programs at the University of Missouri-St. Louis (UMSL).

Spry Digital, LLC is a digital marketing company located in the St. Louis area and we currently employ one graduate and one student of UMSL including Dominic LaFata and myself.

As you may be aware, the region and nation has a substantial shortage of qualified, educated talent in the cybersecurity arena. This talent gap could be addressed by the creation of quality Cybersecurity degree programs at a trusted and reputable learning institution such as UMSL .

As digital technology continues to grow and expand globally, I feel it would be an ideal time to leverage our community into a leading position within the technology world. We can accomplish this by offering educational resources and opportunities such as a Cybersecurity degree from the University of Missouri - St. Louis.

Sincerely,

A handwritten signature in black ink that reads "Sheila Burkett". The signature is written in a cursive style and is followed by a horizontal line.

Sheila Burkett
CEO, Spry Digital, LLC

OPEN - AS&RED - 2-43

April 11, 2019



Dr. Shaji Khan
Director of Cybersecurity Institute
Assistant Professor of Information Systems
College of Business Administration
University of Missouri-Saint Louis
234 Express Scripts Hall, One University Blvd.
Saint Louis, MO 63121

Dr. Khan:

I am writing in support of the creation of new Cybersecurity degree programs at the University of Missouri-St. Louis (UMSL). As a technology services provider in the region, TDK Technologies is always in search of talented technology professionals. As the unemployment rate in technology continues to run well below the national average, employers are in need of additional sources of candidates to fill their needs. New cybersecurity threats arise in the US and globally on a seemingly daily basis; it will be critical for organizations to have qualified professionals to protect against those threats.

We have been very pleased with the web developers from UMSL we have utilized as interns and hired as full-time employees on our development staff. I expect that students in the new Cybersecurity degree programs will enjoy the same level of success in the business community.

Sincerely,

A handwritten signature in black ink, appearing to read 'Kristin Tucker', is written over the typed name. The signature is fluid and cursive.

Kristin Tucker
Managing Principal

HUSSMANN®

Hussmann Corporation
12999 St. Charles Rock Road
Bridgeton, MO 63044-2483
Office: (314) 291-2000; Fax: (314) 298-4756
www.hussmann.com

March 5, 2018

Dr. Shaji Khan
Director of Cybersecurity Institute
Assistant Professor of Information Systems
College of Business Administration
University of Missouri-Saint Louis
234 Express Scripts Hall, One University Blvd.
Saint Louis, MO 63121

Dear Dr. Khan:


As an IT leader in the St. Louis business community and member of the school's IS Advisory Board, I am encouraged to see the continued commitment by the University of Missouri - St. Louis to the development of information technology professionals in the St. Louis community. The school's formation of a cybersecurity degree program is an exciting and valuable extension of this commitment.

Cybersecurity is a very important topic for Hussmann and a major focus of mine. When I returned to an IT role in 2016 after spending approximately 10 years in a business side, it amazed me how sophisticated and persistent cybersecurity threats had become. No business or organization is immune from these threats and many small to mid-market companies in the St. Louis market might be especially susceptible given their lack of resources. Our local business community needs a qualified pipeline of security professionals to adequately protect against these growing threats.

As an alum, I am proud to say that Hussmann has several talented UM-St. Louis grads in key positions within our IT department. These UMSL grads represent some of our best and brightest IT professionals. As an example, our Director, Application Development and Support, also an alum, is leading a major modernization of Hussmann's customer-facing application platform. Similarly, I was proud to support the promotion of a young lady who is a 2014 computer science grad into a highly visible role within our technology VC/incubator program.

Please know that Hussmann will be a very supportive business partner as you bring your new program to life.

Kindest Regards,



Michael Seals
Vice President and Chief Information Officer
Hussmann Corporation
University of Missouri - St. Louis, BSBA 1986

OPEN - AS&RED - 2-45

April 11, 2019

Appendix E: BS Cybersecurity Financial Projections

	FY20	FY21	FY22	FY23	FY24	FY25	FY26	FY27
Enrollment Projections								
Head Count Students - new incoming	30	108	177	236	291	325	326	326
Head Count Students - transfers within campus	10	19	26	33	39	39	39	39
Student Credit Hours	816	2,591	4,141	5,488	6,732	7,426	7,446	7,446
Tuition Rate/Credit Hour	\$349.70	\$356.69	\$363.83	\$371.10	\$378.53	\$386.10	\$393.82	\$401.70
Fee Rate/Credit Hour (A&S Fees)	\$10.40	\$10.61	\$10.82	\$11.04	\$11.26	\$11.48	\$11.71	\$11.95
Fee Rate/Credit Hour (CoBA Fees)	\$81.70	\$83.33	\$85.00	\$86.70	\$88.43	\$90.20	\$92.01	\$93.85
Tuition Discount Rate (%)	19%	19%	19%	19%	19%	19%	19%	19%
Revenue Projections								
Tuition	\$285,355	\$924,123	\$1,506,684	\$2,036,473	\$2,548,241	\$2,867,002	\$2,932,376	\$2,991,024
Supplemental & Other Fees (A&S Fees)	\$5,924	\$19,186	\$31,281	\$42,280	\$52,905	\$59,523	\$60,880	\$62,098
Supplemental & Other Fees (CoBA Fees)	\$20,127	\$65,181	\$106,270	\$143,638	\$179,734	\$202,217	\$206,828	\$210,965
Scholarship Allowances	-\$59,167	-\$191,613	-\$312,405	-\$422,254	-\$528,367	-\$594,461	-\$608,016	-\$620,176
Net Tuition and Fees	\$252,239	\$816,877	\$1,331,830	\$1,800,136	\$2,252,512	\$2,534,281	\$2,592,068	\$2,643,910
Other Income								
TOTAL PROGRAM REVENUE	\$252,239	\$816,877	\$1,331,830	\$1,800,136	\$2,252,512	\$2,534,281	\$2,592,068	\$2,643,910
Recurring State Support								
TOTAL REVENUE	\$252,239	\$816,877	\$1,331,830	\$1,800,136	\$2,252,512	\$2,534,281	\$2,592,068	\$2,643,910
Expenditure Projections								
Faculty Salaries	\$0	\$210,000	\$314,200	\$320,484	\$326,894	\$333,432	\$340,100	\$346,902
(1.1% IST, 1.0% with 2% salary increase)								
Total Salaries	\$0	\$210,000	\$314,200	\$320,484	\$326,894	\$333,432	\$340,100	\$346,902
Benefits	\$0	\$74,802	\$111,918	\$114,156	\$116,440	\$118,768	\$121,144	\$123,567
Subtotal Salaries and Benefits	\$0	\$284,802	\$426,118	\$434,640	\$443,333	\$452,200	\$461,244	\$470,469
Operating Expense								
Advertising Expenses	\$50,000	\$40,000	\$30,000	\$25,000	\$25,000	\$25,000	\$25,000	\$25,000
Subtotal Operating Expense	\$50,000	\$40,000	\$30,000	\$25,000	\$25,000	\$25,000	\$25,000	\$25,000
One-time Expenditures (Startup Costs)			\$75,000					
Additional Space Costs								
Subtotal One-time Expense	\$0	\$0	\$75,000	\$0	\$0	\$0	\$0	\$0

	FY20	FY21	FY22	FY23	FY24	FY25	FY26	FY27
TOTAL EXPENDITURES	\$50,000	\$324,802	\$531,118	\$459,640	\$468,333	\$477,200	\$486,244	\$495,469
DIRECT MARGIN	\$202,239	\$492,075	\$800,712	\$1,340,495	\$1,784,179	\$2,057,081	\$2,105,824	\$2,148,441
CUMULATIVE DIRECT MARGIN	\$202,239	\$694,314	\$1,495,026	\$2,835,522	\$4,619,701	\$6,676,782	\$8,782,606	\$10,931,047
Subtract:								
Revenue from Transfers within Campus	\$63,050	\$122,210	\$170,579	\$220,835	\$266,206	\$271,530	\$276,961	\$282,500
NET MARGIN TO THE CAMPUS	\$139,179	\$369,865	\$630,133	\$1,119,661	\$1,517,973	\$1,785,551	\$1,828,864	\$1,865,941
CUMULATIVE NET MARGIN TO THE CAMPUS	\$139,179	\$509,044	\$1,139,177	\$2,258,838	\$3,776,811	\$5,562,362	\$7,391,226	\$9,257,167
Campus Overhead Allocation	\$97,104	\$308,305	\$492,803	\$653,024	\$801,108	\$883,646	\$886,074	\$886,074
MARGIN AFTER CAMPUS OVERHEAD	\$42,075	\$61,559	\$137,330	\$466,637	\$716,865	\$901,905	\$942,790	\$979,867
CUMULATIVE MARGIN AFTER CAMPUS OVERHEAD	\$42,075	\$103,635	\$240,965	\$707,602	\$1,424,467	\$2,326,372	\$3,269,161	\$4,249,028
Assumptions Note: The enrollment and graduation projections may not be applicable beyond the 8-year planning horizon used in this proposal.								
Assumptions for Enrollment Projections								
Enrollment Projections are based on Enrollment Projections Sheet. All figures account for Graduations and Attrition to arrive at how many students are enrolled (taking courses) each year.								
Graduation based reductions in yearly enrollments is based on assumptions made using UMMSL graduation data. See footnote 1 in Enrollment Projections Sheet.								
Assumptions for Financial Calculations (more details in proposal document)								
Credit Hour Calculation: Full-time Undergraduate Course Load of 12 credit hours per semester * 2 semesters * number of students enrolled each semester after taking into account graduation and attrition. 24 as opposed to typical full-time load of 30 is used to account for some students taking longer to finish while not being completely part-time. Part-time load is taken as 12 credits per year. Major Specific Course Credits for each year are difficult to estimate as two emphasis areas are of different lengths and it is not feasible to predict which student will take which courses in a given year.								
Fee Calculation: Courses are from College of Business Administration and College of Arts & Sciences which have different fees. Based on the course makeup across emphasis areas, approximately 69.8% credit hours were taken to be from A&S and 30.2% from CoBA.								
Revenue from Transfers within Campus (item 9): Total Revenues from item 5 were reduced by a proportion of Transfers Student Numbers divided by Total Enrolled each Year.								
Tuition Rate and Fee Rates Based on Year 2019 data and increased at an assumed CPI rate of 2% annually.								
No one time startup costs, renovation costs, etc. are anticipated. Existing facilities are deemed enough. A \$75000 upgrade for lab equipment (servers, networking equipment) etc. is included only in year 3.								
Additional facility lines requested in second and third year if enrollment projections met.								
Campus Overhead Allocation: Assumes \$63/SCH for college overhead and \$64/SCH for campus overhead, excludes campus depreciation. This calculation may be skewed in the sense adding Cybersecurity isn't anticipated to add college or campus overhead.								

New Program Template for MDHE Approval

Please fill in the fields within the < > symbols.

Implementation Date: <06/03/2019>

Where is this program to be delivered? <Main UMSL Campus>

CIP Code: <11.1003> <https://nces.ed.gov/ipeds/cipcode/browse.aspx?v=55>

Program Name: <Cybersecurity>

Degree Level: <BS-Bachelor of Science>

Options: <Computer Science (CS); Information Systems and Technology (IST)>

Collaboration: <Not applicable>

Mode of Delivery: <Classroom; Online; Hybrid>

Student Preparation: <none>

Population Served: <not applicable>

Faculty Characteristics:

Special Requirements: <Normative departmental standards in Computer Science and Information Systems and Technology will apply.>

Credits for FTE Faculty: < 75% for Full-Time Faculty >

Expectations: <All faculty members are actively involved in their own professional development, student mentoring and guidance toward developing applied cybersecurity skills, as well as in various activities related to community outreach, partnership development, and service. Core cybersecurity faculty are also consistently involved in developing innovative lab infrastructures, assignments, and learning tools for students by drawing on external grant funding, donations from/partnerships with cybersecurity related firms, and collaborations with other academics within and outside UMSL.>

Student Enrollment Projections: Fill in the below table

Year One Projections			
Full Time: 28	Part Time: 12	Total: 40	
Year Two Projections			
Full Time: 89	Part Time: 38	Total: 127	
Year Three Projections			
Full Time: 142	Part Time: 61	Total: 203	Graduates: 14
Year Four Projections			
Full Time: 188	Part Time: 81	Total: 269	
Year Five Projections			
Full Time: 231	Part Time: 99	Total: 330	Graduates: 38

Licensing or Certification: <not applicable>

Program Accreditation: <UMSL has already been designated a Center of Academic Excellence in Cyber Defense Education (CAE-CDE) by the National Security Agency and the US Department of Homeland Security for its existing cybersecurity certificates. This degree program is designed to comply with the CAE-CDE undergraduate degree standards and is expected to meet CAE guidelines when designation is reviewed/renewed in 2021>

Program Structure:

Credits: <120 for CS Emphasis or 126 for IST Emphasis>

Residency Requirements: <Transfer students must complete at least 30 hours and at least 15 major hours in residence.>

General Education Credits: <27 (CS Emphasis) or 15 (IST Emphasis) out of 42 total general education credits>

Major Credits: <CS Emphasis = 80; IST Emphasis = 111>

Courses: Fill in the below table (adding lines as needed) with courses included in the program.

General Education Courses (specific courses OR distribution area and credits)

Computer Science Emphasis		Information Systems and Technology Emphasis	
Distribution Area	Credits	Distribution Area	Credits
First Year Writing	3	First Year Writing	3
Communications Proficiency	3	Communications Proficiency	3
Mathematics Proficiency ³	0/3	Mathematics Proficiency	0/3
Information Literacy	0/3	Information Literacy	0/3
US History & Government	3	US History & Government	3
Humanities & Fine Arts ⁶	9	Humanities & Fine Arts	6/9
Social Sciences ⁶	9	Social Sciences	0/9
Math & Sciences	0/9	Math & Sciences	0/9
GENERAL EDUCATION TOTAL (42 total hours - 15 hours included as major requirements)	27	GENERAL EDUCATION TOTAL (42 total hours - 27 hours included as major requirements)	15

Course Number	Credits	Course Title
ENGL 3120/3130	3	Business Writing or Technical Writing
MATH 3000	3	Discrete Structures
INFSYS 3848	3	Introduction to Information Security
INFSYS 3868	3	Secure Software Development
INFSYS 3878	3	Information Security Risk Management and Business Continuity
CMP SCI 1250	3	Introduction to Computing
CMP SCI 2250	3	Programming and Data Structures
CMP SCI 2261	3	Object-Oriented Programming
CMP SCI 2700	3	Computer Organization and Architecture
CMP SCI 2750	3	System Programming and Tools
CMP SCI 4700	3	Computer Forensics
CMP SCI 4732	3	Introduction to Cryptography for Computer Security
	36	Core courses applicable to both emphasis areas
MATH 1320	3	Introduction to Probability and Statistics
MATH 1800	5	Analytic Geometry and Calculus I
CMP SCI 3010	3	Web Programming
CMP SCI 3130	3	Design and Analysis of Algorithms
CMP SCI 3760	3	Cyber Threats and Defense
CMP SCI 3780	3	Software Security
CMP SCI 4730	3	Computer Networks and Communications
CMP SCI 4750	3	Introduction to Cloud Computing
CMP SCI 4760	3	Operating Systems
CMP SCI 4782	3	Information Security
CMP SCI 4794	3	Introduction to Security of IoT Systems
	9	Major Specific Electives
	44	Total Required for Computer Science Emphasis Area
MATH 1030	3	College Algebra (MOTR MATH 130)
MATH 1100	3	Basic Calculus
MATH 1105	3	Basic Probability and Statistics
ECON 1001	3	Principles of Microeconomics (MOTR ECON 102)
ECON 1002	3	Principles of Macroeconomics (MOTR ECON 101)
BUS AD 2900	3	Legal Environment of Business
	3	Cultural Diversity Requirement
INFSYS 2800	3	Information Systems and Technology Concepts and Applications
ACCTNG 2400	3	Fundamentals of Financial Accounting
ACCTNG 2410	3	Managerial Accounting
SCMA 3300	3	Business Analytics and Statistics
SCMA 3301	3	Introduction to Supply Chain Management
MGMT 3600	3	Management and Organizational Behavior
FINANCE 3500	3	Financial Management
MKTG 3700	3	Basic Marketing
MGMT 4219	3	Strategic Management
INFSYS 3820	3	Introduction to Systems Administration
INFSYS 3842	3	Data Networks and Security
INFSYS 3806	3	Managerial Apps of Object-Oriented Prog. I
INFSYS 3815	3	Object Oriented Applications in Business
INFSYS 3845	3	Database Management Systems
INFSYS 3858	3	Advanced Security and Information Systems and Technology
SCMA 4347	3	Introduction to Project Management
	6	Major Specific Electives
	75	Required for Information Systems and Technology Emphasis Area

Elective Credits: <Free Electives: CS emphasis = 13; IST emphasis = 0>

Thesis/Capstone/Internships: <none (internship included as a major specific elective)>

Assurances:

Read and check the below assurances, and sign your name at the bottom (electronically or by hand).

X	I certify that the program is clearly within the institution's CBHE-approved mission. The proposed new program must be consistent with the institutional mission, as well as the principal planning priorities of the public institution, as set forth in the public institution's approved plan or plan update.
X	I certify that the program will be offered within the proposing institution's main campus, CMHE-approved service region or CBHE-approved off-site location.
X	I certify that the program will not unnecessarily duplicate an existing program within the geographically applicable area.
X	I certify that the program will build upon existing programs within the geographically applicable area.
X	I certify that the program can be launched with minimal expense and falls within the institution's current operating budget.
X	I certify that the institutions has conducted research on the feasibility of the proposal and it is likely the program will be successful. Institutions' decision to implement a program shall be based upon demand and/or need for the program in terms on meeting present and future needs of the locale, state, and nation based upon societal needs, and/or student needs.

Signature: _____

Name: _____