University of Missouri - Saint Louis
Master of Science in Cybersecurity

Table of Contents

Tables

Appendices

Executive Summary

Despite growing concerns about cybersecurity for industry, government, and national security, reports indicate a continued severe shortage of skilled cybersecurity talent. Trends also suggest that working professionals from diverse undergraduate backgrounds are seeking educational opportunities in cybersecurity in order to transition into this high-demand field. This proposal seeks to add a STEM designated (CIP Code 11.1003) multi-disciplinary **Master of Science (M.S.) in Cybersecurity** degree at the University of Missouri-St. Louis (UMSL) in order to address the talent shortage. The degree 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). This prestigious designation requires degree programs to meet requirements set forth by the NSA and DHS.

Cybersecurity is a strategic initiative at UMSL. The proposed program leverages significant investments in faculty, course work, and lab infrastructure since 2014. Thus, no new faculty or infrastructure investments are needed to start this program. As enrollments grow, two faculty lines are included in financial planning starting year 4. The program is strongly supported by industry and government organizations in the region as indicated by their letters of support. Overall, strong student demand and market conditions suggest a financially and academically viable program that will further strengthen the University of Missouri and the State.

Given the multi-faceted nature of the field of cybersecurity, the degree is designed to be multi-disciplinary. The 30 credit-hour program leverages existing partnerships between the departments of Computer Science (College of Arts and Sciences) and Information Systems and Technology (College of Business Administration). It has two emphasis areas: 1) Information Systems and Technology Emphasis; or 2) Computer Science Emphasis. The program culminates with a capstone course that provides opportunities to participate in real-life projects dealing with various facets of cybersecurity.

The M.S. Cybersecurity program complements the multi-disciplinary *Bachelor of Science (B.S.) in Cybersecurity* program, which is being proposed simultaneously. While the B.S. Cybersecurity degree meets the NSA/DHS CAE-CDE requirements for undergraduate cybersecurity programs, both emphasis areas in the M.S. degree meet or exceed the current NSA/DHS CAE-CDE Knowledge Unit requirements and learning outcomes for graduate cybersecurity programs. The Information Systems and Technology emphasis is geared more toward management of cybersecurity from a business perspective and meets the Non-Technical Core Knowledge Unit requirements set forth by the NSA/DHS. The Computer Science emphasis is geared toward technical aspects of cybersecurity and meets the Technical Core Knowledge Unit requirements and learning outcomes.

Thus, the M.S. Cybersecurity program allows B.S. Cybersecurity graduates with Computer Science or Information Systems and Technology emphasis areas to pursue their respective emphasis areas in greater depth and breadth in the M.S. program. It also allows students to switch emphasis areas at the graduate level. Further, the M.S. Cybersecurity program enables professionals with undergraduate degrees in other majors

to transition into cybersecurity, subject to entry requirements and depending on their technical- or business-oriented backgrounds. The program provides flexibility to students and enables them to pursue a variety of in-demand cybersecurity and Information Technology related work roles. It is also cost effective when compared with similar programs in the Saint Louis region.

1. Introduction

Cybersecurity has become a critical issue for industry, government, and national security. However, reports indicate a continued severe shortage of skilled cybersecurity talent across both public and private sectors.

This proposal seeks to add a STEM designated **Master of Science (M.S.) in Cybersecurity** degree program at the University of Missouri-St. Louis (UMSL). The program addresses the current and future predicted talent shortages in the broad field of cybersecurity (please see Section 3). Given cybersecurity is both a technical as well as a management issue facing organizations, the program is designed to be multi-disciplinary in its curriculum. It leverages existing partnerships between the departments of Computer Science (College of Arts and Sciences) and Information Systems and Technology (College of Business Administration).

This 30 credit-hour interdisciplinary graduate cybersecurity degree program has two emphasis areas:

1) Information Systems and Technology Emphasis *or*

2) Computer Science Emphasis

The Information Systems and Technology emphasis is geared toward management of cybersecurity from a business perspective. The Computer Science emphasis is geared toward technical aspects of cybersecurity. Students must choose an emphasis area at the time of admission and meet different entry requirements depending on the chosen emphasis.

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) and draws on both the NSA/DHS knowledge unit requirements as well as the National Initiative for Cybersecurity Education - *Cybersecurity Workforce Framework* (NICE-CWF) Knowledge, Skills, and Abilities guidelines to create a well-rounded curriculum. Both emphasis areas meet or exceed the NSA/DHS CAE-CDE requirements for graduate cybersecurity programs in terms of knowledge units and learning outcomes and also map to the NICE-CWF. The graduate program complements the *Bachelor of Science (B.S.) in Cybersecurity program,* which is being proposed simultaneously. Section 5 elaborates on the program structure.

Depending on student backgrounds and prior work experience, the program will allow graduates to pursue high-demand work roles such as Cybersecurity Specialist, Cyber

Defense Forensics Analyst, Cyber Defense Incident Responder, Information Security Analyst, Security Architect, Information Systems Security Manager, Cybersecurity Risk Management Analyst, Cybersecurity Awareness and Training Analyst, IT Program Auditor, among a variety of cybersecurity and Information Technology (IT) related roles[1].

This program is being proposed after significant learning and capability development at UMSL as part of its strategic efforts to focus on this important area starting in 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. These existing programs allowed us to develop supporting infrastructure for robust cybersecurity education in the form of a dedicated physical cybersecurity laboratory as well as innovative, fully virtualized cybersecurity lab environments (please see section 4). All of the courses developed earlier toward our initial graduate cybersecurity certificate are included in this proposed M.S Cybersecurity program.

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 in the State. The cybersecurity degree program will be coordinated by the Director of Cybersecurity Institute in conjunction with the College of Arts and Sciences and College of Business Administration.

2. Fit with University Mission and Other Academic Programs

2.A. Alignment with Mission and Goals

The mission statement of the University of Missouri-St. Louis is "*We transform lives*." As a metropolitan, land-grant, research institution serving the diverse and economically vibrant St. Louis region, UMSL's strategic focus revolves around five *compacts* shared by the broader UM System. Among these five compacts "Excellence in Student Success" and "Excellence in Community Engagement and Economic Development" directly support the creation of a strong set of cybersecurity programs sustained by UMSL's efforts at making a broader impact on the region by bringing industry, government, schools, and community colleges, among other stakeholders, to work together for a vibrant and strong cybersecurity eco-system.

Cybersecurity programs and the various surrounding initiatives have been a strategic priority for the campus, as well as for the College of Business Administration and the College of Arts and Sciences. The Information Systems and Technology and Computer Science departments collaborate to offer strong multi-disciplinary cybersecurity certificate and minor programs, supported by the University administration at all levels. Cybersecurity is seen as a growth area and the campus is committed to continue pursuing strong programs in this area.

[1] 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.

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

Currently, the UM System does not offer a graduate cybersecurity degree program. Among other public institutions in Missouri, Missouri State University, Missouri Western State University, University of Central Missouri, and Southeast Missouri State University currently have master's degrees serving those regions. Only one other public institution, Harris-Stowe State University in the Saint Louis region has a management of cybersecurity focused master's degree. These regional programs do not adequately support the Saint Louis metropolitan area. A few private universities also have master's programs related to cybersecurity. The M.S. Cybersecurity program proposed here differentiates itself from cybersecurity related master's programs among Saint Louis region's private universities in at least three ways. First, this program is truly multi-disciplinary in nature. Second, none of these existing programs have a current NSA/DHS CAE-CDE designation as highlighted below. Third, this program makes cybersecurity graduate education more accessible to a wider population in terms of costs and value when compared to the private universities. In summary, there is no duplication within the UM System and little overlap across the state given the wide geographic separation and different foci among the institutions mentioned above.

UMSL's current NSA/DHS CAE-CDE designation sets its programs apart from non-designated programs in the State of Missouri. The new degree program will further strengthen Missouri's standing among the National Centers of Academic Excellence in Cyber Defense Education community. UMSL is also poised to collaborate with other UM System Campuses to further strengthen Missouri's offerings in cybersecurity education as well as for creating cybersecurity related economic development impacts in the region. This focus is in line with the UM System President's call for more systematic collaboration among the four UM System campuses on cybersecurity education, research, and economic development.

In summary, given minimal overlap and UMSL's leadership position in cybersecurity education as a CAE, focus on UM System-wide and State-wide collaboration initiatives, and strong overall demand for cybersecurity talent in the Saint Louis Metropolitan region, we believe that this new program will further strengthen Missouri's standing across the nation.

3. Business-Related Criteria and Justification

3.A. Market Analysis

3.A.1. Need for Program

Industry reports such as the *Frost & Sullivan* and *(ISC)*^{2} 2017 Global Information Security Workforce Study indicate a severe talent shortage in cybersecurity related fields. A projected 1.8 million cybersecurity positions will remain unfilled worldwide by year

2022, a 20% increase from a previous report targeting year 2020[2]. In the study, 68% of North American respondents report that their security departments are understaffed and 52% attribute the cybersecurity talent shortage to an inability to find qualified candidates. This current and projected talent shortage cuts across both public and private sectors and throughout local, regional, national, and international levels.

While many entry level positions in cybersecurity typically require an undergraduate degree in cybersecurity or related fields, industry reports also indicate that many professionals coming from non-cybersecurity backgrounds such as IT and Business are making a career switch into cybersecurity. In fact, due to the current shortage of talent in the field, it is common that people with undergraduate degrees in a diversity of majors are seeking training and education opportunities in cybersecurity to help them make the career-switch into cybersecurity. Further, the *Global Knowledge, IT Skills and Salary Report 2018* indicates that a large majority of organizations are retraining existing staff to address the cybersecurity talent shortage[3]. Current enrollments in UMSL's Graduate Certificate in Cybersecurity also suggest a similar pattern; students with existing undergraduate degrees seeking graduate level education in cybersecurity to enhance their career prospects. The proposed Master of Science in Cybersecurity degree addresses this broad need.

With the increasing strategic focus on cybersecurity among business and government organizations, demand for cybersecurity talent is expected to grow. Within the public sector, the Saint Louis region has a growing contingent of Federal agencies with high demand for cybersecurity related talent. UMSL is in close proximity to the Scott Airforce Base and the newly opened Defense Information Systems Agency (DISA) Global Operations Command. The National Geospatial-Intelligence Agency (NGA) and their new, expanded NGA West location in North Saint Louis also adds to the growing 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 institution such as UMSL, and graduates of such programs are often preferred by "hiring authority" arrangements that follow Federal hiring process guidelines.

In summary, the new program will help address the talent shortage, make Missouri competitive in this increasingly important area and could have significant direct and indirect economic development impacts. Letters of support from industry, government, and alumni (please see Appendix C – 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

As evident from the strong overall demand for cybersecurity talent at the local, state, and national levels described above; strong support from regional and national employers for

[2] Report presented by ISC[2], 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

[3] Please see https://www.globalknowledge.com/us-en/content/salary-report/it-skills-and-salary-report/

this new program; and student demand for new degree programs in cybersecurity, we anticipate good enrollment levels.

UMSL admissions office indicates that cybersecurity was the *second most requested degree program* that UMSL did not offer by prospective students in 2016-2017 based on data collected using inquiry cards during site visits to high schools and community colleges.

In addition, due to its multi-disciplinary nature, this M.S. Cybersecurity program complements the multi-disciplinary Bachelor of Science in Cybersecurity degree in two ways. First, it allows students with Computer Science or Information Systems and Technology emphasis in the undergraduate cybersecurity program to continue pursuing their respective emphasis areas in greater depth and breadth. Second, it allows students to switch emphasis areas when they pursue the graduate degree in order to diversify their skillsets. The new M.S. Cybersecurity program is also attractive to current undergraduates in traditional computer science or information systems and technology programs seeking graduate education specializing in cybersecurity. In addition, the program is attractive to professionals with both technical and non-technical backgrounds seeking to transition into cybersecurity related careers or work roles. Many employers provide tuition-assistance for graduate education. The entry requirements for this degree's two emphasis areas allow professionals to make this transition depending on their background and interests.

Further, and subject to approval of the associated "2+3" campus-level proposal, the Bachelor of Science in Cybersecurity program provides an opportunity for undergraduate students to simultaneously pursue the Master of Science in Cybersecurity in a "*2+3 Undergraduate plus Graduate Cybersecurity Dual Degree*" format. The 2+3 Dual Degree program makes the graduate degree attractive to undergraduate students by allowing them to finish both degrees within 5 years and saving them up to 15 credit hours. The 2+3 program would appear as a separate campus-level proposal after the undergraduate and graduate degree proposals undergo the approval process.

In summary, the M.S. Cybersecurity program will serve students from both non-cybersecurity backgrounds making a transition into cybersecurity as well as students with existing cybersecurity backgrounds who wish to pursue greater depth or those who wish to diversify their skillsets. The programs provide flexibility to students and are cost effective when compared with similar programs in the region.

For this proposal, we arrived at enrollment projections drawing on enrollments data in existing related programs and demand projections from industry reports and initiatives such as CyberSeek.org[4]. In terms of enrollments in existing related programs, UMSL currently has a multi-disciplinary Undergraduate Certificate in Cybersecurity, a Minor in Cybersecurity and a multi-disciplinary Graduate Certificate in Cybersecurity. These programs came into effect in the Fall of 2015. In Fall 2018, 13 students were enrolled in courses toward the Graduate Cybersecurity Certificate and as of Fall 2018, 18 graduate

[4] Please see https://www.cyberseek.org/heatmap.html

cybersecurity certificates have been awarded. The graduate certificate program directly maps to a portion of the requirements in the new degree and could also act as a feeder program for the full degree.

Similarly, undergraduate enrollments in the Information Systems and Technology (233 enrollees in Fall 2017 for the B.S. Information Systems degree) and Computer Science (378 enrollees in Fall 2017 for the B.S. Computer Science degree) departments are quite high and have been at an upward trend for the past few years. These enrollments could also feed into the graduate cybersecurity degree as students are interested in specializing within cybersecurity given the demand.

Table 1a. provides five-year projections for anticipated total number of students enrolled in the M.S. Cybersecurity program each fall[5]. Approximately 30% of total students enrolled are considered to be part-time based on recent UMSL enrollment data. Enrollment figures are cumulative and after accounting for total new students joining the program (new to campus plus transfers within campus), some students leaving the program each year (attrition estimated at 5% of previous year's incoming enrollments) and student graduations on a two- or three-year timeframe. That is, year 1 full-time students graduate at end of year 2 and year 1 part-time students graduate at end of year 3. Graduations factor in at year 3 calculations and beyond. Table 1b. provides projections for students *that will be new to the campus* joining this program (that is, not including existing UMSL students from other majors who may switch into the new program). Again, these figures are cumulative and after accounting for "new to campus" students joining the program, some students leaving the program each year (5% attrition of previous year incoming enrollments), and student graduations calculated using the same approach as described for Table 1a.

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	22	53	70	74	73
Part-Time	10	23	30	32	31
Total	32	75	100	105	104

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	17	41	57	62	62
Part-Time	7	18	24	26	27
Total	24	59	81	88	89

[5] The financial projections spreadsheet attached as Appendix D contains detailed enrollment calculations used to arrive at tables 1a, 1b, and 1c.

Table 1c. provides an estimated number of degrees awarded. We arrived at the estimates as follows. The M.S. degree program is a total of 30 credit hours. We use 15 credit hours load per year estimate for full-time students and calculate full-time student graduations on a 2-year basis for the 30-credit hour program. We estimate that most part-time students should be able to complete in three years taking an average course load of 9 credit hours per year across Fall and Spring semesters for three years (27 credit hours), and adding one Summer course (the remaining 3 hours) in one of the years. Thus, we use a 10 credit hours per year average load for part-time students for ease of calculation. Based on these course loads, we expect graduations to start at end of year 2 for year 1 fall full-time enrollments and end of year 3 for year 1 fall part-time enrollments. We follow the same approach for subsequent year graduations based on enrollment figures given in Table 1a. Graduation numbers exclude students who leave the program (attrition).

Table 1c. Projected Number of Degrees Awarded

Year	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
# of Degrees Awarded	0	21	39	45	44	44	44	44	44	44

3.B. Financial Projections

3.B.1. Additional Resources Needed

As elaborated upon in Section 4, UMSL currently has sufficient capacity to successfully create and grow a strong M.S. Cybersecurity program due to investments made in the past four years in terms of faculty, courses, lab infrastructures, etc. Thus, no new facilities or resources are needed and no one-time initial expenditures are needed. Similarly, no new faculty resources are needed in the first three years. Contingent on adequate enrollments (please see sensitivity analysis below) and in order to expand course capacities, course offerings, and graduate student research support, we request 2 tenure-track faculty lines starting year 4 (total $230,000 per year at 2% salary increase in subsequent years). If enrollment targets are not met then additional faculty lines will not be needed.

In order to promote strong enrollment numbers, the university administration will support marketing expenses of $30,000 per year. The marketing and advertising funds complement the funds allocated for the undergraduate degree. Advertising and promotion are crucial to getting adequate awareness and exposure to our programs. No additional one-time or recurring expenses are needed.

3.B.2. Revenue

Final Revenue projections are provided in Table 2, *Financial Projections.* Revenue sources only include Tuition Fees and Supplemental Fees. The “Total Program Revenue” figures are based on Tuition and Supplemental fees using projected cumulative total student enrollments adjusted for possible attrition and projected graduations as shown in

Table 1a. The total program revenue figures are then adjusted to include only new students to campus (using numbers from Table 1b) as described below. The revenue projections should be considered baseline as they rely solely on in-state per credit hour tuition rate.

The financial projections are based on the "proforma new program spreadsheet" attached as Appendix D. The per year figures were arrived at as follows.

The full-time enrollment numbers from Table 1a were multiplied by a 15-credit hour graduate student load per year. Part-time enrollment numbers were multiplied by 10-credit hour graduate student course load per year. The total credit hours across all students were multiplied by "In-State" graduate tuition fee per credit hour based on 2019 rates.

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 52.50%[6] of the total credit hours while supplemental fees for courses offered through UMSL College of Arts and Sciences were multiplied by 47.50%. 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 graduate 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.

3.B.3. Net Revenue

As listed in Table 2, we do not anticipate any non-recurring expenditures. If the program were to meet enrollment targets, two contingent faculty lines would become a recurring expense beginning in Year 4. Marketing and advertising expenses listed above appear as recurring expenditures in all years. From the total program revenue in each year, we subtracted the total recurring expenditures each year to obtain the Direct Margin to Campus figures. From the Direct Margin to Campus figures, we subtracted revenue generated from "within-campus transfers" to retain only revenue that can be attributed to students who are new to the campus; giving us the Net Margin to Campus figures. The respective figures appear in Table 2. Thus, as shown in Table 2, this program is net revenue positive from year one.

Sensitivity Analysis

In order to assess impact of lower than anticipated enrollments, we looked at 25% fewer enrollments than projected in Table 1a in order to gauge impact on Direct Margin to Campus, Net Direct Margin to Campus, and Margin after Campus Overhead. Both Direct

[6] Due to the program's multi-disciplinary focus, approximately 52.50% of course credits are through the College of Business Administration and the remaining from the College of Arts and Sciences.

Margin to Campus and Net Direct Margin to Campus remain positive. However, Margin After Campus Overhead becomes negative starting year 4, coinciding with faculty line requests. This suggests that we will not request additional faculty lines in year 4 if we have 25% fewer enrollments than projected. Without the additional faculty lines, the programs remain Margin After Campus Overhead 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
New/Renovated Space					
Equipment					
Library					
Consultants					
Other: Advertising	$30,000	$30,000	$30,000	$30,000	$30,000
Total one-time	$30,000	$30,000	$30,000	$30,000	$30,000
B. Recurring					
Faculty	0	0	0	$230,00	$234,600
Staff					
Benefits				$81,926	$83,565
Equipment					
Library					
Other					
Total recurring	0	0	0	$311,926	$318.165
Total expenses (A+B)	$30,000	$30,000	$30,000	$341,926	$348,165
2. Revenue per year					
Tuition/Fees	$142,525	$357,380	$500,454	$554,577	$572,096
Institutional Resources					
State Aid -- CBHE					
State Aid -- Other					
Total revenue					
3. Net revenue (loss) per year	$112,525	$327,380	$470,454	$212,651	$223,932
4. Cumulative revenue (loss)	$112,525	$439,905	$910,359	$1,123,010	$1,346,942

Additional calculations available in Appendix D.
Additional faculty lines requested in year four contingent on enrollment projections.
Revenue includes tuition/fees subtract revenue from transfers within campus.

3.B.4. Financial and Academic Viability

Table 3 provides minimum enrollments for financial and academic viability. While we project that the program will be net revenue positive at the end of first academic year, we estimate that the minimum number of enrollments required at year 5 to break-even (i.e. financial viability) is 10 as a worst-case scenario. 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, after excluding the enrollment contingent recurring faculty line expenses starting in year 4.

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 10 students per year in the degree program.

In summary, based on the make-up of the program in terms 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	**10**
Academic	**10**

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

In addition to UMSL's campus wide recruitment initiatives such as UMSL Day and Graduate Programs Information Sessions etc., we will specifically carry out the following activities. The primary target groups of students for the Master of Science in Cybersecurity degree program will be students who are already working in business or technical fields and are looking for career enhancing educational opportunities often sponsored by employer tuition assistance. In terms of geographic segments, we will initially focus on the Saint Louis Metropolitan area to bootstrap enrollments but will simultaneously target the Mid-west region as well as market the program nationally. Our 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 their own focused recruitment and retention efforts.

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. Our marketing efforts for the M.S. Cybersecurity degree will also benefit from similar efforts geared toward the B.S. Cybersecurity degree program.

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 various aspects of the new cybersecurity degrees. This site will feature both the newly proposed B.S. and M.S. cybersecurity programs.

2) Our advertising budget allows for a reasonable scale web advertising campaign through Google Adwords and if possible, Facebook Ads specifically targeting our market segment described above.

3) Social media accounts using the "UMSL Cybersecurity" brand will be created to maximize the potential use of social media that complements paid advertising and will be used in conjunction with efforts related to our B.S. Cybersecurity programs.

Print Advertising and Other Promotion Efforts

1) UMSL's existing publications and other UM System publications will be requested to feature the new programs and associated developments.

2) When feasible, we will take out reasonably priced advertisements in the Saint Louis Post Dispatch and Saint Louis Business Journal before program launch.

3) UMSL's faculty are also active contributors to media inquiries related to cybersecurity incidents and participate in radio and TV segments on cybersecurity.

4) UMSL proudly hosts a regional conference on cybersecurity, STLCyberCon.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 at no registration costs. It features presentations by distinguished speakers on a variety of topics bridging theory and practice. A number of industry professionals from diverse backgrounds attend this conference making it an attractive venue for recruitment efforts. Both the College of Arts and Sciences and College of Business Administration representatives for graduate admissions have information booths at this event.

5) The College of Business Administration has a full-time college level Recruitment Coordinator as well as a dedicated Internship Coordinator.

Outreach and Scholarships

1) UMSL has good relationships with numerous business and government organizations and a large number of them provide tuition assistance for graduate education.

2) UMSL, the two departments and colleges have a robust Alumni network which is very active in promoting and supporting our programs.

3) Both the Information Systems and Technology as well as Computer Science departments have strong industry advisory boards. The new cybersecurity degrees will also lead to creation of a cybersecurity specific industry advisory board with representation from senior cybersecurity executives from industry and government.

4) The faculty are deeply engaged with the broader cybersecurity community among the public and private sectors. The department 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 $2000 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

Apart from other campus wide retention efforts that will also apply to the new program, 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 a web application dubbed "*MyConnect Early Alert System*" for use by faculty, advisors, and intervening organizations to better engage students in their courses and intervene early when students are becoming at risk. The application provides faculty with tools for early identification of students becoming at-risk of not achieving success in a course. Faculty could then "flag" a student. Flags range from aspects such as "Poor Attendance" and "Danger of Failing" down to "Failure to submit major assignment." Depending on the flag, a member of the relevant support office intervenes in a very methodical fashion. 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 IST department has a long-standing Student Mentorship program strongly supported by the Alumni. The program has regular events pertaining to doing well in school, career advice, and skills development. This program not only provides

opportunities to network and form a community but also plays an important role in keeping students engaged in their programs.

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 enough existing capacity to initiate high-quality M.S. in Cybersecurity program due to its sustained efforts at creating prior cybersecurity certificate programs and support of UMSL leadership. The University hired three tenure-track faculty and one non-tenure track faculty in 2014, dedicated to cybersecurity. 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. The University also draws from experienced cybersecurity professionals to teach on average two or three cybersecurity courses. Almost all of the courses in the new program are already in existence and being taught with current faculty resources. As proposed, the new degree structure requires the creation of only two new courses which can easily be accommodated by current faculty. As explained in Section 3, if enrollment targets are met, we will request additional faculty lines in Year 4 to increase course capacities through additional sections, support graduate student research, and to incorporate new courses as the cybersecurity field evolves. Thus, the creation of this new degree program will be supported with existing resources without any negative impacts on existing certificate programs.

Existing Supporting Infrastructure

As described in the B.S. Cybersecurity proposal, UMSL created a dedicated physical cybersecurity laboratory which is already operational. In addition, the faculty have spent considerable effort in creating three fully virtualized cybersecurity lab environments that are capable of supporting additional students and are highly scalable. Further, UMSL has existing access to software tools relevant for cybersecurity through Academic Alliances with Microsoft, IBM, and VMware among others (please see Appendix B for a brief description of these lab environments and other supporting infrastructure). In addition, the department of Computer Science's Ph.D. program and faculty resources will further support research initiatives for the M.S. Cybersecurity students within the Computer Science Emphasis.

5. Program Characteristics

5.A. Program Outcomes

Just as the B.S. Cybersecurity degree is designed to be meet NSA/DHS CAE-CDE requirements for undergraduate programs, both emphasis areas within the M.S. Cybersecurity degree meet or exceed the current NSA/DHS CAE-CDE Knowledge Unit

requirements and learning outcomes[7] for graduate programs. Meeting these requirements is necessary for designation of this newly proposed degree program in relation to UMSL's standing as a Center for Academic Excellence in Cyber Defense Education.

CAE designation requires specific unit level knowledge and learning outcomes. Within the CAE requirements framework, the Computer Science emphasis meets 1) the three "Foundational Knowledge Unit" requirements[8], 2) the necessary five "Technical Core Knowledge Unit" requirements[9], and 3) an adequate number (seven) of "Optional Knowledge Unit" requirements[10] per the designation criteria.

On the other hand, the Information Systems and Technology emphasis meets 1) "Foundational Knowledge Unit" requirements, 2) the necessary "*Non-Technical* Knowledge Unit" requirements[11], and 3) an adequate number of technical and non-technical "Optional Knowledge Unit" requirements per the designation criteria.

In essence, the NSA/DHS CAE-CDE designation process allows academic programs to be designated with "Technical" or "Non-Technical" cores. The M.S. Cybersecurity program pursues the "Technical" core through the Computer Science emphasis and the "Non-Technical" core through the Information Systems and Technology emphasis. Thus, the two emphasis areas nicely complement each other and are attractive to a diverse array of students with different backgrounds and career goals.

Further, the new programs, when going through the CAE-CDE designation process will require a mapping of program content and learning outcomes to the NICE Cybersecurity Workforce Framework (CWF). The CWF contains seven top level categories of cybersecurity related work roles. Programs are required to identify one or more of these seven categories of cybersecurity related work that the degree program maps to. Table 4 provides a crosswalk of the two emphasis areas with the most closely mapped CWF categories.

Table 4. M.S. Cybersecurity Degree Crosswalk with NICE CWF Categories

Category	Description	Emphasis Area Mapping
Securely Provision (SP)	Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.	Computer Science Emphasis
Operate and Maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information	Information Systems and Technology Emphasis and

[7] Please see https://cyberedwiki.org/index.php?title=Category:Foundational_KUs_(2020) for a list of "Knowledge Unit" requirements and learning outcomes associated with designating academic programs within the NSA/DHS CAE-CDE initiative.
[8] https://cyberedwiki.org/index.php?title=Category:Foundational_KUs_(2020)
[9] https://cyberedwiki.org/index.php?title=Category:Technical_Core_KUs_(2020)
[10] https://cyberedwiki.org/index.php?title=Category:Optional_KUs_(2020)
[11] https://cyberedwiki.org/index.php?title=Category:Non-Technical_Core_KUs_(2020)

Category	Description	Emphasis Area Mapping
	technology (IT) system performance and security.	Computer Science Emphasis
Oversee and Govern (OV)	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.	Information Systems and Technology Emphasis
Protect and Defend (PR)	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.	Computer Science Emphasis and Information Systems and Technology Emphasis

5.B. Structure

The **Master of Science (M.S.) in Cybersecurity** is an interdisciplinary program jointly provided by the departments of Information Systems and Technology (College of Business Administration) and Computer Science (College of Arts and Sciences).

This 30–credit hour degree program has two emphasis areas:

1) Information Systems and Technology Emphasis or

2) Computer Science Emphasis

M.S. Cybersecurity with Information Systems and Technology Emphasis

The Information Systems and Technology emphasis is geared toward management of cybersecurity from a business perspective. Entry requirements include basic technical foundations and/or work experience related to Information Technology (IT). This emphasis is designed for professionals from a diverse set of undergraduate backgrounds who wish to transition into management of information security related roles.

M.S. Cybersecurity with Computer Science Emphasis

The Computer Science emphasis builds on the foundation of an undergraduate cybersecurity or computer science degree and expects students to have prior background in foundational computer science areas or complete some foundational courses upon entry. This emphasis is designed to be focused on technical aspects of cybersecurity and provides greater depth than that afforded at an undergraduate level.

Degree Requirements

Students must meet all University of Missouri-St. Louis Graduate School admission and degree requirements.

Students must choose one of the emphasis areas at the time of application for admission. Admissions requirements vary by emphasis area (see Section 5E). Degree requirements also vary depending on the chosen emphasis area (see Program Structure below).

Common Courses

The degree has up to two common courses across both emphasis areas. It also provides the opportunity for students in one emphasis area to take up to two additional elective courses from the other emphasis area. Thus, the two emphasis areas share anywhere from two to four courses in common depending on student needs. This approach affords flexibility for students to pursue both technical or management aspects of cybersecurity, if they so desire, irrespective of their chosen emphasis. Both emphasis areas will have a newly designed Capstone Course (3 credit hours) that provides application-oriented exposure to students. It is also possible that the capstone courses will be cross-listed so that students with technical and management backgrounds work together in real-life settings to solve security issues; as is common in practice. Students will work with area organizations and take part in various aspects of the security life-cycle (please see Appendix A for course descriptions of the cross-listed capstone courses). In addition, students with Computer Science emphasis have the option of pursuing a 3-credit hour master's thesis if they desire to pursue research in cybersecurity.

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

PROGRAM STRUCTURE

1. Total credits required for graduation: 30

2. Residency requirements, if any: none

3. General education: Total credits for general education courses: **Not Applicable**

4. Major requirements

Total credits specific to degree: 30

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

Computer Science Emphasis		
Course #	**Title**	**Hours**
Required Courses		
CMP SCI 4730	Computer Networks and Communications	3
CMP SCI 4760	Operating Systems	3
INFSYS 6828	Principles of Information Security	3
CMP SCI 5732	Cryptography for Computer Security	3
CMP SCI 5782	Advanced Information Security	3
CMP SCI 5888	Cybersecurity Capstone[1]	3
	Required Courses Total	**18**
Electives (Choose 4. At least 2 must be from Computer Science.)		**12**
CMP SCI 4700	Computer Forensics	
CMP SCI 5750	Cloud Computing	
CMP SCI 5794	Security of IoT Systems	
INFSYS 6858	Advanced Cybersecurity Concepts	
INFSYS 6868	Software Assurance	
INFSYS 6878	Management of Information Security	
Other electives upon approval of Computer Science department chair		
	Total Credit Hours	**30**
1 A student is allowed to work on three credit-hours of Master's Thesis (CMP SCI 6990) in place of Cybersecurity Capstone (CMP SCI 5888)		

Information Systems and Technology Emphasis		
Course #	**Title**	**Hours**
Required Courses		
INFSYS 6820	Systems and IT Infrastructure	3
INFSYS 6836	Management of Data Networks and Security	3
INFSYS 6828	Principles of Information Security	3
INFSYS 6858	Advanced Cybersecurity Concepts	3
INFSYS 6868	Software Assurance	3
INFSYS 6878	Management of Information Security	3
INFSYS 6847	Project Management	3
INFSYS 6888	Capstone in Information Security	3
	Required Courses Total	**24**
Electives (select 2 from following)		**6**

CMP SCI 5732	Cryptography for Computer Security	
CMP SCI 5750	Cloud Computing	
MGMT 5600	Managing People in Organizations	
INFSYS 5890	Internship in Information Systems	
INFSYS 5899	Individual Research in Information Systems	
INFSYS 6818	Management of Software Testing	
INFSYS 6891	Seminar in Information Systems (Spl. Topics)	
INFSYS 6860	Data Integration	
INFSYS 6837	Information Systems Architecture	
Other electives upon approval of Information Systems and Technology dept. chair		
	Total Credit Hours	**30**

5. Free elective credits
Total free elective credits: **none**

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:
Both emphasis areas have a Capstone Course (3 credit hours) that provides application-oriented exposure to students. It is also possible that the capstone courses will be cross-listed so that students with technical and management backgrounds work together in real-life settings to solve security issues as is common in practice. Students will work with area organizations and take part in various aspects of the security life-cycle. In addition, students with Computer Science emphasis have the option of pursuing a 3-credit hour master's thesis if they desire to pursue research in cybersecurity.

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.

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 allowing for flexibility to incorporate the rapid changes within the field of cybersecurity. As explained earlier, the curriculum was designed to be in line with Knowledge Unit requirements set forth by the NSA and DHS for CAE designations. The program also maps to the NICE-CWF. The rigor of the CAE-CDE designation process gives us confidence that the program will address student and industry needs.

Course Sequences

Courses listed in the Program Structure are shown in sequence. Electives listed are either without any prerequisite courses or have their prerequisites met with the required courses. We expect full-time students to complete the programs in 2 years or less.

Descriptions of Courses

All of the courses in the program are already existing or have gone through the campus approval process and course descriptions are available through UMSL Bulletin (http://bulletin.umsl.edu). Newly approved courses appear in Appendix A.

5.D. Program Goals and Assessment

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, skills acquired and ability to perform tasks relevant to cybersecurity professionals (in an applied sense) will be assessed through hands-on labs throughout the cybersecurity courses. The capstone course will provide the opportunity to assess full degree level learning outcomes per the CAE-CDE knowledge units and learning outcomes associated with each unit[12]. 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.

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

Not Applicable.

Performance on national and/or local assessments.

Not Applicable.

[12] Please see https://cyberedwiki.org/index.php?title=Knowledge_Unit for a description of Knowledge Units used in the CAE-CDE evaluation process and for a list of different categories of knowledge units.

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	21	39	45	44

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. St. Louis is in the Top 15 metropolitan areas with the highest level of employment in the "Information Security Analyst" position. The US Bureau of Labor Statistic suggests a 28% growth in this category between 2016-26. As of Nov 2018, Cyberseek.org 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 5300 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 professionals. Taken together, these factors offer strong support for post-graduation success.

5.E. Student Preparation

The M.S. Cybersecurity with Information Systems and Technology Emphasis will require students to possess undergraduate level knowledge in business statistics and at least one semester worth of application development background. The Computer Science Emphasis requires students to possess three semesters worth of programming background; knowledge of computer organization, architecture, or assembly level programming; familiarity with Unix/Linux/OSX and command line scripting; and math foundations equivalent to an undergraduate degree in Computer Science or Cybersecurity. Students without the requisite background can complete coursework at UMSL to fulfill the entry requirements.

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 4.

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

We expect approximately 75% of core cybersecurity credit hours to be taught by full-time faculty with terminal degrees. However, a strong component of our proposed program is courses taught by experienced cybersecurity professionals active in the field. Currently, these professionals teach courses as adjunct faculty but possess highly respected industry certifications such as Certified Information Systems Security Professional (CISSP). All other normal Computer Science and Information Systems and Technology department wise 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 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.

5.G. Alumni and Employer Survey

Congruent with our program goals of providing curriculum that remains relevant in the rapidly changing field of cybersecurity, we will use the following approaches for assessing alumni and employer satisfaction with the help of our Cybersecurity Advisory Board. First, graduating students 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 a) the curriculum itself, b) quality of instructors, and c) supporting resources such as lab infrastructures and career placement help.

Second, leveraging our strong existing relationships with business and government organizations employing our graduates we will conduct brief annual surveys from employers on both the quality of our graduates as well as the changing needs of the employers in terms of skill-sets. We expect many of the regional employers 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. UMSL's current designation is due for renewal in year 2021. In addition, UMSL also holds a Focus Area Designation in Security Policy Development and Compliance. The new program will undergo evaluation to be included in the current and future cycles of the CAE-CDE Designation. The Computer Science Emphasis will undergo CAE evaluation within the Technical Core and the Information Systems and Technology emphasis will undergo evaluation within the Non-Technical Core knowledge unit requirements. If accepted by the NSA and DHS, the new program will then also be due for renewal in 2021. The CAE-CDE designation requires renewal every 5 years.

Appendix A: New Courses

INFSYS 6820 Systems and IT Infrastructure *[Course has been approved on campus]*

Bulletin Description

Prerequisites: Graduate standing.

Establishes the critical role of Linux and Windows server environments in contemporary Information Technology (IT) infrastructure management. Students understand both the technical and management aspects of server infrastructure. Technical aspects include installation, operation, maintenance, virtualization, and systems security. Management aspects include server lifecycles and management of server environments at scale using automation and configuration management tools within the context of application development, security operations, and IT operations. Credit cannot be granted for both INFSYS 3820 and INFSYS 6820.

Credit Hours: Min 3, Max 3

INFSYS 6888 Capstone in Information Security *[Course has been approved on campus]*

Bulletin Description

Prerequisites: INFSYS 6828 and one of either INFSYS 6858 or CMP SCI 5782
Provides students an opportunity to participate in the full information security lifecycle in an applied setting using a project-based approach. Students from technical and non-technical backgrounds work together in teams. Major tasks may include creating an information security management plan, conducting risk assessments, implementing technical and administrative controls to mitigate information security risks, and managing security operations with a focus on incident detection and response. Students may work on projects through an actual organization and demonstrate application of knowledge gained through all prior courses in the degree program. This course must be taken the last semester prior to graduation.

Credit Hours: Min 3, Max 3

CMP SCI 5888 Cybersecurity Capstone *[Course has been approved on campus]*

Bulletin Description

Prerequisites: INFSYS 6828 and one of either INFSYS 6858 or CMP SCI 5782

Provides students an opportunity to participate in the full cybersecurity lifecycle in an applied setting using a project-based approach. Students from technical and non-technical backgrounds work together in teams. Major tasks may include creating an information security management plan, conducting risk assessments, implementing technical and administrative controls to mitigate information security risks, and managing security operations with a focus on incident detection and response. Students may work on projects through an actual organization and demonstrate application of knowledge gained through all prior courses in the degree program. This course must be taken the last semester prior to graduation.

Credit Hours: Min 3, Max 3

Appendix B: 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

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 by 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 is located in Room 204 Express Scripts Hall. It is a state-of-the-art facility capable of holding 40 students. It features fully reconfigurable furniture to facilitate student collaboration. It has three 60" plasma screens for projecting and also provides a dedicated corner for student exercises for computer forensics and other hands-on activities such as monitoring network traffic. The room is equipped with a dedicated laptop cart with machines pre-configured with software including WireShark and Oracle VirtualBox for lab exercises. The lab also hosts its own 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 of their own choosing. Faculty and students have access to scalable compute resources and read-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 along with smaller vendors of analytics and security products. UMSL is part of the Microsoft DreamSpark Premium initiative. Students have 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 access to unrestricted cloud accounts (IBM's Bluemix® PaaS offering) renewable yearly. UMSL's academic subscription with VMWare provides students access to full versions of VMWare's enterprise class virtualization products and hypervisors. In addition, UMSL has academic licenses for fast growing tools from an emerging security vendor called Rapid7. These tools include, Metasploit Pro® (one of the most widely used framework and supporting tools for Penetration Testing) and Nexpose Enterprise® (a widely used 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 C: Support Letters

UNISYS | Securing Your Tomorrow™

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,

Mark Stanley
IBM Executive
Sales & Distribution

ST. CHARLES COUNTY
INFORMATION SYSTEMS

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 Commerce[1]. 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,

S Huang

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

OPEN – AS&RED – 2-39 April 11, 2019

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,

Sheila Burkett
CEO, Spry Digital, LLC

2710 Lafayette | St. Louis, MO 63104 | 314/514.5577 | www.sprydigital.com | holler@sprydigital.com

TDK technologies

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,

Kristin Tucker

Kristin Tucker
Managing Principal

16253 Swingley Ridge Road | Suite 300 | Chesterfield, MO 63017 | 636.778.1404

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

Appendix D: Financial Projections Spreadsheet

	FY20	FY21	FY22	FY23	FY24	FY25	FY26	FY27
Enrollment Projections								
Head Count Students - *new incoming*	24	59	81	88	89	89	89	89
Head Count Students - *transfers within campus*	8	16	19	17	15	15	15	15
Student Credit Hours	432	1013	1350	1418	1404	1404	1404	1404
Tuition Rate/Credit Hour	$476.50	$486.03	$495.75	$505.67	$515.78	$526.09	$536.62	$547.35
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)	$117.40	$119.75	$122.14	$124.59	$127.08	$129.62	$132.21	$134.86
Tuition Discount Rate (%)	19%	19%	19%	19%	19%	19%	19%	19%
Revenue Projections	********** CALCULATED CELLS **********							
Tuition	$205,848	$492,105	$669,263	$716,781	$724,154	$738,637	$753,409	$768,478
Supplemental & Other Fees (A&S Fees)	$2,134	$5,102	$6,938	$7,431	$7,507	$7,658	$7,811	$7,967
Supplemental & Other Fees (CoBA Fees)	$26,626	$63,654	$86,569	$92,715	$93,669	$95,542	$97,453	$99,402
Scholarship Allowances	-$44,576	-$106,564	-$144,926	-$155,216	-$156,813	-$159,949	-$163,148	-$166,411
Net Tuition and Fees	$190,033	$454,297	$617,844	$661,711	$668,517	$681,888	$695,525	$709,436
Other Income								
TOTAL PROGRAM REVENUE	**$190,033**	**$454,297**	**$617,844**	**$661,711**	**$668,517**	**$681,888**	**$695,525**	**$709,436**
Recurring State Support								
TOTAL REVENUE	**$190,033**	**$454,297**	**$617,844**	**$661,711**	**$668,517**	**$681,888**	**$695,525**	**$709,436**
Expenditure Projections								
Faculty Salaries	$0	$0	$0	$230,000	$234,600	$239,292	$244,078	$248,959
(with 2% salary increase)								
Total Salaries	$0	$0	$0	$230,000	$234,600	$239,292	$244,078	$248,959
Benefits	$0	$0	$0	$81,926	$83,565	$85,236	$86,941	$88,679
Subtotal Salaries and Benefits	$0	$0	$0	$311,926	$318,165	$324,528	$331,018	$337,639
Operating Expense								
Advertising Expenses	$30,000	$30,000	$30,000	$30,000	$30,000	$30,000	$30,000	$30,000
Subtotal Operating Expense	$30,000	$30,000	$30,000	$30,000	$30,000	$30,000	$30,000	$30,000
One-time Expenditures (Startup Costs)								
Additional Space Costs								

	FY20	FY21	FY22	FY23	FY24	FY25	FY26	FY27
Subtotal One-time Expense	$0	$0	$0	$0	$0	$0	$0	$0
TOTAL EXPENDITURES	$30,000	$30,000	$30,000	$341,926	$348,165	$354,528	$361,018	$367,639
DIRECT MARGIN	$160,033	$424,297	$587,844	$319,785	$320,353	$327,360	$334,507	$341,797
CUMULATIVE DIRECT MARGIN	$160,033	$584,330	$1,172,174	$1,491,959	$1,812,312	$2,139,672	$2,474,179	$2,815,976
Subtract: Revenue from Transfers within Campus	$47,508	$96,917	$117,390	$107,134	$96,421	$98,349	$100,316	$102,322
NET MARGIN TO THE CAMPUS	$112,525	$327,380	$470,454	$212,651	$223,932	$229,011	$234,191	$239,475
CUMULATIVE NET MARGIN TO THE CAMPUS	$112,525	$439,905	$910,359	$1,123,010	$1,346,942	$1,575,952	$1,810,143	$2,049,618
Campus Overhead Allocation	$51,408	$120,488	$160,650	$168,683	$167,076	$167,076	$167,076	$167,076
MARGIN AFTER CAMPUS OVERHEAD	$61,117	$206,893	$309,804	$43,968	$56,856	$61,935	$67,115	$72,399
CUMULATIVE MARGIN AFTER CAMPUS OVERHEAD	$61,117	$268,010	$577,813	$621,782	$678,638	$740,572	$807,687	$880,086

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 UMSL graduation data. See footnote 1 in Enrollment Projections Sheet.

Assumptions for Financial Calculations

Credit Hour Calculation: Full-time Graduate Course Load of 15 credit hours year * number of students enrolled each semester after taking into account graduation and attrition. Part-time load is taken as 10 credits per 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 47.5% credit hours were taken to be from A&S and 52.5% 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.

Additional faculty lines requested in fourth year if enrollment projections met.

Campus Overhead Allocation: Assumes $65/SCH for college overhead and $54/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.