

**BACHELOR OF SCIENCE IN CYBERSECURITY
A Recommendation**

1. **Division and Department:** Academic Affairs, School of Engineering and Computer Science, Department of Computer Science and Engineering.

2. **Introduction:** Oakland University proposes a new undergraduate degree program in Cybersecurity, specifically the Bachelor of Science in Cybersecurity within the Department of Computer Science and Engineering (CSE), in the School of Engineering and Computer Science (SECS).

A CSE committee composed by faculty experts in cybersecurity was formed to examine existing cybersecurity programs throughout the State of Michigan and the nation, understand labor market data, obtain information regarding the accreditation process (ABET), survey student interest, receive feedback from our community partners including the CSE advisory board, and compose a formal proposal for the Bachelor of Science in Cybersecurity program.

The need for cybersecurity professionals has been growing rapidly, faster than companies can hire—and that demand is expected to continue. In the U.S., there are about one million cybersecurity workers, but there were around 760,000 jobs yet to be filled as of October 2022 including more than 19,500 openings just in the State of Michigan, according to recent reports¹. In this proposed program, the students will practice their technical skills in a realistic cybersecurity setting. These hands-on experiences will help students to learn, and provide companies with more talent to fill open jobs.

The program will include a strong foundation in cybersecurity core concepts. A total of 30 credits in the core cybersecurity curriculum will cover Confidentiality, Integrity, Availability and Authentication (CIAA), and concentrate on data, software, component, network, and systems security, in addition to organizational, human, and societal security. In addition, 39 credits will be applied to deepening understanding through the study of Professional Subjects and six credits in Professional Electives. A further 12 credits in one of the following concentrations will be required: Software Security, AI in Cybersecurity, or Cyber Physical Systems Security. Lastly, 16 credits in Math and Science and 26 credits of university required general areas of study will be added to this curriculum as well as a Capstone project, for a total of 128 credits.

¹ <https://www.cybersack.org/hcatmap.html>

Need for the Bachelor of Science in Cybersecurity degree at Oakland University

Oakland University has already been selected by the National Security Agency as a Center of Academic Excellence and Information Assurance and Cyber Defense (CAE-IA/CD) education. Furthermore, a new center on cybersecurity is established based on funding from the Department of Energy to work closely with local industry to address their training and research needs in cybersecurity, to assist efforts to secure our infrastructure, protect the nation and the state from disinformation threat, and secure our digital assets, including the transition to industry 4.0. Thus, Oakland University is well-positioned to offer a degree in cybersecurity meeting these critical needs of the local community and beyond.

The cybersecurity industry already suffers from a long-standing shortage of cybersecurity professionals. While the occupational growth rate typically averages 8%, the rate for cybersecurity roles is over four times higher at 33%, according to Bureau of Labor Statistics data². A survey by the World Economic Forum found that 59% of businesses would find it difficult to respond to a cybersecurity incident due to the shortage of skills. Data from 2022 showed that the problem is getting worse, with the workforce gap increasing by 26.2% compared to 2021³.

Unlike other existing programs in the state of Michigan, the interdisciplinary nature of the proposed program aims to serve automotive industry, manufacturing, IT, financial, healthcare, law enforcement and defense organizations through its specialized concentrations Software Security, AI in Cybersecurity, or Cyber Physical Systems Security.

3. Previous Board Action: None.

4. Budget Implications: The primary source of funding new resources will be undergraduate tuition, and the program is expected to generate net revenues. The School of Engineering and Computer Science is currently working with University Advancement to identify community donors for additional program funding. Tuition revenue will reach a steady state in year four. Salary expenses include full-time and part-time faculty, and graduate assistants. Operating expenses include supplies and services, library, and marketing.

5. Educational Implications: The proposed program will develop a complete set of curricula in cybersecurity that significantly improves the cybersecurity teaching and

² <https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm>

³ https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

research capabilities at Oakland University. The newly developed courses will be available and beneficial to students majoring in Computer Science (CS) and Information Technology (IT) thus enhancing the existing BS programs offered by the School of Engineering and Computer Science.

6. Personnel Implications: The program would require two (2) new Assistant Professors and four (4) new Teaching Assistants (TAs) over the period of the first five years; however, these resources will be needed gradually, and they are proportional with the growth of the program. One Assistant Professor is expected to be hired in the second year of the program and a second will be hired in the fourth year.

7. University Reviews/Approvals: This proposal for Bachelor of Science in Cybersecurity degree program was reviewed and approved by the School of Engineering and Computer Science Assembly, the University Committee on Undergraduate Instruction (UCUI), the OU Senate, and the Executive Vice President for Academic Affairs and Provost.

8. Recommendation:

WHEREAS, the Bachelor of Science in Cybersecurity degree program is consistent with the objectives contained in Oakland University's Institutional Priorities; and

WHEREAS, the Bachelor of Science in Cybersecurity degree program will build on the academic and research strengths in the Department of Computer Science and Engineering and provide new educational and community engagement opportunities in the field of cybersecurity; now, therefore, be it

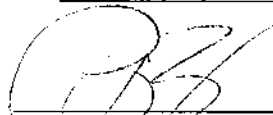
RESOLVED, that the Board of Trustees authorizes the School of Engineering and Computer Science to offer a Bachelor of Science in Cybersecurity degree program; and, be it further

RESOLVED, that the Executive Vice President for Academic Affairs and Provost will complete annual reviews of the Bachelor of Science in Cybersecurity degree program to evaluate academic quality and fiscal viability to determine whether the program should continue.

9. Attachments:

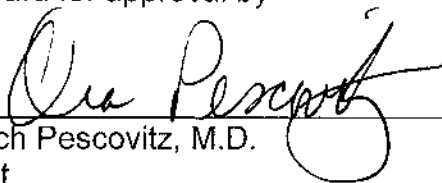
- A. Proposal for the Bachelor of Science in Cybersecurity degree program.
- B. Proforma budget for the Bachelor of Science in Cybersecurity degree program.

Submitted to the President
on 2/1, 2023 by



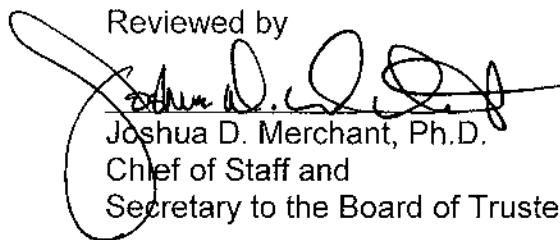
Britt Rios-Ellis, M.S., Ph.D.
Executive Vice President for
Academic Affairs and Provost

Recommended on 2/1, 2023
to the Board for approval by



Ora Hirsch Pescovitz, M.D.
President

Reviewed by



Joshua D. Merchant, Ph.D.
Chief of Staff and
Secretary to the Board of Trustees

Program Degree: Bachelor of Science in Cybersecurity

Requested Program Implementation Term: Winter 2023/Fall 2023

School or College Governance

Date Submitted: March 13, 2022

Date Approved: April 22, 2022

Department of Computer Science and Engineering

Date Submitted: January 13, 2022

Date Approved: February 18, 2022

Undergraduate Committee on Instruction

Date Submitted: February 19, 2022

Date Approved: March 06, 2022

Dean School or College

Date Submitted: April 22, 2022

Date Approved: April 22, 2022

University Committee on Undergraduate Instruction

Date Submitted: September 09, 2022

Date Approved: October 05, 2022

University Governance

Date Submitted

Date Approved

Senate

Date Submitted

Date Approved

Board of Trustees

Date Submitted

Date Approved

Presidents Council

Date Submitted

Date Approved

ABSTRACT

In recent years, cybersecurity has been a topic on the cusp of the business community, and as a growing field the time has come for it to be recognized as a specialty in its own right. The Bureau of Labor and Statistics (BLS) is in alignment with this need, predicting that cybersecurity jobs will grow at 31% per year through 2029, over seven times the national average job growth rate of 4% per annum.¹ In recent years, cybersecurity has been a topic on the cusp of the business community, and as a growing field the time has come for it to be recognized as a specialty in its own right. According to current estimates, currently around 715,000 jobs yet to be filled in area of cybersecurity and the number of openings is expected to reach 3.5 million by 2025 in US alone. Another analysis, by Burning Glass, of national job postings predicts the following fields will experience unprecedented growth over the next 5 years: application development security (164%), cloud security (115%), risk management (60%), threat intelligence (41%), incident response (37%), compliance and controls (36%), data privacy and security (36%), access management (32%), security strategy and governance (20%), and health information security (20%). According to a market survey commissioned by the university, demand for Cybersecurity degrees grew 18.6% between 2016 and 2017 alone. Median salaries for Cybersecurity graduates in Michigan are over \$90,000 per year, more than \$30,000 per year over the average Michigan income.

Although the traditional jobs in the cybersecurity domain are highly technical, the demand is not restricted to the IT sector. For instance, jobs requesting health information and security skills include not just cybersecurity engineers, but also healthcare administrators and insurance sales agents. Likewise, jobs in the legal field also require expertise in data privacy and security. This demand across different sectors creates hybrid roles that blend cybersecurity skills within existing responsibilities.

Students at Oakland University (OU) have expressed interest in a degree path in Cybersecurity, and it is important that OU rise to meet this need. Built upon a solid foundation in Computer Science, Mathematics, Electrical Engineering, Management of Information Systems and Criminal Justice, the proposed degree will take core concepts from each, along with the cornerstones of Cybersecurity: Confidentiality, Integrity, and Availability, and give industry what it demands: qualified professionals with the skills necessary to protect businesses, infrastructure and even governments.

¹<https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm>

Oakland University has a long history of innovation and a unique opportunity to create a degree that will serve as a benchmark for this rapidly growing industry. State of the art curricula, facilities and labs will assist students as they develop into professionals that, beginning in Fall 2023, will take the industry by storm.

Another analysis, by Burning Glass, of national job postings predicts the following fields will experience unprecedented growth over the next 5 years: application development security (164%), cloud security (115%), risk management (60%), threat intelligence (41%), incident response (37%), compliance and controls (36%), data privacy and security (36%), access management (32%), security strategy and governance (20%), and health information security (20%).² According to a market survey commissioned by the university, demand for Cybersecurity degrees grew 18.6% between 2016 and 2017 alone. Median salaries for Cybersecurity graduates in Michigan are over \$90,000 per year, more than \$30,000 per year over the average Michigan income.

Although the traditional jobs in the cybersecurity domain are highly technical, the demand is not restricted to the IT sector. For instance, jobs requesting health information and security skills include not just cybersecurity engineers, but also healthcare administrators and insurance sales agents. Likewise, jobs in the legal field also require expertise in data privacy and security. This demand across different sectors creates hybrid roles that blend cybersecurity skills within existing responsibilities.

Students at Oakland University (OU) have expressed interest in a degree path in Cybersecurity, and it is important that OU rise to meet this need. Built upon a solid foundation in Computer Science, Mathematics, Electrical Engineering, Management of Information Systems and Criminal Justice, the proposed degree will take core concepts from each, along with the cornerstones of Cybersecurity: Confidentiality, Integrity, and Availability, and give industry what it demands: qualified professionals with the skills necessary to protect businesses, infrastructure and even governments.

Oakland University has a long history of innovation and a unique opportunity to create a degree that will serve as a benchmark for this rapidly growing industry. State of the art curricula, facilities and labs will assist students as they develop into professionals that, beginning in Fall 2023, will take the industry by storm.

² <https://www.burning-glass.com/research-project/cybersecurity/>

Table of Contents

ABSTRACT	2
INTRODUCTION	5
RATIONALE	6
Program Need	6
How Program Will Promote the Role and Mission of the University and College/School	8
Program Goals	9
Comparison to Similar Programs (State/National)	9
ACADEMIC UNIT	10
How Program Supports Goals of the Unit	11
Staffing Needs	12
Faculty Qualifications	12
Impact on Current Programs	12
Classroom, laboratory and/or studio space	12
Equipment	13
PROGRAM PLAN	13
Admissions Requirements	13
Degree Requirements	14
Overview of Curriculum	15
Course requirements (minimum of 128 total credits)	17
Description of New classes	20
Support of Other Departments and Academic Units	21
Source of Students	21
Recruiting	21
Expected Enrollment	22
Academic Advising	24
NEEDS AND COSTS OF THE PROGRAM	25
New Resources Needed for the Program	25
Source of New Resource	25
Budget and Revenue from Program	25
Library Holdings	26
IMPLEMENTATION PLAN AND TIMELINE	32
PROGRAM DELIVERY METHOD	32

ASSESSMENT OF STUDENT LEARNING	32
EXPECTED CAREER OPTIONS FOR GRADUATES	32
EQUIPMENT AND SUPPLIES	33
APPENDICES	34
Appendix A – Faculty Profiles	34
Appendix B – Sample Plan of Study	35
Appendix C - Industry Letters of Support	36
Appendix D - Departmental Letters of Support	39
Appendix E - Pro Forma Budget	43

INTRODUCTION

A new program is under consideration by Oakland University's (OU) School of Engineering and Computer Science for a Bachelor of Science in Cybersecurity. The Cybersecurity BS will be offered by the Department of Computer Science and Engineering (CSE), with the assistance of the Mathematics, Electrical and Computer Engineering (ECE), Management of Information Systems (MIS), and Criminal Justice (CRJ) departments. This program is designed to satisfy not only ABET requirements, but also local and national industry needs and student learning perspectives.

The program will include a strong foundation in cybersecurity core concepts. A total of 30 semester hours in the core cybersecurity curriculum will cover Confidentiality, Integrity, Availability and Authentication (CIAA), and concentrate on data, software, component, network, and systems security, in addition to organizational, human, and societal security. In addition, 39 credit hours will be applied to deepening understanding through the study of Professional Subjects and 6 credits in Professional Electives. A further 12 hours in one of the following concentrations will be required: Software Security, AI in Cybersecurity, or CPS Security. Lastly, 16 credits in Math and Science in addition to the university required general areas of study will be added to this curriculum as well as a Capstone project, for a total of 128 semester hours.

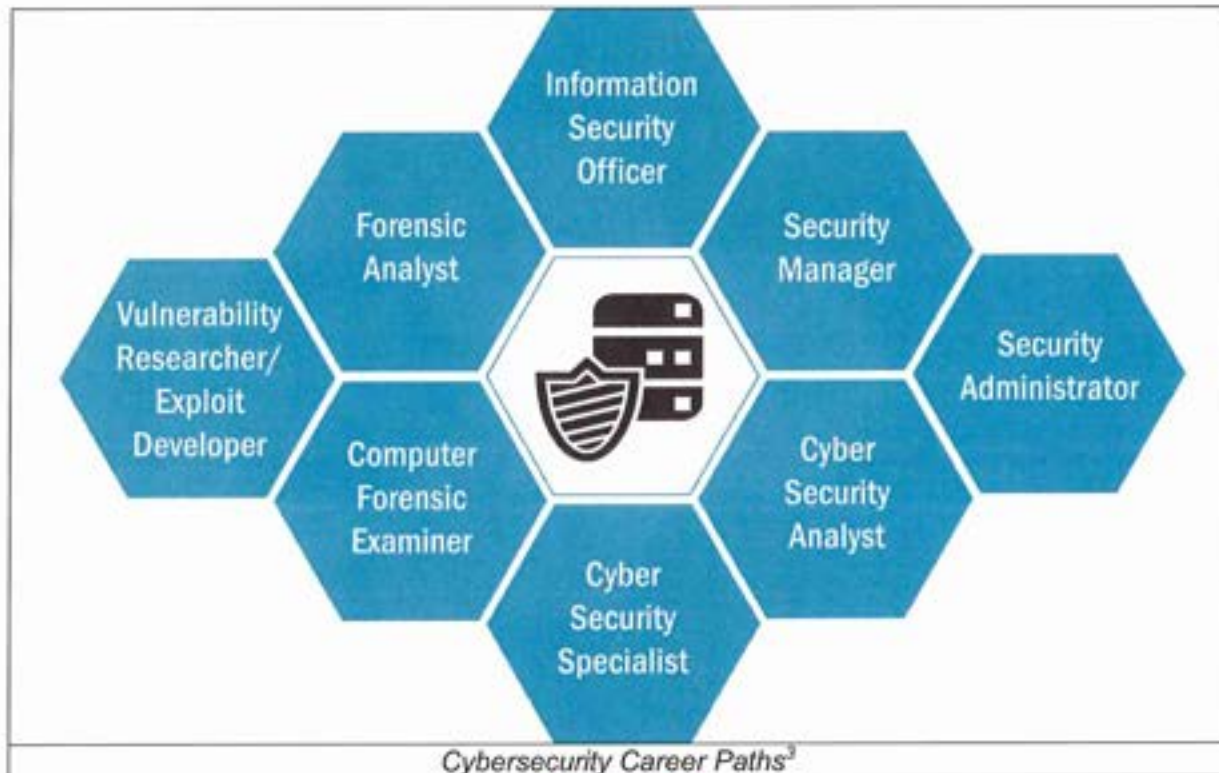
Oakland University has already been selected by the National Security Agency as a Center of Academic Excellence and Information Assurance and Cyber Defense (CAE-IA/CD) education, and many of the core concepts required for a Cybersecurity degree are already offered in courses of Bachelor of computer science and Bachelor of IT programs. Current offerings include classes in Software Security, Information Systems Security, and Cybercrime but these are in disparate programs, sometimes disparate colleges. The proposed degree would tie these existing classes together into one cohesive degree path, Cybersecurity. It is the overall goal of this program to use this diversity to provide domain specific background knowledge to understand the motivation behind cyberattacks and help mitigate them, and a technical foundation to be able to understand, adapt to, and create new solutions to match the ever-changing cyber threat surface.

Students will be prepared in a number of different areas for employment in the public and private sectors.

- Software Security
- AI in cybersecurity
- Cyber physical security and automotive security
- Network and digital forensics and investigation
- Penetration testing and system auditing
- Cybersecurity threat analysis and risk evaluation
- Laws, legislation, and policy related to Cybersecurity
- Cryptanalyst
- Computing and networking theory and practice
- System architecture and administration

By the end of study, the students will be able to analyze complex cybersecurity problems and apply security principles of cybersecurity to identify solutions and react to Cyberthreats. Additionally, they will have the ability to understand and implement advanced security practices to software, hardware and networks based on legal and ethical principles.

Growth in the industry for cybersecurity jobs is reaching unprecedented levels, with an estimated need for more than 16,000 new cybersecurity jobs in 2021, and projected growth of up to 33% per year in the coming decade according to the U.S. Bureau of Labor and Statistics (BLS). Most jobs in the current market require only bachelor's degrees, and typically less than 5 years of experience.



Employment post-graduation will be heavy in the financial, health care, and internet retail sectors, as well as a significant need by the US government. Typical job titles include Information Security Specialist, Information Systems Security Analyst, Information Technology Security Analyst (IT Security Analyst), Network Security Analyst, Security Analyst, and Systems Analyst. Median income for Cybersecurity positions in 2020 was just over \$100,000 per year. The proposed program would address one of the fastest growing industries in the nation.

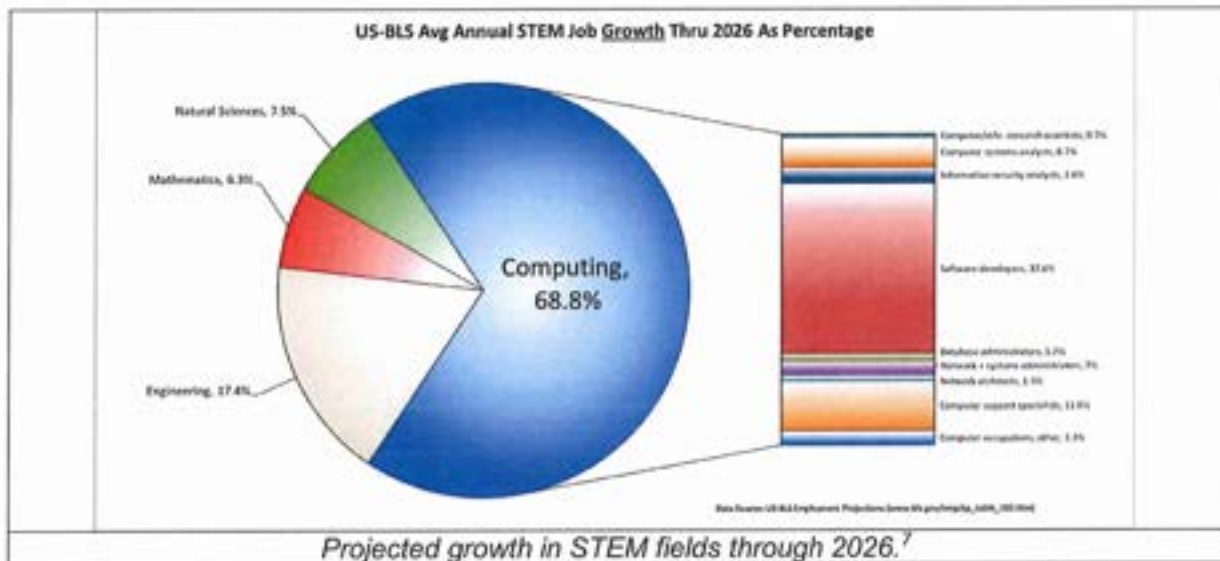
RATIONALE

Program Need

According to the Association for Computing Machinery, "The [Joint Task Force on Cybersecurity Education] defines cybersecurity as a 'computing-based discipline involving technology, people, information, and processes to enable assured operations. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management in the context of adversaries.'

³ <https://ponirevo.com/career-in-computer-science-with-cyber-%E2%80%8B%E2%80%8Bsecurity-and-forensics/>

According to some sources, 86% of businesses experienced some form of successful cyberattack in 2020, while 69% were attacked with ransomware⁵, leading to an increased demand for security analysts, yet in a recent study performed by 451 Research, 34.5% of security managers indicated prospective projects have implementation difficulties directly related to a lack of expertise in the field of Cybersecurity⁶. This translates into a desperate need in the coming decade for cybersecurity specialists.



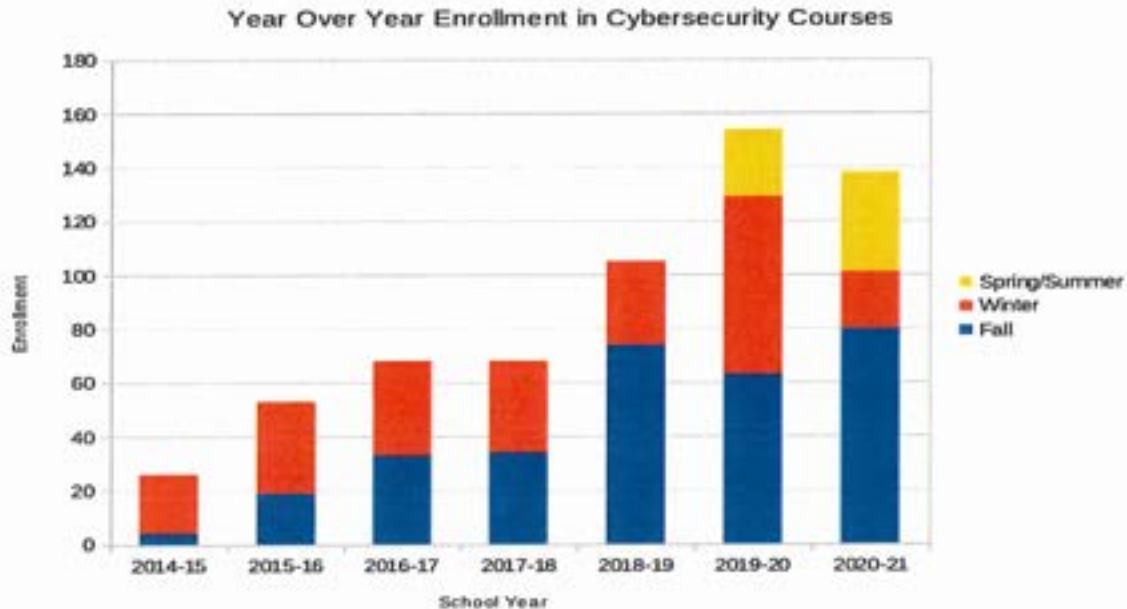
Michigan's major universities have so far largely overlooked this new trend, with no undergraduate cybersecurity degree path currently offered at the University of Michigan main campus, Michigan State, or Wayne State, leaving a noticeable and exploitable gap which may be used to establish Oakland University as a leader in the industry. Students have already expressed a significant desire to have a degree program in Cybersecurity, as evidenced by the interest in the current Cybersecurity concentration in the current Computer Science curriculum as seen in the table below.

⁴ <https://cybered.acm.org/>

⁵ <https://cyber-edge.com/cdr/>

⁶ <https://www.csoonline.com/article/2953258/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html>

⁷ https://calvin.edu/dotAsset/b884e77f-5ee5-4837-8a5f-29833cdacb18?_ga=2.4707637.701657674.1634314039-1500917279.1634314039



How Program Will Promote the Role and Mission of the University and College/School

Oakland University's message to incoming students is this: "Expand your education beyond four-walls. Solve complex problems in the real-world. Because it's the doers who shatter the mold⁸." The proposed degree program embodies this in its completeness: Ever growing knowledge. Complex problem solvers. Doers. These are the cornerstones of cybersecurity professionals.

On a website comparing CS degrees, they offer this advice: "Computer science majors study computer systems, design software, and solve problems using computing technologies. The discipline encompasses programming languages, computer networks, cybersecurity, database management, artificial intelligence, and machine learning. Every modern industry relies on computer science specialists to manage critical technology needs."⁹ Oakland does not offer a degree path for Cybersecurity. This must be rectified to bring Oakland's students to the next level in the business world.

The ultimate measure of the achievement of any educational institution is the success of its graduates and their contribution to society. A degree path in Cybersecurity will help Oakland to achieve this lofty goal by sending graduates to not only an emerging area but also an increasingly important one. As demonstrated, with the advent of more and more cyberattacks, soon the country, and even the world, will not be able to function without a workforce of qualified cybersecurity professionals. It is, therefore, imperative that Oakland bring its considerable resources to bear to produce graduates to populate this vital field.

⁸ <https://www.oakland.edu/futurestudents/>

⁹ <https://thebestschools.org/degrees/computer-science-degree/>

Program Goals

The goal of the proposed Cybersecurity degree program is to give students a solid foundation in the areas of Confidentiality, Integrity, and Availability, a classic concept in security known as the CIA triad. Specifically, students will learn these concepts as they apply to the areas of Software, Component, Connection, Organizational, Human, and Societal security. In addition, the proposed degree offers a strong background in Computer Science.

There is a significant and growing need in the local community for Cybersecurity professionals to cover the needs of the financial, automotive, and healthcare industries, all of which thrive in Michigan. Companies will look locally to serve this need. They will look to the institutions with the vision to establish programs ahead of the trend for candidates, and will keep going back to the programs which better prepare outgoing graduates.

The proposed degree will prepare students to accept entry level positions in the Cybersecurity field or for advanced degrees in Cybersecurity or Cybersecurity research. It will also help outgoing graduates thrive in the fast-paced, technical, and ever changing world of cybersecurity as it relates to the business sector. Lastly, the degree will help increase enrollment, raise the status of Oakland University as an educational leader, and bring the Computer Science Department in line with industry demands.

Comparison to Similar Programs (State/National)

<i>University</i>	<i>Program</i>	<i>Mode</i>
Baker college	B.Sc. in Information Technology and Security	In person and online both
Davenport University	B.Sc. in Cyberdefense	In person and online both
	B.Sc. in Digital Forensic	In person and online both
	B.Sc. in Network Management and Security	In person and online both
	B.Sc. in Information Assurance and Cyber Defense	Online
Eastern Michigan University	B.Sc+M.Sc in Cybersecurity	In person
Ferris State University	B.Sc. in Information Security and Intelligence	Online
Grand Valley State University	B.Sc. in Cybersecurity	In person
Michigan Technological University	B.Sc. in Cybersecurity	In person
Northern Michigan University	B.Sc. in Information Assurance and Cyber Defense	In person
University of Detroit Mercy	B.Sc. in Cybersecurity and Information Systems	In person
University of Michigan, Dearborn	B.Sc. in Cybersecurity and Information Assurance	In person
	B.Sc. in Digital Forensic	In person
Western Michigan University	B.Sc. in Cybersecurity	In person
<i>Cybersecurity Programs in the State of Michigan</i>		

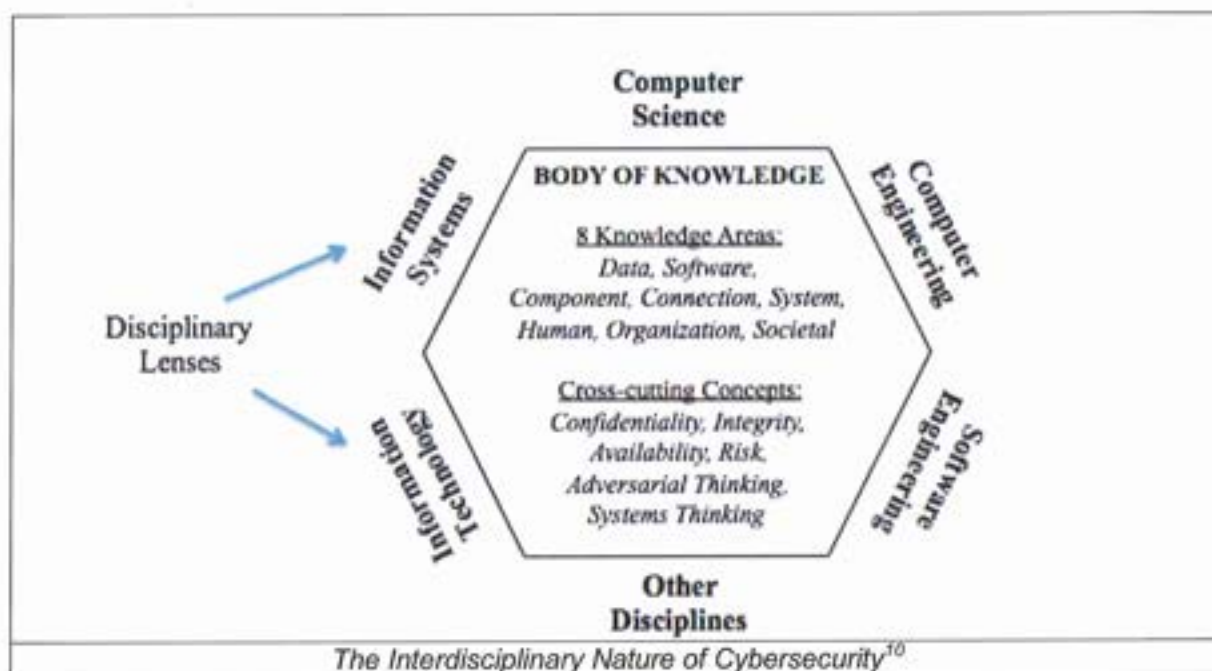
<i>State</i>	<i>University</i>	<i>Program</i>	<i>Mode</i>
Ohio	Cedarville University	B.Sc. in Cyber Operations	In person
	Kent State University	B.Sc. in Cybersecurity Engineering	In person
	Ohio State University	B.Sc. in Information and Computation Assurance	In person
	Franklin University	B.Sc. in Cybersecurity	Online
Wisconsin	University of Wisconsin, Stout	B.Sc. in Cyber Security	In person
Minnesota	Metropolitan State University	B.Sc. in Cybersecurity	In person
	Metropolitan State University	B.A. in Computer Forensics	In person
	Rasmussen University	B.Sc. in Cyber Security	Online
	St Cloud University	B.Sc. in Cybersecurity	In person
Illinois	Illinois State University	B.Sc. in Cybersecurity	In person
	Loyola University	B.Sc. in Cybersecurity	In person
	Northeastern University	B.Sc. in Cybersecurity	In person
	Roosevelt University	B.Sc. in Cyber and Information Security	In person
	University of Illinois, Springfie	B.Sc. in Information Systems Security	In person and online both
Indiana	Anderson University	B.Sc. in Cybersecurity	In person
	Indiana Tech	B.Sc. in Cybersecurity	In person
	Indiana University, Bloominto	B.Sc. in Cybersecurity and Global Policy	In person
	Indiana University Purdue Univ	B.Sc. in Cybersecurity	In person
	Indiana Wesleyan University	B.Sc. in Cybersecurity	Online
	Purdue University	B.Sc. in Cybersecurity	In person
	Purdue University, Northwest	B.Sc. in Computer Information Technology: Cyber	In person
	Taylor University	B.Sc. in Cybersecurity	In person
Indiana State Univeristy	B.Sc. in Cybercriminology and Security Studies	In person	
<i>Midwestern Cybersecurity Degrees</i>			

A comparison to similar programs shows a remarkable diversity of thought. Like other programs, the proposed degree would concentrate on cybersecurity fundamentals. However, unlike other programs at state level, the interdisciplinary nature of the proposed program aims to serve IT, financial, research, healthcare, law enforcement and defense organizations through its specialized concentrations.

The program will require one of three concentrations: Software Security, AI in Cybersecurity, and CPS Security. The need for a software security concentration is evident. CPS speaks directly to the automotive industry, which is so important to the area Oakland serves. AI in cybersecurity strives to meet national security challenges for government and private organizations, while multimedia forensics serves to fill needs at law enforcement agencies and social media. The core and electives provide graduates not only to those organizations but also the IT and financial sectors.

Four new classes will augment the existing offerings in these concentrations. In addition, two new core classes will be added, an introductory class and Digital Forensics in order to both satisfy ABET requirements and to lay a foundation for more advanced classes.

Nationally, major institutions are starting to offer Cybersecurity programs: Purdue, Texas A&M, Rutgers, and Syracuse, to name a few. As one of the fastest growing fields, Cybersecurity programs will only increase. It is past time to address this opportunity in Michigan. Students seeking degrees in Cybersecurity will flock to the few institutions that offer them.



ACADEMIC UNIT

How Program Supports Goals of the Unit

The BS in Cybersecurity Program will:

- Produce competent Bachelor of Science (BS) students to meet the current and futuristic global and national cybersecurity challenges. These students will significantly improve the reputation of Oakland University by exemplifying their technical skills, leadership, and professionalism.
- Develop an innovative program that is marketable to governmental and private industry agencies. Automotive, healthcare, defense, and financial-related organizations are in dire need of a skillful cybersecurity workforce.
- Attract qualified faculty with cyber-security specialties.
- Increase enrollment to undergraduate students with career goals in cybersecurity.
- Meet the staffing needs of the industry.

This program will require experienced faculty with expertise in information and network security, computer programming, and software engineering. These faculty members need experience teaching, evaluating students' learning, supervising student research, and grading students' work. Current faculty with cybersecurity backgrounds will direct and facilitate development.

¹⁰ https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf

Staffing Needs

The program would require two (2) new Assistant Professors and four (4) new Teaching Assistants (TAs) over the period of the first 5 years, however these resources will be acquired gradually. One Assistant Professor will be hired in the 2nd year of the program and a second will be hired in the 4th year. The newly hired faculty members will eventually cover the seven new classes in this proposal and additional sections of these existing courses: CSI 1420, CSI 2300, CSI 2440, CSI 2470, and CSI 3660. Faculty in load will be required in the first and second years to assist with the new class load until the new positions are filled.

One Ph.D. graduate assistant in the first year of the program will assist in additional sections of the lower-level classes, e.g., CSI 1420 and CSI 2300. Two TAs will be needed in the 2nd year for new sections of CSI 1420, CSI 2300, CSI 2440, CSI 2470. In 3rd year, three TAs will be required, and in years 4 and 5, the services of four (4) graduate students will be needed to share the TA load as more cybersecurity classes are offered.

For details see Appendix E.

Faculty Qualifications

The Department of Computer Science and Engineering currently employs several experienced academic professionals who have the capability of teaching students, evaluating students' learning, monitoring students' study progress, and directing and facilitating websites for courses. The qualified Department of Computer Science and Engineering faculty include Dr. Mehdi Bagherzadeh, Dr. Jingshu Chen, Dr. Debatosh Debnath, Dr. Huirong Fu, Dr. Marouane Kessentini, Dr. Dae-Kyoo Kim, Dr. Anyi Liu, Dr. Lunjin Lu, Dr. Tianle Ma, Dr. Khalid Mahmood Malik, Dr. Hua Ming, Dr. Md Atiqul Mollah, Dr. Guangzhi Qu, Dr. Sunny Raj, Dr. Julian Rushi, Dr. Amartya Sen, Dr. Ishwar Sethi, Dr. Mohammad-Reza Siadat, Dr. Gautam Singh, Dr. Steven Wilson, Dr. Lanyu Xu, and Dr. Douglas Zytko.

For a list of faculty profiles, see Appendix A.

Impact on Current Programs

The BS in Cybersecurity Program will bring tremendous impact to the current degree programs at Oakland University as follows:

- The proposed program will significantly increase the enrollment of students who would like to choose cybersecurity as their future career.
- The proposed program will develop a complete set of curricula of cybersecurity that significantly improves the cybersecurity teaching and research capabilities at Oakland University (OU). The newly developed courses will be available and beneficial to students majoring in Computer Science (CS) and Information Technology (IT), Electrical and Computer Engineering (ECE) thus enhancing the existing BS programs offered by the School of Engineering and Computer Science.
- The proposed program will further strengthen the pipeline that leads to the Master of Science in Cyber Security (MSC) at OU. The curricula of the proposed program can be cross-listed and shared with other relevant graduate programs.
- The proposed program will benefit a broader range of degree and certificate programs in other departments and schools, which would like to educate their students with cybersecurity concepts, principles, paradigms, technologies, and skills. Students in different majors will either register for courses or take certificate programs offered by this program.

Classroom, laboratory and/or studio space

Enrollment in the core and foundation classes will be combined into the current undergraduate courses of BS major in Computer Science and Information Technology. The bachelor students in cybersecurity will register for classes, which currently exist. The specialty classes will require two labs. The CSE department already has one lab in EC 554 which was made specifically with Cybersecurity classes in mind. It features lab machines, carefully separated from internal and external networks, designed to help students get hands-on experience with diverse topics from the perspective of defenders AND attackers. The lab currently sees heavy use with CSI 4480, Information Security Practices, but is expected to be heavily leveraged for new Cybersecurity classes.

The second lab will also be developed which will be used to give lectures and facilitate hands-on labs for new proposed cybersecurity classes. This lab will include new machines and servers dedicated to cybersecurity instruction. See the Equipment and Supplies and Appendix E – Pro Forma Budget, for more discussion on the specific equipment requested for the new lab.

Equipment

The program will require computer servers, desktop PCs, equipment, and materials and supplies to develop a second cybersecurity lab. The program will also utilize the online capabilities currently available at the Department of Computer Science and Engineering. See [Equipment and Supplies](#) for details.

PROGRAM PLAN

Admissions Requirements

Generally, freshman admission to Oakland University is based on a combination of criteria:

- A completed Oakland University [admission application](#). While an essay is optional, interested students may choose to include an essay for consideration.
- Cumulative high school grade point averages of 3.2 or above. Applicants with cumulative grade point averages below 3.2, but above 2.5, may be admitted after consideration of the quality of academic preparation. Scholarship awards are based on a student's academic record at the time of admission. However, students may submit updated transcripts and/or test scores for scholarship reconsideration until the March 1 scholarship priority deadline.
- SAT or ACT scores are no longer required for the incoming classes of 2022, for students with a minimum high school GPA of 2.5. You can find more information regarding our test-optional policy [here](#).
- Number and types of college preparatory courses
- Positive trend of grades

Additionally, students must meet their state graduation requirements. First-year college students interested in applying to Oakland University's [Honors College](#) should check their [additional admission criteria](#).

We strongly encourage students to follow a college preparatory curriculum that includes:

- Four years of English
- A minimum of three years of mathematics, including intermediate algebra
- A minimum of three years in social sciences
- A minimum of three years in biological/physical sciences
- A minimum of two years in a foreign language

Oakland University **does not** require letters of recommendation as part of the application for freshman admission.

Admission of individuals whose formal education has been interrupted for three or more years, and who would not normally meet other admission criteria, may be considered based on one or more of the following: sustained employment record; recommendations from employers, educators, and other professionals; and standardized test results. An interview with an Oakland University Admissions Adviser is required for such applicants to be considered for admission.¹¹

Program educational objectives

In the course of their careers, graduates of the BS in Cybersecurity program will:

- Work productively in the creation, maintenance, administration, and improvement of secure computing systems and associated infrastructure.
- Remain current in their profession through lifelong learning, including graduate school.
- Exhibit leadership and exercise their profession with the highest level of ethics, and social responsibility.

Degree Requirements

To earn a Bachelor of Science degree in Cybersecurity students must complete a minimum of 128 credits and meet the following requirements:

General education – Per University Requirements

Mathematics and sciences – 16 credits

Cybersecurity core – 26 credits

Required professional subjects – 39 credits

Professional track – 12 credits

Professional electives – 6 credits

Proposed total: 128 credits

To enroll in 3000- or higher-level courses and to become candidates for the degree of Bachelor of Science in Cybersecurity, students must gain a major standing. An application for major standing should be submitted prior to intended enrollment in 3000- or higher-level courses. Forms may be obtained from the SECS Undergraduate Advising Office or from the SECS website.

To gain major standing in Cybersecurity, students must:

A) have an average GPA of 2.0 in the following mathematics and science courses: MTH 1554, MTH 1555, MTH 2775, APM 2663, and STA 2226.

B) have an average GPA of 2.0 in the following cybersecurity core courses: CSI 1420, CSI 2300,

¹¹ <https://oakland.edu/futurestudents/apply/freshmen/>

CSI 2310, CSI 2460, CSI 2470, and CSI 2999.

C) have no more than two grades below C in the courses listed in A and B above.

D) have not attempted any course listed in A and B above more than three times. Students may petition to repeat a course a fourth time.

E) have not repeated more than three different courses listed in A and B. Courses in which a W (withdrawal) grade is recorded will not be counted.

Conditional major standing may be granted in the semester in which the student will complete requirements A and B above.

Satisfactory completion of the program requires an average grade of at least 2.0 within each group: mathematics and sciences, computer science core, and professional courses (including required professional subjects, professional electives, and professional track). Within professional courses at most two grades below C are permitted, at most two different courses may be repeated, and a total of three attempts per course is permitted.¹²

Overview of Curriculum

Table 1 illustrates the classes in the proposed degree program as they apply to the ABET requirements for the BS in Cybersecurity program. In all, eight knowledge intensives defined by ABET are covered: Data Security, Software Security, Component Security, Connection Security, Systems Security, Human Security, Organizational Security, and Societal Security are explored in depth over the curriculum. For a complete sample degree path see Appendix B. In the table, coverage is completed in three levels, Introductory material is covered, allowing students to easily gain basic knowledge without overburdening. Main material covers the bulk of knowledge required by ABET. Review topics may or may not be rehashed in later classes, in alignment with ABET requirements of those classes.

The Bachelor of Cybersecurity degree provides students the opportunity to gain cutting-edge cybersecurity knowledge and skills with a solid theoretical foundation as well as a good understanding of the social, ethical, legal, and policy aspects of cybersecurity. This bachelor program prepares students for a productive career in industry, lifelong learning, and for graduate study in Cybersecurity. The new degree is strategically designed to build on the strengths of existing computing programs on campus and produce well-rounded students with a balance between strong theoretical foundations as well as practical and hands-on technical skills. The program also includes a strong professional component for the development of skills in technical communication, ethics, and teamwork. The program was designed to satisfy not only ABET requirements, but also local and national industry needs and student learning perspectives.

Students learn to design and develop trusted software systems by adopting best practices and techniques in software development, manage and protect valuable computing infrastructure and data assets in an enterprise environment, and develop next-generation cyber skills to confront emerging cyber threats. It will also offer industry specific skills relevant to cybersecurity based on selected depth areas/concentration.

¹² http://catalog.oakland.edu/preview_program.php?catoid=49&poid=8398

Although most of the classes are offered by the department of computer science and engineering, however, due to interdisciplinary nature of cybersecurity, this program will involve collaboration from Departments of Electrical and Computer Engineering, (ECE), Mathematics, Management of Information Systems (MIS), and Criminal Justice (CRJ).

MATH 104 - Calculus I MATH 102 - Calculus II MATH 275 - Linear Algebra MPM 200 - Discrete Mathematics MPM 300 - Mathematics of Computing STA 320 - Applied Probability and Statistics CSC 140 - Intro to C Programming and Shell CSC 200 - Object-Oriented Computing CSC 230 - Data Structures CSC 240 - Computer Systems CSC 240 - Fundamentals of Cybersecurity CSC 245 - Introduction to Computer Networks CSC 250 - Supplement Project CSC 305 - Software Engineering and Practice CSC 330 - Operating Systems CSC 340 - Database Design and Implementation CSC 360 - System Administration CSC 400 - IT Risk Analysis and Security Controls Development CSC 400 - Cloud Computing CSC 405 - Operating & Digital Forensics CSC 400 - Information Security Fundamentals CSC 400 - Network Security CSC 470 - Software Security CSC 480 - Collaborating Applications: Senior Capstone Project CSC 420 - Software Verification and Testing CSC 480 - Systems Engineering CSC 480 - Mobile Security CSC 470 - Artificial Intelligence CSC 480 - AI For Cybersecurity and Privacy CSC 480 - Machine Learning CSC 470 - Fundamentals of Embedded System Design CSC 470 - Automotive Security CSC 480 - Industrial Control Security CSC 500 - Embedded Security											Introductory(), Main Objective(M), Milestone(S)
Introduction to Cybersecurity Computer Systems Applied Fundamentals of Cybersecurity Design, Analysis, Implementation, Test											400 Level/200
											Cryptanalysis Digital Forensics Data Security and Authentication Access Control Secure Communication Protocols Code Analysis Data Privacy Information Storage Security
											Fundamental Principles Design Implementation Analysis and Testing Deployment and Maintenance Documentation Ethics
											Component Design Component Testing Component Reverse Engineering
											Physical Media Physical Interfaces and Connectors Hardware Architecture Distributed Systems Architecture Network Architecture Network Implementations Network Services Network Defense
											System Thinking System Management System Access System Retirement System Testing Common System Architecture
											Identity Management Social Engineering Personal Compliance with Cybersecurity Rules/Policy/Ethical Norms Awareness and Understanding Social and Behavioral Privacy Personal Data Privacy and Security Mobile Security and Privacy
											Risk Management Security Governance & Policy Analytical Tools System Administration Cybersecurity Planning Business Continuity, Disaster Recovery, and Incident Management Security Program Management Personal Security Security Operations
											Cyberlaw Cyber Law Cyber Ethics Cyber Policy Privacy
											Math Computing

Table 1: Curriculum Matrix for the Proposed Degree

Course requirements (minimum of 128 total credits)

To earn a Bachelor of Science degree with a major in cybersecurity students must complete a minimum of 128 credits and meet the following requirements:

General education

The General Education Requirements are composed of three parts: Foundations, Explorations, and Integration. In addition, U.S. Diversity requirements must also be met. For details, refer to the General Education section of the catalog. In order to satisfy both general education and other program requirements, in some of the general education areas students should select from the courses listed below.

Foundations:

- Writing Foundations (WRT 1060)
- Formal Reasoning (Satisfied by MTH 1554; see Mathematics and sciences)

Explorations: One course from each of the seven Explorations areas

- Arts
- Language and Culture
- Global Perspective
- Literature
- Natural Science and Technology (Satisfied by an approved science elective with lab; see Mathematics and Sciences)
- Social Science
- Western Civilization (Satisfied by PHL 1310; see additional major requirements)

Integration:

- Knowledge Applications (Satisfied by MTH 1555; see Mathematics and sciences)

U.S. Diversity:

- May be met by an approved course in the Explorations area.

Writing Intensive and Capstone:

- Capstone (Satisfied by CSI 4999; see Required professional subjects)
- Writing Intensive in the Major (Satisfied by CSI 4999; see Required professional subjects)
- Writing Intensive in General Education (may be met by an approved course in the Explorations area)

Additional Major Requirements:

All students must complete the following requirement.

- Professional Ethics: PHL 1310 - Introduction to Ethics in Science and Engineering

In order to graduate on-schedule without taking additional courses, it is highly recommended that students meet with SECS Undergraduate Academic Adviser concerning the selection of all of their general education courses.

Math and Statistics [16 credits]

- **APM 2663 - Discrete Mathematics (4)**
- **STA 2226 - Applied Probability and Statistics (4)**
- **MTH 1554 - Calculus I (4)**

- **MTH 1555 - Calculus II (4)**

Cybersecurity Core [22 credits]

- **CSI 1420 - Introduction to C Programming and Unix (4)**
- **CSI 2300 - Object-Oriented Computing (4)**
- **CSI 2440 - Computer Systems (4)**
- **CSI 2460 - Fundamentals of Cybersecurity (4)**
- **CSI 2470 - Introduction to Computer Networks (4)**
- **CSI 2999 - Sophomore Project (2)**

Required professional subjects [43 credits]

- **CSI 3370 - Software Engineering and Practice (4)**
- **CSI 3450 - Database Design and Implementation (4)**
- **CSI 3660 - System Administration (4)**
- **CSI 4240 - Cloud Computing (4)**
- **CSI 4470 - Cyber Laws & Digital Forensics (4)**
- **CSI 4480 - Information Security Practice (4)**
- **CSI 4600 - Network Security (4)**
- **CSI 4700 - Software Security (4)**
- **CSI 4999 - Senior Capstone Project (4)**
- **CRJ 3341 - Cybercrime (4)**
- **MIS 4180 - IS Risk Analysis and Security Controls Development (3)**

Professional Electives [6 credits]

One of the following 2000 level 2-credit courses:

- **CSI 2320 - C++ for Programmers (2)**
- **CSI 2330 - Immersive Python (2)**
- **CSI 2340 - Ruby for Web Developers (2)**
- **CSI 2350 - Programming in Visual C# for .NET Technology (2)**

And one 4-credit class from following choices (A-C):

- Any class in one of the depth areas not chosen as a primary specialty
- Courses at the 5000 level, with instructor approval.
- Any 3000 or 4000 level class in Engineering, Computer Science, or Mathematics not currently part of the Cybersecurity curriculum. Below are some suggested classes:

- **APM 2555 - Introduction to Differential Equations with Matrix Algebra (4)**
- **APM 3332 - Applied Matrix Theory (4)**
- **APM 4333 - Numerical Methods (4)**
- **APM 4334 - Applied Numerical Methods: Matrix Methods (4)**
- **APM 4347 - Mathematics of Cryptology (4)**
- **APM 4663 - Graph Theory and Combinatorial Mathematics (4)**

- **APM 4777 - Computer Algebra (4)**
- **CSI 2310 - Data Structures (4)**
- **CSI 3610 - Design and Analysis of Algorithms (4)**
- **CSI 4500 - Fundamentals of Operating Systems (4)**
- **ECE 3720 - Microprocessors (4)**
- **EGR 2400 - Introduction to Electrical and Computer Engineering (4)**
- **MOR 2442 - Elementary Models in Operations Research (4)**
- **MTH 2775 - Linear Algebra (4)**
- **MTH 3552 - Complex Variables (4)**
- **PHY 3250 - Biological Physics (4)**
- **PHY 3260 - Medical Physics (4)**
- **PHY 3310 - Optics (4)**
- **PHY 3660 - Vibrations and Waves (4)**
- **PHY 3710 - Foundations of Modern Physics (4)**

Depth areas/ Professional track [12 credits]

Select one of the following professional tracks

A) Software Security Track

- **CSI 4390 - Software Verification and Testing (4)**
- **CSI 4560 - Mobile Security (4)**
- **CSI 4880 - Reverse Engineering and malware analysis (4)**

B) AI in cybersecurity Track

- **CSI 4130 - Artificial Intelligence (4)**
- **CSI 4580 - AI for Cybersecurity and Privacy (4)**
- **CSI 4590 - Multimedia Forensics (4)**

C) Cyber Physical System (CPS) security Track

- **ECE 4731 - Fundamentals of Embedded System Design (4)**

Choose two from following three:

- **CSI 4520 - Industrial Control Security (4)**
- **CSI 4720 - Automotive Security (4)**
- **ECE 4780/5780 - Embedded Security (4)**

Description of New classes

1- CSI 2460 - Fundamentals of Cybersecurity (4)

This course covers topics relevant to cybersecurity across many disciplines. Discussions include the CIA triad, cryptography and privacy basics, hardware and software security risks,

guiding principles and cybersecurity ethics. In all, eight knowledge areas are explored: Data Security, Software Security, Component Security, Connection Security, Systems Security, Human Security, Organizational Security, and Societal Security.

Catalog Description: This course covers topics relevant to cybersecurity across many disciplines. Discussions include the CIA triad, cryptography and privacy basics, hardware, and software security risks, guiding principles and cybersecurity ethics. In all, eight knowledge areas are explored: Data Security, Software Security, Component Security, Connection Security, Systems Security, Human Security, Organizational Security, and Societal Security.

Prerequisite: none

Learning Objectives:

- Apply basic concepts such as Confidentiality, Availability, Non-repudiation, and Information integrity
- Apply cryptography and privacy basics, hardware and software security risks, guiding principles, and cybersecurity ethics
- Describe the secure communication protocols
- Apply the fundamentals of Data Security, Software Security, Component Security, Connection Security, Systems Security, Human Security, Organizational Security, and Societal Security
- Implement security defenses at system- and network- level

2- CSI 4520 - Industrial Control Security (4)

This course covers topics in cyber-physical systems security with focus on Industrial Control Systems. The goal is to expose students to fundamental security primitives specific to cyber-physical systems and to apply them to a broad range of current and future security challenges. Much of the course is taught with the focus on one instance of cyber-physical systems - (ICSs). Topics include introduction to cyber physical system (CPS), Machine to Machine connectivity protocols, Introduction to CPS Security and Privacy, basics of Control Systems, Introduction to Industrial Control Systems And Operations, Industrial Network Design and Architecture, Power Delivery Systems, Attack Models for CPS, Industrial Network Protocols, cyber-attacks on Industrial Control Systems and their analysis, Securing Industrial Control Systems, cryptographic solutions for securing the cyber physical systems, and privacy in Cyber-Physical Systems (e.g. smart grid)

Catalog Description: Topics in cyber-physical systems security with focus on Industrial Control Systems. Exposure to fundamental security primitives specific to cyber-physical systems (CPS). Topics include: Introduction to CPS, Communication and Threat Modeling, Industrial Network Design and Architecture, Power Delivery Systems, CPS Cryptography and Privacy (e.g. smart grid).

Prerequisite: CSI 4420 and Major Standing.

Learning Objectives:

- Describe and analyze Industrial control system (ICS) architectures from a security perspective

- Analyze and reverse engineer major ICS network communication protocols and ICS application code
- Describe and reverse engineer Human Machine Interaction applications
- Describe the anatomy and implementation of attack such as malware and defense techniques that apply to ICS
- Design and implement a defensive deception capability for ICS

3- CSI 4560 - Mobile Security (4)

This course provides a general overview of the security and privacy aspects of mobile computing. In particular, this course covers the challenges, vulnerabilities, threats, and possible countermeasures for mobile computing, edge/fog computing, IoT, and artificial intelligence. Possible topics include, but are not limited to, mobile vulnerabilities, mobile malware, smartphone security, secure mobile app development, data privacy, biometrics-, multi-factor-, and codependency-based authentication and vulnerabilities, mobile location privacy, authentication in mobile devices, and secure apps communication. In addition to the lectures and the most recent research papers, this course emphasizes "*learning by doing*", and requires students to conduct a series of labs and projects. Hence, the students will gain practical experience and enhance their understanding of the security and privacy of mobile computing.

Catalog Description: This course provides a general overview of the security and privacy aspects of mobile computing. Topics include, mobile vulnerabilities, mobile malware, smartphone security, secure mobile app development, data privacy, biometrics-, multi-factor-, and codependency-based authentication and vulnerabilities, mobile location privacy, authentication in mobile devices, and secure apps communication.

Prerequisites: Major standing and CSI 2470.

Learning Objectives:

- Understand the fundamentals of mobile security such as telecom protocols and vulnerabilities; mobile/IoT network security; security and privacy in edge computing; mobile application security; and location and activity privacy.
- Analyze security issues faced by mobile application developers, embedded system builders, and smart system designers.
- Understand common mobile application security vulnerabilities
- Define the security controls of multiple mobile operating systems
- Apply the principles of protection strategies and the best practices

4- CSI 4580 – AI for Cybersecurity and Privacy (4)

Study of AI and machine learning algorithms customized for cyber security problems such as intrusion detection, malware classification, or network analysis. Topics include fundamentals of common machine learning and deep learning algorithms, intelligent threat detection and analysis, user behavior analytics, machine learning in hacking, privacy-preserving machine learning, transparency in machine learning, fairness of machine learning, and automated cybersecurity systems. It will also cover adversarial machine learning and countermeasures through real world problems and datasets. Hands-on lab components will also be developed.

Catalog Description: Study of AI and machine learning algorithms customized for cyber security problems such as intrusion detection, malware classification, or network analysis. Topics include fundamentals of machine learning and deep learning, intelligent threat detection, user behavior analytics, machine learning in hacking, privacy-preserving machine learning, adversarial machine learning and countermeasures.

Prerequisites: CSI 4130 and Major standing.

Learning Objectives:

- Apply AI technologies including machine learning and natural language processing in an attempt to help in understanding their role in cyber security
- Describe basic concepts for statistical modeling, including principles for model selection for supervised and unsupervised learning tasks in the context of cybersecurity.
- Select the most appropriate models for various cybersecurity scenarios, such as malware classification, botnet detection, and intrusion detection.
- Detect and defend against adversarial attacks on machine learning models in cybersecurity settings at both training and test times
- Identify and understand means of navigating legal and ethical challenges that emerge from gathering data about human subjects and using it to build machine-learning models

5- CSI 4590 - Multimedia Forensics (4)

This course will introduce current state-of-the-art in digital multimedia (audio, video, images) forgery creation including generative adversarial attacks, its impacts on multimedia tampering, and digital multimedia tamper detection techniques using various statistical and AI techniques. It will also cover attacks on biometrics measures and countermeasures. Lastly, this course will also cover covert communication methods such as steganography and covert channel detection method steganalysis. Hands-on experience will be provided in various aspects of multimedia tampering and analysis and detection through the numerous assignments, labs, and projects.

Catalog Description: Introduction to current state-of-the-art digital multimedia (audio, video, images) forgery creation and digital multimedia tamper detection techniques using statistical and AI methodology. Biometric measures and countermeasures, Steganography and covert channel detection. Various aspects of multimedia tampering and analysis and detection will be explored through assignments, labs, and projects.

Prerequisites: CSI 4130 and Major standing.

Learning Objectives:

- Describe techniques of digital tampering and multimedia tamper detection
- Describe information hiding techniques such as digital watermarking, steganography, and fingerprinting
- To apply emerging information security tools to detect covert channels in the digital media
- Hands-on experience to design and develop tools for digital multimedia forensic analysis

- Hands-on experience to design and develop tools for covert communication detection: steganalysis

6- CSI 4720 - Automotive Security (4)

Study of key theoretical concepts that emphasize automotive cyber security, assessment of security flaws and threats in vehicles, quality, and risk management of vehicles, explore different types of cyber-attacks on vehicles from physical to remote, and measures needed to protect vehicles from cyber threats. Real-world case studies will be given as a term project. Hands-on lab components will also be developed.

Catalog Description: Study of key theoretical concepts that emphasize automotive cyber security, assessment of security flaws and threats in vehicles, quality, and risk management of vehicles. Explore different types of cyber-attacks on vehicles from physical to remote, and measures needed to protect vehicles from cyber threats. Real-world case studies will be given as a term project.

Prerequisites: Major standing and CSI 4420.

Learning Objectives:

- Describe various types of bus protocols, communications in vehicles, and In-vehicle infotainment system
- Apply knowledge of potential cybersecurity threats for automotive systems, threat modeling, and their identification in the automotive industry
- Apply knowledge of various methods of attacking vehicles including ECU hacking and the roles of software and firmware in the hacking process
- Describe the fundamentals of attacking connected/automated vehicles and understand the potential for attacks on automated vehicles
- Apply knowledge of penetration testing of automated vehicles and hardening of various vulnerabilities
- Designing various cryptographic and AI mechanisms to achieve confidentiality, integrity, and authentication in automated vehicles

7- CSI 4880 - Reverse Engineering and Malware Analysis (4)

Study of software and hardware reverse engineering and malware analysis. Topics include principles of reverse engineering, reverse engineering tools and techniques, sandboxing, simulation methods and instrumentation, anti-reverse engineering techniques, static malware analysis, dynamic analysis, threat analysis, and automated analysis.

Catalog Description: Study of software and hardware reverse engineering and malware analysis. Topics include principles of reverse engineering, reverse engineering tools and techniques, sandboxing, simulation methods and instrumentation, anti-reverse engineering techniques, static malware analysis, dynamic analysis, threat analysis, and automated analysis.

Prerequisites: CSI 3660 and Major standing.

Learning Objectives:

- Describe the fundamentals of the Assembly languages and program compilation
- Apply the fundamentals of the binary code and ELF/PE data representations
- Apply the fundamentals of disassembly and common disassembly algorithms
- Apply the fundamentals of static binary and dynamic execution analyses
- Recognize common malware behavior (e.g., control flow hijacking)
- Apply the fundamentals of anti-reverse engineering and obfuscation and overcome their common techniques
- Apply the fundamentals of return-oriented programming
- Apply the fundamentals of runtime memory forensics
- Recognize and identify behavioral detection signatures

8- ECE 4731 Fundamentals of Embedded System Design (4)

This course will discuss an introduction to embedded systems. Topics include microcontroller architecture, operating systems and kernels, instructions, firmware, and the study and development of embedded systems in C using a modern microcontroller (e.g., Microchip PIC32), with common embedded applications using analog inputs/outputs, sensor/actuator interfaces, digital signal processing/filtering, communication standards, PID feedback control, and brushless/stepper motor sizing and control. Students will complete a final project involving system specification, functional partitioning, trade-off analysis, component design, integration, and performance evaluation

Note: This course will be cross listed with the current ECE 5731 (which serves a similar purpose) and the course description and title will be updated to match the proposed ECE4731. No new resources are needed for this course.

Catalog Description: This course will discuss an introduction to embedded systems. Topics include microcontroller architecture, operating systems and kernels, instructions, firmware, and the development of embedded systems in C using a modern microcontroller in a variety of real-world applications. Students will complete a final project involving all aspects of embedded systems design.

Prerequisites: CSI 2440 and Major Standing.

Learning Objectives:

- Analyze combinational logic circuits and describe finite state machines
- Write, analyze, and debug embedded C code.
- Research and select appropriate sensors and actuators that meet design requirements
- Use analog and digital microcontroller I/O ports as peripheral interfaces
- Implement closed-loop feedback control software on a microcontroller
- Effectively use modern embedded systems development tools and equipment
- Work constructively with others to design, analyze, debug, and present an electromechanical system subject to specific constraints

9- ECE 4780/5780: Embedded Security (4)

This course covers fundamental topics in embedded cybersecurity in hardware, system-on-chips, printed circuit board design, embedded IP, microcontrollers, memories, and FPGAs.

Topics include attacks, vulnerabilities, and hardware countermeasures, including reverse engineering attacks, hardware trojans, fault injection, timing attacks, counterfeiting, instruction and logic level obfuscation, electromagnetic side-channel attacks as well as threat modeling and protections. Students will participate in hands-on learning in laboratory experiments.

Catalog Description: This course covers fundamental topics in embedded cybersecurity in hardware, system-on-chips, printed circuit board design, embedded IP, microcontrollers, memories, and FPGAs. Topics include attacks, vulnerabilities, and countermeasures in a variety of hardware scenarios, as well as threat modeling and protection strategies. Experiments in a lab setting round out the experience.

Prerequisites: CSI 2440 and Major Standing

Learning Objectives:

- Real-time security implementation using hardware approach
- Security challenges in IoT and automotive applications
- Timing of algorithms, power consumption analysis for detection
- Security Gateways and network security
- Modeling and testing of hardware-based security

Note: The Department of Electrical and Computer Engineering will provide the teaching resource for this course. No additional resources are requested.

Support of Other Departments and Academic Units

Support for the proposed degree from other departments at Oakland has been very good, with letters from the Department Chairs of Philosophy, Mathematics, and Criminology, and Management Information Systems, partners in the proposed degree, responding. For specific letters of support, please refer to [Appendix D](#).

Source of Students

Based on the study of national trends and related programs in Michigan and the surrounding states, it is expected that the program will attract many new students. Meanwhile, we anticipate that some students may transfer from CS, IT, CE, and EE majors. These are usually students with strong interest in Cybersecurity. The proposed new major would help retain these students by providing them with additional options. There are 13 related Bachelor's degrees in Michigan and 23 degrees in the surrounding states. Some students looking for a career in cybersecurity may transfer to other universities if Oakland University fails to offer this degree.

We also anticipate that this program will be of interest to students with more than one major.

For students who are not in the CS and IT or other majors (such as Computer Engineering or Electrical Engineering majors), they are likely to gravitate to the minor in Cybersecurity. Therefore, this program is expected to increase new enrollment as well as help retention by providing students with additional options on cybersecurity.

Recruiting

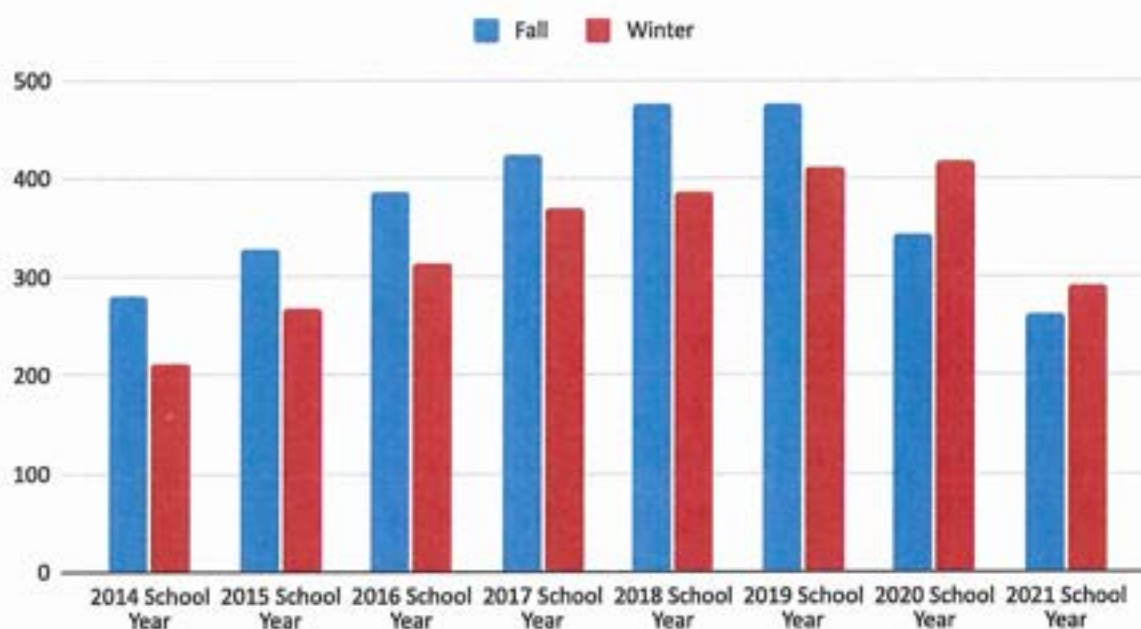
- Open House
- Radio
- Flyers
- Affiliating agencies
- Mailing lists
- Newspapers and journal advertisement
- SECS and CSE web pages

Expected Enrollment

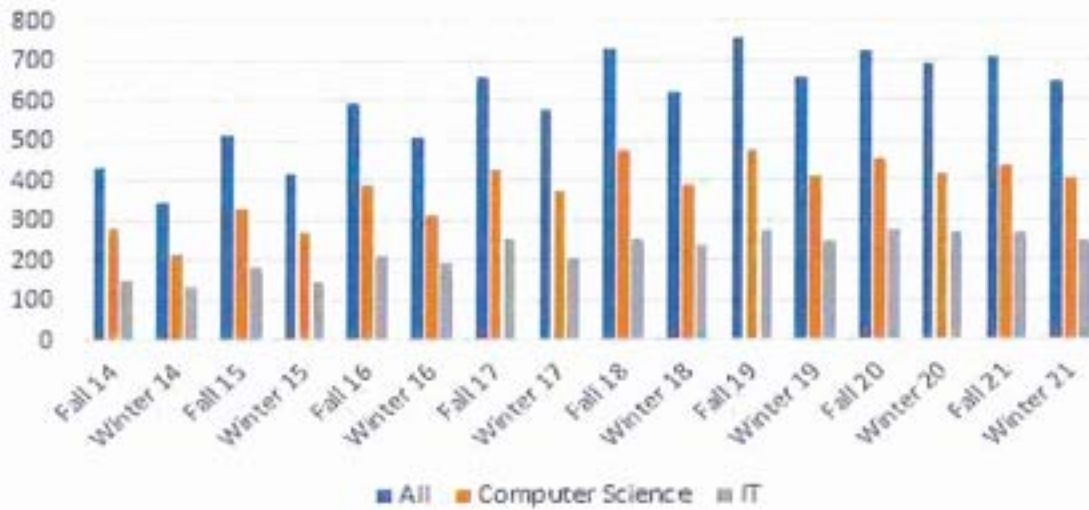
The undergraduate enrollment for both Computer Science and IT students, as shown in figures below, has been on a steady and healthy rise at the Department of Computer Science and Engineering, in the past seven years. Based on these numbers and their upward trends, it is expected that this program will enjoy a similar initial enrollment and continuous steady growth after its initial offering.

Enrollment numbers for the new program can be found in Appendix E. These numbers are cautiously optimistic and depend greatly on the program's start date and degree of promotion.

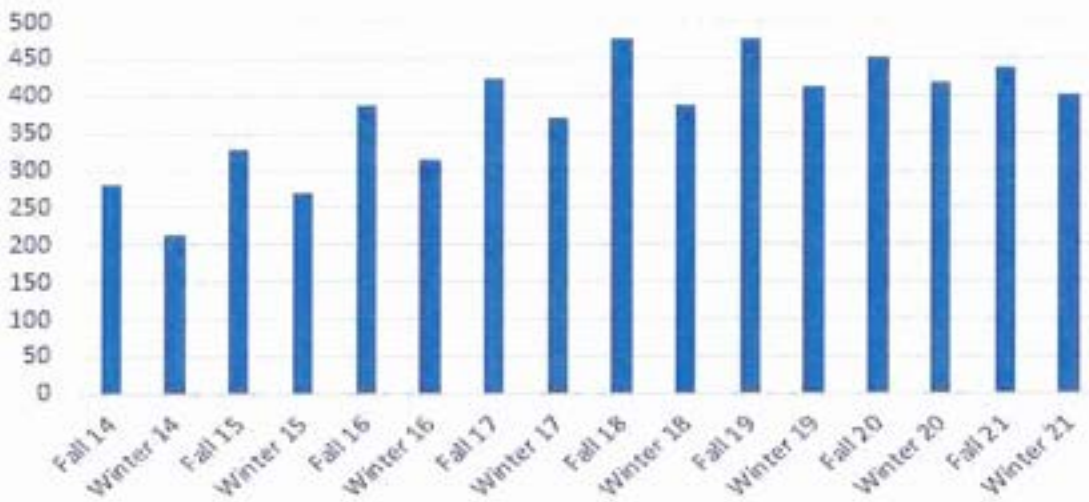
Computer Science Enrollment Year Over Year

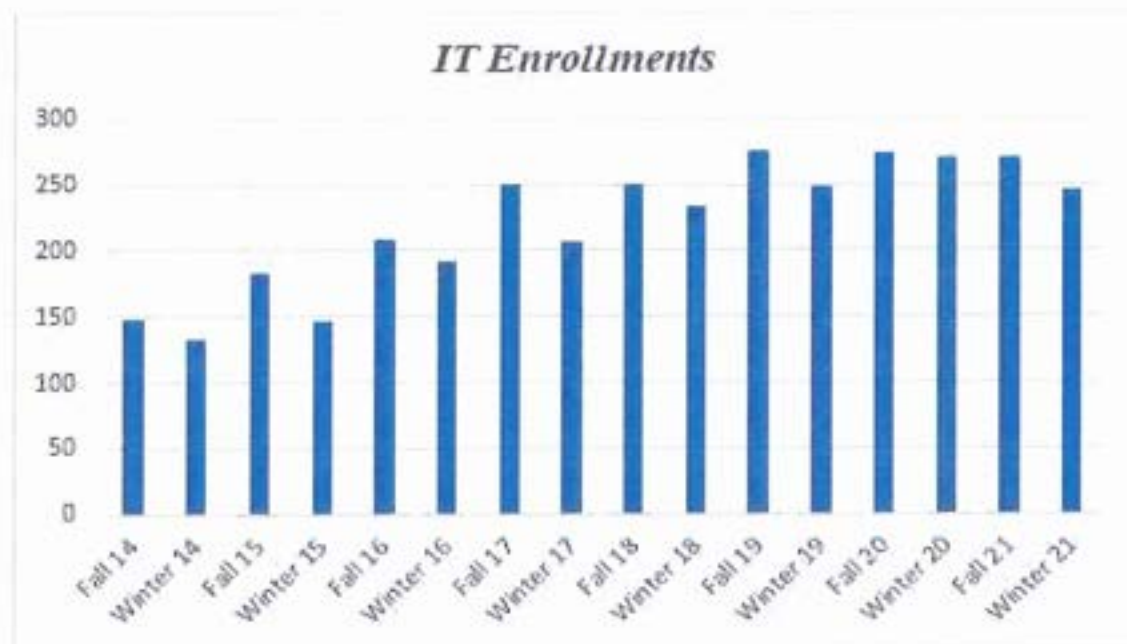


All, Computer Science, and IT Enrollments



Computer Science Enrollments





Academic Advising

Student retention is critical to ensure self-sustainability and high quality of the program. The program will strive to retain a high-quality student enrollment by implementing the following retention plan:

- Set up mentoring for new students to ensure they have clear understanding about the curriculum and milestones/requirements for the successful completion of the program.
- Early identification of students who are performing poorly in the program and make sure appropriate support is presented to these students.
- Ensure sufficient academic advisory to students by coordinating efforts of both the faculty and the academic advisors
- Hosting regular cybersecurity seminars; bring experts to campus to update students the state of the art in the area
- Encourage students to attend professional societies such as IEEE and ACM and participate in activities held by student-organized study groups such as CyberOU.
- Provide professional development opportunities and internships for students who are close to their graduation.
- Help potential employers who may be interested in the graduates of the program to know our program and graduates better by holding cybersecurity job fairs and workshops
- Help graduates to market themselves in their job placement by hosting their resume and homepage on the department's website

NEEDS AND COSTS OF THE PROGRAM

New Resources Needed for the Program

A proposed budget for new computer servers, desktop PCs, equipment, and materials and supplies, is discussed in [Equipment and Supplies](#).

Source of New Resource

The cost of the program initially will be covered by an increase in tuition revenue. In addition, scholarships and grants from the National Security Administration and National Science Foundation are expected.

Budget and Revenue from Program

Tuition revenue projections are based on the pro forma budget analysis in Appendix E for each year in the degree program. The number of credits times the number of students in each year equals the tuition revenue for each year of the pro forma budget. Tuition revenue for 90 Cybersecurity students reaches a steady state in year 4. It should be noted that tuition numbers are conservative as they are taken from lower-level tuition only. A 3% tuition increase per annum is also assumed.

Expenses include salaries and operating expenses. Salaries include full-time faculty (three assistant professors) and one full-time clerical technical support. The three new faculty members assist to develop and teach eight new classes and to teach new sections of the following offerings: CSI 1420, CSI 2300, CSI 2440, CSI 2470, and CSI 3660. In the first year, faculty in load is added. Support for one PhD graduate assistant in the first year and three thereafter is also offered for consideration. In years 4 and 5, in addition to three PhD graduate assistants, services of three Master-level students were also requested.

Operating expenses include supplies and services, travel, library, and Graduate tuition. Travel, including faculty travel, includes attendance at state and national meetings. Operating expenses for supplies and services, equipment, maintenance, and the library are described in the following sections. A budget for equipment upgrades is added to the budget in year 4.

See [Appendix E](#) for pro forma budget.



November 1, 2021

To: Khalid Mahmood Malik, Associate Professor, Department of Computer Science and Engineering, School of Engineering and Computer Science (SECS)

From: Helen Levenson, Associate Professor and Collection Development Librarian, University Libraries
James E. Van Loon, Assistant Professor and Liaison Librarian to SECS, University Libraries

Re: Library collection evaluation for proposed B.S. program in Cybersecurity

In developing this collection evaluation, we reviewed the draft proposal for the bachelor's program in cybersecurity, as well as title lists of core journals and resources in the field. We also referred to the 2014 collection evaluation done in support of the proposal for the master's program in cybersecurity. Overall, the library is well-positioned to support the proposed bachelor's program; only a few resources appropriate for undergraduate use should be added to strengthen the collection in subject areas related to new course offerings. Below is a brief description of the resources currently available, those that should be acquired, and a five-year cost estimate in support of this proposed program.

Journals and Conference Proceedings

Currently, the library subscribes to the IEEE Library, which includes all journals, proceedings and standards produced by the IEEE, as well as journals from IEE. The library also maintains online access to all Association of Computing Machinery (ACM) journals, magazines, transactions and conference proceedings through the ACM Digital Library. The ACM and IEEE digital libraries, along with the library's current subscriptions to the Springer publisher package and to Elsevier's Science Direct and ScienceDirect Freedom Collections, provide full-text access to most of the journal and proceedings literature. Our review of the major journals (Appendix A) and major proceedings (Appendix B) lead us to conclude that the library's current holdings for journals and proceedings would provide strong support for the new BS program.

Indexes

To access the journal and conference literature in computer science, the University Libraries maintain subscriptions to a number of online indexes. The most important of these are Scopus

(from Elsevier), Compendex (a bibliographic index to journals and conference proceedings in engineering and computing from 1969 to the present, accessed through Engineering Village), and Science Citation Index (available online through the Web of Science platform) which indexes journals from 1980 to present in the sciences. The library also provides access to Applied Science and Technology Source, which covers both academic and trade journal literature in science and technology. Other important resources include Criminal Justice Abstracts, which covers legal and ethical aspects of cybercrime and cybersecurity, and ProQuest One Business, which provides full-text access to a number of MIS-related journals. No additional indexes are needed to support the program adequately.

Monographs and Reference Sources

The library purchases the complete collection of Springer eBooks each year, which includes the essential book series Lecture Notes in Computer Science and other book and book series, totaling more than 29,000 volumes related to computer science. Beyond the Springer eBook collection, the library purchases only a minimal number of books related to computer security. Table 1 shows the library's holdings (total, and recently acquired) in the Library of Congress subject classifications most relevant to cybersecurity.

To ensure that the Libraries' monographic collection adequately supports the new proposed bachelors' degree program, we recommend the purchase of approximately five ebooks each year in the subject areas treated by the new courses in the BS program; these materials would be selected at a level appropriate for undergraduate use.

Table 1: Total monograph titles and those acquired within the last five years, subjects related to the proposed B.S. in Cybersecurity

LC call number	Subject	Total number of books owned	Number of books acquired within the last five years
QA76.9.A25	Access control. Computer security	1633	552
TK5105.59	Computer network security	233	78
HV8079.C65	Computer crimes. Digital forensics	38	13
QA76.9.D314	Database security	21	6
HD30.38	Computer network security	18	5
QA76.76.C68	Computer viruses	15	6
HV6773.15.C97	Cyberterrorism	6	3

Library Budget Request

Appendix C provides cost estimates for new resources needed to support the proposed bachelor's level program: funding to purchase approximately five ebooks on topics related to new course content each year (average current cost for these monographs is \$145), with additional funds in year one to purchase important reference works and to support a small amount of retrospective collection development of previously published but essential materials. Because this program will rely heavily on existing library resources, we have also included funding to cover anticipated annual inflationary cost increases for the library's current journals and research databases (estimated at ten percent per year) in computer science. Without additional funding, the library cannot guarantee that we will be able to continue to subscribe to our current resources. Therefore, we ask that the library be given funds each year to assist us in continuing to subscribe to these necessary resources for computer science faculty and students.

Appendix A

Major Cybersecurity Journals

Title	Publisher	OU Access
ACM Transactions on Information and System Security	ACM	yes
ACM Transactions on The Web	ACM	yes
Ad Hoc Networks	Elsevier	yes
Applied Sciences (Basel, Switzerland)	MDPI	no
Applied Soft Computing Journal	Elsevier	yes
Computer Communications	Elsevier	yes
Computer Fraud & Security	Elsevier	yes
Computer Law & Security Review	Elsevier	yes
Computer Networks	Elsevier	yes
Computers & Security	Elsevier	yes
Designs, Codes and Cryptography	Springer	yes
IEEE Access	IEEE IeL	yes - open access
IEEE ACM Transactions on Networking	IEEE/ACM	yes
IEEE Internet of Things Journal	IEEE IeL	yes
IEEE Security & Privacy	IEEE IeL	yes
IEEE Transactions on Dependable and Secure Computing	IEEE IeL	yes
IEEE Transactions on Information Forensics and Security	IEEE IeL	yes
IEEE Transactions on Smart Grid	IEEE IeL	yes
IEICE Transactions on Information and Systems	IEICE	no
IET Information Security	IEEE IeL	yes
Information and Computer Security	Emerald	12 month embargo
Information Sciences	Elsevier	yes
Information Security Journal: A Global Perspective	Taylor & Francis	18 month embargo
International Journal of Computer Science and Network Security	IJCSNS	yes - open access
International Journal of Information Security	Springer	yes
International Journal of Information Security and Privacy	IGI Global	no
International Journal of Networking and Security	Inderscience	no
International Journal of Communication Networks and Information Security	Kohat UP	yes
International Journal of Cyber-Security and Digital Forensics	SDIWC	yes - open access
IT Professional	IEEE IeL	yes
Journal In Computer Virology and Hacking Techniques	Springer	yes
Journal of Computer Security	IOS Press	no
Journal of Cryptographic Engineering	Springer	yes
Journal of Cryptology	Springer	yes
Journal of Grid Computing	Springer	yes
Journal of Information Security and Applications	Elsevier	yes
Journal of Network and Computer Applications	Elsevier	yes
Journal of Strategic Information Systems	Elsevier	yes
Knowledge and Information Systems	Springer	yes
Lecture Notes in Computer Science	Springer	yes
Networks	Wiley	yes
Network Security	Elsevier	yes
Security and Communication Networks	Hindawi	yes
Sensors (Basel, Switzerland)	MDPI	no
Wireless Networks	Springer	yes

Appendix B

Major Cybersecurity Conference Proceedings		
Title	Publisher	OU Access
ACSAC - Annual Computer Security Applications Conference	ACM	yes
ARES - International Conference on Availability, Reliability and Security	ACM	yes
ASIACRYPT - Theory and Application of Cryptology and Information Security	Springer	yes
CCS - SIGSAC Conference on Computer and Communications Security	ACM	yes
CHES - Cryptographic Hardware and Embedded Systems	Springer	yes
CRYPTO - International Cryptology Conference	Springer	yes
CSCloud - Cyber Security and Cloud Computing	IEEE	yes
CSFW - Computer Security Foundations Workshop	IEEE	yes
CSNet - Cyber Security In Networking	IEEE	yes
Cyber SA - Cyber Situational Awareness, Data Analytics And Assessment	IEEE	yes
Cyber Security - Cyber Security and Protection of Digital Services	IEEE	yes
CyCon - Cyber Conflict	IEEE	yes
DCS - Dependable and Secure Computing	IEEE	yes
EdgeCom - Edge Computing and Scalable Cloud	IEEE	yes
EISIC - European Intelligence and Security Informatics Conference	IEEE	yes
ESORICS - European Symposium on Research In Computer Security	Springer	yes
EUROCRYPT - Theory and Application of Cryptographic Techniques	Springer	yes
ICACC - International Conference on Anti-Cyber Crimes	IEEE	yes
ICCST - International Carnahan Conference on Security Technology	IEEE	yes
ICCW5 - International Conference on Cyber Warfare and Security	IEEE	yes
ICITBS - Intelligent Transportation, Big Data & Smart City	IEEE	yes
ICSSA - International Conference on Software Security and Assurance	IEEE	yes
IOTSMS - Internet of Things: Systems, Management and Security	IEEE	yes
ISI - Intelligence and Security Informatics	IEEE	yes
MobiSecServ - Mobile And Secure Services	IEEE	yes
NDSS - Network and Distributed System Security Symposium	open access	yes
SecDev - Cybersecurity Development	IEEE	yes
SIGCSE - Technical Symposium on Computer Science Education	ACM	yes
SIGITE - SIG Conference on Information Technology Education	ACM	yes
SIOT - Secure Internet of Things	IEEE	yes
SP - Security and Privacy	IEEE	yes
SPAC - Security, Pattern Analysis, and Cybernetics	IEEE	yes
SPW - Security and Privacy Workshops	IEEE	yes
SSIC - Security of Smart Cities, Industrial Control System and Communications	IEEE	yes
USENIX Security Symposium	open access	yes
WIFS - Workshop on Information Forensics and Security	IEEE	yes
WiSec - Conference on Security and Privacy In Wireless and Mobile Network	ACM	yes

Appendix C
Library Budget for Proposed B.S. in Cybersecurity

	Year 1	Year 2	Year 3	Year 4	Year 5
Monographs & electronic reference titles ¹	\$ 1,725	\$ 783	\$ 846	\$ 913	\$ 986
Support for current resources ²	\$ 2,800	\$ 3,080	\$ 3,388	\$ 3,727	\$ 4,100
Total	\$ 4,525	\$ 3,863	\$ 4,234	\$ 4,640	\$ 5,086

¹Purchase of 5 eformat monographs per year, with a 8% annual inflation rate in years 2-5. Additional eresources in year 1 only.

²Reflects a 10% annual inflation rate.

cc: Polly Bonuff-Jones, Dean of University Libraries
Amanda Nichols Hess, University Libraries Representative to University Senate

IMPLEMENTATION PLAN AND TIMELINE

The proposed start of the program is the Fall 2022 semester, and a search for new faculty per the pro forma budget and plan is expected to commence at that time, although new faculty is not expected to start until the second year of the program.

PROGRAM DELIVERY METHOD

The program will be offered in person only.

If your proposed new program has a delivery method of either fully online (50% or more of the courses have content that is 75% or more online) or blended (50% or more of the courses have content that is 10%-74% online), please contact the e-LIS department before continuing through this process elis@oakland.edu

I have met with e-LIS prior to completing this proposal:

Yes
 Not applicable

ASSESSMENT OF STUDENT LEARNING

The assessment plan was submitted to OIRA and the committee was advised that the documents would be reviewed after the degree proposal is accepted by the School of Engineering and Computer Science.

EXPECTED CAREER OPTIONS FOR GRADUATES

As previously mentioned, per the Bureau of Labor and Statistics there is expected to be massive growth in the security sector through at least 2031. With the exponential increase in cyberattacks in the last few years, industry in all areas is scrambling to cover this vital area.

Employment post-graduation is expected to be heavy in the automotive, banking, healthcare, and government sectors. The auto industry in particular has shown interest in the proposed degree's concentration in CPS Security. As we move into an age of autonomous vehicles the need for qualified cybersecurity candidates in the auto industry will be of paramount importance, and with this concentration, not offered in any other program, new graduates will be excellently positioned to fill these roles.

The need for information security and transaction security is well documented, and the banking and healthcare sectors are in dire need. Lastly, the importance of well-prepared cybersecurity professionals in all areas of the government cannot be overstated.

In addition, graduates will have the option of the continuation of studies in Oakland's Master of Cybersecurity program.

EQUIPMENT AND SUPPLIES

We request computer servers, desktop PCs, equipment, and materials and supplies for this B.S. in Cybersecurity program. The detailed budget is listed below:

- Three (3) cluster servers: This includes two cluster servers facilitating faculty's teaching activities and students' hands-on practice. The approximate cost per server is \$20,000. The total approximate cost is \$60,000.
- Forty (40) desktop PCs (the display is included): This includes the PCs that will be installed in the student lab. The approximate cost of one desktop PC is \$700. The total approximate cost is \$28,000.
- Equipment: This includes network equipment, such as routers and projectors. The total approximate cost is \$1,000.
- Materials and Supplies: This includes expendable lab materials and supplies for setting up and maintaining the everyday operation of the student lab. The total approximate cost is \$1,000.

APPENDICES

Appendix A – Faculty Profiles

Name	Website
Dr. Mehdi Bagherzadeh	Dr. Bagherzadeh's website
Dr. Jingshu Chen	Dr. Chen's website
Dr. Debatosh Debnath	Dr. Debnath's website
Dr. Huirong Fu	Dr. Fu's website
Dr. Marouane Kessentini	Dr. Kessentini's website
Dr. Dae-Kyoo Kim	Dr. Kim's website
Dr. Anyi Liu	Dr. Liu's website
Dr. Lunjin Lu	Dr. Lu's website
Dr. Tianle Ma	Dr. Ma's website
Dr. Khalid Malik	Dr. Malik's website
Dr. Hua Ming	Dr. Ming's website
Dr. Md Atiqul Mollah	Dr. Mollah's website
Dr. Nilesh Patel	Dr. Patel's website
Dr. Guangzhi Qu	Dr. Qu's website
Dr. Sunny Raj	Dr. Raj's website
Dr. Julian Rrushi	Dr. Rrushi's website
Dr. Amartya Sen	Dr. Sen's website
Dr. Ishwar Sethi	Dr. Sethi's website
Dr. Mohammad-Reza Siadat	Dr. Siadat's website
Dr. Gautam Singh	Dr. Singh's website
Dr. Lanyu Xu	Dr. Xu's website
Dr. Douglas Zytko	Dr. Zytko's website

Appendix B – Sample Plan of Study

Student Schedule - 128 Credits	
Fall I - 16 Credits MTH 1554 - Calculus I (4) CSI 1420 - Introduction to C Programming and Unix (4) General education (4) General education (4)	Winter I - 17 Credits CSI 2300 - Object Oriented Computing (4) MTH 1555 - Calculus II (4) Approved science elective with lab (5) General education (4)
Fall II - 16 Credits Math Elective (4) CSI2440 - Computer Systems (4) General education (4) CSI 2470 - Introduction to Computer Networks (4)	Winter II - 18 Credits CSI 3660 - Systems Administration (4) CSI 2460 - Fundamentals of Cybersecurity (4) CSI 2999 - Sophomore Project (2) General education (4) General education (4)
Fall III - 16 Credits Math Elective (4) CRJ 3341 - Cybercrime (4) CSI 3370 - Software Engineering and Practice (4) CSI 4480 - Information Security Practices (4)	Winter III - 15 Credits CSI 3450 - Database Design and Implementation (4) CSI 4700 - Software Security (4) Professional Track (4) MIS 4180 - IS Risk Analysis and Controls Development (3)
Fall IV - 16 Credits CSI 4240 - Cloud Computing (4) CSI 4470 - Digital Forensics (4) Professional elective (2) Professional track (4) Professional elective (2)	Winter IV - 14 Credits CSI 4600 - Network Security (4) Professional Elective (2) Professional track (4) CSI 4999 - Senior Capstone Project (4)

Appendix C - Industry Letters of Support

From: Fred Killeen <fred.killeen@gm.com>

Date: Mon, Nov 1, 2021 at 4:12 PM

Subject: RE: [EXTERNAL] Help with the development of a BS in Cybersecurity program at Oakland University

To: Lunjin Lu <Lu@oakland.edu>

Lunjin, cybersecurity is critical to GM and finding talent is an ongoing challenge. We have had great success in partnering with Oakland University for IT talent and it would be great to extend that to our cyber program. The demand in the industry far exceeds the supply so having an undergraduate program at OU would be a great opportunity for GM and OU to partner.

Thanks,
Fred



Oakland University
School of Engineering and
Computer Science
115 Library Drive
Rochester, MI 48309

December 21, 2021

Subject: Major in Cybersecurity

To whom it may concern,

As an Oakland University graduate and a hiring manager at Altair Engineering (world-wide engineering and software development firm based in Troy, Michigan) I was excited to hear about this possible Major in Cybersecurity! Having a multi-disciplinary program at Oakland University, especially given your demonstrated abilities to innovate in instruction and research during the COVID-19 pandemic, will be a tremendous development for businesses in Michigan, regionally, and globally.

My firm, Altair Engineering, has a strong internship program and we hire graduates in many fields. Like many organizations, landing cybersecurity talent is increasingly difficult globally, and it is especially challenging since our High Performance Computing footprint, heavy use of Linux containers, and simultaneously processing many types of sensitive data lead into specialized cybersecurity needs.

I would be glad to speak on behalf of your program to my network. Please reach out if I may help to move this forward.

Wishing you Happy Holidays and a very Happy New Year,

A handwritten signature in black ink that reads "JEFF MARRACCINI".

Jeffrey ("Jeff") Maccacini
Senior Vice President, Cloud Strategy and Technology
Altair Engineering, Inc.
jeff@altair.com +12487095471

1820 E. Big Beaver Rd.
Troy, MI 48063 USA

p: 248 614 2400
f: 248 614 2411

altair.com

November 8, 2021

Letter of Support for Emerging Program
Bachelor of Science in Cybersecurity
Computer Science and Engineering
Oakland University, Rochester, Michigan

To Whom It May Concern:

I am a current member of the Engineering Advisory Board and a member of its Executive Committee at Oakland University. I have had the opportunity to participate in development of a leadership class for undergraduate upper classmen and graduate students in engineering. I have served with three engineering deans and three university presidents. I am a former Executive Vice President at DTE Energy, and I am currently the principal and owner of May Technology Group, a company that consults on leadership, change management, and technical subjects.

I am pleased to support the development of the new Bachelor of Science in Cybersecurity program to be offered by the Department of Computer Science and Engineering (CSE). The university has the strength of 26 permanent full-time faculty, of which I am aware, many teach and perform research in the area of cybersecurity. To further strengthen the current offering of a Master of Science program in Cybersecurity, the development of a new Bachelor of Science in Cybersecurity program is underway to expand educational and workforce opportunities for its students.

The goal of the new Bachelor of Science in Cybersecurity program, as declared by Oakland University, is to provide students with both a strong engineering foundation and technical skills in the areas of security, privacy, and cryptography as applied to information systems, networks, and software. The ultimate goal is one of contributing to a better social, ethical and legal environment that continues to be pervasive in all aspects of engineering, business and the community at large. This new program will prepare graduating engineers to be capable of resolving future problems in security, the internet, mobile devices, and the ever-increasing role of software applications.

I believe the need for the new Bachelor of Science in Cybersecurity program is current and long lasting. The capability of the faculty and their facilities at Oakland University are more than sufficient to lead the program to exceed expectations in the goals articulated. Lastly, the department chair, the engineering dean and the larger university is overwhelmingly supportive of this new program. I am pleased to add my support to this new endeavor.

All the best!

Ron A. May, Doctor of Science Honoris Causa, Oakland University

Appendix D - Departmental Letters of Support



Department of Sociology, Anthropology,
Social Work & Criminal Justice

Memorandum

Date: December 8, 2021

RE: Support for Proposed Cybersecurity Major

To: Lunjin Lu, Chair, Computer Science and Engineering

From: Jo Reger, Chair, Sociology, Anthropology, Social Work and Criminal Justice

I am writing to support the proposed Cybersecurity major from the Department of Computer Science and Engineering. I have reviewed the proposal and agree to include our course, CRJ 3341 – Cybercrime, as a required professional subject course in the major.

In addition, I would also like to suggest two additional courses which could be offered as professional electives. Those are CRJ 3340 - White Collar Crime and CRJ 3342 - Surveillance Society. These courses could add valuable context to the work of cybersecurity for students who go on to work in the field. Integrating these courses would aid the department in meeting their goal of providing students with "a good understanding of the social, ethical, legal, and policy aspects of cybersecurity."

The catalog copy for these two courses reads:

CRJ 3340 – White Collar Crime. Overview of white-collar crime and deviance, corporate and organizational crime, and political crimes both by and against the state. (4).

CRJ 3342 – The Surveillance Society. Explores the development and significance of surveillance as a feature of modern society, how surveillance has changed over time with the development of new technologies, its presence in everyday life and different social institutions and contexts and the degree to which surveillance enhances social participation or social control in society.

Identical with [SOC 3860](#). (4)

In sum, I support the proposed cybersecurity major and the inclusion of CRJ 3341 - Cybercrime.

OAKLAND UNIVERSITY
College of Arts and Sciences

DEPARTMENT OF MATHEMATICS AND STATISTICS
Rochester, Michigan 48309-4479

December 13, 2021

To Whom It May Concern:

I am enthusiastically writing this letter on behalf of the Department of Mathematics and Statistics to give our strongest support for a Bachelor of Science Degree in Cybersecurity as proposed by the School of Engineering and Computer Science (SECS). I believe a program in Cybersecurity at Oakland University would be a great way to attract students! The specific program proposed by the SECS would provide students in the Cybersecurity program with a strong foundation in specific aspects of security, privacy, and cryptography. Students would also gain necessary technical skills for working in the field.

The Department of Mathematics and Statistics at Oakland is excited to see that many courses offered by our faculty are required in the program and that many are electives.

In summary, we strongly support the proposal by SECS to have a B.S. in Cybersecurity at Oakland University, and we are very happy to be a part of it. Please feel free to contact me if you have any questions.

Sincerely,



Anna Maria Spagnuolo
Chair
Professor of Mathematics
spagnuolo@oakland.edu

OAKLAND
UNIVERSITY

Mark C. Navin, Ph.D., HEC-C
Professor and Chair of Philosophy
Lecturer in Foundational Medical Studies
Clinical Ethicist

Department of Philosophy
746 Mathematics and Science Center
146 Library Drive
Rochester, MI, 48309-4479
(248) 370-3390
navin@oakland.edu



Lunjin Lu, PhD
Professor and Chair
Department of Computer Science & Engineering
Oakland University

November 30, 2021

Dear Professor Lu:

I write in my capacity as chair of the Department of Philosophy to express my support for the Bachelor of Science in Cybersecurity program you are developing.

Your proposed program will provide students with technical skills they will need to work in cybersecurity. But I especially appreciate your commitment to expose students to the "social, policy, ethical and legal aspects of security and privacy." Along those lines, I am delighted that you will be proposing PHIL 1310 (Introduction to Ethics in Science and Engineering) as a required course for your new program.

Please let me know if I can provide any additional support!

Sincerely,

A handwritten signature in black ink, appearing to read "Mark C. Navin".

Mark C. Navin, PhD
Professor and Chair of Philosophy

From: Vijayan Sugumarar <sugumarar@oakland.edu>
Date: Mon, Dec 20, 2021 at 9:18 PM
Subject: RE: Request for Letter of Support - BS in Cybersecurity
To: Lunjin Lu <Lu@oakland.edu>
Cc: Michael Mazzeo <mazzeo@oakland.edu>, Rajeev Singhal <singhal@oakland.edu>, <sugumarar@oakland.edu>

Dear Professor Lu,

The **DIS** Department supports the BS in Cybersecurity program. Thank you for listing one of our courses (MIS 4180 - IS Risk Analysis and Controls Development) as part of this program. If it is of interest, there are other courses we offer that might be of interest to the program. You could include some of them in the program as well.

- MIS 4130 - Networks (3)
- MIS 4140 - Information Security Lab (3)
- MIS 4700 - IS Security (3)
- MIS 4750 - Mobile Security and Secure Application Development (3)
- MIS 4900 - Information Security Legal Compliance and Ethics (3)

Best wishes for the new program.

Regards,

Vijayan

Vijayan Sugumarar, Ph.D.
Distinguished Professor, Management Information Systems
Chair, Department of Decision and Information Sciences
Co-Director, Center for Data Science and Big Data Analytics
School of Business Administration
Oakland University

Appendix E - Pro Forma Budget

PROFORMA FOR NEW, INCENTIVE AND ONLINE PROGRAMS						
FY:	22			Submission Type:		Budget Projection
College Code:	EG			Program Attribute:		New Programs
Fund:	N/A			Year of Program:		1 - 5
Program Title:	SECS-Bachelor of Sci Cybersecurity			Funding Type:		
REVENUE VARIABLE		2022-2023	2023-2024	2024-2025	2025-2026	2026-2027
Headcount						
UG Lower Level		20	40	70	90	90
UG Upper Level						
Graduate						
Doctoral						
UG Credits Offered						
GR Credits Offered						
PhD Credits Offered						
FYES		10.67	42.67	74.67	96.00	128.00
UG LL Total Credits		320	1,280	2,240	2,880	3,840
UG UL Total Credits						
Grad Total Credits						
PhD Total Credits						
Revenue						
Tuition		\$ 159,200	\$ 655,910	\$ 1,182,272	\$ 1,565,654	\$ 2,150,170
Differential or Non Resident Tuition						
Total Revenue		\$ 159,200	\$ 655,910	\$ 1,182,272	\$ 1,565,654	\$ 2,150,170
EXPENSES						
Salaries						
Faculty Salaries	6101		\$ 100,000	\$ 100,000	\$ 200,000	\$ 200,000
Visiting Faculty	6101					
Administrative Professionals	6201					
Clerical Technical	6211					
Administrative IC	6221					
Faculty Inload/Replacement Costs	6301	\$ 28,000	\$ 14,000			
Faculty Overload	6301					
Part-Time Faculty	6301					
Graduate Assistant	6311	\$ 15,000	\$ 30,000	\$ 45,000	\$ 60,000	\$ 60,000
Wages	6401					
Out of Classification	6401					
Overtime	6401					
Student Labor	6501					
Total Salary Expenses		\$ 43,000	\$ 144,000	\$ 145,000	\$ 260,000	\$ 260,000
Fringe Benefits	6701	\$ 12,295	\$ 47,790	\$ 43,285	\$ 84,380	\$ 84,380
Total Compensation		\$ 55,295	\$ 191,790	\$ 188,285	\$ 344,380	\$ 344,380
Operating Expenses						
Supplies and Services	7101	\$ 10,000	\$ 10,000	\$ 10,000	\$ 10,000	\$ 10,000
Graduate Assistant Tuition	7101	\$ 12,920	\$ 26,615	\$ 41,120	\$ 56,472	\$ 58,166
E-Learning Support	7102					
Travel	7201	\$ 5,000	\$ 3,000	\$ 2,000		
Telephone	7301					
Equipment	7501		\$ 70,000			\$ 20,000
Library	7401	\$ 4,525	\$ 3,863	\$ 4,234	\$ 4,640	\$ 5,086
Total Operating Expenses		\$ 32,445	\$ 113,478	\$ 57,354	\$ 71,112	\$ 93,252
Total Expenses		\$ 87,740	\$ 305,268	\$ 245,639	\$ 415,492	\$ 437,632
Net Income excl. Fees		\$ 71,460	\$ 350,642	\$ 936,633	\$ 1,150,162	\$ 1,712,538
Expenses to Tuition Ratio		0.55	0.47	0.21	0.27	0.20

- Lower-level tuition fees are assumed for the sake of simplicity
- In-state tuition was assumed for all candidates
- One (1) assistant professor will be hired in the 2nd year and the second (2nd) will be hired in the 4th year. For details and justification, see staffing needs section.
- One PhD graduate assistant for the first year, two in 2nd year, three (3) in the 3rd year was used. Also, in years 4 and 5, Four (4) students were requested.
- 3% inflation was used for tuition and GA tuition.
- \$70,000 will be used to develop the new Lab in the 2nd year to accommodate the new student body and offer the labs of new cybersecurity classes, and another \$20,000 will be spent in 5th year to upgrade the equipment.

SBRC Proforma Template

FY2023

Most Likely Scenario

	Year 1	Year 2	Year 3	Year 4	Year 5
Est. New Students to Program	25	27	31	34	34
1st Year Cohort Revenue	\$ 426,525	\$ 460,647	\$ 528,891	\$ 580,074	\$ 580,074
2nd Year Cohort Revenue	\$ -	\$ 413,600	\$ 446,688	\$ 512,864	\$ 562,496
3rd Year Cohort Revenue	\$ -	\$ -	\$ 486,600	\$ 525,528	\$ 603,384
4th Year Cohort Revenue	\$ -	\$ -	\$ -	\$ 471,394	\$ 509,105
Gross Tuition Revenue	\$ 426,525	\$ 874,247	\$ 1,462,179	\$ 2,089,860	\$ 2,255,059
Less: Avg Financial Aid (30%)	\$ (127,958)	\$ (262,274)	\$ (438,654)	\$ (626,958)	\$ (676,518)
Net Tuition Revenue	\$ 298,568	\$ 611,973	\$ 1,023,525	\$ 1,462,902	\$ 1,578,541
Expenses					
Salaries					
Faculty Salaries	6301 \$ -	\$ 100,000	\$ 102,500	\$ 205,000	\$ 210,000
Visiting Faculty	6301				
Administrative Professionals	6201				
Clerical Technical	6211				
Administrative IC	6221				
Faculty Inload/Replacement Costs	6301 \$ 28,000	\$ 14,000			
Faculty Overload	6301				
Part-Time Faculty	6301				
Graduate Assistant	6311 \$ 15,000	\$ 30,000	\$ 45,000	\$ 60,000	\$ 60,000
Casual/Temp	6401				
Out of Classification	6401				
Student Labor	6501				
Total Salary Expense	\$ 43,000	\$ 144,000	\$ 147,500	\$ 265,000	\$ 270,000
Fringe Benefits	6701 \$ 3,440	\$ 45,820	\$ 46,958	\$ 91,515	\$ 93,630
Total Compensation	\$ 46,440	\$ 189,820	\$ 194,458	\$ 356,515	\$ 363,630
Operating Expenses					
Supplies and Services	7101 \$ 10,000	\$ 10,000	\$ 10,000	\$ 10,000	\$ 10,000
Graduate Tuition	7101 \$ 12,400	\$ 24,800	\$ 37,200	\$ 49,600	\$ 49,600
E-Learning Support	7102				
Travel	7201				
Equipment	7501	\$ 70,000			
Maintenance	7110			\$ 20,000	
Recruitment and advertising	7301 \$ 25,000	\$ 5,000	\$ 5,000	\$ 5,000	\$ 5,000
Library	7401 \$ 4,525	\$ 3,863	\$ 4,234	\$ 4,640	\$ 5,086
Total Operating Expenses	\$ 51,925	\$ 113,663	\$ 56,434	\$ 89,240	\$ 69,686
Total Expenses	\$ 98,365	\$ 303,483	\$ 250,892	\$ 445,755	\$ 433,316
Net Income (Loss)	\$ 328,160	\$ 570,764	\$ 1,211,288	\$ 1,644,105	\$ 1,821,743

SBRC Proforma Template

FY2023

Best-Case Scenario

	Year 1	Year 2	Year 3	Year 4	Year 5
Est. New Students to Program	30	35	40	45	50
1st Year Cohort Revenue	\$ 511,830	\$ 597,135	\$ 682,440	\$ 767,745	\$ 853,050
2nd Year Cohort Revenue	\$ -	\$ 496,320	\$ 579,040	\$ 661,760	\$ 744,480
3rd Year Cohort Revenue	\$ -	\$ -	\$ 583,920	\$ 681,240	\$ 778,560
4th Year Cohort Revenue	\$ -	\$ -	\$ -	\$ 565,673	\$ 659,951
Gross Tuition Revenue	\$ 511,830	\$ 1,093,455	\$ 1,845,400	\$ 2,676,418	\$ 3,036,041
Less: Avg Financial Aid (30%)	\$ (153,549)	\$ (328,037)	\$ (553,620)	\$ (802,925)	\$ (910,812)
Net Tuition Revenue	\$ 358,281	\$ 765,419	\$ 1,291,780	\$ 1,873,492	\$ 2,125,229
Expenses					
Salaries					
Faculty Salaries	6101 \$ -	\$ 100,000	\$ 102,500	\$ 205,000	\$ 210,000
Visiting Faculty	6101				
Administrative Professionals	6201				
Clerical Technical	6211				
Administrative IC	6221				
Faculty Inload/Replacement Costs	6301				
Faculty Overload	6301 \$ 28,000	\$ 14,000			
Part-Time Faculty	6301				
Graduate Assistant	6311 \$ 15,000	\$ 30,000	\$ 45,000	\$ 60,000	\$ 60,000
Casual/Temp	6401				
Out of Classification	6401				
Student Labor	6501				
Total Salary Expense	\$ 43,000	\$ 144,000	\$ 147,500	\$ 265,000	\$ 270,000
Fringe Benefits	6701 \$ 3,440	\$ 45,820	\$ 46,958	\$ 91,515	\$ 93,630
Total Compensation	\$ 46,440	\$ 189,820	\$ 194,458	\$ 356,515	\$ 363,630
Operating Expenses					
Supplies and Services	7101 \$ 10,000	\$ 10,000	\$ 10,000	\$ 10,000	\$ 10,000
Graduate Tuition	7101 \$ 12,400	\$ 24,800	\$ 37,200	\$ 49,600	\$ 49,600
E-Learning Support	7102				
Travel	7201				
Equipment	7501	\$ 70,000			
Maintenance	7110			\$ 20,000	
Recruitment and advertising	7101 \$ 25,000	\$ 5,000	\$ 5,000	\$ 5,000	\$ 5,000
Library	7401 \$ 4,525	\$ 3,863	\$ 4,234	\$ 4,640	\$ 5,086
Total Operating Expenses	\$ 51,925	\$ 113,663	\$ 56,434	\$ 89,240	\$ 69,686
Total Expenses	\$ 98,365	\$ 303,483	\$ 250,892	\$ 445,755	\$ 433,316
Net Income (Loss)	\$ 413,465	\$ 789,972	\$ 1,594,509	\$ 2,230,663	\$ 2,602,725

SBRC Proforma Template

FY2023

Worst-Case Scenario

	Year 1	Year 2	Year 3	Year 4	Year 5
Est. New Students to Program	8	10	12	15	15
1st Year Cohort Revenue	\$ 136,488	\$ 170,610	\$ 204,732	\$ 255,915	\$ 255,915
2nd Year Cohort Revenue	\$ -	\$ 132,352	\$ 165,440	\$ 198,528	\$ 248,160
3rd Year Cohort Revenue	\$ -	\$ -	\$ 155,712	\$ 194,640	\$ 233,568
4th Year Cohort Revenue	\$ -	\$ -	\$ -	\$ 150,846	\$ 188,558
Gross Tuition Revenue	\$ 136,488	\$ 302,962	\$ 525,884	\$ 799,929	\$ 926,201
Less: Avg Financial Aid (30%)	\$ (40,946)	\$ (90,889)	\$ (157,765)	\$ (239,979)	\$ (277,860)
Net Tuition Revenue	\$ 95,542	\$ 212,073	\$ 368,119	\$ 559,950	\$ 648,340
Expenses					
Salaries					
Faculty Salaries	6101 \$ -	\$ 100,000	\$ 102,500	\$ 205,000	\$ 210,000
Visiting Faculty	6101				
Administrative Professionals	6201				
Clerical Technical	6211				
Administrative IC	6221				
Faculty Inload/Replacement Costs	6301 \$ 28,000	\$ 14,000			
Faculty Overload	6301				
Part-Time Faculty	6301				
Graduate Assistant	6311 \$ 15,000	\$ 30,000	\$ 45,000	\$ 60,000	\$ 60,000
Casual/Temp	6401				
Out of Classification	6401				
Student Labor	6501				
Total Salary Expense	\$ 43,000	\$ 144,000	\$ 147,500	\$ 265,000	\$ 270,000
Fringe Benefits	6701 \$ 3,440	\$ 45,820	\$ 46,958	\$ 91,515	\$ 93,630
Total Compensation	\$ 46,440	\$ 189,820	\$ 194,458	\$ 356,515	\$ 363,630
Operating Expenses					
Supplies and Services	7101 \$ 5,000	\$ 5,000	\$ 5,000	\$ 5,000	\$ 5,000
Graduate Tuition	7101 \$ 12,400	\$ 24,800	\$ 37,200	\$ 49,600	\$ 49,600
E-Learning Support	7302				
Travel	7201				
Equipment	7501			\$ 70,000	
Maintenance	7110				
Recruitment and advertising	7301 \$ 25,000	\$ 5,000	\$ 5,000	\$ 5,000	\$ 5,000
Library	7401 \$ 4,525	\$ 3,863	\$ 4,234	\$ 4,640	\$ 5,086
Total Operating Expenses	\$ 46,925	\$ 38,663	\$ 51,434	\$ 134,240	\$ 64,686
Total Expenses	\$ 93,365	\$ 228,483	\$ 245,892	\$ 490,755	\$ 428,316
Net Income (Loss)	\$ 43,123	\$ 74,479	\$ 279,993	\$ 309,174	\$ 497,885

BOARD OF TRUSTEES FORMAL SESSION



COMPUTER SCIENCE AND ENGINEERING
SCHOOL OF ENGINEERING AND COMPUTER SCIENCE

» SEEK VIRTUE AND KNOWLEDGE

B.S. in Cybersecurity Proposal

Department of Computer Science and Engineering
School of Engineering and Computer Science
Oakland University

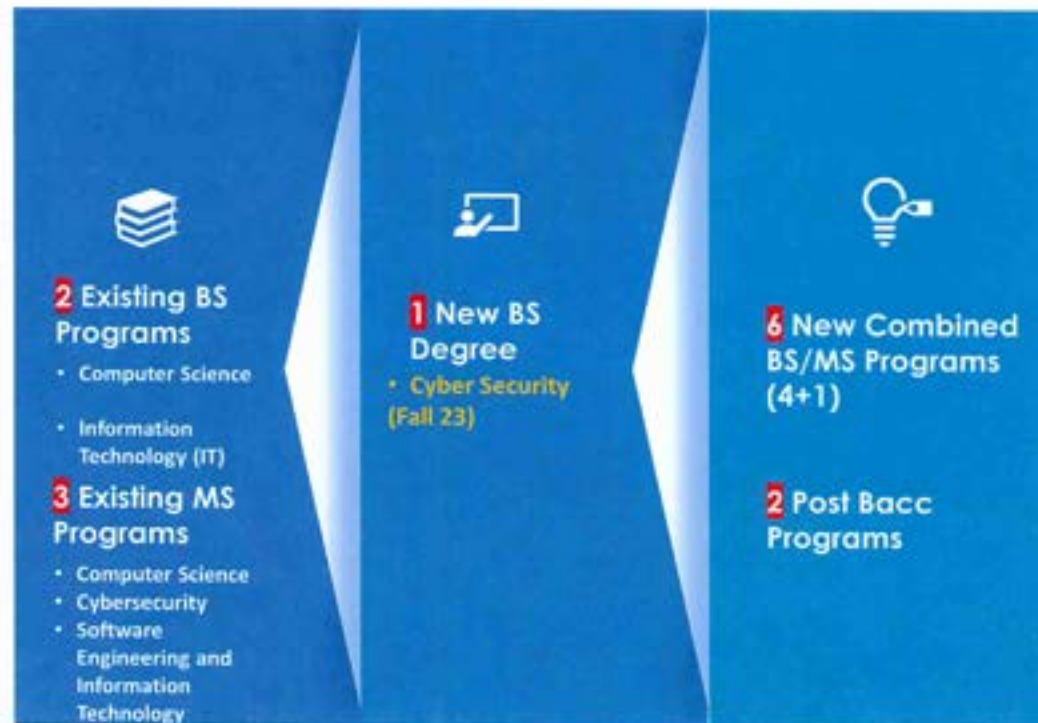


OU Strategic Planning and B.S. in Cybersecurity



COMPUTER SCIENCE AND ENGINEERING
SCHOOL OF ENGINEERING AND COMPUTER SCIENCE

- Goal 1: Foster student success through a robust teaching and learning environment and comprehensive student services.



January 2023



OU Strategic Planning and B.S. in Cybersecurity



COMPUTER SCIENCE AND ENGINEERING
SCHOOL OF ENGINEERING AND COMPUTER SCIENCE

- Goal 2: Be recognized as a strong research and scholarly environment focused on creative endeavors and on the discovery, dissemination, and utilization of knowledge.

\$1 million in funding from the Department of Energy to establish the OU Cybersecurity Center (2023-2024): Research and training opportunities to enhance the security and resilience of U.S. critical energy infrastructure

\$3.1 million CyberCorps Scholarship for Service: Cyber Defense of Intelligent Systems (2022-2027): Establishing or continuing scholarship programs in cybersecurity and aligns with the U.S. National Cyber Strategy to develop a superior cybersecurity workforce.

The Department of Homeland Security and the National Security Agency designated Oakland University as a National Center of Academic Excellence in Cyber Defense Education.



Evolving Threats to Energy Infrastructure



CyberCorps® Scholarship For Service (SFS)

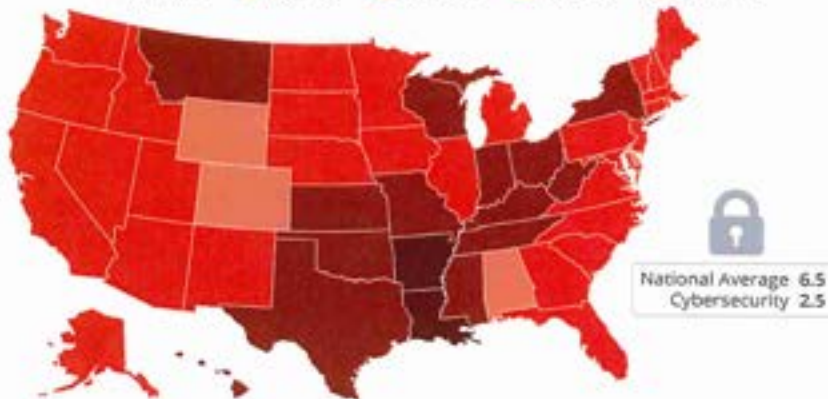


- Goal 3: Become a leader in serving the needs and aspirations of our communities and region through expanded community relationships, institutional reputation and visibility, and engagement.

Which States Have a Shortage of CyberSecurity Workers?

Ratio of existing cybersecurity workers to cybersecurity job openings by state, 2018*

0.0 - 0.9 1.0 - 1.9 2.0 - 2.9 3.0 - 3.9 4.0 - 4.9

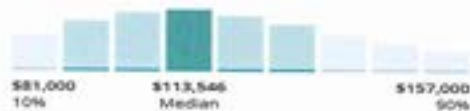


* Numbers closer to 0 indicate a shortage
@StatistaCharts Source: Cyber Seek

Average Cyber Security Engineer Salary in Rochester, MI

\$113,546 yearly
\$54.59 hourly

Entry level Salary
\$81,000 yearly



statista

CYBERSECURITY SUPPLY/DEMAND HEAT MAP

Public Sector Data
Private Sector
Total job openings

Cybersecurity talent gaps exist across the country. Closing these gaps requires detailed knowledge of the cybersecurity workforce in your region. This interactive heat map provides a granular snapshot of demand and supply data for cybersecurity jobs at the state and metro area levels, and can be used to grasp the challenges and opportunities facing your local cybersecurity workforce.



Michigan

TOTAL CYBERSECURITY JOB OPENINGS

19,310

TOTAL EMPLOYED CYBERSECURITY WORKFORCE

21,834

SUPPLY/DEMAND RATIO



68% national average
62% Michigan

GEOGRAPHIC CONCENTRATION

High

LOCATION QUOTIENT

1.4

National average
1.0

TOP CYBERSECURITY JOB TITLES

- Cybersecurity Analyst
- Penetration & Vulnerability Tester
- Software Developer
- Cybersecurity Consultant
- Network Engineer
- Cybersecurity Manager
- Systems Engineer
- IT Auditor
- Incident & Response Analyst

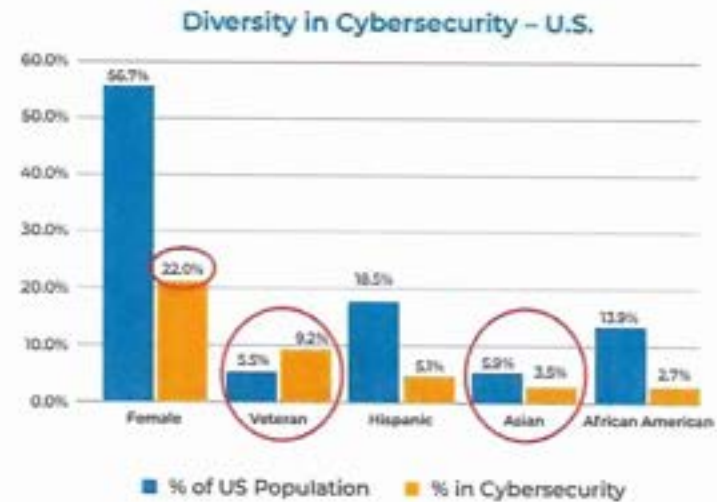
January 2023



OU Strategic Planning and BS in Cybersecurity

- Goal 4: Advance diversity, equity, and inclusion in an environment of mutual trust and respect at all levels of the institution and facilitate opportunities and success for all community members.

The new B.S. in Cybersecurity will offer opportunities to train minority students in this National Priority area and increase diversity at OU



U.S. Bureau of Labor Statistics



BS in Cyber Security: Curriculum



COMPUTER SCIENCE AND ENGINEERING
SCHOOL OF ENGINEERING AND COMPUTER SCIENCE

BACHELOR OF SCIENCE IN CYBERSECURITY

The interdisciplinary nature of the Bachelor of Science in Cybersecurity at Oakland University aims to serve IT, financial, research, healthcare, law enforcement and defense organizations through its specialized concentrations. Students will be prepared for employment in the public and private sectors.

Oakland University is a National Science Foundation SA Center of Academic Excellence and Information Assurance and Cyber Defense (CAE-IA/CD) Education.

CORE COURSES

Introduction to C Programming and Unix
Object-Oriented Computing
Computer Systems
Fundamentals of Cybersecurity
Introduction to Computer Networks
Sophomore Project

PROFESSIONAL SUBJECTS

Software Engineering and Practice
Database Design and Implementation
System Administration
Cloud Computing
Cyber Laws and Digital Forensics
Information Security Practice
Network Security
Software Security
Cybercrime
Risk Analysis and Security Controls Development
Senior Capstone Project

PROFESSIONAL TRACKS

Select one track

Software Security

Software Verification and Testing
Mobile Security
Reverse Engineering and Malware Analysis

AI in Cybersecurity Track

Artificial Intelligence
AI for Cybersecurity and Privacy
Multimedia Forensics

Cyber Physical System Security Track

Fundamentals of Embedded System Design
Industrial Control Security
Automotive Security
Embedded Security



BS in Cyber Security: Enrollment and Budget



COMPUTER SCIENCE AND ENGINEERING
SCHOOL OF ENGINEERING AND COMPUTER SCIENCE

Est. New Students to Program

	Year 1	Year 2	Year 3	Year 4	Year 5
	25	27	31	34	34
1st Year Cohort Revenue	\$ 426,525	\$ 460,647	\$ 528,891	\$ 580,074	\$ 580,074
2nd Year Cohort Revenue	\$ -	\$ 413,600	\$ 446,688	\$ 512,864	\$ 562,496
3rd Year Cohort Revenue	\$ -	\$ -	\$ 486,600	\$ 525,528	\$ 603,384
4th Year Cohort Revenue	\$ -	\$ -	\$ -	\$ 471,394	\$ 509,105
Gross Tuition Revenue	\$ 426,525	\$ 874,247	\$ 1,462,179	\$ 2,089,860	\$ 2,255,059
Less: Avg Financial Aid (30%)	\$ (127,958)	\$ (262,274)	\$ (438,654)	\$ (626,958)	\$ (676,518)
Net Tuition Revenue	\$ 298,568	\$ 611,973	\$ 1,023,525	\$ 1,462,902	\$ 1,578,541

Expenses

Salaries

Faculty Salaries	6101	\$ -	\$ 100,000	\$ 102,500	\$ 205,000	\$ 210,000
Visiting Faculty	6101					
Administrative Professionals	6201					
Clerical Technical	6211					
Administrative IC	6221					
Faculty Inload/Replacement Costs	6301	\$ 28,000	\$ 14,000			
Faculty Overload	6301					
Part-Time Faculty	6301					
Graduate Assistant	6311	\$ 15,000	\$ 30,000	\$ 45,000	\$ 60,000	\$ 60,000
Casual/Temp	6401					
Out of Classification	6401					
Student Labor	6501					
Total Salary Expense		\$ 43,000	\$ 144,000	\$ 147,500	\$ 265,000	\$ 270,000
Fringe Benefits	6701	\$ 3,440	\$ 45,820	\$ 46,958	\$ 91,515	\$ 93,630
Total Compensation		\$ 46,440	\$ 189,820	\$ 194,458	\$ 356,515	\$ 363,630
Operating Expenses						
Supplies and Services	7101	\$ 10,000	\$ 10,000	\$ 10,000	\$ 10,000	\$ 10,000
Graduate Tuition	7101	\$ 12,400	\$ 24,800	\$ 37,200	\$ 49,600	\$ 49,600
E-Learning Support	7102					
Travel	7201					
Equipment	7501		\$ 70,000			
Maintenance	7110				\$ 20,000	
Recruitment and advertising	7101	\$ 25,000	\$ 5,000	\$ 5,000	\$ 5,000	\$ 5,000
Library	7401	\$ 4,525	\$ 3,863	\$ 4,234	\$ 4,640	\$ 5,086
Total Operating Expenses		\$ 51,925	\$ 113,663	\$ 56,434	\$ 89,240	\$ 69,686
Total Expenses		\$ 98,365	\$ 303,483	\$ 250,892	\$ 445,755	\$ 433,316
Net Income (Loss)		\$ 328,160	\$ 308,490	\$ 772,633	\$ 1,017,147	\$ 1,145,225

NEW DEGREE PROPOSAL



COMPUTER SCIENCE AND ENGINEERING
SCHOOL OF ENGINEERING AND COMPUTER SCIENCE

» *SEEK VIRTUE AND KNOWLEDGE*

B.S. in Cybersecurity Proposal

Department of Computer Science and Engineering
School of Engineering and Computer Science
Oakland University