CYBERSECURITY, M.S.

Program Description

The M.S. in Cybersecurity program curriculum is aimed at professionals with a background in business management, information technology, computer science, or criminal justice. This multidisciplinary curriculum is designed for busy adult learners and draws courses from our information technology leadership, computer information science, and economic crime forensics programs. The curriculum is intended to create a better understanding of:

- Information security policies and procedures
- Computer crimes and related legislation
- Investigative practices and procedures
- Corporate ethics and compliance

The program is offered in a totally online format. It follows the traditional academic calendar of a fall and spring semester and a shorter summer semester. The fall and spring semesters are divided into two 8 week terms. A full-time graduate student carries a minimum of 6 semester credit hours. Some courses may require more hours per week in some areas of instruction. All courses are online and 3 credits in the length. The courses will meet both synchronously (optional) and asynchronously. Students are required to participate in chat sessions and/or discussion boards, which will take the place of classroom meetings. Synchronous sessions will be recorded for students who are not able to attend the actual session. Students who are not able to attend the synchronous sessions will be asked to complete a short assignment related to the recorded session. Depending on their personal schedules, students may elect to take courses every term or wait for the next term to continue studies. Courses in the summer are also 8 weeks in length. If a student decides to take two courses during the summer session, they will overlap in the time frame.

Mission

The graduate program in M.S. Cybersecurity educates students in theoretical and practical knowledge of cybersecurity. The program develops competencies in cybersecurity management as well as breach detection, mitigation and prevention. The faculty and students develop and maintain relationships with industry practitioners to encourage excellence and provide attention to ethical principles and changes related to cybersecurity.

Program Specific Information

Progression through the Program

Ten courses (30 credits) are required for the degree. Each student is required to satisfy all eight required courses (which includes the capstone) and an elective.

4+1 Graduate Program Option

During their senior year, students with a GPA of at least 3.0 may apply for the 4+1 BS/BA Computer Science, BS Cybersecurity, BS Information Technology to MS Cybersecurity option. Students apply to graduate programs during their junior or senior year. The student is expected to have an overall GPA of 3.0. If they are candidates for acceptance into the graduate program, they are able to take two graduate level courses (6 credits—2 courses) which will be counted towards their undergraduate 120 credit requirement. If the grades in the graduate courses are B or better, they will also be counted towards the graduate programs. Students will receive their bachelor's degree and once it is completed, the student will be enrolled in the master's program. Students will be required to complete the remaining 24 credits (8 courses) to earn the graduate degree. In order to complete they M.S. Cybersecurity, students would need to complete a total of 8 additional classes (24 credits). This graduate degree can be completed in as few as four semesters after graduation (approximately 15 months).

Degree or Certificate Earned

- Master's of Science (M.S.)

Required for Program Completion

- Courses
  - 10
- Credits
  - 30
- GPA
  - 3.0

Program Goals

- Prepare students to explain Internet infrastructure and enterprise network connections.
- Prepare student to assess organizational security policies, plans and procedures and implementations.
- Prepare students to identify and assess legislation related to cybersecurity.
- Prepare students to enter specialized careers in cybersecurity.

Student Learning Outcomes

- Explain Internet structures, enterprise network structures, and consulting services related to network infrastructures
- Identify and analyze federal global legislation related to security and data threats.
- Differentiate between cybercrime, cyber espionage, and cyberwar.
- Analyze plans to protect personal, corporate and national infrastructures.
- Formulate plans for securing and analyzing digital forensic data

Code	Title	Credits
CIS 619	Crisis Management and Business Continuity	3
CYB 612	Ethics, Issues, and Government Regulations	3
CYB 604	The Computer and Internet Fraud	3
CYB 628	Cybercrime, Cyber Warfare and Cyber Espionage	3
CYB 644	Information Security	3
CYB 665	Computer Digital Forensics	3
CYB 668	Computer and Network Security	3
COM 604	Strategic Communication Research	3
Pick one course from the following:		*3*
ECF 610	Criminal Justice and Legal Concepts	
ECF 625	Litigation Support Practices and Procedures	
CIS 654	Artificial Intelligence	
CYB 880	Integrative Capstone	3
Total Credits		**30**

Course Sequence

Tentative Schedule

Course	Title	Credits
First Year		
First Semester		
CIS 619	Crisis Management and Business Continuity	3
Elective		3
	Credits	**6**
Second Semester		
COM 604	Strategic Communication Research	3
CYB 604	The Computer and Internet Fraud	3
	Credits	**6**
Third Semester		
CYB 612	Ethics, Issues, and Government Regulations	3
CYB 668	Computer and Network Security	3
	Credits	**6**
Second Year		
First Semester		
CYB 628	Cybercrime, Cyber Warfare and Cyber Espionage	3
CYB 644	Information Security	3
	Credits	**6**
Second Semester		
CYB 665	Computer Digital Forensics	3
CYB 880	Integrative Capstone	3
	Credits	**6**
	Total Credits	**30**

Course Descriptions

Cybersecurity

CYB 540 Network Theory
Lecture/theory course considers the current methods, practices, and standards used to enable communication on computer and voice networks. This includes a study of the physical layers, architectural layers, design, operation, management, and ISO standards, with particular and telephony technologies. Both local and wide area networks are examined.

CYB 604 The Computer and Internet Fraud
Computers have made organizations easier to run. All accounting information, inventory records, customer data, and intellectual property that an organization possesses is contained somewhere in an electronic file. As such, these electronic files are vulnerable to attacks from both employees and outsiders from around the world. This course will provide the student with an understanding of how computer fraud and manipulation is accomplished and what security measures should be instituted to prevent it.

CYB 612 Ethics, Issues, and Government Regulations
This course considers privacy both on- and off-line; legal background of intellectual property and e-mail; ethics and codes of ethics; effects of computers on work and society; and responsibilities and risks of computing, including topics such as accuracy of information, e-waste, and multitasking. This course includes an examination of government policies and regulations related to data security and information assurance.

CYB 628 Cybercrime, Cyber Warfare and Cyber Espionage
This course introduces students to the differences between cybercrime, cyber espionage, and cyber warfare by discussing the relationship of cyber intrusions and cybersecurity to nations, businesses, society, and people. Students will use case studies to analyze the threats, vulnerabilities and risks present in these environments, and develop strategies to reduce the breaches and mitigate the damages.

CYB 644 Information Security
This course explores all aspects of computing and communications security, including policy, authentication, authorization, administration, and business resumption planning. It examines key security technologies, such as encryption, firewalls, public-key infrastructures, smart cards, and related technologies that support the development of an overall security architecture. Coursework includes plans for developing and implementing a technology security strategy focused on business needs.
Prerequisite(s): CIS 540

CYB 652 Leadership Assessment and Evaluation
This experiential course emphasizes the importance of feedback and self- assessment for leadership development. It includes extensive assessment of each participant's management style and skills based on self-evaluations (using structured questionnaires) and feedback from coworkers, faculty, and other participants. Leadership development experiences emphasize time and stress management, individual and group problem-solving, communication, power and influence, motivation, conflict management, empowerment, and team leadership. Each participant identifies skills he or she needs to develop and reports on efforts to develop those skills.

CYB 665 Computer Digital Forensics
This course examines techniques used to conduct computer crime investigations and gather probative evidence to secure a conviction under state and federal laws. Students will simulate a computer forensic investigation: developing an investigation plan, securing the crime scene, analyzing evidence, preparing the case for court, and testifying in a moot court situation.

CYB 668 Computer and Network Security
Students will study and implement basic computer and network security strategies on Window and Linux networks. Students examine and analyze network traffic, including investigating wireless transmission, install firewalls and define Internet Protocol Security Controls (IPSEC). Labs include system hardening, dissecting network packet structure and creating encryption formats; managing authentication and access controls. Students study implementing a public key infrastructure and best strategies for using intrusion detection systems.

CYB 880 Integrative Capstone
The capstone project is an opportunity to pursue an independent learning experience focused on a specific aspect of economic crime forensics based on the student interest. The capstone is intended to extend students beyond the coursework and cases to apply knowledge in ways that are relevant to their professional goals. Students will work on a research project or in an experiential learning environment. Each student will be required to present his/her capstone both as an oral presentation and a summary written document. Students are expected to complete the capstone with a grade of B or better in order to graduate from the program.

Computer Information Science

CIS 523 Data Processing and Database Management
This course entails analysis and evaluation of database designs in relation to the strategic mission of the project. Topics include database systems, database architectures, and data-definition and data-manipulation languages. Also included are logical and physical database design, database models (e.g., entity-relationship, relational), normalization, integrity, query languages including SQL, and relational algebra, in addition to social and ethical considerations and privacy of data. This course incorporates case studies and a project using a relational DBMS.

CIS 619 Crisis Management and Business Continuity
This course explores the area of Risk Management with particular emphasis on Business Continuity Management. Risk Management involves assessing threats which may lead to disastrous events, evaluating control alternatives and implementing solutions. Potential threats include terrorist, criminal, industrial, natural, technological, environmental, economic and political. Practical solutions to enable an organization to protect assets, mitigate risk, manage crisis and recover after a disaster will be discussed. The role of business and government will be explored, as well as professional practices, standards and strategies. The course is designed to expose the student to all aspects of a holistic Business Continuity & Crisis Management program and to determine the most appropriate requirements.

CIS 633 Data Analysis with R
This course will require students to learn the R programming language and assess how to use it and find interesting features in data. Students will learn about R and statistical best practices and how to display data in a manner that will help you explain your findings to those who do not have a technical background. Moreover, the course introduces students to modeling and simulation. Topics may include basic queueing theory, the role of random numbers in simulations, and the identification of input probability distributions.

CIS 654 Artificial Intelligence
This course introduces students to the field of artificial intelligence (AI). Students will learn how big data and data mining techniques are utilized by machines to create the AI models used by autonomous aircraft and automobiles, personal assistants, IT security software, fraud investigations and credit bureaus. The course will review the history, present day use, and future of artificial intelligence. Through case studies and current events, students will examine the benefits and risks associated with AI. The course will cover issues related to AI and privacy, ethics, and machine bias. Neuromorphic computing, the Open Neural Network Exchange (ONNX), and data analytics will also be discussed.

CIS 658 Data Mining
This course introduces the field of data mining, with specific emphasis on its use for Machine Learning algorithms. Techniques covered may include conceptual clustering, learning decision rules and decision trees, case-based reasoning, Bayesian analysis, genetic algorithms, and neural networks. The course covers data preparation and analysis of results. Skills in Microsoft Excel are useful. Prerequisite(s): CIS 523

Faculty

Program Director: Yang Wang, Ph.D.
Associate Professors: Blum, Highley, Wang
Assistant Professors: Waldron, Yin
Lecturers: Casey, Hilkowitz, McCoey, McGinley, Monaghan, Walters

Program Contact Information

If you have any questions regarding the Cybersecurity program, please contact:

Holroyd Hall, Room 123
gradcis@lasalle.edu
(215) 951-1222

Staff Contact Information

Yang Wang, Ph.D.
Program Director
Holroyd Hall, Room 123
wang@lasalle.edu
(215) 951-1222