GRADUATE PROGRAM

UNIVERSITY OF DETROIT MERCY

CYBERSECURITY

M.S. IN INFORMATION ASSURANCE | MAJOR: CYBERSECURITY

Detroit Mercy's Master of Science in Information Assurance with a major in Cybersecurity is a multi-disciplinary 30-credit-hour graduate degree. It is designed to produce a comprehensively knowledgeable cybersecurity professional. The aim is to produce capable and rigorously educated leaders to engage in the serious business of protecting the nation's information infrastructure.

Protection of America's critical infrastructure is an emerging national priority. Due to its implications for national security, the responsibility for this program has been placed jointly with the National Security Agency (NSA) and the U.S. Department of Homeland Security. Universities who meet the rigorous criteria established by these two federal agencies are granted designations as Centers of Excellence in IA education. This is a highly competitive annual process involving rigorous review of the target curriculum by national experts.

In 2016, our program received a new category for designation as a National Center of Academic Excellence in Cyber Defense Education (CAE-CDE).

Approximately 200 top colleges and universities across 44 states, the District of Columbia, and the Commonwealth of Puerto Rico are designated CAEs for cyber-related degree programs. CAE graduates help protect national security information systems, commercial networks, and critical information infrastructure in the private and public sectors. University of Detroit Mercy's curriculum received its Center of Excellence (CAE/IAE) designation in 2004 and has maintained it through 2016. In 2016 our program received designation as a National Center of Academic Excellence in Cyber Defense Education (CAE-CDE). This is a four-year designation approved through 2021.

The Future of the Field

The title of our degree reflects University of Detroit Mercy's early involvement with the field. It was termed "Information Assurance" back in 2003. As the profession evolved, the term "information assurance" is now more commonly referred to as "cybersecurity", but the content and purpose of our degree remains the same. Information Assurance is the key means of defense against terrorist threats to homeland security and it is also of vital importance to businesses and organizations concerned about protecting their cyber assets. According to the National Initiative for Cybersecurity Careers and Studies, the official website of the Department of Homeland Security, approximately one in five Americans has been the victim of a cybercrime and the economic impact of these attacks can cost an average U.S. company more than $15 million annually. Cybersecurity professionals are in great demand to defend our networks and infrastructure. According to the NICSS, cybersecurity professionals report an average salary of $116,00, which is almost three times the national average.

Online Program

This program is available as an online course of study which is ideal for individuals who are balancing multiple commitments and can't meet at regular class times. Detroit Mercy's online programs come at a substantial cost savings over traditional in person classes.

Website: udmercy.edu/cyber

Rita Barrios, Ph.D
Department Chair
Email: barriosrm@udmercy.edu
Phone: 313-993-3338

Daniel Shoemaker, Ph.D
Program Director
Email: shoemadp@udmercy.edu
Phone: 313-993-1053

Theresa Carson
Graduate Admissions Counselor
Email: carsonta@udmercy.edu
Phone: 313-993-3309

GRADUATE PROGRAM

UNIVERSITY OF DETROIT MERCY

CYBERSECURITY

M.S. IN INFORMATION ASSURANCE | MAJOR: CYBERSECURITY

CURRICULUM

Required (27 credits)

CYBE 5700 Principles of Cybersecurity
CYBE 5720 Incident Response
CYBE 5730 Cyberlaw
CYBE 5740 Secure Acquisition
CYBE 5750 Cybersecurity Technologies
CYBE 5770 Cyber Defense Operations
CYBE 5780 Risk Management Processes
CYBE 5790 Cybersecurity Management Processes
CYBE 5910 Information Audit

Electives (choose 1 from the list below)

CYBE 5200 Specification
CYBE 5300 Software Assurance
CYBE 5580 System Forensics
CYBE 5710 Ethical Hacking
CYBE 5800 Advanced Topics in Cybersecurity
CYBE 5900 Security Analyst

Total: 30 credit hours

Admission Materials

Applicants for this program must submit the following:

- A University of Detroit Mercy Graduate Application Form and application fee;
- Official transcripts for all previous academic work;
- Any other information that the applicant feels is important to the admission decision.

Degree Requirements

A degree candidate for the Master of Science in Information Assurance must complete 30 credit hours which is comprised of nine core courses and one elective.

Submit Your Application Online

1. Go to udmercy.edu/admission/apply.php

Notes

We know you will have some questions. Write them here and send us an email or give us a call. We'd love to speak with you!

UNIVERSITY OF DETROIT MERCY

CYBERSECURITY

M.S. IN INFORMATION ASSURANCE | MAJOR: CYBERSECURITY

COURSE DESCRIPTIONS

Required Courses

CYBE 5700 Principles of Cybersecurity

This course will present the process, tools, and methodologies used when responding in real-time to computer security incidents. It will present an overview of pre-incident preparation, initial response procedures, and the formulation of responses. Special attention will be paid to identifying and assessing risk in the appropriate context as well as escalation and notification procedures. Students will produce and present a semester project to demonstrate mastery of processes, tools, and methodologies. Literature reviews will be conducted on legal and regulatory issues related to incident response.

CYBE 5720 Incident Response

Focuses on abstraction and object based modeling. Students will develop and design programs using the UDL and an object based programming language. The student of this course will have the ability to conceptualize and clearly communicate concrete models of abstract structures.

CYBE 5730 Cyberlaw

The purpose of this course is to educate students in the criminal and civil processes that underwrite legal and regulatory compliance in cyberspace. It will present and evaluate a range of legal concepts and models for that purpose; including all of the elements necessary to ensure the contractual compliance with information security.

CYBE 5740 Secure Acquisition

Secure acquisition is a management/technical discipline that ensures the integrity of purchased systems and networks. Secure acquisition ensures that all purchasing risks and single points of failure are identified and mitigated to a sufficient level of satisfaction for all of the stakeholders up and down the supply chain. Secure acquisition is built around a strategic, enterprise level planning and control process. Secure acquisition is widely thought to be a function of generic risk management and technical assurance. However, because of the multifaceted environment it operates in, secure acquisition involves a much more comprehensive set of basic activities than simple software assurance. Mitigation development and deployment of a secure acquisition process involves a range of academic disciplines from governance, to specification and analysis, legal and regulatory compliance to knowledge management and testing.

Secure acquisition processes are typically industry specific in their particulars. Because of that focus of this course, which is cyber defense, the end-product will be a process engineering plan for a model case (provided) that will incorporate the life-cycle process recommendations of the ISO 12207-2008 Standard. These recommendations will be integrated into a single coherent system for the assurance of secure purchased hardware and software products and services. Acquisition assurance is typically established at three levels in the organization, strategic process, project infrastructure and measures for individual product assurance. We are going to examine all three of these from a top down perspective. We will move from the model that defines and relates all of these processes, through the specific itemization of the activities and tasks embodied within this model, down to specific practices used to identify, validate, and resolve supply chain issues.

UNIVERSITY OF DETROIT MERCY

CYBERSECURITY

M.S. IN INFORMATION ASSURANCE | MAJOR: CYBERSECURITY

COURSE DESCRIPTIONS, continued

Required Courses

CYBE 5750 Cybersecurity Technologies

This course presents the fundamental concepts that underlie the deployment of a fully functional electronic countermeasure response. As such, it concentrates on those areas that ensure electronic security. These include network assurance, cryptology, and operating system and application assurance. At the end of this course the student will be able to create and maintain a defense-in-depth solution that will meet the protection needs as well as the resource realities of any organization.

CYBE 5770 Cyber Defense Operations

This course presents the fundamental concepts and KSAs that underlie the deployment of a fully functional cyber defense response. As such, it concentrates on those areas that ensure security of organizational operations. These include software, systems and network assurance, cryptology and operating system and application assurance, as well as more general areas of operation such as data bases, and legal and ethical compliance. All of this is dictated in the detailed knowledge, skill and ability (KSA) requirements of the National Security Agency's cyber defense criteria.

In addition to the detailed content in each of these areas, this course will explore several adjunct bodies of knowledge that are necessary to ensure a secure operation, such as policy, procedure and planning. The purpose of each of these contextual areas is to establish the exact status of and assure some aspect of a fully functioning cyber defense system. Students learn what each of these are and how they inter-relate in the applied universe. They will also learn how to work in a team to tailor out as well as deploy a complete and systematic array of cyber defense countermeasures for each relevant area.

The aim of this course is to produce a student who is fully competent to secure the cyber defenses of an organization; including its systems, networks and software and the information that transitions those processed. In order to do this the student must master all aspects of the process of analyzing, designing, planning and implementing comprehensive defenses in depth for these elements.

That includes attack categorization, threat identification, risk mitigation decision-making, deployment, and assessment of the appropriate set of controls for the traditional areas of cyber operations security. The final product of this course will be able to maintain a competent secure space that meets both the protection needs as well as the resource realities of the organization.

CYBE 5780 Risk Management Processes

This course presents the fundamental concepts of comprehensive lifecycle security risk management. The content is presented at a mastery level of understanding. It is rooted in several bodies of knowledge. The purpose of each of these is to establish the exact status of and ensure the containment and mitigation some aspect of organizational risk. You will learn what each of these are and how they relate.

UNIVERSITY OF DETROIT MERCY

CYBERSECURITY

M.S. IN INFORMATION ASSURANCE | MAJOR: CYBERSECURITY

COURSE DESCRIPTIONS

Required Courses, continued

CYBE 5790 Cybersecurity Management Processes

This course presents the managerial countermeasure areas that are part of the information assurance life cycle. These areas encompass every relevant topic in legal and regulatory compliance, physical and personnel security, business continuity and disaster recovery and secure development. The student will learn the details of each of these areas as well as how they interrelate. Students will also learn how to tailor a governance infrastructure as well as deploy appropriately tailored countermeasures to ensure organizational security.

CYBE 5910 Information Audit

This course presents the fundamental concepts of the IT audit and control process. The purpose is to establish the exact status of an IT operation. Students will create an audit based control structure, establish systematic accounting and control procedures and build complete and coherent information assurance capability into the IT function. This will revolve around defining a control framework, the attendant control objectives and the reporting system for an organization. Guidance for carrying this out will be provided in the form of expert models; however, the primary example that will be employed is ISACA's COBIT open standard. The end product of this course should be fully capable of structuring and performing Sarbanes-Oxley, HIPAA and Basel 2 audit programs.

Electives

CYBE 5200 Specification

This course concentrates on the BOK necessary to do effective requirements specification and development of a Software Requirements Specification (SRS). Emphasis is on formal specification approaches, methods and standards. This course is for Information Assurance Cybersecurity students.

CYBE 5300 Software Assurance

This course presents the principles and methods necessary to assure software. It covers all aspects of the assurance life cycle as embodied in the current set of proven best practices for acquiring, developing, and sustaining secure code.

CYBE 5580 System Forensics

This course presents the legal concerns, investigation techniques and incident response tactics of forensic investigation and forensic auditing. It centers around the basic operating system concepts that underlie this area. Students will learn evidence gathering and presentation techniques based around the Windows Incident Response Collection Report (IRCR). They will also learn how to employ IDS and CERT for effective incident response. Students will study the real-world investigation issues and concepts developed through the Honeynet Project.

UNIVERSITY OF DETROIT MERCY

CYBERSECURITY

M.S. IN INFORMATION ASSURANCE | MAJOR: CYBERSECURITY

COURSE DESCRIPTIONS

Electives, continued

CYBE 5710 Ethical Hacking
This course covers particular genres of cyber attack tools and techniques, examining the most widely used and most damaging tools from each category. Ways to design and implement the most effective defenses to ensure the confidentiality, availability, and integrity of software systems and data will be explored both in lecture and in laboratory exercises with state of the art equipment. Emphasis will be placed on ethical and professional conduct. Exploration of the role of industry, government, and academia in cyber security will be facilitated through guest lectures. Students will conduct a semester project to demonstrate mastery of the ethical hacking process. Literature Reviews will be conducted on contemporary breaches.

CYBE 5800 Special Topics in Cybersecurity
Discussion of current leading-edge topics in Cybersecurity.

CYBE 5900 Security Analyst
The Certified Security Analyst program explores the analytical phase of ethical hacking while focusing on how to identify and mitigate security risks to infrastructure. The program provides training on how to analyze the results of vulnerability assessments.

SAMPLE COURSE ROTATION - ONE CALENDAR YEAR
Please note that elective availability is subject to change each semester.

Fall
CYBE 5700 Principles of Cybersecurity
CYBE 5730 Cyberlaw
CYBE 5780 Risk Management Processes

Winter
CYBE 5750 Cybersecurity Technologies
CYBE 5770 Cyber Defense Operations
CYBE 5790 Cybersecurity Management Processes
CYBE 5900 Security Analyst (elective)

Summer I
CYBE 5720 Incident Response
CYBE 5910 Information Audit
CYBE 5200 Specification (elective)

Summer II
CYBE 5740 Secure Acquisition
CYBE 5800 Special Topics (elective)
CYBE 5300 Software Assurance (elective)