CYBERSECURITY ENGINEERING (M.S.)

https://manchester.unh.edu/program/ms/cybersecurity-engineering

Description

This program is offered in Manchester.

Cybersecurity touches nearly every facet of an organization. From marketing to legal to finance, employees across the industry are more aware of the flow of data and the measures needed to keep it secure. Technical systems need technical solutions—which is why the University of New Hampshire has launched a Master of Science in Cybersecurity Engineering.

Designed for working professionals and those with a strong interest in cybersecurity, the program combines in-class and online learning on how to develop, engineer and operate secure information systems. You will learn the theoretical underpinnings of information security and have opportunities to apply your knowledge and skills to real-world scenarios and authentic project experiences.

With a greater emphasis on the collection and storage of big data, information security and cloud computing, the demand for cybersecurity engineers has never been higher. The M.S. in Cybersecurity Engineering gives you the technical skills and experience to meet that demand, preparing you to secure information, communications, networks and control systems for any organization.

Career Opportunities

Graduates of the Cybersecurity Engineering program are able to identify, analyze and respond to the complex information security threats that are increasingly common in today's digital landscape. You'll learn skills in core and advanced information security, preparing you to develop, integrate and evaluate secure IT systems and services for any organization.

Requirements

The M.S. in Cybersecurity Engineering program will have two options:

- The Capstone option requires the completion of 11 courses (**33 credits**). The capstone is a work-based project, internship experience or other appropriate activity that integrates the skills and knowledge you developed during the degree program, along with your past experiences, areas of specialization and professional goals. In consultation with an advisor, each student develops a project plan and prepares and delivers a final project agreed upon by the student and advisor.
- The Thesis option consists of 10 courses (**30 credits**) including 6 credits of COMP 899 Master's Thesis (counts as 2 courses) and requires you to research, write and defend a publishable-quality, graduate-level paper. The thesis track is designed for students who may be interested in pursuing further studies (i.e., a doctoral experience).

Code	Title	Credits
Required Courses		
COMP 815	Information Security	3
COMP 835	Secure Networking Technologies	3
COMP 880	Topics (Software Security Principles)	3
COMP 880	Topics (Computer Forensics)	3
COMP 880	Topics (Cryptography)	3
One (1) 3-credit policy course from the following:		**3**
CPRM 810	Foundations of Cybersecurity Policy	
CPRM 830	Security Measures I	
CPRM 850	Security Measures II	
CPRM 870	Cybersecurity Risk Management	
CPRM 880	Cybersecurity Metrics and Evaluation	
Internship [1]		
COMP 890	Internship and Career Planning	1-3
or COMP 891	Internship Practice	
or COMP 892	Applied Research Internship	
One (1) elective course for Thesis Option or three (3) elective courses for Capstone Option:		
COMP 805	Full Stack Development	
COMP 820	Database Systems and Technologies	
COMP 821	Big Data for Data Engineers	
COMP 825	Programming Languages	
COMP 830	Software Development	
COMP 840	Machine Learning Applications and Tools	
COMP 850	Neural Networks	
COMP 851	System Integration and Architecture	
COMP 860	Data Visualization & Communication	
COMP 880	Topics	
Capstone Project		
COMP 898	Master's Project	3
or		
COMP 899	Master's Thesis	6

1 Students are required to enroll in at least one credit of internship experience by enrolling in COMP 890 or COMP 891 or COMP 892 upon successful completion of nine credits in their program of study. COMP 891 and COMP 892 may be repeated for a maximum of 6 credits.

Student Learning Outcomes

- Analyze complex computing problems and identify solutions by applying principles of computing.
- Design, implement, and evaluate computing solutions that meet computing requirements with focus on security aspects.
- Communicate effectively in a variety of professional contexts.
- Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.
- Function effectively as a member or leader of a team engaged in IT activities.
- Apply security principles and practices to maintain operations in the presence of risks and threats.