# 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).

### Accelerated Master's

This graduate program is approved to be taken on an accelerated basis in articulation with certain undergraduate degree programs.

General Accelerated Master's policy, note that some programs have additional requirements (e.g. higher grade expectations) compared to the policy.

Please see the Graduate School website and contact the department directly for more information.

## 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.

### Code Title Credits

<table>
<thead>
<tr>
<th>Required Courses</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>COMP 815</td>
<td>Information Security</td>
</tr>
</tbody>
</table>

### One (1) 3-credit policy course from the following:

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPRM 810</td>
<td>Foundations of Cybersecurity Policy</td>
</tr>
<tr>
<td>CPRM 830</td>
<td>Security Measures I</td>
</tr>
<tr>
<td>CPRM 850</td>
<td>Security Measures II</td>
</tr>
<tr>
<td>CPRM 870</td>
<td>Cybersecurity Risk Management</td>
</tr>
<tr>
<td>CPRM 880</td>
<td>Cybersecurity Metrics and Evaluation</td>
</tr>
</tbody>
</table>

### Professional Experience

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMP 801</td>
<td>Integrated Computing Practice</td>
</tr>
<tr>
<td></td>
<td>Internship (Select from the following) 2</td>
</tr>
</tbody>
</table>

### Elective Courses

- Select 1 course (3 credits) for Thesis Option or 3 courses (9 credits) for Project Option

### Topics

- Secure Networking Technologies
- Topics (Software Security Principles)
- Topics (Computer Forensics)
- Topics (Cryptography)
- Foundations of Cybersecurity Policy
- Security Measures I
- Security Measures II
- Cybersecurity Risk Management
- Cybersecurity Metrics and Evaluation

### Internship

Students are required to enroll in at least 1 credit of Professional Experience upon successful completion of nine credits in the program. COMP 891 Internship Practice and COMP 892 Applied Research Internship may be repeated for a maximum of 6 credits.
• 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.