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

- Organization.
- To develop, integrate and evaluate secure IT systems and services for any organization.
- To learn skills in core and advanced information security, preparing you for the complex information security threats that are increasingly common in today’s digital landscape. You’ll analyze and respond to the complex information security threats.
- Graduates of the Cybersecurity Engineering program are able to identify, control systems for any organization.
- Preparing you to secure information, communications, networks and critical systems for any organization.
- Giving you the technical skills and experience to meet that demand, 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 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.

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).

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMP 815</td>
<td>Information Security</td>
<td>3</td>
</tr>
<tr>
<td>COMP 820</td>
<td>Topics (Software Security Principles)</td>
<td>3</td>
</tr>
<tr>
<td>COMP 820</td>
<td>Topics (Computer Forensics)</td>
<td>3</td>
</tr>
<tr>
<td>COMP 820</td>
<td>Topics (Cryptography)</td>
<td>3</td>
</tr>
</tbody>
</table>

- One (1) 3-credit policy course from the following:
- COMP 810 Foundations of Cybersecurity Policy
- COMP 830 Security Measures I
- COMP 850 Security Measures II
- COMP 870 Cybersecurity Risk Management
- COMP 880 Cybersecurity Metrics and Evaluation

Professional Experience

In the Capstone option, 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.

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.
• 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.