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).

**Required Courses**

<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>
</tbody>
</table>

**Electives**

- The Thesis option requires 1-3 credits 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.