CYBERSECURITY, MS

School of Interdisciplinary Informatics, College of Information, Science & Technology

Vision Statement
The School of Interdisciplinary Informatics (Si2) is the academic home of the Master of Science (MS) in cybersecurity (previously information assurance). Cybersecurity is a rapidly expanding, multi-faceted science that integrates a diverse set of disciplines to address fundamental problems in the design, development, implementation and support of secure information systems. The Master of Science is a full graduate degree program balancing theory with practice in order to provide students with the knowledge and skills necessary to protect information systems. Because of the wide variety of subject areas to which cybersecurity can be applied, this degree program has two paths; cyber operations, a concentration with highly technical content, and interdisciplinary, with the opportunity for the students to tailor the degree to specific management goals. Students may also choose between a thesis or capstone exit option based on their individual interests.

Program Contact Information
Matt Hale, PhD, Graduate Program Chair (GPC)
174D Peter Kiewit Institute (PKI)
402.554.3978
mhale@unomaha.edu

Carlee Heylmun
176C Peter Kiewit Institute (PKI)
402.554.3819
carleepbrown@unomaha.edu


Other Program Related Information

Fast Track
The College of Information Science & Technology has developed a Fast Track program for highly qualified and motivated students providing the opportunity to complete a bachelor’s degree and a master’s degree in an accelerated time frame. With Fast Track, students may count up to 9 (nine) graduate credit hours toward the completion of their undergraduate program as well as the graduate degree program. Students will work with both undergraduate and graduate advisors to ensure graduate classes selected will count toward both programs, should a student wish to earn a graduate degree in a separate CIST area than their undergraduate degree.

Program Specifics:

• This program is available for undergraduate students pursuing any CIST undergraduate degree desiring to pursue an MS in either the same or a related CIST field.
• Students must have completed no less than 60 undergraduate hours.
• Students must have a minimum undergraduate GPA of 3.0, with the exception of Computer Science, which requires a minimum undergraduate GPA of 3.5.
• Students must complete the Fast Track Approval form and obtain all signatures and submit to the Office of Graduate Studies prior to first enrollment in a graduate course.
• Students will work with their undergraduate advisor to register for the graduate courses.
• A minimum cumulative GPA of 3.0 in the graduate coursework is required to remain in good standing.

• Students remain undergraduates until they meet all the requirements for the undergraduate degree and are eligible for all rights and privileges granted undergraduate status including financial aid.

Admissions
General Application Requirements and Admission Criteria (http://catalog.unomaha.edu/graduate/admission/)

Program-Specific Requirements
Application Deadlines (Spring 2022, Summer 2022, and Fall 2022)

• Fall: July 1
• Spring: December 1
• Summer: April 1

Other Requirements

• The minimum undergraduate grade point average (GPA) requirement for the MS in Cybersecurity program is 3.0 or equivalent score on a 4.0 scale. Applicants should have the equivalent of a four-year undergraduate degree.
• Entrance Exam: International applicants without a baccalaureate or equivalent degree from the United States are required to submit GRE scores. There is no minimum GRE requirement, but for international applicants the score will be one factor used in evaluating the student’s portfolio.
• English Language Proficiency: Applicants are required to have a command of oral and written English. Those who do not hold a baccalaureate or other advanced degree from the United States OR a baccalaureate or other advanced degree from a predetermined country on the waiver list, must meet the minimum language proficiency score requirement in order to be considered for admission. Minimum acceptable scores are:
• Statement of Purpose: a two-page, double-spaced, word-processed essay that addresses the following two topics:
  - Discussion of two accomplishments that demonstrate your potential for success in the graduate program
  - Discussion of your unique personal qualities and life experiences that distinguish you from other applicants to this graduate program
• Resume: Submit a detailed resume indicating your work experience and background.
• Letters of Recommendation: At least one but no more than three letters of recommendation from references who can evaluate your work and/or academic achievements.
• Applicants with International Transcripts: Any applicant to this program who has completed undergraduate or graduate coursework at an international higher education institution outside of the United States may submit transcripts and degree certificates (with an English translation) in lieu of a course-by-course transcript evaluation from World Education Services (https://www.wes.org/) (WES), Educational...
Credential Evaluators (https://www.ece.org/) (ECE), or Educational Perspectives (https://www.edperspective.org/). This graduate program will conduct an in-house credential evaluation of your transcript(s).

- UNO reserves the right to require a course-by-course evaluation from WES, ECE, or Educational Perspectives if the program is unable to complete an evaluation or should there be any questions or concerns about the documentation that is received. The applicant will be notified by the individual program if an external course-by-course evaluation is required.
- *Note: If admitted, official transcripts and degree certificates (with an English translation) official course-by-course transcript evaluation, and any applicable official exam scores are required.
- Interview (optional): Although not required, the graduate program committee may ask to conduct a telephone interview to further assess the experiences of the applicant.

**Requirements**

**Foundation Courses**

Foundation courses ensure that all students in the degree have a solid groundwork upon which to build the rest of the program. These courses not only provide essential prerequisite knowledge and skills for other courses in the program, but they also contain a distinct body of knowledge that is an important part of the cybersecurity professional’s education. All foundation courses are required for all students, however, students who have obtained an undergraduate degree in a related field may already have this foundation. In such a case, most, if not all, foundation courses are waived. Students with undergraduate degrees in other disciplines, including computer science, management information systems, or engineering, will usually require one or more foundation courses. Occasionally, a student’s work experience may be sufficient to waive one or more of the foundation courses.

Waivers for foundation courses are potentially granted by the graduate program committee upon the recommendation of the faculty member who is responsible for an individual course. Students requesting a waiver for a particular course should be prepared to meet with a faculty member and answer questions in the area of the course. They should bring to the meeting any relevant transcripts, course syllabi, course material, or evidence of practical experience. Some foundation courses may have an option for testing out.

Foundation courses cannot be used to satisfy the 33 semester hours required for the MS in Cybersecurity (CYBR) degree. Students who have not completed all the foundation course requirements may be admitted on a provisional status until those requirements have been completed. All foundation courses must be completed prior to or concurrent with the first six (6) hours of MS in CYBR graduate coursework.

**Foundation Courses**

(Nine hours if not waived)

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCI 2240</td>
<td>INTRODUCTION TO C PROGRAMMING</td>
<td>3</td>
</tr>
<tr>
<td>or CYBR 2250</td>
<td>LOW-LEVEL PROGRAMMING</td>
<td></td>
</tr>
<tr>
<td>CYBR 2600</td>
<td>SYSTEM ADMINISTRATION</td>
<td>3</td>
</tr>
<tr>
<td>CSCI 3550</td>
<td>COMMUNICATION NETWORKS</td>
<td>3</td>
</tr>
<tr>
<td>or ISQA 3400</td>
<td>INFORMATION TECHNOLOGY INFRASTRUCTURE</td>
<td></td>
</tr>
</tbody>
</table>

**Total Credits:** 9

**Degree Requirements**

**Capstone Option**

<table>
<thead>
<tr>
<th>Core Courses</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBR 8366</td>
<td>FOUNDATIONS OF CYBERSECURITY</td>
<td>3</td>
</tr>
<tr>
<td>or CSCI 8366</td>
<td>FOUNDATIONS OF CYBERSECURITY</td>
<td></td>
</tr>
<tr>
<td>CYBR 8410</td>
<td>CRYPTOGRAPHY AND NETWORK SECURITY</td>
<td>3</td>
</tr>
<tr>
<td>or CSCI 8410</td>
<td>CRYPTOGRAPHY AND NETWORK SECURITY</td>
<td></td>
</tr>
<tr>
<td>CYBR 8420</td>
<td>SOFTWARE ASSURANCE</td>
<td>3</td>
</tr>
<tr>
<td>or CSCI 8420</td>
<td>SOFTWARE ASSURANCE</td>
<td></td>
</tr>
<tr>
<td>CYBR 8490</td>
<td>CYBER INVESTIGATIONS</td>
<td>3</td>
</tr>
</tbody>
</table>

**Concentration**

Select a concentration 18

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBR 8950</td>
<td>GRADUATE CAPSTONE IN INFORMATION ASSURANCE</td>
<td>3</td>
</tr>
</tbody>
</table>

**Total Credits:** 33

**Thesis Option**

<table>
<thead>
<tr>
<th>Core Courses</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBR 8366</td>
<td>FOUNDATIONS OF CYBERSECURITY</td>
<td>3</td>
</tr>
<tr>
<td>or CSCI 8366</td>
<td>FOUNDATIONS OF CYBERSECURITY</td>
<td></td>
</tr>
<tr>
<td>CYBR 8410</td>
<td>CRYPTOGRAPHY AND NETWORK SECURITY</td>
<td>3</td>
</tr>
<tr>
<td>or CSCI 8410</td>
<td>CRYPTOGRAPHY AND NETWORK SECURITY</td>
<td></td>
</tr>
<tr>
<td>CYBR 8420</td>
<td>SOFTWARE ASSURANCE</td>
<td>3</td>
</tr>
<tr>
<td>or CSCI 8420</td>
<td>SOFTWARE ASSURANCE</td>
<td></td>
</tr>
<tr>
<td>CYBR 8490</td>
<td>CYBER INVESTIGATIONS</td>
<td>3</td>
</tr>
</tbody>
</table>

**Concentration**

Select a concentration 15

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBR 8990</td>
<td>THESIS IN CYBERSECURITY</td>
<td>6</td>
</tr>
</tbody>
</table>

**Total Credits:** 33

**Exit Requirements:**

- Capstone 3 Credits CYBR 8950
- Thesis 6 Credits CYBR 8990
  - All candidates should carefully review the Graduate College requirements for forming a supervisory committee, Thesis/Thesis Equivalent Proposal Approval forms and final approval and submission of a thesis.

**Cyber Operations Concentration**

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBR 8000</td>
<td>CENTER OF ACADEMIC EXCELLENCE: CYBER OPERATIONS COMPLETION CERTIFICATE</td>
<td></td>
</tr>
</tbody>
</table>

**Electives**

Select 18 hours from the following: 18

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBR 8396</td>
<td>MOBILE DEVICE FORENSICS</td>
<td></td>
</tr>
<tr>
<td>CYBR 8436</td>
<td>QUANTUM COMPUTING AND CRYPTOGRAPHY</td>
<td></td>
</tr>
<tr>
<td>CYBR 8440</td>
<td>SECURE SYSTEMS ENGINEERING</td>
<td></td>
</tr>
<tr>
<td>CYBR 8446</td>
<td>INDUSTRIAL CONTROL SYSTEM SECURITY</td>
<td></td>
</tr>
<tr>
<td>CYBR 8450</td>
<td>APPLIED CRYPTOGRAPHY</td>
<td></td>
</tr>
</tbody>
</table>
Interdisciplinary Concentration

A maximum of five cross-listed courses (courses ending in 8xx6) can be included on a plan of study for the MS in CYBR degree.

Electives

Select 18 hours from the following:

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISQA 8080</td>
<td>RESEARCH IN MIS</td>
<td></td>
</tr>
<tr>
<td>ISQA 8080</td>
<td>SEMINAR IN MANAGEMENT INFORMATION SYSTEMS</td>
<td></td>
</tr>
<tr>
<td>ISQA 8530</td>
<td>E-COMMERCE SECURITY</td>
<td></td>
</tr>
<tr>
<td>ISQA 8546</td>
<td>COMPUTER SECURITY MANAGEMENT</td>
<td></td>
</tr>
<tr>
<td>ISQA 8560</td>
<td>INFORMATION WARFARE AND SECURITY</td>
<td></td>
</tr>
<tr>
<td>ISQA/CYBR 8570</td>
<td>INFORMATION SECURITY POLICY AND ETHICS</td>
<td></td>
</tr>
<tr>
<td>ISQA 8580</td>
<td>SECURITY RISK MANAGEMENT AND ASSESSMENT</td>
<td></td>
</tr>
<tr>
<td>ISQA 8596</td>
<td>IT AUDIT AND CONTROL</td>
<td></td>
</tr>
<tr>
<td>CSCI 8340</td>
<td>DATABASE MANAGEMENT SYSTEMS II</td>
<td></td>
</tr>
<tr>
<td>CSCI 8430</td>
<td>TRUSTED SYSTEM DESIGN, ANALYSIS AND DEVELOPMENT</td>
<td></td>
</tr>
<tr>
<td>CSCI 8530</td>
<td>ADVANCED OPERATING SYSTEMS</td>
<td></td>
</tr>
<tr>
<td>CSCI/MATH 8566</td>
<td>NUMBER THEORY &amp; CRYPTOGRAPHY</td>
<td></td>
</tr>
<tr>
<td>CSCI 8610</td>
<td>FAULT TOLERANT DISTRIBUTED SYSTEMS</td>
<td></td>
</tr>
<tr>
<td>CYBR 8080</td>
<td>SPECIAL TOPICS IN INFORMATION ASSURANCE</td>
<td></td>
</tr>
<tr>
<td>CYBR 8900</td>
<td>INDEPENDENT STUDY AND RESEARCH IN CYBERSECURITY</td>
<td></td>
</tr>
<tr>
<td>CYBR 8910</td>
<td>INTERNSHIP</td>
<td></td>
</tr>
<tr>
<td>CYBR 8986</td>
<td>SPECIAL TOPICS IN INFORMATION ASSURANCE</td>
<td></td>
</tr>
<tr>
<td>PSCI 8256</td>
<td>INTELLIGENCE AND NATIONAL SECURITY</td>
<td></td>
</tr>
<tr>
<td>PSCI 8266</td>
<td>INTERNATIONAL LAW</td>
<td></td>
</tr>
</tbody>
</table>

Total Credits 18

Quality of Work Standards

The Graduate College’s Quality of Work Standards shall be applied to foundation courses as well as courses taken as part of the degree program. In particular, the GPC will recommend to the Graduate College that any

1. Student receiving a grade of “C-” or below on any foundation course will be dismissed from the program or, in the case of unclassified or non-degree students, be automatically denied admission.
2. Student receiving a grade of “C+” or “C” in any foundation course will be placed on probation or dismissed from the program.
3. Student not maintaining a “B” (3.0 on a 4.0 scale) average in foundation courses will be placed on probation or dismissed from the program.