

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
mlhale@unomaha.edu

Emily Wiemers, Graduate Advisor
170 Peter Kiewit Institute (PKI)
402.554.3819
ewiemers@unomaha.edu

Program Website (<https://www.unomaha.edu/college-of-information-science-and-technology/school-of-interdisciplinary-informatics/cybersecurity/ms-cybr.php>)

Other Program Related Information

Fast Track

The School of Interdisciplinary Informatics (SI2) 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 graduate credit hours towards 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 College of Information Science & Technology (CIST) area than their undergraduate degree.

Program Specifics:

- This program is available for undergraduate students pursuing any of the following:
 - Students pursuing a CIST undergraduate degree desiring to pursue an MS in either the same or a related CIST field
 - Students pursuing a Bachelor of Multidisciplinary Studies with a concentration in cybersecurity who wish to pursue the MS in cybersecurity.
- Students must have completed no less than 60 undergraduate hours.
- Students must have a minimum undergraduate GPA of 3.0.
- 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 is required for graduate coursework 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.
- Near the end of the undergraduate program, formal application to the graduate program is required. All applicants will need to meet any other admission requirements established for the MS in selected CIST program. The application fee will be waived if the applicant contacts the Office of Graduate Studies for a fee waiver code prior to submitting the MS application.
 - Admission to Fast Track does NOT guarantee admission to the graduate program.
 - The admit term must be after the completion term of the undergraduate degree.

Admissions

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

Program-Specific Requirements

Application Deadlines (Spring 2024, Summer 2024, and Fall 2024)

- 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.
- **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:
 - Internet-based TOEFL: 80, IELTS: 6.5, PTE: 53, Duolingo: 110
- **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.
- **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 Requirements

(Nine hours if not waived)

Code	Title	Credits
CIST 1600	INTRODUCTION TO PROGRAMMING USING PRACTICAL SCRIPTING	3
or CIST 1400	INTRODUCTION TO COMPUTER SCIENCE I	
CYBR 2600	SYSTEM ADMINISTRATION	3
CSCI 3550	COMMUNICATION NETWORKS	3
or ISQA 3400	INFORMATION TECHNOLOGY INFRASTRUCTURE	
Total Credits		9

Degree Requirements

Capstone Option

Code	Title	Credits
Core Courses		
CYBR 8366	FOUNDATIONS OF CYBERSECURITY	3
or CSCI 8366	FOUNDATIONS OF CYBERSECURITY	
CYBR 8410	DISTRIBUTED SYSTEMS AND NETWORK SECURITY	3
or CSCI 8410	DISTRIBUTED SYSTEMS AND NETWORK SECURITY	
CYBR 8420	SOFTWARE ASSURANCE	3
or CSCI 8420	SOFTWARE ASSURANCE	
CYBR 8490	CYBER INVESTIGATIONS	3
Concentration		
Select a concentration		18
CYBR 8950	CYBERSECURITY GRADUATE CAPSTONE	3
Total Credits		33

Thesis Option

Code	Title	Credits
Core Courses		
CYBR 8366	FOUNDATIONS OF CYBERSECURITY	3
or CSCI 8366	FOUNDATIONS OF CYBERSECURITY	
CYBR 8410	DISTRIBUTED SYSTEMS AND NETWORK SECURITY	3
or CSCI 8410	DISTRIBUTED SYSTEMS AND NETWORK SECURITY	
CYBR 8420	SOFTWARE ASSURANCE	3

or CSCI 8420	SOFTWARE ASSURANCE	
CYBR 8490	CYBER INVESTIGATIONS	3
Concentration		
Select a concentration		15
CYBR 8990	THESIS IN CYBERSECURITY	6
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.

Concentrations

Cyber Operations Concentration

Code	Title	Credits
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:		18
CYBR 8396	MOBILE DEVICE FORENSICS	
CYBR 8436	QUANTUM COMPUTING AND CRYPTOGRAPHY	
CYBR 8446	INDUSTRIAL CONTROL SYSTEM SECURITY	
CYBR 8450	APPLIED CRYPTOGRAPHY	
CYBR 8456	HOST-BASED VULNERABILITY DISCOVERY	
CYBR 8466	NETWORK-BASED VULNERABILITY DISCOVERY	
CYBR 8470	SECURE WEB APPLICATION DEVELOPMENT	
CYBR 8480	SECURE MOBILE DEVELOPMENT	
CYBR 8546	COMPUTER SECURITY MANAGEMENT	
CYBR 8080	SPECIAL TOPICS IN CYBERSECURITY	
CYBR 8900	INDEPENDENT STUDY AND RESEARCH IN CYBERSECURITY	
CYBR 8910	INTERNSHIP	
CYBR 8986	SPECIAL TOPICS IN CYBERSECURITY	
CYBR 9460	SECURITY OF EMBEDDED SYSTEMS	
Total Credits		18

Interdisciplinary Concentration

Code	Title	Credits
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:		18
ISQA 8060	RESEARCH IN MIS	
ISQA 8080	SEMINAR IN MANAGEMENT INFORMATION SYSTEMS	
ISQA 8546	COMPUTER SECURITY MANAGEMENT	
ISQA 8560	INFORMATION WARFARE AND SECURITY	
ISQA/CYBR 8570	INFORMATION SECURITY POLICY AND ETHICS	

ISQA 8580	SECURITY RISK MANAGEMENT AND ASSESSMENT
CSCI 8340	DATABASE MANAGEMENT SYSTEMS II
CSCI 8430	TRUSTED SYSTEM DESIGN, ANALYSIS AND DEVELOPMENT
CSCI 8530	ADVANCED OPERATING SYSTEMS
CSCI/MATH 8566	NUMBER THEORY & CRYPTOGRAPHY
CSCI 8610	FAULT TOLERANT DISTRIBUTED SYSTEMS
CYBR 8080	SPECIAL TOPICS IN CYBERSECURITY
CYBR 8900	INDEPENDENT STUDY AND RESEARCH IN CYBERSECURITY
CYBR 8910	INTERNSHIP
CYBR 8986	SPECIAL TOPICS IN CYBERSECURITY
PSCI 8256	INTELLIGENCE AND NATIONAL SECURITY
PSCI 8266	INTERNATIONAL LAW

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.