CYBERSECURITY

Master of Science in Cybersecurity

The M.S. in Cybersecurity represents a comprehensive, multidisciplinary curriculum that prepares students to advance their careers and pursue their academic ambitions through leadership and management positions within the cybersecurity field. The degree represents a fully online, asynchronous curriculum comprised of 34 credits to include 7 core courses, 3 track courses, and 2 capstone courses (a one-credit capstone preparation course and a three-credit capstone course) to satisfy degree requirements. UW-Green Bay, UW-La Crosse, UW-Oshkosh, UW-Parkside, UW-Platteville, UW-River Falls, UW-Stevens Point, and UW-Superior will offer the program jointly. The program will equip students with the skills needed to effectively develop, implement and maintain a security strategy within diverse organizations and industry sectors. Core courses provide students with a solid foundation in data and network security, compliance, strategic planning, program design and management, legal and ethical issues in cybersecurity, cryptography, risk management and technical communications. Students must complete one of four unique tracks which assist students in tailoring their coursework to meet their career goals: digital forensics, cyber response, governance and leadership, and security architecture. The curriculum was developed in alignment with defined requirements of the Center for National Centers of Academic Excellence in Cyber Defense (CAE-CD) and several established and recognized industry certifications.

Student Learning Outcomes and Program Objectives

Students completing the M.S. in Cybersecurity degree will gain the following core competencies:

1. Analyze and resolve security issues in networks and computer systems to secure an IT infrastructure
2. Design, develop, test, and evaluate secure software
3. Develop policies and procedures to manage enterprise security risks
4. Evaluate and communicate the human role in security systems with an emphasis on ethics, social engineering vulnerabilities, and training
5. Interpret and forensically investigate security incidents

Admission and Program Requirements

Admission to the Master of Science in Cybersecurity program requires:

- Bachelor's degree
- 3.0 GPA
- Prerequisite coursework in:
  - Introduction to Computer Science (must include significant programming content)
  - Calculus or Statistics (Students will be required to satisfy all program prerequisites prior to formal admission into the program. Academic Directors are provided the option to waive one or more prerequisites based, in part, on student background and work experience.)
- Two letters of recommendation (can be professional or academic)
- Resume
- Up to 1,000 word statement of personal intent describing decision to pursue this degree and what you believe you will bring to the information technology field
- No required aptitude tests (GRE, GMAT, e.g.)

Provisional Admission Process

Provisional admission will be considered using the following guidelines:

- 2.5 and above at the discretion of the Academic Director and home campus
- Below 2.5 – with Academic Director Approval – student can remediate by taking two of the following MS-C introductory courses and earning a B or better in each course:

Code	Title	Hours
CYB 700	Cybersecurity Fundamentals	3.00
CYB 703	Network Security	3.00
CYB 705	Cybercrime	3.00

Faculty and Instructional Staff

Jonathan Totushek, Assistant Professor, Academic Director
Shin-Ping Tucker, Professor

Curriculum and Courses

Code	Title	Hours
Core Courses		
CYB 700	Cybersecurity Fundamentals	3.00
CYB 703	Network Security	3.00
CYB 705	Cybercrime	3.00
CYB 707	Cybersecurity Program Planning	3.00
CYB 710	Introductory Cryptography	3.00
CYB 715	IT Security Architecture	3.00
CYB 720	Cybersecurity Ethics and Communication	3.00
Track		
Select one of the following Tracks:		9.00-12.00
Track 1 - Digital Forensics		
CYB 725	Computer Forensics	
CYB 730	Computer Criminology	
CYB 735	Network Forensics	
Track 2 - Cyber Response (Defense, Incident & Attack Response)		
CYB 740	Incident Response and Remediation	
CYB 745	Secure Operating Systems	
CYB 750	Offensive Security	
Track 3 - Governance & Leadership (Communication, Management, Policy, Compliance)		
CYB 755	Security Administration	
CYB 760	Leadership & Teams	
CYB 765	Security Program Management	
Track 4 - Security Architecture (Systems, Software, Data)		
CYB 770	Security Architecture	
CYB 775	Advanced Cryptography	
CYB 780	Software Security	
CYB 785	Cyber-Physical Sys. Security	
Capstone Courses		
CYB 789	Cybersecurity Pre-capstone	1.00

CYB 790	Cybersecurity Capstone	3.00
Total Hours		**34.00-37.00**