CYBERSECURITY (MS)

Department website (https://www.uwp.edu/learn/programs/mscyb.cfm)

College: College of Business, Economics, and Computing

The online M.S. in Cybersecurity program represents a fully online fixed curriculum consisting of 34 credits – seven three-credit core courses, three courses in a concentration/track area, a one-credit capstone preparation course and a project-based capstone course. UW-Green Bay, UW-La Crosse, UW-Oshkosh, UW-Parkside, UW-Platteville, UW-River Falls, UW-Stevens Point, UW-Superior offer the program jointly. Graduates of the program will gain the core competencies required to assume a variety of roles across a wide range of industries to include cybersecurity analyst, security consultant, cybersecurity manager, computer system analyst, security application analyst, and information technology specialist. 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 to include the Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH) and CompTIA Security+ certifications. In addition to courses in key areas such as cybersecurity program planning, security risk, foundational aspects of security, the required capstone course, which represents the culminating experience in the program, will provide students with the opportunity to apply skills acquired from coursework through a project-based experience in their track/concentration area.

Goals of the Program

The degree addresses a recognized high-need area of Cybersecurity as supported by research and input from employers and industry representatives. M.S. in Cybersecurity will predominantly serve adult and nontraditional students who possess a minimum of a completed bachelor's degree, currently work in the field, and have a desire to continue their education toward a master's degree primarily to expand knowledge and specialized skills in cybersecurity. Upon completion of this degree program, students will develop advanced knowledge and skills in both technical and managerial aspects of cybersecurity. Depending on their career goals, students can choose one of the four tracks in the program --- Digital Forensics, Cyber Response, Governance and Leadership, Security Architecture --- to complete the electives.

Student Core Competencies and Learning Outcomes

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

Competency A – Analyze and resolve security issues in networks and computer systems to secure an IT infrastructure

Upon completion of the program, students will be able to:

- Interpret and analyze operating system and machine level structures
- Interpret and analyze network protocols
- Design, evaluate, and test systems including networks, computers, and hardware for security requirements

Competency B – Design, develop, test, and evaluate secure software

Upon completion of the program, students will be able to:

- Implement best practices in secure software development
- Implement effective cryptographic systems and assess their vulnerabilities
- Assess security implications for emerging software technologies

Competency C – Develop policies and procedures to manage enterprise security risks

Upon completion of the program, students will be able to:

- Conduct security risk management assessments
- Develop and implement threat management framework
- Evaluate and create security policies and processes for an organization and apply appropriate security frameworks
- Implement identity and access management controls

Competency D - Evaluate and communicate the human role in security systems with an emphasis on ethics, social engineering vulnerabilities, and training

Upon completion of the program, students will be able to:

- Assess trends in computer criminology and social behaviors related to technology use including physical security
- Engage in ethical decision-making and apply ethical principles to cybersecurity
- Engage in professional collaboration and communication with technical and nontechnical stakeholders on issues related to security

Competency E – Interpret and forensically investigate security incidents

Upon completion of the program, students will be able to:

- Develop and implement an incident response strategy
- Identify and assess attacks through forensics
- Interpret legal implications of security incidents and conduct investigations using industry best practices

Requirements for the Master of Science in Cybersecurity

Code	Title	Credits
Required Core Courses		
CYB 700	Fundamentals of Cybersecurity	3
CYB 703	Network Security	3
CYB 705	Sociological Aspects of Cybersecurity	3
CYB 707	Cybersecurity Program Planning and Implementation	3
CYB 710	Introduction to Cryptography	3
CYB 715	Managing Security Risk	3
CYB 720	Technical Communication for Cybersecurity	3
Required Capstone Courses		
CYB 789	Cybersecurity Pre-Capstone	1
CYB 790	Cybersecurity Capstone	1
Completion Options		

In addition to the core and capstone courses listed above, choose one of the concentrations listed below and complete a minimum of 9 credits in the chosen concentration.		9
Total Credits		**32**

Digital Forensics Concentration

Code	Title	Credits
Required Courses		
CYB 725	Computer Forensics and Investigations	3
CYB 730	Computer Criminology	3
CYB 735	Network Forensics	3
Total Credits		**9**

Cyber Response Concentration (Defense, Incident & Attack Response)

Code	Title	Credits
Required Courses		
CYB 740	Incident Response and Remediation	3
CYB 745	Secure Operating Systems	3
CYB 750	Offensive Security and Threat Management	3
Total Credits		**9**

Governance & Leadership Concentration (Communication, Management, Policy, Compliance)

Code	Title	Credits
Required Courses		
CYB 755	Security Administration	3
CYB 760	Cybersecurity Leadership and Team Dynamics	3
CYB 765	Cybersecurity Management	3
Total Credits		**9**

Security Architecture Concentration (Systems, Software, Data)

Code	Title	Credits
Select three of the following:		**9**
CYB 770	Security Architecture	
CYB 775	Applied Cryptography	
CYB 780	Software Security	
CYB 785	Cyber Physical System Security	
Total Credits		**9**

University Requirements for Master's Degree Programs

To receive a master's degree from UW-Parkside, students must meet the following minimum requirements (note that individual programs may impose more stringent requirements):

1. Complete at least 30 graduate credits, of which no more than 12 may be transferred from another institution.
2. Have an overall GPA of at least 3.00 for all graduate work taken at UW-Parkside that is applicable to the degree program.
3. Satisfy all requirements of the graduate degree program.

Students may take no more than seven years to complete a degree, beginning with the semester in which they complete their first course as a UW-Parkside degree-seeking graduate student, unless they apply for and receive an extension through the appropriate graduate program. Some programs may impose a shorter time limit. To graduate, students must file a request for graduation. The request form, signed by the student's advisor and filed in the appropriate graduate program office, initiates the final review of the candidate's records. Students also need to apply to graduate with the Office of the Registrar.

Admission to the master of science in cybersecurity program requires:

- Bachelor's degree with, at minimum, a 3.0 undergraduate GPA
- Prerequisite coursework in Introduction to Computer Science—which must include programming content, and prerequisite coursework in Calculus or Statistics

CYB 700 | Fundamentals of Cybersecurity | 3 cr
Introduces fundamental concepts and design principles in cybersecurity. Students will understand what, why and how to protect in the cyberworld. Topics include CIA (Confidentiality, Integrity, and Availability), threats, attacks, defense, least privilege, access control and password management, security policies, critical controls, incident-handling and contingency planning, risk assessment and management.
Prerequisites: Admitted MS-CYB degree seeking students only or program advisor consent on space available basis.
Offered: Yearly.

CYB 703 | Network Security | 3 cr
Examines network architectures, threats and attack surfaces exploited by these threats. Students will look at network traffic inspection, common attacks and defensive techniques encryption, network segmentation, firewalls, application proxies, honeypots, DMZs, monitoring networks using intrusion detection and intrusion prevention systems, and network access control.
Prerequisites: Admitted MS-CYB degree seeking students only or program advisor consent on space available basis.
Offered: Yearly.

CYB 705 | Sociological Aspects of Cybersecurity | 3 cr
Presents the principles of applied sociology that account for the human factors in security systems. Topics include an examination of the human role in cybersecurity, the role of security in the context of an organization, and a special focus on the development and implementation of cybersecurity policies.
Prerequisites: Admitted MS-CYB degree seeking students only or program advisor consent on space available basis.
Offered: Yearly.

CYB 707 | Cybersecurity Program Planning and Implementation | 3 cr
Provides instruction on the process used to develop and maintain appropriate security levels for an organization with a focus on implementing a comprehensive security program, a documented set of security policies, procedures, guidelines, and standards. Topics include security planning, strategies, controls, and metrics for measuring effectiveness.
Prerequisites: CYB 700; admitted MS-CYB degree seeking students only or program advisor consent on space available basis.
Offered: Yearly.

CYB 710 | Introduction to Cryptography | 3 cr

Introduces fundamentals of applied cryptography, including encryption and decryption, symmetric and asymmetric systems, pseudorandom functions, block ciphers, hash functions, common attacks, digital signatures, key exchange, message authentication and public key cryptography. Covers implementation of cryptographic systems in approved programming language, and survey of relevant mathematical concepts, including elementary number theory.
Prerequisites: Admitted MS-CYB degree seeking students only or program advisor consent on space available basis.
Offered: Yearly.

CYB 715 | Managing Security Risk | 3 cr

Covers risk management processes and tools, risk assessment and analysis models, economic and control implications, risk measurement, and the ethics of risk. Students will communicate the technical and management aspects of risk, based on research of their chosen industry, related regulation, recent industry reports, and risk implications to organizations, individuals and the nation.
Prerequisites: Admitted MS-CYB degree seeking students only or program advisor consent on space available basis.
Offered: Yearly.

CYB 720 | Technical Communication for Cybersecurity | 3 cr

Research, organize, and present technical information to audiences with varying goals and technical needs. Emphasis on ethics, critical thinking, listening skills, and feedback to develop effective Messages utilizing verbal and nonverbal communication strategies and visual aids. Individual and group presentations and projects will emulate professional scenarios in cybersecurity.
Prerequisites: Prerequisites: Admitted MS-CYB degree seeking students only or program advisor consent on space available basis.
Offered: Yearly.

CYB 725 | Computer Forensics and Investigations | 3 cr

Provides instructions on the investigative and forensics processes of digital evidence with a focus on identifying indicators of compromise, the use of common forensic tools, and the preservation of forensics tools. Topics include forensics iconology, and the analysis of disk, memory, chip-off, mobile device, and OS artifacts.
Prerequisites: CYB 703; admitted MS-CYB degree seeking students only or program advisor consent on space available basis.
Offered: Yearly.

CYB 730 | Computer Criminology | 3 cr

A primer on modern criminology with specific attention to the aspects of technology that facilitate criminal behaviors. Topics include computer crime laws, criminological theories of computer crime, court room and evidentiary procedure, idiographic and nomothetic digital profiling, computer crime victimology, habit/authorship attribution, stylometry, and case linkage analysis.
Prerequisites: Admitted MS-CYB degree seeking students only or program advisor consent on space available basis.
Offered: Yearly.

CYB 735 | Network Forensics | 3 cr

Covers protocol analysis, identification of malicious behavior in systems, and forensic investigations through event log aggregation, correlation and analysis. Students will analyze clips of wired and wireless network protocol analysis to discern methods of attacks and malicious activities.
Prerequisites: CYB 703; admitted MS-CYB degree seeking students only or program advisor consent on space available basis.
Offered: Yearly.

CYB 740 | Incident Response and Remediation | 3 cr

Students will learn about the phases of an incident response system, and the use of IDS and forensics, dealing with false alarms and the remediation process to minimize business impact, plan business continuity, and work with law enforcement, auditors, insurance, and compliance in how to prevent future incidents.
Prerequisites: Admitted MS-CYB degree seeking students only or program advisor consent on space available basis.
Offered: Yearly.

CYB 745 | Secure Operating Systems | 3 cr

Covers operating systems security infrastructure. Topics include, for a given operating system (Windows/Linux), updates and patches, access controls and account management, configuration management, hardening and securing services, and the use of scripting languages to automate security management. Additional topics may include auditing and forensics, virtualization and cloud computing.
Prerequisites: Admitted MS-CYB degree seeking students only or program advisor consent on space available basis.
Offered: Yearly.

CYB 750 | Offensive Security and Threat Management | 3 cr

Covers active defenses such as penetration testing, log management, hacking, threat management and system posturing. Students completing this course will have an understanding of, and the ability to preemptively secure computer and network resources by utilizing information about threats, actors and attack vectors and the ethics behind using this data.
Prerequisites: CYB 700, CYB 703; admitted MS-CYB degree seeking students only or program advisor consent on space available basis.
Offered: Yearly.

CYB 755 | Security Administration | 3 cr

Covers the policy and governance aspects of security. Topics include application of security policies, standards, procedures and guidelines to administration of IT and communications, assessment of compliance including contractual, legal, industry standard, privacy and regulatory requirements, and implementation of security audits and assessment of security performance and security policy-efficacy.
Prerequisites: Admitted MS-CYB degree seeking students only or program advisor consent on space available basis.
Offered: Yearly.

CYB 760 | Cybersecurity Leadership and Team Dynamics | 3 cr

Focuses on leadership best practices and the interpersonal processes and structural characteristics that influence the effectiveness of teams. Emphasis will be placed on leadership models, principles of team building, group dynamics, problem solving, and crisis management in cybersecurity issues. Course will include case studies of modern security incidents.
Prerequisites: Admitted MS-CYB degree seeking students only or program advisor consent on space available basis.
Offered: Yearly.

CYB 765 | Cybersecurity Management | 3 cr

Covers management of cybersecurity policies and strategies at the organizational, national, and transnational levels. Examines the implications of key domestic and international regulations and changes in information technology and communications on security operations. Includes development of organizational security preparation, processes, and responses, and developing a disaster recovery program.
Prerequisites: Admitted MS-CYB degree seeking students only or program advisor consent on space available basis.
Offered: Yearly.

CYB 770 | Security Architecture | 3 cr
Focuses on security architectures for the protection of information systems and data. Students completing this course can identify potential vulnerabilities in system architectures and design secure architectures. Topics include common enterprises and security architectures and their key design elements, such as secure cloud computing and virtualization infrastructures.
Prerequisites: CYB 703; admitted MS-CYB degree seeking students only or program advisor consent on space available basis.
Offered: Yearly.

CYB 775 | Applied Cryptography | 3 cr
Provides an in-depth study of modern cryptography. Topics include public key and private key cryptography, types of attacks, cryptanalysis, perfect secrecy, hashing, digital signatures, virtual private networks, and quantum key cryptography. Topics from number theory and discrete probability necessary for understanding current cryptosystems and their security will be covered.
Prerequisites: CYB 710; admitted MS-CYB degree seeking students only or program advisor consent on space available basis.
Offered: Yearly.

CYB 780 | Software Security | 3 cr
Covers the foundations of engineering secure applications, including techniques used to engineer secure software and assess the security of applications. Topics include exploring web vulnerabilities, secure development processes, implementing security features such as secure data storage and transmission, threat modeling, security requirements, code analysis, and penetration testing.
Prerequisites: Admitted MS-CYB degree seeking students only or program advisor consent on space available basis.
Offered: Yearly.

CYB 785 | Cyber Physical System Security | 3 cr
Covers the fundamentals and techniques to design and implement cyber-physical systems. Topics include the architecture of cyber-physical systems, exploiting software vulnerabilities, secure coding, microservices security, cloud services security, reverse engineering, security assessment of cyber-physical systems, and data analytics for security.
Prerequisites: CYB 775; admitted MS-CYB degree seeking students only or program advisor consent on space available basis.
Offered: Yearly.

CYB 789 | Cybersecurity Pre-Capstone | 1 cr
Prepares student for capstone experience. Drawing on skills learned, students will submit a written project proposal -- with organization, timeline, learning objectives, and specific deliverables identified --for faculty approval. This course is a prerequisite for the capstone course.
Prerequisites: CYB 700, CYB 703, CYB 705, CYB 707, CYB 710, CYB 715, and CYB 720; admitted MS-CYB degree seeking students only or program advisor consent on space available basis.
Offered: Yearly.

CYB 790 | Cybersecurity Capstone | 3 cr
Students present project identified in Capstone Preparation and submit a written report plus oral presentation to both faculty and host organization. Students will be assessed on clarity and content of written report and presentation.
Prerequisites: CYB 789; admitted MS-CYB degree seeking students only or program advisor consent on space available basis.
Offered: Yearly.