CST - Cybersecurity Graduate Program

Cybersecurity Program
Director: Jennifer Butler Modaff
4219 Centennial Hall; 608.785.6717
Email: jbutlermodaff@uwlax.edu

uwex.wisconsin.edu/cybersecurity/ (https://uwex.wisconsin.edu/cybersecurity/)
www.uwlax.edu/academics/grad/cybersecurity/ (https://www.uwlax.edu/academics/grad/cybersecurity/)

The Master of Science in Cybersecurity Program is a fully **online** graduate program consisting of 34 credits (seven core courses, three concentration or track courses, a capstone preparation course and a project-based capstone course). The degree program is offered jointly by UW-La Crosse, UW-Green Bay, UW-Oshkosh, UW-Parkside, UW-Platteville, UW-River Falls, UW-Stevens Point, and UW-Superior. This program 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 program will equip students with the skills needed to effectively develop, implement and maintain a digital security strategy within diverse organizations and industry sectors.

In addition, the program offers four unique tracks to assist students in tailoring their coursework to meet their career goals:

- Digital forensics
- Cyber response
- Governance and leadership
- Security architecture

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.

Program length

The Master of Science (M.S.) in Cybersecurity Program is typically a two-year program. The program length is based on how long the required UWL coursework would take to complete for a part-time student taking six credits a term, who does not need to complete any prerequisite coursework. Program length may be extended if students take fewer than six credits per term or due to the requirements of an individual student's plan of coursework, research or capstone project.

Graduate degree

- Cybersecurity - MS (http://catalog.uwlax.edu/graduate/programrequirements/cybersecurity/cybersecurity-ms/)

Courses

CYB 700 Cr.3
Fundamentals of Cybersecurity
This course 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. Consent of department. Offered Fall, Spring, Summer.

CYB 703 Cr.3
Network Security
This course examines network architectures, threats and attack surfaces exploited by these threats. Students will look at network traffic inspection, common attacks and defensive techniques like encryption, network segmentation, firewalls, application proxies, honeypots, DMZs, monitoring networks using intrusion detection and intrusion prevention systems, and network access control. Consent of department. Offered Fall, Spring, Summer.

CYB 705 Cr.3
Sociological Aspects of Cybersecurity
This course 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. Consent of department. Offered Fall, Spring, Summer.

CYB 707 Cr.3
Cybersecurity Program Planning and Implementation
This course 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 the effectiveness. Prerequisite: CYB 700. Consent of department. Offered Fall, Spring, Summer.

CYB 710 Cr.3
Introduction to Cryptography
This course introduces the 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. It covers implementation of cryptographic systems in an approved programming language, and survey of relevant mathematical concepts, including elementary number theory. Consent of department. Offered Fall, Spring, Summer.

CYB 715 Cr.3
Managing Security Risk
This course 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. Consent of department. Offered Fall, Spring, Summer.

CYB 720 Cr.3
Communication in Cybersecurity
Students research, organize, and present technical information to audiences with varying goals and technical needs. There will be an 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. Consent of department. Offered Fall, Spring, Summer.

CYB 725 Cr.3
Computer Forensics and Investigations
This course provides instruction on the investigative and forensics processes of digital evidence with a focus on identifying indicators of compromise, the use of common forensics tools, and the preservation of forensics tools. Topics include forensics iconology, and the analysis of disk, memory, chip-off, mobile device, and OS artifacts. Prerequisite: CYB 700, CYB 703. Consent of department. Offered Fall, Spring, Summer.

CYB 730 Cr.3
Computer Criminology
This course is 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. Consent of department. Offered Fall, Spring, Summer.

CYB 735 Cr.3
Network Forensics
This course 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. Prerequisite: CYB 703. Consent of department. Offered Fall, Spring, Summer.

CYB 740 Cr.3
Incident Response and Remediation
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. Prerequisite: CYB 700, CYB 703, CYB 705, CYB 707, CYB 715, and CYB 720. Consent of department. Offered Fall, Spring, Summer.

CYB 745 Cr.3
Secure Operating Systems
This course 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. Consent of department. Offered Fall, Spring, Summer.

CYB 750 Cr.3
Offensive Security and Threat Management
This course 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. Prerequisite: CYB 700, CYB 703. Consent of department. Offered Fall, Spring, Summer.

CYB 755 Cr.3
Security Administration
This course 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. Prerequisite: CYB 700, CYB 703, CYB 705, CYB 707, CYB 715, and CYB 720. Consent of department. Offered Fall, Spring, Summer.

CYB 760 Cr.3
Cybersecurity Leadership and Team Dynamics
This course 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. Consent of department. Offered Fall, Spring, Summer.

CYB 765 Cr.3
Cybersecurity Management
This course covers the management of cybersecurity policies and strategies at the organizational, national, and transnational levels. It examines the implications of key domestic and international regulations and changes in information technology and communications on security operations. It also includes the development of organizational security preparation, processes, and responses, and developing a disaster recovery program. Prerequisite: CYB 700, CYB 703, CYB 705, CYB 707, CYB 715, and CYB 720. Consent of department. Offered Fall, Spring, Summer.

CYB 770 Cr.3
Security Architecture
This course 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 enterprise and security architectures and their key design elements, such as secure cloud computing and virtualization infrastructures. Prerequisite: CYB 703. Consent of department. Offered Fall, Spring, Summer.

CYB 775 Cr.3
Applied Cryptography
This course 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. Prerequisite: CYB 710. Consent of department. Offered Fall, Spring, Summer.

CYB 780 Cr.3
Software Security
This course covers the foundations of engineering secure applications, including techniques used to engineer secure software and assess the security of applications. Topics include exploiting web vulnerabilities, secure development processes, implementing security features such as secure data storage and transmisson, threat modeling, security requirements, code analysis, and penetration testing. Consent of department. Offered Fall, Spring, Summer.

CYB 785 Cr.3
Cyber Physical System Security
This course 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. Prerequisite: CYB 775. Consent of department. Offered Fall, Spring, Summer.

CYB 789 Cr.1
Cybersecurity Pre-Capstone
This course prepares students for the 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. Prerequisite: CYB 700, CYB 703, CYB 705, CYB 707, CYB 710, CYB 715, CYB 720. Consent of department. Offered Fall, Spring, Summer.

CYB 790 Cr.3
Cybersecurity Capstone
Students present the 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 their written report and presentation. Prerequisite: CYB 789. Consent of department. Offered Fall, Spring, Summer.