Wisconsin Online Collaboratives

Summer 2026

[Request Permission Number](#)
Course Preview Week: May 19 - May 25, 2026
Semester Dates: May 26 - August 07, 2026

Core Courses

CYB 703: Network Security

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.

[CYB 703 Syllabus](#)

CYB 705: Sociological Aspects of Cybersecurity

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.

[CYB 705 Syllabus](#)

CYB 720: Communication in Cybersecurity

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.

[CYB 720 Syllabus](#)

Digital Forensics

CYB 735: Network Forensics

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

[CYB_735_Syllabus](#)

Cyber Response

CYB 745: Secure Operating Systems

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.

[CYB 745 Syllabus](#)

Governance and Leadership

CYB 755: Security Administration

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: CYB 700, CYB 703, CYB 705, CYB 707, CYB 715, CYB 720

[CYB_755_Syllabus](#)

Security Architecture

CYB 780: Software Security

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 transmission, threat modeling, security requirements, code analysis, and penetration testing.

Students may choose to take CYB 780 or CYB 785 to satisfy Security Architecture track requirements.

[CYB 780 Syllabus](#)

CYB 785: Cyber Physical System Security

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.

Students may choose CYB 780 or CYB 785 to satisfy the Security Architecture track requirements.

Prerequisites: CYB 775

[CYB 785 Syllabus](#)