

# CYBERSECURITY (CYB)

---

## **CYB 700 Cybersecurity Fundamentals 3.00**

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.

### **Typically Offered:**

- Fall, Spring, and Summer Terms

## **CYB 703 Network Security 3.00**

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.

### **Typically Offered:**

- Fall, Spring, and Summer Terms

## **CYB 705 Cybersecurity and Society 3.00**

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.

### **Typically Offered:**

- Fall, Spring, and Summer Terms

## **CYB 707 Cybersecurity Planning 3.00**

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.

### **Prerequisites:**

CYB 700 prerequisite

### **Typically Offered:**

- Fall, Spring, and Summer Terms

## **CYB 710 Introductory Cryptography 3.00**

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. Implementation of cryptographic systems in an approved programming language. Survey of relevant mathematical concepts, including elementary number theory.

### **Typically Offered:**

- Fall, Spring, and Summer Terms

## **CYB 715 Managing Security Risk 3.00**

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.

### **Typically Offered:**

- Fall, Spring, and Summer Terms

## **CYB 720 Communication in Cybersecurity 3.00**

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.

### **Typically Offered:**

- Fall, Spring, and Summer Terms

## **CYB 725 Computer Forensics 3.00**

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.

### **Prerequisites:**

Successful completion of CYB 700, 703

### **Typically Offered:**

- Fall, Spring, and Summer Terms

## **CYB 730 Computer Criminology 3.00**

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.

### **Typically Offered:**

- Fall, Spring, and Summer Terms

## **CYB 735 Network Forensics 3.00**

Covers protocol analysis, identification of malicious behavior in systems, and forensic investigations through event log aggregation, correlation and analysis. Students will analyze clips of network protocol analysis to discern methods of attacks and malicious activities. Reviews wired and wireless protocols and cover their associated attacks, with case studies involving protocol analysis, log analysis, and other tools.

### **Prerequisites:**

Successful completion of CYB 703

### **Typically Offered:**

- Fall, Spring, and Summer Terms

**CYB 740 Incident Response and Remediation 3.00**

Addresses how to set up an incident response system in an organization and the phases of an IR: Preparation, Identification, Notification, Containment, and Eradication of the threat actors, and Recovery and Reporting to prevent future incidents. Students will learn about 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.

**Prerequisites:**

Successful completion of CYB 700, 703, 705, 707, 715, 720

**Typically Offered:**

- Fall, Spring, and Summer Terms

**CYB 745 Secure Operating Systems 3.00**

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.

**Typically Offered:**

- Fall, Spring, and Summer Terms

**CYB 750 Offensive Security 3.00**

This course includes 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:**

Successful completion of CYB 700, 703

**Typically Offered:**

- Fall, Spring, and Summer Terms

**CYB 755 Security Administration 3.00**

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:**

Successful completion of CYB 700, 703, 705, 707, 715, 720

**Typically Offered:**

- Fall, Spring, and Summer Terms

**CYB 760 Leadership & Teams 3.00**

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.

**Typically Offered:**

- Fall, Spring, and Summer Terms

**CYB 765 Cybersecurity Management 3.00**

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:**

Successful completion of CYB 700, 703, 705, 707, 715, 720

**Typically Offered:**

- Fall, Spring, and Summer Terms

**CYB 770 Security Architecture 3.00**

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.

**Prerequisites:**

Successful completion of CYB 703

**Typically Offered:**

- Fall, Spring, and Summer Terms

**CYB 775 Applied Cryptography 3.00**

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:**

Successful completion of CYB 710

**Typically Offered:**

- Fall, Spring, and Summer Terms

**CYB 780 Software Security 3.00**

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.

**Typically Offered:**

- Fall, Spring, and Summer Terms

**CYB 785 Cyber-Physical Sys. Security 3.00**

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:**

Successful completion of CYB 775

**Typically Offered:**

- Fall, Spring, and Summer Terms

**CYB 789 Cybersecurity Pre-capstone 1.00**

Prepares student for capstone experience. Draws 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 pre-requisite for the capstone course.

**Prerequisites:**

Completion of CORE courses CYB 700, 703, 705, 707, 710, 715, 720, 725, 730, 740, 745, 750, 755, 760, 765, 770, 775, 780, 785

**Typically Offered:**

- Fall, Spring, and Summer Terms

**CYB 790 Cybersecurity Capstone 3.00**

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:**

Successful completion of CYB 789

**Typically Offered:**

- Fall, Spring, and Summer Terms