CYBERSECURITY (CYB)

**CYB 501. Foundations of Cyber Security.** 1 Credit.
This course introduces students to fundamental security principles and security defense. Students learn the concepts of information security risks, vulnerabilities, assets and threats.
**Offered:** Every year, Fall and Spring

**CYB 502. Introduction to Cyber Threats.** 1 Credit.
This course introduces students to the analysis of cyber threats. Students learn to identify bad actors in cyberspace and assess their resources, capabilities, techniques and motivations. Students learn to describe different types of cyber attacks and their characteristics.
**Corequisites:** Take CYB 501.
**Offered:** Every year, Fall and Spring

**CYB 503. Introduction to Cyber Defense.** 1 Credit.
Students learn about cyber defense tools and techniques. This course covers how to apply cyber defense tools and techniques to prepare a system to repel attacks.
**Corequisites:** Take CYB 502.
**Offered:** Every year, Fall and Spring

**CYB 506. Introduction to Programming for Security Professionals.** 1 Credit.
This course introduces students to basic scripting and programming concepts needed for security defense. Course topics include writing scripts for Windows and Linux; understanding basic programming security concepts; basic programming constructs, such as variables, types, loops, functions and data structures.
**Offered:** Every year, Summer

**CYB 509. Operating Systems Security.** 1 Credit.
This course introduces students to operating systems and the software to support these systems. Topics include operating system security configuration, control objectives, control maintenance and forensics. The course includes hands-on implementation of security controls, including access management, file and process security configuration, and security monitoring.
**Offered:** Every year, Spring

**CYB 517. Introduction to Cryptography.** 1 Credit.
This course introduces students to cryptography algorithms, protocols and applications. Topics include history, applications, such as SSL and SSH; and protocols, such as hash functions, symmetric and asymmetric cryptography, and attack-vectors for systems.
**Offered:** Every year, Spring

**CYB 524. Relational Database Security.** 1 Credit.
This course introduces students to different relational database management systems (DMS) and DMS security concerns and methods. Topics covered include hashing and encryption, database access controls, unauthorized access, data corruption and injection.
**Offered:** Every year, Spring

**CYB 526. Non-Relational Database Security.** 1 Credit.
This course introduces students to the theory, application and security of nonrelational database systems. It focuses on data management, query and security aspects of nonrelational databases. Topics include a comparison between relational and nonrelational database models, NoSQL storage types for different databases such as MongoDB, Hadoop, Amazon DynamoDB, document-based databases and graph databases.
**Corequisites:** Take CYB 524;
**Offered:** Every year, Spring

**CYB 540. Introduction to Secure Networking.** 1 Credit.
This course introduces students to the theoretical and practical aspects of designing, developing and defending computer networks. Topics include network models, media, architectures, devices, protocols, services, applications and use of network security tools.
**Offered:** Every year, Spring

**CYB 550. Cyber Policy.** 3 Credits.
There are three parts to this course. The first part covers the applicable federal and state laws and policies related to cyber defense, pertaining to the storage and transmission of data. In the second part, students analyze and develop enterprise security policies. Finally, students learn how to implement machine security policies.
**Corequisites:** Take CYB 503.
**Offered:** Every year, Fall and Summer

**CYB 610. Hands-on HIPAA Compliance Risk Management.** 1 Credit.
This course introduces students to the HIPAA Privacy, Security and Breach Notification Regulations. The focus is on regulations and compliance. Students will be able to assess the HIPAA privacy, security and breach notification compliance of their own organizations or a model healthcare organization described within the course. Students will get hands-on experience using cloud-based security and privacy assessment tools.
**Prerequisites:** Rising senior status minimum. Previous exposure to health organizations necessary, either through academic course work or professional work.
**Offered:** Every year, Summer

**CYB 611. Hands-On HIPAA Security Risk Analysis and Risk Management.** 1 Credit.
This course will teach the theory and practice of Enterprise Cybersecurity Risk Management. The focus will be on risks associated with healthcare organizations. These risks go beyond compliance risks and include risks related to safeguarding the exploding quantities of healthcare data, systems, and devices. Students will learn best practices for risk analysis, what the Office for Civil Rights demands in a risk analysis and will conduct a risk analysis of a model healthcare organization created for the course. Students will get hands-on experience using cloud-based risk analysis tools.
**Prerequisites:** Rising senior status minimum. Previous exposure to health organizations necessary, either through academic course work or professional work.
**Offered:** Every year, Summer

**CYB 612. Enterprise Cybersecurity Risk Management in Healthcare.** 1 Credit.
This course will cover what it takes to establish, implement, and mature an Enterprise Cybersecurity Risk Management (ECRM) program. ECRM is a part of enterprise risk management and supports the business needs and mission of the organization. We will cover case studies of healthcare organizations and how they did or did not secure their health information. Lessons learned from actual breach events will be discussed along with lessons learned from organizations with effective ECRM programs. Students will learn how to organize for effective security defense including: governance, people, process, technology, and engagement. Students will get hands-on experience using cloud-based risk management tools.
**Prerequisites:** Rising senior status minimum. Previous exposure to health organizations necessary, either through academic course work or professional work.
**Offered:** Every year, Summer
Offered: Every year, Summer
Corequisites: Take CYB 506.

CYB 665. Workforce Access Security. 1 Credit.
This course focuses on authentication and user access technologies and practices within the enterprise. Topics include Active Directory services and architecture, and enterprise network access protocols.
Offered: Every year, Fall

CYB 670. IoT Security. 1 Credit.
This course covers security as it pertains to embedded devices, embodied by the growth of the Internet of Things (IoT). Students learn about the specific security issues related to embedded devices, including Linux malware, DDoS attacks, botnets, cryptography and personal privacy.
Corequisites: Take CYB 526.
Offered: Every year, Spring

CYB 682. Securing Workloads in Azure. 1 Credit.
This course covers concepts and practices for securing Azure workloads. Students are introduced to security controls, such as access controls using IAM, logging and auditing, and other AWS security services.
Corequisites: Take CYB 680.
Offered: Every year, Fall

CYB 683. Resilient System Design and Development. 1 Credit.
This course introduces students to the concepts of secure system design and cyber resilience. The content of this course includes best security processes recommended in NIST 800-160 and techniques and technologies needed for secure system design and development.
Prerequisites: Take CYB 680.
Offered: Every year, Spring

CYB 685. Operating Resilient Systems. 1 Credit.
This course includes hands-on experience with tools for security activities such as intrusion detection and cloud security monitoring. Other topics this course covers include Site Reliability Engineering (SRE), maintaining situational awareness and dynamic threat.
Corequisites: Take CYB 684.
Offered: Every year, Spring
CYB 691. MS Cybersecurity Capstone.  3 Credits.
This capstone course is designed to enable students to directly utilize what has been learned in the tools and applications courses in order to analyze and offer solutions for a major cybersecurity challenge. A definition of the problem, analysis of options and a comprehensive presentation of findings and solutions are required components of the course.

Prerequisites: Permission of the Program Director.
Offered: Every year, Spring and Summer