CYBERSECURITY (CYS)

CYS 167. Introduction to Cybersecurity. 3 Credit Hours.
This course introduces cybersecurity and the NIST Framework from three different perspectives: technology, societal dynamics in cybercrime, and policy and law. Cybersecurity principles including confidentiality, integrity and availability as well as assurance, authenticity and anonymity are demonstrated via examples from each perspective. Students gain awareness of the broad scope of cybersecurity through readings, discussions, and hands-on exercises.

CYS 203. Communicating Connections. 1 Credit Hour.
This practicum will allow participants to learn and apply professional communication practices in order to explore and develop connections to professional industry experts. Students will prepare a plan for accessing discovered industry-related contacts, develop and practice interview techniques, create questions for informational interviews, reach out to potential contacts, and ultimately, pursue vocational goals by connecting with industry experts. Participants will practice for and execute phone, email, and written communication to establish professional, industry-related connections in order to complete informational interviews. From the resulting interviews, students will reflect, explore, prepare and pursue determined vocational goals. Throughout the six classes, industry experts will be invited as guests to offer professional acumen and insights for students pursuing opportunities to further connect to potential careers. Pass/fail only. Open to all majors.
Cross-listed Courses: CMM 203, PSF 203, ENI 203, CSC 203, BUS 203

CYS 263. Introduction to Cybersecurity Risk and Protection Strategies. 3 Credit Hours.
This course focuses on cyber risks faced by individuals and organizations, and protection mechanisms to mitigate these risks. Examples are used to demonstrate risks posed by data at rest, data in use, and data in transit. This course will cover statistical models of risk, different risk assessment strategies (including the NIST 800 series) and methods of protecting information systems and data from unauthorized access and use. The strengths and limitation of protection mechanisms will be discussed, and will include access control, encryption, credentialing, operational policies and procedures, and risk mitigation policies (e.g., password update policy, least privilege). Students will get hands on experience on risk assessment and protection mechanisms.

CYS 269. Introduction to Detection, Response, & Recovery Strategies. 3 Credit Hours.
This course covers detection mechanisms that focus on identifying abnormal versus normal behaviors, and response and recovery actions based on a detected cybersecurity incident. The strengths and limitations of detection mechanisms will be discussed, and will include detecting abnormal behavior, performing continuous monitoring, and analyzing data from multiple sources. response and recovery planning and implementation of these plans will be discussed. Students will get hands-on experience on protection mechanisms, and response and recovery planning.

CYS 331. Network Security. 3 Credit Hours.
This course will provide students an in-depth look into principles of network security and protection strategies. Students will learn how different threats and attacks work, and how to defend against these through both case studies and hands-on labs. Students will also learn how different technologies work that are related to network security such as: firewalls, VPN, IDS/IPS, and more. Students will come away from this class with a technical and theoretical understanding of how to best secure a network.
Prerequisite: CYS 263 or CYS 269.

CYS 337. Scripting for Cybersecurity. 3 Credit Hours.
Students will learn to implement scripts to automate cybersecurity functions of protection and detection using python and linux shell. Detection related applications include system administration tasks, firewall maintenance, scanning log files, malware development and detection. Protection related applications include encryption, signatures, hash functions, access control mechanisms, authentication, and database account management statements (e.g., grant, revoke).
Prerequisites: CYS 167, CYS 263 or CYS 269, and CYS 175.

CYS 347. System and Software Security. 3 Credit Hours.
This course gives an introduction to secure administration of operating systems and software. Common vulnerabilities, their associated attacks and current defenses in systems and software are discussed. Students are introduced to penetration testing and other means of detecting vulnerabilities. Students also learn system administration skills for managing configurations (hardware and software), accounts, access control, firewalls, ports, patches and virtual machines and to create simple scripts. Both Linux/Unix and Windows operating systems are discussed.
Prerequisites: CYS 263 or CYS 269.

CYS 390. Cybersecurity Independent Study. 1-9 Credit Hours.
A student who wishes to pursue an independent study project for academic credit must submit, prior to registration, a proposed plan of study that includes the topic to be studied and goal to be achieved, the methodology to be followed, schedule of supervision, end product, evaluation procedure and number of credits sought. The proposal must be approved by the supervising faculty member, the department chair and the academic dean. It will be kept on file in the academic dean's office.

CYS 421. Ethical Hacking and Digital Forensics. 3 Credit Hours.
This course focuses on ethical hacking and digital forensics. It will provide a deeper understanding of how malicious actors think by studying real world case studies and performing hands-on activities. Tools commonly used by hackers will be discussed, with students learning methods on how to defend against these types of attacks. In addition, digital forensic analysis is also discussed. This will provide students an in-depth look at the process of digital forensics and give them hands-on opportunities to perform forensics.
Prerequisites: CYS 331 or CYS 347.

CYS 431. Security Architecture. 3 Credit Hours.
This course will give students the ability to apply the concepts and technologies learned in the cybersecurity program. Students are able to apply best practices to build and maintain a defensible security architecture. Students will setup and apply security best practices on a network of their own design. The class will also provide hands-on opportunities for students to test their designs by providing a capture-the-flag like exercise.
Prerequisite: CYS 331 and CYS 347.

CYS 490. Cybersecurity Internship. 1-12 Credit Hours.
A service learning course where students complete CISRM identified projects or an internship.
Prerequisite: Junior or Senior level standing.

CYS 499. Honors Project in Cybersecurity. 3 Credit Hours.
This course must be completed by those cybersecurity majors seeking to qualify for a Departmental Honors degree in cybersecurity. The student conducts an independent study honors project under the guidance of at least one faculty member in the program. Prior to registration for this course, a student must submit a proposal and have it approved by the department chair. A student may propose a research project culminating in a research paper or a hands-on project culminating in artifacts which describe the results of the project.
Prerequisite: Senior Standing.